Víctor Luke*

Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas.

Cyber Security and International Public Law In The XXI Century

Resumen

Perfeccionar nuestro Estado de Derecho implica una clara definición de las atribuciones y responsabilidades que las fuerzas armadas poseen a fin de proteger los activos estratégicos claves para el desarrollo de nuestra sociedad en el siglo XXI. Es razonable asumir que la protección de la infraestructura informática que permite el exitoso funcionamiento de las sociedades de la información, quede entregada al menos en parte a la Defensa Nacional.

Sin embargo, no existe un conjunto coherente de normas jurídicas que permitan a un Estado defender de manera legítima aquel tipo de activos frente a una agresión externa ejecutada mediante armas informáticas.

Junto con ofrecer una reseña de las particularidades de la seguridad informática, se explican los actuales esfuerzos de la doctrina jurídica internacional por establecer un marco legal coherente y eficaz sobre la materia. Asimismo, se describen las dificultades que presenta la interpretación y en especial, la aplicación analógica de las normas vigentes a las peculiaridades de la ciberguerra.

Esta breve investigación aborda desde una perspectiva jurídica las atribuciones, derechos y obligaciones de los Estados frente a la protección de su infraestructura informática, considerada como uno de los activos claves para su desarrollo exitoso en la era de la información.

** Abogado de Gabinete, Subsecretaría de Justicia, Ministerio de Justicia (2011) Consultor Empresas IT y Seguridad Informática.*

Palabras Clave

Seguridad Informática – Derecho Internacional – Infraestructura Informática – Marco Legal – Ciber Guerra

Abstract

Upgrading the standards of our State of Law implies an accurate establishment of the duties and powers held by the armed forces in order to protect the key strategic assets that will enable the further development of our society in the XXI century. Reasonably, the protection of the information infrastructure which enables the successful functioning of information societies could be assumed, at least in part by the National Defense. Notwithstanding, there is no coherent body of legal norms that allows States to legitimately defend that sort of assets against foreign aggression executed by cyber weapons.

This paper offers a brief introduction to Information security along with an explanation of the current efforts of the international law experts in order to establish a coherent and effective legal frame on the subject. Likewise, it describes the difficulties of interpretation and, specially, the analogous application of the current norms of International Public Law to the peculiar nature of cyber warfare.

From a legal perspective, this brief investigation address the duties, rights and liabilities of the States regarding the protection of information infrastructure, considering the latter as a key asset for future development of societies in the information age.

Key words

Information security – International Law – Cyber warfare – Information Age – Legal Frame

1. Introducción

En el ámbito del quehacer intelectual la ambición por teorías revolucionarias parece ser desmedida y es fácil identificar a "la impaciencia académica por el progreso como el factor causante del enunciado fácil de teorías seductoras e impactantes"[1]. Teniendo esta precaución como presupuesto, este trabajo admite a la vez, que nuestras ideas de Estado y soberanía, no poseen una esencia invariable o deslindes conceptuales

[1] Ortiz, *El Estudio de las Relaciones Internacionales,* Fondo de Cultura Económica, Santiago, p. 53.

permanentes. Es la indeterminación de estos conceptos lo que permite admitir que la realidad política, económica y tecnológica pueda modificar nuestra forma de concebir el ejercicio del poder público y reevaluar los medios con que este debe ser desplegado.

En el debate contemporáneo sobre teoría política es posible identificar dos polos extremos en cuanto a la situación actual del Estado. El primero de ellos se caracteriza por manifestar una "ansia excesiva por declarar la muerte del Estado"[2]. El polo opuesto sigue concibiendo al Estado como el ente sobre el cual gravitan tanto las relaciones internacionales como el ejercicio del poder público en un contexto nacional y global. Desde luego, ambas posiciones son extremas. Quienes sugieren que la figura del Estado va de salida, parecen ignorar que "los principales Estados siguen siendo los actores más destacados en el escenario internacional, y el ideal de intervención humanitaria no ha sido invocado todavía para desafiar la soberanía de ningún Estado poderoso. Lo que es más, tales Estados siguen siendo, con mucho, los actores más importantes dentro de sus propios territorios"[3]. En el sentido opuesto, la defensa de un punto de vista estrictamente estatista parece ignorar de forma casi negligente "la aparición de corporaciones multinacionales y otras agencias que, al controlar la inversión y el empleo, fuerzan a los Estados individuales a dar cabida a sus demandas aun cuando éstas puedan estar en conflicto con las prioridades sociales y económicas de dichos Estados"[4]. Asimismo, una postura excesivamente estatista ignora el creciente robustecimiento de un concepto global de derechos humanos y con ello, desconoce la posibilidad de que algunos organismos internacionales, como la Corte Europea de Derechos Humanos, "para asegurar tales derechos, puede permitirse interferir, con fuerza militar si fuese necesario, en las disposiciones internas de Estados supuestamente soberanos"[5].

Sea que el Estado se encuentre en franco declive y caída, sea que el Estado continúe siendo el ente más poderoso de la esfera pública, deberá acomodarse a las lógicas y fuerzas que modelarán la vida en sociedad en el siglo XXI. Estos ajustes no sólo se deberán hacer en un nivel conceptual, reevaluando las múltiples ideas de Estado que coexisten en nuestra herencia intelectual, sino también desde un punto de vista práctico, reconsiderando la forma en que el Estado ejerce su poder, los activos que debe proteger y los medios que para ello utiliza.

Una de las más potentes fuerzas modeladoras del siglo XXI son las tecnologías de la información[6]. La adopción de estas tecnologías como medios a través de los cuales el Estado podrá ejercer su poder, prestar sus servicios y desplegar sus funciones será sin dudas, una variable importante en el perfeccionamiento del Estado de Derecho. Asimismo, el potencial que estas tecnologías ofrecen para solucionar problemas prácticos de la democracia es enorme. En este sentido, los vicios y limitantes a que está afecta la representación política ofrecida por partidos políticos abiertamente no representativos

2 Skinner, Una Genealogía del Estado moderno, Escuela de Gobierno Universidad Adolfo Ibáñez, Santiago, p. 49.
3 *Ibíd.*
4 *Ibíd.*, p. 48.
5 *Ibíd.*
6 En adelante, se abrevia "tecnologías de la Información" por TI.

y antidemocráticos, podrán ser subsanados a través de la implementación de soluciones informáticas, que eliminen todo *bypass* antidemocrático, entre las decisiones públicas y la voluntad de los individuos obligados por ellas.

Sin embargo, las tecnologías de la información no sólo prometen eventuales soluciones y beneficios para la esfera pública. La creciente dependencia de las sociedades contemporáneas en complejos sistemas de información crea un gran flanco de vulnerabilidad. A este respecto la ciberguerra se erige, no ya como un peligro extrapolado desde la ciencia ficción, sino como una amenaza real contra la seguridad de los Estados. Es en este sentido que los presupuestos de este trabajo cobran relevancia: La reevaluación de las normas y conceptos jurídicos es forzosa cuando tales normas y conceptos no logran dar cuenta de la realidad. No obstante, el producto de dicha reevaluación no debe ser una mera ambición de progreso, sino sólo constituir un pequeño paso útil hacia la comprensión de las consecuencias jurídicas de un fenómeno que cuesta encasillar eficazmente con las herramientas ya existentes.

En tal dirección, este trabajo expone la disfuncionalidad de la noción física del objeto sobre el cual recae la soberanía, noción sobre la cual se erige el Derecho Internacional y que influye directamente en el concepto de Conflicto armado regulado por el Derecho de Guerra. Esta breve investigación ofrece una introducción a uno de los tantos estimulantes desafíos que la sociedad de la información impondrá a las ciencias del Derecho. Dicho desafío consiste en abordar desde una perspectiva jurídica las atribuciones, derechos y obligaciones de los Estados frente a la protección de su infraestructura informática, considerada como uno de los activos claves para su desarrollo exitoso en la era de la información.

2. Sociedad de la información y activos estratégicos.

Es un hecho innegable que hoy, a comienzos del siglo XXI, la información se ha convertido en uno de los activos más valiosos tanto para las empresas privadas como para la sociedad en su conjunto. Su manipulación, transacción, almacenamiento y producción ya no es sólo información contenida en la mente de expertos ni en obras académicas. En una enorme medida, la información que permite a una sociedad contemporánea desenvolverse de forma eficiente se compone de datos informáticos, de códigos numéricos que al ser procesados por un computador, se traducen en la ejecución de tareas.

Fundada o no, es pretensión del Estado[7] de Chile el alcanzar la categoría de país desarrollado para fines de la segunda década del siglo XXI. La modernización necesaria para adquirir dicha categoría, implica una creciente dependencia tecnológica. "Dado al incremento en velocidad y eficiencia de las redes y sistemas informáticos, el suministro de insumos militares y cadenas logísticas ha sido automatizado; agencias

[7] Este trabajo no pretende hacerse cargo de la afirmación de que un Estado logre tener una intención, más allá de representar una determinada agenda de gobierno. Al respecto ver, *Authority in the Modern State*, de Harold Laski.

gubernamentales de emergencia confían crecientemente en procesos electrónicos; y servicios económicos críticos han migrado hacia tecnologías que dependen de protocolos de internet."[8] En esta dirección, Chile avanza a paso firme y sostenido. Ejemplo de ello es la modernización del servicio de impuestos internos, que a través del desarrollo de una plataforma informática líder en la región, se suma al boom mundial de lo que se conoce como *e–government.* La modernización de dicho servicio, a través de la creación de una infraestructura informática que multiplicó la eficiencia de la administración fiscal nacional, permite admitir razonablemente, que los objetivos de desarrollo y modernización que Chile se ha propuesto pueden llegar a concretarse en un plazo de 15 a 20 años.

Sin embargo, para ello es necesaria la gradual creación de plataformas informáticas que contemplen no sólo el desempeño de un servicio determinado, sino el simultáneo actuar de todo el Estado. El satisfactorio funcionamiento de una sociedad moderna supone el eficiente desempeño de una serie de elementos tangibles e intangibles denominada *infraestructura crítica*. Esta es un complejo sistema compuesto de mecanismos, servicios, agencias, entes y bienes presentes en un país e incluso, dependiente de factores y elementos ubicados fuera de sus fronteras físicas. Esto hace de la *infraestructura crítica* una compleja red, cuyo comportamiento es difícil analizar y más aún, prever. Con el fin de establecer un marco teórico que permita analizar las amenazas y riesgos a que la infraestructura crítica de un país es vulnerable, la teoría de redes y la teoría de sistemas complejos, emergen como modelos de análisis adecuados[9].

Frente al abstruso concepto de Infraestructura crítica y habiendo constatado su extrema sensibilidad a factores difícilmente controlables por el actuar del gobierno, tras los hechos ocurridos en Nueva York el 11 de septiembre de 2001, el Congreso de los Estados Unidos de Norteamérica aprobó la denominada USA PATRIOT Act. En ella se definió legalmente el concepto de *infraestructura crítica* como "los sistemas y activos, sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de tales sistemas y activos tendría un debilitador impacto en la seguridad, en la seguridad económica nacional, en el sistema nacional de salud pública o cualquier combinación de tales aspectos."[10] Si bien no hay consenso sobre cuáles son los sistemas y activos que conforman la infraestructura crítica, hay claridad sobre el papel que juegan las tecnologías de la información e Internet como red conectora de este sistema.

Podemos concluir que no obstante el número y la identidad de los elementos que conforman la infraestructura crítica de un país pueden ser indeterminados, arbitrarios o al menos variables, la red que los vincula debe ser objeto de especial protección. La teoría de redes justifica esto precisamente, en que el correcto funcionamiento del siste-

[8] Kramer, *Cyberpower and National Security*, National Defense University Press, Washington, p. 543.

[9] Sin embargo, dichas teorías no han permeado en las capas de análisis propios de la creación de políticas públicas ni menos al debate legislativo, permaneciendo aún como herramientas experimentales propias de las ciencias informáticas y neurobiológicas. Al respecto ver, Cilliers, Paul; *Complexity and Postmodernism: Understanding Complex Systems*, Routledge, 1998.

[10] Kramer, *Cyberpower and National Security*, National Defense University Press, Washington, p. 544.

ma es más importante que la autosuficiencia de cada uno de sus elementos. Evidencia recabada a través del estudio de sistemas complejos, sugiere que la forma más eficaz de garantizar la sobrevivencia y disminuir la vulnerabilidad de una red compleja, es interconectando de mayor y mejor forma cada uno de los elementos que la conforman[11]. Así, la infraestructura informática que subyace a una sociedad desarrollada y permite su eficiente despliegue, es un activo de sumo valor y el presupuesto práctico de su existencia[12]. Por tanto, toda red que permita y garantice la eficiente y segura interconexión de la estructura crítica de un país, es un activo estratégico, tanto comercial, como institucionalmente. Desde el punto de vista de la defensa y la inteligencia, un activo de esta importancia es, desde luego, relevante para la seguridad del Estado.

Ahora, es razonable preguntarnos por qué atañe a la Defensa Nacional la protección de la infraestructura informática de un país. La razón básica de ello es que la dependencia tecnológica abre un flanco de vulnerabilidad de enorme envergadura para todo el Estado. Esa vulnerabilidad se acentúa debido a la consolidación de la ciberguerra como una amenaza real a la seguridad de los Estados en el siglo XXI. "El peligro de un ciberataque es en la actualidad ampliamente reconocido por las sociedades avanzadas, las cuales son completamente dependientes de redes computacionales tanto para el funcionamiento del día a día como para la defensa nacional"[13]. La protección que por parte de la defensa tuvieron puertos y carreteras desde principios del siglo XIX, se justificó por ser aquellos los elementos esenciales del desarrollo industrial del país. Hoy, el desarrollo de una sociedad moderna no requiere de la implementación, conservación y protección de medios exclusivamente físicos que permitan el intercambio de mercancías, el desarrollo industrial y la prestación de servicios. También es necesaria la protección de aquellos "medios electrónicos, que sin ocupar un espacio físico, constituyen el terreno a través del que fluye una creciente cantidad de datos que incluso pueden controlar procesos físicos"[14]. Es sobre tales medios electrónicos, que la ciberguerra y las armas informáticas dirigen su amenaza.

Las defensas apropiadas para este tipo de amenazas no son las armas convencionales, sino las informáticas. "Esta vulnerabilidad de las fuerzas armadas y de las sociedades modernas a los medios de la guerra informática debe ser tratada con las defensas

[11] Una red está compuesta básicamente de nodos y flujos de información. Los nodos producen, reciben y transportan información. La mayor o menor distribución de los flujos de información entre los distintos nodos le da a una red robustez y resistencia. Cuando una red, ajeno a la cantidad de nodos que posea, depende de unos pocos nodos que acaparan gran parte de la información del sistema, la red se torna vulnerable. Si se daña o pierde uno de esos nodos densos, el sistema completo no tiene la capacidad de suplir su pérdida y desempeñar su función. En cambio, cuando los flujos de información involucran a una gran cantidad de sus nodos (a través de muchas conexiones que distribuyen el peso en toda la red), el sistema se torna flexible. Ello le permite adaptarse y suplir la falta de uno de sus nodos. Al respecto ver Albert, Rèka; *Statistical Mechanics of Complex Systems*, Reviews of Modern Physics 74, 2002.

[12] Tal interconexión es la causa de la sociedad de la información, no su consecuencia. De ello se puede concluir que es más importante proteger aquello que permite la interconexión de sus elementos, que a los elementos interconectados.

[13] Neewsweek Magazine, Britain Biggest Security Threat.

[14] Carr, *Inside Cyberwarfare*, O'reilly, Cambridge, p. 40.

apropiadas"[15]. En este sentido, continuar concibiendo a la defensa nacional como una fuerza basada en la posesión de medios disuasivos de carácter físico es mantener una actitud anacrónica. Esto cobra especial relevancia frente a la aparición de amenazas que utilizan armas inmateriales, que se valen de defensas inéditas y que se despliegan en un campo de batalla virtual.

La seguridad de la infraestructura informática de un país no es una cuestión privada, sino pública pues involucra a todo el sistema y no sólo al desempeño de cada uno de sus elementos. El exponencial incremento en la dependencia de sistemas computacionales y de redes de comunicación para todo, desde operaciones gubernamentales hasta la completa infraestructura financiera, médica, de transportes, de servicios públicos y otros sistemas que determinan el efectivo desenvolvimiento de las sociedades modernas pone en peligro no sólo los resultados comerciales de las compañías privadas que los utilizan sino el funcionamiento de la sociedad en su conjunto. La interdependencia en los flujos de información entre compañías privadas, servicios públicos y órganos del Estado, pone en riesgo a todo el país, hasta el punto de poder inhabilitarlo si varios de ellos son atacados de forma conjunta. Una afirmación de esta naturaleza podría sonar exagerada de no existir evidencia concreta que la avale. El hecho es que ya no es una mera posibilidad que un ataque cibernético pueda comprometer la seguridad de todo un país. En este sentido, la literatura contemporánea sobre ciberseguridad ya cita como un caso emblemático el ataque informático sufrido por Estonia a mediados del año 2007, más aún hoy, que el desarrollo tecnológico logrado en sólo cuatro años permite, en teoría, desplegar ataques mucho más sofisticados y dañinos.

Si bien es válido el argumento de que Chile aún no posee una infraestructura informática crítica que justifique la inclusión de la ciberguerra y la seguridad informática como desafíos nacionales de Defensa, es un hecho que nuestro país necesita adquirir tal infraestructura como requisito previo para alcanzar la categoría de país desarrollado. Esperar al momento en que se adquiere un bien, para luego deliberar sobre la forma de protegerlo, es una lógica irresponsable y miope. En este sentido, es conveniente poner en perspectiva la suma prioridad que a estos temas le han otorgado otras potencias que ya gozan la categoría de países desarrollados, precisamente por el hecho de reconocer que se encuentran "en un estado deplorablemente inadecuado para hacerse cargo de esta creciente amenaza"[16]. Así por ejemplo, a fines del año 2010, el Consejo de Seguridad Nacional del Reino Unido emitió en su reporte anual la decisión de establecer a la ciberguerra como primera prioridad de seguridad nacional[17]. A principios del año 2010, la administración de Barack Obama también otorgó el carácter de alta prioridad al

15 Binnendijk, *Protecting Cyberspace; Transforming America's Military*, National Defense University Press, Washington, p. 331.

16 Newsweek Magazine, Britain's Biggest Security Threat.

17 No sólo se le ha otorgado la categoría de prioridad nacional al comprometer US$760 millones para su implementación, sino que tal medida está acompañada de un recorte presupuestario que implicará la reducción de personal (7000 personas a lo largo de 5 años) así como la reducción de un 40 por ciento en el presupuesto para tanques y artillería pesada. Al respecto, ver Reporte Anual 2009 – 2010 del Consejo de Seguridad Nacional del Reino Unido.

diseño de una estrategia coherente respecto a la ciberseguridad[18]. "La OTAN considera la amenaza de la ciberguerra de forma tan seria que aprobó un reporte especial sobre el tema durante su asamblea parlamentaria en octubre de 2009"[19]. Estas son muestras claras de una tendencia mundial, que un país que busca alcanzar el desarrollo en un corto plazo no puede ignorar. Es esencial no sólo la creación de una masa crítica que pueda debatir sobre este tema y su importancia para el Estado sino también la adopción de una política nacional de formación de expertos que logre satisfacer esta necesidad. Los avances tecnológicos se suceden con tal velocidad, que limitar el análisis de estos temas a un mero quehacer teórico sin tomar medidas prácticas al respecto significa la pérdida de uno de los activos más valiosos desde el punto de vista de la defensa: tiempo.

Sin embargo, contrastando la aparente premura con que estos desafíos deben ser asumidos, es forzoso considerar que el Estado, sea a través de sus fuerzas armadas u otro organismo, debe sujetar su actuar a las restricciones constitucionales que delimitan sus atribuciones. Aludir a circunstancias de vulnerabilidad o tiempos de emergencia para atribuir al Estado poderes desmedidos con el fin de protegerse a sí mismo no puede fundarse sino en argumentos populistas o teorías absolutistas del poder político. "Si hay una crisis nacional genuina, debe existir un buen argumento para decir que la persona cuya vida es más urgente salvar es la persona del Estado"[20]. Asimismo, es esencial comprender que hoy, la defensa debe satisfacer una serie de expectativas que van más allá de sólo desempeñar de forma eficaz labores estrictamente militares. En este sentido equilibrar transparencia, seguridad y modernización es uno de sus más arduos desafíos.

Frente a estos desafíos, la inversión en capital humano en materia de ciencia y tecnologías de la información va de la mano con el objetivo país de alcanzar el estatus de desarrollo. De tal forma asumir este desafío como una oportunidad y no sólo como una nueva amenaza, es un curso de acción prudente, incluso para quienes consideran que Chile aún no depende de las tecnologías de la información de forma tan importante. Dicha carencia actual no es motivo para relegar la preparación del contingente militar especializado a un último lugar de la tabla de prioridades, sino por el contrario, se debe aprovechar este breve lapso de tiempo, para invertir en la capacitación y experticia, que permitan proteger aquel estado de desarrollo que el país pretende alcanzar en menos de 20 años.

El veterano general Maginot logró a fines de la primera guerra mundial convencer a Francia de construir una línea de fortificación a lo largo de toda la frontera con Alemania e Italia, asumiendo que las futuras amenazas a la seguridad de su nación obedecerían a la misma lógica de aquellas batallas que había experimentado en carne propia: la guerra de trincheras. Aquí, la cuestión no es determinar si Chile se verá expuesto a una ciberguerra dentro de los próximos 10 años. La cuestión a tener en

[18] Neewsweek Magazine, Cyberwar is Hell.
[19] Newsweek Magazine, The Evil (Cyber) Empire.
[20] Skinner, Una Genealogía del Estado moderno, Escuela de Gobierno Universidad Adolfo Ibáñez, Santiago, p. 53.

cuenta es que los conflictos inevitablemente se producirán y que uno de los frentes en los cuales se librarán será el cibernético. Frente a tal posibilidad, un país que busca alcanzar el desarrollo a través de una imprescindible modernización tecnológica, no puede pretender defender con tanques y fusiles aquellos blancos que sólo pueden ser atacados con medios informáticos. Conservar el énfasis en la adquisición exclusiva de armas convencionales o en el desarrollo de destrezas de combate que impliquen músculo y sudor de soldados, es una política centrada en las necesidades de antaño y por tanto, una estrategia tan riesgosa como la que justificó la construcción de la tristemente famosa línea Maginot[21].

3. Ciberguerra: el Derecho de Guerra frente a una nueva forma de guerra asimétrica.

La reticencia, no sólo de los académicos del Derecho, sino de todas las ramas del quehacer científico, a salirse de los parámetros y lógicas inherentes a su propia área de conocimientos es una actitud con un futuro poco auspicioso. "Nuevas realidades, como la revolución de las comunicaciones o la expansión de la tecnología y el conocimiento, han traído consigo nuevas formas de vida, movimientos migratorios y estilos universalmente aceptados que barren fronteras estatales o las relativizan. La vida internacional, como ocurre por lo demás en la relación de la realidad con cualquier otra rama del Derecho, se ha modificado tan profunda y vertiginosamente que la norma jurídica no da cuenta de ella en propiedad, al menos a ese ritmo..."[22]. Frente al análisis de sistemas complejos, como las redes neuronales, los sistemas informáticos, las relaciones internacionales, una aproximación interdisciplinaria es forzosa.

La vinculación de dos materias que a priori pueden parecer tan disímiles como el Derecho y la Informática deben necesariamente dialogar a fin de lograr soluciones aplicables a la realidad del siglo XXI. Este diálogo debe recaer sobre un creciente número de áreas en donde la tecnología y el Derecho se influencian, restringen y superponen recíprocamente[23]. Una de estas áreas es la de los conflictos bélicos. La

[21] Esta estrategia no es sólo riesgosa desde el punto de vista estratégico, sino también desde una perspectiva presupuestaria. Bajo esta lógica, China ha decidido invertir en la formación de un pequeño pero sofisticado ejército de hackers, en vez gastar recursos en la obtención de medios de combate convencional de segunda mano que jamás podrá competir con el arsenal bélico de EEUU. Con este objetivo en mente es que "ha creado una estructura de reserva especializada en computación, capaces de emplear armas electrónicas y de información para alcanzar a un adversario en otro continente. Asimismo, el Ejército de liberación Nacional ha incorporado tácticas de guerra cibernética en ejercicios militares y ha creado escuelas que se especializan en la guerra informática". Al respecto ver *Ciberguerra y ciberterrorismo ¿realidad o ficción? Un nueva forma de de guerra asimétrica*, en Dos décadas de posguerra fría: actas de las I jornadas de estudios de seguridad de la comunidad de estudios de seguridad General Gutiérrez Mellado.

[22] Ortiz, El Estudio de las Relaciones Internacionales, Fondo de Cultura Económica, Santiago, p. 41.

[23] En cuanto a la seguridad informática el énfasis, no sólo en Chile sino en el mundo, ha recaído sobre la protección de datos personales y el cibercrimen, relegando la discusión sobre la responsabilidad que a privados y entes públicos cabe en la seguridad de la infraestructura informática del país, a un quehacer teórico. Debido a ello, la seguridad informática es un nicho de mercado celosamente resguardado por las grandes empresas contratistas

guerra es una actividad humana presente desde los inicios de nuestra civilización. De hecho, el desarrollo tecnológico de una sociedad y la guerra han avanzado de la mano desde la edad de piedra hasta hoy.

La repetición inmemorial de un conjunto de prácticas y costumbres vinculadas con la forma en que la guerra debía llevarse a cabo dieron lugar a una primitivo cuerpo de normas jurídicas internacionales, muchas de ellas constituyentes del antiguo *corpus iuris gentium.* No fue sino hasta entrado en la modernidad que se comenzó a regular la guerra a través de la creación de pactos y tratados. "Entre el siglo XIX y la primera mitad del XX, ese derecho ha seguido un proceso de codificación parcial por medio de diversos instrumentos, en especial de las convenciones de Ginebra y de La Haya."[24] De este modo, la regulación jurídica internacional conocida como Derecho de Guerra, es producto de una lenta destilación de costumbres, acuerdos y decisiones de tribunales internacionales cuyo básico presupuesto consiste en concebir los conflictos armados como fenómenos desplegados en el mundo físico. El mismo concepto de arma utilizado en este conjunto de normas, involucra la idea de instrumentos kinéticos utilizados para atacar o defenderse, cuyos efectos son percibidos por los sentidos y producidos contra objetos corpóreos a través de medios físicos. Desde luego, una bayoneta perforando el pulmón de un soldado de infantería encaja dentro de tal concepto. Asimismo, la inhalación de agentes químicos como el Napalm, producen en el cuerpo de la víctima efectos materiales evidentes. Bombardeos aéreos por saturación, envenenamiento o corte de suministros de agua, destrucción de torres y redes eléctricas son también medios cuya utilización, legítima o ilegítima, encajan dentro de los conceptos de arma y conflicto armado del Derecho de Guerra.

Sin embargo, la irrupción de la electrónica y la informática en el ámbito bélico obliga a efectuar algunas piruetas intelectuales a la hora de someter su utilización o abuso a las normas del Derecho de Guerra. "El progreso tecnológico y la invención de nuevas armas, son más rápidos que el desarrollo del derecho y su codificación. Sin embargo, en los llamados casos no regulados los beligerantes no tienen absoluta libertad de acción."[25]

La necesidad de llevar a cabo un análisis sobre la legitimidad o ilegitimidad de los nuevos mecanismos ofensivos y defensivos de la ciberguerra, no es un mero capricho intelectual. Lo que justifica este análisis es que la violación de las normas que regulan

de defensa. No obstante, confiar en los productos y servicios de seguridad informática parece estar siendo una tendencia sometida a revisión en muchos Estados, principalmente debido a la falta de confianza que un número creciente de ataques informáticos sufridos por estas empresas han generado en la población y en las autoridades. Ejemplo de ello, son los ataques informáticos sufridos durante el año 2011 por la consultora Hamilton Booz Allen, encargada, irónicamente, de la seguridad informática de gran parte del departamento de Defensa de Estados Unidos o el masivo robo de información clasificada sufrido por Mitsubishi Heavy Industries, uno de los más importantes contratistas de defensa de Japón. Si bien, los errores y fallas en la prestación de tales servicios conllevan asociadas altas multas para los contratistas de seguridad informática, es difícil cuantificar y establecer en cláusulas contractuales montos que logren compensar monetariamente ataques cuya sofisticación comprometa la seguridad de todo el Estado. Más aún, la sensibilidad del sistema financiero global a las expectativas de confianza que brindan los mercados ha hecho reevaluar al prestigio como uno de los activos más importantes de un Estado.

[24] Sorensen, *Manual de Derecho Internacional Público*, Fondo de Cultura Económica, Mexico D.F., p. 734

[25] *Ibíd.*

la forma en que los Estados pueden hacer uso de la fuerza en el contexto internacional, muchas veces implica un costo mayor que el beneficio obtenido a través de ella. Para aquellos Estados cuyas fortalezas no se basan en su arsenal bélico ni en su poder económico sino en su prestigio, el respeto del Derecho Internacional es un factor de suma relevancia. Por ello, el costo de llevar a cabo acciones u omisiones que puedan considerarse como un uso ilegal de la fuerza (o tan sólo una ilegítima amenaza de su uso), puede ser sumamente alto en términos de prestigio internacional. Frente a este hecho y considerando que Chile mantiene una política exterior que otorga alta importancia al prestigio, un conocimiento acabado del marco jurídico internacional que lo protege y obliga frente a las amenazas a la seguridad propias del siglo XXI, es esencial.

El problema emerge al tratar de aplicar las normas de dicho marco jurídico a la ciberguerra. Subsumir normas que fueron creadas para aplicarse a acciones y objetos con existencia corpórea, a una realidad compuesta de cosas inmateriales genera problemas que la interpretación analógica no siempre logra resolver. Las armas informáticas sólo consisten en información, en pulsos eléctricos organizados bajo códigos lógicos que expresados en un lenguaje matemático pueden traducirse en órdenes ejecutables por un computador[26]. Asimismo, estas armas tienen como blanco otros códigos, otros sistemas de información, cosas que aun siendo inmateriales permiten en una creciente medida, el efectivo desempeño de toda una sociedad.

Las particularidades de este tipo de armas generan una serie de interrogantes desde el punto de vista jurídico. Por ejemplo, surge la duda sobre si se puede concebir como agresión una acción que no ha implicado el traspaso de fronteras físicas protegidas por la soberanía de un Estado, ni la movilización de tropas, ni la muerte de soldados o civiles en el Estado víctima del ataque, ni la destrucción de bienes físicos como edificios, represas o caminos. Asimismo, es objeto de debate determinar si un ataque informático que logra causar un perjuicio físico o económico de carácter sustancial en el Estado Víctima, justifica o no, desde el punto de vista del Derecho Internacional, una respuesta armada de este o la responsabilidad de aquel.

4. Derecho Internacional y regulación jurídica de la ciberguerra.

Como se ha mencionado a la largo de este trabajo, la ciberguerra no sólo se presenta como un desafío estratégico para el Estado, sino también un desafío jurídico. En E.E.U.U., a principios del año 2010, líderes del Pentágono fueron reunidos en una

[26] Aparentemente es redundante afirmar que las armas informáticas consisten puramente en información. Sin embargo, ello permite hacer hincapié en el hecho de que tales armas no son el medio físico en que están contenidas, no son los computadores, los cables o el hardware que permiten su transporte, ejecución o inteligencia. Las armas informáticas son, en esencia una creación intelectual. De ello emanan grandes dificultades a la hora de intentar homologar la regulación existente sobre producción de armas nucleares o de destrucción masiva a los procesos de creación propios de las armas informáticas. Estas dificultades serán abordadas más adelante.

sala de simulación a fin de conocer la forma en que responderían a un sofisticado ataque informático dirigido a paralizar las fuentes de energía del país, los medios de comunicación nacional y las redes financieras. Los resultados de la simulación fueron desalentadores. Ninguno de ellos pudo detectar el país desde donde se originó el ataque y por tanto, toda estrategia de represalia carecía de su objetivo básico, a saber, un Estado contra el cual dirigirse. Tampoco se logró establecer un protocolo para evitar la propagación de los daños ocasionados, pues los flancos de ataque eran impredecibles y la estrategia utilizada para destruir los distintos objetivos no respondía a un patrón táctico reconocible. Más aún, los comandantes militares involucrados notaron que carecían de la autoridad legal para responder al ataque, especialmente porque nunca quedó claro si él fue un acto de vandalismo, un intento de espionaje comercial o una operación apoyada por un Estado con el objeto de aturdir a los Estados Unidos, quizás como preludio a una guerra convencional[27]. Frente a un ciberataque, las herramientas que el Derecho de Guerra ofrece a los Estados para hacer uso legítimo de su fuerza pierden eficacia. Si bien la facultad de un Estado para defenderse de una agresión externa está regulada tanto por la costumbre jurídica internacional como por los tratados internacionales que versan sobre la materia, en especial las normas del Derecho Internacional de La Haya, no existe un marco normativo que regule completa, aislada y coherentemente las facultades, derechos y obligaciones que los Estados tienen frente a la Ciberguerra[28]. Más aun, el vacío existente en esta materia es difícil de llenar a través de la aplicación analógica de normas que fueron creadas pensando en armas convencionales que debían aplicarse en el mundo físico. Los mismos conceptos de territorio, fronteras, soberanía, actos de guerra, agresión y en especial, la idea de atribución e imputación de responsabilidad, sobre los cuales se erige el Derecho Internacional, ven desdibujados sus contornos, debido a la naturaleza sui generis del contexto en que se desarrolla la ciberguerra y a las complejas características técnicas de las armas informáticas.

Frente a este vacío legal la doctrina internacional se encuentra dividida, coexistiendo diversas propuestas sobre cuál sería el conjunto de normas vigentes que podría servir más eficazmente como marco desde el cual proyectar un sistema que regule esta materia. Estas propuestas pretenden extrapolar las normas pertenecientes a cuatro ámbitos distintos del Derecho Internacional. La primera propone a los tratados de no proliferación de armas nucleares como sistema idóneo para dicho fin. Las segunda, sugiere como idóneas a las normas del tratado antártico y las del Derecho del espacio debido a la similitud entre las características del ciberespacio y la vastedad y desregulación imperante en ambos escenarios. La tercera, propone las normas de la Convención de las Naciones Unidas sobre Derecho de los Tratados del Mar (UNCLOS) también de-

[27] Lo sorprendente de esta operación de simulación es que fue la versión de un ataque idénticamente perpetrado meses antes contra la compañía Google, tras el cual, ejecutivos de la compañía, lograron rastrear como fuente de origen a 7 servidores taiwaneses con huellas rastreables hasta territorio físico chino. Al respecto ver, The New York Times, *CyberWar; in Digital Combat, U.S. finds no easy deterrent.*

[28] De hecho, ningún tratado internacional vigente sobre la materia establece una definición legal de "acto de agresión cibernética" ni tampoco una definición de "ciberguerra". Toda referencia actual a "actos de agresión" alude exclusivamente a conflictos armados con medios convencionales. Al respecto ver *From Nuclear War to Net War: Analogizing Cyber Attacks in International* Law en Berkeley Journal Of International Law, vol. 25 nº 3.

bido a la similitud en cuanto a la vastedad del objeto sobre el cual recaen sus normas. Finalmente, una línea de pensamiento sugiere la extrapolación de las lógicas presentes en las normas vigentes sobre Acuerdos de Asistencia Legal Mutua (MALT).

Sin embargo, todas estas propuestas terminan chocando con mayor o menor violencia contra la pared que imponen las particulares de la Ciberguerra. "Los tratados sobre no proliferación de armas nucleares están diseñados para limitar la propagación de armas nucleares en sus primeras etapas de desarrollo"[29]. La eficacia de estos tratados se basa en que la producción y comercialización de los componentes utilizados en la creación de estas armas es fuertemente vigilada y monitoreada por un gran número de agencias internacionales. Sin embargo, a diferencia de los elementos necesarios para la creación de armas de destrucción masiva, los componentes de la guerra informática son sumamente fáciles de conseguir y a un costo insuperablemente menor, todo lo cual elimina la efectividad de toda propuesta regulatoria análoga a la de los tratados de no proliferación de armas de destrucción masiva.

Respecto a la posibilidad de extrapolar normas análogas a las contenidas en el tratado antártico, peculiaridades propias de las tecnologías de la información hacen inviable una homologación de criterios. En efecto, se intenta establecer que el uso de internet por parte de las fuerzas armadas se rija por las mismas limitantes impuestas a las bases militares ubicadas en dicho continente. Dicha limitante consiste en utilizar estas bases militares sólo con fines científicos o propósitos pacíficos. "Esto no se podría analogar a la ciberguerra, pues al ser las armas informáticas meros códigos, es imposible distinguir entre aquellos utilizados para fines pacíficos y aquellos utilizados para fines maliciosos"[30].

En cuanto al derecho del espacio como marco desde donde fundar una regulación para la ciberguerra, tampoco sería el más indicado pues se basan en supuestos opuestos: sólo unos pocos países del mundo tienen la capacidad para llevar a cabo acciones militares en el espacio, "en cambio más de 120 naciones tienen la habilidad de librar guerras en el ciberespacio"[31].

Las normas del Tratado del Mar, parecen tener incluso menos potencial que las antedichas, ya que el intento de su aplicación analógica por parte de las Naciones Unidas a objeto de regular los requisitos exigibles a las transferencias tecnológicas, ha recibido un sistemático rechazo por parte de Estados Unidos, Alemania y el Reino Unido. Si no sirvió para regular una materia como aquella, menos servirá para regular una materia donde el papel del desarrollo tecnológico es tan controversial como en la ciberguerra.

Finalmente se sugiere establecer un marco regulatorio internacional que aborde a la ciberguerra a través de acuerdos de asistencia y cooperación mutua. No obstante, en esta última opción los argumentos estrictamente jurídicos parecen perder fuerza frente a intereses de otra índole. En esta materia, no es posible abstraerse de las presiones

[29] Carr, *Inside Cyberwarfare*, O'reilly, Cambridge, p. 32.
[30] *Ibíd.*, p. 33.
[31] *Ibíd.*

políticas, muchas veces antagónicas, ejercidas por aquellas potencias que mayor interés han demostrado en regular jurídicamente la ciberguerra. A modo de ejemplo, E.E.U.U. se ha manifestado partidario de incentivar la cooperación internacional a través de tratados bilaterales y multilaterales de extradición y persecución conjunta del cibercrimen. Por su parte, Rusia, se ha opuesto a estas iniciativas, proponiendo la creación de tratados que regulen la proliferación de armas informáticas de forma análoga a la existente respecto a armas de destrucción masiva. "Aunque la razón aquí expresada [por Rusia] se basa en consideraciones de soberanía nacional y de no interferencia, dicha posición también protege un activo estratégico clave del arsenal cibernético ruso: su propia población de hackers patrióticos altamente educados, quienes están más que dispuestos a pelear por parte de su país en los dominios del ciberespacio."[32]

Todas las propuestas mencionadas hasta ahora son sólo aproximaciones hipotéticas sobre cómo debería regularse la ciberguerra. Mientras tal regulación no exista, los Estados deberán valerse del Derecho vigente. Frente a este conjunto de normas no hay claridad sobre cómo y cuándo pueden los Estados víctimas reaccionar frente a ciberataques ni sobre cómo o por qué podría perseguirse la responsabilidad de los Estados agresores. Parte de la doctrina ha propuesto estrategias legales que permitan un uso legítimo de la fuerza frente a dicha hipótesis y que sólo se sirven del Derecho Internacional vigente. Sin embargo, todas estas propuestas asumen que el Derecho de Guerra se desarrolló sobre la base de guerras convencionales libradas entre Estados en el plano físico y por tanto existe una serie de dificultades que deben ser sorteadas satisfactoriamente antes de admitir la viabilidad de dichas proposiciones.

La breve extensión de este ensayo no permite abordar dichas dificultades con mayor profundidad. Nos limitamos a mencionar que básicamente, estas se derivan, en primer lugar, de la dificultad de establecer si frente a un ataque informático se está bajo las normas del Jus ad Bellum, es decir las normas del Derecho de Guerra que durante la paz permiten a un Estado reaccionar a través del uso de la fuerza o bien, bajo las normas del Jus in Bello, aquellas normas que regulan la forma en que la guerra, una vez comenzada, debe librarse. La velocidad con que las operaciones bélicas de la ciberguerra se pueden desplegar y la dificultad técnica que implica determinar el origen de tales ataques, deja poco tiempo a los asesores legales para llevar a cabo este primer análisis. En segundo lugar, resulta sumamente difícil establecer si un ciberataque logra calificar como un "uso de la fuerza" prohibido por el Derecho Internacional. Como mencionamos el concepto de arma y la noción de conflicto armado que impregna al Derecho Internacional se basa en elementos kinéticos y fue con base en la utilización de este tipo de medios que se construyó toda la regulación jurídica internacional atingente a la materia. Frente a esta problemática, se distinguen dos escuelas de pensamiento: una que resta toda "importancia a los medios con que se lleva a cabo el ataque y se concentra en la cantidad de los daños provocados"[33] y otra que afirma que "cualquier

[32] *Ibíd. 35.*

[33] Kramer, *Cyberpower and National Security,* National Defense University Press, Washington, p. 525.

cosa distinta a un ataque armado –algo como la amenaza de tanques cruzando la frontera que la carta (de las Naciones Unidas) tuvo por objeto regular– no está prohibida por el Derecho internacional"[34].

Las propuestas de la doctrina jurídica internacional, en orden a adecuar el Derecho Internacional vigente a los particulares desafíos que impone la ciberguerra, conducen sus soluciones por dos vías distintas. La primera, busca homologar los ciberataques a ataques armados convencionales; la segunda, intenta reconducir estas agresiones hacia conductas típicas de la ley penal doméstica del país víctima[35].

La primera de las vías mencionadas en el párrafo anterior, intenta homologar los ataques informáticos a la figura de un conflicto armado convencional, con el objeto de justificar dos cosas: primero, la respuesta que a través del uso de la fuerza pueda dar el Estado víctima y segundo, la responsabilidad del Estado desde donde se produjo el ataque.

Respecto a la justificación que permite a un Estado Víctima hacer uso de la fuerza es imprescindible mencionar que el Derecho Internacional establece la prohibición general del uso (o de la amenaza del uso) de la fuerza contra otros Estados[36]. Esta prohibición general sólo admite dos excepciones[37] y la tradicional interpretación restrictiva de ellas, es el primer problema que se erige al intentar homologar estas normas a los ataques informáticos. La primera excepción a la prohibición del uso de la fuerza es la autorización del Consejo de Seguridad de las Naciones Unidas para hacer uso de ella con el fin de restablecer la paz y la seguridad internacional. La segunda excepción, es la legítima defensa del Estado, frente a toda forma de ataque contra su integridad territorial o independencia política.

Justificar una respuesta armada ante un ataque informático basándose en la primera excepción, a saber, la autorización del Consejo de Seguridad, es difícil puesto que la posibilidad de reaccionar a través del uso de la fuerza con el objeto de "restaurar la paz y la seguridad internacional" asume que tal reacción pondrá fin a una situación de violencia actual. En el caso de las operaciones informáticas, las agresiones, si se puede calificar con ese nombre a la irrupción, destrucción o bloqueo de sistemas de información, son llevadas a cabo en cuestión de minutos y todo indica que tal velocidad seguirá incrementándose. En este sentido, la movilización de ejércitos y arsenal bélico convencional contra el Estado agresor sería un gasto de recursos y energías carente de un objetivo justificable, más aún si como consecuencia del ataque informático, el país víctima no ha sufrido daños materiales. Cabe mencionar que la autorización

[34] Ibíd., p. 526.

[35] Este trabajo no se referirá a esta segundo grupo de argumentos pues ello implica abordar no sólo la forma en que el Derecho Penal Especial se hace cargo del cibercrimen, el crimen organizado y la responsabilidad penal de las personas jurídicas, sino también cómo la parte general de esta rama del derecho debe adecuar sus categorías y supuestos a la utilización de las armas informáticas. La complejidad de estas materias justifica una investigación aislada.

[36] Esta prohibición está contenida en el artículo 2(4) de la Carta de las Naciones Unidas.

[37] Ver Artículos 39, 41, 42 y 51 de la Carta de las Naciones Unidas.

del Consejo se justifica en el restablecimiento de la paz y la seguridad. Ello excluye la posibilidad de que el Estado víctima movilice a su defensa con el objeto de invadir, destruir o sitiar al Estado responsable como forma de represalia.

Justificarse en la segunda excepción es también difícil ya que la defensa propia se gatilla frente a un "ataque armado". Este concepto, como se ha señalado, denota una acción llevada a cabo en el plano físico, a través de medios materiales. Asimismo, la legítima defensa se justifica frente a un ataque dirigido contra "la integridad territorial o la independencia política" de un Estado. La precisión en cuanto a los blancos atacados que las armas informáticas ofrecen, alcanza niveles de sofisticación sin precedentes. "Se ha producido una evolución desde la guerra total a la guerra limitada, tanto por objetivos perseguidos como por el escenario, la duración y las capacidades envueltas"[38]. Por ello es posible, teóricamente, el diseño de un ataque que sólo busque destruir la capacidad competitiva de una potencia enemiga en una determinada área del mercado, dejando intacta su integridad territorial y su independencia política. Este grado de sofisticación y la creciente importancia de activos no físicos, frustra los objetivos de las normas del Derecho Internacional, en general, y del Derecho de Guerra, en particular, al construir una legislación que protege bienes estrictamente materiales, cuyo valor parece ir en declive. Concebir que los únicos bienes que pueden ser puestos en riesgo a través de un ataque armado sean la integridad territorial y la independencia política, demuestra una anacrónica concepción de los activos esenciales de una sociedad moderna.

Finalmente, la doctrina internacional que aboga por homologar los ataques informáticos a los ataques armados convencionales, ha propuesto algunas estrategias jurídicas que permiten justificar en el derecho internacional vigente la responsabilidad del Estado Agresor. Sin embargo, hasta ahora la mayoría de los ataques informáticos que han sido perpetrados contra objetivos nacionales y admitidos[39] por los países víctimas, demuestran que el diseño de las estrategias, la creación de las armas y la ejecución de las operaciones, han sido orquestadas por actores no estatales. Este hecho constituye una gran barrera jurídica contra la posibilidad de amparar la defensa de los Estados en las normas del Derecho de Guerra, pues el agresor no es un Estado. Perseguir la responsabilidad de este por un hecho sólo atribuible a un privado ubicado en su territorio violaría un principio jurídico básico de la responsabilidad internacional de los Estados, en función del cual "la conducta de actores privados –sean entidades o personas naturales– no es atribuible al Estado, a menos que este directa y explícitamente haya delegado parte de sus tareas y funciones a un actor privado."[40] Frente a este obstáculo, una parte de la doctrina internacional argumenta a favor de la posibilidad de atribuir responsabilidad a los Estados donde se ubiquen los actores no estatales que produjeron

[38] Ministerio de Defensa de Chile, Libro Blanco de la Defensa; El Marco Internacional de la Defensa, Santiago, p. 80.

[39] Por ejemplo, Korea del Sur el 4 de julio de 2009, Irán el 14 de junio del 2009, Tartaristán en junio del mismo año, Estados Unidos el 21 de abril de 2009 y entre el 4 y el 6 de julio de 2009, Kirguistán el 18 de enero de 2009, Israel y Zimbawe en diciembre de 2008. Ver The Legal Status of Cyber Warfare, en Inside Cyber Warfare. P. 34–38.

[40] Carr, Inside Cyberwarfare, O'reilly, Cambridge, p. 32.

y efectuaron el ataque, aludiendo a que el estricto paradigma que establece el principio aludido se ha hecho mucho más flexible.

Dicha argumentación se refuerza hoy, por la aprobación de las resoluciones 1368 y 1373 del Consejo de Seguridad de la ONU, que permitieron a Estados Unidos ejercer su derecho a la defensa propia contra Afganistán, no obstante los ataques del 9/11 habían sido perpetrados por Al Qaeda[41], un agente no estatal[42].

Otra parte de la doctrina construye una argumentación basada en la obligación legal de los Estados a aplicar la debida diligencia en la prevención de la comisión, dentro de su territorio, de actos criminales en contra de otros países o de su población[43]. Existiendo así una serie de deberes entre Estados, el tolerar la ejecución de ciberataques desde su territorio hacia objetivos de otro Estado constituiría de suyo, un crimen desde la perspectiva del Derecho Internacional. También en este sentido, La Corte Internacional de Justicia declaró en el Corfu Channel Case respecto a los límites al ejercicio de la soberanía, que es "obligación de todo Estado no permitir, con su conocimiento, que su territorio sea utilizado en actos contrarios a los derechos de otros Estados"[44]. De este modo, tras verificarse el lugar físico desde donde se generó un ciberataque, podrían justificarse represalias en contra de ese Estado, basándose en el hecho de que dicho país, aun cuando no haya tenido el "control directo" de las operaciones y ni siquiera el "control general" de ellas, habría tolerado su ejecución.

5. Conclusión.

Aparentemente, el énfasis de la política exterior está centrado en ubicar a Chile como un socio comercial exitoso, confiable y atractivo. Frente a dicha lógica, la preocupación sobre seguridad nacional, espionaje y en definitiva, la admisibilidad de la existencia de conflictos armados, podría parecer descontextualizada, injustificada, o un simple

41 Estas resoluciones permitieron a E.E.U.U. actuar amparados en el artículo 51 de la Carta de la ONU, reconociendo su legítimo derecho a la autodefensa, no obstante haber podido fundar su resolución en el artículo 42 del mismo cuerpo legal. Al respecto ver http://www.un.org/Docs/scres/2001/sc2001.htm

42 Esta resolución cristaliza el cambio de paradigma desde el "control directo" hacia la "responsabilidad indirecta" de los Estados huéspedes. Esta tendencia ya se había manifestado incipientemente en el caso Tadic, cuando el Tribunal Internacional para la ExYugoslavia demostró una significante relajación respecto del estándar exigido a un Estado para poder responsabilizarlo por actos cometidos por actores no estatales cuando aquel tiene al menos un "control general" sobre las operaciones de estos, sin ser ya necesario "el control directo" de aquellas. Este razonamiento relajó la exigencia de que el Estado sólo era responsable por el actuar de sus agentes calificados, sus órganos o instituciones.

43 Dicha obligación jurídica sería un principio general del Derecho Internacional ampliamente aceptado. También habrían Judicial Opinions en este sentido, como las ofrecidas en el Corfu Channel Case y el Caso Tellini, donde se sostuvo que puede perseguirse la responsabilidad del Estado en aquellos casos en que estos han abandonado todas las medidas razonables para prevenir la comisión de crímenes y todo esfuerzo por perseguir, arrestar y presentar ante la justicia a los criminales. Asimismo, se ha plasmado esta obligación en declaraciones de la Asamblea General Unidas como la Declaración sobre Relaciones Amistosas de 1970, la Declaración sobre Medidas para Eliminar el Terrorrismo de 1994 o la Declaración sobre fortalecimiento de la Seguridad Internacional. Al respecto ver Responding to International Cyber Attacks as Acts of War, en Inside Cyber Warfare.

44 Sorensen, Manual de Derecho Internacional Público, Fondo de Cultura Económica, México D.F., p. 318.

resabio de las obsesiones propias de la guerra fría. "Sin embargo, dado el dinamismo de los entornos internacionales, la incertidumbre continúa siendo un componente de las condiciones en que el mundo evoluciona. Del mismo modo, el conflicto armado, en todas sus formas, permanece presente en el mundo."[45] Dicho de otro modo, desarrollarse a través de las lógicas del mercado y del comercio internacional es un curso de acción eficaz, pero también es prudente modernizar los medios que permitan proteger el desarrollo alcanzado mediante tales mecanismos.

Sin duda, estas materias serán parte relevante del debate jurídico internacional del siglo XXI, debate que incluso deberá evaluar la noción física de los activos, bienes y valores sobre los cuales el Estado puede o debe ejercer su soberanía. No obstante ello, la viabilidad de las teorías jurídicas esbozadas en este trabajo están supeditadas a la superación de las limitaciones técnicas que impone esta nueva forma de guerra. Asimismo, la innovación y la misma producción del arsenal bélico propio de la guerra informática, está regido por una lógica inédita, pues a diferencia del proceso de fabricación de armas convencionales, los límites impuestos por la producción industrial desaparecen, y la creatividad humana se erige como la materia prima casi exclusiva de nuevas herramientas informáticas. Por ello es que la inversión en capital humano es tan importante para un país que pretende competir como país desarrollado, en un plazo de 20 años.

Es de esperar que la recién promulgada ley 20.420 permita la inclusión de estas materias en el debate nacional sobre Defensa y logre, mediante la labor de la Subsecretaría de Defensa, el cometido propuesto en su artículo 15 letra b), actualizando y proponiendo una apreciación de los riesgos y amenazas que efectivamente deberá encarar nuestro país a lo largo del siglo XXI.

Bibliografía

Libros

CLARKE, R. (2010). *Cyberwar; the next threat to national security and what to do about it* (1ª ed.). Estados Unidos: HarperCollins Publishers.

CARR, J. (2010), *Inside Cyber Warfare* (1ª ed.). Estados Unidos: O'reilly media.

KRAMER, F.; Starr. S.; Wetz, L.; (2009). *Cyberpower and National Security* (1ª ed.). Estados Unidos, National Defense University Press.

DIRECCIÓN DE INTELIGENCIA DEL EJÉRCITO (2002). MEMORIAL DEL EJÉRCITO DE CHILE, *La Ciberguerra,* Santiago.

[45] Ministerio de Defensa de Chile, Libro Blanco de la Defensa; El Marco Internacional de la Defensa, Santiago, p. 77.

BINNENDIJK, H. (2002). *Transforming America's Military* (1ª ed.) National Defense University Press.

SORENSEN, M. (2010). *Manual de Derecho Internacional Público* (11ª edición). México: Fondo de Cultura Económica.

Capítulo de libro con editor/es o compilador/es

SÁNCHEZ MEDERO, Gema. *Ciberguerra y Ciberterrorismo ¿realidad o ficción? una nueva forma de guerra asimétrica.* En: Amérigo Cuervo–Arango, comp. y Peñaranda Algar, Julio, comp. Dos décadas de posguerra fría: actas de las I jornadas de estudios de seguridad de la comunidad de estudios de seguridad General Gutiérrez Mellado. Madrid, Instituto Universitario General Gutiérrez Mellado, 2009. pp. 215–241.

THE JOURNEY AHEAD, Security in the Information Age, En: Alberts, D.; Garstka, J. y Stein, F. Network Centric Warfare, Washington D.C., 1999, pp. 224-240.

Artículo de revista científica

SAN PERLO, F.; Sköns, E. (2008, septiembre). Sipri Insights on Peace and Security, *The Private Military Services Industry*. Volumen nº 2008/1.

SHACKLEFORD. S. (2009, octubre). *"From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*". En Berkeley Journal Of International Law, vol. 25 nº 3.

Artículo de revista no especializada

NAGORSKI, A. (2010, julio). Newsweek Magazine, *Cyberwar Is Hell.*

MARKOFF, J., Sanger, D.; Shanker, T. (2010, enero). The New York Times, *Cyberwar; In digital combat, U.S. finds No Easy Deterrent.*

UNDERHILL, W. (2010, octubre). Newsweek Magazine, *Britain's Biggest Security Threat.*

SCHNELL, L. (2009, diciembre) Newsweek Magazine, *The Evil (Cyber) Empire, Inside the world of Russian Hackers.*

RAMÍREZ, J. (2020, abril). Newsweek Magazine, *All is not Quiet on the Digital Front.*

MOROZOV, E. (2009, abril). Newsweek Magazine, *The Fog if Cyberwar.*

Documentos en Internet:

MINISTERIO DE DEFENSA NACIONAL; *ESTATUTO ORGÁNICO DEL MINISTERIO DE DEFENSA NACIONAL* (PROMULGACIÓN 04–02–2010) DISPONIBLE EN: HTTP://WWW.LEYCHILE.CL/NAVEGAR/?IDNORMA=1010682&IDVERSION=2010–02–04&IDPARTE

SERVICIO DE IMPUESTOS INTERNOS DE CHILE, *Cuenta Pública año 2010.*

DISPONIBLE EN: HTTP://WWW.SII.CL/CUENTA_PUBLICA/CTA_2010.PDF

CONSEJO DE SEGURIDAD NACIONAL DE REINO UNIDO, *Reporte Anual 2009 – 2010*. Disponible en: http://www.cabinetoffice.gov.uk/sites/default/files/resources/isc.annualreport0910.pdf

ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Carta de las Naciones Unidas.*

DISPONIBLE EN: HTTP://WWW.UN.ORG/EN/DOCUMENTS/CHARTER/INDEX.SHTML

ORGANIZACIÓN DE LA NACIONES UNIDAS, *Resoluciones del Consejo de Seguridad de las Naciones Unidas.* Disponible en: http://www.un.org/Docs/scres/2001/sc2001.htm