Importancia de la implementación de un laboratorio de ciberdefensa?*

Fredy Alejandro Hernández Linares [a]
Johan Alberto Jiménez Montañez [b]

* Artículo Resultado de investigación denominado Implementación de un laboratorio de ciberdefensa.

[a] Profesional en ciencias militares y especialista en Derecho Internacional de la Escuela Militar de Cadetes General José María Córdova; diplomado en Ciberseguridad de la Universidad Santo Tomás. Correo electrónico: fredeje45@outlook.com

[b] Profesional en ciencias militares de la Escuela Militar de Cadetes General José María Córdova; piloto de helicóptero Bell 206, instructor en aeronaves no tripuladas US Army. Correo electrónico: johanjimenez1980@hotmail.com

RESUMEN: A partir de un recuento de los antecedentes históricos más recientes sobre ataques cibernéticos, este artículo, en primer lugar, identifica los nuevos peligros que enfrenta la seguridad nacional con ocasión del crecimiento del ciberespacio y la intensificación de su actividad en todos los planos; segundo, plantea la necesidad de los estados modernos de prepararse para la acción defensiva en ese nuevo campo de batalla llamado ciberespacio; y tercero, llama la atención sobre la necesidad de un ordenamiento jurídico internacional más eficaz frente a esta preocupante realidad contemporánea.

PALABRAS CLAVES: ciberataque, ciberespacio, ciberguerra, infraestructura crítica, stuxnet.

Mañana no estaremos en el ciberespacio,
seremos el ciberespacio.
Paul Rexton Kan

INTRODUCCIÓN

La búsqueda permanente de una comunicación eficiente y que abarque largas distancias ha sido el origen de sofisticados inventos que de alguna forma han cambiado el modo como hoy se relacionan los seres humanos y, además, han generado el fenómeno de la dependencia tecnológica. Es así como la evolución humana pasó de la emisión de ruidos, expresiones y señales rudimentarias, cara a cara, a la transmisión de voz, imágenes y datos a larga distancia y, ahora, a través de una red mundial de computadores que todos conocemos como la internet, una invención que en su primer momento se empleó con objetivos militares: se diseñó como una red capaz de funcionar incluso en caso de que algunos de sus nodos fueran destruidos, ya que la información circularía por otros cauces del mismo sistema. Posteriormente, las universidades y las industrias se interesaron por esta red y poco a poco fueron cobrando protagonismo allí. Actualmente, la internet es un fenómeno social y económico por su extensión y por las dificultades que plantea su regulación.

> La complejidad hace que el ámbito cibernético sea difícil de estudiar. La complejidad estructural es el resultado del crecimiento exponencial del poder de la computación y la cantidad de dispositivos conectados a internet. La complejidad interactiva se deriva de la participación del ser humano en el sistema. El cambio tecnológico exponencial ha tornado el medio ambiente más complejo que nunca. Las cifras que ilustran este cambio son asombrosas: más de 2,1 mil millones de personas conectadas vía internet, 1,8 zettabytes de datos electrónicos creados en el 2011 y un total de 555 billones de sitios web. Se proyecta que en el 2016 la cifra de dispositivos móviles conectados a la internet supere la cantidad total de personas en el planeta (Chang, W. & Granger, S. 2012, p. 83).

Aunque no era su objetivo inicial, la masificación de internet ha alcanzado un área inimaginable, cada vez más extensa y más difícil de controlar. Esta área es el ciberespacio, definido como «el ambiente formado por componentes tangibles e intangibles, caracterizado por el uso de computadoras y del espectro electromagnético, para almacenar, modificar e intercambiar datos usando redes de computadores» (NATO Cooperative Cyber Defense Center of Excellence, CCDCOE, 2014: P. 4). De tal suerte,

> El desarrollo de la tecnología informática (procesadores y la internet) como producto del avance científico de la Tercera Revolución Industrial, la posterior concatenación de lo que se ha denominado como el Ciberespacio, y como producto de esto, que las Fuerzas Militares de diversos países se encuentren generando estrategias, operaciones y tácticas por medio de estos ha permitido dilucidar la configuración (en etapa inicial) de un nuevo poder militar; el poder cibernético (Gaitán, A., 2011: p. 23).

Bajo este escenario ha surgido una nueva tipología de enfrentamiento interestatal denominado ciberguerra, que busca paralizar o destruir las conexiones y las infraestructuras críticas de un país al anular sus sistemas informáticos (Instituto Español de Estudios Estratégicos, 2010: p. 16).

De lo anterior se infiere la importancia de entender el concepto de ciberataque como una forma de ciberguerra que, combinada con un ataque físico o sin este,

intenta impedir al adversario el empleo de los sistemas de información o su acceso a la ella (Instituto Español de Estudios Estratégicos, 2010: p. 333). En el escenario del ciberespacio como nuevo campo de batalla, los ciberataques (amenaza que afecta o desarticula los centros de gravedad de un enemigo) podrían ser tipificados como un crimen de agresión, ya que se violan las redes y los sistemas del adversario y por ende su seguridad. Además, al no existir una legislación armonizada que le haga frente a esta amenaza, es necesario el desarrollo de iniciativas lideradas por los estados, que permitan el control de los ataques que afectan transversalmente al sector privado, al público y al de los ciudadanos.

Así, pues, la pregunta que anima este trabajo gira en torno a la importancia de implementar un laboratorio de ciberdefensa, como medio proactivo para la identificación y estudio temprano de las amenazas cibernéticas que podrían vulnerar al Estado y a sus infraestructuras críticas por la acción de ciberataques provenientes de otros estados, organizaciones promovidas por estados, grupos terroristas o particulares con motivaciones atentatorias de la seguridad nacional.

Teniendo en cuenta el alto grado de afectación de los ciberataques a la Seguridad Nacional, se puede inferir que el impacto es más que suficiente para tener una posición radical y decisiva que haga frente a esta amenaza, que aqueja a la comunidad internacional.

Se considera acto de agresión el uso de las fuerzas armadas de un Estado contra otro sin justificación de defensa propia o autorización del Consejo de Seguridad de la Organización de las Naciones Unidas, ONU. La definición de acto de agresión así como de las acciones que califican como actos de agresión (como la invasión a través de las fuerzas armadas, bombardeos o bloqueos) fue influenciada por la Resolución 3314 de la Asamblea General de la ONU del 14 de diciembre de 1974 (Corte Penal Internacional, 2012).

De allí la importancia de este trabajo, pues esta nueva amenaza debilita la capacidad de respuesta de un Estado hasta el punto de volver obsoleta su defensa estratégica y afectar directamente sus ámbitos social, político y económico, para reducirlo a una situación de indefensión total. Esto ya ha ocurrido. Los ciberataques han afectado no solo al Estado sino a diferentes entidades gubernamentales y a la sociedad civil, por lo cual es necesario aunar esfuerzos para enfrentar esta amenaza cada vez más preocupante. En el marco de los conflictos armados internacionales, resulta aún más importante un estudio exhaustivo de los ciberataques, con el fin, en primer lugar, de encontrar su sitio en la normatividad jurídica, con el propósito de que pueda, si es el caso, ser tipificado como acto de agresión; y, en segundo lugar, para que el Estado logre anticiparse a cualquier intención de ciberataque contra sus infraestructuras críticas.

La naturaleza de la guerra ha tenido varias transformaciones gracias a factores como

> los alcances tecnológicos [que] abarcaron el desarrollo de las armas de fuego y la artillería, [cuando] el poder se concibió como terrestre. Al desarrollarse la industria de guerra naval, surgió el poder marítimo. Con la llegada de las aeronaves se instauró el poder aéreo. Finalmente, posterior al advenimiento del hombre al espacio exterior de la Tierra se determinó el poder espacial (Gaitán, 2011: p. 23).

Es así que el ciberespacio fue señalado por *The Economist* como el quinto dominio después de la tierra, el mar, el aire y el espacio.

Hoy, en la era de las tecnologías de la información y las comunicaciones, se observa cómo es cada vez más factible que una persona con conocimientos informáticos básicos, promovida por un Estado o por su propia cuenta, logre a través de un computador emprender una serie de acciones en contra de la infraestructura crítica de una nación, para dañar gravemente sus capacidades, para tratar de imponerle la aceptación de un objetivo propio o, simplemente, para sustraerle información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos. Es decir, para efectuar acciones características de lo que habitualmente hemos entendido como guerra, definida por Clausewitz (2002, p. 6) como un «acto de fuerza que se lleva a cabo para obligar al adversario a acatar nuestra voluntad», con la diferencia de que el medio empleado no sería la violencia física, la cual ha cambiado dada la facilidad de hacer un ataque informático que permita obtener una ventaja sobre el enemigo o, incluso, para derrotarle definitivamente en caso de guerra a través del ciberespacio.

Ciberespacio, es el ambiente formado por componentes tangibles e intangibles, caracterizado por el uso de computadoras y del espectro electromagnético, para almacenar, modificar e intercambiar datos usando redes de computadores.

Ante el presente panorama, donde las amenazas cibernéticas son cada vez mayores para la comunidad, los estados han tomado una serie de iniciativas orientadas a fortalecer su infraestructura física e informática, de tal forma que les permita desarrollar capacidades para prevenir, evitar, contener y responder ataques cibernéticos. Para lograr este objetivo, países como Estados Unidos, China, Reino Unido y Rusia, entre otros, han creado entidades dedicadas a la ciberdefensa, e incluso han llegado más allá con la conformación de ciberejércitos (Aguilar, 2010: p. 31). El ciberespacio, ciertamente, formará parte de cualquier guerra que se produzca en el futuro.

Ya como comunidad internacional, en su intento por enfrentar estos peligros, el Estatuto de Roma, en el artículo 8bis adoptado en Kampala, define el crimen de agresión individual como la planificación, preparación, inicio o ejecución de un acto de hostilidad por parte de una persona en posición de liderazgo e implica que la agresión constituya una violación manifiesta a la Carta de las Naciones Unidas. Aunque con estas características bastaría la voluntad de los estados para tipificar los ciberataques como crímenes de agresión, subsiste la necesidad de frenar esta amenaza jurídicamente, pues permanece entreabierta una ventana legal a través de la cual, aunque esté identificada, cualquier fuente de ciberataque contra un Estado podría llegar quedar impune.

La lentitud de la conceptualización y definición del crimen de agresión se ha tornado en una limitante para su aplicación en actos tales como los ciberataques, aunque, como ya se ha dicho, estos implican un impacto semejante o a veces superior a los causados por confrontaciones o ataques de tipo militar. De allí la necesidad perentoria de recapitular los antecedentes históricos de ciberataques y las correspondientes acciones posteriores adoptadas por los estados afectados, para, sobre esta base de conocimiento, establecer una normatividad que supere el escollo jurídico y dé claridad sobre las medidas más proactivas de ciberdefensa.

El papel de la seguridad nacional en el nuevo juego del ciberespacio, ciberguerras y ciberataques

Como ya se mencionó, la evolución de la guerra ha ido a la par con el cambio de la tecnología. También se dijo —y ahora se amplía— que el origen del ciberespacio se remonta a los inicios de internet, en los años 60, época de la Guerra Fría, cuando Estados Unidos crea una red exclusivamente militar con el objetivo de prevenir y defenderse de un eventual ataque soviético orientado a saquear la información militar. Arpanet —así llamado inicialmente por el acrónimo inglés de la expresión Advanced Research Projects Agency Network— fue dispuesta por el Departamento de Defensa de los Estados Unidos con el propósito de establecer un vínculo de comunicación entre los organismos y centros gubernamentales dedicados a labores de inteligencia y defensa de la nación.

Hoy se observa cómo los estados empiezan a funcionar a través de internet y el ciberespacio, ya que agiliza procesos y permite la supervisión y el control de diferentes actividades gubernamentales. Sin embargo,

> se puede afirmar que las sociedades que se han erigido sobre la base de la dependencia de las redes de computadores y el ciberespacio para sus actividades estándares, han incrementado los niveles de vulnerabilidades de su defensa y seguridad (Gaitán, 2011: p.27).

Este panorama indica que no solo puede ser utilizado para objetivos legales o actividades positivas, también para atacar y vulnerar diferentes ámbitos de otro Estado, como su infraestructura y su economía, hasta inclusive llegar a desestabilizar su sociedad. La estrecha relación entre tecnología y guerra hace que el ciberespacio sea el nuevo campo de batalla en el siglo XXI: «Los conflictos armados y políticos que se desatan alrededor del globo están contando con nuevas tecnologías, escenarios y estrategias para su consecución» (Gaitán, 2011: p. 23), las grandes potencias ya se han puesto en alerta por este nuevo escenario. De allí que las fuerzas militares de diversos países se encuentren generando estrategias, operaciones y tácticas por medio de las cuales han permitido dilucidar la configuración inicial de un nuevo poder: el poder cibernético (Gaitán, 2011: p. 23).

Como el ciberespacio cambia permanentemente el panorama del cual es parte integral, puede ser entendido como un tipo de NetWare que consiste en su utilización para objetivos ofensivos o defensivos militares desde internet. Es una confrontación entre dos o más partes, donde al menos una de ellas utiliza los ciberataques contra el otro. Por ello

> La formación de unidades militares específicas de ciberguerra no es más que la obligación que tienen los ejércitos de adaptar sus funciones a las tecnologías del momento, como en su día se hizo con la incorporación de las unidades de misiles, NBQ nuclear, bacteriológico y químico o guerra electrónica (Instituto Español de Estudios Estratégicos, 2010: p.172)

Los ciberataques son la nueva amenaza a la que se enfrentan los estados,

> lo cual conlleva que la expansión de la tecnología digital tiene sus riesgos al exponer a los ejércitos y a la sociedad a los ciberataques (ataques digitales). La amenaza es compleja, en múltiples aspectos y potencialmente muy peligrosa (Aguilar, L., 2010: p.79).

Es menester evocar el concepto de seguridad nacional para relacionarlo directamente con el ciberespacio,

ciberguerra y específicamente con el ciberataque. Así entonces, someramente, entendemos por seguridad un estado o situación de la nación en la cual los intereses nacionales se encuentran protegidos, libres de amenazas[1] tanto internas como externas (invasión, guerrillas, insurgencia, conflictos fronterizos, guerras de coalición, misiones de paz, mantenimiento de la paz, entre otras) y para hacerle frente a estas amenazas es necesario el empleo del poder militar.

La seguridad nacional es un interés vital, un fin que nace como precondición para la preexistencia ordenada del Estado, como un mecanismo de defensa para garantizar la permanencia y la prosperidad.

La evolución del concepto en el escenario global está sujeto al desarrollo de las nuevas amenazas de carácter trasnacional[2]: el terrorismo, el crimen organizado, las drogas, la corrupción el tráfico ilícito de armas, el lavado de activos, el deterioro del medio ambiente, entre otras (Cujabante, X., 2012: p 18). Por ende se ha creado la necesidad de modificar la capacidad de respuesta para hacerle frente a los riesgos[3] o amenazas que son más difíciles de localizar.

En consecuencia, la defensa (como medio para lograr el fin de la seguridad) se puede entender como la respuesta, militar y no militar, frente a las amenazas o riesgos (Vargas, A., 2008: p. 5). Es un medio que hace posible la protección de los intereses nacionales. Sin duda alguna, el interés nacional es la guía para la política de seguridad y defensa, ya que sirve para determinar la política nacional.

1 Como «indicio de probable mal, violencia o daño futuro; algo que da indicio de ocasionar mal o daño; advertencia. Algo o alguien que puede dañar a una particular persona o cosa; algo percibido por el gobierno como una posible amenaza para la seguridad nacional [...]. En realidad, el aspecto fundamental es la percepción de la amenaza, dado que, como ha sido agudamente señalado, aún ninguna teoría relativa a la seguridad ha proporcionado una medida objetiva acerca de si determinada circunstancia es realmente una amenaza; ello, sin perjuicio de advertir que también se ha sostenido que resulta de fundamental importancia que exista objetivamente una amenaza para que pueda hablarse válidamente del ámbito de la seguridad y de la adopción de medidas derivadas de dicho ámbito» (Vargas, A., 2008: p. 3). Por ello es de vital importancia precisar en cada caso quién define las amenazas en una sociedad determinada.

2 Es necesario considerar que las nuevas amenazas y riesgos a la seguridad tienen crecientemente un carácter transnacional y no necesariamente estatal, por lo cual «la seguridad [...] ya no puede plantearse en términos exclusivamente nacionales, sino desde una óptica regional o internacional. Muchas de las violencias que apreciamos en el mundo contemporáneo, como el terrorismo, el narcotráfico, los enfrentamientos raciales y religiosos, las luchas entre bandas o mafias, o la misma contaminación, para poner unos ejemplos, no respetan fronteras ni identidades geográficas, por lo que han de ser combatidas a partir de la cooperación entre varios Estados o directamente desde organismos regionales o internacionales» (Vargas, A., 2008: p. 5).

3 El riesgo es igual a amenaza más vulnerabilidad, entendiéndose el riesgo como el grado de pérdida que puede causar un evento particular en un lugar y período determinado. El nivel de riesgo, lo definimos por dos factores; por el nivel de la amenaza y por el grado de vulnerabilidad. La vulnerabilidad se entendería como el grado de exposición de una sociedad a las amenazas y la capacidad de resistencia y respuesta de sus estructuras sociales, económicas y físicas (Vargas, A., 2008: p. 5).

SEGURIDAD NACIONAL Y SU VULNERABILIDAD: RELACIÓN CON CIBERESPACIO, CIBERGUERRA Y CIBERATAQUE

Dice el secretario de Defensa de los Estados Unidos y ex-director de la CIA, Leon Panetta:

> Lo cierto es que existe la capacidad cibernética para tumbar nuestras redes eléctricas o paralizar el sistema financiero de nuestro país. Por lo tanto, considero que tenemos que estar preparados no solo para defendernos contra esta clase de ataques sino también, en caso necesario, para ser agresivos (Cfr. Fuentes, L., 2012: p. 3).

Se puede deducir que la preocupación con respecto al impacto de los ciberataques en un Estado, en este caso Estados Unidos, es que afecta su estabilidad y seguridad en el sistema internacional. Por tal razón, no se debe subestimar su poder destructivo, todos los estados son vulnerables ante un eventual ataque sorpresivo. Es necesario, además de reforzar las defensas cibernéticas como parte de la estrategia militar, proponer una estrategia de contención y negación frente a esta amenaza de escala mundial, que le apueste a la voluntad política de los estados para tipificar los ciberataques como crímenes de agresión, y a partir de este hecho crear hitos para promulgar una normatividad jurídica con la cual proceder, con amparo en el derecho internacional, ante un posible caso de ciberataque; esto con el fin de abordar las cuestiones legales más desconcertantes de la ciberguerra.

> **La formación de unidades militares específicas de ciberguerra no es más que la obligación que tienen los ejércitos de adaptar sus funciones a las tecnologías del momento, como en su día se hizo con la incorporación de las unidades de misiles, NBQ nuclear, bacteriológico y químico o guerra electrónica**
>
> (Instituto Español de Estudios Estratégicos, 2010: p.172)

Entre las incidencias reales y potenciales más preocupantes de las acciones en el ciberespacio se mencionan especialmente los daños a la infraestructura crítica, los impactos sobre la psicología humana y la configuración de nuevas modalidades de armamento. Respecto a la primera, la vulnerabilidad estratégica es especialmente preocupante debido a que se trata de un riesgo para el sistema básico que permite el funcionamiento de un país, y cuando todo comienza a funcionar a través de internet —ya que facilita el trabajo, permite la supervisión a distancia y en tiempo real— el riesgo es aún mayor. Dentro de los posibles perjuicios se encuentran el sabotaje a la prestación de los servicios públicos, la paralización de la red de transporte ferroviario o la interrupción del fluido de energía eléctrica, ataques a reactores nucleares, entre otros cuyo funcionamiento dependan de sistemas informáticos. Estas afectaciones suponen un serio quebranto para la normalidad y seguridad de la sociedad (Caro, 2010: p. 59).

Para ilustrar cómo un arma cibernética puede afectar gravemente la infraestructura de un Estado, vale traer a colación el caso de la intrusión de un programa *stuxnet* al sistema informático del reactor nuclear de Busher, en Irán: con este procedimiento se intervino sobre la estructura del mundo concreto y real, en centrales eléctricas, plantas de agua y unidades industriales (BBC News, 2010), un ciberataque que, en la actualidad, revisado en diversas investigaciones y catalogado como una de las formas más poderosas de empleo de la informática, se le atribuye a Israel (Gaitán, 2012: p. 18).

En cuanto a la psicología humana, se puede inferir que tales afectaciones se propician por del caos organizacional y civil del cual es la población la que sale directamente afectada, ya que se pone en riesgo su funcionamiento adecuado. Ejemplo de este tipo de afectaciones puede ser el "pánico virtual" causado por la noticia del supuesto colapso financiero del Banco Davivienda, en Colombia: hace algunos años, miles de clientes del banco Davivienda retiraron sus ahorros inducidos por la preocupación que suscitó un rumor según el cual la entidad estaba en quiebra y sería intervenida. Al final se descubrió que el correo provino de un comerciante de Buenaventura, quien terminó en la cárcel por desatar la propagación de este infundio. En tres días, el monto retirado por los cuentahabientes superó los mil millones de pesos (*El País*, 2013).

En lo referente al armamento, ya hay toda una nueva generación de artefactos bélicos, como los aviones no tripulados (pero teledirigidos a través del ciberespacio) o los tanques de aviones. Este nuevo desarrollo militar tecnológico está a merced del ataque de un *hacker*, quien puede acceder a su manipulación y ocasionar consecuencias letales. A pesar de la superioridad tecnológica que puedan tener los ejércitos y los estados, más vulnerables pueden llegar a ser también, ya que sus sistemas fácilmente podrían estar o ser permeados por sus enemigos (Gaitán, 2012, p. 23).

EL DILEMA DE LOS ESTADOS

En materia estratégica, el objetivo de las tecnologías informáticas y del ciberespacio es destruir y desarticular los centros de gravedad del adversario o enemigo para deshabilitarlo en el conflicto (Gaitán, 2012, p. 24). Según Clausewitz (1832), el centro de gravedad constituye fuente de fortaleza moral y física en el aspecto estratégico, por lo cual es asimismo el punto más vulnerable del enemigo, pueden ser varios, pero hay que identificarlo(s) muy bien para que el ataque sea el camino directo a la victoria.

Adicionalmente, es importante tener en cuenta que en el marco de la seguridad nacional la esencia de los ciberataques es ofensiva, defensiva y de inteligencia (Instituto Español de Estudios Estratégicos, 2010). Estos ataques son tan eficaces que alcanzan cualquier objetivo en la distancia y en tiempo real, al exponer redes y sistemas a ser interrumpidos o tomados por un hacker o por un código dañino automático.

En conclusión, si bien se tiene la noción del ciberataque como crimen de agresión, al entrar en sus particularidades no es posible hacer frente a esta amenaza de una manera efectiva y progresiva. De esta manera, y teniendo en cuenta su importancia en el nuevo orden mundial, es menester fortalecer mecanismos de contención y respuesta de los estados para no poner en riesgo su seguridad nacional, o bien para sancionar a los que afecten la seguridad, tanto del Estado como de los ciudadanos.

A continuación se hace una descripción de algunos de los casos más relevantes de ciberguerra.

> **Hoy, en la era de las tecnologías de la información y las comunicaciones, se observa cómo es cada vez más factible que una persona con conocimientos informáticos básicos, promovida por un Estado o por su propia cuenta, logre a través de un computador emprender una serie de acciones en contra de la infraestructura crítica de una nación**

CIBERATAQUE A ESTONIA

El 15 de abril del 2007, el gobierno de Estonia decidió remover del centro de Tallin el monumento en bronce del soldado soviético, conmemorativo de los soldados caídos durante la Segunda Guerra Mundial. Esta determinación le generó un fuerte enfrentamiento diplomático con Rusia. El 26 de abril, a las diez de la noche, Estonia comenzó a sufrir el ataque cibernético. Al final de la primera semana, todas las páginas web gubernamentales y de los diferentes partidos políticos habían sido bloqueadas. Para la segunda semana, todos los medios de comunicación quedaron completamente desconectados, lo que hizo imposible informar al mundo lo que estaba ocurriendo. El 9 de mayo, a medianoche ocurrió el ataque más fuerte: los hackers desconectaron todo el sistema bancario, bloquearon sus páginas web y los cajeros electrónicos dejaron de funcionar. Durante tres semanas, los sitios web del gobierno, los bancos, medios de comunicación y todas las universidades fueron sistemáticamente atacados y desconectados. El 19 de mayo, los ataques cesaron y la primera ciberguerra llegó a su fin. Estonia inmediatamente acusó al gobierno de Rusia, pero nada ha podido ser demostrado (Ministerio de Defensa Nacional, 2009, p.3).

Este caso pone al descubierto la vulnerabilidad de un Estado ante un ataque cibernético que, por su naturaleza, se dirige a redes extensas interconectadas de las cuales dependen las infraestructuras tecnológicas e informativas. Las consecuencias de este tipo de agresión son nefastas, ya que ponen en riesgo el sistema financiero del Estado, los medios de comunicación y, en general, los epicentros que dan estabilidad a la nación.

Lo anterior sin contar, como ya se ha señalado, con la afectación a la psicología del ser humano. El efecto sería tan devastador que el Estado quedaría indefenso, sin capacidad de respuesta y la sociedad se vería gravemente involucrada. Un hipotético ataque a Wall Street que paralice por un solo día sus operaciones, causaría la pérdida

de decenas de millones de dólares, pues la falla generaría en los inversionistas una profunda y larga desconfianza en la operación de inversiones.

Si se tiene en cuenta que la identidad el autor del ciberataque puede ser difusa y su procedimiento exento de trazabilidad alguna, el reto para el Estado es cada vez mayor, ya que le será difícil señalar quién perpetró el ataque y, sobre todo, comprobarlo. Por tal razón, es de vital importancia considerar las amenazas ciberespaciales en las agendas de seguridad, si no en la totalidad, al menos sí en la gran mayoría de los países del mundo. Esta característica del ciberataque no le fue ajena a Estonia, que pese a tener pruebas del origen del ataque, nada pudo demostrar contra Rusia:

> [...] aun cuando Estonia dio a entender que pudo identificar algunos ataques a oficinas del gobierno ruso, no estableció de hecho ningún enlace gubernamental directo. Rusia mantuvo siempre que los ataques vinieron de cibernacionalistas renegados, que actuaban de acuerdo a su propio sentido de patriotismo deformado pero no por órdenes de ninguna oficina o agencia gubernamental oficial. Es más un testimonio de estado de percepción pública global que nadie hoy en día cree la versión rusa de los ataques y da por sentada la versión estonia; nunca hubo una prueba irrefutable que demostrara que la política gubernamental formal rusa fuera la culpable principal de los ataques estonios (Crosston, M. D., 2011: p. 104).

Las fronteras del ciberespacio, vistas y analizadas en casos como el de Estonia, resultan de fácil acceso, frágiles y porosas, vulnerables ante la perspicacia y capacidad de daño de cualquiera que tenga la facilidad de acceder a un computador y con un nivel necesario de conocimientos que le permitirá de la manera más cómoda y efectiva desarticular la base de un Estado, hasta el punto de colapsar su infraestructura y afectar directamente a la población en sus dimensiones social, política y económica.

Ciberataque a Georgia

Este fue el primer caso en el que se combinaron operaciones militares y operaciones cibernéticas. Al igual que en el relatado caso de Estonia, la Federación Rusa estuvo detrás de la coordinación de las ciberoperaciones, pero, al día de hoy, la demostración legal no es posible (Aguilar, 2010: p. 330). Es un claro ejemplo de cibercampaña que apunta a un conflicto armado.

Para su comprensión, deben tenerse en cuenta los antecedentes del ataque. El 7 de agosto de 2008 se inició la Guerra de Osetia del Sur, entre Georgia, por un lado, y Osetia del Sur, Abjasia y Rusia, por el otro. Comenzó con un ataque sorpresivo de las Fuerzas Armadas de Georgia contra fuerzas separatistas, lo que provocó la reacción inmediata de Rusia, que consideró la acción como un ultraje fuera de las fronteras contra ciudadanos rusos, a quienes se dispuso a defender en cumplimiento de la que consideró su obligación como Estado. Al día siguiente, el 8 de agosto de 2008, en territorio de Osetia del Sur, los rusos iniciaron una serie de operaciones militares que se extendieron posteriormente a otras regiones de Georgia y al Mar Negro.

El 9 de agosto de 2008, el presidente de Georgia, Mikheil Saakashvili declaró el estado de guerra al considerar los hechos acontecidos como una agresión militar de la Federación Rusa contra Georgia. Tres días más tarde, el 12 de agosto, el presidente de la Federación Rusa, Dmitri Medvédev, decreta el fin de las operaciones militares rusas en territorio georgiano y acepta el plan de paz propuesto por la Unión Europea, plan que, entre otras estipulaciones, obliga a las fuerzas en pugna a volver a sus posiciones anteriores al comienzo del conflicto (Ganuza, 2011, p 197).

Inicialmente se efectuaron ataques DDoS —acrónimo en inglés de *distributed denial of service*, o, en español, *ataque distribuido de denegación de servicios*, una modalidad de ciberataque consistente en saturar la capacidad de reacción de un servidor mediante numerosas solicitudes procedentes de muchos terminales conectados, hasta exceder sus posibilidades de respuesta—. Estos fueron ataques de pequeña escala contra sitios web oficiales de Georgia. El primer ataque se registró en junio del 2008 en la fase del preconflicto y en el marco de las tensas relaciones entre Rusia y Georgia. Para la fase del conflicto armado, los ataques fueron bien organizados y coordinados. Durante los cinco días que duró el conflicto armado se sucedieron ciberataques contra sitios web pertenecientes al presidente de la República de Georgia, el Parlamento, Ministerios de Defensa y Asuntos Exteriores, el Banco Nacional y las principales agencias de noticias.

> Los ciberataques han afectado no solo al Estado sino a diferentes entidades gubernamentales y a la sociedad civil, por lo cual es necesario aunar esfuerzos para enfrentar esta amenaza cada vez más preocupante.

A medida que el conflicto armado se intensificaba, se incrementaba el número de ciberataques, los cuales debilitaron la capacidad de toma de decisiones políticas y militares de Georgia y su capacidad de consolidación de información y de comunicación entre su gobierno y los ciudadanos. Además, a través de la ciberpropaganda, trataron de inclinar la opinión pública hacia la postura defendida por Rusia, Osetia del Sur y Abjasia.

A la par con la finalización del conflicto armado, el 12 de agosto de 2008, las operaciones cibernéticas sufrieron una importante reducción en número e intensidad, pero el conflicto en el ciberespacio parecía no estar incluido en el acuerdo de paz y las ciberoperaciones continuaron hasta el 28 de agosto. El fin de las operaciones cibernéticas no se debió a ningún tipo de acuerdo entre las partes sino a su poca rentabilidad.

A diferencia del caso de Estonia, los ciberataques a Georgia influyeron directamente en el desarrollo de las operaciones armadas y las redes sociales fueron usadas como medio para reclutar voluntarios.

El objetivo era provocar la pérdida de la capacidad operativa y de confianza en las instituciones políticas, militares y financieras del país y bloquearles su capacidad de comunicación entre ellas y entre Georgia y el mundo exterior. Los objetivos políticos se concretaron en los sitios web del presidente de la República de Georgia, del Parlamento, del Ministerio de Asuntos Exteriores, del Ministerio de Ciencia y Educación y de instituciones educativas; los objetivos militares, en los sitios web del Ministerio de Defensa; los financieros, en los sitios web del Banco Nacional de la República de Georgia y del TBC Bank, la mayor institución bancaria del país; los objetivos de comunicaciones, en los sitios web y foros de las principales agencias de comunicaciones, agencias de noticias y televisión (Ganuza, 2010: p. 199).

Ciberataque a Estados Unidos

Otro ciberataque de gran relevancia fue el perpetrado por China a diferentes organismos expertos en la seguridad estadounidense:

> A finales de la década de los 90, Estados Unidos acusó a China de atacar a varias agencias gubernamentales y trató de infiltrar las instalaciones nucleares de Estados Unidos. [...]. China recluta activamente y facilita apoyo a algunos de los piratas más brillantes desarrollados localmente, llamados "*honkers*", [quienes], en su descarado patriotismo virtual, creen en la filosofía de que la "mejor defensa es una ofensa capaz". No se consideraran ellos mismos empleados necesarios del gobierno ni miembros de la comunidad de inteligencia china; simplemente creen que China necesita protegerse de sus adversarios (Crosston, 2012).

A despecho del argumento chino, según el cual se trata de acciones defensivas, su Operación Lluvia de Titanes (Titan Rain, así denominada por Estados Unidos) fue una

> iniciativa [...] puesta en práctica por el gobierno chino y el Ejército Popular de Liberación a partir del año 2002, con el fin de *hackear* los sistemas informáticos gubernamentales y de industria nacional de países como Estados Unidos de Norteamérica y Alemania, entre otros (Gaitán, 2011: p. 11).

Lo que pretendía China era «extraer o desarrollar operaciones para controlar centros de almacenamiento de información clasificada gubernamental, estratégica e industrial de los estados afectados» (Gaitán, 2011 p, 11). Los hackers de Lluvia de Titanes consiguieron acceder a varias redes informáticas estadounidenses, tales como Lockheed Martin, Sandia National Laboratories, Redstone Arsenal y la NASA.

Los expertos en seguridad trabajaron bastante para detectar de dónde provenían los hackeos, como lo hizo «Shawn Carpenter, un analista de seguridad para Sandia National Laboratories, donde buena parte del arsenal nuclear estadounidense es diseñado. Logró rastrearlos hacia la provincia sureña de Guangdong, en China» (Barrueto, 2009).

Esos sucesos ocurrieron en el 2002, y más adelante, «estudios realizados al respecto en el 2007, evidenciaron que mediante esta operación, China ya había logrado hackear (piratear) más de veinte terabytes (1.024.000.000'000.000 gigabytes equivalen a un terabyte) de información prioritaria» (Gaitán, 2011).

Ante el presente panorama, donde las amenazas cibernéticas son cada vez mayores para la comunidad, los estados han tomado una serie de iniciativas orientadas a fortalecer su infraestructura física e informática.

Por otro lado, también se demostró que «un grupo de hackers chinos entrenados en el ciberespionaje lograron descargar aproximadamente entre 10 y 20 terabytes de información sensitiva (pero no confidencial) del Departamento de Defensa de Estados Unidos a través de Non-Secure Internet Protocol Router Network (NIPRNet)» (Gaitán, 2012).

Es así que la revisión de la operación Lluvia de Titanes detectó cómo China adquiría información de toda índole. El peligro de este tipo de acciones reside en que sus consecuencias, según las intenciones predeterminadas pueden ser catastróficas: «Titan Rain es una de las amenazas de ciberespionaje más invasivas que las redes estadounidenses han enfrentado, ya que han comprometido redes de comunicación de bastante importancia como algunos planes de vuelo del ejército» (Barrueto, 2009).

Ciberataque a Irán

El último ciberataque de gran relevancia se ejecutó en el año 2010, cuando

> la problemática del desarrollo del programa nuclear de Irán para los países occidentales y principalmente para Israel se recrudeció. Esto propicio el desarrollo del ciberataque denominado por la comunidad científica como Stuxnet, el cual ha sido el arma virtual más compleja desarrollada hasta el momento para atacar la infraestructura crítica del Estado (Gaitán, 2011, p.13).

Se creó una ciberarma, Stuxnet, que invadió los sistemas informáticos que controlan específicamente la infraestructura crítica de Irán. Este gusano informático viajó por el ciberespacio hasta llegar a los sistemas de control del reactor nuclear Bushehr, instalación en donde, según han denunciado los servicios de inteligencia de otros Estados, se encuentra el centro de operaciones del Gobierno de Mahmoud Ahmadinejad para la posible construcción de armamento nuclear (Gaitán, 2011, p.13).

Stuxnet se activó desde cada una de las computadoras en las cuales se había alojado anónimamente, y así el

ataque fue perpetrado. El gusano, una vez inició su ofensiva, fue programado para que buscara específicamente los sistemas informáticos que controlaban el comando y control del reactor nuclear de Bushehr (Gaitán, 2012).

El ciberataque por medio del virus pretendía «controlar el sistema de operaciones de la instalación, asumió el control de este y lo llevó a operar bajo comandos erróneos y desestabilizadores que ultimaron un daño tal, que el reactor no pudo ser puesto en actividad» (Gaitán, 2011, p.13).

Vale aclarar que «al igual que los casos europeos, las investigaciones efectuadas plantean a Estados Unidos e Israel como los posibles ejecutores del Stuxnet; no obstante, los dictámenes no son fiables y concretos en la actualidad» (Gaitán, 2011).

Adicionalmente,

> según los análisis de las autoridades y sectores de defensa e inteligencia iraníes, el gusano, con la capacidad de reproducirse rápidamente por el ciberespacio y por terminales conectadas, entró a la red informativa de Irán por medio de una Flashdrive, que fue utilizada al procesador con conexión a esta (Gaitán, 2011, p.16).

Las intenciones de crear esta arma no solo pone en alerta a países como Irán, ya que puede afectar a cualquier país:

> el arma se difundió por la red mundial hacia miles de procesadores, que incluso se encontraban en países como India, China y Paquistán, y así esperar a la ejecución del ataque programado con el que fue diseñado para afectar la infraestructura del Estado (Gaitán, 2012).
>
> Al final del ataque lo que se puede constatar, es que hasta el presente el reactor todavía no ha podido ser inaugurado por el gobierno de Ahmadinejad. Desde un principio mantuvo como objetivo la infraestructura crítica nuclear iraní (Gaitán 2012, p, 83)

Lo preocupante en este contexto es que con solo oprimir un enter se pueda desatar un ataque que pueda dañar a miles de personas. La facilidad de los ciberataques permite imaginar innumerables de hipótesis de este tipo catastrofista.

CONCLUSIONES

La comunidad internacional ha de estar de acuerdo en qué es un ciberataque y cómo entenderlo como agresión para que se proteja la psicología del ser humano, la infraestructura crítica y el armamento, desde todas las dimensiones que conocemos.

El escaso conocimiento del ciberespacio no excusa la falta de defensa de este plano, por el contrario, no puede perderse de vista que de este depende la supervivencia de un Estado. En ese sentido, ha de tenerse claridad acerca de lo que se considera como agresión a la seguridad por parte de los estados en el sistema internacional, que en este caso versaría sobre los conceptos de injerencia, soberanía, amenazas, seguridad humana, orden público, etc.

El cambio de la guerra pone en vilo las existentes garantías que las instancias internacionales brindan, exigiendo mayor compromiso, responsabilidad trazabilidad y corresponsabilidad. Dicha exigencia no resulta ajena para los ciberataques y para el crimen de agresión por separa-

do, ya que, en cumplimiento de la finalidad del presente escrito, se han constatado las falencias que a su vez presenta la evolución del crimen de agresión. Pese al avance después de Kampala, aún queda mucho por hacer y a la espera de que en el 2017 la Corte pueda ejercer jurisdicción. Se avizora un futuro sombrío al respecto, ya que no es mucho lo que los estados hacen al respecto.

Teniendo en cuenta el alto grado de afectación de los ciberataques a la Seguridad Nacional, se puede inferir que el impacto es más que suficiente para tener una posición radical y decisiva que haga frente a esta amenaza, que aqueja a la comunidad internacional.

Sin embargo, como se pudo constatar en las páginas precedentes, este tipo de procesos abarcan periodos muy largos y dependen aún más de la voluntad de los estados para llegar a algún tipo de acuerdos, como se evidenció en el lento proceso de definición del crimen de agresión que data desde 1945, visto por primera vez como un crimen internacional que involucraba la responsabilidad penal individual internacional.

Si bien hasta ahora la constante ha sido la falta de compromiso de los estados con respecto al tema, no se debe relegar la necesidad de poner en las agendas nacionales tan importante prioridad, cada Estado debe impulsar las medidas correspondientes de prevención y contención en contra de las vulnerabilidades del ciberespacio, esto a través de la efectiva y oportuna acción del Estado que, a través de políticas nacionales de ciberseguridad y ciberdefensa, enfrente estas amenazas de carácter transnacional.

Es evidente que la falta de normatividad se constituye como una barrera, pero estar a merced del actuar de la comunidad internacional no parece ser la opción más recomendable; por ende, es necesario fortalecer los mecanismos internos y, si bien no adelantarse a las posibles decisiones de los Estados Parte en el 2017 para criminalizar el crimen, hacer alianzas y procesos interagenciales a través de la cooperación con países aliados y vecinos que perciban también la necesidad de estar a la vanguardia en temas de interés nacional vulnerables por las acciones criminales perpetradas a través del ciberespacio.

REFERENCIAS

Aguilar, L. (2010). Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio. *Biblioteca virtual de defensa*. Recuperado de http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029

Barrueto, L. (2009). *¡Fuera bombas! Titan Rain y la seguridad norteamericana*. Recuperado de http://www.maestrosdelweb.com/editorial/fuera-bombas-titan-rain-seguridad-norteamericana/

Caro, M. (2011). La estrategia internacional para el ciberespacio. En *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*. Instituto Español de Estudios Estratégicos. Recuperado de http://www.ieee.es/Galerias/fichero/docs_ informativos/2011/DIEEEI212011EstrategiaInternacionalCiberespacio.pdf

Chang, W., & Granger, S. (2012). La guerra en el ámbito cibernético. *Air &. Space Power Journal, 24*(3), 83–90.

Clausewitz, K. (2002). De la guerra. Bogotá: Librodot.

Corredor, I. (2012). *El crimen de agresión en Derecho Penal Internacional. Responsabilidad del individuo por acto de Estado*. Bogotá D.C.: Universidad del Rosario.

Corte Penal Internacional (2012). *Cumpliendo con la promesa de una Corte efectiva, justa e independiente. Crimen de Agresión*. Recuperado de http://www.iccnow.org/?mod=-aggression=es

Corte Penal Internacional (S.f.). *La CPI y el Crimen de Agresión*. Recuperado de http://www.iccnow.org

Crosston, M. (2011). World gone cyber MAD. How "mutually assured debilitation" is the best hope for cyber deterrence. *Strategic Studies Quaterly, 5(1)*, Spring, 100–116. [Traducción disponible en: http://www.airpower.maxwell.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_04_crosston_s.pdf: El mundo se ha vuelto "ciberloco". Cómo el "debilitamiento mutuamente asegurado" es la mayor esperanza para la disuasión cibernética].

Cujabante, X. (2012). Unasur: ¿hacia la consolidación de un complejo regional de Centro de Estudios Estratégicos sobre Seguridad y Defensa? *CEESEDEN*, *7*(2) 68–76.

Chang, W. (2012). La Guerra en el ámbito cibernético. *A. &. Power, Cyber Warfare Amenaza Mundial. Journal en español*, *24*, 83–90.

El País (s.f.). *En Internet anda la calumnia*. Recuperado de http://historico.elpais.com.co/paisonline/notas/Marzo012009/eco5.html

Gaitán, A. (2011). Computadores e internet en la guerra interestatal: ¿La consolidación de un nuevo poder militar en el siglo XXI? *Estudios en Seguridad y Defensa, 6*(2), 22–34.

Gaitán, A. (2012). La Ciberguerra y sus generaciones: un enfoque para comprender la incidenica de las tic en la guerra regular. *CEESEDEN, 7*(2), 5–18.

Gaitán, A. (2012). *El Ciberespacio: un nuevo teatro de batalla para los conflictos armados del siglo XXI*. Bogotá D.C.: Escuela Superior de Guerra.

Ganuza, N. (2011). La situación de la ciberseguridad en el ámbito internacional y en la OTAN. En: *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Colección Cuadernos de Estrategia, 149. España: Ministerio de Defensa, Instituto Español de Estudios Estratégicos e Instituto Universitario General Gutiérrez Mellado. P.

Instituto Español de Estudios Estratégicos (2010). *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*. Recuperado de http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029

Ministerio de Defensa Nacional. División de estudios sectoriales (2009). *Ciberseguridad y ciberdefensa: Una primera aproximación*. Recuperado de http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

CCDCOE (2013). *Cooperative Cyber Defence Centre of Excellence.* Recuperado de https://ccdcoe.org/

Vargas, A. (2008). ¿Cómo entender la seguridad y la defensa? *Democracia, Seguridad y Defensa* (boletín bimesetral) *4*(29). Pontificia Universidad Católica de Ecuador. 2–4.