DISUASIÓN Y USO DE LA LEGÍTIMA DEFENSA EN EL CIBERESPACIO

Deterrence and use of self-defense in the cyberspace

MAY. Rodrigo Kinast Werner *

Resumen: El presente artículo pretende establecer algunos argumentos con respecto a la aplicabilidad de la política disuasiva en relación a las nuevas amenazas que se presentan en el ciberespacio. Además de lo anterior, tiene la intención de evidenciar la articulación del arte de la estrategia de la disuasión al emplearse en conjunto con la ciencia y la tecnología. Junto con ello, se discuten las complejidades para justificar el empleo de la legítima defensa frente a una agresión en el ambiente digital, considerando las características del ambiente de la información y de este dominio.

Palabras claves: disuasión, ciberdefensa, ciberataque, legítima defensa, Estado

Abstract: This article aims to establish some arguments regarding the applicability of deterrence policy in relation to new threats in cyberspace. Likewise, how it is articulated the art of deterrence strategy with science and technology is analyzed. In addition, complexities to establish the use of self-defense against a ciberattack or aggression in the digital environment are discussed, considering the characteristics of this domain.

Key words: deterrence, cyber defense, cyberattack, self-defense, State

* Oficial del Arma de Infantería. Oficial de Estado Mayor. Magíster en Ciencias Militares con mención en Gestión Estratégica. Magíster en Inteligencia Económica. Profesor Militar de Academia de la asignatura de Táctica y Operaciones. Actualmente se desempeña como Comandante de Unidad de Combate de la Fuerza Terrestre del Ejército. ✉rkinastw@gmail.com

INTRODUCCIÓN

El siglo XXI se ha caracterizado por un aumento exponencial de las Tecnologías de la Información y las Comunicaciones (TIC), lo que ha permitido la optimización y automatización de los procesos, generando además, la interrelación entre los sistemas informáticos y las bases de datos, para el empleo de la información. Ello ha producido la masificación y ubicuidad en el uso de internet, originando un nuevo escenario o dimensión denominado “ciberespacio”, definido en la Política Nacional de Ciberseguridad (2017) y en la Doctrina Nacional Conjunta 2-11 (2017) como “el ambiente intangible compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior", la que se suma a los tradicionales dominios de tierra, aire, mar y espacio.

En relación con lo anterior, los desafíos en el uso y explotación del ciberespacio son cada vez mayores. Es complejo detectar los orígenes, causales y motivaciones de un ciberataque, los cuales pueden proceder de diversas organizaciones criminales, individuos aislados o incluso desde otros estados. Dichos ataques, pueden generar grave impacto en el funcionamiento de las instituciones, organismos y sistemas, tanto públicos como privados, afectando directamente o indirectamente al Estado y en consecuencia a la población.

Tal como lo plantea la Doctrina Nacional Conjunta 2-11 (2017), la diversidad de amenazas que pueden afectar el estado de normalidad en el uso del ciberespacio, obligan a que distintos actores, tanto públicos como privados, desarrollen una perspectiva holística e integradora que permita disminuir las vulnerabilidades y enfrentar estos riesgos y amenazas; siendo el Estado, el encargado de cumplir el rol fundamental de dirigir los esfuerzos, mediante políticas y directrices claras que permitan el empleo eficaz de las capacidades, con la finalidad de proteger los atributos de la información, su confidencialidad, integridad y disponibilidad.

Al mismo tiempo, es pertinente tener presente que para avanzar en esta materia, se requiere crear soluciones que trasciendan lo puramente tecnológico. Para esto

es necesario un marco legal, colaboración pública y privada y participación y educación de la población. Lo anterior, complementado además, con nuevas herramientas tecnológicas capaces de neutralizar o mitigar ataques cibernéticos cada vez más sofisticados.

En este contexto, el Estado de Chile ha arbitrado desde hace algunos años medidas concretas, destinadas a redituar los beneficios de las nuevas tecnologías. Una de ellas fue la denominada Agenda Digital (AD2020), lanzada el año 2015 y que contenía cinco ejes principales en política pública, con diferentes ejes de acción: derechos para el desarrollo digital, conectividad digital, gobierno digital, economía digital y competencias digitales (AD2020, 2015). Específicamente el eje de gobierno digital, ordenó la creación de una estrategia de ciberseguridad, la que fue presentada en el año 2017 y se encuentra vigente hasta la fecha. Esta definió distintas medidas, siendo una de ellas, la elaboración de una Política de Ciberdefensa (Política Nacional de Ciber Seguridad, 2017), la cual fue promulgada a fines del año 2017, con los siguientes principios básicos:

> El respeto del derecho internacional público, incluyendo la abstención del uso y la amenaza del uso de la fuerza, la legítima defensa y el respeto a la soberanía, la promoción de la democracia y el respeto por los derechos humanos y la protección de la población, de los intereses nacionales y de la integridad nacional. (Política de Ciberdefensa, 2018, p. 3)

En relación con los principios descritos, se evidencia que la Política de Ciberdefensa posee total coherencia y compatibilidad con los siete principios de la Política de Defensa Nacional declarados en el Libro de la Defensa 2017, en especial en cuanto a la aplicación del derecho a la legítima defensa y respecto al uso de sus capacidades (Ministerio de Defensa, 2017, p. 96). En este contexto y considerando esta vinculación, surge la interrogante ¿Son aplicables la disuasión y la legítima defensa como modalidades de empleo de los medios de la Defensa en el dominio del ciberespacio?

Con la intención de dar respuesta a ello, el presente artículo aborda dos de las

tres modalidades de empleo de la Defensa (disuasión, legítima defensa y cooperación internacional). Inicialmente se enfoca en describir la teoría de la disuasión y su aplicabilidad en el dominio del ciberespacio y, posteriormente, evidenciar bajo el amparo de la legítima defensa la factibilidad de empleo de ciber capacidades.

TEORÍA DE LA DISUASIÓN

La teoría de disuasión en el marco estratégico contemporáneo empezó a adquirir importancia a principio de los años 50', dado el crecimiento del armamento nuclear (Chinchilla, 2018). Pero más que una teoría, se trata de un supuesto sobre la conducta de un agresor, cuya utilización abarca diversos campos, como la economía, el derecho, la sociología, la psicología social y la criminología (Bravo, 2017). El supuesto básico de la teoría puede ser planteado de la siguiente forma: a nivel individual, la conducta ilegal puede ser controlada por la amenaza de recibir sanciones ciertas, severas y rápidas. La evidencia acerca de estos tres factores (certeza, severidad y rapidez) no es concluyente, pero es probable que solo el primero de los tres (certeza de castigo/pena) sea un disuasor fuerte, la percepción de la severidad del castigo o pena es un disuasor suave, y la celeridad de castigo o pena parece no ser un disuasor.

En general, ya sea de individuos o de autoridades tomando decisiones en nombre de un Estado, se acepta que la disuasión, de existir, debe hacerlo en la mente del agresor o de la víctima que considera devolver el ataque. La evidencia en el párrafo anterior es, por tanto, aplicable tanto en el caso de estados como de personas; sin embargo, existen consideraciones adicionales que es necesario realizar en el caso de la disuasión como estrategia entre estados.

ESTRATEGIA DE DISUASIÓN EN CONFLICTOS EN EL AMBIENTE FÍSICO

Una estrategia de disuasión es una política declarada de un Estado. Paul Nitze distingue entre la política declarada y la política de acción. Mientras la primera se refiere a "declaraciones públicas de objetivos", la segunda se refiere a "objetivos y planes militares concretos para emplear la fuerza existente" (Nitze citado en Arenas, 2013, p.

223). Según el Libro de la Defensa Nacional de Chile (2017), la disuasión comprende tanto un efecto como la acción que lo causa, por tanto:

> Es un efecto por cuanto corresponde a una dimensión psicológica o subjetiva que se produce en un potencial adversario. La disuasión no pretende paralizar toda acción contraria al interés nacional, sino generar en el potencial adversario la convicción que el costo de transferir coactivamente contra intereses vitales propios será más alto que los beneficios de obtener. (Libro de la Defensa Nacional de Chile, 2017, p. 132)

Esta es una de las variadas definiciones sobre disuasión que declaran los estados. Generalmente, estas se conforman de siete elementos comunes, a saber:

a. Un interés a proteger: todo Estado que emplea una estrategia disuasiva lo hace para proteger algún interés específico, como su población, su soberanía o su infraestructura crítica (servicios básicos, caminos, recursos económicos, entre otros).

b. Una declaración (“No hagas X, o de lo contrario te ocurrirá Y”): por supuesto, puede haber múltiples acciones X y múltiples medidas Y.

c. Reafirmación: en términos lógicos, esta es la declaración inversa de la anterior. Si A no realiza X, entonces de seguro no ocurrirá Y. En la práctica, esto tiene que ver con asegurar a A que B no incurrirá arbitrariamente en medidas de respuesta si no existe una amenaza real de parte de A.

d. Medidas de negación: es la parte defensiva de la disuasión. Consiste tanto en aquellas medidas tomadas para prevenir que X ocurra, así como las medidas tomadas para disminuir o anular los efectos de X si este llegara a tener éxito.

e. Medidas de castigo o respuesta: es la parte ofensiva de la disuasión. Consiste en las acciones que B ejecutará en respuesta a un ataque (es

f. decir, Y). El supuesto básico de una medida de respuesta es que el costo para el país agresor por la respuesta es mayor que el beneficio obtenido por el ataque, es decir, costo A (Y) > beneficio A(X).

g. Credibilidad: el país A debe creer que B es capaz de ejecutar la acción Y; de lo contrario, incurrirá de todas formas en el ataque.

h. Miedo: con esto se alude al temor que produce un ataque sobre la población afectada, es decir, al temor que puede producir Y sobre la población de A. (Bravo, 2017)

Estos siete factores conforman el medio en que opera la disuasión, pero hay que agregar el cálculo costo-beneficio que pondera todos los factores anteriores.

ESTRATEGIA DE DISUASIÓN DIGITAL

¿Cómo deben ser interpretados los conceptos anteriores, si se piensa en una estrategia de disuasión para el ciberespacio? A continuación, se interpretarán algunos de los elementos presentados previamente, con el fin de vincularlos con esta nueva dimensión.

Intereses a proteger

En el mundo digital también existen intereses que son necesarios proteger. Por ejemplo, actualmente existe preocupación entre los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Organización de Estados Americanos (OEA), con respecto a la protección de la infraestructura crítica de información (ICI), la que es entendida en Chile como:

> Las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado. (Política de Ciberdefensa, 2018, p. 4)

Medidas de negación

De los tres componentes que componen el ciberespacio[1], un ataque digital explota dos de ellos; primero, las vulnerabilidades en los sistemas lógicos (software) y el segundo, por las limitaciones y sesgos en las personas (interacciones). Por lo tanto, la mejor forma de defender a un Estado y, por ende, a sus instituciones, es por medio de:

a. Búsqueda y reparación continúa de vulnerabilidades en los sistemas informáticos que forman parte de los intereses a proteger.
b. Capacitación y entrenamiento constante de las personas dentro del Estado y sus instituciones, para evitar que estas sean engañadas y divulguen información relacionada con el acceso a los sistemas.

Medidas de reprimenda

Una medida de respuesta digital necesariamente implica el empleo de una "ciberarma" en contra del atacante. Conforme a lo anterior, las medidas de respuesta constituyen la parte ofensiva de la disuasión. Por lo tanto, una medida de respuesta es, necesariamente, de naturaleza ofensiva, no defensiva. Algunos ejemplos de medidas que un Estado podría tomar en respuesta a un ciberataque son:

a. Medidas de respuesta operacionales: inyectar "malware" en los sistemas informáticos del oponente; utilizar una "botnet", con el objeto de lanzar un ataque de denegación de servicio[2] (DDos) sobre los sistemas del oponente; hacer uso de una vulnerabilidad en un sistema Supervisory Control And Data Acquisition[3] (SCADA) para producir fallas en los sistemas eléctricos, distribución de agua, control de tráfico aéreo, entre otros.

---

1 Ciberespacio es un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior (BPCS, 2015, p. 13).

2 Es un ataque donde muchos servidores llenan de peticiones un servidor, con la finalidad de que deje de funcionar.

3 Es un tipo de Sistema de Control Industrial que monitorea y ejecuta procesos industriales. Se utiliza en todo, desde la gestión y operación de centrales eléctricas hasta la fabricación de envoltorios de dulces.

b. Medidas de respuesta conductuales: capturar las credenciales de acceso a las autoridades civiles o militares del oponente y destruir la información de sus cuentas públicas o privadas; lanzar un ataque masivo de “phishing” sobre la población de otro país, con la intención de capturar sus credenciales de acceso a la banca y transferir dinero de forma masiva a otras cuentas, entre otros.

LA DISUASIÓN ENTRE ESTADOS ¿ES POSIBLE EN EL CIBERESPACIO?

A partir del análisis anterior, es posible aplicar la disuasión digital con ciertas consideraciones:

a. No es cuantificable: La disuasión digital difiere de la cantidad de armamento y personal que posea un Estado, no es algo “cuantificable”.

b. Nivel de desarrollo tecnológico: La disuasión digital no tiene sentido cuando un Estado no posee un desarrollo tecnológico considerable. Por ejemplo, no causaría el mismo efecto la disuasión hacia un estado con un bajo desarrollo tecnológico, en comparación a realizarla hacia otro que posee mayor desarrollo y nivel de implementación de las TIC.

c. El problema de la seguridad: Las vulnerabilidades son parte de las mismas instituciones y organizaciones que componen una nación. Es decir, para disuadir a un adversario no basta tener altas capacidades para ejercer el poder nacional, sino que es necesario contar con una infraestructura robusta, redundante y resiliente, condición que puede ser promovida por los ámbitos público y privado. De esta forma, desincentiva a un posible atacante de generar una agresión. Por ejemplo, si se declara que la capacidad de la Defensa Nacional puede resguardar la soberanía, la defensa tiene los medios para actuar ante una posible agresión enemiga; pero, lo anterior no ocurre de igual forma en el medio digital. La responsabilidad de lo que se desea proteger recae también en privados, por lo tanto, la labor de asegurar este ámbito le compete a un actor que se encuentra fuera del alcance de la defensa, si no es incluido en las políticas.

d. Cooperación internacional: los estados deben participar activamente en ejercicios conjuntos, seminarios, entre otros. En esta área, para lograr disuadir a potenciales amenazas es conveniente continuar los ejercicios de ciberseguridad, ejecutados tanto en la Organización del Tratado Atlántico Norte (OTAN), como también en Unión Europea (EU), con la finalidad de demostrar que es un actor válido, lo que constituiría un indicador para disuadir a un posible atacante, sea este un agente estatal, como no estatal[4]. Ejemplo de esta intención fue la participación de representantes del Ejército, Armada, Fuerza Aérea, Estado Mayor Conjunto y del Ministerio de Defensa Nacional de Chile, en conjunto con especialistas del US Army Cyber Command en la ejecución del primer Ejercicio Conjunto en Ciberdefensa entre ambos países. La actividad, que se desarrolló en la ciudad de Santiago entre 19 y el 23 de agosto, formó parte del acuerdo de cooperación entre Chile y Estados Unidos (Subsecretaría de Defensa, 2019).

En caso de no considerar alguno de los puntos antes presentados, la disuasión en este dominio resultaría menos eficiente y, por ende, un ataque podría ocurrir sin ser detectado a tiempo; por lo tanto, si se evidencia que un ciberataque masivo está ocurriendo contra la soberanía, sus habitantes, su infraestructura, o aquello que dañe sus intereses ¿Cómo se podrían poner en ejecución las capacidades en ciberdefensa del poder nacional?

Legítima defensa

Enfocándose en conceptualizar la legítima defensa como un derecho inmanente de los estados, es de suma importancia conocer que las normas jurídicas pueden ser interpretadas desde variadas perspectivas, siendo una de ellas el punto de vista de los resultados a los que conducen. En este contexto, el artículo 51° señala que:

[4] Agente no estatal: persona física o entidad que no actúa bajo la autoridad legítima de un Estado en la ejecución de actividades comprendidas en el ámbito de la presente resolución (S/RES/1540, 2004, p. 1).

> "Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta que el Consejo de Seguridad tome las medidas necesarias para mantener la paz y la seguridad internacionales". (ONU, 1945)

Lo anterior, puede ser interpretado desde dos perspectivas: una restrictiva y otra extensiva. La diferencia entre ambas radica en que la primera busca siempre la interpretación restrictiva; en otras palabras, la abstención al máximo del uso de la fuerza, estableciendo una clara diferencia con la interpretación extensiva, situación en la que el artículo 51° se puede emplear y justificar en más casos de los que ordena la norma; por ejemplo, bajo esta interpretación, además de reconocer la legítima defensa, se podría justificar también medidas de autoprotección e incluso los ataques preventivos.

Haciendo esta salvedad, se interpretará el derecho a legítima defensa de forma restrictiva a lo largo de este artículo.

Agresión

Sin embargo ¿Cómo se podría invocar el derecho a la legítima defensa? Antes de saber el cómo, es necesario conocer qué tipo de agresiones podrían conllevar el uso del derecho inmanente antes mencionado. En este sentido, la Asamblea General de la ONU, mediante la resolución 3314 de 1974, logró un acuerdo sobre una definición de acto de agresión. A continuación, se presenta un extracto de esta:

> "Con sujeción a las disposiciones del artículo 2° y de conformidad con ellas, cualquiera de los actos siguientes, independientemente de que haya o no declaración de guerra, se caracterizará como acto de agresión:

1. La invasión o el ataque por las fuerzas armadas de un Estado del territorio de otro Estado, o toda ocupación militar, aún temporal, que resulte de dicha invasión o ataque; o toda anexión, mediante el uso de la fuerza, del territorio de otro Estado o de parte de él.

2. El bombardeo por las fuerzas armadas de un Estado al territorio de otro Estado, o el empleo de armas por un Estado contra el territorio de otro Estado.

3. El bombardeo de los puertos o de las costas de un Estado por las fuerzas armadas de otro Estado.

4. El ataque por las fuerzas armadas de un Estado contra las fuerzas armadas terrestres, navales o aéreas de otro Estado, o contra su flota mercante o aérea.

5. La utilización de fuerzas armadas de un Estado que se encuentran en el territorio de otro Estado con el acuerdo del Estado receptor, en violación de las condiciones establecidas en el acuerdo o toda prolongación de su presencia en dicho territorio después de terminado el acuerdo.

6. La acción de un Estado que permite que su territorio, que ha puesto a disposición de otro Estado, sea utilizado por ese otro Estado para perpetrar un acto de agresión contra un tercer Estado.

7. El envío por un Estado, o en su nombre, de bandas armadas, grupos irregulares o mercenarios contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerados, o su sustancial participación en dichos actos" (ONU, 1974).

En la resolución expuesta, se pueden apreciar los siete puntos en los que se considera, a modo de definición, qué se entiende por un acto de agresión entre estados o en su nombre, independiente de si existe una declaración de guerra o no. También se debe agregar que en el párrafo 4° de esta resolución, se aclara que la lista presentada engloba parte importante de los aspectos definitorios, pero pudiesen ser otros más no incluidos y, por lo tanto, el Consejo de Seguridad puede determinar otros actos, de conformidad con la Carta, que constituyen agresión.

Actores y legítima defensa

Entonces ¿Cómo se podría interpretar el concepto recién expuesto ante un ciberataque masivo a la soberanía de un Estado y, por ende, que implique el

despliegue de sus capacidades en ciberdefensa? Antes de contestar esta pregunta, es necesario plantear el problema de determinar qué actores podrían realizar este ataque.

Teniendo en cuenta los diferentes actores (tanto estatales como no estatales), es posible analizar la aplicabilidad del concepto de agresión por medio del uso de ciberarmas. Además, se debe agregar otro aspecto fundamental en el ciberespacio, este es que existe un problema para determinar de dónde proviene un ataque (locación), como también quién lo realizó (actor). Por lo tanto, se genera el desafío de determinar la atribución (identificar al actor) y la motivación (intereses y vinculaciones), elementos esenciales para aplicar el derecho internacional público con la finalidad de sancionar este tipo de ataques.

CASOS DE ESTUDIO ¿SE HA UTILIZADO LA INVOCACIÓN DEL DERECHO A LA LEGÍTIMA DEFENSA EN EL CIBERESPACIO?

A continuación, se presentan tres casos de ciberataques masivos contra estados, y se verifica la posible invocación del derecho a la legítima defensa.

Estonia

El primer ataque informático masivo ocurrido contra un Estado le aconteció a Estonia, el 27 de abril del 2007, prolongándose por 22 días, ocasionando la paralización de los servicios financieros, el comercio y las comunicaciones nacionales, entre otros.

En este contexto, para entender cómo se gestó y desarrolló esta crisis, es necesario tener en consideración que Estonia era un pequeño Estado que pertenecía a la Ex Unión Soviética y que en 1991 comenzó a ser un país independiente. Con tan solo 1.3 millones de habitantes, esta nación ha hecho de su infraestructura digital un motivo de orgullo nacional, ya que antes del ataque, algunas de sus iniciativas de desarrollo digital eran:

En el año 2000, el gobierno declaró Internet como un Derecho Humano Básico, como también suprimió el uso de papel en todas las dependencias estatales,

remplazándose por un soporte electrónico, e incluso los gastos efectuados en el presupuesto general del Estado se pueden seguir en Internet en tiempo real. El 90% de los ciudadanos estonios posee una ID Card, que le permite acceder a diferentes servicios, como por ejemplo, transporte público, salud, validar elecciones electrónicas, entre otros.

Fue el primer país que inició pruebas de voto electrónico a través de Internet en 2004, lo que permitió que las elecciones de 2007 se realizarán vía web a través de ordenadores.

El 98% de las transacciones bancarias del país son digitales. Del mismo modo, el 99% de los casi 1800 trámites oficiales estatales se pueden realizar de manera online.

Estas son tan solo algunas medidas que llevaron a Estonia, en menos de un cuarto de siglo, a ser el país con mayor desarrollo digital en el mundo, pero también el más propenso a las nuevas amenazas en el ciberespacio.

En abril de 2007, el gobierno estonio movió un memorial de la guerra rusa, “el soldado de bronce de Tallin”, desde una intersección céntrica de la capital Tallin hacia un cementerio militar. Los ciudadanos veían la estatua que se emplazaba en ese lugar desde 1947 como un recuerdo de la opresión rusa, pero los ciudadanos de ascendencia y etnia rusa vieron la relocalización de la estatua como una afrenta. Parte de la población étnicamente rusa protestó en las calles: las revueltas duraron dos días, hasta que fueron diluidas por la policía local. Si bien los disturbios fueron controlados, ese mismo día comenzaron una serie de ataques DDoS en contra de la infraestructura gubernamental, financiera y de los medios de comunicación, ya que muchos de los servidores que usualmente antes del ataque recibían 1000 visitas diarias, durante el ataque pasaron a recibir 2000 solicitudes por segundo.

El Gobierno estonio rápidamente se percató que estaba bajo ataque, y conformó un Computer Emergency Response Team (CERT), pero los ataques con el pasar del tiempo cambiaron de forma y se volvieron más sofisticados. Como respuesta,

Estonia cerró sus fronteras en Internet, de manera que los usuarios dentro del país pudieran seguir utilizando los servicios internos. Incluso se solicitó apoyo a Organización del Tratado del Atlántico Norte (OTAN), ya que Estonia es miembro de esta alianza político-militar, y en consecuencia podía invocar la legítima defensa colectiva para atacar o disuadir al atacante de seguir con la agresión.

El gobierno estonio acusó a Rusia del ataque porque según el Ministerio de Defensa descubrió instrucciones circulando por web rusas de cómo unirse al ataque. Rusia negó la responsabilidad como nación sobre el incidente (McGuinness, D., 2017).

Guerra de Osetia del Sur (Georgia)

Luego de la disolución de la URSS, tres regiones que pertenecían a la República Socialista de Georgia reclamaron su independencia, esto generó una serie de conflictos en la región de Osetia del Sur, Abjasia y Adzaria, donde finalmente las fuerzas rusas intervinieron como fuerzas de paz para estabilizar esta zona de importancia estratégica.

En este contexto, el presidente Mijail Saakashvili, al llegar al poder fomentó el nacionalismo georgiano, cambiando su orientación política hacia occidente con una clara posición anti-rusa, lo que se vio reflejado en la solicitud del retiro de las fuerzas de paz rusas para ser reemplazadas por fuerzas de la OTAN; por su parte, Rusia aumentó su grado de influencia en la zona con un mayor acercamiento y protección hacia las regiones de Osetia, Abjasia y Adzaria.

El gobierno georgiano le ofreció autonomía a la región de Osetia del Sur, la que fue rechazada, ya que ellos buscaban su independencia total. Es importante señalar que la mayor parte de la población de esta región es de origen ruso, por lo que Georgia acusó a Rusia de promover el separatismo.

Los hechos anteriormente nombrados provocaron la desestabilización de la zona, con un incremento del asedio por parte de las fuerzas georgianas sobre las fuerzas rebeldes de Osetia, aumentando la militarización de la región, tanto por fuerzas georgianas como por fuerzas rusas.

El 8 de Agosto de 2008 las fuerzas armadas georgianas iniciaron un ataque sobre la localidad de Tsjinval, siendo este el inicio de la guerra en Osetia del Sur.

Es en este conflicto donde se implementó el uso del ciberespacio como una nueva dimensión, ejecutando ciberataques simultáneamente a los ataques militares convencionales. A pesar de que estos ataques no afectaron la infraestructura crítica, sí contribuyeron a las operaciones que buscaban el dominio de la información y propaganda (INFOOPS), principalmente con la denegación de servicios (DDoS) sobre las páginas oficiales del gobierno de Georgia, además de modificar algunos sitios web con ataques "defacement"[5] donde cambiaron la cara del presidente georgiano por la de Adolf Hitler.

Ante estos ataques, presumiblemente efectuados por piratas cibernéticos y hackers rusos (Markoff, 2008) Georgia solicitó cooperación internacional para solucionar esta crisis informática.

Irán (Stuxnet)

¿Es posible vulnerar los sistemas SCADA[6]? o ¿Es viable atacar a una red que "no" esté conectada a Internet? La respuesta a ambas interrogantes es "sí", y uno de los casos más estudiados ocurrió en el año 2010, cuando la planta nuclear de Natanz, en Irán, fue atacada por un "malware"[7].

El malware que atacó la planta fue bautizado como Stuxnet, y se infiltró en los sistemas hasta llegar a comprometer directamente los controladores lógicos programables PLC (Siemens), que manejaban los parámetros de las centrifugadoras de uranio, ya que Stuxnet -mediante una estructura altamente sofisticada- contenía cuatro "zero days"[8], como también certificados de autentificación válidos para Windows, entre otras particularidades, haciendo de

[5] Se conoce como ataques defacement a aquellos donde se toma el control de la página web y se modifica su apariencia.

[6] SCADA es el acrónimo del concepto en inglés "Supervisory Control And Data Acquisition", el que se utiliza para realizar softwares que permiten controlar y supervisar procesos industriales a distancia.

[7] Software malicioso que se crea para infiltrarse en programas y dispositivos con el fin de causar daño.

[8] Zero-day, es un tipo de ataque que explota una vulnerabilidad previamente desconocida.

este código malicioso un "gusano"[9] que se propaga a través de las redes sin la intervención del usuario. Igualmente, se replicaba a través de dispositivos USB[10] extraíbles, sin levantar ninguna sospecha, ni alarma.

¿Pero cómo se infiltró, si estas redes son cerradas? Al respecto, se manejan diversas hipótesis. Una de ellas, de acuerdo a la firma de seguridad cibernética Symantec (BBC, 2015) señala que Stuxnet llegó al programa nuclear iraní desde una memoria USB infectada a la red. Posterior a esto, el "gusano" escaló, realizó movimientos laterales y creó persistencia, llegando a las PLC ya mencionadas.

El uranio que se encuentra en los yacimientos mineros no vale por sí mismo para el uso nuclear, ya que lo que se extrae de la tierra es una mezcla sólida de dos tipos de uranio: 235 y el 238, pero sólo el primero sirve para fabricar combustibles, bombas, entre otras utilidades. Teniendo en cuenta que en el planeta se encuentra una concentración del 99,3% del uranio 238 y solamente un 0,7% del tipo 235, es necesario separarlos. La técnica más habitual es el centrifugado, donde primero se pasa todo el uranio a modo gaseoso (se convierte en hexafloruro de uranio mediante un proceso químico) el que luego se introduce en una centrifugadora. Ahí es donde el uranio 238, más pesado, comienza a girar en la periferia, al tiempo que el 235, más ligero, queda más al centro.

El malware atacó los parámetros de las PLCs, manipulando las velocidades y periodos de tiempo dispuestos, pero sin dar señales en los monitores administrados por los operarios de dichas centrifugadoras.

En consecuencia, estallaron 984 centrifugadoras, por lo tanto, este hecho comprueba la posibilidad que un ataque informático pueda destruir infraestructura física y en un futuro podría afectar directamente la integridad de las personas.

En los tres casos descritos, se estima que los estados afectados, dada la complejidad de efectuar la atribución (identificar los causantes de los ataques), ni

[9] Software malicioso el que una vez infiltrado en un dispositivo se propaga hacia otros.

[10] USB es el acrónimo del concepto Universal Serial Bus. Corresponde a un dispositivo de comunicación que conecta y provee alimentación eléctrica entre computadoras y otros dispositivos electrónicos.

su motivación (intereses y vinculaciones), reaccionaron por medio de la diplomacia y las comunicaciones estratégicas, viéndose imposibilitados de invocar el derecho a la legítima defensa. Estonia, acudió a solicitar la defensa colectiva, trayendo expertos de la OTAN, es decir a través de la cooperación internacional. Georgia, por su parte, solicitó ayuda internacional para solucionar la crisis informática que habían provocado los ataques. Por su parte, Irán denunció el hecho públicamente.

Finalmente, se evidencia un problema que se deriva de la atribución. Hay grupos sin motivación, ni vinculación estatal que pueden realizar ataques de gran capacidad, incluso que afecten la infraestructura crítica de los estados, pero a estos, debido a la normativa nacional e internacional, solo se les puede perseguir criminalmente.

REFLEXIONES FINALES

Ante la interrogante ¿Son aplicables la disuasión y la legítima defensa, como modalidades de empleo de los medios de la defensa en el dominio del ciberespacio?, en el presente artículo, después de efectuar un análisis respecto a la conceptualización de disuasión y legítima defensa, y contextualizarlo dentro del ámbito del ciberespacio, ha quedado de manifiesto que teóricamente es factible el aplicar una política digital disuasiva.

No obstante lo anterior, respecto a la implementación de una política digital disuasiva, se evidencian situaciones que lo dificultan. Entre ellas, es factible destacar dos problemáticas relevantes que deben tenerse en cuenta en su implementación:

a. La primera vinculada al desarrollo tecnológico. Para ejercer la disuasión en el ciberespacio, no basta con tener un desarrollo considerable en ciberarmas, sino que conlleva mantener altos estándares de ciberseguridad y ciberdefensa a nivel país (sector privado y público), enfocándose en la confianza, conocimiento-mutuo, sistemas robustos, redundantes y resilientes, a fin de provocar el efecto de evitar una acción por parte de una amenaza

potencial, a través de medidas de negación y reprimenda, ya que las capacidades propias son capaces de mitigarla.

b. La segunda del punto de vista normativo. Ante un ataque a través de esta dimensión se evidencia como muy complejo para los estados (o las víctimas en general) determinar el origen, la atribución de los ataques y las motivaciones que hay detrás, por tanto, no es posible determinar fácilmente contra qué o quién se pretende ejercer la política de disuasión digital, ya que si el ataque fuera de un Estado o comprobablemente vinculado a este, es posible catalogarlo como una agresión. Por otra parte, tendría un tratamiento diferente al ser ejecutado por un grupo atacante con otra motivación, el cual indefectiblemente concurre por la vía de la persecución criminal (a través del derecho interno o internacional según corresponda), independiente del impacto o daño causado.

Existen interrogantes que podrían orientar al desafío de posicionarse como Estado digitalmente disuasivo: ¿Se posee la infraestructura tecnológica suficiente para mitigar operaciones de las potenciales amenazas? ¿Es posible identificar de manera oportuna la atribución y motivación de mis amenazas?

Las respuestas a estas interrogantes, contrastadas con el nivel de desarrollo y coherencia de la estructura tecnológica y normativa imperantes, conforman las directrices fundamentales a la hora de prevenir, planificar y ejecutar la respuesta ante un ciberataque que afecte a un Estado.

En consecuencia, se podría aseverar -tal cual como en el ejercicio de la disuasión en el ambiente físico- que la disuasión en el ciberespacio es un desafío que involucra diferentes actores y de todos los ámbitos. Se estima que la solidez y modernidad de la infraestructura, de la normativa y de la vinculación intersectorial, generan el efecto sobre una ciberamenaza, para que esta desista de realizar una operación, porque los costos y riesgos de ejecutarla son más altos que sus beneficios.

Por otra parte, en el presente artículo se evidencia -respecto a la invocación de la legítima defensa (restrictiva)-, que el posibilitar el uso de las capacidades con

medidas de reprimenda en el ámbito de las ciberoperaciones, en la práctica es muy complejo pero no imposible si es que se tiene la capacidad de determinar con total certeza el origen, atribución y motivación.

Los casos presentados demostraron que ante la imposibilidad de determinar el origen, atribución y motivación del agresor, debieron utilizar herramientas de mitigación de la amenaza, fuera del ambiente del ciberespacio, a través de la diplomacia y de la comunicación estratégica. Estas herramientas se estiman que también formarían parte importante de la acción digital disuasiva y los efectos y coherencia de la misma. Lo recientemente descrito, no significa que los estados no deban tener cibercapacidades de negación ni reprimenda, sino que es complejo el argumentar en los parámetros de la legítima defensa su uso ofensivo ante un ciberataque.

De acuerdo a ello, además se podría establecer que la cooperación internacional, también forma parte (al igual que en la dimensión física) de las modalidades de empleo de los medios factibles de utilizar como parte de la disuasión y acciones de defensa, ante agresiones a través del ciberespacio.

REFERENCIAS

Arenas M. (2013) *Planificación de Fuerza y la Estrategia Marítima*. https://revistamarina.cl/revistas/2013/3/arenas.pdf

Asamblea General de las Naciones Unidas. (1974). *Resolución 3314*. Organización de las Naciones Unidas. https://www.acnur.org/fileadmin/Documentos/BDL/2007/5517.pdf?file=fileadmin/Documentos/BDL/2007/5517

BBC. (2015). *El virus que tomó el control de mil máquinas y les ordenó autodestruirse.* BBC News. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Bravo, C. (2017). *Apuntes de Ciberseguridad*. No publicado.

Chinchilla, M. (2018). *La efectividad de la teoría de la disuasión en la proliferación de armas nucleares en Oriente Medio*. Documento Marco, Instituto Español de Estudios Estratégicos. http://www.ieee.es/Galerias/fichero/docs_marco/2018/DIEEEM02-2018_Armas_Nucleares_MonicaChinchilla.pdf

Consejo de Seguridad. (2004). *Resolución 1540*. Naciones Unidas. https://undocs.org/sp/S/RES/1540(2004)

Diario Oficial. (9 de marzo del 2018). Ministerio de Defensa Nacional aprueba Política de Ciberdefensa. Número 42.003, Sección I, Ministerio del Interior y Seguridad Pública. http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Gobierno de Chile. (2015). *Agenda Digital 2020: Chile digital para todos*. http://www.agendadigital.gob.cl/files/Agenda%20Digital%20Gobierno%20de%20Chile%20-%20Noviembre%202015.pdf

Gobierno de Chile. (2017). *Política Nacional de Ciberseguridad 2017-2022*. https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Markoff, J. (2008). *Georgia sufre la guerra cibernética.* El País. https://elpais.com/diario/2008/08/14/internacional/1218664803_850215.html

McGuinness, D. (2017). *Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país*. BBC Mundo. https://www.bbc.com/mundo/noticias 39800133#:~:text=Los%20estonios%20de%20habla%20rusa%20protestaron

Ministerio de Defensa Nacional. (2017) *Libro de la Defensa Nacional de Chile*. http://www.defensa.cl/media/LibroDefensa.pdf

Organización de las Naciones Unidas. (1945). *Carta de las Naciones Unidas*. http://www.un.org/es/charter-united-nations/