ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

67/2016 04 de julio de 2016

*Agnese Carlini**

Ciberseguridad: un nuevo desafío para la comunidad internacional

Ciberseguridad: un nuevo desafío para la comunidad internacional

Resumen:

Los ataques en el ámbito cibernético de los últimos años contra los intereses nacionales y privados han incrementado el interés de los Estados en esta área. Como resultado, los Estados están aunando esfuerzos en la defensa de los activos de información más críticos. Las estrategias de ciberseguridad se perciben como mecanismos esenciales para prevenir las conflagraciones cibernéticas que podrían tener repercusiones dramáticas comparables a la confrontación militar tradicional. Las ciberamenazas podrían, potencialmente, poner en peligro a los civiles, el medioambiente o paralizar las actividades gubernamentales y la economía de un estado. Sin embargo, la mayor preocupación se atribuye al hecho de que pueda poner en peligro la estabilidad doméstica. Hay muchos objetivos contra los cuales los terroristas y los hackers pueden llevar a cabo ciberataques de manera interconectada creando un efecto dominó. Por lo tanto, para los países, es una prioridad el conseguir alcanzar una resiliencia cibernética y promover una cooperación efectiva entre los interesados en la ciberseguridad, entidades tanto públicas como privadas, autoridades gubernamentales y organizaciones internacionales.
El presente artículo propone un análisis a las posibles respuestas que la comunidad internacional podría adoptar contra las amenazas cibernéticas.

Abstract:

Attacks against national and private interests, over the past years, within the cyber domain have aroused States' interest in strengthening international effort to defend critical information assets. Cyber-security strategies are perceived as essential mechanisms to prevent cyber conflagrations which could have dramatic repercussions as those resulting from traditional military confrontations. Cyber threats could potentially endanger civilians, the environment or paralyse governments' activities and states' economies but the major concern is that of attribution- who can jeopardize one's domestic stability. There are many targets against which terrorists and hackers can conduct cyberattacks and are all interconnected to each other, creating a domino effect. It is therefore a priority for countries to achieve cyber resilience and promote effective

cooperation among private/public cybersecurity stakeholders, governmental authorities and International Organizations.
The present article proposes an analysis on the possible responses the International Community might adopt against cyber threats.

Palabras clave:

Ciberataques, ciberterrorismo, ciberseguridad, *Jus ad Bellum.*

Keywords:

Cyberattacks, cyberterrorism, cybersecurity, Jus ad Bellum.

Introducción

El advenimiento de Internet y su expansión han demostrado ser una de las revoluciones tecnológicas más importantes de la historia contemporánea. En 21 años ha habido un crecimiento enorme en el número de usuarios de Internet, en 1993 se estima que había 14 millones y en julio 2014 rondaba los 2900 millones.

Hoy en día, las sociedades occidentales dependen profundamente de los sistemas informáticos para los procesos industriales, las fábricas, los bancos, las instalaciones de energía, etc. que además están interrelacionados. El surgimiento del quinto dominio planteó preguntas sobre la evolución de las medidas de seguridad y de la ley para hacer frente a las nuevas amenazas en el ciberespacio.

A pesar de que las operaciones cibernéticas no hayan jugado un papel muy importante en los conflictos, el enfoque de la comunidad internacional sobre este asunto ha aumentado considerablemente a finales de los años noventa y aún más, después de los atentados del 9/11, de Estonia 2007, Stuxnet 2010 y los acontecimientos más recientes, en febrero 2015, con *Charlie Hebdo*. El marco jurídico internacional existente para enfrentarse a este nuevo desafío parece bastante embrionario y todavía no ha habido un debate sobre la interpretación e implementación de las reglas existentes. Esto se debe también al hecho de que la Era Digital ha puesto a prueba el criterio tradicional de las fronteras nacionales, aumentando las dificultades de aplicarlas a la jurisdicción nacional.

Por lo tanto, la guerra moderna de la información lleva consigo muchas preocupaciones jurídicas: qué leyes existentes son relevantes para este nuevo modelo de guerra y cómo se pueden implementar para poder limitar los ataques cibernéticos y el ciberterrorismo. El espacio cibernético es un dominio artificial que se diferencia de los otros cuatros dominios de guerra (tierra, aire, mar y espacio); aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa. El ciberespacio no está aislado sino profundamente vinculado y apoyado por medios físicos, como por ejemplo las redes eléctricas. Por lo tanto esta interconexión tendrá repercusiones graves sobre las estrategias de seguridad nacionales e internacionales[1].

[1] Introduction to cyberspace operations, November 2011: https://doctrine.af.mil/download.jsp?filename=3-12-D01-CYBER-Introduction.pdf

Ciberterrorismo

> «Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb»[2]. *National Research Council.*

Los términos «guerra cibernética» y «terrorismo cibernético» se han usado ampliamente en informes oficiales gubernamentales, por los medios de comunicación social y entre académicos. El ciberterrorismo sigue siendo un concepto algo controvertido, expertos y académicos no se ponen de acuerdo sobre su definición. El debate intelectual se enfoca sobre todo en el ámbito, la motivación, los métodos, y los objetivos del ciberterrorismo, tratando de averiguar la medida en la que podría solaparse con guerra cibernética o terrorismo común[3].

«El terrorismo cibernético se puede definir como el uso intencional del ordenador, de las redes, y el intento político de causar destrucción y causar daño para objetivos personales»[4]. Si el ciberterrorismo se trata como terrorismo tradicional, entonces la única variante a la que nos enfrentamos es el uso de la tecnología para causar la destrucción física de las personas y de las infraestructuras. Los ataques cibernéticos que se han sufrido hasta ahora no se pueden definir como accidentes de ciberterrorismo, a menos que la intención no fuera la de causar terror entre la población.

Una definición más amplia de ciberterrorismo ha sido concedida por el Technolytics Institute: «El uso premeditado de actividades peligrosas, o la amenaza, contra ordenadores o redes, con la intención de causar daño o fomentar objetivos sociales, ideológicos, religiosos o políticos. O para intimidar a las personas con miras a alcanzar los propósitos»[5]. Con el colapso de la URSS, el mundo se dio cuenta de la importancia de la tecnología en el contexto de la seguridad nacional e internacional. Esta dependencia creciente por parte de los Estados ha aumentado el miedo a que los sistemas de información se pudieran utilizar como armas o fueran objeto de ataques. En

---

[2] "Los terroristas de mañana serán capaces de hacer más daño con un teclado que con una bomba."

[3] VICTORIA BARANETSKY "What is cyberterrorism? Even experts can't agree." Harvard Law Record, November 2009
http://web.archive.org/web/20091112093639/http://www.hlrecord.org/news/what-is-cyberterrorism-even-experts-can-t-agree-1.861186

[4] "Cyberterrorism", Matusitz Jonathan, April 2005. American Foreign Policy Interests, p.137-147.

[5]"Cyber operations and Cyber-terrorism, Handbook Number 1.02"
http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA439217

principio, EE.UU. creía que los enemigos, incapaces de derrotar a las tropas americanas utilizarían métodos alternativos para dañarle[6].

El ciberterrorismo se considera un gran desafío para nuestra economía, en cuanto al hecho de que podría poner en peligro todo el sistema económico. Más aún, la expansión continua de Internet causa una fuerte dependencia por parte de la población y el terrorismo en el ciberespacio podría ser uno de los diez eventos que lleve a la extinción de la raza humana[7]. Aunque destaquen problemas como la contratación y gestión del talento, los terroristas tienen muchas ventajas para usar el ciberespacio, respecto a los «viejos» ataques físicos ya que son, por ejemplo, más asequibles, necesitando una inversión menor en armas y personas a la vez que pudiéndose realizar de forma remota. El resultado podría ser un colapso de la economía, insertar virus en las infraestructuras de red, e incluso peor: suprimir las redes energéticas[8].

Después de los ataques terroristas del 11S, el ciberterrorismo es uno de los temas principales en las agendas políticas y de seguridad de muchos países. Aunque el desafío del ciberterrorismo podría ser manipulado por otros intereses, su amenaza a la sociedad no puede ser ignorada. Con la creciente interdependencia en Internet es probable que la amenaza aumente[9].

Motivaciones para el uso del ciberespacio

Como los ataques cibernéticos por parte de hackers u otras entidades, el ciberterrorismo representa una alternativa interesante para los terroristas contemporáneos por varias razones:

---

[6] POLLARD, N.A. (2004)"Indications and warning of infrastructure attack", in Nicander, L. and Ranstorp, M. (eds) "*Terrorism in the Information Age: New Frontiers"?* Stockholm: National Defence College, p. 41-57

[7] "Top ten events that might end the human race", Business Times, December 2010 http://www.businesstimes.co.tz/index.php?option=com_content&view=article&id=586:top-ten-events-that-may-end-the-human-race&catid=37:column&Itemid=60

[8] ARQUILLA J. *"The great cyberwar of 2002"*. (1998) http://www.wired.com/wired/archive/6.02/cyberwar.html

[9] GABRIEL WEIMANN Special Report, United States Institute of Peace. *"Cyberterrorism, How real is the threat?",* May 2004 http://www.usip.org/publications/cyberterrorism-how-real-the-threat

- Un ataque cibernético será siempre más barato que un ataque tradicional. Lo único que se necesita es un ordenador y una conexión a Internet, eliminando el gasto en armas o explosivos.
- Se puede disfrutar del anonimato llevando a cabo ataques remotos. La ventaja es un entrenamiento físico menor y la posibilidad de atacar en cualquier parte del globo sin tener que viajar.
- Un elevado número de objetivos gubernamentales, privados, multinacionales, etc. Varios estudios han demostrado la vulnerabilidad de las infraestructuras esenciales y la amenaza que un ataque de ciberterrorismo representaría para su funcionalidad.
- La cobertura mediática sería muy elevada, causando una grave preocupación entre la población y las autoridades políticas y militares.
- Un ataque simultáneo en el espacio físico así como en el ciberespacio podría llevar la amenaza terrorista a un nivel mucho más avanzado y difícil de contener. Recientemente, Keith Lourdeau, subdirector adjunto de la división cibernética del FBI, ha declarado que la amenaza terrorista en EE.UU. se está expandiendo rápidamente y que «los grupos terroristas podrían desarrollar o contratar a hackers, sobre todo con el objetivo de cumplir ataques físicos más grandes con la ayuda del ciberespacio»[10].

La amenaza representada por el ciberterrorismo ha llamado la atención de los responsables políticos, las agencias de seguridad, las empresas privadas y la población. A pesar de las sombrías predicciones todavía no se ha sufrido ningún accidente. Aun así, el hecho de que los terroristas puedan utilizar la red para infligir daños causa preocupación entre la Comunidad Internacional y, por lo tanto, la necesidad de buscar medidas o adaptar las existentes para protegerse.

Medidas existentes

Con el paso del tiempo aumenta la frecuencia de los ataques cibernéticos y, por lo tanto, evoluciona el consenso general para poder aplicar las leyes internacionales existentes a este nuevo modelo de guerra. En 1996, la Corte Internacional de Justicia, en la Opinión

[10] D. VERTON "CIA to publish cyberterror intelligence estimate", *CompupterWeekly.com*. 2004.

Consultiva sobre las Armas Nucleares, declaró que las disposiciones existentes en la Carta de las Naciones Unidas sobre el uso de la fuerza son aplicables independientemente de las armas utilizadas[11]. En este sentido es importante recalcar la denominada "cláusula Martens", en cuanto se refiere a esos casos que no se mencionan en la Carta de las NN.UU. Dicha cláusula resulta ser muy efectiva en el momento en que la tecnología militar está experimentando una evolución significativa[12].

El problema con el Derecho Internacional depende de las diferencias clave entre el dominio cibernético y los otros cuatro dominios. En primer lugar, un ataque cibernético no siempre conlleva una destrucción física. En segundo lugar, la Carta de las Naciones Unidas cuenta con la atribución de la responsabilidad del Estado durante dichos ataques, pero resulta mucho más difícil cuando se trata del contexto cibernético. Sin embargo, estos límites podrían llevar, en un futuro próximo, a la firma de un nuevo tratado para entender y enfrentarse mejor con este nuevo concepto de guerra[13].

La naturaleza de los ataques cibernéticos ha evolucionado con el paso del tiempo; los programas maliciosos existen desde los años 70 y se dispersaron manualmente hasta el día en el que Internet empezó a jugar un papel importante en la vida diaria. Los ataques más recientes han sido contra páginas webs privadas y públicas con el objetivo de causar caos en un determinado Estado y contra industrias para retrasar proyectos importantes. Se ha observado la dificultad en localizar el origen de estos ataques y, según ha dicho Y.Dinstein -Profesor Emérito de Derecho Internacional en la Universidad de Tel Aviv- solo los ataques lanzados o patrocinados por los Estados son los únicos que pueden ser juzgados por las normas de Derecho Internacional[14].

Jus ad Bellum

La fuente principal moderna del *Jus ad Bellum* deriva de la Carta de las Naciones Unidas, en concreto el artículo 2(4)- «Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la

[11] *"Legality of the threat or use of nuclear weapons, Advisory Opinion",* I.C.J Reports 1996

[12] *Op. cit.*

[13] SCOTT HACKELFORD, "*From Nuclear War to Net War: analogizing Cyber attacks in International Law*", 27 Berkeley Journal of International Law, 2009.

[14] YORAM DINSTEIN, *"Computer Network Attacks and Self-Defense"*, US Naval War College International law Studies, 2002.

integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas»[15] y el artículo 51- «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 haya tomado las medidas necesarias para mantener la paz y la seguridad internacional. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacional»[16].

En primer lugar, los ataques cibernéticos patrocinados por los Estados se califican como «uso de la fuerza» contra otro Estado, violando el artículo 2(4) de la Carta de las Naciones Unidas y provocando un conflicto armado internacional.

En segundo lugar, en caso de operaciones cibernéticas como «ataques armados», el Estado atacado tiene el derecho de legítima defensa, de otra manera prohibido por la Carta de las Naciones Unidas. Por último, los ataques cibernéticos resultan como «actos de agresión y amenaza a la paz», por lo tanto es mandato del Consejo de Seguridad restablecer la seguridad y la paz internacional bajo el respeto de los artículos 2(4) y 51.

Para entender mejor los ataques cibernéticos como «uso de la fuerza» debería tomarse en consideración el instrumento, el objetivo y un enfoque basado en los efectos. El más relevante parece ser este último, analizado sobre todo por el Grupo de Expertos del Manual de Tallin, el cual dijo que «los actos que lesionan o matan personas, que dañan o destruyen objetos son inequívocamente uso de la fuerza» y que «ataques cibernéticos no destructivos cuya finalidad es perjudicar la estabilidad económica y gubernativa de un Estado no se califica como «uso de la fuerza»[17]. El manual enumera ocho factores —propuestos anteriormente por Michael N. Schmitt en 1999— esenciales para determinar si una operación cibernética puede o no ser clasificada como «uso de la

[15] UN CHARTER http://www.un.org/es/sections/un-charter/chapter-i/index.html

[16] *Op. cit.*

[17] MICHAEL N. SCHMITT (ed), Tallin Manual on the International Law Applicable to Cyber Warfare, Cambridge University Ress 2013. P. 45

fuerza». Estos factores consisten en: invasividad, severidad, carácter militar, inmediatez, participación estatal, cuantificación de los efectos, presunta legalidad y franqueza[18]. Según el Grupo de Expertos, una operación cibernética cuenta como «uso de la fuerza» cuando produce el mismo nivel de daño físico a objetos y personas que las *Kinetic Operations*[19] [20]. Sin embargo, Michael N.Schmitt ha recalcado que el enfoque del Manual de Tallin es demasiado ambiguo.

Por su parte, el artículo 2(4) de la Carta ONU se refiere explícitamente a los Estados[21] y prohíbe el uso de la fuerza en lo que se refiere al reconocimiento internacional de la soberanía. Esto significa que el uso de la fuerza debe imputarse a un Estado concreto, incluso cuando estas acciones estén realizadas por personas o agentes del Estado que es responsable internacionalmente por sus conductas. Esas personas o entidades, cuyo vínculo con un Estado no es lo suficientemente claro y que hace imposible empezar un proceso internacional sobre la responsabilidad estatal, se califican como «actores no estatales». Las acciones cibernéticas realizadas por los actores no estatales o hackers privados se consideran bajo el Derecho Humanitario Internacional y el Derecho Penal Internacional, excediendo del ámbito del artículo 2(4) de la Carta ONU[22]. De todas formas, no se puede excluir el riesgo que representan los ataques cibernéticos perpetrados por estas entidades respeto al hecho de que siguen siendo una amenaza para la seguridad y la paz internacional. Sin embargo, antes de tomar en consideración una intervención del Consejo de Seguridad, para preservar la paz y la seguridad, es necesario que los Estados afectados respondan mediante su Derecho Penal Nacional[23].

La prohibición del uso de la fuerza no está preservada solo por la Carta de las Naciones Unidas sino que constituye costumbre internacional[24]. El problema de aplicar normas

---

[18] MICHAEL N. SCHMITT, *"Computer Network Attack and the Use of Force in International Law".* P.19

[19] *Kinetic Operations* es un eufemismo para las medidas militares que implique la fuerza letal.

[20] NOAH TIMOTHY, "Birth of a Washington Word", November 20, 2002.

[21] Article 4 of the UN Charter declares that only states can be "members" of the UN, therefore the prohibition of the use of force concerns States.

[22] ALBRECHT RANDELSHOFER, "Article 2(4)", in Bruno Simma (ed), *"The Charter of the United Nations: A Commentary",* vol. 1, 2002; LASSA OPPENHEIM, "Internationale Law: A Treatise", vol. 2, 1921; ALFRED VERDROSS and BRUNO SIMMA, *"Universelles Völkerrecht: Theirue und Praxis",* 1984.

[23] NILS MELZER, *"Cyberwarfare and International Law"*, 2011

[24] Statute of the International Court of Justice, June 26, 1945, art. 38 1(b), 832 U.S.T.S 993, 1978 Y.B.U.N 1197.

consuetudinarias a los ataques cibernéticos es la discrepancia entre la Carta de la ONU y las normas consuetudinarias internacionales[25] debido a la adaptabilidad de los cambios. Por lo tanto, la norma consuetudinaria adoptará la prohibición del uso de la fuerza a nuevas armas localizadas dentro de la esfera de las Fuerzas Armadas. Aun así, para que los ataques cibernéticos lleguen a ese nivel deben ser similares, si no más graves, como lesiones a humanos y destrucción física de las propiedades[26].

Hasta ahora los ataques cibernéticos están sujetos a confusión. A menos que la comunidad internacional esté dispuesta a aportar unos cambios radicales, las respuestas de los Estados a esta nueva amenaza serán diferentes, resultando en reacciones ilícitas. Para comprender si una nueva tecnología se ha convertido en una forma de guerra es necesario ver «si la técnica está más o menos asociada a las fuerzas armadas de un Estado y que la utilicen»[27]. Numerosos Estados han incluido la tecnología cibernética en sus doctrinas militares; expertos de formación cibernética sugieren que los programas maliciosos, gusanos informáticos, etcétera «son simplemente otros sistemas de armas, más baratos y más rápidos que un misil, potencialmente más encubiertos pero no menos dañinos.» Se ha observado que: «no es ni el diseño de un dispositivo ni su funcionamiento normal lo que lo hace un arma sino la intención con la que se usa y sus efectos. El uso de cualquier dispositivo, o diferentes dispositivos, que conlleven en un número considerable de muertes y/o gran destrucción deben considerarse ataques armados»[28]. El Consejo de Seguridad ha respaldado esta declaración para reafirmar el derecho de legítima defensa después de los ataques del 11S, donde se utilizaron aviones civiles secuestrados por terroristas[29]. La problemática principal en la determinación de si los ataques cibernéticos se pueden considerar armamentos, y por lo tanto representan una amenaza a la paz y seguridad internacional, está más allá de la que estipula la Carta de las Naciones Unidas. En el momento en que se promulgó, los ataques cibernéticos no eran ninguna amenaza y por lo tanto no se tomaron en consideración. De todos

[25] Op. Cit.

[26] MICHARL N. SCHMITT, *"Computer Network Attack and the use of force in International Law: thoughts on a normative framework"*. P. 18

[27] D.B. SILVER, *"Computer Network attack as a use of force under Article 2(4) of the UN Charter".*

[28] KARL ZEMANEK, "Armed Attack", in Rüdiger Wolfrum (ed.), Max Planc Encyclopedia of Public International Law, 2010.

[29] S/RES/1368 (2001) 09/12/2001 and S/RES/1373 (2001) 09/28/2001.

modos, la Carta sigue siendo indispensable en el contexto internacional, aunque podría ser más maleable a los cambios y a las complejas relaciones internacionales[30].

Estrategias contra la amenaza cibernética

Oponerse al cibercrimen requiere de diferentes tácticas comúnmente utilizadas para los demás crímenes. En el espacio cibernético los criminales no tienen que estar físicamente en la escena del crimen, además de que pueden cometer más de una acción simultáneamente. Según el principio de soberanía territorial, los Estados no pueden entrometerse en las infraestructuras cibernéticas con base en otros Estados. Por otra parte, debido a la incertidumbre de los orígenes resulta difícil atribuir los ataques cibernéticos a un determinado Estado.

La falta de seguridad en el ciberespacio deteriora gravemente la confianza entre la comunidad TIC (tecnologías de la información y la comunicación) que está sufriendo una de las revoluciones más importantes en la historia de la humanidad. La seguridad y la prosperidad de cualquier país está conectada a la protección de las redes TIC, a través de las cuales la población puede ejercer sus libertades fundamentales de expresión, asociación e información. Se necesita una atención excepcional para evitar que el ciberespacio se transforme en una plataforma peligrosa para los Estados y las poblaciones. Aunque el ciberespacio es empleado principalmente por el sector privado y va más allá de las fronteras nacionales, los Estados tienen la responsabilidad última de proteger las infraestructuras TIC con sede en su territorio, siendo el deber de cualquier gobierno el de garantizar el cumplimiento de las libertades individuales en el ciberespacio.

La interdependencia de las redes reclama un enfoque holístico para poder garantizar un nivel satisfactorio de seguridad en el ciberespacio. Razón por la cual los responsables políticos y los expertos creen en la importancia de la cooperación entre naciones, logrando, como objetivo último, la capacidad de prevenir el ataque, enfrentarse mientras está ocurriendo, responder activamente, reducir al máximo posible sus efectos, encontrar su origen y restablecer la función original.

[30] *Op. cit* 26, p.16

En un entorno tan evolutivo, los Estados y las organizaciones internacionales como la OTAN, o las organizaciones policiales como la INTERPOL o la EUROPOL, siguen desarrollando sus estrategias respectivas en el quinto dominio. Los Estados miembros de la EU están trabajando para asegurar un acceso seguro y libre a Internet, desarrollando, entretanto, estrategias cibernéticas más sofisticadas para impedir nuevas amenazas.

Los ataques cibernéticos pueden ser muy lucrativos ya que las informaciones robadas podrían ser vendidas a otros adquirentes debilitando así, no solo la economía, sino también la seguridad de un país. Para que todos los países puedan beneficiarse de un espacio cibernético seguro, es importante un esfuerzo de conjunto, por parte de todas las partes interesadas, a nivel nacional. Entre las medidas más importantes de las estrategias de ciberseguridad presentadas por diferentes países están:

- La mejora de las capacidades técnicas, operativas y analíticas de las instituciones involucradas en la seguridad cibernética, aumentando la capacidad estatal en el análisis, la mitigación, la prevención y la capacidad de reacción a cualquier ataque cibernético.
- Asistir en la colaboración entre el sector privado y el público para alentar la protección de la propiedad intelectual nacional.
- Promover una cultura de seguridad entre la población y las instituciones, informando sobre las amenazas en el ciberespacio.
- Aumentar las capacidades de los Estados en la protección de las infraestructuras críticas y estratégicas de los ataques cibernéticos.
- Apoyar de manera incondicional la cooperación internacional en la ciberseguridad, sobre todo esas iniciativas que ya se están debatiendo dentro de las Organizaciones Internacionales.
- Preparar a las Fuerzas Armadas para las nuevas amenazas, estipulando nuevas alianzas en el quinto dominio.
- Alentar la gobernabilidad de Internet para favorecer la innovación de la web; esta medida está patrocinada sobre todo por EE.UU., refiriéndose a esos países que imponen restricciones sobre la información para prevenir o reprimir a la oposición.

Cuando se habla de medidas eficaces contra las amenazas cibernéticas entre los problemas principales se encuentra la falta de definición común del término ciberseguridad. La definición dada por algunas autoridades es diferente a las aceptadas por la mayoría de la Comunidad Internacional, por lo tanto una cooperación en el ámbito cibernético resulta no solo difícil sino casi imposible. La seguridad en el ciberespacio es de interés común, no solo de un único Estado sino también de toda la Comunidad Internacional.

Pese a los esfuerzos, países como EE.UU., China o Rusia tienen un enfoque diferente en todo lo que se refiere al espacio cibernético, las actividades en su interior y las respuestas a las diferentes amenazas. La declaración del ciberespacio como un nuevo dominio de guerra ha suscitado unas cuantas preocupaciones para la administración china que interpretó esta decisión como «una amenaza a la paz mundial que podría causar una carrera armamentista[31] en el ciberespacio y un conflicto militar, con consecuencias desastrosas para toda la humanidad»[32]. A pesar de sus temores, China, por su parte, ha optado por una política de más transparencia en temas de ciberseguridad. Según el Presidente Xi Jinping, las relaciones que se han ido desarrollando entre China y EE.UU. son de confianza no fiable, pero esto no quiere decir que «aquellos que buscan un terreno común mientras mantienen sus diferencias no puedan ser socios. Podemos tener desacuerdos, aun así, no deberíamos tenerlos en temas para la comunicación. Podemos tener argumentos pero no debemos abandonar la confianza […] Deberíamos ver que la cooperación entre China y Estados Unidos trae beneficios a ambos así como a otros países, mientras que un enfrentamiento puede dañar a los dos o incluso al mundo entero»[33]. Finalmente, las diferentes percepciones de ciberseguridad tienen un impacto directo en las relaciones cibernéticas entre China y EE.UU. La percepción china de la superioridad occidental en Internet hace difícil que la República Popular China pueda cooperar internacionalmente en el ámbito cibernético. Mientras que las futuras cumbres verán el intento de China de promover su teoría de una «ciber-hegemonía occidental» a países afines, EE.UU. y Occidente deberían

[31] AMY CHANG *"Warring State- China's Cybersecurity Strategy"*, December 2014, p.27

[32] "The United States bears primary responsibility for stopping Cyber War", Zhong Sheng quoted in "Chinese Views on Cybersecurity in Foreign Relations" by Michael D. Swaine

[33] LU WEI *"China-US should cooperate in cyberspace governance",* December 2014, China-US Focus. http://www.chinausfocus.com/peace-security/china-us-should-cooperate-in-cyberspace-governance/

comprometerse a desarrollar un mayor conocimiento de la mentalidad china en el ciberespacio y disminuir cuanto posible los malentendidos entre las autoridades políticas y militares chinas.

Por su parte, la mayor preocupación para Rusia igual que para China es la de la «soberanía de Internet» que asegura la capacidad del Estado de controlar el espacio de la información. La ciberseguridad está percibida de forma distintiva por Rusia y Occidente; los oficiales rusos creen en la necesidad de las fronteras nacionales, mientras que los países occidentales subrayan la importancia de la libre circulación de la información. Aunque Rusia esté colaborando con Occidente, la definición poco clara de espacio de información dificulta el desarrollo de nuevas negociaciones. El Gobierno ruso, como la contraparte china, suelen declarar que la actividad cibernética realizada es exclusivamente frente a las amenazas externas. A nivel internacional, la Federación Rusa coopera con otros países en ámbitos económico, político y militar para mejorar la seguridad de la información.

Después del ataque cibernético a Estonia en 2007, la OTAN ha decidido expandir su autoridad. En respuesta a la cada vez más amenazadora naturaleza de los ataques cibernéticos, la OTAN ha decidido adoptar una nueva política apoyada por los aliados en la cumbre de Gales[34], en septiembre de 2014. La prioridad principal es la de proteger el sistema de comunicaciones de la Alianza. Además, los aliados han decidido aumentar el intercambio de información y asistencia mutua a través de la cooperación entre la OTAN y las autoridades nacionales para garantizar un nivel apropiado de los sistemas de comunicaciones e información de ciberseguridad. Debido al hecho de que las amenazas cibernéticas no conocen las fronteras nacionales, la OTAN colabora estrechamente con los países y las organizaciones para aumentar la seguridad internacional; sobre todo con la UE, las NN.UU., la OSCE para evitar la duplicación de trabajos.

En la estrategia de ciberseguridad de la UE se reiteran los derechos presentados en la Carta de los Derechos Fundamentales de la Unión Europea, sin los cuales las personas

[34] http://www.ieee.es/Galerias/fichero/docs_informativos/2014/DIEEEI13-2014_Ciberseguridad_CumbreGales_DRM.pdf

no podrían navegar por la red[35]. Un acceso limitado a Internet significaría una restricción de las actividades diarias, inaceptable en el siglo XXI. Aunque la ciberserguridad es un asunto de los Estados miembros, la estrategia de la UE presenta cinco prioridades importantes: alcanzar la *cyber resilience*[36]; reducir el crimen cibernético; desarrollar una política de defensa cibernética conectada a la Política Común de Seguridad y Defensa; promover los recursos industriales y tecnológicos para la ciberseguridad y finalmente establecer una política internacional en el ciberespacio para la UE y promover sus valores fundamentales. La estrategia europea de ciberseguridad ha puesto la base para una política futura, donde instrumentos comunes de comunicaciones entre los miembros deberían ser usados activamente para asegurar la integridad del espacio cibernético. La estrategia actual destaca la importancia de la colaboración entre el sector público y privado. Dicha colaboración se ha desarrollado como medio adecuado para tratar las amenazas tradicionales y no tradicionales a la seguridad pero cuando se habla de seguridad nacional cibernética este convenio resulta problemático. Por lo tanto, una intervención por parte de las agencias de seguridad de la UE es necesaria para tener políticas compartidas e instrumentos para reforzar las estrategias nacionales existentes.

Conclusión

Los ataques cibernéticos, independientemente de su matriz, representan una amenaza para la Comunidad Internacional. Las fronteras desaparecen, creando una interconexión entre los Estados, las personas y el sector público/privado. Todos los actores, incluso los CERTs y las NIS[37], así como las otras partes interesadas, deben asumir las responsabilidades a nivel nacional e internacional para incrementar la ciberseguridad.

El intercambio de información entre el sector público y privado, a nivel nacional, es necesario para tener una visión completa de cuáles podrían ser las posibles y diferentes

[35] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[36] Resiliencia cibernética: se trata de la gestión y no la eliminación de riesgos.

[37] *Network and Information Security.*

amenazas, y así desarrollar tecnologías para responder rápidamente a las amenazas cibernéticas sin sufrir daños importantes.

La coordinación y la colaboración están siendo fomentadas tanto a nivel regional como internacional, estableciendo una estructura de cooperación efectiva donde cada agencia preserva sus peculiaridades y actúa según los valores fundamentales de la Unión Europea, promoviendo un uso pacífico, trasparente y abierto de la web.

En la era digital, todos los actores deben cooperar estrechamente para preservar la libertad y la integridad de Internet. Esta colaboración entre las agencias estatales, las compañías privadas, organizaciones sin ánimo de lucro, organizaciones regionales e internacionales requiere nuevas políticas.

Lamentablemente, un acuerdo formal de cooperación no se ha firmado aún y los países cuentan con medios informales y bilaterales para investigar los crímenes cibernéticos. Es indispensable que participen el mayor número de países en la estipulación de acuerdos, estableciendo conexiones sólidas para preservar la ciberseguridad y organizar acuerdos formales. No será un proceso fácil, dado que cada país tratará de imponer sus prioridades y estrategias, pero sigue siendo de extrema importancia.[38i]

*Agnese Carlini**
Investigadora
Doctora en Relaciones Internacionales

[38] Edited by JAMES ANDREW LEWIS *"Cyber Security: Turning National Solutions into International Cooperation"*, Chapter 1 "International Cyber-Security Cooperation" Michael Vatis.