1-1-2018

Ciberseguridad: los acuerdos de cooperación para el tratamiento de las amenazas en el ciberespacio. El caso de Estados Unidos y China

Eliana Paola Rodríguez Zubieta
Universidad de La Salle, Bogotá

Alba Yaneth Cordero Saavedra
Universidad de La Salle, Bogotá

CIBERSEGURIDAD: LOS ACUERDOS DE COOPERACIÓN PARA EL TRATAMIENTO DE LAS AMENAZAS EN EL CIBERESPACIO. EL CASO DE ESTADOS UNIDOS Y CHINA

Trabajo de grado bajo la modalidad de monografía para optar por el título de Profesional en Negocios y Relaciones Internacionales

ELIANA PAOLA RODRÍGUEZ ZUBIETA
ALBA YANETH CORDERO SAAVEDRA

Asesor:
Carlos Pérez Espitia

UNIVERSIDAD DE LA SALLE

FACULTAD DE CIENCIAS ECONÓMICAS Y SOCIALES

PROGRAMA DE NEGOCIOS Y RELACIONES INTERNACIONALES

BOGOTÁ D.C

2018

CIBERSEGURIDAD: LOS ACUERDOS DE COOPERACIÓN PARA EL TRATAMIENTO DE LAS AMENAZAS EN EL CIBERESPACIO. EL CASO DE ESTADOS UNIDOS Y CHINA

ELIANA PAOLA RODRÍGUEZ ZUBIETA
ALBA YANETH CORDERO SAAVEDRA

UNIVERSIDAD DE LA SALLE
FACULTAD DE CIENCIAS ECONÓMICAS Y SOCIALES
PROGRAMA DE NEGOCIOS Y RELACIONES INTERNACIONALES
BOGOTÁ D.C
2018

TABLA DE CONTENIDO

Resumen

La era digital y la creciente dependencia tecnológica que experimentan los países, especialmente los países desarrollados, platean un desafío crítico al poder de los Estados. La gravedad de los crecientes ataques cibernéticos ha demostrado que los temas relacionados con la ciberseguridad –aunque los Estados quisieran- no pueden ser abordados y/o gestionados única y exclusivamente dentro de las fronteras nacionales, esto teniendo en cuenta que muchos de los riesgos y amenazas provienen de otros Estados u organizaciones que se encuentran fuera de las fronteras estatales. Hacer frente a las amenazas del ciberespacio requiere la cooperación entre los diferentes actores del sistema internacional. Conscientes de las nuevas amenazas, los gobiernos y lo actores no estatales han dirigido la mirada hacia la ciberseguridad, como un mecanismo orientado a elaborar medidas de seguridad que contrarresten el incremento de las amenazas informáticas que afectan significativamente las relaciones interestatales y de esta manera, asegurar sus recursos y actividades en el ciberespacio, reforzando la cooperación multilateral para defenderse de las amenazas cibernéticas; lo que se ha convertido en un reto debido a que estas problemáticas difieren en gran medida de las cuestiones de seguridad tradicionales. Para efectos de esta investigación se analizan las estrategias y los intentos de cooperación –en lo que a ciberseguridad se refiere- entre China y Estados Unidos, y los factores que obstaculizan el éxito de la cooperación en la relación bilateral.

Palabras clave: *Ciberseguridad, Cooperación Internacional, ciberespacio, ciberataques, Relaciones Internacionales.*

Abstract

The digital age and the growing technological dependence experienced by countries, especially developed countries, pose a critical challenge to the power of States. The severity of the increasing cyberattacks has shown that issues related to cybersecurity - even if the States want to - cannot be addressed and / or managed solely and exclusively within national borders, taking into account that many of the risks and threats they come from other states or organizations that are outside the state borders. Addressing the threats of cyberspace requires cooperation among the different actors of the international system. Aware of the new threats, governments and non-state actors have

turned their gaze towards cybersecurity, as a mechanism aimed at developing security measures that counteract the increase in computer threats that significantly affect inter-state relations and thus ensure its resources and activities in cyberspace, reinforcing multilateral cooperation to defend against cyber threats; which has become a challenge because these issues differ greatly from traditional security issues. For the purposes of this research, the strategies and the attempts of cooperation -in terms of cybersecurity- between China and the United States, and the factors that hinder the success of cooperation in the bilateral relationship are analyzed.

Key Words: Cybersecurity, international cooperation, cyberspace, cyberattacks, international relations.

INTRODUCCION

El ciberespacio enfrenta a los Estados a nuevas amenazas que van desde el tradicional hurto y fraude, hasta amenazas más elaboradas como el espionaje, daño a la información, robo de propiedad intelectual y ciberataques. A pesar de que la mayoría de los Estados son conscientes de que una sociedad cada vez más interconectada se puede convertir en un arma de doble filo, también son conscientes que la dinámica tecnológica y la evolución de las herramientas informáticas es imparable; es por ello, que la defensa de dichas amenazas requiere un esfuerzo coordinado no solo a nivel nacional, sino también internacional. La ciberseguridad se presenta como la forma en que las naciones – a través de estrategias de carácter nacional e internacional- buscan prevenir las acciones hostiles de actores maliciosos. La ciberseguridad se ha convertido en los últimos años, en un fenómeno de gran importancia debido al acelerado desarrollo de la era de la información y su repercusión en la esfera de las relaciones internacionales. Los efectos devastadores de algunos ataques cibernéticos (Estonia 2007, Georgia 2008 e Irán 2010) pusieron en relieve la necesidad de hacer de la ciberseguridad una prioridad en la agenda de seguridad.

El desarrollo de políticas y estrategias de ciberseguridad no es una tarea fácil, teniendo en cuenta que el problema empieza porque no hay un consenso respecto a la terminología sobre ciberseguridad. Sin embargo, las naciones deben ser conscientes que se enfrentan al mismo tipo de amenazas y que poner la cooperación internacional como una prioridad en sus agendas de seguridad nacional es necesario.

De acuerdo con Kshetri (2014) desde el punto de vista de la seguridad nacional y las relaciones internacionales el ciberespacio añade tres grandes problemas: 1) éxito limitado en la cooperación en los temas de ciberseguridad, como consecuencia de la falta de normas para la participación en el ciberespacio; 2) falta de evidencias fácticas y concluyentes que permitan conocer a ciencia cierta quien es el perpetrador de los ataques, la mayoría de las evidencias son circunstanciales; 3) las violaciones son más frecuentes en el ciberespacio que en el espacio físico; en realidad esto es una consecuencia del segundo, debido a que la naturaleza del ciberespacio hace más fácil desacreditar la evidencia presentada por los adversarios. En lo que respecta a la cooperación entre Estados Unidos y China, para mitigar las amenazas presentes en el ciberespacio, esta ha sido poco exitosa. Siguiendo a Kshetri (2014) las alegaciones y contra alegaciones son características del discurso entre Estados Unidos y China en el tema de seguridad cibernética. Analistas occidentales han acusado en varias ocasiones al gobierno chino y al EPL de estar involucrados en ataques

cibernéticos internacionales. El poco éxito de la cooperación entre China y Estados Unidos se debe principalmente a la desconfianza mutua entre los dos Estados, como lo afirma Wortzel (2014) China teme que Estados Unidos pueda utilizar el internet y las ciberoperaciones con el objetivo de amenazar la legitimidad del Partido Comunista Chino. "*China y los Estados Unidos están atrapados en el ciclo culpa-contra-castigo"* (Kshetri, 2014)

Por tal motivo, es imperativo para el desarrollo de esta investigación hacer un análisis de la relación China-Estados Unidos, que permita identificar los factores que no les han permitido llegar a un estadio avanzado de cooperación en materia de ciberseguridad. De igual manera se hace necesario identificar los desafíos que enfrenta una sociedad interconectada. Los acontecimientos recientes (ataques cibernéticos) pueden dar cuenta de los desafíos que conlleva tener la mayoría de las funciones conectadas a la red.

La presente investigación se diseñó bajo una estructura argumentativa por capítulos, con el objeto de brindar al lector un enfoque lógico de exposición de la temática. El primer capítulo explora de manera breve el desarrollo y evolución de la cooperación tradicional (cooperación espacial y cooperación nuclear) entre Estados Unidos y China, de manera que se pueda analizar los factores constantes en la cooperación en materia de seguridad entre los dos Estados. El segundo capítulo intenta dar cuenta de la complejidad que agrega la era de la información al concepto de seguridad clásica. Para esto, se analiza a groso modo, dos de los ataques cibernéticos más conocidos: el ciberataque con Estonia en 2009 –único por su magnitud- y el ataque contra una planta nuclear iraní en 2010, conocido por ser el primer ciberataque capaz de ocasionar daños físicos. El tercer capítulo ofrece al lector las estrategias –en el marco de la ciberseguridad- que ambas naciones han puesto en marcha. Finalmente, el trabajo de investigación ofrece un análisis de los factores que no han permitido a China y Estados Unidos avanzar en el tema de la cooperación en ciberseguridad. Por supuesto, al finalizar el documento el lector podrá encontrar las conclusiones.

Problema de investigación

La constante evolución de los fenómenos que impactan la esfera internacional hace necesaria la comprensión de los mismos, así como el comportamiento de los actores, los medios, las motivaciones y el entorno en el cual operan. La exploración de la ciberseguridad – especialmente en la relación Estados Unidos- China- ayuda a ilustrar la complejidad que la era digital- -especialmente el internet- a agregado al concepto de seguridad tradicional y los retos que supone para el principal proveedor de seguridad: el Estado.

En la última década, la ciberseguridad empezó a ocupar un lugar importante en la literatura de las relaciones internacionales, como consecuencia de la realidad de una sociedad cada vez más conectada e interconectada, donde las ventajas que ofrece la tecnología de la información se están ensombreciendo a causa de las actividades criminales que se desarrollan dentro del ciberespacio. Sin embargo, a pesar de que es un tema que ha adquirido relevancia y que aparece con más frecuencia en los discursos entre académicos y políticos, es un tema que, por su novedad, aún carece de estudios suficientes y de un consenso teórico a nivel internacional.

La forma en que se trata la seguridad en el espacio físico diverge en ciertos aspectos del tratamiento de la seguridad en el ciberespacio. El ciberespacio, caracterizado por ser un espacio sin fronteras geográficas, hace difícil la ubicación de los actores maliciosos y por ende complica, en gran medida, la penalización de las actividades criminales. La ciberseguridad se consagra como una serie de medidas que busca prevenir estos problemas y asegurarse de que las actividades maliciosas puedan ser contrarrestadas efectivamente. Aun cuando los Estados –especialmente China y Estados Unidos- han sido consistentes en la creación de diferentes estrategias de ciberseguridad, las constantes amenazas cibernéticas y cibernéticas y el robo de información y propiedad intelectual, ponen de manifiesto la necesidad de que crear estrategias que trasciendan las fronteras estatales. Analizar la relación entre estos dos Estado se convierte en un reto teniendo la complejidad de esta relación bilateral.

Pregunta de investigación

¿Cuáles han sido los intentos de cooperación internacional, entre Estados Unidos y China para el tratamiento de las amenazas dentro del ciberespacio?

Justificación

La era digital y la interconexión –cada vez más grande- han facilitado tareas que antaño requerían más tiempo y recursos. El internet, sin duda alguna, ha facilitado muchas funciones y abierto una amplia gama de oportunidades para los Estados, las organizaciones y los individuos. Sin embargo, esa misma tecnología se ha convertido en el escenario de diversas actividades criminales (ciberataques, ciberespionaje, robo de información y propiedad intelectual, entre otros) que ponen en riesgo la seguridad nacional e internacional. Las amenazas que se gestan dentro del ciberespacio son tan importantes como las que se desarrollan dentro del espacio físico. Si bien las amenazas tradicionales siguen siendo tan vigentes como antaño, las naciones se enfrentan a nuevas amenazas con características totalmente diferentes (origen del ataque y perpetrador del mismo son casi invisibles). Resolver las cuestiones relacionadas con el ciberespacio y tratar de mitigar el impacto de los conflictos que surgen dentro del mismo, hace necesaria la cooperación entre los diferentes Estados.

Es de vital importancia para las relaciones internacionales como disciplina, tratar de comprender los fenómenos que denotan la complejidad de la realidad contemporánea. La ciberseguridad, aunque parezca un fenómeno complejo y distante, es ejemplo claro de la constante evolución de la tecnología y su importancia dentro de las relaciones internacionales. Casos como el de Estonia (2007) e Irán (2010) ejemplifican de manera clara las nuevas formas de actuación de los diferentes actores del sistema internacional. Comprender las motivaciones y los objetivos de los actores en el ciberespacio, exige un estudio profesional, profundo y constante.

El estudio de la cooperación en materia de ciberseguridad –especialmente en la relación Estados Unidos-China- da cuenta de la complejidad de las interacciones en el sistema internacional y de la dificultad para llegar a un estadio avanzado de cooperación. Este trabajo busca rescatar y analizar los intentos de cooperación entre Estados Unidos y China en el marco de la ciberseguridad.

Objetivo general

Analizar los intentos de cooperación internacional entre Estados Unidos y China para el tratamiento de las amenazas en el ciberespacio.

Objetivos Específicos

- Documentar la evolución de la era digital en las relaciones interestatales.
- Determinar los logros y desafíos de la ciberseguridad como el nuevo reto de los Estados en el marco de la cooperación internacional.
- Identificar las estrategias en materia de ciberseguridad que han permitido a Estados Unidos y China hacer frente a las problemáticas en el ciberespacio.

MARCO DE REFERENCIA

El uso del término "ciber" se ha extendido muy rápidamente en los últimos años para referirnos a todas aquellas actividades que estén conectadas a las redes. Cada vez, es más común escuchar términos como ciberdefensa, cibercrimen, ciberseguridad, ciberataques, etc. De acuerdo con Caro (2011) el término "ciber" ha sufrido grandes cambios desde 1948 cuando Norbert Wiener definió el término de cibernética en su libro *Control y comunicación en el animal*. El término de ciberespacio, siguiendo a Caro, fue acuñado a principios de los años 80 por el autor de ciencia ficción William Gibson en uno de sus libros.

El rápido desarrollo del mundo virtual -con el internet, las tecnologías de la información y la comunicación (TIC)-, ha convertido al ciberespacio en un ámbito de gran importancia en la política y seguridad nacional e internacional. De acuerdo con la Escuela Superior de Ingenieros de Telecomunicaciones (2013) el ciberespacio puede ser definido como: el espacio artificial creado por los sistemas de comunicaciones e informáticos (CIS), es decir de redes de ordenadores y de telecomunicaciones a nivel mundial, "*el ciberespacio es un ámbito caracterizado por el uso de la electrónica y el espacio electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura física asociada*" (Escuela Superior de Ingenieros de Telecomunicaciones, 2013). La Escuela Superior de Ingenieros de Telecomunicaciones, al igual que Leiva (2015) definen el ciberespacio como un ambiente único, sin fronteras geográficas, anónimo, asimétrico y considerado fácilmente clandestino.

Afirmar exactamente cuándo se empieza a hablar de ciberseguridad es difícil, una búsqueda a través de la web nos muestra que los estudios en materia de seguridad cibernética son relativamente muy recientes; la mayoría se han realizado a partir del año 2011. Si bien, es cierto esto, se puede encontrar que para el año 2002 ya se empezaban a vislumbrar los primeros estudios referentes al tema. Smith & Rupp (2002) en su artículo "Issues in cybersecurity; understanding the potential risks associated with hackers/crackers", ya intentaban clasificar los riesgos asociados a las cuestiones de seguridad cibernética, como consecuencia del creciente número de casos judiciales relacionados con internet – derechos de propiedad intelectual, comercio electrónico - que para ese año se presentaban; y hacían énfasis en la necesidad de que la sociedad no se convirtiera en una víctima de la guerra cibernética. Kemmerer (2003) miembro de la IEEE (Institute of Electrical and Electronics Engineers) Computer Society, para el año 2003, ya identificaba el problema de

ciberseguridad como un problema de seguridad nacional, en la medida en que el internet se empezaba a tornar como una amenaza crítica, no solo al poder de los Estados, sino también al de las compañías, las instituciones financieras, inclusive al de los individuos. Kemmerer (2003) al igual que Smith & Rupp (2002), categoriza las amenazas e intenta analizar los mecanismos de protección para contrarrestar las mismas. En el 2005, Fischer dentro de "Creating a national framework for cybersecurity: An analysis of issues and options" ya planteaba la necesidad de la creación de un marco de seguridad cibernética, que involucrara los esfuerzos del sector público y privado, con el objetivo de alcanzar un nivel aceptable de ciberseguridad dentro de los Estados. El mismo autor, identifica las principales debilidades de la seguridad cibernética: interrupción de los servicios, robo de activos, captura y control, así como, las percepciones erróneas de los riesgos, el fracaso a la hora de abordarlos y los posibles mecanismos para abordarla (adopción de estándares o mejores prácticas, mejoras en ingeniería de software, inversión en capacitación y educación, o corrección de fallas del mercado).

El virus Stuxnet podría ejemplificar claramente la interrupción de los servicios (una de las debilidades que Fisher presenta). De acuerdo con Aguilar (2011) el 27 de septiembre de 2010 los sistemas de control de la central nuclear de Bushehr, así como otras industrias, fueron afectadas por este virus. "*Los expertos consideran que el Stuxnet es el primer virus capaz de penetrar en los sistemas automáticos de control de infraestructuras públicas como centrales eléctricas y nucleares, presas e industrias químicas*" (Aguilar, 2011)

Las crecientes amenazas a las que se enfrentan los Estados en el ciberespacio han hecho que un gran número de académicos y relacionistas internacionales en los últimos años, intenten estudiar el tema de ciberseguridad. Los trabajos actuales en lo que respecta ciberseguridad, tienen algunos puntos en los que convergen, es decir, hay cuestiones que a todos interesa. La primera de ellas es lograr acercarse a lo que puede significar el término "ciberseguridad" o "seguridad cibernética". Aun no existe un consenso sobre el significado que debe ser aceptado mundialmente; es por ello, que cada autor intenta dar una definición lo más precisa posible. Los problemas, amenazas o principales conflictos sobre la ciberseguridad, son temas que se analizan en la mayoría de los trabajos.

El crecimiento de la sociedad de la información viene acompañado por nuevas e importantes amenazas y la adaptación de los Estados a desafíos que son invencibles, intangibles y en algunos

casos poco probables de localizar, convierten a la ciberseguridad en un reto para toda la comunidad internacional. Según Carlini (2016), 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, incentivando sus esfuerzos en implementar estrategias de ciberseguridad.

Carlini (2016) define la ciberseguridad como: "mecanismos esenciales para prevenir las conflagraciones cibernéticas que podrían tener repercusiones dramáticas comparables a la confrontación militar tradicional", también definida por CARI (2013), como "conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propia y negarlo a terceros".

Metodología

La presente investigación es de carácter cualitativo, donde la obtención de resultados concretos, mediante el uso de diversas herramientas, se ubica como la principal característica. Como primera medida se realizó un análisis previo o lectura de documentos. En esta etapa el investigador se familiariza con los diversos documentos disponibles y empieza a orientar el tema de investigación. Posteriormente se llevó a cabo la preparación del material, donde se hizo la selección pertinente de los documentos que serían sometidos a análisis. Para dar respuesta la pregunta de investigación, se tomaron los documentos seleccionados y se hizo un análisis de contenido que permitiera extraer los elementos más significativos de cada texto y que aportaran de manera concreta a la presente investigación.

El desarrollo de esta investigación se hizo a través de un análisis documental de fuentes primarias y secundarias como: artículos académicos –principalmente de bases de datos-, artículos de revistas, paginas oficiales de gobierno, entrevistas y comunicados; con el objetivo de recolectar información académica y verídica para el desarrollo eficaz de dicho proyecto. La investigación documental facilitó la obtención de los datos pertinentes, para el desarrollo de los primeros capítulos, sin embargo para el capítulo final, donde se analizó la relación China-Estados Unidos en materia de ciberseguridad, se hizo necesario realizar un análisis de prensa, pues al ser la ciberseguridad un tema relativamente nuevo son pocos los autores que han escrito respecto al tema (especialmente respecto a la cooperación en materia de ciberseguridad), de modo que el análisis de prensa permitió recolectar información actual.

La presente investigación fue analizada y estudiada desde la cooperación Internacional, basado en el creciente desarrollo y complejidad que presenta las relaciones de cooperación China-Estados Unidos, principalmente en materia de seguridad cibernética. Se eligió este enfoque teniendo en cuenta la capacidad de la cooperación Internacional, de coordinar políticas y esfuerzos para alcanzar objetivos en el plano internacional.

Capítulo 1

Cooperación y Seguridad Internacional; China y Estados Unidos

Tradicionalmente, como los afirma Ripoll (2007) en el Sistema Internacional coexisten dos formas a través de las cuales se relacionan los Estados: la primera es el uso de la fuerza, siendo la guerra su máxima expresión y; la segunda, la diplomacia que incluye acuerdos y tratados –formales e informales- que van desde la concertación hasta estadios mucho más avanzados como la integración, que contiene un alto grado de cooperación.

La cooperación puede ser entendida, de acuerdo con Keohane (1998), como el proceso mediante el cual, determinados actores ven las políticas de sus contrapartes como facilitadores para la consecución de sus objetivos. Para autores como Jiménez (2003), la cooperación entre Estados, desde la perspectiva política internacional, supone visualizarla como fuente de incentivos para el desarrollo de intercambios políticos y sociales institucionalizados, que favorezcan una mayor estabilidad y gobernabilidad democráticas dentro de los mismos. De las diversas definiciones existentes sobre Cooperación Internacional, Ayllón (2007), propone la de Calduch que define la cooperación internacional como: "*Toda relación entre actores internacionales orientada a la mutua satisfacción de intereses o demandas, mediante la utilización complementaria de sus respectivos poderes en el desarrollo de actuaciones coordinadas y/o solidarias*". *(Calduch, 1991: 88).*

Ayllón (2007), quien toma las ideas de Holsti (1967), afirma que una relación de cooperación, para que se pueda identificar como tal, debe contener los siguientes elementos: 1) la percepción de que dos o más intereses coinciden y pueden ser alcanzados por ambas partes simultáneamente; 2) la expectativa de una de las partes de que la actuación seguida por la otra parte, o las otras partes si la cooperación fuese multilateral, en orden a lograr sus propios objetivos, le ayuda a realizar sus intereses y valores; 3) la existencia de un acuerdo (expreso o tácito) sobre los aspectos esenciales de las transacciones o de las actividades a realizar; 4) la aplicación de reglas y pautas (protocolos de actuación) que guiaran las futuras transacciones; y 5) el desarrollo de las transacciones o actividades para el cumplimiento del acuerdo.

Como lo afirma Lipson (1984), los problemas de cooperación y orden no se abordan únicamente como alianzas tácticas o como casos limitantes de anarquía internacional. Las relaciones

internacionales y la política internacional se caracterizan por su atención continua a arreglos cooperativos -o al menos guiados por reglas-, y por la creación de normas e instituciones, por muy frágiles y circunscritas que puedan llegar a ser. En materia económica en particular, hay expectativas estables, sin embargo, las perspectivas de cooperación en materia de seguridad son menos alentadoras.

La cooperación en materia de seguridad es mucho más compleja que cualquier otro tipo de cooperación. De acuerdo con Mutschler (2015), la distribución desigual de las ganancias -desde una perspectiva neorrealista- y, el temor al fraude - desde una mirada neo institucionalista- son los principales obstáculos para la cooperación Internacional exitosa. La primera teoría es mucho más radical pues no acepta pérdidas relativas frente a sus rivales. Los neoinstitucionalistas reconocen que existe la posibilidad del fraude, pero también son conscientes que la interdependencia que experimentan los Estados hace necesaria la cooperación entre los actores del sistema internacional.

> La cooperación en materia de seguridad implica depender de otros Estados para la supervivencia nacional, difícil de garantizar única y exclusivamente bajo la noción de la autoayuda. Además, la cooperación de seguridad limita la libertad de actuar y restringe la capacidad del otro para maximizar el poder militar. En las alianzas de guerra, la dependencia mutua es alta. (Müller, 2002)

Mustchler (2015) argumenta que ha habido varios intentos de cooperación en materia de seguridad, pero el éxito fue limitado. Las principales causas, han sido las dificultades para lograr ganancias equilibradas, la cooperación no recíproca, y la incertidumbre acerca de las intenciones de los demás, lo que alimenta la sospecha y fomenta la ansiedad de atacar primero. Esto indica, que es la lucha competitiva y las condiciones anárquicas, las que limitan el alcance y durabilidad de los acuerdos de seguridad entre los adversarios potenciales. *"El problema estándar en el dilema de seguridad, radica en que, a pesar del deseo de seguridad por parte de los actores, la interacción y su forma de accionar están generando inseguridad en el sistema internacional*" (Jervis, 1985).

De acuerdo con Charles Lipson (1984), a pesar de los riesgos y las limitaciones que se pueden presentar, los acuerdos siguen siendo posibles si cada una de las partes tienen motivos razonables para percibir y generar confianza frente al adversario; es allí donde el tema del pacto de la buena fe entra a jugar un papel importante en la cooperación en materia de seguridad.

1.1 Cooperación Estados Unidos - China

La relación China-Estados Unidos es quizá una de la más diversas y complejas dentro del sistema internacional. En la era posterior a la guerra fría, las relaciones entre China y Estados Unidos se han visto perturbadas por cuestiones económicas, políticas, de derechos humanos, entre otras; sin embargo, el tema de la seguridad parece ser el punto álgido de las relaciones bilaterales entre dichos países, debido a la discrepancia – cada vez mayor- sobre conceptos y prácticas de seguridad. Si bien, la relación Estados Unidos-China se ha caracterizado por ser una relación competitiva y hostil, es importante rescatar algunos intentos de cooperación en el ámbito de seguridad tradicional.

1.2 Cooperación en materia nuclear

Históricamente la cooperación entre estos dos países –especialmente en materia de seguridad- ha sido un tema bastante enredado. Esta complejidad la ilustra claramente el Acuerdo de Cooperación Nuclear de 1985 entre los Estados Unidos y la República Popular de China, que constituyó un avance significativo en el campo de la cooperación de alta tecnología y estableció un precedente para la cooperación futura entre las dos naciones.

Durante la década de 80´s, Estados Unidos vio con inquietud el inicio de la carrera nuclear de China; dicha preocupación, de acuerdo con Chin (1986) comenzó cuando los planes de desarrollo de armas nucleares fueron incorporados en el plan quinquenal de China. La posibilidad de quedar excluido de los proyectos de dicho país se convirtió en el principal incentivo en la búsqueda de un acuerdo nuclear que fundamentara las bases para la cooperación y *"proporcionara un marco jurídico para la exportación de reactores nucleares, combustible y componentes y para el intercambio de tecnología, incluida la cooperación en materia de salud y seguridad"* (Tan, 1989)

Si bien, las motivaciones económicas constituyeron el objetivo primordial del acuerdo –Estados Unidos buscaba asegurar su participación en el mercado chino- los intereses de no proliferación estadounidenses fueron decisivos en la cooperación nuclear pacífica. Explícitamente Estados Unidos buscaba que China reconociera y aceptara las normas internacionales de no proliferación. Sin embargo, esto no sería fácil, como lo afirma Tan (1989), China consideraba que el acuerdo era discriminatorio y lo catalogaba como un "juego de superpotencia" que buscaba monopolizar las armas nucleares y detener la carrera nuclear china que se encontraba en curso.

Durante los años sesenta y setenta, China mantuvo una postura bastante crítica frente al Tratado de No Proliferación Nuclear (TNPN) argumentando que, contrariamente a lo que se creía, el aumento del número de Estados poseedores de armas nucleares reduciría el riesgo de una guerra nuclear. Para el gobierno estadounidense, según Tan (1986) las principales preocupaciones estaban relacionadas con el hecho de que China aún no había asumido obligaciones internacionales ni había adoptado una política que exigiera salvaguardias de la Organización Internacional de Energía Atómica (OIEA).

> Durante las negociaciones, los Estados Unidos dejaron claro que un acuerdo de cooperación nuclear pacífica sólo sería posible si China aclaraba sus políticas de no proliferación. Para cumplir con los requisitos legales de los Estados Unidos para tal acuerdo, China tomó varias medidas importantes para redefinir su posición sobre el régimen internacional de no proliferación. (Tan, 1989)

El tema de la distribución desigual de ganancias (neorrealismo) y el temor al fraude (neo institucionalismo) sin lugar a dudas fueron dos obstáculos en la consecución del tratado. Por un lado, el gobierno chino sabía que adherirse a las normas internacionales de no proliferación, se traduciría en una restricción a su carrera nuclear; por su parte, el gobierno estadounidense temía no tener claridad sobre las políticas de no proliferación de sus homólogos chinos, haciendo énfasis en la preocupación sobre la trasmisión de tecnología nuclear China a otras naciones. El acuerdo nuclear de 1985 *"tuvo una influencia inmediata en el cambio de China de su política nuclear declarativa a un reconocimiento y aceptación de normas y prácticas internacionales de no proliferación"* (Tan, 1989).

1.3 Cooperación en materia espacial

"El espacio ultraterrestre, junto con el espacio marítimo, el espacio aéreo y el ciberespacio, constituye un dominio clave de los bienes comunes mundiales: nadie lo posee exclusivamente, pero todos tienen una participación en él" (Obama, 2010).

La seguridad espacial, sin lugar a dudas, es un problema de seguridad internacional, que en el caso de Estados Unidos y China es bastante complejo. Los programas de defensa antimisiles estadounidenses han generado gran preocupación en los chinos y se han convertido en "la piedra en el zapato" de las relaciones entre los dos Estados. Las constantes disputas y la percepción que

cada uno tiene de su contraparte no han permitido que Estados Unidos y China se suscriban a un acuerdo de cooperación para mitigar las amenazas en el espacio.

Tomando las ideas de Shen (2011), durante el gobierno de Ronald Reagan la carrera de armamento nuclear entre Estados Unidos y la Unión Soviética se volvió crítica. El programa Star Wars, creado por Estados Unidos con el fin de interceptar cualquier misil soviético, obligó a la Unión Soviética a expandir su arsenal nuclear. Como continúa Shen (2011), a pesar de la desaparición de la Unión Soviética, Estados Unidos continuó con el desarrollo de su programa de defensa antimisiles, incorporando medidas como la Propuesta de Protección Global de Ataques Limitados (GPALS) y el Sistema Nacional de Defensa Antimisiles (NMD). Este último fue posible, cuando el presidente George W. Bush, desechó el Tratado de Misiles Antibalísticos.

La continuidad y extensión de los programas militares estadounidenses despertaron el interés y la preocupación del gobierno chino, siendo estos percibidos como una amenaza para la seguridad de China. El comportamiento de Estados Unidos fue rechazado por Rusia y China, quienes intentaron poner límites a la carrera de armamento estadounidense, a través de numerosas propuestas para prevenir una carrera de armamentos en el espacio ultraterrestre (PAROS).

La cooperación en materia de seguridad espacial, como lo afirma Mustchler (2015), fue un tema en los foros multilaterales desde 1981, pero fue solo hasta 1985 cuando finalmente fue remitida a la Conferencia de desarme en Ginebra, donde se creó el Comité Ad Hoc para la Prevención de una Carrera de Armas en el Espacio Ultraterrestre (PAROS). Desde el inicio este comité presentó diversos problemas. Por un lado, había numerosos Estados que respaldaban la prohibición de armas espaciales, y, por otro lado, Estados Unidos rechazaba esta propuesta. Estados Unidos argumentada que el peligro de desarrollar una carrera de armamentos en el espacio ultraterrestre era realmente bajo, por tal motivo, no era necesario crear nuevas estipulaciones sobre el uso del espacio. Al no ver un compromiso sustancial por parte de los Estados Unidos, China decidió empezar a prepararse para contrarrestar las amenazas futuras.

Durante algunos años, de acuerdo con Shen (2011), China encubrió su proceso de desarrollo antimisiles, pero el 1 de enero de 2007 Beijing llevo a cabo –con éxito- el primer lanzamiento de un misil anti satélite (ASAT), ante la mirada de Estados Unidos. El desarrollo de los sistemas

ASAT por parte de los dos países y, la desconfianza que ha caracterizado –desde antaño- sus relaciones bilaterales, no les ha permitido llegar a un estadio avanzado de cooperación.

De acuerdo con Xinbo (2000), Estados Unidos posee las fuerzas armadas más poderosas del mundo y actualmente sigue invirtiendo fuertemente en sus industrias de defensa para desarrollar sistemas de armas más sofisticadas y con mayor potencial, con el principal objetivo de mantener su hegemonía, no sólo en armamento sino también en estrategias de defensa que le permitan estar protegido de posibles ataques de otros países, sin embargo, al aumentar su capacidad ofensiva y defensiva, este tipo de seguridad unilateral ha generado malestar en diversos países, especialmente China, pues considera que la construcción de estos sistemas de defensa y su fuerte capacidad armamentística, está generando una fragmentación en la estabilidad estratégica tanto regional como global, lo cual genera una mayor inseguridad incentivando a que otros países reaccionen desarrollando sus propios medios, generado un círculo vicioso de acumulación de armas y aumentando las tensiones en el sistema internacional.

Como lo afirma Xinbo (2000), se ha hecho evidente que China y Estados Unidos presentan un conflicto de intereses, y divergen en algunas cuestiones, por un lado, Estados Unidos ha trabajado constantemente y sigue trabajando en pro de conseguir una seguridad absoluta, y se empeña por preservar el poder militar superior y el fortalecimiento de las alianzas de seguridad, a diferencia de China, considera que la mejor manera de mejorar la seguridad es optimizar las relaciones políticas, ampliar las interacciones económicas y persistir en la cooperación en materia de seguridad, implementado la transparencia y medidas que aprueben el fomento de confianza, puesto que la dependencia excesiva de los enfoques militares en muchos casos se presentan como un impedimento para resolver las controversias, y además debilita el desarrollo y aplicación de la paz y la seguridad.

No obstante, como lo afirma Twomey (2009), a pesar de que China considera que la optimización de las relaciones políticas es el mejor paso para mejorar la seguridad, este no se ha quedado atrás, China esta implementado una modernización estratégica, mejorando su arsenal, desplegando misiles carretera-móviles y de combustible sólido, invirtiendo en investigación y desarrollo de una amplia gama de tecnologías que le permitan una mayor precisión y defensa, lo cual le da un alto grado de seguridad en su capacidad armamentística y le permiten un equilibrio estratégico. Los sistemas de defensa antimisiles estadounidenses han impulsado claramente a la toma de medidas

anticipadas por parte de China y en la acumulación cuantitativa en sus arsenales de misiles regionales. Estas contramedidas implementadas por China han demostrado sus capacidades similares, las cuales fortalecen su capacidad de seguridad frente a un posible ataque estadounidense, empeorando aparentemente la percepción de amenazas.

Cooperar les permitiría a estos dos países, contrarrestar amenazas que geográficamente los incluyen (en el caso de China) y que amenazan la seguridad internacional. *"Mientras tanto Estados Unidos como China se enfrentan a la amenaza común de proliferación de misiles, su disputa interestatal bilateral ha socavado su legítima necesidad de erigir una defensa antimisiles para contrarrestar la amenaza común"* (Shen, 2011).

La amenaza de los misiles anti-satélite y la carrera armamentística –tanto de Estados Unidos como de China- no es el único problema que enfrentan estos dos países. *"La presencia militar global de Estados Unidos ha estado cada vez más expuesta a la amenaza debido a la proliferación de tecnologías de misiles y cohetes"* (Shen, 2011).

Washington ha expresado su preocupación por la capacidad intercontinental que durante más de una década ha venido acumulando la República Democrática Popular de Corea (RPDC) y por el programa nuclear de Irán. Sin duda, esto se convierte en un problema de gran envergadura para la seguridad internacional. Las acciones de Corea del Norte y de Irán socaban los intereses de China y Estados Unidos, esto debería convertirse en un incentivo para la cooperación entre los dos países. Sin embargo, China teme romper sus relaciones con Irán y Corea del Norte.

Las relaciones entre China y Estados Unidos han estado marcadas por disputas y desacuerdos constantes. Si bien, han existido momentos en los que han intentado cooperar como en el caso del Tratado de no proliferación de 1985, sus relaciones siguen siendo muy débiles y esto quedó demostrado en el caso de los misiles ASAT. Mientras no exista un acuerdo de carácter vinculante para estas dos naciones, -que controle sus sistemas ASAT y su carrera armamentística-, garantizar la seguridad en el espacio y en el espacio terrestre seguirá siendo una tarea complicada. Si la cooperación en estos temas ha sido bastante compleja ¿Qué podemos esperar en materia de ciberseguridad? ¿Cómo pueden avanzar estas dos naciones en las cuestiones de seguridad cibernética, cuando aún no han podido resolver otras cuestiones de seguridad más antiguas?

Teniendo en cuenta que ambas partes siguen persiguiendo sus intereses de seguridad, y la aplicación de tratados y convenios sobre seguridad cibernética internacional se han tornado altamente difíciles debido a los nuevos desafíos planteados por el vertiginoso cambio tecnológico, es importante que cada una de las partes se adapte a los cambios que se están presentado en el panorama de seguridad y que ambos países realicen un ajuste en sus políticas en este tema, efectuando medidas que controlen la implementación de capacidades ofensivas y defensivas y promuevan medidas que vislumbren el fomento de la confianza- teniendo en cuenta que es una de las principales limitaciones para que acuerden un cese bilateral- y den paso a un mejor ambiente de seguridad en el sistema internacional.

Capitulo 2
El internet: un arma de doble filo para las naciones

Desde comienzos del siglo XXI, con los avances tecnológicos y el creciente uso de las redes de información a escala global, el mundo se ha tenido que enfrentar a un importante fenómeno denominado: la revolución de las comunicaciones. La tecnología de la información en general y la difusión de Internet en particular, sin duda, se han convertido en uno de los rasgos dominantes de la globalización y han modificado el entorno social, cultural y económico. Si bien, *"Internet ha sido la herramienta tecnológica que revolucionó (y sigue revolucionando y evolucionando) las comunicaciones a escala global"* (Rabinad, 2008), es de vital importancia analizar en el presente capítulo, los efectos (positivos y negativos) de la tecnología insignia de la era digital: el internet, en la esfera de las relaciones internacionales y el impacto en la seguridad Nacional e internacional.

La era digital y el uso masivo de las tecnologías de la información han abierto un abanico de oportunidades sin precedentes para todas las naciones, pero así mismo, han planteado nuevos retos para el grueso de la comunidad internacional. Como lo afirma Don (1999), la evolución de la tecnología subyace en la complejidad e incertidumbre en el ámbito de las relaciones internacionales. *"Este nuevo escenario facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero al mismo tiempo conlleva serios riesgos y amenazas que pueden afectar a la Seguridad Nacional"* (Leiva, 2015). La era digital ha permeado – en menor o mayor grado – todos los ámbitos que se puedan imaginar. La esfera de las Relaciones Internacionales no es ajena al impacto que genera una sociedad cada vez más interconectada.

El rápido avance de las tecnologías de la información -especialmente del internet- y su fácil integración a las funciones estatales, convierten a la nuestra, como lo afirma Carr (2011) en una sociedad totalmente dependiente de una red de información abierta y poco segura. A pesar de la universalidad del internet y de su importancia para un sin número de funciones, aún es insuficiente la comprensión que se tiene sobre los efectos e implicaciones para la seguridad dentro del marco de las relaciones Internacionales. Ninguna otra tecnología ha significado para las naciones una fuente de poder y a la vez su talón de Aquiles, en el sentido que internet lo ha hecho. Como lo afirmó en una rueda de prensa el ex presidente Barak Obama, *"Esa es la gran ironía de la era de la información, las tecnologías que nos permiten construir y crear son las mismas que utilizan*

aquellos que destruyen y perturban el orden; es una paradoja que vemos cada día" (El País Internacional, 2009).

De acuerdo con Carr (2011) a finales de los años sesenta cuando las primeras computadoras logran conectarse a través de protocolos IP, la seguridad cibernética no fue una prioridad; esto debido a que el grupo que podía acceder a esta red estaba compuesto por investigadores que trabajaban en defensa, ciencia y academia, por lo que el temor de que esta red se usara de forma ilícita, quedo descartado. Sin embargo, las oportunidades que ofrecían las computadoras hicieron crecer exponencialmente su adquisición y las redes a las que inicialmente solo podían acceder un grupo limitado de investigadores, quedaron a disposición de otros sectores.

> En la segunda mitad de los años noventa, Internet era una entidad muy diferente a la que había estado al principio de esa década. En cuestión de varios años, había sido privatizada, abierta al tráfico comercial, la Web había sido inventada y la amplia aceptación de Jyfosaic y computadoras personales habían hecho que Internet fuera ampliamente accesible para aquellos que no poseían conocimientos informáticos, dinero o experiencia. (Carr, 2011).

Desde el momento de su liberalización, internet se propagó de forma extraordinaria. De acuerdo con Castells (2014), para 1996 el número de usuarios en internet se calculó en 40 millones, para el año 2013 la cifra de usuarios conectados a esta red global sumaba un total de 2.500 millones. Mientras el número de usuarios crecía exponencialmente, las vulnerabilidades que se gestaban en el seno de esta red crecían a la misma velocidad.

Sin duda alguna, la era de la información, ha agregado complejidad al concepto de seguridad tradicional y plantea nuevos retos al poder de los Estados. Cuando se habla del impacto que la era digital – más exactamente el internet- tiene sobre las relaciones internacionales, surge entre académicos y políticos una duda generalizada: ¿sobre quién recae la soberanía, en un mundo interconectado? ¿Seguirá siendo el Estado el principal actor en el campo, manteniendo su papel como supremo proveedor de seguridad en el ciberespacio? Como lo afirma Rabinad (2008), y como ya se mencionó anteriormente, este espacio, donde no existen fronteras geográficas, permite la convergencia de diversos actores, lo que origina serios conflictos al intentar establecer las pautas bajo las cuales van a actuar y sobre quien recae la soberanía.

Aún es difícil saber cuáles son las implicaciones reales que la era digital tiene sobre la seguridad nacional e internacional. No existe un consenso general sobre el papel que desempeñan los Estados en una sociedad interconectada. De acuerdo con Erikson y Giacomello (2006) para autores como Fountain (2001) el Estado sigue conservando su papel como principal proveedor de seguridad, tanto en el espacio físico como en el ciberespacio; para autores como (Arquilla y Ronfeldt, 2001; Castells, 1998, 376, Henry y Peartree, 1998, Nye, 2003, 2004a, 2004b) el surgimiento de la era de la información y con ella el aumento de la importancia de actores no estatales (empresas, movimientos sociales, redes transnacionales e individuos) se convierte en un reto para los Estados y para quienes se encargan de proveer seguridad.

> Los Estados seguirán siendo el actor dominante en la escena mundial, pero encontrarán el escenario mucho más concurrido y difícil de controlar. Una parte mucho mayor de la población dentro y entre los países tiene acceso al poder que proviene de la información. (Nye, 2010).

Teorías tradicionales de las relaciones internacionales, como el realismo y el liberalismo, de acuerdo con Rabinad (2008), no han sido indiferentes al impacto del internet sobre el ejercicio de la soberanía. Por un lado, siguiendo las ideas de Rabinad, están los realistas quienes defienden la tesis de que Internet es un factor de riesgo para la soberanía; de acuerdo con esta teoría cuatro argumentos son fundamentales: 1) la difusión de las tecnologías de la información y de la comunicación propias de internet, quebrantan el poder soberano a favor de la actividad económica; -2) debido a los problemas jurisdiccionales en el plano formal y las desigualdades entre los países en materia de cultura, leyes y valores, la cooperación internacional se ve debilitada notablemente; 3) internet representa una fuerte amenaza a la capacidad del Estado soberano de intervenir y controlar los eventos políticos o sociales que se desenvuelven dentro de sus fronteras; y 4) la cooperación internacional se ve socavada por las constantes disputas sobre jurisdicción extraterritorial y los regímenes legales propios de cada país.

Por otro lado, el pensamiento liberal -en discrepancia con los realistas-, sostiene que Internet fortalece los gobiernos nacionales e internacionales y fortalece el Estado de derecho: 1) reconfortando el derecho internacional mediante tratados de manera que permitan establecer una diplomacia virtual; 2) incentivando a una interdependencia gradual entre países y promoviendo la creación y apoyo de instituciones Internacionales; y 3) apoyando mecanismos internacionales de seguridad.

El acelerado crecimiento de las tecnologías de la información, especialmente de internet, se ha traducido en una digitalización masiva de datos. De acuerdo con Castells (2011) quien toma las ideas de Martin Hilbert (2010) el 95% de toda la información que existe en el planeta se encuentra digitalizada y una parte significativamente alta está disponible para el acceso a través de internet u otras redes informáticas, *"La cantidad de información digital aumenta diez veces cada cinco años"* (Nye 2010). Sin duda alguna, este aumento desmedido de la digitalización de la información y más aún, el fácil acceso a la misma, tienen consecuencias directas sobre el poder y la gobernabilidad de los Estados. El ciberespacio añade nuevos retos, inclusive para los Estados más poderosos y con larga experiencia de poderío militar y económico.

> Incluso los grandes países con impresionantes recursos de poder duros y blandos, como los Estados Unidos, se encuentran compartiendo escenario con nuevos actores y tienen más problemas para controlar sus fronteras en el dominio del ciberespacio. El ciberespacio no reemplazará el espacio físico y no abolirá la soberanía estatal, pero la difusión del poder en el ciberespacio coexistirá y complicará enormemente lo que significa ejercer el poder. (Nye, 2010)

Así mismo:

> En el sistema estatal moderno, las naciones han liderado guerras y los países con activos físicos más grandes han tenido mayores posibilidades de ganar. Sin embargo, con el fácil acceso y los bajos costos de los ataques la tecnología de la información ha contribuido a aumentar el número de individuos o actores que pueden ejecutar acciones que amenazan la seguridad y generan conflictos militares. (Bae, 2003).

Aguirre y Morandé (2015) coinciden con Nye, al afirmar que la identificación de un nuevo espacio, o dominio virtual -el ciberespacio-, construido como un escenario de interacción humana, en donde al ejercicio tradicional de los agentes estatales, se suman individuos y organizaciones no gubernamentales que desempeñan determinados roles en la utilización de las TIC en el ámbito internacional, constituye un gran reto para la gobernanza de los Estados; teniendo en cuenta que la intervención de distintos actores, pueden amenazar los ámbitos propios de la esfera estatal.

La complejidad del ciberespacio –en contraste con el aire, el mar y el espacio - subyace como lo plantea Nye (2010) en tres factores: el primero de ellos es la diversidad de actores; el segundo, la facilidad de entrada y; el tercero la facilidad para ocultarse o lo que autores como Torres (2013)

llamarían “problemas de atribución”. Si bien, como el mismo Nye lo advierte, estas características las comparte también la guerra terrestre, en el ciberespacio estas adquieren dimensiones mayores. Hablar de un dominio total del ciberespacio resulta casi imposible, inclusive para países como Estados Unidos, China o Rusia. La dependencia de las tecnologías de la información y de complejos sistemas cibernéticos para apoyar los sistemas militares y económicos, crea grandes vulnerabilidades, que, en el caso de los grandes Estados, pueden acarrear costos altamente significativos, ya que estas vulnerabilidades pueden ser explotadas por Estados mucho más pequeños y por actores no estatales.

Las amenazas presentes en el ciberespacio, de acuerdo con Carr (2011) abren una nueva esfera de conflictos globales donde, ni siquiera los Estados más poderosos tienen control. El poder militar que los caracterizó antaño y que les permitió el dominio parcial del espacio físico, no les garantiza el control del ciberespacio. Como continúa afirmando Carr (2011), los Estados más pequeños y con menos poderío, actores no estatales y grupos terroristas –que en el pasado eran considerados como poseedores de poca potencia- en el nuevo escenario se tornan relativamente más poderosos. Carr (2011) al igual que Nye (2010) coinciden en que el poder absoluto en el ciberespacio parece tener menos significado que en el espacio físico. Inclusive, un país como Estados Unidos con una larga trayectoria de poder militar y económico sin precedentes, aun no puede garantizar la seguridad en este ámbito.

Para Torres (2013), el dilema de los productos informáticos y las redes de información que conectan nuestros sistemas subyace en el precario equilibrio entre versatilidad (facilidad de uso) y seguridad. *“Los aspectos que convierten a los ordenadores y otras herramientas de la era de la información en instrumentos versátiles y fáciles de usar son las mismas características que los transforman en objetivos susceptibles de ser atacados”* (Torres, 2013).

> Debido a que Internet fue diseñado para facilitar su uso en lugar de seguridad, el delito tiene actualmente la ventaja sobre la defensa. Esto podría no ser el caso a largo plazo a medida que la tecnología evoluciona, incluyendo los esfuerzos de "reingeniería" de algunos sistemas para una mayor seguridad, pero sigue siendo el caso en esta etapa. (Nye, 2010)

Así mismo:

> El internet fue diseñado para maximizar la simplicidad de la comunicación, no la seguridad de la comunicación. El precio para esto ha sido la creciente oportunidad para criminales o malhechores de explotar la vulnerabilidad de la red para sus propios fines. (Erikson & Giacomello 2007).

Como lo afirman Aguirre y Morandé (2015) el Ciberespacio se ha convertido en un espacio de creciente complejidad y eventualmente de conflicto transnacional, esto se hace evidente con casos como el de Wikileaks, Al Qaeda o el Estado Islámico (ISIS), así como también el concepto de moneda virtual conocida como Bitcoins, casos que demuestran como este espacio permite la interacción de diversos grupos para que actúen acorde a diferentes objetivos e intereses en los asuntos internacionales, lo que indica que el desarrollo de la ciencia y la tecnología ha sido una fuerza importante que induce a importantes cambios en las relaciones internacionales.

De acuerdo con Bae (2003) quien toma las ideas de Arquilla y Ronfeldt (1997) el desarrollo de la tecnología de la información y las telecomunicaciones ha cambiado la forma en que se libra una guerra, así como el significado de las fuerzas militares y la seguridad, la reestructuración del orden militar y de seguridad internacional. En la era de la información, el poder militar no es únicamente la fuerza de fuego si no la precisión del sistema armamentístico, dicha precisión está relacionada con la capacidad de obtener información sofisticada, monitoreo, vigilancia, etc. De manera que la competitividad en la era de la información depende de quien obtiene información más estratégicamente importante. Autores, como Bae (2003), Erikson & Giacomello (2007) sostienen que, en esta era, no se requiere de bombas o explosivos para atacar, solo basta tener una computadora conectada a la red para ocasionar estragos en el mundo, esto es suficiente para paralizar un sector de la economía, apagar una red eléctrica, hasta tal punto que la sociedad y el gobierno perderían la capacidad de funcionar normalmente.

Dentro de los numerosos ataques cibernéticos cometidos en los últimos años, hay algunos que, por sus efectos dramáticos en la sociedad, son un reflejo de los verdaderos alcances de la guerra cibernética. Los ciberataques cometidos contra Estonia, en la primavera de 2007 y el famoso ataque cibernético contra la planta nuclear iraní Bushehr en 2010, son -por sus nefastas consecuencias, su magnitud e impacto en la comunidad internacional- dos ejemplos claros de los peligros de la tecnología y de la necesidad de proteger las redes y los servicios de la información.

"Los Ministros de Defensa desarrollan estrategias para combatir la amenaza con misiles, bombardeos navales, ataques aéreos y avances de tanques. Pero ¿una invasión digital?" (Davis, 2007). Los ataques cibernéticos contra Estonia e Irán, demostraron que la ciberseguridad debe convertirse en un punto clave en las agendas de los países y que la protección del ciberespacio es tan importante como la protección del espacio físico.

2.1 Ataque cibernético Estonia (2007)

> *"El ataque más espectacular contra instituciones estatales e importantes negocios ocurrió en la primavera de 2007 en Estonia y fue obra de los piratas informáticos rusos"* (Fernández, 2009)

Durante el 27 de abril y el 22 de mayo de 2007, Estonia fue asediada por una red de robots informáticos (botnets), que se deslizaron y esparcieron por todo el país a través de la frontera menos protegida: internet. Como lo comenta Davis (2007) en un artículo para la revista "*Wired",* afuera todo estaba tranquilo, los guardias transfronterizos no habían reportado ninguna intrusión o violación al espacio aéreo estonio, hasta que un asistente explicó lo que estaba sucediendo: estamos siendo atacados por una red informática deshonesta.

Como lo expresó Jaak Aaviksoo, Ministro de Defensa de Estonia para ese entonces, *"Este no fue el primer ataque de botnet, ni el más grande. Pero nunca antes se había atacado a un país entero en casi todos sus frentes digitales al mismo tiempo, y nunca antes el propio gobierno había respondido"*

Asi mismo:

> Todos los principales bancos comerciales, empresas de telecomunicaciones, medios de comunicación, servidores de nombres en internet, guías telefónicas de internet, sintieron el impacto, y esto afecto a la mayoría de la población estonia. Esta fue la primera vez que un botnet amenazaba la seguridad nacional de una nación entera. (Jaak Aaviksoo en entrevista para Wired, 2007)

De acuerdo con Lauri Almann (2008), ex Secretario Permanente del Ministerio de Defensa de Estonia y miembro del equipo de respuesta contra los ciberataques de 2007, los ataques cibernéticos se dividieron en dos fases. La primera fase (del 27 al 29 de abril) se caracterizó por ataques simples -llevados a cabo por los llamados "hackivistas"- y el uso de herramientas

relativamente primitivas. De acuerdo con Almann, estas herramientas estaban especialmente diseñadas para atacar sitios web de Estonia, especialmente del gobierno, del Ministerio de Defensa y de los principales partidos políticos de Estonia.

> Estos ataques, eran básicamente de naturaleza simple, es decir, sin grandes complejidades de carácter técnico y organizativo y sin capacidad de convocar a un número de atacantes lo suficientemente grande, como para causar daños serios y poner en una situación de crisis o indefensión a Estonia. (Ganuza, 2009; pp.178)

En la segunda fase –del 3 de abril al 18 de mayo- de acuerdo con Ganuza (2009) los ataques adquieren mayor complejidad a nivel técnico, organizativo y de coordinación. Estos ataques requerían de un mayor conocimiento de las herramientas de ciberguerra, el uso de numerosos robots informáticos (botnets) y de una coordinación detallada y precisa. *"La segunda fase de los ataques utilizó herramientas de ataque mucho más sofisticadas, principalmente botnets. Esta es una estimación aproximada, pero [aprendimos] que los ataques vinieron de 75 o más jurisdicciones usando 1 millón o más de computadoras"* (Almann, 2008)

Los sitios web desde los cuales habían sido lanzados los ataques en la primera fase seguían en funcionamiento en la segunda fase, pero, como lo afirma Ganuza (2009) ahora tenían mejoras incluidas, como lista de objetivos y calendario con hora y lugar del ataque, con el objeto de lanzar peticiones simultaneas sobre los mismos servicios informáticos y así dejarlos fuera de servicio.

Siguiendo a McGuinness (2017) debido a los niveles sin precedente de tráfico en internet, las páginas de bancos, organismos gubernamentales y medios de prensa colapsaron. Redes de robots informáticos (botnets) enviaron grandes cantidades de mensajes basura (spam) y pedidos automáticos online para saturar los servidores. Como consecuencia, los cajeros automáticos y servicios de banco online dejaron de funcionar, lo empleados estatales no pudieron comunicarse por correo electrónico y los medios de comunicación se encontraron con que no podían transmitir las noticias.

De acuerdo con José Nazario (2007), destacado analista de ciberamenazas a nivel mundial, tan solo entre el 3 y 11 de mayo de 2007, se registraron 128 ataques de denegación de servicios distribuidos (DDoS), de los cuales 21 se presentaron durante el 3 de mayo, 17 durante el 4 de mayo, 31 durante el 8 de mayo, 58 durante el 9 de mayo y 1 durante el 11 de mayo.

Pero ¿qué hacía que Estonia fuera un blanco perfecto para un ataque cibernético? ¿Qué características convirtieron a esta nación en uno de los mayores ejemplos de guerra cibernética en

los últimos años? Como asevera el mismo Almann (2008), Estonia es un país dependiente –casi en su totalidad- de todo tipo de servicios electrónicos. El 97% de todas las transacciones bancarias se realizan en línea, omitiendo por completo la fase de la chequera y demás servicios en línea. Estonia, de acuerdo con Ganuza (2009), es un país donde la actividad política se desarrolla mayoritariamente a través de la web.

> Las sesiones del gobierno y los consejos de ministros se realizan exclusivamente a través de intranet evitando casi al 100% la burocracia del papel. Un ataque con éxito a las redes que controlan dicha actividad provoca de inmediato una crisis de comunicación política. (Ganuza, 2009; pp. 185)

Con una avanzada infraestructura digital, de acuerdo con Fernández (2009) Estonia fue el primer país –en 2004- que inicio pruebas de votos legales a través de internet y el primero donde fue posible votar a través del ordenador en las elecciones de 2007. Con la mayoría de sus funciones estatales conectadas a la red y con el 97% de sus transacciones bancarias digitales, un ataque cibernético a este país podría ser devastador.

La respuesta

Si alguien preguntase ¿Qué es lo que hace excepcional el caso de Estonia?, y ¿Por qué se convierte en ejemplo para otras naciones? La respuesta sería la capacidad del gobierno estonio para hacer frente a los ataques y salvaguardar su infraestructura critica. De acuerdo con Ashmore (2009) los ataques solo causaron interrupciones a corto plazo, gracias a que los estonios pudieron responder de manera competente a los ataques, evitando daños permanentes a su infraestructura de la información.

El gran triunfo de la nación estonia fue *"Identificar la gravedad del asunto con celeridad y organizar inmediatamente un equipo de respuesta multidisciplinar e investirle de la autoridad necesaria"* (Ganuza, 2008; pp: 179) y "*Reconocer desde el primer momento ante el mundo que estaban siendo víctimas de un ciber ataque*" (Ganuza, 2008; pp: 191). Aceptar públicamente que estaban bajo ataque cibernético, es quizá uno de los grandes logros por parte de los estonios. Reconocer que se ha sufrido o que se está sufriendo un ataque cibernético no es una práctica habitual por parte de ningún gobierno ni una gran empresa, por temor a la perdida de fiabilidad y reputación.

Los ataques de 2007 no derrotaron a la nación báltica, por el contrario, la hicieron más fuerte. A raíz de esta experiencia y según Ashmore (2009) Estonia se establece como un jugador de gran

importancia en un campo emergente: la ciberseguridad. La asistencia de especialistas estonios del Equipo de Respuesta de Emergencia Informática (CERT) en los ataques cibernéticos que sufrió Georgia en 2008 y la ayuda que brindaron para controlar y responder a los ataques, son ejemplo claro de su importancia en el ámbito cibernético.

Estonia, como lo afirma Ashmore (2009) es una nación muy pequeña para tener gran impacto o influencia en la escena internacional, mediante el uso del poder económico o militar; pero es un actor –que en el ámbito de la ciberseguridad- tiene algo que los otros Estados no tienen: experiencia.

Es precisamente la experiencia y una respuesta exitosa ante un ataque cibernético, lo que le permitió a Estonia convertirse en un jugador importante en Europa y entre los miembros de la OTAN como un experto en ciberseguridad y guerra cibernética.

"Algún día el mundo estará tan conectado como esta región báltica" (Davis, 2009), será igual de vulnerable y necesitara grandes defensas cibernéticas para salir bien librado –como lo hizo Estonia- de un ataque cibernético.

En 2007 Estonia, en 2008 Georgia, en 2010 Irán, en 2017 varias naciones fueron afectadas por el virus WannaCry. Los ataques cibernéticos son tan reales como cualquier otra amenaza y todas las naciones son vulnerables mientras estén conectadas a la red. Cualquier país puede ser el siguiente en unirse a la lista de los países que han sido asediados por ataques cibernéticos, por ello es importante preguntarse ¿tienen defensas suficientes para responder? Seguramente después de 10 años las amenazas son más sofisticadas y elaboradas, las respuestas que se usaron hacen 10 0 5 no surtirán el mismo efecto en la actualidad.

2.2 Ataque cibernético Irán 2010

Como lo afirma Joyanes (2015), Stuxnet es un software malicioso que es detectado por primera vez en junio del 2010, por la empresa VirusBlockAda (empresa de seguridad radicada en Bielorrusia), que, de acuerdo con el Instituto Español de Estudios Estratégicos (2013), fue el primer virus informático conocido, capaz de sabotear por sí mismo procesos industriales, plataformas petroleras, centrales eléctricas, sobre todo aquellas capaces de fabricar misiles con cabezas nucleares.

Dado que va dirigido contra infraestructuras críticas que no utilizan Internet, autores como Shakarian (2012) y Joyanes (2015) afirman que el troyano se introdujo en los ordenadores a través

de lápices de memoria tipo USB y luego se multiplicó a sí mismo, pasando de un ordenador a otro, instalando programas troyanos de espionaje para recoger información de manera oculta, impidiendo el funcionamiento normal y consiguiendo dañar tanto sitios web como sistemas operativos. *"Las implicaciones reales de Stuxnet están más allá de cualquier amenaza que hemos visto en el pasado*". (Benedicto, 2013).

Según medios como la BBC y New york times señalan que Israel y Estados Unidos son los responsables de crear el virus informático con el fin de dañar y retrasar el programa nuclear iraní, puesto que, mientras para Irán este programa nuclear representa progreso y prestigio internacional, para ellos representa una amenaza potencial; de modo que tanto Estados Unidos como Israel solicitaron detener el proyecto nuclear de dicho país. Ante la negativa de Irán a paralizar sus planes, Stuxnet parece haber sido una de las fórmulas de Estados Unidos seguido de Israel para ralentizar el proceso.

De acuerdo con Joyanes (2015), expertos en el tema afirman que el 60% de los ordenadores iraníes se vieron afectados, al igual que el 20% en Indonesia y el 8% en India. El virus Stuxnet ha sido el ataque cibernético que por primera vez logró dañar la infraestructura del "mundo real", desde entonces como lo afirma Medero (2012), Stuxnet se ha convertido en un arma casi perfecta. En primer lugar, ha provocado daños en las centrifugadoras, bloqueo y retraso. En segundo lugar, la creación de este virus habría llevado seis meses para un equipo de cinco personas, lo cual representa unos costes muy bajos para un Estado. Y, en tercer lugar, puede alcanzar unos objetivos que son invulnerables por otros medios, y además el uso de esta ciberarma no limita el empleo simultáneo de tácticas más convencionales.

No obstante, el caso de Stuxnet ayudo a Irán a mejorar su defensa cibernética, una vez detectado el malware Stuxnet que afecto a su central de enriquecimiento de uranio de Natanz, de acuerdo con Servitja (2013) el gobierno de Ahmadineyad dio origen a "*la organización de la ciberseguridad la cual está formada por una vertiente defensiva, la ciber unidad especial dentro de la organización de defensa pasiva de las fuerzas Armadas de Irán dirigidas por el General de Brigada Gholam Reza Jalali y cuya función es contrarrestar y detectar los ciberataques y el ciberespionaje"(Servitja, 2013).* Así, la Organización de la Ciberseguridad se dota de capacidades para desarrollar operaciones encubiertas y de contrainteligencia utilizando el ciberespacio.

Gracias a este ataque cibernético contra sus instalaciones nucleares, no solo Irán, si no lo países en general se han dedicado a mejorar su preparación contra esos actos de sabotaje para estar preparados ante cualquier amenaza. De hecho, autores como Medero (2012) afirman, que no sería extraño que en un futuro no muy lejano se haga uso de ciberarmas como alternativa a las operaciones militares clásicas, incluso ya se ha implementado una nueva versión del virus, al que los expertos en seguridad han denominado "Duqu", un virus que está diseñado para robar la información necesaria para organizar un ataque como el llevado a cabo por su predecesor, este virus, fue creado en gran parte del mismo código que Stuxnet, pero se concentró en el espionaje en lugar de sabotaje, absorbiendo los datos de los ordenadores que infecta. De igual forma, después apareció Flama, otro código malicioso que hace lo mismo que Duqu, pero parece ser aún más sofisticado. "*Este virus representa una escalada de una guerra cibernética preocupante que se libra entre los estados-nación*". (Benedicto, 2013).

Casos como los de Stuxnet, Duqu y Flame, demuestran que los ataques cibernéticos y las guerras cibernéticas cada vez están más latentes, y aunque es cierto que aún no se ha producido ningún conflicto que se pueda calificar como una verdadera ciberguerra, estos casos se encuentran cerca de ello. Para algunos países, entre ellos Estados unidos, el desarrollo de ciberarmas ofensivas y defensivas se ha convertido en su principal defensa, de manera que las cuestiones de ciberdefensa y ciberataques, hayan entrado a formar parte de la agenda política de los gobiernos. Medero (2012), quien toma las ideas de Crowell sostiene que en el curso de los próximos veinte o treinta años, el papel de los ciberataques en caso de guerra cobrará cada vez más importancia.

Capítulo 3

Estrategias implementadas por Estados Unidos y China para garantizar su seguridad en el ciberespacio

"Además de enfrentarse a los enemigos en los campos de batalla tradicionales, ahora Estados Unidos [y China] debe estar preparado[s] para amenazas asimétricas, como las que se dirigen a nuestra dependencia en el espacio y el ciberespacio" (Obama, 2010)

Los ciberataques y el robo de información del que han sido víctimas Estados Unidos y China han obligado a cada uno de sus gobiernos a crear estrategias encaminadas a proteger la infraestructura crítica de la nación y a asegurar sus recursos y actividades en el ciberespacio. La confirmación de la realidad de los ataques cibernéticos, con casos como el de Estonia, Georgia e Irán, configuraron a la ciberseguridad como tema principal en la agenda de las naciones.

La importancia subyacente del internet y la dependencia que experimentan los países del mismo, convierte a la ciberseguridad en una prioridad dentro de la agenda del gobierno norteamericano y el gobierno chino. *"Desde finales de los 90, tanto Estados Unidos como China han identificado el ciberespacio como crítico para su seguridad económica y nacional y han adoptado una serie de estrategias nacionales e internacionales para dar forma a Internet"* (Segal, 2013). El presente capitulo tiene por objeto identificar las principales estrategias nacionales -en el marco de la ciberseguridad-, que han implementado China y Estados Unidos para mitigar y hacer frente a las amenazas dentro del ciberespacio.

3.1 Estados Unidos y sus Estrategias Nacionales sobre Ciberseguridad

Estados Unidos fue pionero en la formulación de políticas de ciberseguridad a nivel nacional, comenzando con la creación en 1988 del primer Equipo de Respuesta a Emergencias Cibernéticas (CERT) en la Universidad Carnegie Mellon en respuesta a un número creciente de intrusiones en la red. (Shackelford & Craig, 2014).

Siguiendo las ideas de Shackelford & Craig (2014), los esfuerzos destinados a la ciberseguridad de la Infraestructura Critica Nacional (CNI) tienen su origen en el bombardeo en Oklahoma City al Edificio Federal Murrah en abril de 1995. En respuesta a este atentado, el presidente Clinton emite la "Presidential Decision Directives 39" (PDD 39), mediante la cual se crea un Grupo de

Trabajo de Infraestructura Critica y se establece como primer objetivo la protección de la infraestructura como una prioridad nacional. Tres años después del atentado y como producto del PDD 39, el gobierno Clinton publica la Directiva de la Decisión Presidencial 63, donde se define la infraestructura crítica, -los sistemas físicos y cibernéticos-, esenciales para el correcto funcionamiento del gobierno y la economía.

Estados Unidos ha sido uno de los países más activos en el desarrollo e implementación de estrategias en el tema de seguridad cibernética. De acuerdo con Pernik, Wojtkowiak & Verschoor-Kirss (2016) su primera estrategia nacional de seguridad cibernética fue publicada en 2003, mientras que los primeros países de la UE que abordaron el tema de seguridad cibernética fueron Alemania y Suecia, en 2005 y 2006 respectivamente. Desde la publicación de la Estrategia Nacional para la protección del ciberespacio en el 2003, el gobierno norteamericano ha hecho públicas otras estrategias (Estrategia 2010 y 2015) que permitan prevenir y responder adecuadamente a las nuevas amenazas que ponen en jaque la infraestructura crítica y la estabilidad del Estado.

Los ataques del 11 de septiembre, siguiendo a Candau (2010), incentivaron la creación de una estrategia de defensa nacional más activa que respondiera eficazmente a la naturaleza de las nuevas amenazas. Es por ello que se empieza a desarrollar una fuerte legislación respecto a la ciberseguridad de la infraestructura crítica. Las estrategias para salvaguardar la estructura crítica de las amenazas cibernéticas han sido parte importante de los distintos gobiernos de Estados Unidos.

> Además de las Directivas de Clinton, los presidentes Bush y Obama han emitido Directivas que tienen como objetivo asegurar la CNI (Critical National Infrastructure). Además, más de cincuenta leyes estadounidenses influyen en la ciberseguridad en una u otra capacidad, aunque ninguna de ellas constituye un marco general. (Shackelford & Craig, 2014).

3.1.1 Estrategia Nacional para Asegurar el Ciberespacio-2003

Publicada por la Casa Blanca en 2003, la Estrategia Nacional para Asegurar el Ciberespacio-2003, responde a la necesidad de proteger la infraestructura de la información y los activos que la soportan, de la amenaza constante. Esta estrategia contempla tres objetivos estratégicos: el primero, prevenir los ataques contra la infraestructura crítica; el segundo, reducir la vulnerabilidad

de la nación frente a los ataques; y el tercero, minimizar los daños y agilizar la recuperación cuando estos ocurran.

Para la consecución de dichos objetivos, dentro de esta estrategia se consagran 5 prioridades: I. creación de un sólido Sistema Nacional de Respuesta. Teniendo en cuenta que ningún programa de seguridad cibernética es totalmente seguro, el Sistema Nacional de Respuesta –como se consagra en la Estrategia emitida por la Casa Blanca en 2003-tiene como objetivo principal, la identificación rápida, el intercambio de información y la recuperación, para mitigar los daños causados por la actividad maliciosa dentro del ciberespacio; II. Programa para la reducción de la vulnerabilidad y la amenaza. Dentro de esta prioridad se visibiliza la necesidad de mejorar las capacidades de la policía para reconocer y perseguir los ataques en el ciberespacio, así como la implementación de un proceso evaluativo que permita comprender de manera más acertada el nivel de amenaza y vulnerabilidad; III. Concientización y capacitación. La falta de conciencia por parte de muchos usuarios, administradores y desarrolladores de tecnología, así como de funcionarios, auditores y directores de información frente al hecho de que las vulnerabilidades cibernéticas son reales y están a la orden del día, aumentan el riesgo de los ataques maliciosos y el robo de información; IV. Ciberespacio seguro para los gobiernos. Si bien, dentro de la estrategia se reconoce que los gobiernos administran realmente una minoría de los sistemas informáticos de infraestructura critica de la nación, también se hace énfasis en la necesidad de asegurar las redes federales e incentivar a los gobiernos a establecer programas de seguridad tecnológica; V. Cooperación internacional para la seguridad del ciberespacio. El ciberespacio conecta al mundo entero y ningún Estado puede quedar excluido de su dinámica, es por ello que las estrategias nacionales de seguridad cibernética deben estar conectadas con estrategias internacionales de ciberseguridad.

3.1.2 Estrategia Nacional de Seguridad 2010

La administración del ex presidente Barak Obama fue una de las más activas en la creación de estrategias de ciberseguridad. De acuerdo con Shackelford & Craig (2014) estas iniciativas incluyen el nombramiento de un coordinador de seguridad cibernética, una ley de seguridad cibernética y la Ley de Seguridad IT.

> La Estrategia de Seguridad Nacional de 2010 (ENS 2010) fue la primera estrategia de seguridad nacional de Estados Unidos dedicada a prestar atención sustancial a las amenazas cibernéticas; también representó un cambio en la caracterización de las amenazas cibernéticas por parte del gobierno federal, con énfasis en pasar del terrorismo no estatal a actividades patrocinadas por el Estado y de una preocupación predominantemente política a una preocupación económica. (Pernik, Wojtkowiak & Verschoor-Kirss, 2016)

La estrategia Nacional de Seguridad de 2010 se consagra como la primera estrategia dentro del mandato del presidente Barak Obama y como la primera estrategia que reconoce que los ataques cibernéticos no solo son perpetrados por grupos terroristas: *"Las amenazas que enfrentamos varían desde hackers criminales individuales hasta grupos criminales organizados, desde redes terroristas hasta naciones avanzadas"* (Obama, 2010). Los objetivos y prioridades de la ENS 2010 no están muy alejados de La Estrategia Nacional para Asegurar el Ciberespacio 2003. Al igual que en la de 2003, la ENS 2010 concede gran importancia a la inversión en las personas y la tecnología, con el objeto de diseñar tecnología más segura que favorezca las redes gubernamentales e industriales críticas. Fomentar la conciencia sobre seguridad cibernética y la alfabetización digital es una prioridad en las dos estrategias, así como el trabajo conjunto del sector público y privado. Involucrar a la población civil en los esfuerzos para mitigar las amenazas cibernéticas es una necesidad, teniendo en cuenta que la mayoría de los sistemas informáticos están controlados por individuos. Pensar que la seguridad de las redes solo compete a los expertos en seguridad informática es cosa del pasado. Gobiernos, instituciones e individuos son ahora actores importantes en el ámbito de ciberseguridad.

3.1.3 Estrategia Internacional para el Ciberespacio 2011

> El mundo debe reconocer colectivamente los retos que plantea la entrada de los actores malévolos en el ciberespacio y actualizar y fortalecer nuestras políticas nacionales e internacionales en consecuencia. Las actividades emprendidas en el ciberespacio tienen consecuencias para nuestras vidas en el espacio físico, y debemos trabajar para construir el imperio de la ley. (Oficina de la Casa Blanca, 2011).

Consiente de la necesidad de formular estrategias que trasciendan las fronteras estatales, la Estrategia Internacional para el Ciberespacio 2011 se configura como una invitación a que las

demás naciones se unan a la protección del ciberespacio. Como lo afirma la administración Obama dentro del documento (2011), Estados Unidos trabajará a nivel internacional, en la creación y consolidación de una infraestructura de comunicación e información abierta, interoperable, segura y fiable, que incentive el comercio seguro, la seguridad nacional, la libertad de expresión y la innovación.

Las normas son un pilar importante y necesario en todas las esferas de las relaciones internacionales. El gobierno de Estados Unidos, consciente de que las normas hacen previsible el accionar de un Estado y que de una u otra forma regulan su accionar, busca establecer unas normas de comportamiento general –con Estados que compartan sus ideales y valores- que guíen la política exterior de defensa. De acuerdo con la Oficina de la Casa Blanca (2011) los principios que deben soportar la norma general en el ciberespacio son: a) defensa de las libertades fundamentales, b) respeto de la propiedad, incluyendo patentes, secretos comerciales, marcas y derechos de autor; c) valoración de la privacidad, d) protección contra la delincuencia. Se debe identificar e imponer castigos a los responsables de ataques cibernéticos y actos maliciosos; y, d) legítima defensa como se contempla en la Carta de las Naciones Unidas.

3.1.4 Estrategia Nacional de Seguridad 2015

La Estrategia Nacional de Seguridad 2015, la segunda durante el gobierno de Barack Obama, como lo afirman Pernik, Wojtkowiak & Verschoor-Kirss (2016), reconoce que el peligro de los ataques cibernéticos crece rápidamente, haciendo necesario el fortalecimiento de la ciberseguridad de la infraestructura crítica y hace énfasis en la necesidad de que los actores cibernéticos maliciosos asuman los costos de sus acciones. La Estrategia 2015 reafirma los objetivos de la ESN anteriores: asociación del sector público y el sector privado, intercambio de información y el avance en las capacidades tecnológicas. De igual manera dentro del documento se contempla como objetivo la promoción de las normas internacionales en el ciberespacio.

Si bien, no son estas las únicas estrategias -a nivel nacional- que el gobierno norteamericano ha planteado para hacer frente a un enemigo poco tradicional, estas nos permiten hacer un balance de los principales objetivos, que como se puede evidenciar- si bien han tenido varias transformaciones- han conservado su esencia. Las estrategias nacionales para salvaguardar a los

gobiernos, las industrias y los ciudadanos, son realmente importantes, ya que preparan al grueso de la población – o por lo menos a una parte importante de ella- para enfrentar y sobreponerse a los ataques informáticos, cada día más elaborados y más agresivos; sin embrago es necesario que estas se acompañen de estrategias internacionales, donde la cooperación sea un pilar en el tema de seguridad cibernética.

3.1.5 Otras Iniciativas sobre ciberseguridad

Estados Unidos es uno de los países con mayor número de estrategias e iniciativas dirigidas al mantenimiento de la seguridad cibernética. De acuerdo con Pernik, P., Wojtkowiak, J., & Verschoor-Kirss (2016) dentro de estas iniciativas podemos encontrar algunas de carácter militar como:

1. Estrategia Nacional Militar de los Estados Unidos de América (2011): dentro de esta estrategia se contemplan las capacidades abstractas de los militares como la defensa en las redes y la mejora de la resistencia. Igualmente, Estados Unidos afirma que está tan preparado para disuadir en el ciberespacio como en el espacio físico.

2. Las Operaciones de Información (JP 3-13) de 2012: dentro de esta iniciativa se suministra una doctrina común para la planificación, preparación, ejecución de las operaciones de información y se incluyen interpretaciones de ius in bello e ius ad bellun en el ciberespacio.

3. Las Actividades Cibernéticas Electromagnéticas (FM 3-38) del Ejército de los Estados Unidos (2014): se brindan directrices en el desarrollo de actividades electromagnéticas, así como las tácticas para llevarlas a la práctica.

El Plan X: el Plan X se constituye como un programa de guerra cibernética que desarrolla plataformas donde el Departamento de defensa (DoD) pueda planificar, llevar a cabo y evaluar la guerra cibernética.

Una de las últimas acciones del gobierno Obama frente al tema de ciberseguridad, de acuerdo con CNN (2016) es el Plan de Acción de Ciberseguridad Nacional que pondrá en marcha una estrategia a largo plazo que busca aumentar la seguridad cibernética y su respectivo control. Dentro del Plan se contempla la creación de la Comisión de Mejoramiento de Ciberseguridad Nacional, que busca reunir expertos capaces de hacer recomendaciones al gobierno para fortalecer la seguridad

cibernética en el sector público y privado. De igual manera se planea una inversión de 19.000 millones de dólares en ciberseguridad para el año 2017, lo que representa un incremento en la inversión del 35%. Igualmente se planea la creación de alianzas estratégicas con gigantes tecnológicos como Google, Facebook, DropBox y Microsoft, que permitan asegurar las cuentas de millones de usuarios.

3.2 China y sus Estrategias sobre Ciberseguridad

Al igual que en otros gobiernos, el tema de seguridad cibernética ha desencadenado una gran preocupación para China, lo cual ha dado lugar al aumento de los esfuerzos para controlar a información en el país y con ello la creación de una nueva legislación para consolidar los esfuerzos de ciberseguridad. Desde el periodo en que Estados Unidos amenazo con imponer sanciones cibernéticas contra China por presunto espionaje industrial, China se ha comprometido a redactar y aprobar leyes en materia de ciberseguridad con el fin de mejorar su postura de seguridad y así mismo proteger sus intereses económicos. (Lasiello, 2017).

De acuerdo con Xingan Li (2015) están son algunas leyes estatutarias y regulaciones administrativas que China ha implementado con el fin de ejercer control sobre el internet y contrarrestar la actividad criminalizadora, el filtrado de contenido y el monitoreo de usuarios para mantener la seguridad y la estabilidad a nivel comunitario y estatal.

1). En el año 1994 se instauró la norma definida sobre ciberdelincuencia: cuando el Consejo de Estado promulgó la Ordenanza sobre protección de la seguridad del sistema informático de información (Decreto del Consejo de Estado No. 147, 18 de febrero de 1994). Este estatuto establece responsabilidad legal para cinco tipos de actividades: - violar o amenazar los sistemas informáticos de información; - violar el sistema informático de registro de información de redes internacionales; - no informar de los casos ocurridos en los sistemas informáticos de información de acuerdo con el tiempo prescrito; - negarse a mejorar la situación de seguridad, después de recibir el aviso de la agencia de seguridad pública.

2). La ley penal de China de 1997: Esta ley penal fue difundida a principios del año cuando se expandió el uso del internet de forma acelerada, esta ley proporcionó criterios y directrices fundamentales para condenar a los ciberdelincuentes, con la ayuda de otras leyes estatutarias y reglamentos administrativos, se está implantando un sistema legal y regulatorio para eliminar la

propagación del ciberdelito de diversas formas, la llamada pestilencia del nuevo siglo, en el ciberespacio.

3). En el año 2000, el Comité Permanente de la Asamblea Popular Nacional promulgó una ley integral para mantener la seguridad en Internet, en respuesta a los nuevos retos a los que se estaban enfrentado, que fue a única ley sobre seguridad en internet aprobada por la legislatura.

A pesar de algunas de las estrategias y leyes implementadas por la república de China, el cibercrimen continuaba creciendo a pasos agigantados en el año 2011.

> *"Según estimaciones, los daños que ha causado el delito cibernético a la economía de este país representaron más de los 830 millones de dólares y afectaron a más del 20% de los usuarios y sitios Web, de manera que la "seguridad de la información" hasta entonces no se mostraba como una "seguridad de la red" técnica efectiva"* (Lindsay 2015).

De acuerdo con Lindsay (2015) y Lasiello (2017), El gobierno de China ha instaurado una nueva legislación e iniciativas relacionadas con la seguridad de la información que respaldan sus intereses directamente en el plano interno, dentro de estas iniciativas se encuentran:

3.2.1 Creación del Grupo Líder de Seguridad en Internet en 2014

Antes de 2014, la responsabilidad de la política de seguridad cibernética pertenecía al Subcomité del Grupo Líder de Información del Estado CCP (SILG), que fue creada en el año 2001 y su objetivo consistía en guiar el desarrollo nacional de la tecnología de la información. En febrero de 2014, a causa de las tensiones procedidas por las filtraciones de Snowden, el Partido Comunista Chino (PCCh), notificó la creación del Grupo Líder en Ciberseguridad e Informatización (CILG), dirigido por el presidente Xi Jinping, este grupo líder en ciberseguridad se creó con el fin de reforzar la disciplina del partido y responder a las amenazas cibernéticas procedentes del extranjero, así mismo según Lasiello 2017, este grupo líder tiene como objetivo proteger la seguridad nacional, salvaguardar los intereses nacionales y promover el desarrollo de la tecnología de la información. El grupo tendrá completa autoridad sobre las actividades en línea, incluidas las económicas, políticas, culturales, sociales y militares. El grupo líder demuestra el compromiso de China en la creación e implementación de futuras políticas cibernéticas para el país, de hecho, China diseño su Esquema de estrategia Nacional de Desarrollo de TI (Technology Industry), con el fin de posicionar a China como dominio de internet para el 2050.

3.2.2 Ley Antiterrorista de 2015

En diciembre de 2015, China aprobó una nueva "ley antiterrorista" la cual ayudaría a abordar las crecientes amenazas terroristas en el país y reforzar la seguridad internacional. De acuerdo con Lasiello (2017) esta ley obliga a las compañías de tecnología a descifrar información que brinda a las autoridades chinas y el acceso a datos encriptados. La ley refuerza aspectos de control de la información, monitoreo organizacional, cumplimiento tecnológico y colaboración con las autoridades chinas en nombre de la seguridad.

Según un comunicado de prensa de CNN, esta ley exige a las empresas de telecomunicaciones y proveedores de servicios de internet a proporcionar apoyo y asistencia técnica, "incluyendo el descifrado", a las autoridades. El gobierno dice que el aumento de la actividad en línea de los terroristas justifica los nuevos requisitos.

3.2.3 Ley de "Seguridad Cibernética" de 2016

En noviembre de 2016, de acuerdo con Moran (2017), el gobierno chino aprobó la ley de "Seguridad Cibernética, esta ley regula aspectos como la protección de datos, la prohibición de uso de la red para actividades que inciten la destrucción de la soberanía nacional, prohíbe la creación o explotación de redes con fines delictivos o que los promuevan, y autoriza al gobierno a bloquear activos de individuos y organizaciones extranjeras involucradas en ataques a las infraestructuras de la información. Según esta ley, "las agencias gubernamentales emitirían directrices adicionales para la seguridad de la red en "industrias críticas" como telecomunicaciones, energía, transporte, finanzas, defensa nacional y asuntos militares, y la administración gubernamental. De igual forma El gobierno adoptará una protección prioritaria sobre la infraestructura de información clave que compromete seriamente seguridad nacional y el interés público, especialmente en caso de datos dañados o filtrados". (Lasiello, 2017). Esta ley salvaguarda la soberanía en el ciberespacio, la seguridad nacional y los derechos de los ciudadanos.

3.2.4 Ley de Ciberseguridad de 2017

Según un comunicado de la agencia de noticias Xinhua para China Daily, el 1 de junio entró en vigor la nueva ley sobre ciberseguridad en China, esto con el fin de incrementar la censura y el control de internet. Según la Administración de Ciberespacio de China (CAC), el principal objetivo de esta ley es "salvaguardar la soberanía en el ciberespacio, la seguridad nacional y el interés

público, así como los derechos y los intereses de los ciudadanos". De igual forma, según las autoridades del país, esta ley busca proteger la privacidad de los datos y reducir la vulnerabilidad de ataques como el del virus WannaCry que afectó a miles de sistemas informáticos en todo el mundo.

Este comunicado de prensa también asegura que esta ley prohíbe que los usuarios de Internet puedan publicar contenido que perjudique o afecte "el honor nacional" o que pueda intentar "degradar el sistema socialista" o la alteración del orden social y económico vigente. Esta ley también estipula que quienes violen las disposiciones e infrinjan la información personal enfrentarán fuertes multas.

Esta ley se ha considerado polémica, pues según Vidal (2017), en un comunicado del País Internacional, las empresas extranjeras se quejan por posibles limitaciones a su capacidad de hacer negocios en el país. Sin embargo, La CAC asegura que la medida "*no restringe la entrada de empresas extranjeras o su tecnología y productos en el mercado chino, ni limita el flujo libre y ordenado de datos de acuerdo con la ley*" (2017). China, fundamenta que es una víctima frecuente de ciberataques y necesita instrumentos para defenderse de ellos.

Como lo afirma David Morán (2017) y Lindsay (2015), muchas de estas estrategias y leyes implementadas son insuficientes para la regulación de un contexto tan complejo como el ciberespionaje en China. Las políticas cibernéticas y la aplicación de la ley se han convertido en un desafío para todos los Estados, pero la falta de transparencia gubernamental de China empeora el problema, la descentralización del poder en la toma de decisiones, la falta de comunicación adecuada, la cooperación institucional desordenada, crean un ambiente permisivo para la ciberdelincuencia.

Capítulo 4

El problema cibernético China-Estados Unidos

Desde antaño, la relación Estados Unidos-China se ha caracterizado por la confrontación y desconfianza mutua. A las fuentes de conflicto tradicionales entre los dos Estados (economía, política, derechos humanos, etc.), en la actualidad, se le suma una fuente de conflicto con características totalmente diferentes, que pone en la cuerda floja la estabilidad de las relaciones entre los dos países: la ciberseguridad. Si la cooperación en temas de seguridad tradicional ha sido complicada entre China y Estados Unidos, la cooperación en materia de seguridad cibernética es aún más compleja y problemática. Las crecientes operaciones cibernéticas, las percepciones erróneas de las capacidades reales de la contraparte, el dominio del ciberespacio, la falta de una terminología mundialmente aceptada y las intrusiones y el robo de propiedad intelectual, son solo algunos de los agravantes a la hora de abordar la cooperación entre los dos países.

La cooperación en materia de ciberseguridad –entre China y Estados Unidos- ha sido realmente escasa. Inicialmente, se podría decir que la falta de cooperación se debe a la novedad del conflicto y que, por ende, aún es muy prematuro hablar de acuerdos o reglas que reduzcan las amenazas en el ciberespacio. Sin embargo, la falta de cooperación entre estas dos potencias es un factor constante aun en las cuestiones se seguridad tradicional- como se demostró en el primer capítulo-. Al igual que en la cooperación en materia nuclear y espacial, la cooperación en ciberseguridad se ve fuertemente afectada por la desconfianza mutua y la falta de compromisos. *"La ausencia de compromisos firmes con las normas que rigen la actividad en este nuevo dominio, representa un importante riesgo para la relación bilateral, la paz y la estabilidad regional y el orden global"* (Scott, Libicki & Cevallos, 2016; pp: 18)

Como lo afirma Lejarza (2013) China y Estados Unidos se han visto enfrentados en un cruce de acusaciones mutuas sobre ataques a las redes informáticas de su infraestructura crítica y robo de información de sectores cruciales para los intereses nacionales. Aunque los gobiernos de Washington y Beijing han centrado sus esfuerzos diplomáticos en diseñar un marco de actuación en el ciberespacio, lo cierto es que ambos países se han embarcado en una carrera para incrementar sus capacidades defensivas en este ámbito, originando lo que se podría denominar "la ciberguerra fría del siglo XXI".

De acuerdo con Scott *et al*., (2016) quienes toman las ideas de Yi Wenly (2012) la desconfianza creciente entre Estados Unidos y China está minimizando la oportunidad del dialogo en materia de ciberseguridad –inclusive en las áreas de interés común-, lo que significa, que las oportunidades para empezar a negociar posibles reglas y normas sobre ciberseguridad se están obscureciendo. Así mismo, como argumentó Amy Chang, especialista china en seguridad cibernética:

> Las dos naciones continúan enfrentando obstáculos sustanciales para desarrollar esfuerzos de cooperación y mejorar el entendimiento mutuo sobre temas del ciberespacio, de manera que las relaciones han descendido a la desconfianza casi total de los motivos, las acciones y las agendas mutuas, que afectan otras facetas de la relación bilateral. (Chang, 2014).

Si bien, Estados unidos y China han presentado dificultades en su relación bilateral, son las diferencias en objetivos, valores y prácticas entre los elementos diplomáticos, de inteligencia, militares y económicas, los obstáculos primordiales que enfrentan dichos países en su camino hacia la cooperación.

Para autores como Leiva (2015) y Warren, Libicki & Stuth (2016), el tema sobre el uso y entendimiento de la terminología de ciberseguridad es uno de los problemas que revelan las profundas brechas que existen entre estos dos países para lograr estrategias de seguridad conjuntas. Chang (2014) afirma que las definiciones de "seguridad cibernética" divergen conceptualmente entre EE. UU y China. Por un lado, en China el término "ciberseguridad" rara vez es utilizado y no es congruente con la forma en que se entiende en comunidad de políticas estadounidenses, al igual que "seguridad cibernética" y otros términos derivados de la palabra "cibernético". Mientras que Estados Unidos emplea el término "ciberseguridad" para referirse a la protección y defensa de una amplia gama de información electrónica y de comunicación, China usa el término "red de seguridad" o "Seguridad de la información", para referirse más específicamente a la protección de redes de información digital.

La cooperación en el campo de la ciberseguridad, como se mencionó anteriormente, se ve seriamente obstruida por diversos factores. Scott, Libicki & Cevallos (2016) agrupan los desacuerdos –en el ciberespacio- entre China y Estados Unidos en cinco áreas: 1) la legitimidad del uso del ciberespacio como medio para el espionaje económico o industrial; 2) el uso del ciberespacio para formas de espionaje tradicional, relacionado con la seguridad nacional; 3) el uso

del ciberespacio para llevar a cabo actividades militares; 4) el derecho que tienen o no los Estados para controlar el flujo de información dentro de sus fronteras y; 5) la gobernanza de internet. Estos desacuerdos o preocupaciones emanan principalmente del gobierno estadounidense.

Desde la perspectiva de Estados Unidos, las constantes intrusiones en las redes corporativas y el robo de propiedad intelectual y secretos comerciales, ha sido una de las principales quejas contra China. De acuerdo con Larry Wortzel (2015) miembro de la Comisión de Revisión económica y de Seguridad de Estados Unidos-China, el ciberespionaje por parte de China, es una seria amenaza para los intereses comerciales de Estados Unidos y la competitividad de las industrias claves del país. En palabras de Thomas Donilon, ex asesor de seguridad nacional de Estados Unidos, el tema de la seguridad cibernética no es solo una preocupación de seguridad nacional, así:

> Cada vez más, las empresas estadounidenses hablan sobre sus serias preocupaciones sobre el robo sofisticado y dirigido de información comercial confidencial y propiedad tecnológica a través de intrusiones cibernéticas que emanan de China a una escala sin precedentes. (Donilon, 2013)

Para Scott *et al.,* (2016) es difícil de establecer el valor total del robo de propiedad intelectual y empresarial-del que ha sido objeto Estados Unidos-, sin embargo, de acuerdo con Keith Alexander, ex director de la Agencia de Seguridad Nacional y ex comandante del Comando Cibernético de Estados Unidos, el valor de las pérdidas es aproximadamente de 338 mil millones al año, incluyendo pérdidas de propiedad intelectual y tiempo de inactividad destinado a responder a las intrusiones. Esto es a lo que el mismo Keith ha denominado como "*la mayor transferencia de riqueza de propiedad intelectual*".

De acuerdo con Wortzel (2015) -como factor agravante- estas actividades están apoyadas por el gobierno chino, el EPL y el Ministerio de Seguridad del Estado, quienes proporcionan información y datos de empresas estatales -extraídos durante las operaciones de espionaje cibernético-, con el objeto de mejorar la competitividad de sus industrias, reducir sus calendarios de I+D y reducir los costos propios del desarrollo de nuevas tecnologías.

Si bien, detectar el origen de un ataque en el ciberespacio, es realmente difícil, existen pruebas circunstanciales que señalan a China como el principal perpetrador de las intrusiones a través de la red. De acuerdo con Lindsay (2015) existe una amplia gama de evidencias circunstanciales, pero

colectivamente aceptables –uso de malware y configuración de teclado en idioma chino, direcciones de internet y dominios registrados en China- que apuntan a este como el culpable de dichas actividades.

El ciberespionaje y robo de propiedad intelectual por parte del gobierno chino, fue discutido por funcionarios estadounidenses en privado por muchos años. Sin embargo, de acuerdo con la compañía de inteligencia FireEye (2016) es hasta 2013 cuando el gobierno estadounidense traslada el ciberespionaje chino a la esfera pública. El informe APT1 (Advanced Persistent Threats 1), publicado por FireEye en 2013, atribuyó años de robo corporativo de propiedad intelectual a la Unidad 61398 del PLA. De acuerdo con FireEye (2016) el informe mostró las herramientas, tácticas y objetivos de las operaciones cibernéticas chinas, dejando al descubierto evidencias que soportaban las sospechas de larga data del espionaje cibernético sobre blancos estadounidenses.

Aun cuando las quejas por parte de Estados Unidos son constantes, el gobierno chino también ha manifestado ser una víctima del espionaje cibernético por parte de Estados Unidos. En respuesta a las diferentes acusaciones, la República popular de china ha asegurado en numerosas ocasiones que ellos son víctimas, no villanos. *"China también es víctima de ciberataques"* (Xiaokun &Yingzi, 2012; Yang Yujun, 2012; en China Daily; Yie, 2010) y que "*es poco profesional e irresponsable emitir juicios sin una investigación exhaustiva y pruebas confiables"* (Xinhua,2012)

De acuerdo con Lindsay (2015) las revelaciones de Snowden no solo revitalizaron el debate sobre el equilibrio entre la privacidad y la seguridad en una democracia, sino que además cuestionaron la legitimidad moral de las quejas de Estados Unidos. *"Las fugas de inteligencia de Edward Snowden en 2013 subrayaron la sofisticación y el alcance de la vigilancia por Internet de Estados Unidos y sus aliados contra blancos en todo el mundo, incluso en China"* (Lindsay, 2015)

La Agencia de Noticias Xinhua –la agencia oficial de noticias del gobierno de la República Popular de China y la mayor del país- ha sido insistente en aclarar que China también es una víctima constante de los ciberataques que se originan alrededor del mundo. De acuerdo con la agencia (2012) China se ha convertido en la mayor víctima de ciberataques. Un informe publicado por la principal red de monitoreo de seguridad informática de China -Centro Nacional de Coordinación de Respuesta de Emergencia de China (CNCERT/CC)- afirmó que un total de 47.000 IPs (Internet

Protocol) en el extranjero estuvieron involucrados en ataques contra 8,9 millones de computadoras chinas en 2011, 3.9 millones de computadoras más en comparación con el año anterior.

De acuerdo con Yan Jie (2010) en una entrevista para Xinhua, Zhou Yonglin, subjefe del departamento de operaciones del Equipo Técnico de Respuesta a Emergencias de la Red Nacional Informática de China (CNCERT/CC), indicó que la creciente alza de cibernautas chinos –con una conciencia de seguridad de internet rezagada- los ha convertido en el principal blanco de ciberataques. Además, Zhou acusó a piratas extranjeros –especialmente estadounidenses- de controlar de manera ilegal las computadoras en China, implantando programas maliciosos como troyanos y zombis. Zhou, señaló que los IP maliciosos con sede en Estados Unidos, Japón y Corea, representaron la mayor amenaza a la seguridad nacional de la República Popular de China, durante 2011.

En "US Cyberattacks against China (2009-present)", una infografía realizada por China Daily Website (2014), basada en datos del CNCERT y Symantec, se señala a Estados Unidos como el principal atacante del espacio cibernético chino. De acuerdo con el informe, Estados Unidos ocupa el primer lugar –durante el periodo comprendido entre 2009 y 2013- controlando las computadoras chinas a través de troyanos y botnets. *"Aproximadamente el 20.3% de las actividades maliciosas de la Web en el mundo en 2013 provienen de los EE. UU., lo que lo convierte en el productor No.1 de dichas actividades"* (China Daily, 2014). El mismo informe indica que en 2013, 10,9 millones de ordenadores chinos fueron controlados por servidores extranjeros y que el 32% de ellos estaban ubicados en Estados Unidos. Así mismo, el 42% de las 30,199 direcciones falsas en chino pertenecían a Estados Unidos.

4.1 Cooperación en materia de Seguridad cibernética

En respuesta a los problemas de ciberespionaje que han puesto a prueba las relaciones entre las dos naciones, Estados Unidos y China llegaron a un acuerdo en materia de seguridad cibernética en 2015, que, de acuerdo con Louie (2017) busca disminuir el espionaje económico entre los dos países, especialmente el robo de propiedad intelectual y secretos comerciales.

Durante la visita de Estado del 24 al 25 de noviembre de 2015, el presidente Xi Jinping y el presidente Barack Obama, llegaron a un acuerdo cibernético. Tomando las ideas de John Rollins (2015), miembro del Servicio de Investigación del Congreso (CRS) y especialista en terrorismo y

seguridad nacional, el acuerdo contempla: 1) respuesta oportuna a la solicitud de información y asistencia sobre actividades cibernéticas maliciosas; 2) abstenerse de realizar o apoyar deliberadamente el robo de información y propiedad intelectual por medios cibernéticos; 3) identificar y promover normas apropiadas de comportamiento estatal en el ciberespacio; y 4) establecer un mecanismo de dialogo conjunto de alto nivel, para tratar el delito cibernético y las cuestiones relacionadas.

Aunque algunos han visto el acuerdo con optimismo, otros creen que el acuerdo es solo una formalidad diplomática entre las partes, que no frenará el robo de propiedad intelectual patrocinado por el Estado. Para Brown & Yung (2017a) si bien, el acuerdo es una señal de esperanza –por ser el primer acuerdo sobre el tema- existen serias dudas sobre si este tendrá un efecto significativo en el comportamiento de ambas naciones, especialmente en China, teniendo en cuenta que no goza de la reputación de adherirse con cuidado a los acuerdos internacionales.

En junio de 2016 –a casi un año de haberse firmado el acuerdo- la compañía de inteligencia FireEye, público un informe donde se asegura que el número de redes comprometidas por parte de los grupos de piratería con base en China, se redujeron de 60 en febrero del 2013 a menos de diez en mayo de 2016. Sin embargo, parece que el informe es bastante optimista. Como lo afirma Segal "*La ausencia de pruebas no es lo mismo que la evidencia de ausencia, y los chinos pueden ser cada vez más furtivos y sofisticados en sus ataques"* (2016; párr. 2). Para Louie (2017) el hecho de que los ataques estén disminuyendo desde la República Popular de China, no necesariamente significa una disminución, esto podría significar que existe un tipo de tercerización de los ataques cibernéticos, lo que daría cuenta de la sofisticación de los ataques y del desafío que representan para las naciones.

Greer & Montierth (2017) sostienen que, si bien hay informes, como el de FireEye, que indican que el acuerdo ha contribuido al descenso significativo del robo de propiedad intelectual, otros informes señalan que, en materia cibernética, las relaciones entre Estados-Unidos siguen experimentando un alto grado de hostilidad. Así mismo:

> No solo las actividades de ciberespionaje [de ambas partes] probablemente estén en curso…, sino que los analistas sugieren que continúan los esfuerzos para infiltrarse en las empresas de

> EE.UU., [con la diferencia de que estos esfuerzos] son simplemente más sofisticados, específicos y calculados. (Greer & Montierth, 2017; párr. 1)

Aunque el acuerdo firmado entre Obama y Xi Jinping no haya logrado su objetivo y el espionaje y robo de propiedad intelectual siga latente entre las dos naciones, y aunque haya escepticismo sobre si china cumplirá o no el acuerdo, es importante rescatar como lo afirman Brown & Yung (2017a) la voluntad de china de hablar sobre el espionaje económico como una categoría diferente de espionaje.

> En el pasado, China no parecía estar de acuerdo en que haya una categoría separada de espionaje económico, afirmando en cambio que las medidas adoptadas para fortalecer la economía china, en última instancia, [responden al] propósito de la seguridad nacional. (Brown & Yung, 2017a; párr. 16)

El poco éxito del acuerdo tiene diferentes explicaciones. Para Greer y Montierth (2017) –quienes califican de fallido el acuerdo-, la principal explicación es que ninguno de los gobiernos estaba preparado para abrazar el acuerdo -de manera integral- desde el comienzo. Las tendencias constantes de robo cibernético – a pesar del acuerdo- responden, según Greer & Montierth (2017) al hecho de que sea casi imposible hacer cumplir la ley cibernética internacional y responsabilizar a los infractores (problemas de atribución), sumado a los fuertes incentivos económicos que tienen las organizaciones dedicadas a la piratería.

Para Brown y Yung (2017c) la interpretación del acuerdo es uno de los principales problemas. Los términos del acuerdo suponen que cada uno de los Estados cumpla con sus leyes nacionales, lo que puede ser un gran obstáculo para el éxito del acuerdo, teniendo en cuenta que tanto China como Estados Unidos tienen un enfoque diferente de gobernanza en el ciberespacio. Esto podría generar divergencias en la interpretación del acuerdo, como consecuencia de las leyes nacionales de cada país. Como continúan Brown y Yung (2017c) otro problema es el significado y la importancia que cada país le da al acuerdo. Mientras que, para China esto solo es un "consenso" para Estados Unidos es una Acuerdo con líneas específicas de actuación.

Adam Segal, experto estadounidense en ciberseguridad y Director del Programa de Políticas Digitales y Ciberespaciales en el Consejo de Relaciones Exteriores, es poco optimista frente al acuerdo. Para Segal (2016) aunque Estados Unidos y China tienen intereses compartidos de

Ciberseguridad –evitar la proliferación de capacidades cibernéticas, por parte de actores no estatales y limitar los ataques contra las redes financieras- es muy difícil llevar esto a una cooperación concreta, teniendo en cuenta que la desconfianza estratégica entre las dos naciones sigue siendo alta y, como lo afirma Segal (2016) continúan teniendo opiniones y percepciones divididas frente a varios asuntos cibernéticos como el flujo libre de información, la gobernanza de internet, la localización de datos y la mejor forma de proteger sus productos de tecnología de la información y las cadenas de suministro.

CONCLUSIONES

La revolución tecnológica, abrió para la humanidad un abanico de oportunidades sin precedentes. El ciberespacio se consagró como un escenario que brinda nuevas oportunidades a los diferentes actores del sistema internacional, pero que, a su vez, exige una fuerte regulación para controlarlo y hacer frente a los retos que trae consigo. La naturaleza incontrolable del ciberespacio lo convierte en un aliado perfecto en los conflictos actuales. La precisión y el sigilo de las acciones maliciosas a través de la red ponen de manifiesto la capacidad real de los ataques cibernéticos y la dificultad para controlarlos.

Antaño, el poderío militar y económico fue la clave para ejercer poder o influencia sobre otros Estados. En la actualidad no se requiere de grandes flotas terrestres, marítimas o aéreas para amedrentar o causar daños a los adversarios; basta una(s) computadora(s) –como se demostró en el caso de Estonia- para desestabilizar un país y causar grandes pérdidas. Aunque aún no se conoce un caso de ciberguerra, Estonia e Irán se convierten en un ejemplo plausible de los alcances de un ataque cibernético. El caso de estonia es una advertencia para las demás naciones, de lo vulnerables que pueden llegar a ser, cuando la mayoría de sus funciones están conectadas a la red. El ataque contra irán en 2010, es un punto de inflexión en la historia de los ataques cibernéticos. Hasta ese momento –a excepción del caso de Estonia (2007) y Georgia (2008) la mayoría de las actividades maliciosas en el ciberespacio estaban relacionadas con el espionaje y el robo de información. Sin embargo, en 2010, un ataque cibernético –por primera vez en la historia- logra causar daño físico real, exclusivamente a través de medios tecnológicos.

La era digital ha traído serias implicaciones sobre la seguridad nacional. Aunque se considera que los Estados seguirán siendo el actor dominante en la escena mundial, se augura para los actores estatales nuevos retos, debido al aumento de actores no gubernamentales que tienen acceso al poder que proviene de la información, de modo que se enfrentaran a un desafío bastante grande ya que encontraran el escenario mucho más concurrido y difícil de controlar. Así mismo, el ciberespacio brinda nuevas oportunidades para los Estados que no cuentan con gran poder económico o militar y permite la entrada de nuevos jugadores en el ajedrez internacional. Georgia y Estonia se han convertido en dos actores claves en el ámbito de la ciberseguridad, haciendo uso de algo que otros actores no tienen: experiencia. La creciente creación de ejércitos cibernéticos por parte de numerosas naciones complica aún más el control del ciberespacio. La contundencia y

precisión de los ciberataques se ha convertido en un fuerte atractivo para explotar las vulnerabilidades del ciberespacio y causar daño sin hacer uso de grandes recursos.

El ciberespacio, ha generado un impacto en la política mundial debido a los cambios y trasformaciones que afectan al ejercicio y actividades de la política internacional, así como los indicios tradicionales de las relaciones internacionales, lo cual plantea nuevos retos para la comunidad internacional. Este nuevo espacio afecta no solo las relaciones entre los estados, sino que además trae consigo influencias de nuevos actores no gubernamentales que también tienen poder gracias a su amplio dominio, convirtiéndose en un escenario vulnerable de constantes amenazas y delitos.

Ataques cibernéticos como el de Estonia e Irán han demostrado la debilidad de internet y la vulnerabilidad de las defensas cibernéticas. Cualquier país que use internet o que tenga su infraestructura crítica conectada a internet, debe ser consciente de las vulnerabilidades y de las consecuencias de un ciberataque a su sistema. La necesidad de asegurar las redes crece a pasos agigantados a medida que los Estados se enfrentan a amenazas cada vez más sofisticadas. La lucha contra las amenazas cibernéticas requiere esfuerzos coordinados y la creación de estrategias nacionales e internacionales sólidas. Como se ha dicho en repetidas ocasiones, la creación de estrategias nacionales no es suficiente para abordar las problemáticas de un espacio que no conoce fronteras. Los Estados tienen que ver la cooperación internacional como el medio facilitador para la administración y control de este dominio.

Aunque la cooperación en materia de ciberseguridad es insuficiente y muy frágil –especialmente en la relación Estados Unidos-China- y aunque las diferencias ideológicas siguen siendo muy grandes, el Acuerdo sobre Seguridad Cibernética firmado en 2015, es un avance significativo y una luz de esperanza, no solo para las dos naciones sino para la comunidad internacional. Aunque para muchos el acuerdo parece haber fallado -a pesar de la aparente cooperación bilateral-, el Acuerdo Obama-Xi sienta un precedente para las actuales y futuras administraciones. En la actualidad los dos países tienen la oportunidad de aprovechar el dialogo conjunto que se inició en 2015 para reenfocar el acuerdo hacia temas con mayor oportunidad de cooperación. Es probable que el espionaje de Estado a Estado continúe en los próximos años, así como también el robo de información y datos comerciales. Es por esta razón que Estados Unidos y China deben encontrar intereses mutuos y reenfocar sus esfuerzos de cooperación.

La protección e integridad de los datos financieros puede ser un buen comienzo para la cooperación entre estos dos países. Estados Unidos y China están de acuerdo en que la protección de los datos financieros mundiales es una de los principales problemas que enfrentan las redes mundiales. Las actividades cibernéticas maliciosas, sin duda, representan un peligro para la estabilidad de los sistemas financieros mundiales.

La disputa constante entre China y Estados Unidos ha sido un obstáculo en la identificación de actores que representan quizá una mayor amenaza. China y Estados Unidos pueden liderar iniciativas para la protección del ciberespacio que incluyan a países como Corea del Norte, Irán, Georgia, Estonia, entre otros. Es importante que China y Estados Unidos pongan especial atención en actores como Corea del norte y que su disputa no los deje ciegos ante las nuevas amenazas. Aunque la cooperación en este campo sea compleja, es importante que los países encuentren incentivos para crear estrategias comunes para el tratamiento, la gestión y prevención de las actividades maliciosas en el ciberespacio.

Es indispensable que los países se adapten a los cambios que se están presentando en este nuevo ámbito internacional, principalmente en materia de seguridad. En la relación bilateral entre China y Estados Unidos es de vital importancia garantizar medidas que controlen la implementación de capacidades ofensivas y defensivas y sobre todo promover mediadas que respondan al fomento de la confianza, dado que es uno de las principales limitantes a la hora de llegar a un acuerdo bilateral. Así mismo es importante la participación de un mayor número de países en la estipulación de acuerdos para preservar la ciberseguridad y alcanzar acuerdos formales los cuales permitan vislumbrar un ambiente de seguridad en el sistema internacional. No será una tarea fácil teniendo en cuenta que cada uno de los países trata de imponer sus preferencias y objetivos que mejor le convengan, sin embargo, es un tema que no se puede dejar de lado y necesita mayor atención.

Actualmente no se han logrado reglas o normas internacionales que rijan el conflicto internacional en el ciberespacio pues los cambios tecnológicos y los nuevos desafíos que plantea el ciberespacio dificultan los acuerdos sobre una convención cibernética internacional, adoptando una preferencia por parte de los Estados por los acuerdos informales y la disuasión estratégica para limitar el conflicto directo. Muestra de ello es la relación de Estados Unidos y China que hasta el día de hoy se han visto enfrentados por disputas y desacuerdos y se han visto grandemente afectados por ataques cibernéticos. Es cierto que tanto China como Estados Unidos han realizado intentos de

cooperación como se evidenció en el tratado de no proliferación de 1985, sin embargo, al día de hoy su relación se muestra aún muy débil.

REFERENCIAS BIBLIOGRAFICAS

Abbott, K., & Snidal, D. (1998). Why states act through formal international organizations. Journal of conflict resolution, 42(1), 3-32.

Aguilar, L. (2011). Introducción. Estado del arte de la ciberseguridad. Cuadernos de estrategia, (149), 11-46.

Aguirre, D., & Morande, J. (2015). El ciberespacio y las Relaciones Internacionales en la era digital. Instituto de Estudios Internacionales. Universidad de Chile, Santiago, Chile.

Aust, A. (2008). The Theory and practice of informal international instruments. British Institute of International and Comparative Law. (35), 4, pp. 787-812.

Ayllon, B. (2007). La cooperación Internacional para el Desarrollo: fundamentos y justificación en la perspectiva de la Teoría de las Relaciones Internacionales, *Carta International*, 24-40.

BBC News. (2015). Cyber-suspicion strains US-China relations.

Benedicto, M. (2013). EE. UU ante el reto de los ciberataques. *Instituto Español de estudios estratégicos*, 37, 1-12.

Calduch, R. (1991*). Relaciones Internacionales*, Madrid: Ciencias Sociales.

Candau, J. (2010). Estrategias nacionales de ciberseguridad, Ciberterrorismo. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, Cuadernos de Estrategia, (149), 259-323.

Carlini, A. (2016). Ciberseguridad: Un nuevo desafío para la comunidad internacional. Instituto Español de Estudios Estratégicos, 67, 1-16.

Carr, M. (2011). The irony of the information age: US power and the internet in international relations.

Cari. (2013). Ciberdefensa-Ciberseguridad Riesgos y amenazas.

Caro, M. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. *Cuadernos de estrategia*, (149), 47-82.

Castells, M. (2014). El impacto de internet en la sociedad: una perspectiva global. C@mbio, 19.

Chang, A. (2014). China´s Cyberscurity Strategies. *Center for new American security*. 5-32.

China Daily. (2014). "US Cyber attacks against China (2009-present)". Infografía. Recuperado el 14 de enero, de URL http://www.chinadaily.com.cn/china/2014-05/29/content_17552029.htm

CNN. (2016). Obama presenta nuevas estrategias de seguridad cibernética en EE.UU.

David, M. (2017). Ciberseguridad en China. *Instituto Español de Estudios Estratégicos*, 1,1-7.

Don, B. (1999). Revolutionary Adaptations: Science and Technology in International Relations. *Harvard International Review*, 21(3), 42-46. Retrieved from http://www.jstor.org/stable/42762552

Donilon, T. (2013). Remarks by Tom Donilon, National Security Advisor to the President: "The United States and the Asia-Pacific in 2013". Recuperado el 27 de octubre de 2017 de https://obamawhitehouse.archives.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-states-an

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? International Political Science Review / Revue Internationale De Science Politique, 27(3), 221-244. Retrieved from http://www.jstor.org/stable/20445053

Erikson, J., & Giacomello, G. (2007). International Relations and Security in the Digital Age. London, New York: Taylor & Francis group.

Escuela Superior de Telecomunicaciones. (2013). Seguridad Nacional y Ciberseguridad. Aproximación conceptual: Ciberseguridad y Ciberguerra.

FireEye Isight Intelligence. (2016). Redline Drawn: China recalculates its use of cyber espionage. Recuperado el 23 de enero de 2018 de URL

https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-chinaespionage.pdf

Fischer, E. (2005). Creating a national framework for cybersecurity: An analysis of issues and options. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE

González, C. (2003). Las teorías de la cooperación internacional dentro de las relaciones internacionales. *Investigación y Análisis Sociopolítico y Psicosocial*, 2, (3), 115-147.

Hawkins, D. G., Lake, D. A., Nielson, D. L., & Tierney, M. J. (2006). Delegation under anarchy: states, international organizations and principal agent theory. Delegation and agency in international organizations, 3, 27-31.

Holsti, K. (1967). International Politics. A Framework for Analysis, Englewood Cliffs, pp. 494.

Jervis, R. (1985). From Balance to Concert: A Study of International Security Cooperation. *World Politics*, 38 (1), 58-79.

Jie, Yan. (25 de enero del 2010). China "biggest victim" of cyber attacks. *China Daily*.

Joyanes, L. (2015). Estado del arte de la ciberseguridad. *Pensamiento penal*, 13-46.

Kemmerer, R. (2003). Cybersecurity. In Software Engineering, 2003. Proceedings. 25th International Conference on (pp. 705-715). IEEE.

Kenneth, L. & Peter W. Singer (2012). Cybersecurity and U.S.-China Relations. Century defence initiative at booking, 21-3-54.

Keohane, R. (1984). After hegemony. Cooperation and discord in the world political economy. Princeton University Press, Princeton.

Koremenos, B. (2013). What's left out and why? Informal provisions in formal international law. Rev Int Organ, 8, 137-162.

Kshetri, N. (2014). Cybersecurity and International Relations: The US Engagement with China and Russia. In Proc. FLACO-ISA Joint Conf.

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingeniería de Software*, 3(4), 161-176.

Lindsay, J. (2015). The impact of China on cybersecurity: fiction and friction. *International security*, 39 (3), 7-47.

Lipson, C. (1984). International Cooperation in Economic and Security Affairs. Cambridge University Press 37, (1), 1-23.

Lipson, C. (1991). Why are Some International Agreements Informal? The MIT Press, (45), 4, pp. 495-538.

Louie, C. (2017). U.S.-China Cybersecurity Cooperation. *Jackson School of International Studies.* Recuperado el 20 de enero de 2018 de URL https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/

Medero, G. (2012). La ciberguerra: los casos de Stuxnet y Anonymous. *Nueva Época*, 11, 124-133.

Miguel, B. (2013). EE. UU ante el reto de los ciberataques. Instituto Español de Estudios Estratégicos, 37, 1-14.

Muller, H. (2002). Security cooperation. In: Carlsnaes W, Risse T, Simmons BA (Eds) Handbook of international relations. Sage, London, pp. 369–391

Mutschler, M. (2015). Security Cooperation in Space and International Relations Theory. In Handbook of Space Security (pp. 41-56). Springer New York.

Newmeyer, k. & Cubeiro, E. & Sánchez, M. (2015). Ciberespacio, Ciberseguridad y Ciberguerra.

Nye, J. (2010). Cyber power. HARVARD UNIV CAMBRIDGE MA BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS.

Obama, B. (2010). National Security Strategy of the United States (2010). DIANE Publishing.

Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). National Cyber Security Organisation: UNITED STATES.

Rabinad, G. (2008). La soberanía del Ciberespacio. *Lecciones y ensayos*, 85, 85-107.

Rauscher, K. & Yaschenko, V. (2011). Russia-US bilateral on cybersecurity: Critical terminology foundations. New York, USA: EastWest Institute.

Ripoll, A. (2007). La cooperación internacional: alternativa interestatal en el siglo XXI. *Revista de relaciones internacionales, estrategia y seguridad*, 2 (1).

Rollins, J. (2015). U.S.–China Cyber Agreement. Recuperado el 18 de enero de 2018 de URL https://www.hsdl.org/?view&did=788047

Sangbae, K. (2014). Cyber Security and middle power diplomacy: A Network Perspective. The Korean journal of international studies, 12, (2), 323-352.

Sangiovanni, M. (2017). Why the World Needs an International Cyberwar Convention. Crossmark, 1-29

Segal, A. (2013). The code not taken: China, the United States, and the future of cyber espionage. *Bulletin of the Atomic Scientists*, 69(5), 38-45.

Segal, A. (2016). The U.S.-China Cyber Espionage Deal One Year Later. Council on Foreign Relations. Recuperado el 24 de enero de 2018 de URL https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later

Servitja, X. (2013). Ciberseguridad, Contrainteligencia y operaciones encubiertas en el programa nuclear de Irán: de la neutralización selectiva de objetivos al "cuerpo ciber" iraní. *Instituto Español de estudios estratégicos*, 42, 1-24.

Shackelford, S., & Craig, A. (2014). Beyond the New'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity.

Shakarian, P. (2012). Stuxnet: Revolución de ciberguerra en los asuntos militares. *Air and Space Power Journal*. 50-59.

Shen, D. (2011). A Collaborative China-US Approach to Space Security. *Asian Perspective*, 35(4), 521-536.

Smith, A. & Rupp, W. (2002) "Issues in cybersecurity; understanding the potential risks associated with hackers/crackers", Information Management & Computer Security, Vol. 10 Issue: 4, pp.178-183

Torres, M. (2013). Ciberguerra. Manual de Estudios Estratégicos y Seguridad Internacional, 329-348.

Twomey, C (2009). Chinese-U.S. Strategic Affairs: Dangerous Dynamism. Arms Control Association, 39, (1), 17-20.

United States, White House Office, & Obama, B. (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. White House.

UNODC, (2013). Estudio exhaustivo sobre el delito cibernético. United Nations Office on drugs and crime, New York, 4-435

White House & United States of America. (2003). National Strategy to Secure Cyberspace.

Wortzel, L. La modernización militar y la ciberactividades de China.

Xiaokun, L. & Yingzi, T. (9 de mayo del 2012). Cyber attacks affect “both nations”. *China Daily.*

Xinbo, W. (2000). U.S. Security Policy in Asia: Implications for China—U.S. Relations. ISEAS - Yusof Ishak Institute, 22 (3), 479-497.

Xingan Li. (20015). Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. International Journal of Cyber Criminology, 9, 1-20.

Xinhua. (29 de marzo del 2012). China is victim of cyber attacks: spokesman. *China Daily.*