Universidad Siglo 21

Licenciatura en Relaciones Internacionales

Trabajo Final de Graduación

Las políticas en ciberseguridad de la
Organización del Tratado del Atlántico Norte (OTAN)
Período 2008-2013

Mauro Pessino

2017

Universidad Siglo 21
Trabajo Final de Graduación

Las políticas en ciberseguridad de la
Organización del Tratado del Atlántico Norte (OTAN)

Período 2008-2013

Autor: Mauro Pessino – Legajo Nº VRIN01745

Tutora: Prof. Florencia Rubiolo

Comisión Académica de Evaluación:
Profesoras Florencia Rubiolo y Claudia Guevara

ÍNDICE

Resumen Ejecutivo

El presente Trabajo Final de Graduación (TFG) indaga sobre las políticas en ciberseguridad desarrolladas por la OTAN entre 2008 y 2013 luego del ataque informático perpetrado contra Estonia en 2007. Este suceso puso en evidencia una nueva dimensión del concepto de seguridad que la OTAN había mantenido hasta ese momento en cierta manera relegado. Como consecuencia de estos acontecimientos, la OTAN colocó a la ciberseguridad en el foco de sus políticas de defensa que comenzaron a ser elaboradas en torno a una serie de instituciones y protocolos comunes basados en la cooperación/coordinación de tareas entre los Estados miembros. Por lo tanto, tomando como marco teórico al Institucionalismo Neoliberal y mediante un examen crítico de las políticas de la OTAN resultantes en el campo de la ciberseguridad, se analizará de qué manera la ciberseguridad pasó a formar parte de la agenda de la Organización; cómo fue readecuada la doctrina de la OTAN en función de esta nueva dimensión de la seguridad; las instituciones y agencias que se crearon en el seno de la OTAN tras el episodio en Estonia y el desarrollo de un marco legal aplicable al ciberespacio materializado en el Manual de Tallinn. Finalmente, desde este TFG se pretende generar reflexiones y conclusiones acerca de la construcción de las políticas cooperativas e institucionales dentro de la OTAN, como así también de los desafíos para enfrentar a un enemigo común e invisible como son las ciberamenazas.

Abstract

The present Final Graduation Work (FGW) investigates the cyber security policies developed by NATO between 2008 and 2013 after the computer attack perpetrated against Estonia in 2007. This event highlighted a new dimension of the concept of security that NATO had maintained until that moment in some way relegated. As a result of these developments, NATO placed cybersecurity at the center of its defense policies, which began to be developed around a series of common institutions and protocols based on cooperation / coordination of tasks between Member States. Taking as a theoretical framework the Neoliberal Institutionalism and through a critical examination of the resulting NATO policies in the field of cybersecurity will analyze how cybersecurity became part of the Organization's agenda; how the NATO doctrine was readjusted in terms of this new dimension of security; the institutions and agencies that were created within NATO after the episode in Estonia and the development of a legal framework applicable to cyberspace materialized in the Tallinn Manual. Finally, from this FGW is intended to generate reflections and conclusions about the construction of cooperative and institutionalized policies within NATO, as well as the challenges to face a common and invisible enemy such as cyber threats.

INTRODUCCIÓN

Los profundos avances de las tecnologías del conocimiento y de la información, potenciados por el fenómeno de la globalización en un mundo interconectado, han transformado nuestras realidades cotidianas. Prácticamente no hay actividad, cuyo paso o registro no sea canalizado por las redes, sean estas comerciales, educativas, financieras, estratégico-militares o de cualquier otro tipo. En otras palabras, las nuevas Tecnologías de la Información y el Conocimiento (TIC) han modificado sustancialmente las relaciones humanas y la globalización ha impactado en las bases del Estado y de la sociedad mundial a punto tal que ha nacido una dimensión paralela a la física: el ciberespacio (Reguera, 2015)

En este proceso, el desarrollo y crecimiento de Internet sumado a las TIC, han llevado a formar lo que se conoce como *Sociedad de la Información.* Esta evolución se expresa en la presencia que tienen estas tecnologías en todas las actividades cotidianas y la sustancial importancia que revisten para el funcionamiento de los Estados (Tikk, 2011).

En otras palabras, este mundo interconectado e interdependiente que en su momento postularon Keohane y Nye (1988), encuentra su máxima expresión en las actuales redes digitales y las TIC. Millones de dispositivos interconectados y el crecimiento exponencial de actores digitales además de la penetración de la red, indican que nuestro aparato económico-productivo está en gran medida digitalizado.

Las *smart factories* o fábricas inteligentes interconectadas mediante protocolos ciberfísicos que constituyen la base de la incipiente cuarta revolución industrial a la que estamos asistiendo; la producción y almacenamiento de grandes volúmenes de información en la *nube*; y los procesos de gestión y administración estatal en red, son solo algunos ejemplos de un mundo cada vez mas interconectado, dependiente del ciberespacio que amplía los beneficios del sistema, pero a su vez, incrementa las vulnerabilidades (Wegener, 2013).

Esto significa que las nuevas tecnologías han cambiado no solo la manera de comunicarnos y de informarnos, sino también las formas en que se están desarrollando las guerras en el siglo XXI. Hasta el surgimiento de Internet en 1969 y su posterior

expansión en la década del 90, las guerras estaban circunscriptas a los espacios físicos tradicionales, es decir, aéreo, marítimo y terrestre (Reguera, 2015).

Sin embargo, los "Juegos de Guerra" de tipo informático que años atrás parecían pertenecer a un mundo de ficción propio de Hollywood, hoy se han hecho realidad y forman parte de la estrategia de los Estados que asignan buena parte de sus presupuestos nacionales para crear estructuras especiales, formar recursos humanos y desarrollar tecnologías aplicadas al ámbito militar. Ello implica la aparición de un fenómeno relativamente reciente, subsidiario de estas nuevas tecnologías y que es la posibilidad de afectar las estructuras integrales y en particular las estructuras críticas de un Estado como resultado de un ciberataque (Areng, 2014).

En este sentido, con el afianzamiento de la tecnología, el ciberespacio se presenta como un nuevo campo de batalla, que permite la utilización hostil de estas tecnologías con características particulares, como son la intangibilidad, la masividad y la auto-replicación, pero que a su vez pueden llegar a ocasionar daños concretos, físicos y económicos (Río Durán, 2011).

En los últimos 25 años la informática ha tenido una importante evolución, dejando de ser una simple herramienta administrativa de oficina para transformarse en un instrumento estratégico de los Estados, las sociedades modernas y de organizaciones internacionales como la OTAN (Theiler, 2011).

En este contexto, entre los meses de abril y mayo de 2007, Estonia uno de los países más digitalizado e interconectado del mundo y miembro de la OTAN, sufrió un masivo ciberataque que paralizó los sitios web y los sistemas informáticos del país dejándolo al borde la inoperancia. Este acontecimiento inusitado e inesperado obligó a Estonia a requerir apoyo externo de la OTAN y países de la Unión Europea durante varios días para contener el ataque y minimizar los daños (Lejarza Illaro, 2014).

Como resultado, los incidentes en Estonia significaron un llamado de atención para la OTAN en un área que hasta ese momento había sido descuidada, y condujo a la incorporación de la ciberseguridad en la agenda de la OTAN. De este modo, las políticas tradicionales de seguridad debieron ser actualizadas y modificadas, creando al mismo tiempo instituciones y elaborando protocolos específicos que incluyen el trabajo

de expertos provenientes tanto del sector público como del privado con el objeto de adaptarse y posicionarse frente a la emergencia de un nuevo tipo de amenaza a la seguridad (Caro Bejarano, 2012).

El ataque informático a Estonia, de alguna manera sorprendió a propios y a extraños evidenciando una singularidad desconocida en el contexto actual. Son varios los aspectos destacables de esta nueva forma de amenaza, entre los que sobresalen la posibilidad de generar daño físico a partir de armas inmateriales, la simultaneidad, la masividad, la inmediatez y el anonimato. Estas circunstancias obligaron a los Estados de la OTAN a cooperar y a tomar medidas dentro de las estructuras institucionales frente a una situación hasta ese momento ignorada e imposible de contener individualmente.

Por lo tanto, se abre la posibilidad de formular la siguiente pregunta de investigación: ¿Qué tipo de políticas en ciberseguridad comenzó a desarrollar la OTAN tras el ataque informático? En consecuencia, el presente Trabajo Final de Graduación (TFG) tiene como objetivo analizar las políticas de ciberdefensa de la Organización del Tratado del Atlántico Norte (OTAN) desarrolladas entre los años 2008 y 2013 desde una perspectiva teórica más cercana a los enfoques liberales e institucionales. Esta tarea implica indagar el proceso institucional, que incluye la creación de agencias, protocolos e instituciones, y las políticas de ciberdefensa desarrolladas por la OTAN entre los años 2008 y 2013, considerando que hasta el momento de llevarse a cabo el ataque, la OTAN había subestimado la importancia estratégica que tenía el ciberespacio y sus capacidades de respuesta eran prácticamente nulas (Theiler, 2011).

Asimismo, la selección del período 2008-2013 para el TFG está relacionada con la intensa actividad desarrollada por la OTAN en el ámbito de la ciberseguridad, que abarca lo inmediato posterior al ataque y la edición del Manual de Tallinn en 2013. De acuerdo a las indagaciones previas realizadas en el marco del TFG, es en este lapso de tiempo donde fueron creadas las bases fundamentales y definidas las directrices generales de las políticas en ciberseguridad de la OTAN.

Por lo tanto, se considera que el estudio de las políticas de ciberseguridad desarrolladas por la OTAN en el citado período constituye un problema de investigación orientado a realizar un aporte en una de las áreas que se enmarca en los avances de la ciencia y la

tecnología, las cuales se estructuran y organizan en respuesta a un evento hasta ese momento desconocido en el marco de un contexto tan dinámico y con continuas transformaciones como es la disciplina de las Relaciones Internacionales.

Por una parte, esta investigación puede ayudar a explicar y comprender en qué consisten estas nuevas formas de amenaza, como se utilizan y de qué manera los Estados miembros de la organización articularon sus respuestas y sus políticas de defensa, fundamentalmente desde lo institucional, lo técnico y lo legal. Por la otra, específicamente indagará en el ámbito de la OTAN que tipos de políticas se llevaron a cabo, que instituciones se crearon y cuales son sus funciones, cuál es la doctrina de la OTAN en ciberseguridad, que vínculos se establecieron con el ámbito privado y que iniciativas se están realizando en materia legal desde el derecho internacional.

Existen numerosas investigaciones previas que en el área de la ciberguerra y de las políticas de ciberseguridad desarrolladas desde la OTAN dan cuenta de una considerable cantidad de trabajos académicos abordados desde distintos centros de estudio y autores.

En tal sentido se destacan los trabajos desarrollados por el Instituto Español de Estudios Estratégicos dependiente del Ministerio de Defensa de España con sus Cuadernillos de Estrategia, El Real Instituto Elcano, los Research Papers de la OTAN, el Military Education Research Library Network, el Grupo de Estudios en Seguridad Internacional, la Corporación RAND, el Centro Común de la Investigación de UE, el Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN, el Atlantic Council de los Estados Unidos, el Wilson Center, el Center for Strategic & International Studies como también, desde el ámbito privado, las Compañías de Seguridad Informática Kaspersky, Panda y Arbor Networks.
Asimismo, un importante número de investigadores han elaborado trabajos e indagaciones profundas relacionadas con la temática, entre los que se incluyen a especialistas militares e informáticos y a expertos en derecho internacional.

Sin llegar a ser exhaustivos, se puede mencionar a Ferrero (2013) que trata y estudia la evolución de los ataques informáticos, las distintas tecnologías desarrolladas como también los tipos y descripción de las ciberarmas más utilizadas. Asimismo, realiza un enfoque de la situación del ciberespacio en el ámbito militar y las políticas de ciberseguridad implementadas por la OTAN luego del ataque a Estonia, que incluyen la

creación de equipos especiales, centros de investigación en ciberdefensa, hojas de ruta para lograr capacidad de respuestas, entre otros.

Por su parte, Artiles (2011) aborda los peligros que amenazan a la seguridad de las sociedades actuales debido a su dependencia de las tecnologías de la información. Estudia y analiza detalladamente, por un lado, los dos ciberataques de mayor repercusión: contra Estonia en 2007 y Georgia en 2008, y por el otro, la situación de ciberseguridad en la OTAN y el proceso de transformación de la OTAN en esa área.

Acosta, Pérez Rodríguez, Arnaíz de la Torre, y Taboso Ballesteros (2009) examinan de forma integral las estrategias y actividades de ciberdefensa e iniciativas de ciberejércitos desarrolladas por un importante número de países (Estados Unidos, Rusia, China, Noruega, Irán, Francia, Alemania, Reino Unido, Unión Europea, España, Pakistán). Incluye los planes, la legislación y la organización de actividades e instituciones en el ámbito de la OTAN, como así también las infraestructuras y los esfuerzos específicos en ciberdefensa.

Healey y Van Bochoven (2011) abordan en forma integral el desarrollo y evolución de las capacidades cibernéticas de la OTAN y al mismo tiempo realizan recomendaciones de cara al futuro. Para una mejor comprensión, su análisis se divide en seis bloques: el número uno toma como punto de partida las capacidades de la OTAN en 1999 durante la guerra de Kosovo; el dos los acontecimientos de Estonia en 2007; el tres las ciber operaciones concretadas en Libia en 2011; el cuatro la estructura institucional de la OTAN en el área de la ciberseguridad y su gobernanza ; el cinco y seis las materias pendientes.

Joubert (2012) recorre los cinco años posteriores al ataque sufrido por Estonia, realizando un análisis crítico de la evolución de las políticas de la OTAN respecto a la ciberseguridad como así también de los desafíos pendientes. Por otra parte, aborda la problemática del art. 5to. de la organización en cuanto a la consideración de que si un ciberataque puede activar los mecanismos de defensa colectiva. Finalmente, evalúa los logros alcanzados y los peligros e incertidumbres remanentes.

Lewis (2013) construye su publicación tomando como base lo que considera una cuestión central en la doctrina cibernética de la OTAN. Esta cuestión es cómo la

ausencia de un articulado más robusto de los recursos cibernéticos ofensivos de la OTAN puede afectar sus capacidades para disuadir o defender. Desde el texto se realiza un análisis crítico de las políticas cibernéticas de la OTAN, destacando la necesidad de no limitarse a una posición defensiva y reactiva sino que se cree conveniente adoptar posturas ofensivas y con mayor protagonismo. Asimismo, realiza una serie de aportes y propuestas en cuanto a lo que considera cuáles deberían ser las medidas a adoptar que permitan dotar a la OTAN de mayores recursos acordes con este cambio en la doctrina.

Reguera (2015) elabora un recorrido que va desde los inicios de Internet hasta su expansión actual, analizando las implicaciones que tiene para la sociedad actual y como las nuevas tecnologías han revolucionado la manera de relacionarse del hombre. Por otra parte plantea las consecuencias del vacio legal existente en el ciberespacio y las estrategias desarrolladas por la OTAN para enfrentarlo desde el derecho internacional.

Lejarza Illaro (2014) realiza un profundo análisis acerca de cómo a partir de la expansión de Internet, el ciberespacio se fue transformando de un medio para intercambiar información a un escenario de conflicto con importantes consecuencias en la políticas de los estados, destacando los contextos de ciberconflictos; la evolución de las amenazas informáticas; los aspectos de la Guerra de Información Estratégica y el perfil de las ciberarmas y modos de empleo.

Wegener (2013) argumenta que el uso de las nuevas tecnologías con fines beligerantes u ofensivos deberían ser deslegitimados, donde todos los actores interesados actúen en la conformación de estrategias comunes para evitar y reducir los daños. El autor hace una pormenorizada indagación respecto a los parámetros estándar de seguridad en la nube; la cooperación internacional sobre respuestas en las emergencias; las respuestas institucionales y legales de la OTAN vinculadas a la ciberguerra; el incremento de los esfuerzos para armonizar leyes internacionales en materia cibernética y la necesidad de crear una cultura de ciberseguridad en base a los conceptos de ciberestabilidad y ciberpaz.

Veenendaal, Kaska y Brangetto (2016) estudian la adaptación de la doctrina de la OTAN al ciberespacio indicando que la OTAN debe colocarse en posición para defender la libertad y la seguridad de los Estados miembros de las amenazas derivadas del ciberespacio. Asimismo señalan la necesidad de reconocer al ciberespacio como un

dominio para operaciones militares, así como la de desarrollar y profundizar doctrinas, procedimientos y un marco legal que permitan el despliegue de las capacidades cibernéticas durante las misiones de la OTAN.

En síntesis, se puede destacar que la literatura disponible, principalmente bajo el formato de papers y publicaciones especializadas, es amplia y heterogénea respecto al enfoque de la temática, ya que mientras algunas se dirigen al estudio de estas nuevas formas de amenaza en cuanto a que implicancias tienen desde lo político y la seguridad en el ámbito de la OTAN, otras lo abordan desde lo técnico, económico o legal.

Finalmente, a partir de las lecturas efectuadas hasta el momento, es posible señalar que la ciberguerra ha comenzado a ocupar un lugar central en las políticas de seguridad de la OTAN, que los gobiernos destinan cada vez mayor cantidad de recursos humanos y económicos hacia estas áreas y que las tareas requieren de trabajos cooperativos y colaborativos tanto desde el nivel público como del privado.

Para tal efecto, el TFG se llevará a cabo bajo las directrices de un objetivo general que a su vez será complementado por objetivos específicos. Estos objetivos se detallan a continuación como así también algunos de los documentos y recursos académicos que serán utilizados como bases para la investigación.

• *Objetivo General:* Analizar las políticas en ciberseguridad desarrolladas por la OTAN a nivel mundial en el período 2008-2013 desde una perspectiva teórica más cercana a los enfoques liberales e institucionales.

• *Objetivos Específicos:*

a) Describir el contexto histórico y las características del ataque informático a Estonia en 2007.

b) Indicar y señalar las políticas, las agencias e instituciones desarrolladas por la OTAN en el área de la ciberseguridad en el período 2008-2013.

c) Analizar y examinar, tanto desde lo técnico como desde su modo de empleo, las nuevas formas de amenaza cibernéticas, sus objetivos, qué impacto tienen en la OTAN y la readecuación de la Organización ante este nuevo escenario.

d) Estudiar los avances en el derecho internacional aplicable a la ciberguerra promovidos desde la OTAN en el período 2008-2013.

Para los fines del objetivo (a) se recurrirá a investigaciones de diversos autores especializados en ciberseguridad y centros de estudios internacionales, como el Real Instituto Elcano y los Cuadernillos de Defensa del Ministerio de Defensa de España. También se utilizarán trabajos publicados por el Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN, la revista NATO Review y los Research Papers de la OTAN.

En cuanto a los objetivos (b), (c) y (d) se tomarán como base de la investigación y se analizarán los documentos publicados por el Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN; los informes del Roma Defense College de la OTAN; los reportes de las Asambleas Parlamentarias de la OTAN; las declaraciones y acuerdos firmados en el marco de la Cumbres de la OTAN (Praga 2002, Bucarest 2008, Lisboa 2010, Chicago 2012); las declaraciones conjuntas de los Ministros de Defensa de los Estados miembros; el Tratado de Washington constitutivo de la OTAN y el Manual de Tallinn para el derecho aplicable a la ciberguerra.

Marco Teórico

El presente Proyecto del Trabajo Final de Graduación tendrá como marco teórico de referencia el Institucionalismo Neoliberal desarrollado desde la perspectiva de Robert Keohane (1985, 1988, 1993, 1995), Robert Nye (1987, 1988, 2012), y Robert Axelrod (1985). Además, se emplearán aportes contemporáneos desde la visión de Helen Milner (2009), Andrew Moravcsik (2009), Lisa Martin (1998, 1995), Beth Simmons (1998), Michael Gilligan (2009), Randall Stone (2009), Elizabeth DeSombre (2009), Ronald Mitchell (2009), Jonathan Aronson (2009) y Vinod Aggarwal (2009).

A modo de introducción, se puede señalar que esta línea teórica, por un lado, coincide con el realismo en la naturaleza anárquica del sistema internacional y la importancia del poder y la seguridad en las conductas estatales, pero por el otro, señala el rol que

cumplen las instituciones en las políticas estatales, y en la capacidad de coordinación y cooperación de los Estados para enfrentar, desde las instituciones, problemas comunes que los afectan y que no podrían resolver en forma aislada (Keohane,1993).

Para Keohane (1993) la política internacional esta institucionalizada, es decir existen una serie de normas, reglas y convenciones aportadas por las instituciones, definiendo a estas como "conjuntos de reglas (formales e informales) persistentes y conectadas, que prescriben papeles de conducta, restringen la actividad y configuran las expectativas" (Keohane, 1993: 17). De este modo, los flujos de información, la credibilidad entre los actores del sistema, el control recíproco entre los actores para cumplir lo pactado y las expectativas mutuas se ven reforzadas y configuradas conjuntamente.

De acuerdo a esta teoría, existen tres tipos de instituciones internacionales: a) organizaciones internacionales gubernamentales o no gubernamentales, estas poseen una burocracia permanente, reglas explícitas y funciones específicas.; b) regímenes internacionales que de acuerdo a Stephen Krasner son “un conjunto de principios, reglas, normas y procedimientos de toma de decisiones implícitos o explícitos alrededor de los cuales convergen las expectativas de un determinado campo de actividad” (Krasner, 1982); y c) convenciones, estas son ontológicamente preexistentes a las dos anteriores y son definidas como instituciones informales con reglas implícitas que configuran las expectativas de los actores.

Según Keohane (1993) se deben dar dos condiciones para el funcionamiento del Institucionalismo Neoliberal: los agentes deben tener intereses mutuos y que a mayor grado de institucionalización de las áreas problemáticas, mayor es la influencia que las instituciones ejercen en el comportamiento de los agentes. En consecuencia, para que los Estados cooperen entre si, deben tener intereses mutuos y pensar en ganancias absolutas lo que en términos de Deutsch sería una Comunidad Política, aunque con un importante grado de institucionalización (Bartolomé, 2013).

La distinción entre ganancias absolutas y relativas marca una frontera entre los postulados teóricos realistas e institucionalistas neoliberales y es un concepto clave para comprender las conductas estatales desde la perspectiva de Keohane.

En este sentido, según el realismo en un sistema estatal anárquico y de autoayuda, las ganancias relativas son las que realmente importan. De acuerdo a Gilpin (2001), en los sistemas internacionales las ganancias raramente se distribuyen en forma equitativa, por lo tanto los Estados tienen un fuerte incentivo para orientar sus acciones con el objetivo de salvaguardar sus propios valores e intereses, en particular su bienestar económico, poder y libertad de acción. Además, según Gilpin (2001), en el sistema internacional la idea realista de las ganancias relativas implica un juego de suma cero en donde la ganancia de una parte necesariamente determina la pérdida de la otra parte. De ahí que, según el realismo, el hecho de que los Estados estén más preocupados en sus ganancias relativas que en las ganancias absolutas dificulta la cooperación en el sistema internacional (Grieco, 1990).

Sin embargo, para Keohane (1993), las relaciones internacionales distan mucho de este juego de suma cero, ya que existen situaciones donde pueden lograrse beneficios mutuos mediante la cooperación, reglas y expectativas prevalecientes. En palabras de Keohane (1993) "(…) de forma coherente con el liberalismo, me niego a asumir, ya definiciones inmutables del interés en términos de ganancias relativas, ya modelos de conflicto entre los Estados. Para mí, la política es abierta y potencialmente progresiva, más que desoladamente cíclica." (Keohane, p. 28)

En estudios posteriores Keohane y Martin (2003), continuaron analizando esta cuestión señalando que se deben tener en cuenta dos aspectos significativos: 1) las condiciones bajo las cuales las ganancias relativas son importantes y 2) el rol de las instituciones cuando las ganancias relativas están en juego. Asimismo los autores destacan que la lección mayor que dejó el debate en este asunto es que la importancia de las ganancias relativas está condicionada por factores tales como el número de grandes actores del sistema internacional y si son favorecidas las ventajas militares ofensivas o defensivas.

Keohane y Martin (2003) afirman que cuando están en juego la distribución de ganancias el rol de las instituciones es de central importancia, debido a que uno de los mayores obstáculos que se le presentan a los Estados es la posibilidad de que otros Estados actúen en forma desleal y engañosa y que los resultados de la cooperación no tengan las implicaciones distributivas esperadas. En consecuencia, las instituciones se convierten en canales y mecanismos de coordinación, que permiten la construcción de

puntos focales sobre aspectos cooperativos prominentes para los Estados, y los cuales están basados en la reciprocidad y el intercambio de información.

Por consiguiente, tomando como punto de partida y profundizando desde este *corpus conceptual* serán analizadas las políticas en ciberseguridad desarrolladas por la OTAN en el período 2008-2013. En primer lugar, de acuerdo al Institucionalismo Neoliberal, los *intereses mutuos* de los Estados en un determinado asunto pueden favorecer la cooperación, entendiendo que la cooperación ocurre cuando los actores ajustan mutuamente sus conductas a las expectativas actuales o futuras de otros actores mediante la coordinación de políticas (Keohane, 1993). Este aspecto será considerado una pieza central en el presente estudio para analizar cómo a partir intereses mutuos en ciberseguridad, los Estados miembros desplegaron una serie de políticas cooperativas y coordinadas en el ámbito de la OTAN. En otras palabras, a mayores intereses mutuos en el área de la ciberseguridad, mayores serán los incentivos, las instituciones y las políticas cooperativas adoptadas por los Estados miembros como mecanismos promotores de la cooperación en la búsqueda de soluciones pensadas en términos de ganancias absolutas.

Sobre esta base, para el estudio del caso es importante distinguir entre *cooperación* y *armonía de intereses*. Para Axelrod y Kehoane (1985) "(...) cooperación no equivale a armonía. La armonía exige una total identidad de intereses, pero la cooperación solo puede tener lugar en situaciones en las que hay una mezcla de intereses conflictivos y complementarios (…)" (Axelrod y Keohane, p. 226). A primera vista, los Estados miembros de la OTAN, distan mucho de tener una total identidad de intereses. La heterogeneidad de sus miembros, si consideramos por ejemplo, a Turquía, Alemania o Estados Unidos, difícilmente puedan conducir a una situación de ese tipo. Sin embargo, una situación conflictiva y de intereses complementarios, como es la ciberseguridad, impulsarían las prácticas cooperativas entre los Estados miembros de la OTAN.

A su vez, el incremento de la cooperación posibilitaría un juego de suma variable entre los Estados de la OTAN, facilitando una mejor distribución de los resultados, traducidos en ganancias absolutas donde todos ganan a partir de la mutua adecuación. Como señalan Keohane y Martin (2003) la distribución de ganancias implican un rol activo por parte de las instituciones para lograr una eficiente gestión. En este sentido la OTAN evitaría la actuación desleal de los Estados miembros en el ámbito de la ciberseguridad

favoreciendo la reciprocidad y fundamentalmente el intercambio de información mediante dispositivos de coordinación.

Es aquí donde los *costos de transacción* emergen como factores esenciales para la consecución de objetivos comunes. El concepto de los costos de transacción es central en el esquema teórico de Keohane y básicamente se entiende en función al intercambio de información. Si se tiene en cuenta la enorme dinámica de los asuntos internacionales, los avances en el área de ciberseguridad de la OTAN requieren necesariamente del intercambio de información, siendo éste un aspecto a tener en cuenta si la OTAN pretende alcanzar los objetivos planteados con éxito.

Según Keohane (1984) para que los Estados cooperen deben tener certeza de que partes están interesadas en el asunto, que tipos de acuerdos son posibles y que comportamiento se espera de cada parte. Si estas cuestiones son negociadas desde cero constantemente imponen altos costos de transacción y riesgos, por lo tanto en la política mundial la información es muy costosa y frecuentemente se presenta desigual para los diversos actores.

Los costos de transacción, que incluyen costos de organización y pagos colaterales pueden llegar a ser muy altos, de modo que las instituciones internacionales permiten generar una información de alta calidad centralizada, reducir la incertidumbre sobre el comportamiento de las partes, establecer foros para la toma de decisiones, establecer vínculos constantes y asignar roles y mecanismos para la resolución de disputas reduciendo los costos y los riesgos de la cooperación (Gilligan, 2009). Considerando esta cuestión, la OTAN presenta una ventaja importante, debido a que las políticas en ciberseguridad se presentan en un entorno institucional ya establecido y donde los costos de transacción están asumidos. Esta situación implicaría una rápida respuesta de la OTAN a la hora de concretar y poner en marcha las políticas en ciberseguridad.

Es decir, los objetivos comunes en ciberseguridad de los Estados de la OTAN y las políticas desplegadas para alcanzarlos, serán negociados y realizados con mucha más eficiencia dentro de un *régimen institucionalizado* permitiendo el intercambio y una equilibrada distribución de la información.

Al respecto, si bien la idea de régimen se encuentra asociada al neoinstitucionalismo, se debe destacar que algunos de sus conceptos también se ajustan a la teoría realista. Los regímenes no deben entenderse como una superación del Estado-nación westfaliano, sino que deben percibirse como acuerdos promovidos desde el auto-interés dentro de un sistema donde la soberanía continúa siendo un elemento constitutivo. Los regímenes no dictan lo que deben hacer los Estados sino que ayudan a que los Estados logren alcanzar sus propios intereses mediante la cooperación (Keohane, 1993). Además, el autointerés egoísta puede conducir a la creación de regímenes en seguridad del mismo modo que en los asuntos económicos. Sin embargo, es preciso subrayar que en asuntos de seguridad, comprobar las intenciones de los actores se hace más dificultosa y se encuentra limitada por la ideología y la competición. Por lo tanto, los regímenes de seguridad exitosos deben involucrar advertencias oportunas para que los Estados no se vean afectados en su vulnerabilidad en caso de defección, pero eso no significa que los regímenes estén limitados únicamente a los asuntos económicos (Nye, 1987).

En este punto se considera necesario destacar que es llamativo el hecho de que el debate neorrealismo-neoliberalismo se haya enfocado en el área de la cooperación y que prácticamente haya dejado íntegra la de los estudios sobre el conflicto (Salomón, 2002). Según Salomón, "(…) en la práctica, empero, los estudios de seguridad siguen estando prácticamente monopolizados por el neorrealismo. (Salomón, 2002, p. 17). Como afirma Keohane (1993):

> El institucionalismo neoliberal también insiste en la significación de los regímenes internacionales y la importancia de la constante exploración de las condiciones bajo las cuales emergen y persisten. Juzgando por la bibliografía de los periódicos de las relaciones internacionales, esta batalla se ha ganado en el área de la economía política: los estudios sobre regímenes económicos internacionales han proliferado. (…) Pero debemos llevar mas adelante la investigación de los regímenes internacionales, hasta el área de la seguridad, como un conjunto de autores ha empezado a hacerlo (Keohane, 1993, p. 32).

El fin de la Guerra Fría acompañado por el proceso de globalización transformó el escenario internacional forzando a analistas y académicos a reformular las bases

teóricas de la disciplina. La seguridad no escapó a este proceso. Como muy bien lo identifica Tulchin:

> Uno de los rasgos más preocupantes de la comunidad global de la post Guerra Fría ha sido la confusión que existe en torno a las discusiones sobre seguridad, o sea, la definición de los límites e interconexiones entre seguridad nacional y seguridad internacional. La propia definición del concepto de seguridad es poco clara. Existe una confusión generalizada sobre algunos de los aspectos más fundamentales, tales como: ¿qué constituye una amenaza externa? ¿Cuál es el rol de las fuerzas armadas? ¿En qué circunstancias la seguridad debería ser un tema que concierne a las agencias multilaterales? Y ¿cuál es la respuesta apropiada que se le debe dar a las amenazas que provienen de actores no estatales? (Tulchin, 2006, p. 97).

El mundo post Guerra Fría y más tarde el 11-S sumaron varias dimensiones al concepto de seguridad, modificando asimismo el objeto referente de la seguridad frente al surgimiento de nuevas amenazas, entre las que se destacan el terrorismo, contaminación ambiental, narcotráfico y más recientemente las que provienen del ciberespacio, dejando de manifiesto la vulnerabilidad de los Estados miembros de la OTAN, incluso los más poderosos, y la necesidad de enfrentar estas amenazas dentro de un marco colaborativo y coordinado dentro de estructuras institucionales.

De esta manera, el concepto de seguridad se fue transformando y evolucionando de la mano, y como resultado, de las revoluciones técnico, científicas, comunicacionales e informáticas que están profundamente entrelazadas con las dinámicas de la interdependencia y globalización y de este modo han modificado los retos y amenazas a los que los Estados deben enfrentar como las percepciones que tienen de los mismos (Del Arenal; 2002).

A causa de ello, se considera pertinente hacer mención al aporte de Buzan y sus niveles de seguridad, que si bien provienen desde otra corriente teórica, corrobora la existencia de cierto consenso académico acerca de las nuevas dimensiones de seguridad propuestas por el autor, y confirma la tendencia analítica en cuanto a la resignificación del concepto de seguridad.

En este sentido, Buzan define a la seguridad como la capacidad que tienen Estados y sociedades de librarse de amenazas y de mantener su identidad e integridad funcional frente a fuerzas de cambio consideradas hostiles. Asimismo, señala la existencia de cinco niveles de seguridad: estatal, política, económica, social y medioambiental (Buzan, 1991).

Ahora bien, las políticas en ciberseguridad ejecutadas en forma multilateral desde la OTAN, remiten a reflexionar y estudiar sobre la conformación de este nuevo plano y sector de seguridad como es el ciberespacio; que las herramientas desarrolladas para afrontar este tipo de amenazas deben ser pensadas desde el multilateralismo y que las voluntades e intenciones de los actores estatales requieren de entramados institucionales generando un marco genuino para el diseño de nuevos modelos de seguridad.

En otras palabras, las nuevas dinámicas de la agenda internacional exigen posturas flexibles ante problemas que tienen una asombrosa capacidad de transformación, mutación y propagación. Es así que esta situación forzosamente conduce a revisar los modelos de seguridad y el diseño de políticas públicas acordes a las nuevas circunstancias donde los Estados difícilmente puedan encontrarlas desde posiciones aislacionistas y del tradicional poder militar (Nye, 2012).

En efecto, el surgimiento de nuevos modelos de seguridad, más cercanos a los entornos contemporáneos, entre los que se destaca el *complejo interdependiente o relacional* promovido desde el Institucionalismo Neoliberal están asociados a estas nuevas formas de amenaza. Este modelo incluye un conjunto de normas, protocolos y condiciones de relación estables, los cuales diseñan una agenda, que posibilitaría a los Estados miembros de la OTAN atemperar los dilemas de la ciberseguridad en el marco de un sistema cooperativo. De esta manera se hace hincapié en las vinculaciones de interdependencia e intereses comunes como garantía de la seguridad (Orozco, 2006).

En consecuencia, la políticas en ciberseguridad de la OTAN desarrolladas dentro de un régimen institucionalizado, estarían motivadas a partir de intereses mutuos que al mismo tiempo descansan en el auto-interés de los Estados miembros en su seguridad. Asimismo, este auto-interés se modifica y cambia a partir del *aprendizaje*. El aprendizaje sucede cuando nuevo conocimiento es utilizado para redefinir los intereses nacionales. La interpretación y recepción de nueva información afecta las convicciones

y prioridades Estatales. A nivel sistémico la nueva información y su aprendizaje se presentan en términos de complejidad, impulsando a los Estados a la creación de regímenes para un mejor manejo de la misma (Nye, 1987).

De esta manera, los ciberataques se pueden interpretar como nueva información cuyo aprendizaje condujo a los Estados miembros de la OTAN a una redefinición de sus intereses en términos de seguridad, y al desarrollo de una serie de políticas institucionalizadas para llevarlos a cabo en el marco de la complejidad del sistema internacional, siendo éste un aspecto a considerar en el caso de estudio.

En efecto, Milner (2009) citando como ejemplo el fenómeno de la *Globalización,* señala que el sistema internacional es complejo y se encuentra interconectado tal como Keohane y Nye previeron desde su concepto de *Poder e Interdependencia* años atrás. Asimismo, tendencias mundiales tales como la creciente importancia de los actores no estatales que incluye corporaciones multinacionales, organizaciones no gubernamentales e instituciones internacionales, han evidenciado la complejidad del sistema.

Las políticas en ciberseguridad desarrolladas por la OTAN permiten la posibilidad de analizarlas dentro de este contexto y revelan la emergencia de actores no estatales y transnacionales que contribuyen a generar espacios de acción autónomos que escapan al control de los Estados. Como señala Nye (2012), la dependencia de los sistemas cibernéticos para las actividades militares y económicas crea nuevas vulnerabilidades que pueden ser explotadas por actores no estatales, con un costo económico bajo, distancia física inmaterial y donde los Estados tienen capacidades limitadas para desarmar al atacante, ya que no pueden ocupar territorio o usar estrategias de contrafuerza de manera efectiva

Para Milner (2009), el paso del tiempo ha reforzado el concepto de interdependencia compleja que involucra algo más que solo interdependencia económica y presenta al menos tres características: 1) la relaciones transnacionales son importantes e incluyen múltiples canales que conectan sociedades de los diferentes países a través de lazos formales e informales; 2) la agenda mundial de los Estados incluyen múltiples asuntos y, 3) la fuerza militar no es el principal medio para resolver desacuerdos entre los Estados.

Si se toman en consideración estas tres características enunciadas *supra* los ciberataques se adecuan a cada una de ellas, confirmando la complejidad del asunto y la preocupación de la OTAN en resolverlo. Es decir, 1) las relaciones transnacionales son un hecho constante, potenciadas por las nuevas tecnologías de comunicación e información que involucran a actores no estatales con capacidad para llevar a cabo un ciberataque; 2) los ciberataques pasaron a formar parte de la agenda de la OTAN, y 3) *prima facie* en la OTAN la fuerza militar no se presenta como un recurso viable para enfrentar los ciberataques.

Por lo tanto siguiendo a Milner (2009), se puede afirmar que existen cuatro elementos claves que deben someterse a análisis y discutir en el desarrollo de las políticas de ciberseguridad de la OTAN. Estos conceptos centrales son: el énfasis en los actores no estatales, incluidas las organizaciones internacionales; el poder más allá de la fuerza militar; el rol de interdependencia sumada a la anarquía del sistema internacional y la importancia de la cooperación como así también el conflicto en la política mundial.

En un contexto de interdependencia Moravcsik (2009) indica que la variación en la naturaleza y distribución de la información es una variable sistémica en la política mundial y ayuda a explicar la capacidad de los Estados para superar los problemas colectivos. Como se viene afirmando, los regímenes institucionalizados pueden ayudar a una mejor distribución de la información evitando las asimetrías. La información en ciberseguridad es central, ya que por naturaleza la información es un elemento constitutivo del ciberespacio donde convergen múltiples actores, estatales y no estatales. De ello se prevé que los esfuerzos de la OTAN se encaminen al desarrollo de mecanismos de coordinación que permitan el simétrico intercambio de información e involucren la necesaria participación del sector privado por su posición de vanguardia y conocimientos en investigación y desarrollo (I&D) tecnológico.

Sin embargo, el intercambio de información que involucre al sector privado puede afectar un área tan compleja como el derecho a la propiedad intelectual. De acuerdo a Aronson (2009) los derechos de propiedad intelectual comprenden un juego estratégico entre Estados y sus empresas transnacionales, quienes defienden y buscan prolongar su posición de privilegio respecto a los Estados en desarrollo y nuevas empresas que desean tener acceso a tecnología e ideas ya desarrolladas. En un contexto de

globalización, interdependencia y desarrollo tecnológico, los derechos de propiedad intelectual necesariamente deben gestionarse, de manera que ayuden a cerrar la brecha digital entre Estados desarrollados y en desarrollo sin afectar la seguridad de los primeros.

En el entorno OTAN, a través de la cooperación activa y la creación de regímenes de gobernanza, sería posible asegurar un justo equilibrio entre el cobro de derechos, incentivos para investigación y el acceso a nuevas tecnologías que refuercen la ciberseguridad de los Estados miembros más atrasados. Se deduce que en el análisis de las políticas en ciberseguridad de la OTAN esta cuestión se presentará al momento de su diseño. No obstante, más allá de las problemáticas derivadas de conflictos por la propiedad intelectual, en mayor o menor medida el cambio tecnológico transformó a toda la sociedad mundial. De hecho, la globalización incrementó la magnitud de la violencia informal beneficiada por la rapidez de las comunicaciones y su bajo costo, donde actores no estatales ayudados por la tecnología pueden ejecutar actos de violencia informal con consecuencias a gran escala (Tickner, 2009).

La estrategia de la OTAN para enfrentar a las ciberamenazas basada en la cooperación internacional, el intercambio de información en distintos niveles y participación de distintos actores/canales revela la actualidad de los postulados del Institucionalismo Neoliberal.

Sin embargo, si bien la colaboración es posible y deseable, se deben sortear diversos obstáculos al momento de llevar adelante el proceso. La construcción de instituciones internacionales es un asunto arduo y trabajoso donde los intereses comunes no son simples de identificar y mantener. Por lo tanto, alcanzar la cooperación a nivel internacional es una tarea difícil (Axelrod y Keohane, 1985).

De acuerdo a Keohane (1993), existen tres fuentes de dificultades particularmente importantes para la cooperación internacional: información asimétrica, riesgo moral e irresponsabilidad. En primer lugar, en el marco del diseño institucional de la OTAN, la información asimétrica implica que algunos actores pueden llegar a saber más que otros en cuestiones de ciberseguridad, por lo que la información suministrada teniendo en cuenta los intereses nacionales, puede no ser lo suficientemente detallada constituyéndose en un obstáculo para la cooperación. En esta situación, la creación de

instituciones y agencias de la OTAN actuarían como mediadores y facilitadores de información igualitaria para los Estados miembros reduciendo la incertidumbre. Al mismo tiempo suministran modelos de conducta donde los Estados miembros pueden evaluar recíprocamente sus desempeños y reputaciones. En segundo lugar, el riesgo moral puede alentar actitudes menos cooperativas es decir, el hecho de que un Estado miembro se sienta protegido por la política de ciberseguridad de la OTAN en su conjunto, puede llevarlo a descuidar sus obligaciones con el sistema. En tercer lugar, la irresponsabilidad conlleva a que algunos Estados miembros de la OTAN puedan asumir compromisos entendiendo que el entorno será siempre favorable, pero si se producen eventualidades desfavorables, tal vez no sean capaces de cumplir sus obligaciones, ya que los Estados más proclives a la cooperación son los que esperan ganar más en relación a lo que contribuyen al sistema.

Sin embargo, las instituciones creadas por la OTAN para llevar adelante la política de ciberseguridad ayudarían a solucionar estos problemas. Según Keohane (1993) con las normas y las reglas se reducen el rango de conducta esperada y la incertidumbre. A su vez, el acceso a información igualitaria reduce la asimetría de su distribución, y los monitoreos de conducta recíprocos atenúan el riesgo moral.

Por otra parte, siguiendo los conceptos de Martin y Simmons (1998), es esencial que desde las instituciones de la OTAN se distingan *efectos convergentes y efectos divergentes* de las políticas de ciberseguridad sobre los Estados miembros. Desde la lógica más racionalista, las políticas institucionalizadas en ciberseguridad creadas en el ámbito de la OTAN conducirían a un efecto convergente. Este modelo aspira a metas que los Estados difícilmente puedan alcanzar por sí mismos como consecuencia de fallas y límites en la acción estatal unilateral. Una vez que las políticas son institucionalizadas, la conducta de los Estados convergirá adoptando similares prácticas en ciberdefensa, pudiendo ser medidas e identificadas mediante indicadores relevantes.

Por otro lado, de acuerdo a Martin y Simmons (1998), las políticas en ciberseguridad de la OTAN pueden llegar a provocar efectos divergentes en aquellos Estados que poseen patrones de conductas preexistentes. En el espacio OTAN estos efectos divergentes pueden producirse cuando los Estados miembros poseen políticas en ciberseguridad diferentes a las establecidas desde la organización y sólo mostraran un

pequeño cambio en sus conductas, mostrándose reticentes a adoptar las nuevas directrices.

En este aspecto, Stone (2009) ha analizado que factores motivan la resistencia y el cambio en las instituciones internacionales, notando que la mayoría de las grandes instituciones internacionales que existen, como por ejemplo la OTAN, son criticadas por la opinión pública debido a que no cumplen enteramente con los objetivos para los cuales fueron creadas, indicando que tal como Keohane lo había previsto en su teoría, los costos asociados con la negociación y reforma de áreas problemáticas y de procedimiento son altos y plantean problemas para los Estados miembros. De esta manera, si bien la OTAN cumple un rol clave en el sistema de seguridad colectiva de los Estados miembros, su capacidad de adaptación y expansión en el área de la ciberseguridad podría ser lenta debido a los altos costos de negociación y a los intereses enraizados de los miembros fundadores. Stone (2009) sostiene que en la creciente sociedad global e interdependiente, el poder estatal y las instituciones internacionales interactúan de manera sutil y que la posibilidad de alcanzar objetivos comunes quizás dependen mas de la distribución del poder o del diseño formal de las instituciones internacionales que de aquellas interacciones.

Profundizando aún más en esta dirección Mitchell (2009) indaga sobre la influencia de las instituciones internacionales en el comportamiento estatal. El autor señala que identificar la influencia de las instituciones internacionales requiere tener en cuenta la *estructura del problema*, a la que define como un conjunto de factores que influyen en el comportamiento del Estado, de manera que los algunos Estados pueden llegar a ver los resultados actuales en determinadas áreas como sub-óptimos y verse motivados a crear una institución internacional para mejorarlos. Siguiendo a Mitchell (2009) la OTAN debe evitar que en el diseño institucional de las políticas en ciberseguridad sea completamente endógeno a la estructura, es decir creado por los Estados miembros con procedimientos afines a sus propios intereses, dónde no exista espacio para la influencia institucional, y que por el contrario, si se demuestra que la estructura del problema no es utilizada para el diseño de las políticas en ciberseguridad de la OTAN, en consecuencia ésta puede jugar un rol más independiente y efectivo.

En síntesis, en forma evidente la realidad internacional descripta desde el Institucionalismo Neoliberal ha tenido continuidad y se ha mostrado con fuerza en los

últimos tiempos. Un mundo interconectado y complejo; asimétricamente interdependiente; con la emergencia de actores no estatales/transnacionales y donde los Estados siguen manteniendo su predominio aunque a costos cada vez mayores. En efecto, la agenda global es mucho más extensa, variada, abarca numerosas áreas y temáticas, y es allí donde los Estados se ven en la necesidad de cooperar y trabajar en forma coordinada e institucionalizada para alcanzar resultados más beneficiosos y con menores costos asociados.

Indudablemente, la irrupción de las nuevas tecnologías y la conformación de la Sociedad de la Información, indican que el ciberespacio no escapa a estas nuevas realidades y desafíos que implican para las relaciones internacionales. Teniendo en cuenta que en el ciberespacio se modifican principios básicos del paradigma clásico en seguridad, se entiende que la OTAN, se ha visto forzada a readecuar su doctrina y a la construcción de una serie de políticas en el área de la ciberseguridad. Por ejemplo, la flexibilidad geográfica/temporal, el anonimato y el hecho de que actores no estatales, actuando incluso en forma aislada, puedan afectar seriamente la seguridad de un Estado presentan todo un reto a dicho paradigma. En otras palabras, el proceso de globalización y la configuración del ciberespacio como una nueva dimensión de la seguridad implican, por un lado, no caer en el error de subestimar las capacidades materiales y el poder militar como herramientas de seguridad, pero por el otro, en la necesidad de adecuar las políticas de seguridad de la OTAN frente a amenazas no tradicionales tanto en sus aspectos cuantitativos como cualitativos.

De esta manera, los ataques cibernéticos constituyen un aprendizaje y un nuevo desafío a la hora de construir políticas relativas a la ciberseguridad en la OTAN, no sólo por el hecho en sí mismo, sino por el enorme potencial que pueden llegar a alcanzar las nuevas tecnologías en términos de amenazas y daños para los Estados miembros y sus sociedades.

Desarrollo de la Metodología

El presente TFG se apoyará en una investigación de tipo exploratoria que utilizará herramientas descriptivas. El perfil exploratorio, que será el pilar de la investigación, se basará en el hecho de que la lectura crítica realizada hasta el momento demostró que si

bien se han realizado un importante número de publicaciones en relación al tema de estudio, a su vez se ha podido detectar la existencia de puntos ciegos o poco explorados respecto a la contextualización de los acontecimientos en Estonia desde una perspectiva institucional, a la emergencia del ciberespacio como una nueva dimensión de seguridad para la OTAN y la posterior construcción de toda una política en ciberseguridad en el ámbito de la Organización. En este sentido, la actividad exploradora busca descubrir nuevos datos, ideas y relaciones que permitan responder con mayor claridad sobre la naturaleza del problema allí donde hay muy poco conocimiento acumulado del mismo (Vieytes, 2004).

Desde la dimensión descriptiva se analizarán y examinarán los rasgos y atributos del objeto de estudio. Es decir, desde lo descriptivo se busca indagar para obtener un perfil del objeto que permita ofrecer a la investigación un conocimiento exhaustivo del mismo o de alguno de sus aspectos (Vieytes, 2004). De esta manera, se hace imprescindible un estudio profundo de las características de los sucesos, actores y componentes del problema que permita la elaboración de una cartografía analítica del caso.

Respecto al tipo de investigación se utilizará una metodología preponderantemente cualitativa, en cuanto a que desde los estudios y análisis se hará una referencia general orientada a comprender los hechos a partir de la interpretación de conductas, intenciones y motivaciones de los actores implicados, utilizando en la investigación conceptos y categorías emergentes en forma inductiva y se privilegiarán análisis en profundidad en relación al contexto (Sautu, 2003). No obstante lo antedicho, sin perjuicio de la posibilidad de utilizar procedimientos de tipo cuantitativo si las exigencias de la investigación lo requieren, como por ejemplo la utilización de datos estadísticos, situación que anticipa que el estudio adoptará un diseño de tipo flexible y abierto de acuerdo a las alternativas que vayan a presentarse en el transcurso del caso.

En relación a las variables e indicadores, y considerando lo expuesto en el marco teórico, los intereses mutuos de los Estados de la OTAN en el área de la ciberseguridad actuarían como promotores de la cooperación en la búsqueda de soluciones pensadas en términos de ganancias absolutas. De este modo, es posible esquematizar una serie de variables e indicadores a partir de los cuales se pueda guiar la investigación:

Variable Independiente

- Intereses mutuos de los Estados miembros de la OTAN en ciberseguridad.

Variables Dependientes

- Instituciones y agencias creadas y promovidas en la OTAN a partir de intereses mutuos de los Estados miembros en ciberseguridad en el período 2008-2013.

- Nuevo Concepto de Ciberdefensa establecido por los Estados miembros de la OTAN y definido en términos de ganancias absolutas.

- Declaraciones, convenios y acuerdos en ciberseguridad celebrados por los Estados miembros.

Indicadores

- Cantidad y tipo de convenios celebrados en el marco de la OTAN en relación a la ciberseguridad.

- Número de agencias e instituciones creadas en el ámbito de la OTAN en el área de la ciberseguridad.

- Información vinculada a la ciberseguridad publicada por la OTAN.

- Funciones y especificidad de las instituciones y agencias vinculadas a la ciberseguridad de la OTAN.

- Cantidad de Estados miembros que participan en las agencias, e instituciones en ciberseguridad de la OTAN.

- Ejercicios comunitarios vinculados a la ciberseguridad realizados por la OTAN.

Finalmente, en lo que concierne a las fuentes se utilizarán fuentes primarias y secundarias. En cuanto a las fuentes primarias se realizará un análisis crítico de documentos publicados y convenciones sobre ciberseguridad celebrado en el ámbito de la OTAN. Entre estos documentos se destacan los publicados por la OTAN en materia de ciberseguridad a través de los Research Papers de la NATO Defense College desde 2008 hasta la actualidad y los Tallinn Papers publicados en 2013, 2014 y 2015 por el Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN.

Del mismo modo, se analizará la evolución de las políticas de ciberseguridad delineadas en las diferentes cumbres de la OTAN, en particular Praga 2002, Bucarest 2008, Lisboa 2010 y Chicago 2012 plasmadas en documentos y declaraciones oficiales, así como el Manual de Tallinn, preparado a instancias de la OTAN por un grupo de expertos internacionales en derecho internacional bajo la dirección de Michael Schmitt, y publicado en el año 2013 por la Universidad de Cambridge.

También serán utilizados los informes publicados a partir de 2012 por la NATO Computer Information Response Capability (NCIRC) y por la NATO Communications and Information Agency (NCIA) como material de análisis y referencia estadística.

Además se empleará información provista por la NATO Industrial Advisory Group (NIAG) en cuanto a la conformación de vínculos públicos/privados para fomentar la cooperación en investigación y desarrollo (I&D) en el ámbito de la ciberseguridad para los países de la organización.

Entre las fuentes secundarias identificamos a los artículos periodísticos publicados en la edición *on line* de la prensa (El País de España, La Nación, entre otros), y de revistas y organizaciones especializadas como RSA Security y Arbor Networks. Asimismo publicaciones de otros investigadores y centros de estudios del mundo académico relacionados con la temática, consideradas fuentes esenciales para el trabajo y que fueron oportunamente descriptas en el apartado de los objetivos.

En cuanto a su estructura, el presente TFG se divide en 4 capítulos y las conclusiones. El Capítulo 1 indagará respecto a los antecedentes de la OTAN en ciberseguridad, los primeros incidentes sufridos por la organización, y el ataque cibernético a Estonia que motivó las posteriores políticas de la OTAN en el área de la ciberseguridad. El Capítulo 2 abordará en qué consisten las amenazas cibernéticas, cómo fueron evolucionando, de qué manera se utilizan y como respondió la OTAN a ellas. El Capítulo 3 profundiza el análisis de la respuesta institucional de la OTAN como organización internacional a los ciberataques, cómo readecuó su estructura institucional y cuál fue la respuesta de los Estados miembros. El Capítulo 4 examinará los avances en el campo del derecho internacional aplicable a la ciberguerra desarrollado desde la OTAN, en particular el Manual de Tallin. Las Conclusiones resumirán los aspectos centrales del tema de estudio, las fortalezas, las debilidades y las propuestas de acción.

CAPÍTULO 1

Antecedentes de la OTAN en ciberseguridad y el ataque cibernético a Estonia

La OTAN y la ciberseguridad

La Organización del Tratado del Atlántico Norte (OTAN) fue creada el 4 de abril de 1949 en Washington entre Estados Unidos, Reino Unido, Francia, Canadá, Bélgica, Holanda, Luxemburgo, Islandia, Dinamarca, Noruega, Italia y Portugal mediante un tratado conocido como el Tratado de Washington, con el objetivo de conformar un sistema de seguridad colectiva para asegurar la defensa de estos países de la amenaza soviética (Jones, 2015).

En el Preámbulo del Tratado, se manifiesta el propósito fundamental de la OTAN que es preservar a los Estados miembros de un modo de vida que les es propio y que se cimienta en el hecho de pertenecer a una sociedad común, democrática, respetuosa de las libertades individuales y del imperio de la ley (Ortega, 2016)

De acuerdo a Ortega (2016), resulta evidente que la idea subyacente de la Organización era proteger los logros alcanzados por el capitalismo y las democracias liberales que en 1949 se percibían amenazadas en un contexto de expansión del comunismo soviético. Sin embargo, los valores proclamados en el Preámbulo y que deberían actuar como condicionantes ante futuros Estados ingresantes, no fueron respetados ya que, por ejemplo, al constituirse la OTAN Portugal era una dictadura, y al momento de su adhesión, tanto Grecia como Turquía no respetaban los derechos individuales ni las libertades de sus ciudadanos (Ortega, 2016)

De hecho, con el paso del tiempo, la organización fue incorporando nuevos miembros llegando en la actualidad a 28 e incluyen, a los ya mencionados Grecia (1952) y Turquía (1952), Alemania (1955), España (1982), República Checa (1999), Hungría (1999), Polonia (1999), Bulgaria (2004), Estonia (2004), Letonia (2004), Lituania (2004), Rumania (2004), Eslovaquia (2004), Eslovenia (2004), Albania (2009) y Croacia (2009) (Brunet, 2016).

Adicionalmente, con la caída del bloque soviético en 1991, los objetivos primigenios expuestos anteriormente y para los cuales la OTAN había sido creada, tuvieron que ser adaptados a medida que emergían nuevos desafíos y amenazas provenientes de un sistema internacional que se estaba transformando (Brunet, 2016).

Efectivamente, la finalización de la Guerra Fría redujo considerablemente las amenazas convencionales sobre Europa, lo que condujo a la OTAN a desarrollar un *aggiornamento* de su doctrina y de los conceptos estratégicos, entendiendo que debía llevar adelante un rol mucho más activo en términos globales atendiendo los cambios en el sistema internacional producto de la globalización (Gisbert, 2016)

De acuerdo a Gisbert (2016), de ahí que la OTAN comenzó a actuar en operaciones llamadas *fuera de zona* para hacer referencia a aquellas operaciones que estaban fuera del área original de cobertura del Tratado. De estas primeras operaciones se destacan la participación en el bloqueo naval de 1993 en el Mar Adriático contra Yugoslavia; el apoyo logístico y de infraestructura para consolidar el área de exclusión en Bosnia – Herzegovina en 1994, y la participación en la Guerra de Kosovo en 1999.

Precisamente, es durante la crisis de Kosovo, cuando la OTAN enfrentó al primer incidente de relativa magnitud relacionado a ciberataques. El serbio Dragan Vasiljković comandó un ejército de 450 voluntarios compuesto por expertos informáticos de varias naciones con el objetivo de romper el cerco informativo impuesto por la OTAN y llevar al mundo su visión de la guerra. El grupo, instalado en un rascacielos, logró infiltrarse en los sistemas informáticos de la OTAN, bloquear su cuenta de e-mail y dejar repetidamente su portal web fuera de servicio. (Lejarza Illaro, 2014)

Sin embargo, considerando el contexto de época, la dimensión cibernética de un conflicto fue simplemente entendida como una forma de obstaculizar la campaña de información de la OTAN y lo ciberataques comenzaron a ser vistos como un riesgo limitado en alcance y potencial que demandaban únicamente respuestas de tipo técnica acompañada por bajos esfuerzos para asegurar la información pública (Theiler, 2011).

Los acontecimientos del 11/9 del 2001 en Estados Unidos, comenzaron a cambiar tal percepción. Antes de los ataques de Al Qaeda, hubiese sido ciertamente imposible para cualquiera, incluidos los autores del Tratado de Washington imaginar actores no

estatales convertir aviones en misiles y lanzar ataques contra un Estado. De la misma manera, ya nadie podía asegurar hasta adonde podría llegar el alcance y el daño de un ataque cibernético (Jones, 2015).

Un año después del 11/9, la OTAN hizo un llamado para mejorar sus capacidades de defensa cibernética que se plasmó en un compromiso adoptado en la Cumbre de Praga del año 2002 (Theiler, 2011). No obstante, debido al alto impacto que habían tenido los ataques terroristas en Estados Unidos, los asuntos relacionados con la ciberseguridad tuvieron un trato poco más que superficial.

Este hecho se puede constatar en el texto oficial de la Declaración Final de la Cumbre de Praga expresado con liviandad en la sección 4, inciso f, donde los Estados miembros de la OTAN se comprometen a "fortalecer nuestras capacidades de defensa contra ataques cibernéticos" (OTAN, Declaración Cumbre Praga, 2002).

El compromiso se materializó con la instrumentación del Programa de Ciberdefensa de la OTAN, cuya finalidad era al menos mejorar parcialmente las capacidades de la OTAN luego de los ataques que distintos activistas habían llevado a cabo contra la organización durante la operación Allied Force en Kosovo 1999. El elemento más importante del Programa fue la creación en 2004 de la *Capacidad de Respuesta ante Incidentes Informáticos de la OTAN* (NCIRC por sus siglas en inglés) cuya misión era prevenir, detectar y responder ante ciberincidentes (Healey y Van Bochoven, 2011).

El NCIRC a su vez estaba constituido por un centro de apoyo y coordinación y por un centro técnico. En estos dos centros se reunían la mayoría de los expertos de la OTAN en ciberseguridad. En caso de ciberataque, el NCIRC coordinaría respuestas de tipo multidisciplinar dentro del entorno OTAN. A su vez, sería el encargado de estudiar la estandarización de los protocolos en ciberdefensa, coordinación con los Estados miembros y comunicaciones con otras áreas de seguridad de la OTAN (Artiles, 2011).
Sin embargo, en los años posteriores a la creación del NCIRC, la OTAN se focalizó en implementar medidas en ciberseguridad de tipo amplias y de protección pasiva, tal como fueron denominadas en su momento sin comprender cabalmente la potencialidad y la dimensión que podía alcanzar un ciberataque (Theiler, 2011)

Estas medidas de protección pasiva eran regidas por directrices generales basadas en distintos acuerdos como el Compromiso de Capacidades de Praga en 2002 y la Orientación Política Integral en 2005 (Theiler, 2011)

En la de Cumbre de Riga en 2006, los Estados miembros de la OTAN continuaron realizando esfuerzos por mejorar sus capacidades en ciberseguridad, aunque en realidad se trataron más de expresiones de deseo que de políticas concretas. Tal como expresa el texto oficial de la Declaración de la Cumbre de Riga:

> La adaptación de nuestras fuerzas debe continuar. Hemos aprobado un conjunto de iniciativas para aumentar la capacidad de nuestras fuerzas para hacer frente a las amenazas y desafíos contemporáneos. Éstas incluyen: (…) trabajar para desarrollar la NATO Network Enabled Capability, para compartir información, datos e inteligencia de forma fiable, segura y sin demora en las operaciones de la Alianza, mejorando al mismo tiempo la protección de nuestros sistemas de información clave contra el ciberataque. (OTAN, Riga Summit Declaration, 2006, Sección 24)

No obstante, no fue hasta que ocurrieron los ataques contra Estonia en 2007, que la OTAN realmente realizó a fondo la escala técnica y las potenciales implicaciones políticas de los ciberataques (Healey y Van Bochoven, 2011).
En efecto, el creciente reconocimiento por parte de la OTAN al potencial de las amenazas cibernéticas fue confirmado por un incidente posterior caracterizado por un alto nivel de sofisticación y organización. Este punto de inflexión fue el masivo ciberataque lanzado contra Estonia en 2007, ya que únicamente los eventos ocurridos en Estonia provocaron que la OTAN repensara la necesidad de una política de ciberdefensa y la implementación de contramedidas (Theiler, 2011).

Los ciberataques contra Estonia marcaron un desafío histórico para la OTAN, ya que fue la primera vez que un país solicitó apoyo a la OTAN por un ataque a sus sistemas de comunicación. Sin embargo, hasta ese momento, la OTAN no contaba con un plan de acción contra un ataque cibernético contra un Estado parte, lo que llevó a los ministros de Defensa a colaborar y poner en marcha y en forma urgente un programa para la implementación de medidas y de una política en ciberseguridad (Theiler, 2011).

Para una primera aproximación al caso de estudio, el análisis en profundidad del ataque a Estonia, tanto desde el contexto como desde la forma de ejecución, es importante. No sólo para entender el clima de época, las políticas en ciberdefensa y la estructura institucional luego implementadas por la OTAN para todos sus miembros y que serán analizados en los próximos capítulos. Sino también para comprender como, en la Sociedad de la Información actual y futura, un ciberataque puede afectar el funcionamiento de un Estado en su totalidad, y que dicha experiencia llevó a que los Estados miembros de la OTAN, redefinieran sus intereses nacionales a partir del aprendizaje y de la nueva información adquirida. En efecto, esto significó por un lado, una toma de conciencia sobre la dimensión que ocupa el ciberespacio en el sistema internacional y, por el otro, posibilitó un nuevo diseño institucional de la OTAN, protocolos de acción, trabajos de investigación en ciberseguridad, propuestas de legislación aplicables al ciberespacio y toda una readecuación de su doctrina de seguridad

Estonia y el fin de la Guerra Fría.

Tras la caída del Muro de Berlín en noviembre de 1989, la República de Estonia era uno de los estados bálticos pertenecientes a la Unión Soviética que comenzó a presionar para alcanzar mayores niveles de autonomía que le permitiesen despejar el camino hacia su independencia.

Después de décadas de dominación e intervencionismo soviético, que incluyeron la colectivización de la economía y la militarización de su territorio, el 20 de agosto de 1991 Estonia finalmente declara la reinstauración de su independencia (Red de Información de Andalucía, 2004).

La independencia implicaba enormes desafíos para un país que había transcurrido casi 45 años bajo dominio soviético, y pasaba de un entorno controlado, aislado y hermético hacia uno abierto, interconectado y en plena transformación debido a los cambios del sistema internacional, la evolución tecnológica y el fenómeno de la globalización.

Luego de las elecciones generales realizadas bajo el amparo de la nueva Constitución los sucesivos gobiernos de Estonia, se esforzaron para transformar a Estonia en una economía de mercado e integrada a Europa, situación que fue alcanzando

paulatinamente con su incorporación a la Unión Europea y la OTAN en 2004, la afiliación a la OCDE en 2010, sumando la adopción del euro como moneda en 2011.

Si bien desde mediados de los años sesenta, y de la mano de la Unión Soviética, Estonia había comenzado a transitar el mundo de la informática, es a partir de 1992 cuando empieza a desarrollar todo un proceso de cambio, tanto en términos cualitativos, cuantitativos, estructurales, y por sobre todas las cosas conceptuales, acerca de la importancia que se le asignó a las redes informáticas.

De esta manera, se inicia un verdadero salto al mundo de internet que sería fundamental para transformar toda su infraestructura de telecomunicaciones. En 1992, se registra el dominio nacional ".ee" y en 1994 el Parlamento Estonio aprueba la Ley de Información que implicaba el compromiso del gobierno a financiar la compra de software, hardware, conservación de infraestructuras, promoción y apoyo a proyectos para el sector provenientes del sector privado (Fernández, 2015). En sintonía, el acceso a internet se convierte en un derecho protegido por la Constitución.

En 1996 se presenta un plan revolucionario denominado *Tigriihüpe* (Salto del Tigre), orientando al sector educativo, y cuyo objetivo era dotar a todas las escuelas de Estonia de computadoras y de la infraestructura en redes necesaria que permitan una mayor accesibilidad y calidad del servicio (Fernández, 2015).

Como señala Fernández, a partir de ese punto Estonia comenzó a profundizar la digitalización de su sociedad destacándose el proyecto más ambicioso conocido como la autopista *X-Road* concebido en 2001 para proporcionar la interacción de bases de datos públicas y privadas e integrar lentamente internet en la vida corriente de los ciudadanos, firmando y encriptando la información saliente por un lado, y autenticando y registrando la entrante por el otro (Fernández, 2015).

Dentro del marco provisto por la autopista *X-Road* (figura 1), convertida en una red abierta adonde se integran empresas, organizaciones e instituciones tanto públicas como privadas, los ciudadanos pueden llevar adelante toda una serie de actividades de control, gestión o trámites en forma totalmente digitalizada.

Dentro de esta sociedad digital en Estonia se destacan entre otros:

- *Digital ID*, o DNI electrónico introducido en 2002

- *i-Voting*, o voto electrónico que permite a los ciudadanos votar desde cualquier PC.

- *e-Tax*, para consultar o realizar pagos de impuestos.

- *e-Law*, para informarse sobre las actividades parlamentarias.

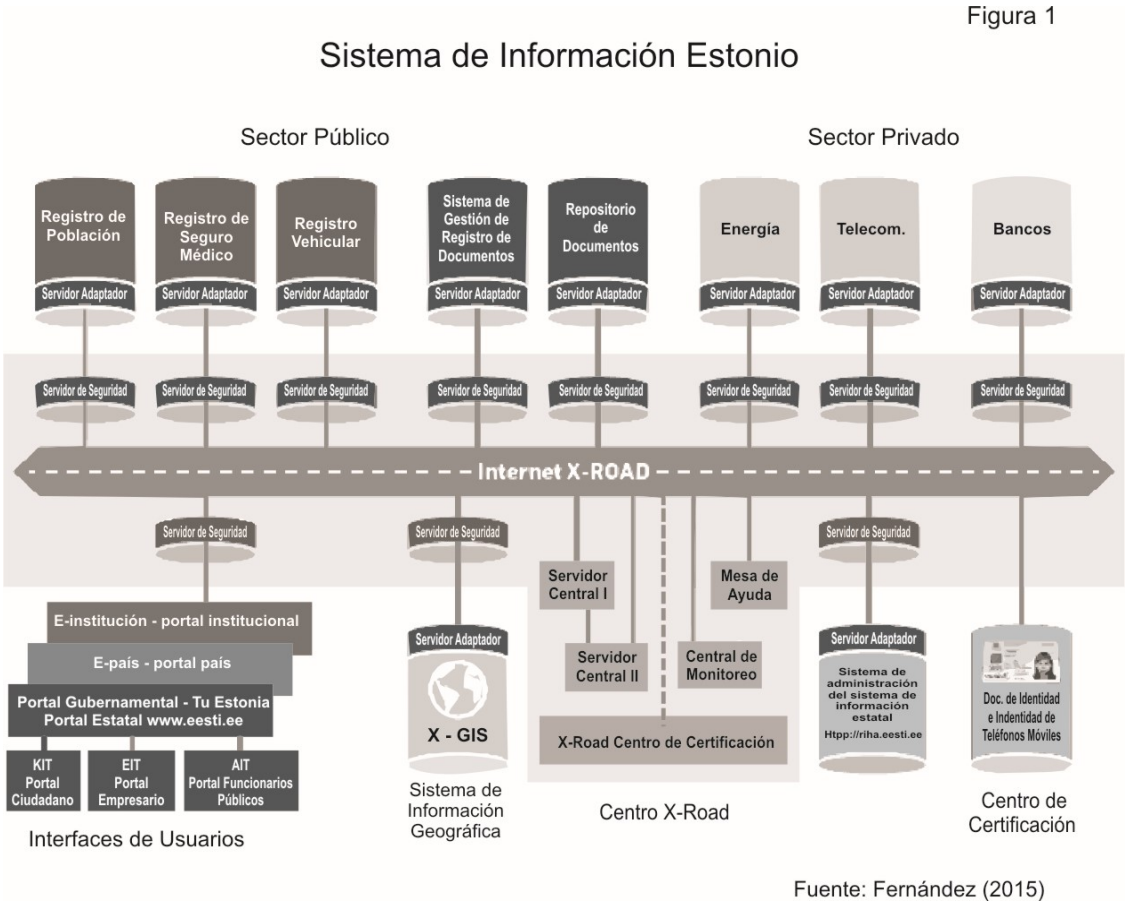
- *e-police,* base de datos policial a través de la cual los agentes tienen acceso a la información de cualquier ciudadano con solo ingresar su ID.

- *Electronic Health Registry* y la *e-Prescription,* se accede al historial médico y faculta al médico recetar sin necesidad de acudir a una consulta cuando no es necesario.

- *e-education,* docentes, padres y alumnos interconectados, proporciona acceso a notas, información, o solicitudes de ingreso a establecimientos educativos.

- *e-bank*, la sociedad estonia realiza un 90% de sus transacciones financieras por la banca electrónica.

Figura 1



Fuente: Fernández (2015)

De este modo, se observa cómo desde su independencia en 1991, Estonia llevó adelante toda una serie progresiva de políticas encaminadas a integrarse y reconvertirse dentro del nuevo contexto internacional globalizado, interconectado y dinamizado por la impronta del avance técnico-científico y de libre mercado que se fue configurando tras la caída del Muro de Berlín, por lo cual el acceso a las nuevas tecnologías era sinónimo de progreso y bienestar.

Como consecuencia, estas políticas no sólo permitieron a Estonia pasar a formar parte activa de la dinámica mundial emergente, sino que por otro lado, la fueron colocando a la vanguardia en cuanto a la digitalización e informatización de la sociedad.

El ataque informático a Estonia de 2007

Los extraordinarios avances en materia de infraestructura, tecnología y redes digitales obtenidos por Estonia no ocultaron la existencia de un clima tenso en las relaciones con Rusia y que se fue retroalimentando desde ingreso de Estonia a la Unión Europea y la OTAN en 2004.

En abril de 2007 el gobierno estonio anunció la decisión de realizar excavaciones en la Plaza de Tonismäe, en Tallin su capital, con el propósito de identificar restos de soldados caídos durante la Segunda Guerra Mundial y trasladarlos al cementerio militar de Tallin. Esta decisión incluía el traslado de la estatua conocida como *el soldado de bronce* erigida en la entrada del cementerio militar de Tallin, e instalada en 1947 por los soviéticos con motivo de su victoria sobre el ejército nazi (Ferrero, 2013).

La estatua del soldado de bronce representaba para la comunidad rusa de Tallin a la gloria soviética y su esplendor. Era costumbre depositar flores a sus pies en fechas patrias rusas, por lo que para las minorías rusas personificaba al libertador, pero para los estonios simbolizaba el opresor. Sin embargo, hasta mayo de 2006 se vivió una situación de normalidad donde la comunidad rusa concurría a la plaza y los estonios consentían sin otorgarle demasiado interés (Artiles, 2011).

Desde entonces, lentamente se inaugura una etapa de surgimientos nacionalistas que habían estado contenidos durante la Guerra Fría. La contienda ideológica había dejado

su impronta y las demandas reprimidas empezaron a ser canalizadas en el marco de un entorno internacional que se había modificado sustancialmente.

De este modo, el soldado de bronce se transformó en el punto de choque de una sociedad cada vez más polarizada y que derivó en enfrentamientos entre grupos pro-rusos y nacionalistas estonios, generándose disturbios cada vez más violentos y que obligó a la policía a intervenir para contenerlos (Artiles, 2011).

Ante este escenario, el gobierno de Estonia entendió necesario desplazar un objeto-símbolo que era motivo de continuas tensiones y hostilidades, situación que se concreta el 26 de abril de 2007 y que provocó la reacción de las minorías rusas en medio de protestas, disturbios, gases lacrimógenos, arrestados y heridos en lo que se denominó la *noche de los cristales.* La tensión siguió en aumento en gran medida instigada desde los medios de comunicación rusos, lo que llevó a que el conflicto se trasladase a Rusia, y se produzca el bloqueo durante una semana de la Embajada de Estonia en Moscú y la agresión de su embajadora Marina Kaljurand por parte de manifestantes enardecidos. Ante los reclamos estonios, el gobierno ruso se comprometió a finalizar con el bloqueo de la embajada bajo la condición de que la embajadora Kaljurand se marchase de Moscú, hecho que ocurre el 5 de mayo (Ferrero, 2013).

En este contexto comienzan los ciberataques, que se llevan a cabo entre el 27 de abril y el 18 de mayo de 2007. De acuerdo a Artiles (2011) durante su desarrollo fueron modificándose la intensidad, los objetivos y la metodología, pero en líneas generales pueden identificarse dos fases.

La primera fase, del 27 al 29 de abril, desarrollada en medio del fragor y las tensiones nacionalistas, cargada de componentes simbólicos y emocionales, fue llevada a cabo por *hacktivistas* mediante herramientas de ciberataque técnicamente básicas y elementales cuyos objetivos eran los sitios web del gobierno y los principales partidos políticos (Ferrero, 2013). Estos ataques mal coordinados, también dirigidos hacia algunos portales de noticias, fueron en principio fácilmente controlados. Incluso, en muchos casos las instrucciones, la información de objetivos y el software de ataque fue distribuido por canales de chat y correo electrónico (Río Durán; 2011).

Una vez confirmado que el país estaba bajo un ciberataque se produce uno de los mayores logros del gobierno estonio: reconocer rápidamente la gravedad del ataque, organizar un equipo para afrontarlo y asignarle la autoridad necesaria (Artiles, 2011).

La segunda fase se puede ubicar entre el 30 de abril y el 18 de mayo. Esta vez los ataques fueron mucho más sofisticados y complejos tanto desde el punto de vista técnico como desde la organización y el volumen. Las herramientas de software empleadas, como por ejemplo, programas de ejecución automática desde servidores ubicados en Egipto, Vietnam y Perú permiten tomar dimensión de la magnitud del ataque. Los ataques afectaron a casi toda Estonia paralizando sus actividades políticas y financieras e incrementándose con fuerza en ocasión de la conmemoración de la victoria rusa sobre el ejército alemán el día 9 de mayo (Río Durán, 2011).

Los ataques no fueron realizados mediantes instrumentos que puedan adquirirse en mercados paralelos de fácil acceso, sino que son productos que responden a capacidades estatales desarrolladas y orientadas a la ciberguerra (Artiles, 2011). Por lo tanto, estas capacidades exigen una importante inversión en investigación y desarrollo (I+D) situación que explica como el ciberespacio ha pasado a formar parte de las estrategias de seguridad de los Estados a partir de la resignificación del concepto de seguridad y de sus distintos niveles.

El impacto de los ataques

La notable transformación de Estonia post Guerra Fría y su sociedad digital habían sido vulneradas, lo que en alguna medida ponía en duda el prestigio y la confianza en el sistema que con esfuerzo fue construyendo desde su independencia. El mundo había cambiado, sin embargo los riesgos y amenazas asumieron nuevas formas adaptadas al contexto y con otros objetivos.

Los ataques, perfectamente organizados y coordinados, tuvieron características y propósitos bien definidos, circunstancia que indica que los autores formaban parte de una estructura compleja y dotada de recursos para tal fin.

La agresión informática se caracterizó por denegaciones de servicio, desfiguración de los sitios web, ataque a los sistemas de nombres de dominio y el envío de correo basura

(spam). Las denegaciones de servicio tornaron inaccesible los sitios web a los usuarios corrientes mediante múltiples peticiones simultáneas que provocaron una sobrecarga en la banda ancha. La desfiguración de los sitios web consistió en la alteración y modificación de los contenidos originales de las páginas web gubernamentales, bancarias, o de portales de noticias, colocando en su lugar mensajes hostiles pro-rusos o con simbología rusa. El ataque a los sistemas de nombre de dominio y su bloqueo fue muy dañino ya que impidió direccionar y conectar los equipos informáticos a nivel nacional e internacional. Finalmente, el correo basura (spam) consistió en el envío de miles de correos hacia oficinas gubernamentales y políticos prestigiosos saturando sus casillas de entrada con mensajes y propaganda rusa (Artiles, 2011).

Por otro lado, los ataques tuvieron propósitos bien definidos enfocados a provocar daños a nivel político, económico, comercial y comunicacional. Para considerar el impacto de los ataques en las distintas áreas en primer lugar, tal como se viene desarrollando en este documento, se debe tener en cuenta que Estonia es una sociedad totalmente digitalizada y sumamente dependiente de las redes informáticas, con un importante grado de integración tanto de las redes públicas como de las privadas. Por lo tanto, un ataque informático de esa magnitud equivale prácticamente a paralizar a un país.

Los perjuicios a nivel político fueron importantes si se repara en el hecho de que en Estonia la actividad política se canaliza en su totalidad por la red. Por ejemplo, las sesiones de gobierno y de ministros se realizan mediante intranet, evitando el 100% de gestiones administrativas en papel y los ciudadanos, como se ha visto, pueden hacer un seguimiento de las actividades legislativas mediante el *e-law*. Asimismo, el ataque a nivel político tuvo una fuerte carga simbólica ya que se puso en juego el prestigio y la seguridad nacional en un sector sensible.

En el área económica uno de los sectores más perjudicados fue el *e-banking*, en particular los bancos Hansapank y SEB Eeesti Uhispank que controlan el 80% del mercado estonio y que quedaron imposibilitados para operar. En cuanto a al sector comercial, en simultáneo con los ataques, la Federación Rusa cerró sus fronteras a los transportes de carga pesada provenientes de Estonia sumando en forma indirecta un daño colateral. Finalmente, respecto a las comunicaciones, los más afectados fueron los

proveedores de servicios de Internet, los administradores de nombres de dominio y los portales de noticias más importantes como Postimees, EPL y Baltic News quedando el país virtualmente incomunicado (Artiles, 2011).

Una rápida lectura de los acontecimientos posibilita comprender de que manera el mundo globalizado e interconectado ha transformado al ciberespacio en un nivel de seguridad de consideración. De la misma manera, se puede observar como un ataque informático bien organizado y coordinado puede llegar a paralizar la estructura política y productiva de un país, pudiendo incluso en casos extremos afectar el funcionamiento de infraestructuras críticas, como por ejemplo, una represa hidroeléctrica o una central nuclear con los riesgos que suponen para la población.

La réplica de Estonia

Tras entender la gravedad de los acontecimientos, el gobierno de Estonia formó un equipo multidisciplinario de respuesta denominado Equipo Nacional de Respuesta ante Incidentes Informáticos (CERT, por sus siglas en inglés), quien se hizo cargo de la situación y comenzó a ensayar respuestas para normalizar y reestablecer en lo inmediato la conectividad en la red.

Como primera medida se eliminaron funciones de los sitios web y se cortó todo tráfico procedente de Rusia para liberar ancho de banda y poder recuperar el transito de datos en la red. Por ejemplo, el periódico Portinees eliminó la posibilidad de hacer comentarios, las publicidades y las fotografías (Artiles, 2011).

Sin embargo, esta primera medida no fue suficiente y luego de comprobarse que la mayoría de las peticiones automáticas procedían de Egipto, Vietnam y Perú el CERT tomó la decisión de cortar la conexión de la red de Estonia con el exterior. La disponibilidad de la red fue recuperada inmediatamente, pero solo dentro de Estonia, por lo que el país estaba aislado digitalmente y la prensa no podía informar al mundo lo que estaba sucediendo (Ferrero, 2013).

El equipo de respuesta fue un producto de la coyuntura y la emergencia por lo que el CERT no tenía la capacidad para enfrentar por si solo los hechos. Como señala Artiles, las naciones no poseen capacidad técnica y legal, para llevar adelante y en forma

individual, acciones sobre el tráfico de de Internet que está fuera de sus jurisdicciones por lo que las mismas sólo pueden emprenderse desde la cooperación internacional (Artiles, 2011).

En efecto, en sintonía con lo que se viene considerando en este trabajo, el ciberespacio y las resultantes amenazas para la seguridad requieren del esfuerzo conjunto y la cooperación internacional que posibiliten arribar a soluciones concretas.

Este concepto que se podría denominar *ciberseguridad cooperativa* proviene de la misma naturaleza de la red, ya que por esencia el ciberespacio implica la idea de coordinación, contacto, vínculo y comunicación. La ciberseguridad cooperativa a su vez requiere de marcos institucionales y legales apropiados para la prevención de los ataques, limitación de los daños, acciones defensivas, asignar responsabilidades y reparaciones.

Estonia durante el ataque informático comunicó inmediatamente a sus aliados de la OTAN y de la Unión Europea, quienes comenzaron a colaborar para anular los programas de ejecución automático que tenían en jaque a casi toda una nación. En particular se destaca la labor del CERT de Finlandia para coordinar la operación entre los equipos de respuesta de la OTAN incluido el de Estados Unidos (Ferrero, 2013).

Como indica Ferrero, el ataque informático a Estonia se transformó en un suceso histórico y en un desafío para la OTAN, ya que puede considerarse la primera acción de ciberguerra a gran escala contra la infraestructura crítica de un país. Hasta ese momento la OTAN carecía de un plan de acción en la materia y entendía que se trataba de un problema de carácter nacional (Ferrero, 2013).

El ataque informático puso en evidencia el alto grado de vulnerabilidad que existe en un área del ciberespacio, hasta ese momento un poco relegada, y al mismo tiempo materializando una nueva dimensión para la seguridad estatal.

En este sentido, quedó en claro la importancia de asumir una respuesta política coordinada y colaborativa en el marco de los vínculos establecidos entre los Estados con el objetivo de neutralizar el ciberataque.

La cooperación internacional fue efectiva para contener los ataques, sin embargo el traslado de los programas de ataque a paraísos ciberlegales o la negativa rusa a ayudar en la investigación hizo estéril todo el trabajo legal llevado adelante por Estonia luego de los hechos (Artiles, 2011).

En otras palabras, a pesar del aprendizaje y de las lecciones positivas que habían dejado los acontecimientos, aún quedaba mucho camino por recorrer y sería la OTAN quién asumiría la iniciativa para inaugurar una nueva etapa en la organización, tanto en sus políticas como en sus estrategias de ciberseguridad.

Analizando lo expuesto, es evidente que el dinamismo y las transformaciones del sistema internacional, de la mano de cambios geopolíticos y de la innovación tecnológica, modificaron las percepciones de seguridad de los Estados miembros de la OTAN. El masivo ciberataque sufrido por Estonia terminó por confirmar esas ideas y condujo a la OTAN a tomar mucho más seriamente la potencialidad de los ciberataques en el contexto de una Sociedad de la Información interdependiente. Consecuentemente, de manera urgente los Estados miembros de la OTAN dirigieron sus acciones cooperativas hacia el estudio profundo de estas nuevas formas de amenaza, como son empleadas y que tipo de recursos técnicos y estrategias son necesarios para afrontarlas exitosamente.

Conclusiones Preliminares

Las políticas y la doctrina en seguridad de la OTAN, se vieron afectadas en el término de poco más de 10 años por dos acontecimientos inesperados: la finalización de la Guerra Fría y el ataque terrorista del 11S a las Torres Gemelas.

En este contexto, la emergencia de actores no estatales con capacidad para poner en riesgo la seguridad de los Estados miembros modificó la percepción de amenazas de los mismos, y obligó a la organización a readecuar sus políticas en seguridad. El sistema internacional se volvió más complejo y comenzó a demandar respuestas que requerían acciones y estrategias innovadoras.

Asimismo, la evolución tecnológica sumó una nueva arista a la complejidad del sistema internacional. Los ciberataques pasaron a ser una nueva forma de agresión que hizo su primer blanco en la OTAN durante la operación en Kosovo del año 1999.

Subestimados en su momento por la OTAN, los ciberataques llevados a cabo luego contra Estonia en 2007 fueron de tal magnitud que por primera vez un Estado miembro solicitó ayuda a la organización por un ataque contra sus sistemas de información.

Este incidente disparó un accionar urgente por parte de la OTAN y la obligó a diseñar una nueva doctrina de seguridad. Esta tarea implicaría la construcción de políticas y especialmente un cambio de paradigma de la seguridad. La seguridad ya no estaría orientada a contener amenazas físicas, sino también virtuales. En otras palabras, nacía una nueva dimensión de la seguridad.

Los incidentes de Estonia demostraron que la cooperación internacional fue efectiva para contener el ataque, pero de alcance limitado en el mediano plazo. Serían necesarias otro tipo de medidas de carácter estructural, basadas en el compromiso mutuo, la cooperación, la coordinación y el intercambio de información.

La OTAN tomó con seriedad el desafío y consecuentemente comenzó a desarrollar una serie de políticas, instituciones y directrices en el área de la ciberseguridad que serán analizadas en el próximo capítulo.

CAPÍTULO 2

Amenazas cibernéticas: origen, desarrollo y evolución. La respuesta de la OTAN

Origen y evolución de las ciberamenazas

Aún cuando los aspectos técnicos relacionados a las ciberamenazas exceden el objetivo de este TFG, en este capítulo se considera necesario hacer una referencia general de los mismos para una completa compresión de la problemática.

Internet es el resultado de un proyecto militar realizado en Estados Unidos y que se materializó en 1969 con la ARPANET (Advanced Research Projects Agency Network). Un circuito cerrado que permitía comunicar personas y sus investigaciones a través de computadoras en el ámbito militar. Es decir, Internet no fue originalmente concebido para el uso público.

Sin embargo, en 1990 la extensión y la apertura de Internet hacia el uso público posibilitó la conformación de una nueva comunidad global, denominada *Sociedad de la Información* y que al mismo tiempo modificó la naturaleza de los problemas derivados de su uso (Tikk, 2011).

En sintonía con la perspectiva de Keohane, esta Sociedad de la Información se edificó sobre redes interdependientes, a través de canales múltiples de interacción, favoreciendo la autonomía y la acción de actores no estatales.

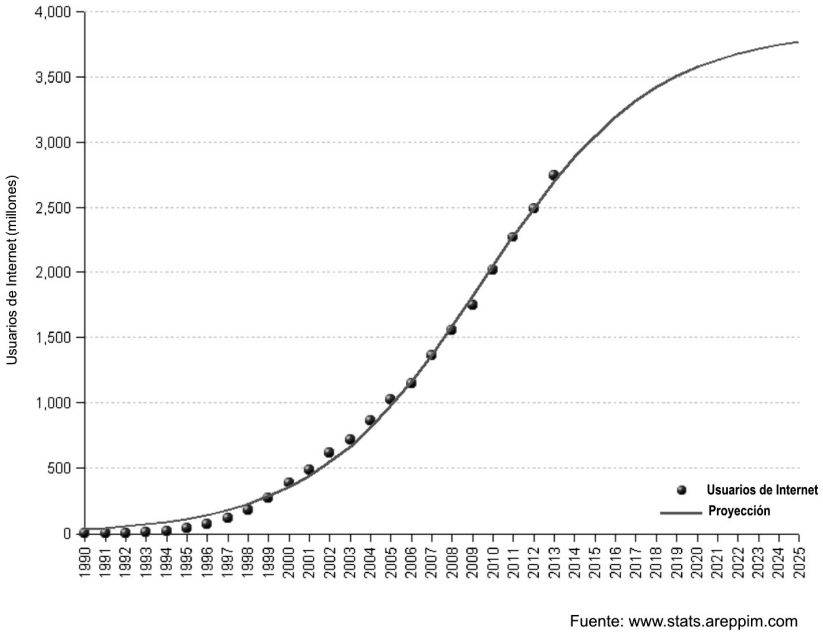
Al mismo tiempo, los Estados y el sector privado debieron trabajar y cooperar en forma conjunta para el establecimiento de estándares y protocoles comunes que hicieron posible el desarrollo y la expansión de Internet, como por ejemplo, a través de la ICANN (Corporación de Internet para la Asignación de Nombres y Números).

De acuerdo a Tikk (2011), para entender el impacto que esta Sociedad de la Información tuvo en términos de usuarios una pequeña estadística puede ser útil. Hacia 1990, Internet tenía cerca de 3 millones de usuarios donde el 73% estaban ubicados en América del Norte. En el año 2000, la cantidad de usuarios creció hasta 360 millones donde el 25 % provenían de Asia.

En 2011, el número total de usuarios se ubicó aproximadamente a las 2.000 millones, cerca de 1/3 de la población mundial, donde de acuerdo a las estadísticas el 40% son de Asia, el 24% de Europa y el 14 % de América del Norte.

Figura 2

Evolución de usuarios
de Internet a nivel mundial



Fuente: www.stats.areppim.com

Sin embargo, esta nueva realidad social no sólo expandió las posibilidades de acceso a la información y comunicación, sino que también condujo a la aparición de innovadoras formas de amenaza hacia este tipo de redes.

La Ley Moore, que duplica el desarrollo informático cada 18 meses, se mantiene vigente y el incesante crecimiento hacia un *Internet de las cosas* con microprocesadores incorporados en tejidos, anteojos o electrodomésticos amplían el espectro de las amenazas más allá de las computadoras tradicionales (Wegener, 2013).

Como acertadamente lo señala Tikk (2011), el concepto de seguridad relacionado a las TICs ha ido acompañando la evolución de Internet. En sus orígenes, muchos de los problemas que hoy tiene Internet no existían.

Por ejemplo, el anonimato no era posible debido al alcance limitado que en su momento tenía la red y el control que ejercía el gobierno de Estados Unidos sobre la misma. Por lo tanto, la mayoría de los desafíos que hoy existen en materia de ciberguridad comenzaron luego de que Internet fuera de uso público y masivo, posibilitando su acceso en forma anónima y modificando la naturaleza de los problemas relacionados a su uso.

En otras palabras, al igual que en el mundo físico, el ciberespacio permite a delincuentes llevar adelante distintas formas de fraude o a terroristas reclutar nuevos miembros para sus organizaciones. Es decir, individuos, Estados y actores no estatales usan anónimamente el ciberespacio como medio para alcanzar distintos objetivos (Jones, 2015).

Conforme a lo que se viene sosteniendo desde este TFG, esta progresiva evolución de las amenazas informáticas condujo a la redefinición del concepto de seguridad en relación al ciberespacio. En efecto, la idea sobre ciberseguridad se fue modificando desde los años sesenta cuando no era denominada ciberseguridad, sino seguridad de las computadoras.

Esto indica que para ese momento, en ese ámbito y en sentido amplio la dimensión de ciberseguridad no era una característica relevante que implicase una amenaza a la seguridad de los Estados (Tikk, 2011). Sin embargo, de acuerdo a Tikk, el concepto actual de ciberseguridad se ha modificado y puede entenderse "como la sostenibilidad de los recursos de información relevantes a nivel nacional y, en la medida de lo posible, seguir apoyando el avance de los objetivos de la sociedad de la información en general" (Tikk, 2011, p. 42).

Este concepto incluye medidas y controles que aseguren la confidencialidad, la integridad y la disponibilidad de la información y las redes, como así también la protección de los sistemas informáticos contra accesos no autorizados y maliciosos (Osula y Kaska, 2013).

De acuerdo a Tikk (2011), desde la misión inicial en ciberseguridad, focalizada en la defensa interna de los sistemas de información, la OTAN emprendió el continuo desarrollo de una agenda en ciberseguridad que por un lado, garantice la asistencia de

los Estados miembros y, por el otro, refuerce la cooperación en ciberseguridad entre la OTAN y las autoridades nacionales.

Esta agenda continúa sujeta a los objetivos y a la misión general de la OTAN establecidos en el Preámbulo del Tratado de Washington, los cuales se focalizan en la cooperación para la ciberseguridad entre los Estados miembros que han decidido unir esfuerzos para la defensa colectiva y para la preservación de la paz y la seguridad. Como resultado, este posicionamiento convirtió a la OTAN en un nuevo e importante actor en el escenario global de la ciberseguridad.

Por tal motivo, en sus trabajos preparatorios para la Cumbre de Lisboa 2010, la OTAN emitió un reporte donde fue trazando una hoja de ruta con definiciones que permitiesen orientar las futuras políticas en ciberseguridad que comenzaban a gestarse. En el citado reporte, denominado *Introducción a un Nuevo Concepto Capstone de la OTAN para la Contribución Militar contra las Amenazas Híbridas,* la OTAN indica la evidencia del potencial de los ataques cibernéticos sobre los sistemas de la red de la OTAN.

En virtud de la creciente dependencia de los Estados miembros en las TICs, esto significa que los Estados miembros de la OTAN son cada vez más vulnerables en este aspecto a las amenazas híbridas, dentro de las cuales se incluyen a los ciberataques. Estas amenazas son definidas *"…como aquellas utilizadas por adversarios, con la capacidad de emplear simultáneamente medios convencionales y no convencionales de manera adaptativa en la consecución de sus objetivos"*(New NATO Capstone Concept, 2010).

El informe además señala, que si bien la OTAN tenía en ese momento una política y un concepto sobre la defensa cibernética, era imperativo evaluar y profundizar el desarrollo de un concepto sobre todo el espectro de las operaciones cibernéticas y la protección de los sistemas.

Por otro lado, también se indica que la creciente disponibilidad de sofisticada tecnología en armas para actores no estatales aumentará significativamente la vulnerabilidad de la OTAN y sus Estados miembros, atacando blancos de alto valor civil y militar. Los ataques seguirán siendo un tema de grave preocupación, incluido el potencial de acción contra las grandes instalaciones civiles industriales. De igual modo, la amenaza de los

adversarios se verá exacerbada por los cambios geopolíticos y el patrocinio estatal más la participación de los actores no estatales (New NATO Capstone Concept, 2010).

Por esto, la disuasión y la política en ciberdefensa de la OTAN comenzó a pensarse principalmente para prevenir ataques tanto de actores estatales como no estatales. Teniendo en cuenta que la experiencia de los últimos incidentes, había quedado demostrado que ahora los adversarios disponían de una variada y abundante gama de recursos para realizar acciones hostiles y obtener resultados beneficiosos incluso frente a fuerzas tanto tecnológica como militarmente superiores. (OTAN, 2010).

En este sentido, de acuerdo a Acosta et al. (2012), parece lógico pensar que el conjunto de capacidades necesarias para llevar adelante una efectiva política en ciberdefensa en el ámbito de la OTAN, debía ser un producto derivado del incremento de las capacidades en ciberseguridad.

Dentro de los conceptos seminales de la nueva política en ciberdefensa de la OTAN se destaca el término de *Aseguramiento de la Información,* que según la Política de Gestión de la información de la OTAN de 2010 es entendida como "el conjunto de medidas para alcanzar un determinado grado de confianza en la protección de los sistemas de comunicaciones y de los sistemas de información, (...) con respecto a la confidencialidad, integridad, disponibilidad, no repudio y la autentificación".

Entre las directrices propuestas en el Nuevo Concepto Capstone para las políticas en ciberseguridad de la OTAN se señala que:

> "La Organización debe mejorar su capacidad para participar en un enfoque integral para contrarrestar las amenazas híbridas. Su complejidad requiere una respuesta holística con una comunidad más amplia comprometida con una causa común. En algunos aspectos, los Estados miembros pueden también asumir el rol de liderar la contención de la amenaza con el componente militar de la OTAN como rol de apoyo" (OTAN, New Capstone Concept, 2010, p.5).

El informe prosigue señalando que la capacidad de los potenciales adversarios para explotar el medio de información puede requerir que la OTAN adopte una política de comunicación más robusta y adoptar un cambio de mentalidad operacional y cultural

mediante los cuales la comunicación y el intercambio de información sean la bases de sus operaciones donde la interoperabilidad para contrarrestar las amenazas cibernéticas debe extenderse mas allá del campo militar dentro de un enfoque integral.

En este aspecto es importante contar con la participación de todos los actores y partes interesadas para mejorar las capacidades y crear vínculos eficientes de negociación que permitan alcanzar soluciones sustentables basado en la cooperación entre la OTAN, Estados extra OTAN, organizaciones internacionales y actores privados (OTAN, New Capstone Concept, 2010)

En definitiva, el nacimiento y evolución de Internet, modificó no solo las características de la sociedad global, sino también las amenazas surgidas como consecuencia de su uso público y masivo. Esta situación motivó acciones por parte de la OTAN que presentan vínculos razonablemente sólidos con lo previsto en el marco teórico que guía este TFG.

A partir del aprendizaje resultante de los ciberataques, la configuración de una nueva dimensión de la seguridad, conocida como ciberseguridad, condujo los Estados miembros de la OTAN a reconocer intereses mutuos sobre esta cuestión.

El peligro que representaban los ciberataques tanto para la OTAN como institución, como para la seguridad nacional de los Estados miembros, los motivó a comenzar a desarrollar nuevas estrategias y políticas cooperativas en ciberseguridad basadas en intercambio de información y mecanismos de coordinación en el marco de una estructura institucional.

A su vez, el carácter transnacional del ciberespacio dentro del cual tienen especial importancia el accionar de los actores no estatales, favorece relaciones que se configuran en términos de complejidad. Este fenómeno implica para la OTAN la necesaria participación de múltiples actores y obliga a repensar sus estrategias de seguridad desde una perspectiva que excluye, en principio, a las acciones militares.

Ciberespacio y Ciberatacantes

En lo concerniente al ámbito del ciberespacio, ¿a qué tipo de amenazas hace referencia la OTAN? El ciberespacio no es físico sino virtual y es mucho más amplio que Internet. Es un entorno transnacional formado por redes de computadoras y por todo lo que éstas conectan y controlan. En este contexto, la OTAN y todos los actores que conforman la sociedad contemporánea, dependen de la seguridad en el ciberespacio.

Por ejemplo, la OTAN como organización, tiene 30 redes principales de comunicación y más de 100.000 computadoras personales. La estructuras de Internet son también cruciales para los Estados miembros, ya que sus sociedades y economías dependen de ellas (Hegenbart, 2014)

En consonancia con su naturaleza, el ciberespacio es funcional a los flujos de información, es así que para la OTAN, "el entorno de información se define como el espacio virtual y físico en el que se recibe la información, se procesa y es transportada. Consiste en la información misma y en los sistemas de información" (NATO, Allied joint Doctrine for informations operations AJP-3.10, 2009)

Según Ottis y Lorents, (2010), considerado desde la perspectiva de la OTAN el ciberespacio puede ser definido como un conjunto temporal-dependiente de sistemas de información interconectados y de usuarios humanos que interactúan con esos sistemas.

La idea de temporalidad significa que usuarios y conexiones pueden aparecer o desaparecer y la que información se modifica continuamente. En el ciberespacio los cambios importantes pueden tener lugar en tiempo extremadamente corto.

Por ejemplo, una *malware* puede replicar e infectar con precisión gran parte de la red global en cuestión de minutos. Por esto, en el ámbito de la OTAN, la noción de temporalidad es relevante debido a las implicaciones que tienen para el despliegue rápido de acciones ofensivas/defensivas, la factibilidad de un mapeo permanente del ciberespacio y la necesidad de reconocimientos constantes (Ottis y Lorents, 2010).

Al mismo tiempo, la expansión geométrica del ciberespacio, tanto en volumen como en operaciones, implicó un aumento de las actividades ilícitas cometidas en ella traducidas en el robo de información sensible, el bloqueo de redes informáticas y el espionaje con

el objetivo de sacar ventajas sobre competidores que afecta la soberanía y seguridad de los Estados (Lejarza Illaro, 2014).

Se debe tener en cuenta que en la era digital son otras las reglas que gobiernan. Los ataques digitales son no violentos en estricto sentido militar, tienen un coste relativamente bajo y se ejecutan exclusivamente en forma electrónica a través de la red.

Un ataque de este tipo proviene de un enemigo invisible ya que es difícil de identificar; es asimétrico debido a que es complicado evaluar su amplitud, y sus consecuencias podrían ser desastrosas para la población y la economía. Incluso, actores estatales o no estatales podrían efectuar ataques bajo *bandera falsa* haciéndose pasar por otros países con resultados difíciles de imaginar (Wegener, 2013).

Por estas razones, la invisibilidad y la asimetría provocan, llegado el caso, dudas sobre la proporcionalidad de las respuestas (Lejarza, Illaro, 2014). De ahí que, la extrema dependencia que tiene la actual Sociedad de la Información en las redes explica las motivaciones de los ataques digitales. Para un mejor entendimiento del fenómeno, tanto los ataques, como el perfil y la motivación de los atacantes pueden ser categorizados.

En su informe para la NATO Defense College, Hegenbart (2014), señala que se pueden distinguir seis perfiles de atacantes:

- *Ciberactivistas y Cibervandálicos:* el ciberactivismo describe a grupos independientes antisistema que buscan explotar las vulnerabilidades en las redes mediante técnicas específicas como medio de protesta y con fines políticos. En cambio, el cibervandalismo es motivado por la curiosidad y el deseo por la autoafirmación, no por la agenda política.

- *Cibercriminales:* motivados por las ganancias financieras utilizan el ciberespacio para promocionar sus actividades ilegales, en ocasiones sobre una base organizada. Sus operaciones cubren un amplio rango, por ejemplo, robos de identidad o estafas con tarjetas de crédito.

- *Ciberespionaje:* protagonizado por compañías o Estados mediante técnicas sofisticadas. Debe distinguirse espionaje económico del espionaje político o militar. El primero involucra información de negocios o propiedad intelectual, mientras que en el

segundo caso, el objetivo es capturar información clasificada y estratégica afectando los niveles de seguridad estatal.

- *Cibersaboteadores:* Nuevamente es necesario distinguir entre sabotaje económico del político o militar. Los límites entre ciberespionaje y cibersabotaje generalmente son borrosos ya que suelen estar involucrados los mismos actores, siendo el cibersabotaje una consecuencia de vulnerabilidades identificadas mediante el ciberespionaje. El cibersabotaje atenta directamente contra la integridad económica, política o militar de un Estado dañando equipamiento o información.

- *Ciberterroristas*: Utilizan el ciberespacio para llamar la atención, promover sus actividades o reclutar miembros. También pueden llevar a cabo potenciales ataques poniendo en peligro personas y propiedades.

- *Ciberejércitos*: con una estructura, nivel de sofisticación y capacidad financiera muy superior a los atacantes corrientes. Generalmente patrocinados por Estados, pueden utilizar técnicas avanzadas para dañar, destruir o interrumpir objetivos militares, sistemas de comunicación o infraestructuras de otro Estado.

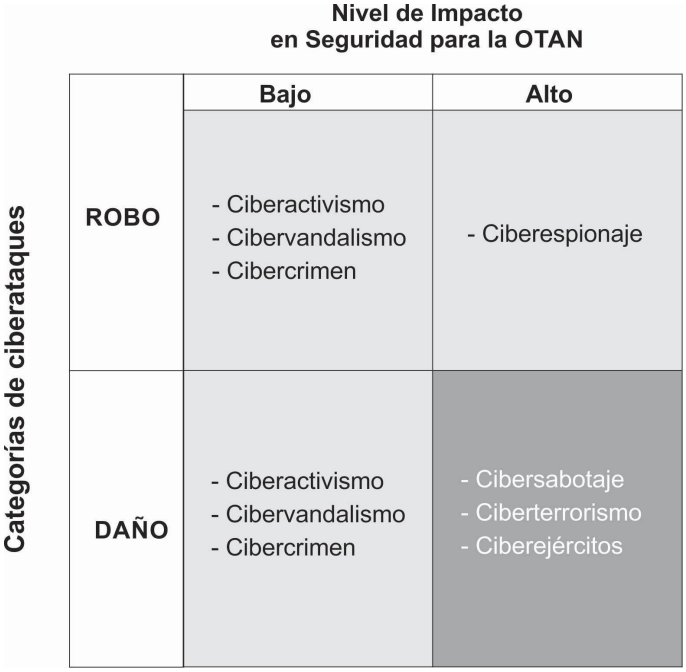
Según Hegenbart (2014) siguiendo estos perfiles y considerando los objetivos y mandatos de la OTAN, el ciberespionaje, el cibersabotaje y los ciberejércitos son altas prioridades para la organización debido al impacto que tienen en la seguridad y en la economía de los Estados.

Desde estos conceptos, el ciberespionaje se ubica en una posición importante a causa del daño indirecto y las derivaciones que puede llegar a provocar. Por un lado, el vínculo con el cibersabotaje es fluido y, por el otro, la información robada puede ser utilizada por ciberterroristas o ciberejércitos para efectuar operaciones masivas.

En consecuencia, la OTAN coloca al ciberespionaje como una de sus prioridades en ciberseguridad, prestando particular atención a las asociaciones que pueda establecer con estas tres últimas categorías siendo una tarea que se debe planificar desde la organización y con los Estados miembros (Hegenbart, 2014)

El modelo se puede esquematizar de este modo:

Figura 3



Fuente: Hegenbart (2014)

En esta línea, Calvo (2013) señala que las ciberamenazas han ido modificando su *modus operandi* en un período de 35 años, identificando 4 etapas:

- *1980 al 2000:* ataques benignos, realizados por hackers movilizados por la curiosidad.

- *2000 al 2005:* etapa protagonizada por *script kiddies* o personas inexpertas, que sin objetivos claros buscaban ser famosas utilizando herramientas informáticas elaboradas por otros.

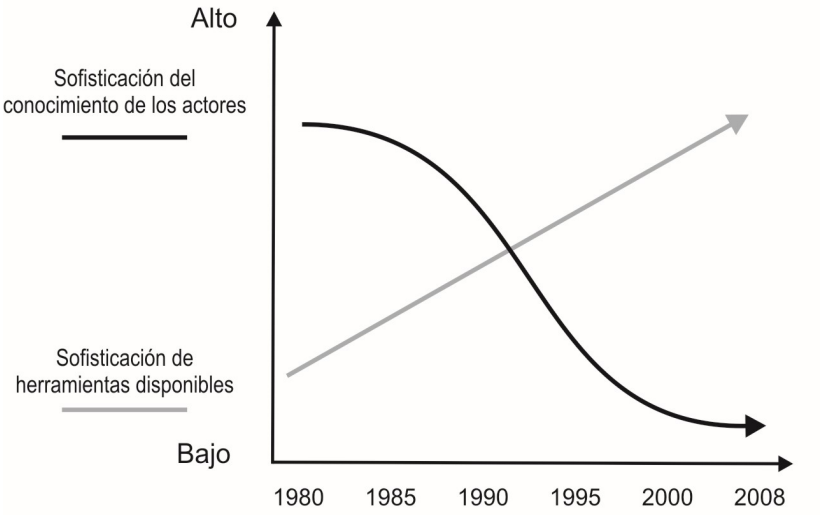
- *2005 al 2010:* aparecen los cibercriminales utilizando nuevas técnicas para fines comerciales.

- *2010 a la actualidad*: evoluciona el perfil del actor hostil que comprende a profesionales, equipos de ciberguerra o hacktivistas movilizados por motivos políticos o estratégicos.

Según Calvo (2013), actualmente es muy sencillo y simple generar un ataque cibernético masivo subcontratando o alquilando las herramientas necesarias que existen.

Por lo tanto, el nivel de conocimiento y la capacidad para llevarlos a cabo evolucionaron en forma inversa al nivel de sofisticación de los ataques (figura 4).

Figura 4



Fuente: Elaboración Propia en base a NATO Review Magazine (2016)

Ante este escenario, para Calvo (2013) es imprescindible y necesario compartir información. La red global es tan grande y con tantos capilares que es imposible que un solo actor pueda vigilarla y controlarla enteramente, destacando que la información debe ser mutuamente compartida.

Naturalmente, este proceso será ejecutado teniendo en cuenta los intereses nacionales en cuanto a la información intercambiada, pero debe ser una tarea casi supranacional, coordinada y cooperativa en la que deben intervenir tanto el sector público como el privado. En concreto, para Calvo (2013) es imprescindible compartir la información ya que en la mayoría de los casos los actores no podrán defenderse en solitario ni tampoco tendrán todo el conocimiento de lo que está sucediendo.

Es interesante destacar como Calvo al analizar la problemática de las ciberamenazas, coloca sobre la mesa los postulados teóricos del Institucionalismo Neoliberal. Claramente se pueden visualizar la idea de costos de transacción; los mutuos beneficios al compartir información; considerar la importancia de los intereses nacionales; la necesidad de afrontar las amenazas de manera global, coordinada y cooperativa con

otros actores internacionales del sector público/privado; y la magnitud que alcanzaron los actores no estatales.

La OTAN y las Ciberarmas

Conforme a lo examinado hasta el momento, los cambios tecnológicos y el uso de las ciberarmas comenzaron a constituir para la OTAN un asunto serio y de especial importancia. Como se dijo, éstas por naturaleza tienen características particulares dentro de un contexto de asimetría e invisibilidad y son diseñadas para causar daño tanto físico como funcional en objetivos civiles y militares (Hegenbart, 2014).

En este sentido la OTAN ha señalado:

> "Las amenazas cibernéticas trascienden las fronteras estatales y las fronteras organizacionales. Sus vulnerabilidades y riesgos son compartidos por todos. Reconociendo la naturaleza verdaderamente global del ciberespacio y sus amenazas asociadas, la OTAN y los Aliados trabajarán con los socios, las organizaciones internacionales, el mundo académico y el sector privado de manera que promueva la complementariedad y evite la duplicación. La OTAN adaptará su compromiso internacional basado en valores compartidos y enfoques comunes. La cooperación en el ámbito de la ciberseguridad podría abarcar actividades como la sensibilización y el intercambio de mejores prácticas" (OTAN, 2011, p. 1)

En efecto, claramente el ciberespacio y las amenazas cibernéticas derivadas de su utilización han configurado una nueva dimensión en el ámbito de la seguridad internacional para la OTAN. Como puede verse, la organización reconoce el carácter transnacional de las amenazas cibernéticas y la necesidad de trabajar en forma cooperativa y complementaria con otras organizaciones internacionales, la academia y el sector privado basándose en intereses comunes.

Al respecto, a partir de esta concepción en cuanto a la ciberseguridad, las mayores preocupaciones de la OTAN empezaron focalizarse en la defensa de las *infraestructuras críticas*.

De acuerdo a Wegener (2013), se entiende por infraestructura crítica a un conjunto de recursos y servicios esenciales que constituyen las bases para el funcionamiento de la sociedad y que en el actual contexto de globalización e interconexión son los primeros en la lista de objetivos de un ataque cibernético.

En sentido amplio, comprenden los sistemas de energía, telecomunicaciones, salud, transporte, finanzas y producción, dentro de los cuales, al sector energético se lo considera como el más vulnerable. Esta concepción, revalida en términos del Institucionalismo Neoliberal, la idea de ausencia de jerarquía de los temas que forman parte de las prioridades de los Estados y que las mismas están articuladas dentro de una amplia agenda que excede a los asuntos estrictamente militares.

Sobre este último punto, a modo de ejemplo, es conveniente destacar dos hechos que ponen en perspectiva la gravedad del tema, grafican la vulnerabilidad a la que están expuestos los Estados miembros de la OTAN y abren la posibilidad de ubicarlos dentro del modelo propuesto por Hegenbart (2014) que sigue la secuencia *cibespionaje-cibersabotaje-ciberguerra.*

En 1982, Ronald Reagan, presidente de Estados Unidos, aprobó un plan de la CIA que consistía en permitir que los rusos robasen un tipo de software utilizado para gestionar el funcionamiento de gasoductos. Tal como fue planeado, el software fue posteriormente robado por los rusos en Canadá y tenía incorporada una bomba lógica diseñada para que en determinado momento y circunstancia, las velocidades de las bombas y los ajustes de las válvulas en los gasoductos no funcionen correctamente. El resultado fue una tremenda explosión no nuclear y el ataque, considerado como la primera utilización de ciberarmas, tuvo un enorme impacto económico y psicológico sobre la Unión Soviética (Schreier, 2015).

El segundo episodio que merece destacarse se produjo veintiocho años después, en 2010. Fue protagonizado por el troyano conocido como *Stuxnet.* El Stuxnet fue descripto por la OTAN como la transición desde el ciberespacio al espacio físico (Hegenbart, 2014). En conformidad con lo que se viene exponiendo, este nuevo agente se caracterizó por un bajo nivel de conocimiento para su filtración en los sistemas y un alto nivel de sofisticación en su funcionamiento.

El Stuxnet, definido por los expertos como un troyano y donde todos los indicios parecen conducir hacia Estados Unidos e Israel como sus creadores, estaba orientado a atacar los sistemas de software de Control de Supervisión y Adquisición de Datos (SCADA) desarrollado por la compañía alemana Siemens y necesario para el funcionamiento de las centrifugadoras de enriquecimiento de uranio en la planta iraní de Natanz.

El Stuxnet simplemente fue introducido a través de pendrives en los sistemas de Siemens, y una vez que estos fueron instalados en Irán, produjeron la destrucción de miles de centrifugadoras retrasando, según las estimaciones, el programa nuclear iraní en aproximadamente dos años (Wegener, 2013).

Estos dos episodios, por un lado demuestran la evolución, la sofisticación y el poder destructivo de las ciberarmas a lo largo del tiempo, y por el otro, la tremenda potencialidad que pueden llegar a adquirir con el paso del tiempo convirtiéndose en recursos alternativos a los ataques militares convencionales. Incluso, posibilitarían a los Estados que tienen supremacía tecnológica, aprovechar de su posición para introducir en forma deliberada tecnología capaz de controlar los sistemas críticos de terceros Estados, o mantenerlas en estado latente para ser activadas luego en caso de conflicto (Salvador Carrasco, 2014).

En pocas palabras, el avance tecnológico dentro del mundo globalizado, que se podría denominar *Internet-dependiente,* comenzó a modificar la naturaleza de las amenazas hacia la seguridad de los Estados. Si bien el campo de acción de estas amenazas es bastante amplio, existe una creciente preocupación en relación a los potenciales daños que pudieran afectar a las denominadas infraestructuras críticas, un área muy sensible especialmente en el sector energético, hacia donde la OTAN comenzó a centrar su atención.

La OTAN y las infraestructuras críticas

El interés en el ámbito de la OTAN por el concepto de Protección de las Infraestructuras Críticas (PIC) comenzó a estudiarse con seriedad en 2001, luego del 11/9, con una revisión del nivel de preparación y la elaboración de una estrategia de acción (Jopling, Asamblea Parlamentaria de la OTAN, 2007).

Sobre este aspecto, la OTAN ha subrayado el peligro de las ciberamenazas:

> Las tecnologías de la información y la comunicación constituyen una parte cada vez más importante de nuestras vidas, y muchos de estos sistemas, servicios y redes se han convertido en vitales para nuestras economías y sociedades. Aunque las autoridades gubernamentales han reconocido la grave amenaza teórica que representan los ataques cibernéticos sobre estas infraestructuras durante más de una década, los acontecimientos de los últimos dos años han subrayado la posible irrupción masiva de los ataques cibernéticos y la urgente necesidad de abordar este problema. En resumen, nuestras infraestructuras digitales se han convertido en activos nacionales estratégicos, y ahora están en riesgo. (Myrli, NATO Parliamentary Assembly, 2009, p. 1)

Este concepto será reafirmado en una publicación posterior de la OTAN, donde asegura que el escenario de la seguridad del siglo XXI ha cambiado notablemente. Las sociedades y economías modernas están interconectadas por redes, cables y las direcciones IP de las computadoras. Dependiendo cada vez más de los complejos sistemas críticos de comunicación e información, la OTAN debe adaptar y mejorar sus defensas para hacer frente a las nuevas amenazas (OTAN, 2011, p. 1).

Se puede advertir, que a partir de sus percepciones y preocupaciones respecto a la ciberseguridad, en estas declaraciones los Estados miembros de la OTAN manifiestan intereses mutuos y objetivos compartidos orientados a la protección de sus sistemas nacionales. Además, se enfatiza la necesidad de trabajar de manera conjunta y muestra en forma coherente los principios teóricos que guían a este estudio.

En la misma tónica, los líderes de la OTAN reconocieron que la interrupción de las infraestructuras críticas como consecuencia de un ciberataque puede afectar la seguridad

nacional, por lo tanto declararon la necesidad de llevar adelante esfuerzos coordinados para evaluar los riesgos y aumentar la seguridad de las mismas (Acosta et al, 2009).

Como señala el reporte de la Asamblea Parlamentaria de la OTAN de 2007 la globalización ha conducido a una creciente interdependencia e interconexión de las redes en sectores fundamentales como comunicaciones, transporte, energía e información aumentando la vulnerabilidad de cada una de esas infraestructuras.

En este contexto, son partes interesadas tanto el sector público como el privado, por lo tanto el intercambio eficiente de información es necesario y sólo ocurrirá si las reglas apropiadas aseguran que la información intercambiada se da en un modo completamente seguro. Además, la OTAN considera a la información y comunicación como dos de los sectores estratégicos que necesitan mayor protección contra potenciales amenazas desconocidas acción (Jopling, Asamblea Parlamentaria de la OTAN, 2007).

Asimismo, de acuerdo al reporte de la OTAN, el amplio alcance de la las redes digitales en las sociedades modernas implica que virtualmente cualquiera puede convertirse en blanco potencial de un ciberincidente. En segundo lugar, involucra un número infinito de grupos de interés, por lo tanto es este sector más que en cualquier otro es donde los esfuerzos nacionales deben ser complementados por la cooperación multilateral.

Si bien el reporte de la OTAN indica que los masivos y coordinados ciberataques contra Estonia afortunadamente no resultaron en consecuencias severas, constituyeron una señal de alarma acerca del potencial efecto destructivo que pueden llegar a alcanzar y la necesidad de la OTAN de comenzar a elaborar una nueva estrategia de defensa para el sector.

De modo que la nueva estrategia deberá basarse en tres pilares: intercambio de información entre los gobiernos y el sector privado, construcción de un marco jurídico-legal contra el cibercrimen, y por último desarrollo e intensificación de la cooperación internacional (Jopling, Asamblea Parlamentaria de la OTAN, 2007).

Claramente, estas estrategias reafirman el carácter transnacional del ciberespacio, la múltiple convergencia de actores estatales/no estatales y la necesidad de abordar sus desafíos en forma conjunta entre la OTAN y los demás agentes del sistema internacional.

Simultáneamente, como señala Efthymiopoulos (2009), ante las nuevas circunstancias el Comité Militar de la OTAN definió lo que pasó a llamar el *Concepto de Ciberdefensa*. El objetivo del concepto era ofrecer resultados prácticos que mostrasen, por un lado, a la OTAN como una organización colectiva en un mundo globalizado e inseguro y, por el otro, que reflejasen la capacidad de la organización para ofrecer nuevos resultados en sus políticas teniendo en cuenta nuevas formas de amenazas asimétricas.

Aunque por cuestiones de seguridad los detalles exactos del Concepto de Ciberdefensa permanecen clasificados, de acuerdo a lo publicado oficialmente por la Asamblea Parlamentaria de la OTAN en su Reporte Anual de 2009, estos tenían como propósitos fundamentales:

- Proveer para la organización conceptos y doctrinas relacionadas en materia cibernética;

- Organizar y conducir talleres de entrenamiento, cursos y ejercicios entre los Estados miembros;

- Conducir actividades de investigación y desarrollo;

- Estudiar los ataques pasados y los actuales para aprender de las experiencias;

- Brindar asesoramiento a los Estados miembros si es requerido en el curso de un ciberataque.

En este marco, la aplicación de una política en materia de ciberdefensa, se consideró como la segunda más importante de la OTAN en materia de seguridad. Esta visión impulsó a la OTAN a destinar importantes recursos para llevar adelante estudios e investigaciones que permitiesen a la organización adoptar las políticas apropiadas en consonancia con los nuevos desafíos, focalizando la importancia de las ciberinfraestructuras (Efthymiopoulos, 2009).

El resultado de una de estas investigaciones fue el Manual del Marco de Seguridad Nacional Cibernética publicado por la OTAN como guías de acción para sus Estados miembros, elaborado en el marco del Programa de Ciencia y Paz para la Seguridad de la OTAN.

En principio, el documento expresaba que todos los Estados miembros de la OTAN debían enfrentarse con el hecho de que su dependencia del ciberespacio era una vulnerabilidad importante y que era un imperativo invertir y trabajar para disminuir las vulnerabilidades y evitar un deterioro de las defensas globales. Por lo tanto, la OTAN, las organizaciones internacionales, y actores no estatales que operaban en el ciberespacio, se exponían a riesgos conocidos y desconocidos.

Los trabajos en el área incluían el diseño institucional, la adquisición de capacidades y la administración y control de los elementos y actividades asignadas por la OTAN en el sector. En consecuencia, era un gran desafío con riesgos operacionales, logísticos, económicos, políticos, técnicos, ambientales y de reputación (Ekstedt, Parkhouse, y Clemente, 2012).

En este sentido, Luiijf y Healey (2012) proponen que se deben considerar cinco mandatos y seis elementos para un modelo integral para la protección de ciberinfraestructuras de los Estados de la OTAN.

Si se observa el modelo de Luiijf y Healey (2012), el mismo utiliza una concepción amplia de la seguridad, en el sentido de que el mandato de las operaciones militares está contemplado dentro de los límites del ciberespacio.

Asimismo, la propuesta dispone de otros cinco mandatos que implican necesariamente la participación del sector público y privado, a través de la gobernanza de internet, la diplomacia y el derecho internacional contra el cibercrimen. En suma, es una muestra más de la complejidad que deben asumir las respuestas a los nuevos desafíos que presenta el sistema internacional a los Estados miembros de la OTAN.

Luiijf y Healey (2012), esquematizan el modelo completo de la siguiente manera:

Figura 5

	PROACCIÓN	PREVENCION	PREPARACIÓN	RESPUESTA	RECUPERACIÓN	MANTENIMIENTO/ SEGUIMIENTO
Gobernanza de Internet/ Ciberdiplomacia	PROACCIÓN	PREVENCION	PREPARACIÓN	RESPUESTA	RECUPERACIÓN	MANTENIMIENTO/ SEGUIMIENTO
Gestión de Crisis y			PREPARACIÓN	RESPUESTA	RECUPERACIÓN	MANTENIMIENTO/ SEGUIMIENTO
Protección de Infraestructuras Críticas		PREVENCION	PREPARACIÓN	RESPUESTA	RECUPERACIÓN	MANTENIMIENTO/ SEGUIMIENTO
Operaciones Cibermilitares		PREVENCION	PREPARACIÓN	RESPUESTA	RECUPERACIÓN	
Inteligencia y Contrainteligencia		PREVENCION		RESPUESTA		MANTENIMIENTO/ SEGUIMIENTO
Contracibercrimen	PROACCIÓN	PREVENCION	PREPARACIÓN	RESPUESTA	RECUPERACIÓN	MANTENIMIENTO/ SEGUIMIENTO

Fuente: Luiijf y Healey(2012)

No obstante, para implementar el modelo se deberán tener en cuenta tensiones y conflictos de interés. Hathaway y Klimburg (2012) señalan que una de las claves es lograr un equilibrio entre sectores sensibles tanto del sector público como del privado de los Estados miembros.

Al respecto, es posible identificar las tensiones previstas por Aronson (2009) en cuanto a los conflictos que se pueden suscitar respecto a la propiedad intelectual, el acceso al desarrollo tecnológico y las presiones de los grupos interesados.

Hathaway y Klimburg (2012) subrayan las presiones de los grupos económicos que impulsan la modernización y la apertura de las infraestructuras frente a las fuerzas de sectores que demandan protección de esas mismas infraestructuras; a los defensores de la protección de la información frente a los del libre intercambio de información; y a los garantes la libertad de expresión frente a los que hacen hincapié en la estabilidad política.

Adicionalmente, se debe tener en cuenta que todos estos sectores se benefician de las continuas innovaciones, por ejemplo, acceso a banda ancha y dispositivos que comprenden un cada vez mayor y heterogéneo número de hardware y software

utilizados a través de diferentes mecanismos, complejizando aún más el debate y las presiones (Hathaway y Klimburg 2012).

Sin embargo, en un mundo globalizado e interconectado la ciberseguridad nunca es nacional en sentido estricto. Requiere la cooperación a nivel internacional de una amplia variedad de actores internacionales que debe ser apreciada en su complejidad y que incluye a Estados, organizaciones internacionales y actores no estatales (Luiijf y Healey, 2012).

Reforzando este concepto, los miembros de la OTAN están dejando cada vez más en claro que las agendas de ciberseguridad, tanto nacional como colectiva, están profundamente vinculadas.

Como resultado, las estrategias de ciberseguridad de la OTAN para la protección de las infraestructuras críticas se inscribieron dentro del *Proceso de Planificación de la Defensa de la OTAN* (NDPP, por sus siglas en inglés) adoptado por los Estados miembros de la OTAN. Esta es una de las herramientas más importantes de la organización en el intento de facilitar a los Estados miembros el acceso a una serie de recursos que los beneficien mediante el trabajo cooperativo.

Esencialmente, el NDPP tiene como meta evitar la renacionalización de las políticas de defensa preservando al mismo tiempo los derechos soberanos de los Estados miembros. Además promueve y facilita el enfoque común y amplio de la Organización para el desarrollo de capacidades de defensa cibernética y define objetivos para la implementación de capacidades nacionales de defensa cibernética de los Estados miembros (NATO Encyclopedia, 2015).

De acuerdo a nuestro marco teórico y en términos de Martín y Simmons (1998), la NDPP de la OTAN se focaliza en los *efectos convergentes* donde políticas institucionalizadas facilitan la conducta de los Estados miembros adoptando similares prácticas en ciberdefensa minimizando los *efectos divergentes* producto de prácticas preexistentes.

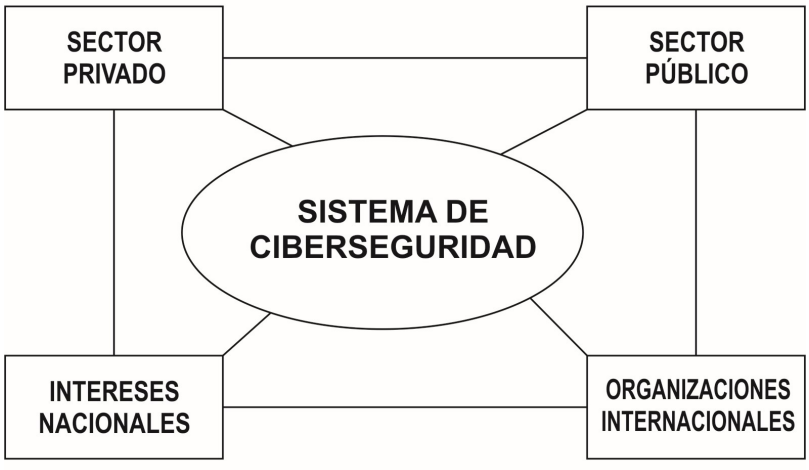
En este marco, el NDPP, se compone de una serie de pasos, instituciones y comités de apoyo donde uno de los aspectos más importantes es el *reparto de la carga,* en alusión a los aportes que deben destinar los Estados miembros para la construcción de la infraestructura para la ciberdefensa.

En este sentido, desde el NDPP se asume que un completo sistema de ciberseguridad incluye el comportamiento de terceros Estados, por lo tanto su logro depende completamente de la cooperación internacional y de la creación de marcos normativos internacionales sobre seguridad cibernética (Ekstedt, Parkhouse, y Clemente, 2012).

En consecuencia, dado que la mayor parte de la infraestructura del ciberespacio es de propiedad privada, se infiere que la OTAN deberá asignar fondos para la financiación directa de ciberinfraestructura. Asimismo, orientar sus políticas para establecer vínculos basados en intereses mutuos donde converjan lo público, lo privado, los intereses nacionales y la cooperación internacional, en un sistema que se podría denominar *Modelo Transnacional en Ciberseguridad* (figura 6).

Figura 6

Modelo Transnacional en Ciberseguridad



Fuente: Elaboración Propia

Ahora bien, el análisis de los sucesos y acciones descriptas hasta el momento exponen una serie de elementos que pueden ser constatados con los previstos en el marco teórico del TFG.

En primer lugar, los Estados miembros de la OTAN evidentemente interactúan en un sistema internacional complejo e interdependiente en extremo. Es un contexto de relaciones transnacionales crecientes, potenciadas por las nuevas tecnologías en comunicación e información. Estas relaciones involucran múltiples canales de conexión en las tienen un protagonismo cada vez mayor los actores no estatales de identidad difusa.

Es decir, existen espacios de acción autónoma que escapan al control estatal dejando vacíos y vulnerabilidades que pueden ser explotadas sin necesidad de movilidad física. En los sucesos de Estonia estos factores actuaron y facilitaron el éxito del ciberataque dejando de manifiesto su factibilidad.

De esta manera, dentro de las nuevas dimensiones al concepto de seguridad que la post Guerra Fría y el 11-S sumaron al sistema internacional, los ciberataques pasaron a conformar un dominio propio.

El hecho de que un Estado como Estonia se vea inmovilizado en su funcionamiento a raíz de una agresión cibernética y proveniente de actores no estatales de identidad difusa, demuestra como en el actual sistema internacional las capacidades materiales no siempre se muestran eficaces en un conflicto de relación asimétrica.

Si se examinan detenidamente los acontecimientos, se observa que la OTAN se mostró sorprendida y en cierto modo fue sobrepasada por la situación, por lo que tuvo una conducta netamente reactiva y necesitó de ayuda de la cooperación de países extra-OTAN, como por ejemplo Finlandia, para contener el ataque.

En otras palabras, la cooperación entre Estados se mostró como una herramienta eficaz al servicio de un Estado en problemas. Como lo señala la OTAN, "…los ataques demostraron la necesidad de una política de defensa cibernética que también abordaría la necesidad de cooperar para proteger los sistemas críticos de comunicación más allá de las redes de la OTAN" (Myrli, NATO Parliamentary Assembly, 2009, p.2).

Por lo tanto, está claro que la agenda global es amplia e involucra una variedad de temas. Los ciberataques en Estonia motivaron una seria reacción de la OTAN para revisar sus políticas de seguridad. Esto es particularmente importante si se tiene en cuenta que la OTAN fue creada en un contexto totalmente diferente y desde una óptica exclusiva de fuerza militar y protagonismo estatal. Las problemáticas mundiales ya no se presentan en forma lineal y mecánica para la OTAN y no todas las soluciones pasan por la respuesta armada.

Es evidente, que las demandas no son estáticas, están en continua transformación y es esta dinámica la que impulsó a los Estados miembros de la OTAN a reconsiderar sus políticas de seguridad incluyendo la dimensión del ciberespacio.

Asimismo, el análisis del caso muestra que el aprendizaje fue el punto de partida desde el cual los Estados miembros de la OTAN comenzaron a desandar el camino de la ciberseguridad.

Como acertadamente señalaba Nye (1987), el aprendizaje se presentó en términos de complejidad impulsando a los Estados miembros de la OTAN a trabajar en forma conjunta para afrontar el desafío. De acuerdo al reporte de la Asamblea Parlamentaria de OTAN (2007), siete semanas luego del ataque cibernético contra Estonia, expertos de la OTAN confeccionaron un informe sobre las lecciones aprendidas que proporcionaba el marco para la futura labor necesaria en el ámbito de la ciberdefensa.

El informe recomendó funciones específicas y la aplicación de una serie de nuevas medidas destinadas a mejorar la protección contra los ciberataques. Además evaluó minuciosamente el enfoque de la OTAN en materia de ciberdefensa. (Myrli, NATO Parliamentary Assembly, 2009, p.6).

En otras palabras, desde el aprendizaje de los hechos se redefinieron los intereses de los Estados miembros de la OTAN en función de sus intereses mutuos. En términos de la OTAN:

> Los Aliados de la OTAN comparten un amplio consenso político tanto sobre la gravedad de las amenazas cibernéticas como sobre el posible papel valioso de la OTAN en este ámbito. Esto permitió un rápido acuerdo

> sobre una Política de la OTAN sobre la Ciberdefensa, que actualmente está siendo implementada por los cuerpos militares y técnicos pertinentes de la Alianza y los Aliados individuales. (Myrli, NATO Parliamentary Assembly, 2009, p.1).

De igual modo, el propósito del informe fue proporcionar a los Estados miembros información confiable sobre las amenazas provenientes de los ataques cibernéticos, así como las respuestas apropiadas (Myrli, NATO Parliamentary Assembly, 2009, p.2).

En síntesis, se puede afirmar que la progresiva complejidad que el sistema internacional fue adquiriendo en las últimas décadas incluyó el accionar de actores no estatales como elementos desestabilizantes de la seguridad estatal.

Ante este escenario, los ciberataques fueron receptados por los Estados miembros de la OTAN como una nueva dimensión de la seguridad que desencadenó la formación de intereses compartidos, a partir de la cuales, se comenzó a considerar su abordaje desde el aprendizaje, la información compartida y la cooperación.

Conclusiones Preliminares

Lo expuesto hasta aquí lleva a la conclusión de que la globalización e informatización de la sociedad condujo al nacimiento de la Sociedad de la Información caracterizada por una fuerte dependencia de las redes digitales en una situación que podría definirse como de Internet-dependiente.

Sin embargo, la geométrica expansión de la red global también llevó al surgimiento de amenazas derivadas de su uso. Estas amenazas fueron evolucionando en el transcurso del tiempo, a tal punto, que pueden llegar a afectar considerablemente la seguridad de los Estados especialmente atacando sus infraestructuras críticas. En otras palabras, nacía el ciberespacio como nueva dimensión de la seguridad.

En este contexto, tanto la OTAN considerada desde el punto de vista funcional, así como sus Estados miembros y las sociedades que involucran, dependen de la seguridad cibernética.

Como consecuencia de la creciente vulnerabilidad de los sistemas digitales y de hechos concretos, como por ejemplo el ciberataque a Estonia, los Estados miembros de la OTAN identificaron intereses mutuos y comenzaron a construir toda política cooperativa en ciberdefensa que implica superar una serie de desafíos y tensiones tanto desde lo técnico como desde lo económico y político.

Estas actividades conllevan a la participación del sector público y el privado, manifestando por una parte, el carácter transnacional y heterogéneo del sistema internacional, y por el otro, la necesidad de preservar los intereses nacionales en el ámbito de la cooperación internacional.

Por lo tanto, en el siguiente capítulo se analizarán de qué manera la OTAN afrontó estos desafíos y transformó los conceptos y directrices en políticas comunes, agencias e instituciones concretas.

CAPÍTULO 3

Las políticas en ciberseguridad de la OTAN

Las Cumbres de la OTAN y los primeros pasos en ciberseguridad

Como se ha visto en el Capítulo 1, en las cumbres de Praga 2002 y Riga 2006, la OTAN esbozó, aunque superficialmente, los primeros lineamientos de una política en ciberseguridad cuyo resultado más importante fue la creación del NCIRC. Sin embargo, esta política se caracterizó por su pasividad y en cierta manera fue estática en cuanto a la relevancia que se le adjudicaron a las amenazas provenientes del ciberespacio.

Posteriormente, los masivos ciberataques ocurridos de Estonia en 2007 demostraron, por una parte, la limitación de estas políticas y la escasa capacidad operativa del NCIRC y, por la otra, provocaron en los Estados miembros de la OTAN la identificación de intereses mutuos y un auténtico llamado a la acción que condujo a que los Estados miembros trabajasen en forma urgente y conjunta en esta nueva dimensión de la seguridad que hasta ese momento había sido postergada.

En este contexto, la OTAN realizó un estudio del caso y confeccionó un informe con las lecciones aprendidas llamado *Informe del examen de las lecciones aprendidas de los recientes ataques cibernéticos* (Artiles, 2011). En otras palabras, desde el aprendizaje los Estados miembros coincidieron en identificar un nuevo tipo de amenaza que motivó intereses comunes para enfrentarla.

En el Capítulo 2 se analizó cómo desde el surgimiento de las nuevas formas de amenaza derivadas del ciberespacio, la OTAN colocó dentro de sus máximas prioridades en sus políticas de ciberseguridad a las infraestructuras críticas, habida cuenta de la dependencia cada vez más profunda que éstas tienen de los sistemas informáticos. Al mismo tiempo, como se ha visto, se desarrollaron una serie de iniciativas y lineamientos para lo que serían las futuras políticas en el sector de la ciberseguridad.

Ahora bien, en este Capítulo se analizará de qué manera, desde el aprendizaje y los lineamientos basados en intereses comunes, se fueron construyendo las políticas concretas, las acciones y las instituciones en relación a la ciberseguridad. De esta manera, para analizar el camino recorrido por la OTAN en la construcción de sus

políticas en ciberseguridad, resulta de suma utilidad examinar los comunicados de sus cumbres (González, 2012).

En el marco de este TFG, se considera que las cumbres de la OTAN claves a analizar, en cuanto a los acuerdos logrados para aplicar en el campo de la ciberseguridad son Bucarest 2008, Lisboa 2010 y Chicago 2012. En cada una de ellas se realizaron aportes centrales y se constituyeron las guías esenciales para las nuevas políticas en ciberseguridad de la OTAN.

Como primera medida el 7 de enero de 2008 el Consejo de la OTAN adopta la Política en Ciberdefensa, que se basaba fundamentalmente en la mejora de las capacidades de defensa de sus sistemas informáticos (Artiles, 2011).

Esta política incluía el desarrollo del ya referido Concepto de Ciberdefensa, el cual define la protección de los sistemas informáticos de la OTAN como una responsabilidad esencial de los Estados miembros, enfatizando la necesidad de cooperar entre los socios y otros actores internacionales para fomentar e impulsar acciones que permitan establecer en forma urgente agencias y centros de investigación en ciberseguridad (Caro Bejarano, 2011).

Asimismo, asignaba roles y responsabilidades tanto para la OTAN como para los Estados miembros. La OTAN debía proteger sus propios sistemas TIC y los Estados miembros se convertían en responsables de las redes propias que manejaban información de la OTAN, coordinando sus acciones para proteger los sistemas mutuamente. En definitiva, los Estados miembro compartían responsabilidades disminuyendo el riesgo moral a través del monitoreo recíproco.

Al mismo tiempo, la Política en Ciberdefensa establecía que si un Estado miembro era blanco de un ciberataque que pusiera en riesgo su seguridad nacional, la OTAN debía estar preparada, a petición, para prestar auxilio (Acosta et al., 2009).

En otras palabras, los objetivos centrales en ciberseguridad de la OTAN desde esta política inicial, se situaron en proteger sus propias redes; en la protección de las infraestructuras críticas que utilizan redes de datos e información; y en asistir como también defender a los Estados miembros en caso de ciberataque.

Es así que, la Política en Ciberdefensa estableció tres principios básicos a partir de los cuales se desarrollarían las futuras acciones en ciberseguridad (Theiler, 2011):

- *Subsidiariedad*: El hecho de que las políticas en ciberseguridad de la OTAN, en origen, estén focalizadas en sus propios sistemas y el principio de la soberanía estatal en cuanto a las propias responsabilidades de los Estados miembros sigue aplicando, no impide que la OTAN provea asistencia a un Estado miembro si la solicita en caso de sufrir un ciberataque masivo.

- *No Duplicación:* La OTAN debe prevenir e impedir una duplicación innecesaria de estructuras o capacidades a nivel nacional, regional o internacional.

- *Seguridad:* La cooperación basada en la confianza y el intercambio de información, teniendo en cuenta la sensibilidad de la información relacionada gestionada convenientemente garantizando el acceso a todos los Estados miembros.

La Cumbre de Bucarest 2008

A partir de la Política en Ciberdefensa adoptada, en la Cumbre de Bucarest de abril de 2008 los Estados miembros comenzaron a sentar las bases y directrices de una verdadera política en ciberseguridad. Inspirada en los ciberataques, la sección 47 de la Declaración de los Líderes de la Cumbre de Bucarest de la OTAN señala:

> La OTAN sigue comprometida con el fortalecimiento de los principales sistemas de información de la Alianza contra los ciberataques. Recientemente hemos adoptado una Política de Defensa Cibernética, y estamos desarrollando las estructuras y autoridades para llevarla a cabo. Nuestra Política de Ciberdefensa enfatiza la necesidad de que la OTAN y las naciones protejan los sistemas de información clave de acuerdo con sus respectivas responsabilidades, compartir las mejores prácticas, y proporcionar una capacidad para ayudar a las naciones aliadas, a petición, para contrarrestar un ataque cibernético. Esperamos con interés continuar con el desarrollo de las capacidades de defensa cibernética de la OTAN y reforzar los vínculos entre la OTAN y las autoridades nacionales. (OTAN Bucharest Summit Declaration, 2008)

Adicionalmente, la OTAN reafirmó su compromiso con el intercambio de información y la cooperación entre los Estados miembros. Como señala Hughes (2009), en la cumbre el concepto de Asociaciones Globales pasó a ocupar un lugar prominente en la agenda de la OTAN.

> (..) Seguiremos esforzándonos por promover una mayor interoperabilidad entre nuestras fuerzas y las de las naciones socias; para mejorar aún más el intercambio de información y las consultas con las naciones que contribuyen a las operaciones dirigidas por la OTAN; y ofrecer a los países socios asesoramiento y asistencia de la OTAN en los aspectos de la reforma relacionados con la defensa y la seguridad (OTAN Bucharest Summit Declaration, 2008).

En este sentido, la Cumbre de Bucarest proporcionó algunos de los elementos centrales de las futuras políticas y comenzó el proceso para centralizar las políticas de ciberseguridad a través de instituciones y agencias de la OTAN.

Como se desprende de la Declaración, entre estos elementos se destacan: enfatizar la protección de los sistemas de información clave; compartir las mejores prácticas para la ciberdefensa; desarrollar a petición, la capacidad para ayudar a los Estados miembros a contrarrestar un ataque cibernético; expandir las capacidades de defensa cibernética de la OTAN y fortalecer los vínculos entre la OTAN y las autoridades nacionales (Caton, 2016)

En otras palabras, en la Cumbre de Bucarest, se consolidaban las tres guías de acción que incluían medidas a adoptar por la propia OTAN; por los Estados miembros; y por ambas partes para aumentar la coordinación, intercambio de información y el apoyo mutuo (Caro Bejarano, 2011)

Como resultado, la OTAN estableció las dos mayores instituciones para mejorar las capacidades en ciberseguridad y reforzar al NCIRC: la *Autoridad de Gestión para la Ciberdefensa* (CDMA, por sus siglas en inglés) y el *Centro de Excelencia de Ciberdefensa Cooperativa* (CCDCOE, por sus siglas en inglés).

La CDMA , bajo la gobernanza del *Consejo de Gestión de la Ciberdefensa* (CDMB, por sus siglas en inglés), comenzó a operar en el mismo mes de abril de 2008 con la misión de coordinar las ciberdefensas, revisar las capacidades y llevar adelante un gestión apropiada de los riesgos en ciberseguridad y la ciberdefensa de todos los sistemas de la OTAN. Asimismo, prestar ayuda y colaboración a los Estados miembros, para mejorar sus propias capacidades nacionales en ciberdefensa (Healey y Bochoven, 2012).

De acuerdo a Artiles (2011), la creación de la CDMA probablemente fue en su momento el hito más trascendente en las políticas de ciberseguridad de la OTAN, al establecer una autoridad única con las responsabilidades y los recursos necesarios para coordinar las acciones en ciberdefensa ante un ataque, que estaba a disposición de los Estados miembros, y quienes puedían recurrir a ella en caso de ciberataque.

Como se mencionó, la CDMA gestionaría todas las cuestiones relativas a la ciberdefensa a través del CDMB que estaba constituido por el Consejo del Atlántico Norte, el Comité Militar, la autoridad de gestión política, las autoridades de emergencia política y civil y el Comité de Seguridad.

Específicamente, el objetivo de la CDMA se focalizaba en las amenazas cibernéticas; la valoración de las vulnerabilidades y la continuidad de los sistemas de información y comunicación (Artiles, 2011). Sin embargo, siguiendo el criterio de *No-duplicación* con posterioridad la OTAN decidió dar de baja al CDMA e integrarlo en el CDMB, siendo éste último organismo quien asumió la totalidad de sus funciones (Healey y Jordan, 2014)

La otra institución impulsada y creada desde la Cumbre de Bucarest fue Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE). El CCDCOE, ubicado en Tallin capital de Estonia, no tiene una función operativa en caso de ciberataque, pero realiza un trabajo complementario al del CDMB y el NCIRC, perfeccionando la cooperación y el intercambio de información (Healey y Van Bochoven, 2012).

El CCDCOE es una organización militar internacional acreditada por la OTAN que en su momento fue establecido por siete naciones: Estonia, Alemania, Italia, Lituania, Letonia, República Eslovaca y España, quienes firmaron el Memorándum de Entendimiento el 14 de mayo de 2008. El CCDCOE fue activado como Organización

Militar Internacional por la decisión del Consejo del Atlántico Norte de la OTAN en octubre de 2008 (NATO CCDCOE, 2016).

Con el paso del tiempo, se fueron incorporando más Estados a la institución, como por ejemplo, Hungría (2010), Polonia y Estados Unidos (2011); llegando al momento de realizar el presente TFG a 16 miembros. Como afirma el CCDCOE:

> El Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE de la OTAN) es un centro de investigación y capacitación acreditado por la OTAN que trata de la educación, la consulta, las lecciones aprendidas, la investigación y el desarrollo en el ámbito de la ciberseguridad. Cuenta con 16 Estados miembros de la OTAN patrocinantes y 2 participantes contribuyentes (Austria y Finlandia). El CCDCOE de la OTAN es financiado, dirigido y encargado por las Naciones Patrocinadoras, pero los servicios también son solicitados por la OTAN a través del Comando Aliado de la Transformación (…) (OTAN, CCDCOE, 2016)

Asimismo, el CCDCOE tiene por misión dar respuestas y soluciones a problemas concretos mediante el desarrollo de programas de investigación, formación y análisis de casos reales. Sus proyectos son abordados por equipos multidisciplinarios que involucran asuntos operativos, militares, tecnológicos y legales.

Tiene estatus legal de Organización Militar Internacional, que sin llegar a formar parte de la estructura formal de mando de la OTAN, está incorporado en la estructura organizativa de la ciberseguridad en la OTAN formando parte del CDMB y manteniendo un fluido e intenso vínculo con el NCIRC y la Ciberdefensa Activa (NATO ACT).

Del mismo modo, está obligado a considerar los pedidos de la OTAN con la máxima preferencia y lleva adelante una importante y estrecha cooperación con el sector privado y la academia (Artiles, 2011).

Es por esto que los acuerdos alcanzados en la Cumbre de Bucarest confirmaron al ciberespacio como una nueva dimensión de la seguridad y que las políticas en ciberseguridad de la OTAN se comenzaron a construir sobre la base del intercambio de

información, la ayuda recíproca, la cooperación, la participación del sector privado y la creación de un régimen institucionalizado para la gestión de crisis y amenazas.

La Cumbre de Lisboa 2010

La Cumbre de Lisboa de noviembre de 2010 significó un salto cualitativo en cuanto a las políticas de ciberseguridad de la OTAN. Utilizando términos informáticos, Theiler (2011) señala que si las políticas en ciberseguridad de la OTAN iniciadas en Praga 2002 comenzaron con la construcción de una *Ciberdefensa 1.0*, fue a partir de Lisboa 2010, donde se edificó y actualizó una *Ciberdefensa 2.0.*

Estos términos se afirmaron en la Declaración Oficial de la Cumbre de Lisboa, donde los Estados miembros manifiestan:

> Las amenazas cibernéticas están aumentando rápidamente y evolucionando en su sofisticación. Con el fin de garantizar el acceso permanente y sin restricciones de la OTAN al ciberespacio y la integridad de sus sistemas críticos, vamos a tener en cuenta la dimensión cibernética de los conflictos modernos en la doctrina de la OTAN y mejorar sus capacidades para detectar, evaluar, prevenir, defender y recuperar en caso de ciber ataque contra los sistemas de importancia crítica para la Alianza. Nos esforzaremos en particular para acelerar el equipo de Capacidad de Respuesta a Incidentes de la OTAN (NCIRC) a Plena Capacidad Operativa (FOC, *Full Operational Capability*) en 2012 y la reunión de todos los órganos de la OTAN bajo la protección cibernética centralizado. Vamos a utilizar los procesos de planificación de la defensa de la OTAN con el fin de promover el desarrollo de las capacidades de ciberdefensa de los aliados, para asistir a los Aliados a petición, y para optimizar el intercambio de información, la colaboración y la interoperabilidad. Para hacer frente a los riesgos de seguridad que emanan desde el ciberespacio, trabajaremos en estrecha colaboración con otros actores, tales como la ONU y la UE, según lo acordado. Hemos encomendado al Consejo que elabore, basándose sobre todo en las estructuras internacionales existentes y sobre la base de una revisión de nuestra política actual, una política de la

> OTAN ciberdefensa en profundidad antes de junio de 2011 y preparar un plan de acción para su aplicación (NATO, Lisboa Summit Declaration, 2010).

Por consiguiente, el elemento central de esta actualización y plan de acción fue la adopción y aprobación del nuevo *Concepto Estratégico* de la OTAN. Dentro de este concepto, la ciberdefensa pasó a ocupar un lugar mucho más amplio que en cualquier documento estratégico previo de la Organización. En el mismo, la OTAN reconoce que los ciberataques pueden afectar la seguridad nacional de los Estados miembros mediante el ataque a sus infraestructuras críticas y sus sistemas de redes informáticas, y por lo tanto, se tornaba esencial desarrollar y aumentar las habilidades y capacidades en el área del ciberespacio (Hegenbart, 2011)

Como resultado, la OTAN publicó un documento del nuevo Concepto Estratégico adoptado por la Organización. En la sección 12 del documento aprobado, los Estados miembros reconocen que:

> Los ataques cibernéticos son cada vez más frecuentes, organizados y más costosos en los daños que inflingen a las administraciones públicas, empresas, economías y potencialmente también al transporte, redes de suministro y otras infraestructuras críticas; pueden alcanzar un umbral que amenaza a la prosperidad, la seguridad y la estabilidad Euro-Atlántica. Los militares extranjeros y los servicios de inteligencia, criminales organizados, terroristas y / o grupos extremistas pueden ser cada uno de ellos la fuente de tales ataques (NATO Strategic Concept, 2010)

Asimismo en las secciones 13 y 14 del documento se afirma:

> Todos los países dependen cada vez más de las vías vitales de comunicación, transporte y tránsito que dependen del comercio internacional, la seguridad energética y la prosperidad. Estas requieren mayores esfuerzos internacionales para asegurar su resiliencia contra ataques o interrupciones. Algunos países de la OTAN dependerán más de los proveedores extranjeros de energía y, en algunos casos, de las redes extranjeras de suministro y distribución de energía para satisfacer sus

> necesidades energéticas. A medida que una mayor proporción del consumo mundial se transporta por todo el mundo, los suministros de energía están cada vez más expuestos a la interrupción. Una serie de importantes tendencias relacionadas con la tecnología -incluyendo el desarrollo de armas láser, la guerra electrónica y las tecnologías que impiden el acceso al espacio- parecen tener efectos mundiales importantes (…) (NATO Strategic Concept, 2010)

Esta idea se refuerza en la sección 19 que indica:

> Desarrollar aún más nuestra capacidad de prevenir, detectar, defenderse y recuperarse de los ataques cibernéticos, incluso utilizando el proceso de planificación de la OTAN para mejorar y coordinar las capacidades nacionales de ciberdefensa y de respuesta con los Estados miembros (NATO Strategic Concept, 2010)

Finalmente en las secciones 27 y 28 se sostiene que:

> La promoción de la seguridad Euro-Atlántica se garantiza mejor a través de una amplia red de relaciones con los países y organizaciones de todo el mundo. Estas asociaciones constituyen una contribución concreta y valiosa al éxito de las tareas fundamentales de la OTAN. El diálogo y la cooperación con los asociados pueden contribuir de manera concreta a mejorar la seguridad internacional, a defender los valores en los que se basa nuestra Alianza, a las operaciones de la OTAN y a preparar a las naciones interesadas para formar parte de la OTAN. Estas relaciones se basarán en la reciprocidad, el beneficio mutuo y el respeto mutuo (NATO Strategic Concept, 2010).

Para estos fines, el nuevo Concepto Estratégico continuaría focalizado en mejorar las capacidades defensivas reconociendo al mismo tiempo al ciberespacio como la dimensión de los futuros conflictos. Asimismo, a nivel operacional, la Cumbre Lisboa decidió la integración de la ciberdefensa dentro del NDPP, que fue antes analizado en el Capítulo 2, y comprometió a los Estados miembros para que revisen y mejoren sus

políticas en ciberseguridad evitando la renacionalización de sus políticas de ciberseguridad (Healey y Jordan, 2014).

De la lectura de ambos documentos resulta evidente que los Estados miembros de la OTAN, al momento de adoptar el nuevo Concepto Estratégico, enfatizaron una serie de elementos considerados esenciales desde la perspectiva adoptada en el marco del presente TFG. Por ejemplo, se pueden identificar términos tales como: el ciberespacio como nueva dimensión de la seguridad; la importancia del intercambio de información; la interdependencia tecnológica; las infraestructuras críticas digital-dependientes; la necesidad de cooperación internacional entre distintos actores; la emergencia de actores no estatales; la reciprocidad y los beneficios mutuos.

De acuerdo a lo que se viene sosteniendo, a partir del aprendizaje de los hechos sucedidos en Estonia los Estados miembros de la OTAN redefinieron sus intereses en el ámbito de la ciberseguridad impulsando conductas cooperativas.

En este sentido, la OTAN señala,

> Los acontecimientos de los últimos dos años han puesto de manifiesto los trastornos potencialmente masivos que pueden causar los ciberataques y la urgente necesidad de abordar este problema. En resumen, nuestras infraestructuras digitales se han convertido en activos estratégicos nacionales, y ahora están en riesgo. (Myrli, NATO Parliamentary Assembly, 2009, p.2).

De este modo, desde esta redefinición los intereses nacionales pasaron a ser mutuos y pensados en términos de ganancias absolutas. Como se ha visto, según el reporte de la OTAN (2009), los Estados miembros comenzaron a compartir un amplio consenso político sobre la gravedad de las amenazas cibernéticas y del aporte que debía realizar la OTAN en este ámbito. Esto permitió que se llegue a un rápido acuerdo sobre las políticas de la OTAN sobre la Ciberdefensa, que comenzó a implementar tanto por personal de la organización como de los Estados individuales.

Los avances y acuerdos que se fueron dando en cada una de las Cumbres respecto a la creación de instituciones y organismos vinculados a la ciberseguridad, como así

también la inclusión de la ciberseguridad en el Nuevo Concepto Estratégico 2010, son fuertes indicadores de la presencia de intereses mutuos pensados en términos de ganancias absolutas.

Es así que las prácticas cooperativas, entendidas como un proceso de mutua adaptación de conductas, se llevaron a cabo más allá de la heterogeneidad de los Estados miembros de la OTAN, facilitadas por costos de transacción ya asumidos dentro de su estructura institucional. En decir, si las políticas e instituciones en ciberseguridad de la OTAN se hubiesen tenido que negociar constantemente desde cero, la adopción de medidas y políticas en ciberseguridad habrían demandado mayores tiempos y costos.

En consecuencia, los costos de transacción ya asumidos posibilitaron un rápido despliegue político e institucional en el campo de la ciberseguridad. Tal como lo muestra la figura 7, se pueden observar la cantidad de agencias, organismos, comités y comandos que pasaron a conformar la estructura institucional de la OTAN en un período relativamente corto de tiempo.

Sin embargo, es preciso notar que la cooperación no es automática y que no equivale a armonía de intereses, si se tiene en cuenta, por ejemplo, que al momento de realizar el presente TFG solo 16 de los 28 Estados miembros de la OTAN pertenecían al CCDCOE.

De todas maneras, los objetivos comunes en ciberseguridad de los Estados miembros de la OTAN, se prevén alcanzar con mayor eficacia y eficiencia en el marco de un régimen institucionalizado. De igual modo, mediante una secuencia programada y reglas establecidas, la OTAN procuró reducir la información asimétrica y la incertidumbre facilitando medidas y acciones que beneficien tanto a la seguridad de organización como a la de los Estados miembros.

En efecto, a nivel operacional todos estos elementos comenzaron a ser gestionados y canalizados en un régimen institucionalizado de ciberseguridad mediante agencias, organismos e instituciones tales como el NCIRC, el CDMB y el CCDCOE situación que significó un cambio y una readecuación de la OTAN ante un nuevo escenario en cuanto a seguridad del sistema internacional.

La renovación de la Política en Ciberdefensa y el Plan de Acción de 2011

A tono con la dinámica permanente del sector, en los años siguientes, la OTAN continuó expandiendo sus capacidades en ciberseguridad renovando su Política en Cibedefensa, incorporando un *Plan de Acción*, creando los *Rapid Reaction Teams* y acrecentando sus vínculos con el sector privado, otras organizaciones internacionales y la academia.

Como indican Healey y Jordan (2014), la Política en Ciberdefensa y el Plan de Acción de junio de 2011 constituyeron un nuevo salto de calidad y una maduración de las cibercapacidades de la Organización y de sus estructuras de gobernanza. Aprobado durante las operaciones llevadas a cabo en Libia, el plan se focalizó en incrementar los mecanismos políticos y operacionales que permitieran expandir las capacidades tanto de la OTAN como de los Estados miembros.

A partir del estudio del contexto internacional y en cumplimiento de los mandatos establecidos en la Cumbre de Lisboa 2010 y el Concepto Estratégico, en marzo de 2011 la OTAN elaboró por primera vez un concepto sobre la defensa cibernética para los Ministros de Defensa. Este instituyó el modelo básico de la Política de la OTAN sobre la defensa cibernética renovada.

La Política fue elaborada y acordada por los Ministros de Defensa de la OTAN el 8 de junio junto a una herramienta de implementación denominada Plan de Acción, que representa un documento detallado con tareas y actividades específicas para las estructuras propias de la OTAN y las fuerzas de defensa de los Estados miembros (NATO Policy on Cyber Defence, 2011).

Los elementos medulares de esta renovación de la política en ciberdefensa incorporaban un enfoque, objetivos, principios, respuesta, el acoplamiento con la comunidad internacional y los pasos prácticos de procedimiento.

De acuerdo a lo publicado por la *NATO Policy on Cyber Defence* (2011) pueden ser analizados cada uno de ellos:

- *Enfoque*: garantizar la integridad y el funcionamiento continuo de sus sistemas de información. Por consiguiente, la principal preocupación de la OTAN es la protección de sus propios sistemas de comunicación e información. Además, defender mejor sus sistemas y redes de información mejorando su capacidad para enfrentar a la gran variedad de amenazas cibernéticas.

- *Objetivos:* La OTAN aplicará una acción coordinada de la ciberdefensa que abarque planificación y desarrollo de las capacidades, además de los dispositivos de respuesta ante un ciberataque, incorporando medidas de ciberdefensa para el desarrollo de recursos de defensa cibernética. Además, el Proceso de Planificación de Defensa de la OTAN (NDPP) conducirá la integración de la defensa cibernética en los marcos de defensa nacional de los Estados miembros.

A partir de una protección centralizada, la OTAN implementará requisitos mínimos para aquellas redes nacionales que estén conectadas o procesen información de la OTAN, y trabajará coordinadamente con los Estados miembros para desarrollar obligaciones mínimas de defensa cibernética de manera que garanticen la protección y defensa de los sistemas y redes de información crítica nacionales. Además, en caso de solicitud, la OTAN ayudará a los Estados miembros a lograr un nivel mínimo de ciberdefensa nacional.

- *Principios:* En la actualización de su Política en Ciberdefensa de 2011, la OTAN mantuvo los principios de *subsidiariedad* y *no-duplicación* y adicionó dos: *prevención y resiliencia*. La prevención de los ciberataques se producirá y se logrará mediante el aumento del nivel de preparación y atenuación del riesgo, mientras que por resiliencia se entienden todas aquellas acciones que faciliten la capacidad de recuperación rápida luego de un ciberataque.

- *Respuesta*: en este punto, quizás el más sensible, la OTAN señala:

> Como se indica en el Concepto Estratégico, la OTAN defenderá su territorio y sus poblaciones contra todas las amenazas, incluidos los emergentes desafíos de seguridad, como la ciberdefensa. La Política en

> Ciberdefensa de la OTAN reitera que cualquier respuesta de defensa colectiva está sujeta a las decisiones del Consejo del Atlántico Norte. La OTAN mantendrá la ambigüedad estratégica, así como la flexibilidad sobre cómo responder a diferentes tipos de crisis que incluyen un componente cibernético. La OTAN también integrará aspectos cibernéticos en los procedimientos de gestión de crisis de la OTAN, que guiarán la respuesta de la OTAN en el contexto de una crisis o conflicto más amplio. La OTAN proporcionará asistencia coordinada si un Aliado o Aliados son víctimas de un ataque cibernético. Para facilitar esto, la OTAN mejorará los mecanismos de consulta, la alerta temprana, el conocimiento de la situación y el intercambio de información entre los Estados miembros. Para facilitar estas actividades, la OTAN cuenta con un marco de Memorandos de Entendimiento sobre defensa cibernética en vigor entre las autoridades nacionales de defensa cibernética de los Estados miembros y el Consejo de Administración de la OTAN para la Defensa Cibernética. Para responder a los incidentes dentro de la propia infraestructura de información de la OTAN, la Capacidad de Respuesta ante Incidentes Informáticos de la OTAN (NCIRC) se ocupa de los asuntos cotidianos y aplica medidas de mitigación apropiadas (NATO Policy on Cyber Defence, 2011).

- *Acoplamiento con la Comunidad Internacional:* Las amenazas cibernéticas trascienden las fronteras estatales y alcanzando sus vulnerabilidades y riesgos a todas las sociedades interconectadas del mundo. Considerando la naturaleza global del ciberespacio y sus amenazas asociadas, la OTAN y los Estados miembros trabajarán con las organizaciones internacionales, el mundo académico y el sector privado de manera conjunta para promover la complementariedad y evitar la duplicación.

- *Pasos Prácticos de Procedimiento:* finalmente, la nueva Política en Ciberdefensa y el Plan de Acción proponen una serie de pasos prácticos como guías de las operaciones en ciberdefensa. Para tal fin, la OTAN desarrollará requisitos mínimos en los sistemas de información nacionales que son críticos para llevar a cabo las tareas básicas de la OTAN y ayudará a los Estados miembros a lograr un nivel mínimo de ciberdefensa.

Del mismo modo, la defensa cibernética se integrará plenamente en el NDPP y las Autoridades Militares de la OTAN evaluarán cómo la defensa cibernética apoyará el desempeño de las tareas básicas de la OTAN.

También se contemplan los requisitos de defensa cibernética para los Estados que no son miembros, y además un Estado miembro puede ofrecer ayuda a otro Estado miembro o a la OTAN en caso de ciberataque. Asimismo, la OTAN mejorará la capacidad de alerta temprana, conciencia de la situación y análisis; desarrollará programas de sensibilización; ejercicios en ciberdefensa y alentará a los Estados miembros a recurrir a la experiencia y el apoyo del CCDCOE en la materia.

Para implementar en forma eficaz esta nueva política en caso de ciberataque, la OTAN estableció una estructura de gobernanza. El principal órgano de gobierno para la ciberdefensa, quedó constituido en el CDMB, quien ha firmado Memorandos de Entendimiento con las autoridades de cada Estado miembro, y a su vez informará regularmente estos avances al máximo órgano político de la Alianza, el *Consejo del Atlántico Norte* (NAC, por sus siglas en inglés).

Al mismo tiempo se constituye un nuevo y permanente *Comité para la Ciberdefensa* (CDC, por sus siglas en inglés) para gestionar la gobernanza política, prestar supervisión y brindar asesoramiento a las Estados miembros (Healey y Jordan, 2014).

Por otra parte, en 2012 la OTAN se comprometió a invertir 58 millones de euros para mejorar sus capacidades en ciberseguridad, especialmente al NCIRC, y en la creación de células de evaluación de amenazas cibernéticas (Healey y Jordan, 2014).

Al mismo tiempo, en el año 2013 se perfeccionaron los ciberejercicios que habían comenzado en mayo de 2010, llamados *Locked Shields*. Divididos en cinco equipos, *Directivo* (responsable del plan y diseño del ejercicio); *Blanco* (responsable de crear las reglas, puntuaciones y control); *Azul* (compuesto por el sector privado, la academia e individuos); *Rojo* (integrado por el sector privado, agencias de gobierno y el NCIRC) y el equipo *Verde*, también llamado el equipo técnico (responsable de preparar la infraestructura técnica de laboratorio), “cada año, los equipos son sometidos a una intensa presión para mantener las redes y servicios de un país ficticio.

La tarea implica manejar e informar incidentes, resolver desafíos forenses, y responder a comunicaciones legales y estratégicas y proyectos de escenarios. Para mantenerse al tanto de los desarrollos del mercado, Locked Shields se centra en tecnologías, redes y métodos de ataque realistas y de vanguardia" (CCDCOE, 2012).

Finalmente, para 2013 la OTAN a nivel político desarrolló un encuentro de Ministros de Defensa de los Estados miembros, para tratar exclusivamente temas relacionados a la ciberseguridad, quienes acordaron continuar con la expansión de los recursos y capacidades en el área.

A su vez, a nivel operacional, se constituyó la *Smart Defense*, que abarcaba tres proyectos: el Desarrollo Multinacional de Capacidades de Defensa Cibernética; la Plataforma de Intercambio de Información sobre Malware; y el énfasis en la educación estratégica, política y técnica a través de una red de instituciones como la NATO Scholl Oberammergau y la NATO Communications and Information Systems Scholl (Healey y Jordan, 2014).

De acuerdo a Healey y Jordan (2014), quizás lo más importante, es que la política cibernética ha clarificado el proceso que se utilizará para cumplir con su misión de defensa colectiva, manteniendo la ambigüedad en casos específicos. Este proceso comienza a nivel técnico con la participación del NCIRC.

En cambio, si un incidente tiene derivaciones políticas, las acciones se elevan de la NCIRC al CDMB y al CDC a través del NAC. La política de la OTAN no especifica en forma pormenorizada sobre lo que sucede luego, pero el proceso probablemente llevaría a una réplica como en cualquier otro tipo de suceso donde la seguridad de la OTAN o un Estado miembro esté amenazada (Healey y Jordan, 2014).

En este caso, ante un ataque cibernético, un Estado miembro puede llamar a consulta formal bajo el artículo 4º del Tratado de Washington, si siente que su integridad territorial, o seguridad nacional está amenazada.

Si el ciberataque fuese destructivo o afectase a las infraestructuras críticas, el NAC podría considerar por invocar la defensa colectiva a través del artículo 5º, un proceso que sucedió rápidamente después del ataque terrorista del 11-S (Jones, 2015).

Según Joubert (2012), toda esta nueva política se puede sintetizar y enfocar en tres niveles:

- *Operacional*: con el establecimiento del CDMB y las mejoras introducidas al NCIRC;

- *Estratégico*: donde se definen claramente roles y responsabilidades tanto de la OTAN como de los Estados miembros, y se detallan los Pasos Prácticos de Procedimiento para la gestión e implementación de la nueva política;

- *Doctrinal*: a partir de la creación del CCDCOE y del diálogo con otros actores internacionales, impulsó trabajos de investigación a largo plazo que permitan abordar los desafíos pendientes.

Es decir, de acuerdo a lo analizado, las políticas en ciberdefensa de la OTAN se focalizaron en la protección de sus propias redes, y, en la idea de defensa colectiva en caso de un ciberataque a un Estado miembro.

Asimismo, de acuerdo a Joubert (2012), teniendo en cuenta estos niveles, las políticas en ciberseguridad de la OTAN también se pueden examinar desde una perspectiva legal, operacional y estratégica.

Desde la perspectiva legal, se pueden considerar las circunstancias y condiciones bajo las cuales se puedan activar los mecanismos de la defensa colectiva a través de los artículos 4º y 5º del Tratado de Washington. Sin embargo, la decisión de invocar la aplicación de estos artículos es bastante compleja en el ámbito del ciberespacio.

Como señala Artiles (2011), dilucidar las situaciones que desencadenarían la aplicación del artículo 5º en el contexto del ciberespacio, por ejemplo, considerar el volumen y fuerza de ataque, y la violación de la integridad territorial o independencia política es controvertido debido a la falta de definición de un *jus in bello* relativo al ciberespacio.

Por lo tanto, esta situación ha conducido a que los Estados miembros de la OTAN hayan decidido, mantener la ambigüedad y flexibilidad en cuestiones referentes a los ciberataques y optasen por evaluar caso por caso.

En cuanto a la perspectiva operacional, resulta evidente que la OTAN necesitaba expandir sus capacidades en ciberseguridad, donde el NCIRC por si solo no podría

gestionar eficazmente un ciberataque lanzado contra los sistemas informáticos de la OTAN o de Estados miembros (Joubert, 2012).

Por último, siguiendo a Joubert (2012), las amenazas provenientes del ciberespacio significan todo un desafío intelectual para la OTAN, dado que las doctrinas elaboradas anteriormente por la OTAN para otro tipo de riesgos a la seguridad, no pueden adecuarse fácilmente al domino digital. Este hecho constituye otro indicador de la dinámica del sistema internacional, de la constitución del ciberespacio como nueva dimensión de la seguridad y de la necesidad de abordarlo desde otra perspectiva.

En este punto, la estrategia se orienta hacia la *disuasión.* La disuasión puede entenderse como *negación* o como *castigo*. La disuasión por negación básicamente consiste en adoptar las medidas y estrategias tecnológicas necesarias que impidan un ciberataque exitoso, y por lo tanto, que el atacante se sienta frustrado y abandone el intento.

En cambio, la disuasión por castigo implica la idea de represalias, lo que sería motivo suficiente para prevenir el ataque. Sin embargo, en el ámbito del ciberespacio la identificación de los autores, debido a su naturaleza difusa, es difícil de establecer y la atribución de responsabilidades el mayor problema (Litwak y King, 2015).

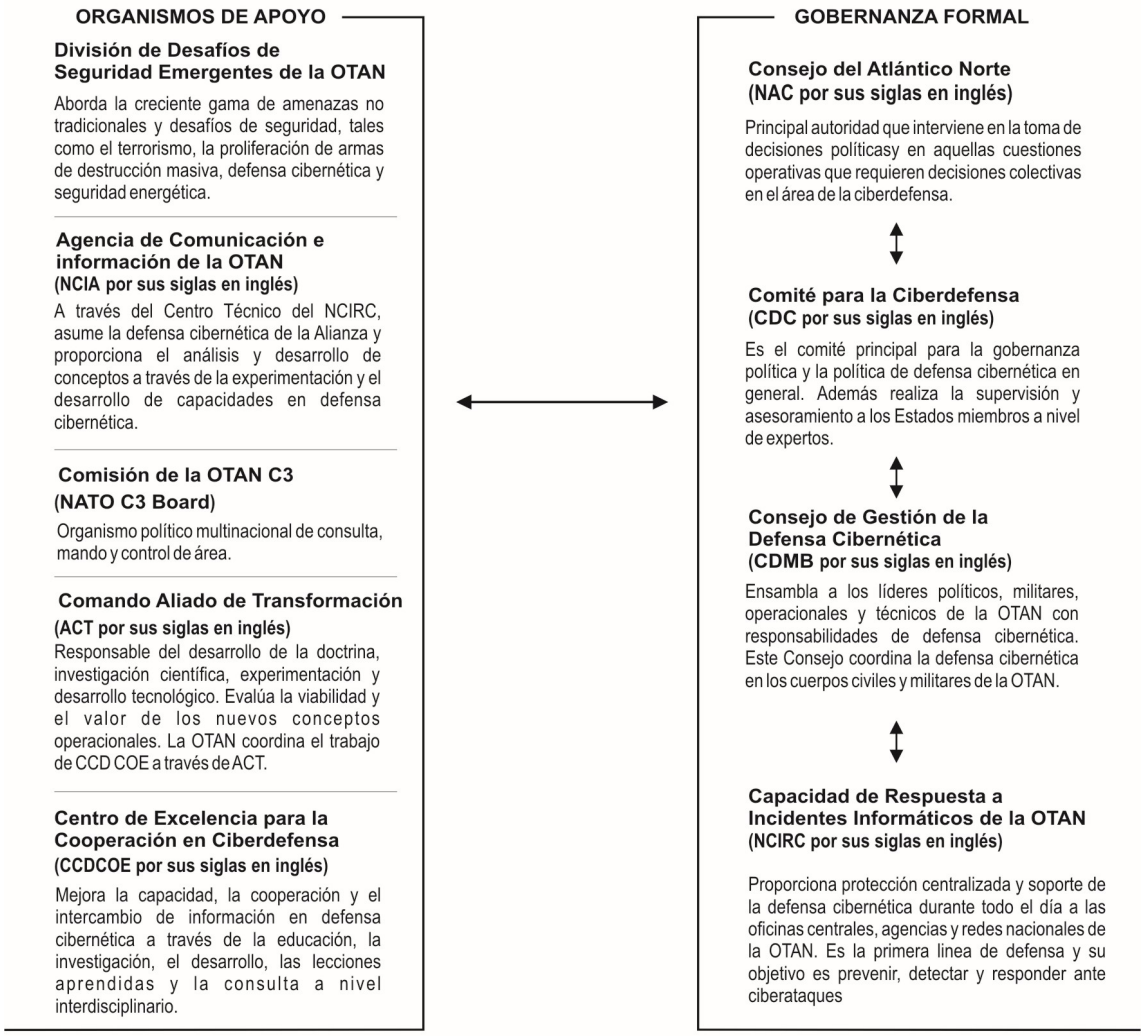
Dicho de otra manera, la disuasión por castigo es problemática teniendo en cuenta la dificultad para constatar quien es el responsable por el ataque y que objetivos deberían seleccionarse como parte de las represalias y por cuanto tiempo éstas serían efectivas. También se debe tener en cuenta cuándo un ciberataque debe ser considerado acto de guerra o bajo qué condiciones terceras partes participarían en las represalias (Joubert, 2012).

En definitiva, la OTAN fue desarrollando progresivamente una serie de políticas, organismos e instituciones en el área de la ciberseguridad. Al mismo tiempo, a cada una de estas partes le fueron asignados roles, objetivos y responsabilidades dentro de una estructura institucional donde se organizan y complementan en distintos niveles.

En la figura 7 se puede apreciar esta disposición y el sistema de relaciones:

Figura 7

Estructura Institucional en Ciberdefensa de la OTAN



Fuente: Elaboración propia en base a Healey y Jordan (2014)

La Cumbre de Chicago 2012 y los vínculos con el sector privado

En este último apartado del Capítulo 3 se analizarán los lazos y asociaciones impulsadas desde la OTAN con el sector privado y la industria como medios que permitan mejorar sus capacidades en ciberseguridad.

En forma coherente con el marco teórico que dirige a este TFG, la interdependencia y la globalización, revelaron la emergencia y la importancia de los actores no estatales y transnacionales en el sistema internacional. También se debe señalar, que en el ámbito del ciberespacio y las TICs, el sector privado tiene una posición de vanguardia, en cuanto a gestión, protocolos, investigación y desarrollo de nuevos productos y dispositivos.

En otras palabras, la naturaleza transnacional del ciberespacio implica para la OTAN dialogar y relacionarse con otras organizaciones internacionales, la academia y el sector privado (Joubert, 2012). En este marco, en la Cumbre de Chicago 2012, los Estados miembros de la OTAN expresan:

> (…) debemos profundizar las conexiones entre los Aliados y entre ellos y nuestros socios sobre la base del beneficio mutuo. Mantener una industria de defensa fuerte en Europa y aprovechar al máximo el potencial de la cooperación industrial de defensa a través de la Alianza sigue siendo una condición esencial para alcanzar las capacidades necesarias para el 2020 y más allá. (…) La *Smart Defense* está en el corazón de este nuevo enfoque (…) Representa una perspectiva cambiada, la oportunidad para una cultura renovada de cooperación en la que la colaboración multinacional da nueva prominencia como una opción eficaz y eficiente para desarrollar capacidades críticas (NATO, Summit Declaration on Defence Capabilities, 2012, Sec. 6,7,8).

La lectura del fragmento de la Declaración sobre Capacidades de Defensa realizada en el marco de la Cumbre de Chicago demuestra, por una parte, como la OTAN enfatiza la necesidad de incrementar los lazos de cooperación y colaboración internacional sobre la base de los beneficios mutuos y, por la otra, el convencimiento de renovar la perspectiva en la doctrina de seguridad incorporando a la industria como socio estratégico en el área de la tecnología.

Como resultado, en el año 2013 la OTAN acordó conformar un marco para promover la interacción de la OTAN y el sector privado/industria, publicando el *Marco para el Acoplamiento OTAN-Industria.*

El objetivo de este Marco era mejorar los medios y las formas de acoplamiento entre la OTAN y la industria dentro de una relación mutuamente beneficiosa, transparente y coherente. A su vez, este Marco institucional no suponía una intromisión de la OTAN en las políticas nacionales de los Estados miembros, sino que servía de apoyo para la implementación completa del nuevo Concepto Estratégico aprobado en la cumbre Lisboa 2010 y un eficaz gestión del NDPP sobre la base institucional de la OTAN según lo previsto en los acuerdos preexistentes.

Asimismo, una serie de reglas y principios clarificarían la relación OTAN-Industria identificando las maneras y métodos para aplicar las contribuciones del sector privado en mejorar las capacidades de la OTAN en la Smart Defense (NATO, Framework for NATO-Industry Engagement, 2013).

El Marco se apoya en una serie de *principios universales y específicos*. Los principios universales comprenden los conceptos de: control del Marco por los Estados miembros; participación voluntaria; confianza y transparencia; imparcialidad, inclusión, tratamiento igualitario; y beneficios mutuos.

En cuanto a los específicos se hace referencia a la cooperación y a la comunicación clara de la OTAN respecto a sus requerimientos a la industria (NATO, Framework for NATO-Industry Engagement, 2013).

De igual modo, se establece que la implementación del Marco exige una evaluación y una optimización de los acuerdos ya existentes con la industria, que incluyen una descripción detallada de estos acuerdos previos, la evaluación e identificación de mecanismos de coordinación, el desarrollo de un estructura interna con roles, responsabilidades y canales de comunicación entre las partes y plazos de implementación (NATO, Framework for NATO-Industry Engagement, 2013).

Toda esta conceptualización y renovación de la perspectiva en la doctrina de seguridad de la OTAN, que incluía la idea de incrementar las capacidades en ciberseguridad

mediante un marco de acción conformado por el nuevo Concepto Estratégico, la Smart Defense y la participación del sector privado-industrial, se sintetizó y materializó con la conformación de la *Ciber Asociación OTAN-Industria* (NICP, por sus siglas en inglés).

Si bien la NICP inició formalmente sus operaciones en 2014, desde este TFG se entiende necesario hacer mención a sus funciones y al rol que cumple dentro de las políticas de ciberseguridad de la OTAN.

Se debe tener en cuenta que la NICP, es una consecuencia directa del Concepto Estratégico aprobado en Lisboa 2010, y del anteriormente analizado Marco de acoplamiento de 2013 previamente acordado por los Estados miembros en la Cumbre de Chicago 2012, siendo durante ese lapso de tiempo donde comenzó a ser gestada y edificada.

En consecuencia, como respuesta a la complejidad de los desafíos en ciberseguridad que la OTAN debía abordar en el sistema internacional, la cooperación y la articulación de mecanismos con actores no estatales del sector privado/industrial fueron incluidos en la estructura institucional como una herramienta que permitiese mejorar sus capacidades y eficacia.

En este sentido la NICP afirma:

> El carácter interconectado y abierto del ciberespacio ha ofrecido oportunidades sin precedentes a nuestras economías y ha transformado el tejido de nuestras sociedades. Del mismo modo, las amenazas cibernéticas están creciendo tanto en número como en sofisticación. Como la mayoría de las redes son propiedad y son operadas por el sector privado, sus innovaciones tecnológicas y su experiencia son cruciales para la defensa cibernética. La cooperación, en particular el intercambio de información sobre las amenazas, puede reforzar la resistencia de las redes y ayudar a prevenir, responder y recuperarse de los ataques cibernéticos. En este contexto, trabajaremos con la industria como parte de una asociación abierta, transparente y mutuamente beneficiosa, la Ciber Asociación OTAN-Industria (NICP). Esta asociación apoya el papel principal de la OTAN en la defensa cibernética: la protección de sus propias redes (NATO, NICP, 2016)

Como señalan Healey y Jordan (2014), la cooperación con la industria, permite reforzar las capacidades individuales de los Estados miembros avanzando en la gobernanza de la ciberseguridad. A su vez, enfatizando la exigencia en el entrenamiento y la educación, la OTAN ha madurado al entender que es muy difícil mantener los sistemas seguros sin una estrecha cooperación a multinivel basada en el intercambio de información, transparencia e inclusión.

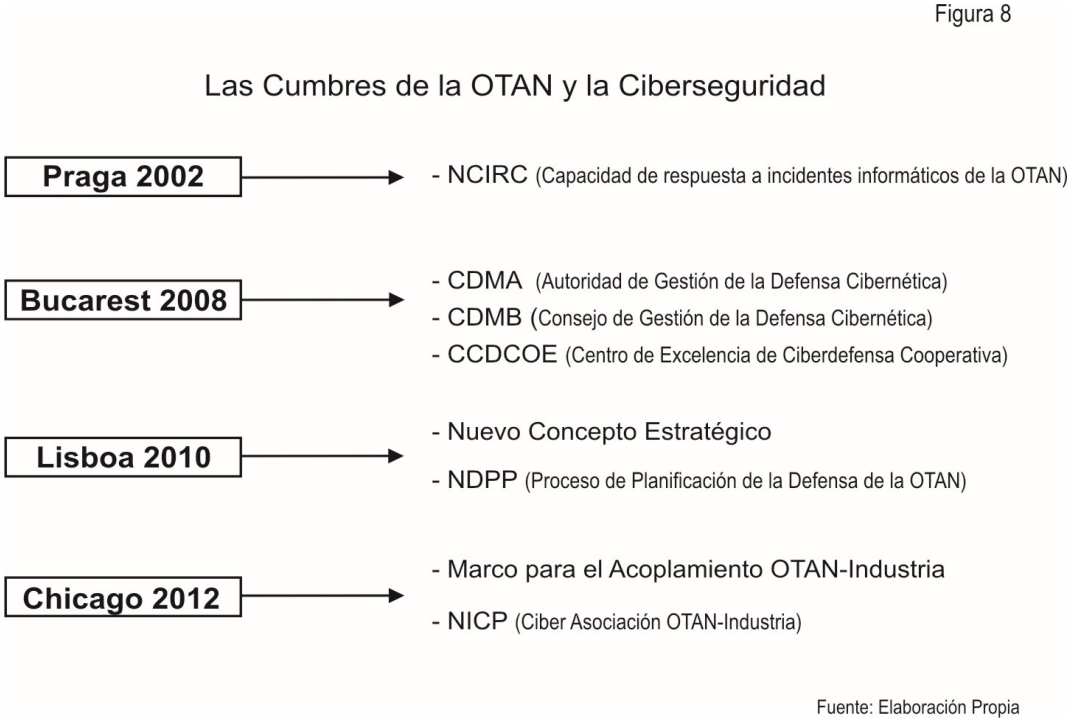
Estos conceptos se ratifican en la misión encomendada a la NICP, entre los cuales sobresalen mejorar la defensa cibernética en la cadena de suministros de la OTAN; facilitar la participación de la industria en proyectos multinacionales; contribuir a los esfuerzos de la OTAN en educación, capacitación y ejercicios en ciberdefensa; ayudar a la OTAN y a los Estados miembros a aprender de la industria; y, aprovechar los desarrollos del sector privado para el desarrollo de capacidades en ciberseguridad (NATO, NICP, 2016).

Es decir, la complejidad del sistema internacional y de sus nuevas formas de amenaza, condujo a los Estados miembros de la OTAN a adoptar conductas que favorecen la cooperación multinivel y la participación de actores estatales y no estatales.

Además, estas conductas y nuevas perspectivas respecto al concepto de seguridad, han sido refinadas en las cumbres analizadas de la OTAN. En cada una de ellas se incorporaron nuevos conceptos, políticas, organismos e instituciones que progresivamente fueron constituyendo un *corpus* y una estructura institucional que permitiese aumentar sus capacidades en ciberseguridad.

Por lo tanto, explorando la evolución de las políticas en ciberseguridad de la OTAN a través de las diferentes cumbres, éstas se pueden sintetizar en forma esquemática (figura 8):

Figura 8



Fuente: Elaboración Propia

Conclusiones Preliminares

En síntesis, las políticas en ciberseguridad desarrolladas y adoptadas en las distintas cumbres de la OTAN, fueron progresivamente ganando en complejidad para enfrentar amenazas que se presentaron en los mismos términos, hasta alcanzar una estructura formal e institucional de gobernanza.

Conforme a lo analizado, la rápida respuesta por parte de la OTAN en el área de la ciberseguridad, y el considerable número de agencias, organismos e instituciones adoptadas, demuestran que los costos transacción cuando están asumidos dentro de una estructura o régimen, no constituyen un obstáculo para la ágil adopción de políticas en la consecución de beneficios mutuos. Sin embargo, la cooperación no se desarrolla en forma automática, requiere de tiempo y de la evaluación de la situación por parte de los Estados miembros.

No obstante, a partir del aprendizaje que significaron los ciberataques, los Estados miembros fueron modificando sus intereses relacionados a la seguridad nacional, y en la medida que estas percepciones era compartidas por otros Estados miembros, es decir

existiendo intereses mutuos, fue posible llevar adelante acciones convergentes pensadas en términos de ganancias absolutas.

Como señala Keohane (1993), estos acuerdos enmarcados dentro de regímenes permiten monitorear los resultados, el mutuo cumplimiento por medio de prácticas y reglas, y el seguimiento de las estrategias comunes. De este modo, la naturaleza transnacional del ciberespacio implica necesariamente la participación de actores transnacionales para abordar sus desafíos y las amenazas emergentes.

La participación de actores estatales, no estatales, organizaciones internacionales gubernamentales y no gubernamentales e individuos, obligan a un cambio de perspectiva o si se quiere de cultura, a la hora de alcanzar soluciones a los riesgos derivados de los cambios tecnológicos.

Por lo tanto, una de las cuestiones más sensibles en relación al ciberespacio tiene que ver con las responsabilidades y atribuciones desde el punto de vista del derecho internacional que puede conllevar un ciberataque.

La cuestión de un derecho internacional aplicable al ciberespacio ha sido un tema de preocupación para la OTAN. En efecto, la Organización comenzó a destinar recursos y promover su estudio desde el Centro de Excelencia de Ciberdefensa Cooperativa cuyos objetivos, avances y resultados serán examinados a continuación.

CAPÍTULO 4

La OTAN y el derecho internacional relativo al ciberespacio

Ciberespacio: una nueva dimensión del Derecho Internacional

La irrupción y expansión de las TICs en todos los ámbitos de la sociedad actual, a su vez favorecidas por el fenómeno de la globalización e interdependencia, incrementó las interacciones humanas hasta niveles inesperados.

Estas interacciones efectuadas a través de redes, que a su vez, se bifurcan en otras sucesivas y múltiples redes, han derivado en la concreción de un nuevo espacio de relación humana. Este campo, denominado *ciberespacio*, se diferencia de otros dominios típicos de relaciones humanas por una característica particular: carece de una forma física concreta, o dicho en otros términos, es virtual.

Sin embargo, su condición de virtualidad, no impide que al igual que en otras áreas de las relaciones globales, se lleven a cabo delitos o ataques contra los bienes de los individuos o la seguridad e integridad soberana de un Estado. Los ya analizados ataques a Estonia y el caso del virus *Stuxnet* en Irán, son sólo algunos ejemplos de una realidad cotidiana que se repite cada vez con mayor frecuencia.

De esta manera, el ciberespacio se presenta como un área donde las acciones pueden quedar impunes por dos características exclusivas: la virtualidad y la imposibilidad de identificar fácilmente a los responsables de delitos (Reguera, 2015).

Esta situación ha llevado a un incremento de las preocupaciones por parte de los Estados, organizaciones internacionales y de la academia para elaborar un marco de derecho internacional que regule las acciones en el ciberespacio.

En otras palabras, el ciberespacio no podía permanecer inmerso en un vacío legal. La llegada de las TICs a todos los ámbitos ha obligado a los Estados por una parte, a regular el uso de estas tecnologías en sus sistemas nacionales, y por la otra, implica crear un marco legal internacional de normas, derechos y sanciones (Wegener, 2013).

Por lo tanto, la emergencia del paradigma de la ciberseguridad resulta en el reconocimiento por parte de los Estados y las Organizaciones Internacionales, de la necesidad de reglas que regulen el comportamiento de los actores en el ciberespacio. (Tikk, 2011)

Como señalan Schmitt y Vihul (2014), si bien existen legislaciones nacionales que buscan gobernar las ciberactividades interestatales y se desarrollan constantes avances en la adopción de estándares técnicos comunes, la evolución y formación de un marco legal internacional específico para la ciberactividades, permanece a la sombra de los otros regímenes legales. En realidad, a nivel internacional, existen muy pocas reglas específicas y expresamente creadas para aplicar en el ciberespacio.

En este sentido, de acuerdo a Streltsov (2007), en el ciberespacio conceptos como fronteras o territorio no existen, por lo tanto, es necesario el desarrollo de nuevos marcos legales para este fenómeno global.

En principio, se debe tener en cuenta si las normas de un marco legal internacional para la ciberactividades son idénticas a los que gobiernan y regulan otros campos. Las diferencias pueden deberse no la variación de las estructuras legales, sino a la naturaleza *sui generis* del ciberespacio. Además, un aspecto esencial a considerar es la terminología. Las diferencias de lenguaje utilizadas por los que pertenecen a ámbitos legales, y los que integran entornos políticos o tecnológicos, son a menudo una fuente de confusión. De este modo, el entendimiento sobre terminología legal clave, es una precondición para cualquier intercambio significativo entre comunidades normativas (Schmitt y Vihul, 2014).

Siguiendo a Schmitt y Vihul (2014), la construcción de una arquitectura legal internacional relativa a gobernar y regular las ciberactividades necesariamente debe comenzar con el Artículo 38 del Estatuto de la Corte Internacional de Justicia. Allí se determina que las fuentes del derecho internacional son:

- Las convenciones internacionales: establecen reglas y normas, que una vez negociadas y ratificadas, los Estados miembros del tratado quedan obligados a cumplirlas.

- La costumbre internacional: es un género único de normas internacionales no escritas, que son cristalizadas mediante un proceso informal de prácticas y conductas que se repiten en el tiempo. Además implica dos factores: un elemento objetivo que es la práctica estatal o *usus*, y un elemento subjetivo u *opinio juris*, que se refiere a la convicción de los Estados de que una práctica es obligatoria, es decir, un sentido de obligación legal.

- Los principios generales del derecho reconocidos por las naciones civilizadas

- las decisiones judiciales y las doctrinas de los publicistas de mayor competencia de las distintas naciones, como medio auxiliar para la determinación de las reglas de derecho.

Las tres primeras son universalmente aceptadas como fuentes primarias del derecho internacional, mientras que las dos últimas se identifican como medios auxiliares o fuentes secundarias que contribuyen a la interpretación y a la formación de derecho.

Ahora bien, considerando que el ciberespacio y las actividades derivadas del mismo son relativamente nuevas, existen pocos tratados internacionales relativos al ciberespacio. Por ejemplo, la *Convención en Cibercrimen* (2004) y su *Protocolo Adicional* (2006), elaborado por el Consejo de Europa, que además es el primer tratado internacional para delitos informáticos, o el *Tratado Internacional para la Seguridad de la Información de la Organización de Cooperación de Shanghai* (2008), son algunos de los esfuerzos que se han realizado en este campo (Schmitt y Vihul, 2014).

También se pueden destacar las Resoluciones 55/63 (2000), 56/121 (2001), 57/239 (2002) y 58/199 (2004) de Naciones Unidas y la *Agenda Digital para Europa* de la Unión Europea (2010). Sin embargo, todos estos trabajos fueron de carácter general y alcance limitado (Reguera, 2015)

Por lo tanto, teniendo en cuenta la escasez de tratados internacionales relativos al ciberespacio, la cuestión es cuando un tratado de otra área del derecho puede aplicar a las ciberactividades. En este sentido, esto parece tener fundamento con la publicación en 2013 del Grupo de Expertos Gubernamentales de Naciones Unidas, quienes afirman

que la ley internaciones y la Carta de las Naciones Unidas, son aplicables y esenciales para mantener la seguridad, la estabilidad y el acceso al entorno de las TICs (Schmitt y Vihul, 2014).

En otras palabras, ante la falta de tratados internacionales relativos al ciberespacio, una forma de superar la laguna legal es mediante analogías y adaptaciones legales de tratados preexistentes en otras áreas.

En la misma línea Wegener (2013), sostiene que el derecho internacional es anterior a la era cibernética. Pero considerando que el ciberespacio se está transformando en un nuevo escenario de operaciones, es generalmente aceptado que el *jus ad bellum* (derecho al uso de la fuerza) y el *jus in bello* (derecho en la guerra o derecho internacional humanitario), pueden ser adaptados adecuadamente para gobernar los conflictos en el ciberespacio.

En cuanto a la costumbre internacional, la relativa novedad material de las ciberactividades no sería necesariamente un impedimento para la emergencia de derecho consuetudinario. La intensa dinámica de las relaciones internacionales contemporáneas, conduce a múltiples interacciones estatales donde los comportamientos recíprocos se constatan casi en forma inmediata.

En ese aspecto, según Schmitt y Vihul (2014), la condición de temporalidad para la emergencia de derecho consuetudinario se ha ido deteriorando a través del tiempo. Un ejemplo claro de la debilidad de la condición de temporalidad, ha sido el rápido desarrollo del derecho consuetudinario relativo al espacio exterior.

Finalmente, si se utilizan como fuente a los principios generales del derecho de las naciones civilizadas, un factor de complicación con respecto a esta fuente es que su naturaleza es objeto de cierta controversia.

No obstante, en general el término hace referencia a un número de principios que son comunes a los diferentes sistemas jurídicos domésticos. Estos principios generales son devienen en importantes, cuando surgen disputas interestatales. Por ejemplo, si un Estado mediante ciberoperaciones violase la soberanía de otro Estado o dañase su

ciberinfraestructura, lo llevaría a la obligación de realizar reparaciones (Schmitt y Vihul, 2014).

De acuerdo a Reguera (2015), si bien el acceso a las TICs y al ciberespacio debe considerarse un derecho, protegiendo el libre uso en condiciones de seguridad y libertad, la creación de marcos legales para el ciberespacio no está exenta de inconvenientes. A la ya mencionada virtualidad, y la dificultad para identificar culpables, se le deben sumar la lentitud en la creación de marcos legales ante los veloces cambios tecnológicos.

En este contexto, la evidencia del vacío legal existente en el ámbito del ciberespacio, comprobada en los sucesos ocurridos en Estonia, se transformó en un elemento de interés común y en un objetivo compartido por los Estados miembros de la OTAN. La imposibilidad de abordar esta temática sumamente compleja en el actual sistema internacional, impulsó a los Estados miembros de la OTAN a emprender estrategias cooperativas y coordinadas para alcanzar soluciones concretas. Por lo tanto, como se ha visto en el Capítulo 2, uno de los pilares establecidos en la Asamblea Parlamentaria de la OTAN en 2007 para su estrategia de ciberseguridad fue la construcción de un marco jurídico-legal contra las amenazas cibernéticas.

La complejidad e interdependencia se muestran en toda su extensión en las TICs y en su consecuencia la Sociedad de la Información. En la medida en que las sociedades actuales y futuras dependan del ciberespacio, la necesidad de crear reglas y normas de conducta se hace imperiosa. Ante este fenómeno, y como ha sido con otros casos durante la historia mundial, como por ejemplo, el espacio aéreo y las aguas territoriales, los Estados deben cooperar para alcanzar ganancias absolutas.

Sin embargo, a diferencia de los temas de carácter técnico, cuando se ingresa al terreno del derecho internacional, la cooperación entre Estados no siempre se presenta en términos fluidos y es quizás donde exhibe una clara debilidad.

Así, por ejemplo durante el estudio del caso, los indicios y resultados de las investigaciones indicaban que los autores del ataque a Estonia provenían de Rusia. No obstante, Rusia negó sistemáticamente cualquier tipo de colaboración tanto con la investigación como en el terreno jurídico para dar con los presuntos culpables. En otras

palabras, los Estados perciben que su integridad soberana es invadida cuando deben someter su sistema jurídico a un mandato externo y la cooperación ya no es tan fácil de lograr.

De esta forma, una de las medidas adoptadas en la Cumbre de Bucarest en 2008 fue la creación del CCDCOE de la OTAN. Con el propósito de comenzar a dar claridad sobre estas preocupaciones compartidas en el campo legal aplicado al ciberespacio, en el año 2009 el CCDCOE invitó a un grupo multidisciplinario de expertos internacionales con el objetivo de producir un manual para el gobierno de los conflictos cibernéticos. El resultado fue la creación y publicación en el año 2013 del *Manual de Tallin*.

El Manual de Tallin

El Manual de Tallin es una consecuencia directa de la preocupaciones compartidas de los Estados miembros de la OTAN respecto a los ciberataques luego de los incidentes ocurridos en Estonia. De hecho, promovido desde el CCDCOE de la OTAN, y publicado por la Universidad de Cambridge, el proyecto lleva el nombre de la capital estonia, Tallin.

Es indudable que a partir de las percepciones mutuas y del aprendizaje de los Estados miembros, la OTAN reconoció la peligrosidad de las amenazas provenientes del ciberespacio para la seguridad de los Estados miembros, y se comprometió a desarrollar capacidades para prevenir, detectar y defenderse de ciberataques. En cada una de las cumbres y de los documentos analizados, la OTAN subrayó este concepto y fue incorporando sucesivos mandatos y lineamientos para su abordaje.

Esta tarea incluiría un proceso planificado y coordinado entre los Estados de la OTAN. Por lo tanto, uno de los desafíos que debían afrontar los Estados miembros era el alcance y la manera de enfrentar las amenazas provenientes del ciberespacio desde el derecho internacional. Además, la labor debía emprenderse de acuerdo a la ley de los conflictos armados y en línea a los pronunciamientos de la Corte Internacional de Justicia. En particular, el concepto de que en el derecho internacional los actos que no están explícitamente prohibidos, generalmente están permitidos (Manual de Tallin, 2013).

El Manual, producido por el Grupo Internacional de Expertos (GIE) que fueran invitados por el CCDCOE de la OTAN en 2009, se considera el principal trabajo de referencia relativo al derecho internacional de los conflictos en el ciberespacio. En particular, busca establecer reglas que abarquen los principios de *jus ad bellum* y *jus in bello* para los conflictos en el ciberespacio (Wegener, 2013).

En esa línea, el Manual pretende ser un instrumento para los juristas en aquellos temas conflictivos relacionados al ciberespacio. Sin embargo, es importante señalar que el Manual no es un documento oficial de la OTAN, ni tampoco la postura de los Estados miembros, sino la opinión de expertos independientes en un esfuerzo para comenzar a dar luz en el complejo mundo de las relaciones cibernéticas (Reguera, 2015).

Esta postura es claramente expresada en el Manual, donde se señala que en el mismo no se refleja ni la doctrina de la OTAN, ni tampoco el punto de vista o posición de los Estados o de organizaciones internacionales. Sólo es la expresión y opinión del GIE actuando en el marco de sus capacidades privadas, individuales y movilizados por la invitación del CCDCOE (Manual de Tallin, 2013)

Como lo señalan sus autores, el Manual examina la ley internacional que gobierna la ciberguerra. Es decir, aquellas actividades que ocurren en un nivel inferior al de *uso de la fuerza* no son abordadas. Todos los conflictos examinados abarcan los contextos de *jus ad bellum* y *jus in bello.*

Es decir, no es un manual en ciberseguridad si se lo considera en términos de ciberespionaje industrial, hackeo o robo intelectual sino que aborda la aplicación del derecho internacional en el uso de la fuerza y conflictos armados.

De igual modo, el Manual de Tallin se focaliza en las operaciones *cyber-to-cyber* en sentido estricto. Por ejemplo, una ciberoperacion contra los sistemas que conforman y gestiona la infraestructura crítica de un Estado y no el bombardeo convencional de un centro de control informático. Asimismo, el Manual aborda tanto los conflictos internacionales como los no-internacionales (Manual de Tallin, 2013)

De acuerdo al Manual, el proyecto que comenzó en el CCDCOE de la OTAN en 2009, convocó a un Grupo Internacional de Expertos que fueron cuidadosamente

seleccionados e incluía profesionales legales, académicos y expertos técnicos. Sobre esa base, la convergencia multidisciplinar se consideró esencial para la credibilidad final del producto.

Este hecho demuestra, por un lado, la necesidad de trabajar en forma cooperativa y coordinada para afrontar los actuales desafíos que se presentan a nivel global, y por la otra, la complejidad que evidencia el sistema internacional.

De este modo, tres organizaciones fueron invitadas para que provean observadores al proceso. Su misión sería participar activamente en los debates y diseño del Manual, pero su consentimiento no se consideraba necesario para la adopción de una determinada regla. Este grupo de observadores estaba integrado por el Comando Aliado de la OTAN, el Ciber Comando de los Estados Unidos y el Comité Internacional de la Cruz Roja (Manual de Tallin, 2013)

El Manual es un compilado de 95 reglas estructuradas en dos partes, la seguridad del ciberespacio en el Derecho Internacional y el Derecho Internacional de los Conflictos Cibernéticos, y en siete capítulos. Muchas de estas reglas son copias o adaptaciones de otras previamente existentes en tratados internacionales aplicadas al contexto de la ciberguerra (Reguera, 2015).

Sin embargo, teniendo en cuenta que son escasos los tratados internacionales, costumbre internacional u *opinio juris* que traten directamente con los ciberconflictos, esta incertidumbre no significa que las ciberoperaciones ocurran dentro de un total vacío normativo. El GIE señaló en forma unánime que el *jus ad bellum* y el *jus in bello* actualmente vigentes aplican a las ciberoperaciones (Manual de Tallin, 2013).

Por lo tanto, las reglas fueron adoptadas aplicando el principio del consenso dentro del GIE. Todos los expertos estuvieron de acuerdo que una vez formuladas, las reglas reproducían el derecho consuetudinario, al menos que fuera expresado explícitamente lo contrario.

Por otra parte, cada regla surgida luego de las deliberaciones y debates, está acompañada de un Comentario. Los comentarios son un intento de identificar la base legal, explicación, interpretación y las implicaciones prácticas en el cibercontexto.

Adicionalmente, incluyen diferentes perspectivas y posiciones de los expertos. (Manual de Tallin, 2013).

Vale destacar que las Reglas y los Comentarios fueron desarrollados y diseñados utilizando numerosas fuentes. En particular, se destacan tres: el estudio del Derecho Internacional Humanitario del Comité Internacional de la Cruz Roja, el Manual de Derecho Internacional Aplicable a la Guerra Aérea y Misilística de la Universidad de Harvard, y el Manual del Derecho para los Conflictos Armados No Internacionales de Michael Schmitt, Charles Garraway y Yoram Dinstein (Manual de Tallin, 2013).

Además, también se recurrió a los manuales militares de Canadá, Alemania, Reino Unido y Estados Unidos, considerados por el GIE como especialmente útiles durante el análisis legal y la investigación. Asimismo, el GIE invitó a quienes diseñaron los citados manuales a participar del proyecto para que aporten su visión invaluable en la gestación, base y significados de provisiones específicas (Manual de Tallin, 2013).

Conceptos significativos del Manual

El mérito más importante del Manual es que el GIE propone bajo el régimen de *lege lata* o, ley existente, una serie de reglas y definiciones. No obstante, reconoce que por su naturaleza específica, las armas cibernéticas pueden causar consecuencias imprevisibles e incontrolables. Asimismo, destaca el posible daño desenfrenado que un ciberataque puede ocasionar, particularmente en las infraestructuras críticas (Wegener, 2013).

En este sentido, Reguera (2015) resalta que el Manual buscó interpretar y adaptar las normas existentes en el derecho internacional a los ciberataques, vincular el derecho con las operaciones cibernéticas y valorar la capacidad de los Estados para alcanzar consenso acerca de los límites éticos en el ciberespacio.

La información contenida en el Manual está en su mayoría escrita en abstracto. Esto es así probablemente debido a que busca constituir un marco ético-legal internacional es un área donde los ciberataques son un fenómeno de naturaleza reciente.

A su vez, existen varias secciones del Manual donde los Estados miembros de la OTAN pueden utilizar como referencia para determinar si un ciberataque desencadenaría una respuesta de la Organización. En otras palabras, si bien el documento aún no tiene fuerza legal, puede ser utilizado como una guía de ayuda en caso de ciberataque (Jones, 2016).

De acuerdo a Reguera (2015), entre algunos aspectos claves del Manual se destacan:

- Ciberataque y conflictos del Derecho Internacional Humanitario
- Soberanía y responsabilidad
- Uso de la Fuerza
- Ataque armado
- Legítima Defensa, inminencia e inmediatez
- Principio de necesidad y proporcionalidad
- Participación directa en las hostilidades

De modo que, como señala Jones (2015), el Manual utiliza la opinión GIE y esboza escenarios para el desarrollo y aplicación de reglas que todavía no han sido utilizadas en conflictos graves y reales vinculados a ciberataques. Sin embargo, el Manual es un esfuerzo y un paso adelante significativo en la construcción de un marco legal relativo al ciberespacio.

Es importante destacar, que en muchos documentos políticos-militares relacionados al ciberespacio se priorizan la ciberdefensa y la cooperación de todos los agentes interesados, como por ejemplo, la Estrategia de Operaciones en Ciberdefensa del Departamento de Defensa de Estados Unidos.

Esto es consecuencia de que el control de los ataques digitales forman parte de un nuevo paradigma en seguridad donde la prevención, la resistencia y la defensa de infraestructuras digitales depende de un extenso armazón conformado por varios sectores y redes cooperativas (Wegener, 2013).

Los conceptos analizados confirman algunos puntos previstos en el marco del TFG. En primer lugar, la complejidad del sistema internacional, máxime si se lo examina desde el impacto que las relaciones que ocurren el ciberespacio tienen para los Estados miembros de la OTAN.

Estas complejas interacciones entre los múltiples actores y sus consecuencias imprevistas han revelado lagunas legales que de alguna manera hacen estériles los esfuerzos estatales, aún los más poderosos, para encontrar culpables y condenarlos. Ante este escenario, el uso de la fuerza armada y la configuración de poder como medidas preventivas o reactivas, no aparecen como los medios más adecuados en la búsqueda de soluciones sólidas.

En segundo lugar, la necesidad de cooperar entendida en la OTAN no sólo a nivel estatal, sino también desde la academia y las organizaciones internacionales en la búsqueda de herramientas y soluciones que apliquen a la problemática. Evidentemente, el derecho internacional solo puede funcionar en base a acuerdos y actitudes cooperativas.

Sin embargo, se debe superar la negativa de los Estados del sistema a someterse a obligaciones legales de tipo supranacional basándose en su derecho soberano. Como se ha visto, los Estados miembros de la OTAN ha dejado bien en claro que el Manual de Tallin no es un documento oficial de la OTAN ni tampoco refleja la posición de los Estados miembros.

En otras palabras, estos factores se pueden amalgamar en la postura de la OTAN y del CCDCOE. El reconocimiento formal hacia las nuevas amenazas destacados en las distintas cumbres y documentos oficiales y la creación de agencias e instituciones en el campo de la ciberseguridad lo confirman.

Asimismo, la invitación para conformar un grupo de expertos internacionales en el campo del derecho internacional es un signo de cambio de paradigma y de un clima de época diferente. Si se considera que el área de la seguridad tradicionalmente se caracterizó por el hermetismo y la desconfianza, esos son pasos que marcan una tendencia y una relación entre problemas comunes y soluciones cooperativas basadas en la participación de múltiples actores dentro de la estructura OTAN.

Conclusiones Preliminares

En sentido amplio, la lectura del Capítulo 4 conduce hacia una reivindicación del derecho internacional. Aún lejos de presentarse en términos kantianos, la preocupación compartida por los Estados miembros de la OTAN que integran el CCDCOE, de alcanzar una codificación del *jus ad bellum* y *jus in bello* para las operaciones cibernéticas, es en última instancia, un fuerte indicador de la importancia del derecho internacional para los Estados.

Estas preocupaciones, sumadas a la necesidad de normas que regulen las ciberoperaciones en el sistema internacional, motivaron que desde el CCDCOE de la OTAN se promueva la construcción de un marco codificador de reglas reguladoras para conflictos cibernéticos. Estas intenciones se concretaron en la publicación del Manual de Tallin en 2013, constituyéndose en un trascendente primer paso orientado a clarificar un ámbito que aún permanece en un cierto vacío legal.

Sin embargo, a diferencia de lo que ocurre generalmente cuando se trata de cuestiones técnicas, en temas de derecho internacional que conlleven para los Estados obligaciones que puedan ser vistas como una invasión a la soberanía, la cooperación estatal se hace mucho más dificultosa. En este sentido, los Estados miembros de la OTAN manifestaron en forma expresa que el Manual de ninguna manera refleja sus posiciones.

De todas maneras, el balance final es positivo considerando las motivaciones iniciales y el despliegue de recursos que los Estados miembros de la OTAN destinaron al estudio e investigación de una temática que representa un permanente desafío en términos de seguridad estatal y del sistema internacional en su totalidad.

CONCLUSIONES

El análisis y la investigación realizada en el marco del TFG exhibieron una serie de aspectos relevantes y resultados que merecen ser considerados.

Para comenzar, en los últimos 25 años la masiva expansión tecnológica alcanzó niveles inesperados llegando a tener una existencia omnipresente en la sociedad actual. Los cambios fueron tan profundos y veloces que las consecuencias del impacto aún no terminan de asimilarse en términos sociales, políticos, económicos y culturales.

A raíz de la evolución tecnológica y de la difusión hacia el uso público de nuevas formas de comunicación, el nivel de transformación que experimentó la humanidad fue tal, que los especialistas y académicos la pasaron a denominar Sociedad de la Información.

En cuanto al campo de acción, la plataforma donde se lleva a cabo toda esta revolución tecnológica es el ciberespacio. El ciberespacio tiene la particularidad de ser virtual y no físico. Además, posibilita interactuar en forma anónima y sin dejar rastros. Por lo tanto, implica todo un cambio de paradigma si se considera que existe naturalmente una concepción física en cuanto a la idea de interacciones humanas.

En muchos aspectos, las nuevas tecnologías de la mano del proceso de globalización, han contribuido a mejorar la calidad de vida de la sociedad mundial. Se ha alcanzado lo que se podría denominar *movilidad social tecnológica.* En la actualidad, es cada vez mayor el número de personas que se beneficia por un lado, de comunicaciones que relativizan las dimensiones tiempo/espacio, y por el otro, del acceso a la información y al conocimiento de calidad y gratuito.

De este modo, una de las características a que distingue a la Sociedad de la Información es su alta dependencia de los sistemas informáticos. La dependencia no se limita al ámbito personal, sino que abarca amplios espacios estructurales que los Estados requieren para su funcionamiento tanto en términos administrativos, económicos y productivos. Por su capital importancia han sido calificadas con el término de infraestructuras críticas.

Sin embargo, de la mano del uso masivo, las nuevas tecnologías comenzaron a ser utilizadas no sólo en términos de beneficios sino también como vehículos de amenazas. El estudio del caso, mostró que la movilidad social tecnológica, implicó la posibilidad de que actores no estatales difusos, tuvieran el acceso a conocimientos y tecnologías capaces de poner en riesgo las infraestructuras críticas, y por ende, la seguridad nacional de los Estados mediante ataques cibernéticos.

Como señala Lanús (2006) el presente escenario mundial esta condicionado por tres sucesos no esperados. La nueva globalización, que acelera flujos, erosiona soberanías y facilita la mundialización financiera. La caída del muro de Berlín que dio fin a la confrontación estratégica e ideológica Este-Oeste. Y, el ataque terrorista de Al Qaeda del 11S, que modificó la percepción de las amenazas y la visión del mundo por parte de los Estados. En otras palabras, estamos en presencia de un sistema internacional complejo, con capacidad de mutación, y que demanda respuestas acordes.

Ahora bien, considerando lo anterior y desde el análisis del caso, se constató que los ciberataques combinan cada uno de los tres fenómenos mencionados en uno solo. Son flujos acelerados de información, erosionan soberanías, no siguen patrones ideológicos y han modificado la percepción de amenaza de los Estados miembros de la OTAN. De esta manera, el fenómeno se complejiza alcanzando altos niveles de dificultad para resolverlo.

En este contexto, a medida que las redes informáticas se fueron expandiendo, las llamadas infraestructuras críticas de los Estados miembros de la OTAN pasaron a ser un objeto referente en cuánto a la necesidad de mantenerlas seguras de cualquier amenaza. No es posible prever con exactitud que podría suceder en el futuro si una central nuclear, una represa, o los sistemas de navegación aeroportuaria son blancos de un ataque informático que implique daños físicos.

Como se ha visto, estas previsiones se hicieron realidad en 2007 en el masivo ciberataques sufrido por Estonia. Durante tres semanas, el país báltico, uno de los más informatizados del mundo, fue blanco de un masivo ataque informático. El ataque paralizó buena parte de su funcionamiento poniendo en jaque a importantes sectores públicos y privados. El ataque motivó que Estonia solicitara ayuda a la OTAN y desencadenó toda una revisión de la doctrina de seguridad de la Organización.

De esta manera, la investigación del TFG estuvo orientada a analizar que tipo de políticas en ciberseguridad llevó adelante la OTAN como respuesta a los incidentes de Estonia. En otras palabras, una búsqueda de respuestas ante un fenómeno relativamente nuevo en el ámbito de las relaciones internacionales y que aportaran porciones de claridad teniendo en cuenta la actualidad y la potencialidad del tema de estudio.

En primer lugar, al término del análisis, la elección de la perspectiva institucionalista neoliberal se considera acertada teniendo en cuenta la mencionada complejidad del sistema internacional contemporáneo. Al mismo tiempo, la utilización de esta línea teórica se mostró apropiada en el área de la seguridad, un espacio donde habitualmente no es utilizada. En la actualidad, la agenda global se presenta múltiple y cada parcela o espacio de acción requieren de un alto grado de especialización y de trabajo multidisciplinario, coordinado y cooperativo por parte de los actores del sistema internacional.

El estudio de la gestación y desarrollo de las políticas en ciberseguridad de la OTAN demostró esa exigencia. La estructura creada por la OTAN para hacer frente a los desafíos en ciberseguridad, implicó la construcción de una serie de instituciones y agencias altamente especializadas. Asimismo, estas se encuentran organizadas dentro de una amplia red de coordinación e intercambio de información, en la búsqueda de una mayor eficiencia dentro de parámetros preestablecidos por los Estados miembros.

En segundo lugar, el componente central del TFG fue el concepto de intereses comunes de los Estados miembros de la OTAN en ciberseguridad. Como movilizadores y disparadores de prácticas cooperativas, el estudio reveló efectivamente que a medida que aumentaban las preocupaciones de los Estados miembros en ciberseguridad, mayores eran las prácticas cooperativas y la voluntad en crear y participar en instituciones ligadas al área.

Este hecho se puede constatar en las dos modificaciones que sufrió la doctrina de la OTAN en poco más de una década, con la adopción de los Conceptos Estratégicos de 1999 y 2010 donde se subraya reiteradamente la necesidad de cooperación y ayuda mutua. Del mismo modo, es visible en la continua y progresiva incorporación de instituciones y organismos ligados a la ciberseguridad dispuestos en las Cumbres de Praga, Bucarest, Lisboa y Chicago.

De manera semejante, los ejercicios conjuntos en ciberseguridad, las investigaciones desarrolladas desde el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, y la interacción con el sector privado-industrial verifican la existencia de intereses compartidos, que incluyen la participación de actores no estatales.

Este concepto quedaría plasmado en un *modelo transnacional en ciberseguridad.* El modelo, incluye al sector público contemplando sus intereses nacionales; al sector privado, y a las organizaciones internacionales como partes de un todo orientado hacia un objetivo común.

Por otra parte, el estudio reveló que la cooperación entre los Estados miembros de la OTAN en el ámbito de la ciberseguridad no es automática. No todos los Estados miembros de la OTAN forman parte del Centro de Excelencia de Ciberdefensa Cooperativa ni tampoco de los ejercicios cibernéticos. La cooperación requiere tiempo y negociación donde los intereses nacionales juegan un papel fundamental máxime en temas de seguridad. En este escenario, el debate entre seguridad nacional y privacidad individual asoma como uno los posibles temas a resolver en el campo de la ciberseguridad de los Estados miembros de la OTAN.

También cabe señalar, que desde la investigación se advierte que los intereses compartidos tienen su origen en intereses nacionales. Si bien los Estados miembros de la OTAN reconocen la necesidad de ayuda mutua ante una realidad compleja, los tiempos y los términos de la cooperación parecen ser decididos desde la percepción subjetiva y el aprendizaje de cada uno de los Estados.

Esta debilidad se manifiesta con fuerza cuando se ingresa al terreno del derecho internacional donde los Estados no parecen estar dispuestos a ceder control soberano en términos jurídicos.

En tal sentido, la promoción desde la OTAN a través del Centro de Excelencia de Ciberdefensa Cooperativa de un derecho aplicable a los conflictos en el ciberespacio mediante la confección y publicación del Manual de Tallin, se presenta como un valioso proyecto a largo plazo con la finalidad de cubrir un vacío importante del sistema internacional.

No obstante, a pesar de constituir un importante primer paso en esa dirección, la percepción que deja el estudio del caso es que queda mucho camino por recorrer a los Estados miembros de la OTAN debido a la continua evolución tecnológica sumada a la incertidumbre sobre la potencialidad que la misma pueda llegar a alcanzar. En otras palabras, existe un desacople de velocidades donde la legislación parece ir muy detrás de los cambios tecnológicos. A su vez, como se ha visto, a estos factores se le debe sumar la resistencia natural de los Estados a asumir obligaciones vinculantes que puedan implicar pérdida de la capacidad soberana.

En este contexto, y en lo que respecta a futuras investigaciones, sería interesante evaluar si existe una tendencia reactiva hacia la cooperación en el comportamiento estatal ante situaciones de extrema vulnerabilidad. Esta conducta estatal parece manifestarse reaccionando en dirección a una respuesta de tipo colectiva con participación estatal/no estatal y en la conformación de un marco institucional regulador. Es decir, los Estados parecen más proclives a asumir obligaciones multilaterales y de tipo cooperativa en casos de extrema vulnerabilidad.

Finalmente, y a modo de reflexión general, el estudio realizado en el marco del TFG evidenció la intensa transformación que sistema internacional sufrió en las últimas dos décadas. Las acciones que se llevan a cabo en el ciberespacio están modificando el paradigma de la seguridad de los Estados miembros de la OTAN en particular y de las relaciones humanas en sentido amplio.

En otras palabras, el ciberespacio y todo lo que ello implica, pasaron a formar parte de la cotidianeidad. Por lo tanto, es un imperativo para todos los Estados del sistema internacional profundizar los estudios relativos al ciberespacio y tomar acciones que contribuyan a conformar una sociedad humana más libre y segura.

Bibliografía

- Acosta, P., Pérez Rodríguez J. A., Arnaíz de la Torre, D., Taboso Ballesteros, P. (2009). Seguridad Nacional y Ciberdefensa. [*Versión Electrónica*]. Cátedra ISDEFE - Universidad Politécnica de Madrid

- Aggarwal, V. (2009). The Dynamics of Trade Liberation. En H. Milner y A. Moravcsik (Ed.) *Power, interdependence, and Nonstate Actors in World Politics* (pp. 164-182) Nueva Jersey, Estados Unidos: Princeton University Press.

- Areppim, (2013). Worldwide Internet users 2013 forecast. Recuperado de: http://stats.areppim.com/archives/insight_internetxfcstx2013.pdf

- Aronson, J. (2009). International Intellectual Property Rights in a Networked World. En H. Milner y A. Moravcsik (Ed.) *Power, interdependence, and Nonstate Actors in World Politics* (pp. 185-203) Nueva Jersey, Estados Unidos: Princeton University Press.

- Areng, L. (2014). Lilliputian States in Digital Affairs and Cyber Security. [*Versión Electrónica*]. En *The Tallinn Papers, Vol. 1,* (4), 1-12

- Artiles, Néstor G. (2011). Situación de la ciberseguridad en el ámbito internacional y en la OTAN. [*Versión Electrónica*], En *Retos y amenazas a la seguridad nacional en el ciberespacio***.** Instituto Español de Estudios Estratégicos , Cuadernos de Estrategia 149 (1), 167-214.

- Axelrod R. y Keohane R. (1985). Achieving Cooperation under Anarchy: Strategies and Institutions. *World Politics, Vol. 38* (1), 226-254.

- Barbé, E. (1989) *"Cooperación y conflicto en las relaciones internacionales (La teoría del régimen internacional)"*, Revista CIDOB d'Afers Internacionals, (17), 57-70

- Bartolomé, Mariano C. (2013). Un abordaje general a la Teoría de las Relaciones Internacionales. [*Versión Electrónica*]. Buenos Aires: Facultad de Derecho y Ciencias Sociales - Universidad de Belgrano

- Bendiek, A. (2014). Tests of Partnership. Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection. [*Versión Electrónica*]. *Transatlantic Academy Paper Series, Vol. 1* (1), 1-33.

- Brunet, P. (2016) Treinta preguntas sobre la OTAN Treinta años después del Referéndum. [*Versión electrónica*], *Centre Delàs d'Estudis per la Pau, Vol, 1* (1), 13-15

- Calvo, J. (2013). Ciberseguridad: nuevas amenazas, nuevos retos. Recuperado de: http://www.7enise.webcastlive.es/

- Caro Bejarano, M. (2011). La Nueva Política de Ciberdefensa de la OTAN. *Documento Informativo.* Instituto Español de Estudios Estratégicos.

Recuperado de http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI37-2011LaPoliticadeCiberdefensaOTAN.MJCaro.pdf

- Caro Bejarano, M (2012). Ciberdefensa. Equipos de Respuesta Inmediata de la OTAN. *Documento Informativo.* Instituto Español de Estudios Estratégicos.

Recuperado de http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI16-2012_NatoRapidReactionTeam_MJCaro.pdf

- Carr, J. (2014). Responsible Attribution: A Prerequisite for Accountability. [*Versión Electrónica*]. En *The Tallinn Papers, Vol. 1,* (6), 1-8

- Caton, J. (2016). NATO Cyberspace Capability: A Strategic and Operational Evolution. [*Versión Electrónica*]. Carlisle, Estados Unidos: Strategic Studies Institute

- Del Arenal, C. (2001). La nueva sociedad mundial y las nuevas realidades internacionales un reto para la teoría y para la política. [*Versión Electrónica*]. En *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz*, Universidad del País Vasco, 17-86

- Díaz del Río Durán, J. (2011). La ciberseguridad en el ámbito militar.[*Versión Electrónica*]. En *Retos y amenazas a la seguridad nacional en el ciberespacio*. Instituto Español de Estudios Estratégicos , Cuadernos de Estrategia 149 (1), 218-256.

- Duque Santa María, R. (2015). Estados Unidos y el control sobre Internet. [*Versión Electrónica*]. Santiago de Chile: Instituto de Estudios Internacionales – Universidad de Chile.

- DeSombre, E. (2009). Power, Interdependence, and Domestic Politics in International Environmental Cooperation. En H. Milner y A. Moravcsik (Ed.) *Power, interdependence, and Nonstate Actors in World Politics* (pp. 147-163) Nueva Jersey, Estados Unidos: Princeton University Press.

- Fernández, Álvaro (2015). Estonia, baluarte de la seguridad europea. *El Orden Mundial*. Recuperado de http://elordenmundial.com/2015/08/estonia-ciberseguridad-europea/

- Ferrero, Julio A. (2013). La ciberguerra. Génesis y Evolución. [*Versión Electrónica*], En *Revista General de Marina. Ministerio de Defensa de España, 264* (1), 81-97

- Fojón Chamorro, E. (2014). La OTAN y la ciberdefensa. *Real Instituto Elcano.* Recuperado de http://www.blog.rielcano.org/la-otan-y-la-ciberdefensa/

- Geers, K. (2014). Pandemonium: nation states, national security, and the internet. [*Versión Electrónica*]. Tallin: Cooperative Cyber Defence Centre of Excellence.

- Gilligan, M. (2009). The Transaction Costs Approach to International Institutions. En H. Milner y A. Moravcsik (Ed.) *Power, interdependence, and Nonstate Actors in World Politics* (pp. 50-65) Nueva Jersey, Estados Unidos: Princeton University Press.

- Gilpin, R. (2001). Global Political Economy: Understanding the International Economic Order. [*Versión Electrónica*]. Nueva Jersey, Estados Unidos: Princeton University Press.

- Gisbert, T. (2016) Treinta preguntas sobre la OTAN Treinta años después del Referéndum. [*Versión electrónica*], *Centre Delàs d'Estudis per la Pau, Vol, 1* (1), 20-22

- Grieco, J. (1990). Cooperation among Nations: Europe, America and Non-Tariff Barriers to Trade. Ithaca, Estados Unidos: Cornell University Press.

- Healey, J., Van Bochoven, L. (2011). NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. [*Versión Electrónica*]. Estados Unidos: Atlantic Council.

- Healey, J., Jordan, K. (2014). NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. [*Versión Electrónica*]. Estados Unidos: Atlantic Council.

- Hegenbart, C. (2014). Semantics Matter. NATO, Cyberspace and Future Threats. [*Versión Electrónica*]. Roma: NATO Defense College.

- Hunker, J. (2010). Cyber war and cyber power. Issues for NATO doctrine. [*Versión Electrónica*]. Roma: NATO Defense College.

- Jones, Ken (2015). Ciber war: the next frontier for NATO. [*Versión Electrónica*]. California: Naval Postgraduate School.

- Joubert, Vicent (2012). Five years after Estonia's Cyberattacks: lessons learned for NATO? [*Versión Electrónica*]. Roma: NATO Defense College.

- Keohane, R. (1993*). Instituciones Internacionales y Poder Estatal.* Buenos Aires: Grupo Editor Latinoamericano.

- Keohane, R., y Nye, J. (1988). *Poder e Interdependencia. La política mundial en transición.* Buenos Aires: Grupo Editor Latinoamericano.

- Keohane, R. y Martin L. (1995). The promise of Institutionalist Theory. [*Versión Electrónica*]. En *International Security, Vol. 20*, (1), 39-51.

- Krasner, S. (1982). Structural causes and regime consequences: regimes as intervening variables. [*Versión Electrónica*]. En *International Organization, Vol. 36* (2), 185-205

- Krause, H. (2014). NATO on its way towards a comfort zone in cyber defence. [*Versión Electrónica*]. En *The Tallin Papers, Vol. 1* (3), 1-6

- Lanús, J. (2006). Dos visiones estratégicas: Europa y Estados Unidos. . [*Versión Electrónica*]. En *Agenda Internacional*, *Vol. 3*, (9), 34-43

- Leiderman, L. (2012). Policy making in 140 characters or less: NATO and social media. [*Versión Electrónica*]. Roma: NATO Defense College.

- Lejarza, Illaro E. (2014). Ciberguerrra, los escenarios de confrontación. *Documento de Opinión.* Instituto Español de Estudios Estratégicos. *(DIEEEO18-2014)*. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf

- Lewis, J. (2013). The role of offensive cyber operations in NATO's Collective Defence. [*Versión Electrónica*]. *The Tallinn Papers, Vol.1,* (8), 1-12

-------,(2014). Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms. [*Versión Electrónica*]. Washington: Center for Strategic & International Studies

- Litwak, R., y King, M. (2015). Arms control in cyberspace? [*Versión Electrónica*]. Washington, Estados Unidos: Wilson Center.

- Martin, L. y Simmons, B. (1998). Theories and Empirical Studies of International Institutions. En *International Organization Vol. 52* (4), 729-757. Recuperado de: https://dash.harvard.edu/bitstream/handle/1/3382862/Theories_Empirical.pdf?sequence=2

- Milner, H. (2009). Power, interdependence, and Nonstate Actors in World Politics: Research Frontiers. En H. Milner y A. Moravcsik (Ed.) *Power, interdependence, and Nonstate Actors in World Politics* (pp. 3-28) Nueva Jersey, Estados Unidos: Princeton University Press.

- Mitchell, R. (2009). The Influence of International Institutions: Institutional Design, Compliance, Effectiveness, and Endogeneity. En H. Milner y A. Moravcsik (Ed.) *Power, interdependence, and Nonstate Actors in World Politics* (pp. 66-84) Nueva Jersey, Estados Unidos: Princeton University Press.

- Ministerio de Defensa de Estonia (2013) Opinión Pública y Defensa Nacional. [*Versión Electrónica*]. Tallinn: Estonian Social and Market Research Company Saar Poll.

- Moravcsik, A (2009). Robert Keohane: Political Theorist. En H. Milner y A. Moravcsik (Ed.) *Power, interdependence, and Nonstate Actors in World Politics* (pp. 243-264) Nueva Jersey, Estados Unidos: Princeton University Press.

- NATO Review Magazine, (2016). *NATO: changing gear on cyber defence*. Recuperado de: http://www.nato.int/docu/Review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm

- Nye, J. (1987). Nuclear learning and U.S.-Soviet Security Regimes. [*Versión Electrónica*]. En *International Organization, Vol. 14,* (3), 371-402

- Nye, J. (2012). *Ciberguerra y Ciberpaz*. Recuperado de: https://www.project-syndicate.org/commentary/cyber-war-and-peace?version=spanish&barrier=accessreg

- Orozco, G. (2006). El concepto de la seguridad en la teoría de las relaciones internacionales. [*Versión Electrónica*]. Revista CIDOB d'Afers Internacionals, (72), 161-180

- Ortega, Pere (2016). Treinta preguntas sobre la OTAN Treinta años después del Referéndum. [*Versión electrónica*], *Centre Delàs d'Estudis per la Pau, Vol, 1* (1), 16-19

- OTAN, (2002). Prague Summit Declaration.
Recuperado de: http://www.nato.int/cps/po/natohq/official_texts_19552.htm?

----------, (2006). Riga Summit Declaration.
Recuperado de: http://www.nato.int/cps/in/natohq/official_texts_37920.htm

----------, (2008). Bucharest Summit Declaration
Recuperado de: http://www.nato.int/cps/in/natohq/official_texts_8443.htm

----------, (2009). NATO Allied Joint Doctrine for Information Operations AJP-3.10
Recuperado de: https://info.publicintelligence.net/NATO-IO.pdf

----------, (2009). NATO Parliamentary Assembly DSCFC 09 E bis. NATO and Cyber Defence. Myrli, N. (compilador).
Recuperado de: http://www.nato-pa.int/default.asp?SHORTCUT=1782

----------, (2010). New NATO Capstone Concept.
Recuperado de: http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

----------, (2010). Lisboa Summit Declaration
Recuperado de: http://www.nato.int/cps/po/natohq/official_texts_68828.htm

---------, (2011). NATO Cyber Defence. Fact Sheet. Recuperado de: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

----------, (2012). Chicago Summit Declaration
Recuperado de http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

----------, (2013). Framework for NATO-Industry Engagement.
Recuperado de: https://diweb.hq.nato.int/indrel/Shared%20Documents/FNIE_Brochure.pdf

----------, (2015). NATO Encyclopedia.
Recuperado de: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20160414_2015-nato-encyclopedia-eng.pdf

----------, (2016). Cooperative Cyber Defence Centre of Excellence. About Cyber Defence Centre. Recuperado de: https://ccdcoe.org/about-us.html

----------, (2016). NATO Industry Cyber Partnership. Welcome to the NATO Industry Cyber Partnership. Recuperado de: http://www.nicp.nato.int/

- Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. [*Versión Electrónica*]. En *NATO Cyber Defence Library*. Tallin: Cooperative Cyber Defence Centre of Excellence.

- Ottis, R. y Lorents, P. (2010). Cyberspace: Definition and Implications. Cooperative Cyber Defence Centre of Excellence.
Recuperado de: https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf

- Pinilla Morón, A. (2012). Análisis cruzado de las respuestas del Neoinstitucionalismo Neoliberal y del Constructivismo Social aplicadas al estudio de la OTAN y sus Estados miembros. [*Versión Electrónica*]. Bogotá: Universidad Colegio Mayor de Nuestra Señora del Rosario.

- Quivy R. y Van Campenhoudt (1998). *Manual de Investigación en Ciencias Sociales.* México: Editorial Limusa.

- Tickner, J. (2009). On Taking Religious Woldviews Seriously. En H. Milner y A. Moravcsik (Eds.) *Power, interdependence, and Nonstate Actors in World Politics* (pp. 223-240) Nueva Jersey, Estados Unidos: Princeton University Press.

- Ramirez Morán, D. (2014). La Ciberdefensa en la Cumbre de Gales de la OTAN. *Documento Informativo.* Instituto Español de Estudios Estratégicos. (*DIEEEI13-2014).* Recuperado de http:// www.ieee.es/Galerias/fichero/docs_informativos/2014/DIEEEI13-2014_Ciberseguridad_CumbreGales_DRM.pdf

- Red de Información de Andalucía (2004). La quinta ampliación de la Unión Europea. Estonia. Recuperado de http://www.andaluciaeuropa.com/descarga/publicaciones/ESTONIA.pdf

- Reguera, J. (2015) Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario. Grupo de Estudios en Seguridad Internacional. Recuperado de: http://www.seguridadinternacional.es

- Salomon, M. (2002). La teoría de las Relaciones Internacionales en los albores del siglo XXI: diálogo, disidencia, aproximaciones. *Revista Electrónica de Estudios Internacionales. (Núm. 4).* Recuperado de file:///D:/Users/usuario/Downloads/Salomon.PDF

- Sautu, R. (2003). *Todo es teoría. Objetivos y métodos de investigación.* Buenos Aires: Lumiere.

- Schmitt, M. (Ed.) (2013). *Tallinn Manual on The International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

- Schmitt, M. (2015). The Law of Cyber Targeting. [*Versión Electrónica*]. En *The Tallinn Papers, Vol.1,* (7), 1-20

- Schreier, F (2015). On Cyberwarefare. [*Versión Electrónica*]. Ginebra, Suiza: Centre for the Democratic Control of Armed Forces.

- Scmitt, M. and Vihul, L. (2014). The Nature on International Law Cyber Norms. [*Versión Electrónica*]. En *The Tallinn Papers, Vol. 1,* (5), 1-31

- Stretsov, A. A. (2007). International Information Security: Description and Legal Aspects. [*Versión Electrónica*]. En *Disarmament Forum Vol. 1* (3), 5-13

- Stone, R. (2009). Institutions, Power, and Interdependence. En H. Milner y A. Moravcsik (Eds.) *Power, interdependence, and Nonstate Actors in World Politics* (pp. 31-49) Nueva Jersey, Estados Unidos: Princeton University Press.

- Theiler, O. (2011). *New Threats: the cyber-dimension*. Recuperado de: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm

- Tikk, E. (2011). Comprehensive legal approach to cyber security. [*Versión Electrónica*]. Tartu: Tartu University Press.

- Tulchin, J. (2006). Creando una Comunidad de Seguridad en el hemisferio. En J. Tulchin, R. Benítez Manaut y R. Diamint (Ed.). *El Rompecabezas: conformando la seguridad hemisférica en el siglo XXI*. Buenos Aires, Argentina: Bononiae Libris.

- Veenendaal, M., Kaska, K., y Brangetto, P. (2016). Is NATO ready to Cross the Rubicon on Cyber Defence? [*Versión Electrónica*]. Tallin: Cooperative Cyber Defence Centre of Excellence.

- Vieytes, R. (2004). *Metodología de la Investigación en organizaciones, mercado y sociedad. Epistemología y técnicas.* Buenos Aires: Editorial de las Ciencias.

- Vihul, L. (2014). The Liability of Software Manufactures for Defective Products. [*Versión Electrónica*]. En *The Tallinn Papers, Vol. 1,* (2), 1-14

- Wegener, Henning (2013). Los riesgos económicos de la ciberguerra. [*Versión Electrónica*], En *La inteligencia económica de un mundo globalizado.* Instituto Español de Estudios Estratégicos, Cuadernos de Estrategia 162 (5)*,* 177-224.

ANEXO E – FORMULARIO DESCRIPTIVO DEL TRABAJO FINAL DE GRADUACIÓN

AUTORIZACIÓN PARA PUBLICAR Y DIFUNDIR TESIS DE POSGRADO O GRADO A LA UNIVERIDAD SIGLO 21

Por la presente, autorizo a la Universidad Siglo21 a difundir en su página web o bien a través de su campus virtual mi trabajo de Tesis según los datos que detallo a continuación, a los fines que la misma pueda ser leída por los visitantes de dicha página web y/o el cuerpo docente y/o alumnos de la Institución:

Autor-tesista *(apellido/s y nombre/s completos)*	Mauro Pessino
DNI *(del autor-tesista)*	21.635.096
Título y subtítulo *(completos de la Tesis)*	Las Políticas en ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN). Período 2008 - 2013
Correo electrónico *(del autor-tesista)*	pessino@red-belgrano.com.ar
Unidad Académica *(donde se presentó la obra)*	Universidad Siglo 21
Datos de Edición: *Lugar, editor, fecha e ISBN (para el caso de tesis ya publicadas), depósito en el Registro Nacional de Propiedad Intelectual y autorización de la Editorial (en el caso que corresponda).*	---

Otorgo expreso consentimiento para que la copia electrónica de mi Tesis sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21 según el siguiente detalle:

Texto completo de la Tesis *(Marcar SI/NO)*[1]	SI
Publicación parcial *(Informar que capítulos se publicarán)*	

Otorgo expreso consentimiento para que la versión electrónica de este libro sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21.

Lugar y fecha: Córdoba, 15 de noviembre de 2017.

Firma autor-tesista **Aclaración autor-tesista**

Esta Secretaría/Departamento de Grado/Posgrado de la Unidad Académica: _____certifica que la tesis adjunta es la aprobada y registrada en esta dependencia.

Firma Autoridad Aclaración Autoridad

Sello de la Secretaría/Departamento de Posgrado

[1] Advertencia: Se informa al autor/tesista que es conveniente publicar en la Biblioteca Digital las obras intelectuales editadas e inscriptas en el INPI para asegurar la plena protección de sus derechos intelectuales (Ley 11.723) y propiedad industrial (Ley 22.362 y Dec. 6673/63. Se recomienda la NO publicación de aquellas tesis que desarrollan un invento patentable, modelo de utilidad y diseño industrial que no ha sido registrado en el INPI, a los fines de preservar la novedad de la creación.