Themis

Recibido: octubre/2025
Aceptado noviembre/2025

Revista de la Facultad de Ciencias Jurídicas
de la Universidad Católica de Salta (Argentina)

Las implicancias de los ciberatentados ocurridos en el año 2007 en Estonia en la ciberdefensa de la Organización del Tratado del Atlántico Norte durante el período 2007 a 2017[1]

The consequences of the 2007 cyber-attacks in Estonia for the cyber defense of the North Atlantic Treaty Organization during the period 2007 to 2017

María Virginia Rueda [2]

Resumen

En el presente artículo se analizó cómo los ciberatentados sucedidos en la República de Estonia en el año 2007 motivaron a la Organización del Atlántico Norte a la creación de una política de ciberdefensa que pudiera proteger y defender tanto a la Alianza Atlántica como a los Estados miembros.

La importancia que la OTAN le asignó a la creación, el desarrollo y la ejecución de una política de ciberdefensa se puso de manifiesto, ya que tras los hechos, se demostró que la OTAN no tenía en práctica una política de actuación ante estos hechos. Si bien existían diferentes cumbres que tan solo mencionan la peligrosidad de los ciberatentados, no existía en la práctica una política.

Es por ello que, a partir de entonces, cada una de las decisiones que se tomó se especificaron en los textos emanados de las cumbres de la Alianza Atlántica, como en otros documentos importantes también creados durante el período de tiempo analizado, es decir, desde el año 2007 a 2017.

Palabras clave: ciberatentados, OTAN, política de ciberdefensa, Estonia, cumbres

Abstract

This article analyzes how the cyberattacks that occurred in the Republic of Estonia in 2007 motivated NATO to create a cyber defense policy that could protect and defend both the Alliance and its member states.

The importance NATO placed on the creation, development, and implementation of a cyber defense policy was evident when the events unfolded, as it became clear that NATO did not have a policy in place to respond to these events. Although various summits had simply mentioned the danger of cyberattacks, there was no policy in practice.

Therefore, from then on, each of the decisions taken was specified in the texts issued by the Alliance Summits, as well as in other important documents also created during the period analyzed, that is, from 2007 to 2017.

Keywords: Ciberatacks, NATO, ciberdefence policy, Estonia, summits

Relaciones Internacionales/ Trabajo final

Citar: Rueda, M. V. (2025). "Las implicancias de los ciberatentados ocurridos en el año 2007 en Estonia en la ciberdefensa de la Organización del Tratado del Atlántico Norte durante el período 2007 a 2017". *Themis*, 2 (2), pp. 75-94.

[1] El presente artículo es una adaptación de la tesis presentada y aprobada para obtener el título de Lic. en Relaciones Internacionales en la Facultad de Ciencias Jurídicas de la Universidad Católica de Salta en diciembre de 2024.

[2] Universidad Católica de Salta

INTRODUCCIÓN

El siguiente artículo tiene por objeto describir las implicancias de los ciberatentados sucedidos en Estonia en el año 2007 en las medidas adoptadas por la Organización del Tratado del Atlántico Norte (OTAN) en su política de ciberdefensa durante el período de 2007 a 2017.

Al partir de la premisa de que la OTAN se creó en el año 1949, cuyos valores fundamentales incluían vivir en paz y respetar las libertades y cuyos principales objetivos abarcaban la seguridad y la defensa de la organización y de los Estados miembros, ha resultado necesario que se adapte a los cambios propios de la vorágine del mundo, como también del avance de la tecnología, a fin de cumplir con ciertos objetivos específicos y buscar además nuevos socios internacionales.

No obstante, llegado el año 2007, la Alianza Atlántica se encontró con un nuevo desafío a la seguridad: los ciberataques. Es por ello que se busca caracterizar las políticas de ciberdefensa de la OTAN previas a los ciberatentados en Estonia de 2007 acordadas en las cumbres de Praga 2002 y de Riga 2006. Luego se analizará la evolución de la definición de ciberdefensa para la OTAN, se tratará de identificar los cambios sucedidos en la estructura orgánica de la OTAN provocados por la nueva política de ciberdefensa y, por último, se buscará describir la evolución del estudio del derecho internacional sobre la ciberdefensa dentro de la OTAN durante el periodo analizado.

El presente artículo permitirá describir el trabajo realizado por la OTAN en los diez años analizados y cómo los ciberataques influyeron en la creación de una política de ciberdefensa de la Alianza Atlántica .

Con el objetivo de llevar a cabo este trabajo, se recurrió a la teoría de la securitización promulgada por Barry Buzan, Ole Waever y Jaap De Wilde. Estos aportes surgieron durante el fin del siglo XX y llegaron a ser más específicos al final de la Guerra Fría, dónde la lógica bipolar (Verdes-Montenegro Escanez, 2015: 111-131) se termina y la concepción de la seguridad-defensa que se mantuvo a raíz de los años de confrontación entre Oriente y Occidente comenzó a cambiar y, por ende, a dar lugar a que nuevos teóricos pudieran compartir sus aportes e incluir en la agenda de la seguridad-defensa nuevos temas que antes solo se restringían al ámbito militar.

Las amenazas a la seguridad de un Estado han existido desde tiempos inmemorables. Es así que las medidas tomadas desde el campo de la defensa para asegurar y garantizar la seguridad también son sumamente antiguas. Sin embargo, en nuestra realidad, en estos últimos años los encargados de la defensa y de la seguridad se toparon con nuevas amenazas: las ciberamenazas.

La teoría de la securitización se basa en ciertos conceptos, como ser el uso de una retórica específica y el uso de un acto discursivo, la existencia de un objeto referente, la adopción de medidas extraordinarias o especiales, la existencia fundamental de la audiencia y el actor securitizador.

Teniendo en cuenta los aspectos metodológicos, este trabajo utilizará como unidad de análisis a la OTAN y, en específico, como única variable, a la política de ciberdefensa mediante un análisis a partir de diferentes dimensiones como, por ejemplo, lo político, lo militar, lo técnico y lo jurídico. Será una investigación de tipo descriptiva-básica y su alcance temporal será longitudinal-retrospectivo (González de Cruz, 2008: 35). Se considerarán como población todos los textos emanados por la OTAN durante los años analizados, y la muestra será no probabilística por conveniencia.

LA ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE (OTAN)

La Organización del Tratado del Atlántico Norte se creó en el año 1949 en un contexto histórico conocido como la Guerra Fría. Esta organización nació a raíz del Tratado de Washington, celebrado el 4 de abril de 1949 en la ciudad de Washington, D.C., Estados Unidos, firmado por doce países miembros[3]. El texto cuenta con un preámbulo, en el cual se reafirman los propósitos y los principios de la Carta de las Naciones Unidas (el deseo de vivir en paz, el respeto por las libertades individuales, la civilización, la democracia, el imperio de la ley), como así también la búsqueda de la estabilidad y el bienestar de los miembros de la Alianza Atlántica; y catorce artículos, los cuales nunca han sido modificados hasta el momento. Además, la razón de ser de la OTAN responde al artículo 51 de la Carta de la ONU, que reafirma el derecho de los países al uso del derecho de la legítima defensa, ya sea de forma individual o de forma colectiva. Tanto es así, que en el artículo 5 del Tratado de Washington se consagra dicha defensa colectiva.

La OTAN es una alianza que busca garantizar a sus miembros la libertad y la seguridad por medios de tipo político y militar. De acuerdo con la OTAN, desde lo político se "promueve valores democráticos y permite que los miembros se consulten y cooperen en cuestiones relacionadas con la defensa y la seguridad para solventar problemas, fomentar la confianza y, a largo plazo, evitar conflictos", y desde lo militar se "tiene un compromiso de resolución pacífica de controversias. Cuando los esfuerzos diplomáticos no dan fruto, la fuerza militar emprende operaciones de gestión de crisis. Estas operaciones se llevan a cabo bajo la cláusula de defensa colectiva (...) o por mandato de las Naciones Unidas" (North Atlantic Treaty Organization, 2023).

En la actualidad la OTAN cuenta con treinta y dos miembros y es una de las organizaciones internacionales más importantes del mundo, que fomenta un vínculo único entre dos continentes y les permite alcanzar la cooperación en los objetivos en común.

LA CIBERDEFENSA EN LAS CUMBRES DE PRAGA Y RIGA

La ciberdefensa debe entenderse como "la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques" (MC0571 North Atlantic Treaty Organization, 2012:42). Esta es parte de la tarea central de la defensa colectiva de la OTAN, por lo que el enfoque principal de la Alianza Atlántica en ciberdefensa es proteger sus propias redes, operar en el ciberespacio (incluso a través de las operaciones y misiones de la organización), ayudar a los aliados a mejorar su resiliencia nacional y proporcionar una plataforma para la consulta política y la acción colectiva (North Atlantic Treaty Organization, 2022).

El primer ciberataque que recibió la OTAN ocurrió en 1999 durante la *Operation Force Allied,* a raíz del ataque producido de forma accidental cuando se bombardeó la Embajada de China en Belgrado. Los *hackers* de nacionalidad rusa, serbia y china llevaron a cabo acciones tales como ataques de denegación de servicios y *defacement* a las páginas web del Cuartel General Supremo de las Potencias Alia-

[3] Los doce países originarios de la OTAN fueron Bélgica, Canadá, Dinamarca, Estados Unidos, Francia, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal y Reino Unido.

das de Europa (SHAPE, por sus siglas en inglés), como así también al ejército de los EE. UU. (North Atlantic Treaty Organization, 2014). La *Operation Force Allied* duró setenta y ocho días, inició el 24 de marzo de 1999 y finalizó el 10 de junio del mismo año. Se produjo a raíz de los conflictos que sucedieron en la antigua República Federativa de Yugoslavia (RFY), cuando las fuerzas serbias atacaron a la población albanesa. La Alianza Atlántica sostiene que el fin consistió en detener la catástrofe humanitaria que acontecía en Kosovo y se dio a raíz de que no se pudo solucionar por vía diplomática. La operación consistió en ataques aéreos sobre objetivos militares (North Atlantic Treaty Organization, 2022). No obstante, existieron ataques a infraestructuras no militares donde murieron civiles, como, por ejemplo, el bombardeo a la Estación de Radio y Televisión (ERT), el incidente en el puente del ferrocarril Grdelica (Montoya Pino, 2010) y el bombardeo accidental a la Embajada China.

Es en la Cumbre de Praga del año 2002, cuando se mencionó la necesidad de fortalecer las capacidades a fin de defenderse de los ciberataques (North Atlantic Treaty Organization, 2002) se dio origen a una política de ciberdefensa naciente que recién inició su desarrollo, pero ya había dado su primer paso: la creación de un nuevo órgano, el NATO Computer Incident Response Capability (NCIRC), que tiene como objetivo prevenir, detectar y responder ante ciberincidentes o incidentes informáticos (North Atlantic Treaty Organization, 2014). El NCIRC trabaja desde su sede en Bélgica, es parte de la NATO Communications and Information Agency y protege las 24 horas las redes de la Alianza Atlántica. Además, cuenta con expertos que integran la organización y comparten información sobre los nuevos ciberdesafíos (North Atlantic Treaty Organization, 2021).

Cabe recordar que el eje de la cumbre de 2002 tuvo como eje principal las consecuencias del ataque del 11S en los Estados Unidos, lo que provocó la aplicación por primera vez del derecho de legítima defensa tanto del artículo 51 de la Carta de ONU como del artículo 5 del Tratado de Washington, por lo que no existió un mayor desarrollo de la temática para la fecha.

Luego, en la Cumbre de Riga de noviembre del año 2006, se señaló que la OTAN continuaba trabajando con el objetivo de mejorar sus capacidades contra los desafíos y las amenazas contemporáneas. En consecuencia, se creó el programa NATO Network Enabled Capability (NNEC) que surgió como necesidad a fin de reducir la brecha tecnológica entre los países aliados (Moreira, 2010: 1). Este programa tiene como eslogan "compartir para ganar", es decir, su objetivo se enfoca en que la distribución de la información obtenida genere la toma de mejores decisiones por parte de los órganos competentes, en lugar de la designación de nuevas autoridades, con el fin último de salvar vidas, recursos y fomentar la cooperación entre las naciones. Cuenta con componentes fundamentales, como la superioridad de la información, es decir, garantizar que la información correcta llegue a las personas correctas, lo que, según la Alianza Atlántica, implica una ventaja operativa. Plantea que esto será posible gracias al intercambio de información entre los diferentes actores, lo que genera una reducción en el tiempo a la hora de la toma de decisiones. El NNEC plantea beneficios tales como una eficiencia mejorada, que se basa en métodos más seguros, al proveer una mejor distribución y calidad de la información y la posibilidad de decisiones más rápidas y eficaces (North Atlantic Treaty Organization, 2015).

ESTONIA Y LOS CIBERATAQUES

La República de Estonia es un país con una historia basada en ocupaciones, conquistas y lucha por la independencia a lo largo de los siglos. Por lo tanto, al examinar la historia del país báltico del siglo XX, se evidencia cómo los conflictos han sido un factor constante también en este centenario.

Tras la llegada de los bolcheviques al Palacio de Invierno, debido a la Revolución rusa, los estonios decidieron aprovechar la circunstancia e independizarse por primera vez del Imperio Ruso. Por consiguiente, en 1920 se firmó el Tratado de Paz de Tartu, en el cual Rusia renunciaba a todas sus pretensiones en Estonia. Por ende, Estonia se convirtió por primera vez en un país independiente. Este nuevo país adoptó una constitución de corte liberal; sin embargo, el crac del 29 impactó de fuerte manera sobre su economía naciente, lo que la dejó devastada por completo.

Durante casi quince años, Estonia logró avances en materia política, educativa y social, como así también comenzó a ocupar un lugar en las relaciones internacionales, mediante la integración en la Sociedad de las Naciones. No obstante, la calma y los avances llegarían a su fin cuando, a raíz del pacto secreto conocido como Molotov-Ribbentrop, que se celebró entre la Alemania Nazi y la Unión de Repúblicas Socialistas Soviéticas (URSS) en el año 1939, se dividiría en dos como lo habían acordado Hitler y Stalin, al igual que ocurrió con otros países del resto de Europa del Este.

La Segunda Guerra Mundial tuvo un fuerte impacto en la nación báltica, ya que las principales ciudades de esta región fueron bombardeadas; sin embargo, recibieron con los brazos abiertos a los nazis luego de la operación Barbarroja y se unieron a la defensa nacional, pero los alemanes no reconocieron a Estonia como un Estado independiente, sino como un territorio ocupado por la URSS; fusilaron a miles de estonios (judíos, colaboracionistas comunistas), y muchos otros huyeron y formaron parte del regimiento estonio del ejército francés. Toda esta situación dejó como consecuencia la pérdida de un cuarto de la población estonia.

Durante los años que duró la Guerra Fría, Estonia se vio anexada a la URSS una vez más, como así también a su modelo económico y político, lo que la llevó a padecer las duras condiciones de vida de la política totalitaria de Stalin. Por lo tanto, surgieron diversos grupos de resistencia, como los *Metsavennad* ("Hermanos del bosque"), que no implicaron un gran impacto para el ejército soviético.

Tras distintas revueltas y desobediencias a Moscú, Estonia llamó a elecciones libres en 1990. Como resultado, recuperaron la independencia en 1991 una vez más. Asimismo, sancionaron una nueva constitución en 1992. A partir de entonces, el Internet supuso un recurso fundamental en la modernización y el desarrollo de las infraestructuras del país. Esta red permitió que se llevaran a cabo distintas acciones tales como la adquisición del dominio nacional *.ee*, como así también la creación de dominios con fines de investigación, educación e innovación, como *kfbi.ee*, es decir, el Keemilise ja Bioloogilise Füüsika Instituut (Instituto Nacional de Física Química y Biofísica), o *ioc.ee*, que designa al Instituto de Cibernética. Otras medidas conllevaron la aplicación del proyecto Salto del Tigre (*Tiigrihüppe* en estonio), por el que todas las escuelas para el año 2000 tendrían computadoras e Internet y se fomentaría la innovación en la Nación estonia.

En la actualidad, Estonia se conforma de quince estados, su capital es Tallin, limita al norte con el golfo de Finlandia, al este con Rusia, al oeste con el mar Báltico y al sur con Letonia. Además, buscó acercarse e integrarse al

mundo occidental al unirse a la UE, a la OTAN, a la Organización para la Cooperación y al Desarrollo Económico (OCDE) y al implementar el uso del euro en 2011 (Lonely Planet, s.f.). Estonia es uno de los países más informáticos del mundo; por ejemplo, los habitantes pueden acceder a distintas páginas a fin de realizar actividades de la vida cotidiana como el *Digital ID* (DNI digital), *i-voting* (voto electrónico desde cualquier pc), *e-law* (consultar sobre decisiones parlamentarias), *e-bank* (realizar transacciones financieras a través de la banca virtual), *e-education* (acceso a notas, formularios, registros, inscripciones por parte de padres, alumnos e instituciones educativas), *electronic health registry* y la *e-prescription* (para acceder a registros médicos como a recetas) (Pessino, 2017: 35) entre otros.

Sin embargo, en 2007, Estonia padeció por primera vez en su historia un ataque a su seguridad: los ciberataques. Se iniciaron en medio de una situación compleja social, la cual se produjo a raíz de la decisión del Gobierno de Estonia de retirar una estatua del soldado de bronce hacia las afueras de Tallin, lo que causó movilizaciones y enfrentamientos entre grupos prorusos como proestonios.

Los ciberataques se desarrollaron en dos etapas. En la primera, los objetivos fueron simples: páginas web del Gobierno de Estonia. Sin embargo, a medida que el conflicto avanzaba entre la población, los ciberataques también se complejizaron, lo que dio inició a una segunda fase, la cual se basó en ataques más complejos y objetivos más variados.

> Los ataques consistieron en una serie de operaciones cibernéticas muy sofisticadas a través de múltiples conexiones, los llamados *botnets*, que inundaron los servidores del país con una cantidad de información mayor de la que podían gestionar. De esta manera, los atacantes convirtieron en «zombis» a cerca de un millón de ordenadores, a los que ordenaron saturar las redes hasta que los servidores colapsaron. Estonia, uno de los países más pequeños de la OTAN, pero también uno de los más conectados, se paralizó virtualmente. (Fuente Cobo, 2022: 84-91)

No obstante, el daño a la infraestructura física fue mucho menor al causado a la infraestructura cibernética de Estonia. A partir de estos hechos, el Gobierno estonio se puso en contacto con la OTAN, en relación con el artículo 4 del Tratado Antártico. Sin embargo, la OTAN no contemplaba un plan de acción ante estos hechos contra la seguridad de los aliados. Por consiguiente, iniciaría a raíz de estos sucesos un nuevo desafío para la mayor alianza político-militar en materia de seguridad y defensa.

REACCIÓN DE LA OTAN

Tras el ciberatentado a Estonia, la OTAN comprendió la necesidad y la importancia estratégica de que la ciberdefensa fuera parte de su estrategia de defensa, ya que había surgido una nueva amenaza a la seguridad, a la integridad de los Estados y de la Alianza Atlántica y la necesidad, entonces, de securitizar los ciberataques. Los ciberataques demostraron la vulnerabilidad de la OTAN, es así que, a partir de 2007, se llevaron sucesivas cumbres en las cuales la temática de los asuntos cibernéticos han tenido un lugar de importancia. Asimismo, se describió a los ciberataques como una amenaza para la OTAN, amenazas que han evolucionado en sofisticación y que pueden llegar a ser tan dañinas como un ataque convencional. Por otro lado, los resultados de las cumbres son de gran importancia, ya que es el momento de reunión entre los representantes de cada país y suponen la aquiescencia de la toma de medi-

das por parte de todos los Estados miembros, es decir, cada medida y opinión que se expresa en estos textos significa la voluntad común de todos los Estados partes.

LA CUMBRE DE BUCAREST

En la Cumbre de Bucarest celebrada en abril de 2008, donde los jefes de Estado y de Gobierno de los países miembros de la OTAN se reunieron en Bucarest, se abordó la decisión de la Alianza Atlántica de crear por primera vez una política de ciberdefensa. La misma manifiesta que la protección de los sistemas de información críticos, como así también la distribución de las mejores prácticas y la provisión de recursos de apoyo a las naciones aliadas a fin de evitar ciberataques es fundamental para la OTAN y los Estados miembros (North Atlantic Treaty Organization, 2008). Esto significa que, a raíz de lo sucedido, la Alianza Atlántica comprendió la importancia de esta nueva amenaza y que, sin un trabajo cooperativo, los resultados serían insignificantes. También la OTAN indicó que los Estados deben trabajar para poder alcanzar esta seguridad.

También es importante destacar que se reafirma como valor fundamental de la OTAN la divulgación de la información, el diálogo y la cooperación. Estos valores son fundamentales para poder cumplir con los objetivos de estabilidad y seguridad en la región euroatlántica (North Atlantic Treaty Organization, 2008).

A partir de esta cumbre, la OTAN llevó a cabo un verdadero avance técnico y político (Healey y Jordan, 2014) en materia de ciberdefensa, al crear una política de ciberdefensa, como así también los órganos necesarios para su cumplimiento.

A su vez, se crearon nuevas estructuras organizativas a fin de proporcionar una respuesta al problema planteado. La primera estructura se trató del Consejo de Gestión de la Ciberdefensa (CDMB, por sus siglas en inglés o *Cyber Defence Management Board*), que tiene el fin de encargarse de la coordinación y la planificación estratégica de la ciberdefensa en todos los órganos, ya sean civiles o militares de la OTAN. Este consejo se conforma de los principales responsables políticos, militares, operativos y técnicos de todos los organismos vinculados a la ciberdefensa de la OTAN, como por ejemplo, el Mando Aliado de Operaciones (ACO, por sus siglas en inglés o *Allied Command Operations*), el Mando Aliado de Transformación (ACT, por sus siglas en inglés o *Allied Command Transformation*), entre otras agencias de la OTAN. Por otro lado, el CMBD también tiene como función fomentar el intercambio de información y la asistencia mutua (Cooperative Cyber Defense Center of Excellence, s.f.) entre las distintas naciones. A su vez, se encarga de la Autoridad de Gestión para la Ciberdefensa (CDMA, por sus siglas en inglés o *Cyber Defense Management Authority*), cuyo objetivo se basa en ayudar a los Estados miembros de la Alianza Atlántica a mejorar sus propias capacidades de ciberdefensa (Haley y Jordan, 2014), como así también dictaminar los principales aspectos de la política de ciberdefensa de la OTAN (European Parliament, s.f.).

El *Cooperative Cyber Defense Center of Excellence* (CCDCOE, por sus siglas en inglés), otro órgano que también surgió para la fecha, se creó como iniciativa de Alemania, Italia, Estonia, Letonia, Lituania, Eslovaquia y España y tiene el estatus de organización militar internacional, título concedido por el Consejo del Atlántico Norte. Este órgano no es "una unidad operativa perteneciente a la Estructura de Mando de la OTAN, pero sí pertenece a una red de Centros de Excelencia acreditados por la OTAN" (Cooperative Cyber Defense Center of Excellence, s. f.). Esto significa que estos cen-

tros son organizaciones militares internacionales que educan a líderes y especialistas de los países miembros y socios de la OTAN. Además, aportan conocimientos que benefician y apoyan a la Alianza Atlántica que ayudan a evitar el malgasto de recursos y activos (North Atlantic Treaty Organization, 2024).

Este Centro de Excelencia tiene como misión la cooperación con la OTAN a través de actividades vinculadas a la ciberdefensa y a la ciberseguridad, ya sea en el marco legal, la investigación, el entrenamiento, los ejercicios de ciberdefensa, las conferencias, entre otros. Desde su creación ha llevado a cabo diferentes actividades fundamentales que han generado un gran aporte a la OTAN, como por ejemplo ejercicios desarrollados de manera exclusiva por este Centro de Excelencia o al acompañar a los ejercicios propios de la OTAN, como por ejemplo, los ejercicios internacionales de ciberdefensa, conocidos como *Locked Shields* (LS) que se organizan de manera anual. En ellos simulan un ciber incidente masivo, en el cual deben proteger los sistemas militares y de información en conjunto con las estructuras críticas y practicar la toma de decisiones estratégicas y la comunicación. *Crossed Swords* (CS, por sus siglas inglés) es un ejercicio internacional, por lo que se desarrolla en diferentes lugares a la vez y busca mejorar las habilidades cibernéticas a fin de prevenir, detectar y responder a un adversario ante un escenario real a gran escala, al experimentar con nuevas tecnologías y nuevas formas de ciberataques (CybExer, 2020).

Por otro lado, existen los siguientes ejercicios en los cuales participa el CCDCOE:

- *Cyber Coalition* es el principal ejercicio colectivo de ciberdefensa de la OTAN, que se realiza de manera anual y se planifica y desarrolla por el ACT. Supone la unión de órganos, aliados y socios de la OTAN a fin de fortalecer las capacidades de disuasión, defensa y, de esa manera, poder contrarrestar las amenazas en el ciberespacio.
- *Trident Jaguar* es un ejercicio operativo en el cual se pone a prueba la capacidad y la preparación militar de la OTAN, que se lleva a cabo a través de respuestas a crisis que suponen el uso de habilidades de combate de alta intensidad en situaciones que no suponen la aplicación del artículo 5 del Tratado de la OTAN.
- *Trident Juncture* es un ejercicio que tiene como fin poner a prueba la capacidad de la OTAN de planificar y ejecutar una operación sobre la defensa colectiva, es decir, "el objetivo general de la OTAN es demostrar la credibilidad de su disuasión militar y la unidad de sus miembros" (Council on Foreign Relations, 2018), que las tropas se encuentren entrenadas y que sean capaces de enfrentar cualquier amenaza.
- *Coalition Warrior Interoperability Exercise* (CWIX), es un ejercicio desarrollado por la OTAN desde el año 1999, en el cual se busca poner en práctica la cooperación con base en el intercambio de tácticas, técnicas y procedimientos con el objetivo de mejorar la detección de ciberincidentes y el tiempo de respuesta necesario a fin de identificar y resolver nuevas amenazas que atenten contra la seguridad (Cooperative Cyber Defense Center of Excellence, s.f.).

Otro órgano creado en la cumbre de Bucarest consistió en el *Rapid Reaction Teams* (RRT, por sus siglas en inglés). Los RRT son pequeños equipos conformados por personas que pueden desplegarse, ya sea en las sedes de la OTAN como también en el país en el que padecieron un ciberataque. Se pone en marcha una vez que algún país miembro de la OTAN solicita la ayuda tras haber sufrido un ciberataque.

Luego, el CDMB lo evalúa y, una vez que se activan aquellos pequeños equipos, comienzan a trabajar a las 24 horas (North Atlantic Treaty Organization, 2012). Para esto, cuentan con todo el equipamiento necesario, como, por ejemplo, equipos informáticos y de telecomunicaciones, teléfonos satelitales y equipos de recolección de evidencia digital, análisis de forensia digital, entre otros (North Atlantic Treaty Organization, 2012).

LA CUMBRE DE ESTRASBURGO/KEHL

Durante la Cumbre de Estrasburgo/Kehl del año 2009, se remarcó la existencia de nuevas amenazas, como los ciberataques, entre otros, por lo que se planteó la necesidad de mejorar las capacidades de respuesta, como también compartir los riesgos y la responsabilidad entre los miembros de la OTAN. Se estableció que es fundamental la cooperación con otros actores internacionales, como las organizaciones internacionales y otros países socios (North Atlantic Treaty Organization, 2009). Se reafirmó una vez más la importancia de la existencia y el desarrollo de la política de ciberdefensa aprobada en Bucarest, como así también la necesidad del trabajo en equipo, tanto de la Alianza Atlántica, de los Estados miembros y las organizaciones internacionales (North Atlantic Treaty Organization, 2009). Se subraya la importancia de comprender a los actores internacionales como un componente esencial de la política de ciberdefensa de la OTAN.

LA CUMBRE DE LISBOA

En noviembre de 2010, en la ciudad de Lisboa, se desarrolló una nueva cumbre, la cual inició con una descripción de las ciberamenazas. Explicaron que este tipo de peligros aumentan de forma rápida y mejoran su sofisticación día tras día, por lo que, a fin de acceder de forma constante y permanente al ciberespacio por parte de la OTAN, se decidió incorporar la dimensión cibernética en los nuevos conflictos, como en la doctrina de seguridad. Asimismo, se resolvió que se mejoraría la capacidad para detectar, evaluar, prevenir, defender y recuperar en caso de un ciberataque contra la infraestructura, que se pondría bajo protección a todos los organismos de la Alianza y que se fomentaría el desarrollo de las capacidades de ciberdefensa de los países aliados, al fomentar el intercambio de información (North Atlantic Treaty Organization, 2010). En este sentido, se reafirma la importancia del trabajo conjunto (tal como se había realizado las cumbres anteriores) y la cooperación con otros actores internacionales, como la UE y la ONU, a fin contrarrestar las amenazas del ciberespacio (North Atlantic Treaty Organization, 2010).

Además, se destacó la solicitud al Consejo para que la Política de Ciberdefensa, acordada en la Cumbre de Bucarest, se revisara y reformara antes de 2011 y para que, a su vez, se elaborara un plan de acción complementario. (North Atlantic Treaty Organization, 2010).

Durante ese mismo período, 2010 fue un año en el cual surgieron múltiples documentos importantes sobre la ciberdefensa para la OTAN. Entre ellos, se destacó el nuevo Concepto Estratégico, es decir, el Séptimo Concepto Estratégico desde que se creó la OTAN en 1949, que se considera una herramienta estratégica de la OTAN, plasmada por medio de un documento escrito. En un Concepto Estratégico se ponen de manifiesto los objetivos y los propósitos a largo plazo (por lo general, a diez años), las tareas a desarrollar en el ámbito de la seguridad de manera que respondan a los constantes desafíos mundiales de seguridad en el cual

surgen, al establecer líneas de acción tanto en el ámbito militar como político (North Atlantic Treaty Organization, 2010).

El Séptimo Concepto Estratégico, que salió a la luz en noviembre, titulado como *Active Engagement, Modern Defence* planteó los objetivos y los valores estratégicos de la OTAN, teniendo como eje principal a la defensa colectiva, el manejo de crisis y la seguridad cooperativa (North Atlantic Treaty Organization, 2010).

Dicho Concepto Estratégico plantea que los ciberataques tienden a ser más comunes, más dañinos, más organizados, lo que provoca daños mayores a los Gobiernos, a las empresas, a las economías, como así también ocasionan daños significativos al transporte, a las redes de suministro y a otras infraestructuras críticas. Por ende, los ciberataques implican una gran amenaza para la prosperidad, la seguridad y la estabilidad de la Alianza Euro-Atlántica. Además, expresa que pueden ser autores de los ciberataques tanto militares extranjeros, servicios de inteligencia, grupos terroristas o extremistas, como así también el crimen organizado (North Atlantic Treaty Organization, 2010).

Por lo tanto, planteó que es menester para la organización un mejor desarrollo de las capacidades que presenten el objetivo de prevenir, detectar, defenderse y recuperarse de los ciberataques; al hacer uso del proceso de planificación de la OTAN a fin de mejorar y coordinar las capacidades nacionales de ciberdefensa y fomentar la integración de respuesta de los países miembros de la Organización (North Atlantic Treaty Organization, 2010).

En junio de 2011, la OTAN informó la publicación de una nueva política de ciberdefensa revisada por los Ministros de Defensa, la cual siguió los lineamientos planteados en el Concepto Estratégico de 2010 y planteó varios ejes, tales como los siguientes:

- la creación de un plan de acción, el cual servirá como herramienta para la implementación de la política de ciberdefensa;
- la cooperación en ciberdefensa entre los países miembros y las organizaciones internacionales, que incluye por primera vez al sector privado como al mundo académico;
- la coordinación de toda la Organización en ciberdefensa, con especial foco en la prevención de las ciberamenazas y en la construcción de la resiliencia;
- la aclaración de los mecanismos tanto políticos como operativos para la respuesta contra los ciberataques;
- la integración de la ciberdefensa dentro del Proceso de Planificación de Defensa de la OTAN (NDPP, por sus siglas en inglés) (North Atlantic Treaty Organization, 2011).

Esta política, junto con el plan de acción, implicaron, por lejos, una de las más importantes acciones que ha tomado la Alianza Atlántica para la maduración de las cibercapacidades y en favor de las estructuras de gobernanzas.

Se remarcó que el artículo 4 del Tratado de Washington, el cual se refiere a la consulta mutua entre los países aliados cuando un hecho atente contra la integridad territorial, política, la independencia o la seguridad, es aplicable también a los asuntos cibernéticos y deja entrever que también es posible aplicar el artículo 5 sobre la defensa colectiva si el ciberincidente generará daños extremos (Haley y Jordan, 2014).

LA CUMBRE DE CHICAGO

En mayo de 2012, en la ciudad de Chicago, los países miembros de la OTAN celebraron una nueva cumbre y dejaron de manifiesto que los ciberataques están en constante cre-

cimiento, tanto en número como en sofisticación, es decir, caracteriza a los ciberatentados. Sin embargo, por sobre todo, esta cumbre se destaca por remarcar la importancia del vínculo de cooperación entre la Alianza Atlántica con otras organizaciones internacionales, como con el sector privado, ya que se entiende que el trabajo en conjunto a fin de hacer frente a las ciberamenazas y mejorar la seguridad común es fundamental (North Atlantic Treaty Organization, 2012).

En esta cumbre, se señaló que en la Cumbre de Lisboa se pidió una revisión sobre la postura de la OTAN en el ámbito de la disuasión como de la defensa en relación con todas las amenazas susceptibles contra la OTAN, teniendo en cuenta los avances de la tecnología. A partir de los resultados se garantiza que exista una capacidad de defensa y disuasión mixta que sigan los lineamientos establecidos en el Concepto Estratégico de 2011 (North Atlantic Treaty Organization, 2012).

También manifiesta que se dio lugar a la creación de un nuevo documento titulado *Summit Declaration on Defence Capabilities: Toward NATO Forces 2020* o también conocido como *Smart Defence*, que también se celebró en el año 2012 y que tenía como fin describir la visión y el camino hacia el objetivo de las fuerzas de la OTAN para el 2020.

La Declaración de las Capacidades de Defensa o *Smart Defence* se definió como "la oportunidad de una cultura renovada de cooperación en la que se otorga un nuevo protagonismo a la colaboración multinacional como opción eficaz y eficiente para el desarrollo de las capacidades críticas" (North Atlantic Treaty Organization, 2012). Manifestó la importancia del trabajo en conjunto que se ha realizado desde hace más de seis décadas por parte de los aliados en materia de defensa, ya que les permitió ofrecer a los respectivos países una seguridad más eficiente, como así también colaborar en el desarrollo de nuevas tecnologías que, si no fuese por el trabajo grupal, no sería posible llevarlas a cabo debido a cuestiones económicas o técnicas. Esta cooperación no debe entenderse solo desde el ámbito de los países aliados, sino también incluir en la suma a terceros Estados, organizaciones internacionales, como así también a la industria, que son fundamentales a fin alcanzar un objetivo común: la defensa.

A partir de la *Smart Defence*, en el 2013 surgieron varios proyectos, el más destacado se tituló *Multinational Cyber Defence Capability Development* (MNCD2, por sus siglas en inglés), el cual Canadá, Países Bajos, Dinamarca, Noruega, Rumania y Finlandia crearon en conjunto (Real instituto El Cano, 2014). Tiene como fin facilitar el desarrollo de las capacidades en ciberdefensa en la OTAN y las naciones a través de iniciativas colaborativas, por las cuales los países elegirán la temática y centrarán sus esfuerzos a fin de alcanzar una mejor capacidad de ciberdefensa (Jordan y Hallingstad, 2011: 81-89).

Por otro lado, también redactaron otro documento fundamental, titulado *Trans-Atlantic Defence Technological and Industrial Cooperation* (TADIC, por sus siglas en inglés), el cual busca fomentar la cooperación transatlántica e internacional entre los Estados miembros de la Alianza Atlántica y la industria, lo que constituye un vínculo beneficioso debido a diversos motivos, tales como identificar mejor las necesidades de ciberseguridad en todos los niveles de la OTAN (desde la adquisición de un cable hasta compartir información encriptada), como desarrollar soluciones y capacidades necesarias (Joubert, 2012), entre otros. Si bien TADIC no es nuevo, se incorporó junto a la *Smart Defense* con el fin de fomentar la cooperación transatlántica y así alcanzar mejores capacidades por menos gasto.

Por otra parte, en consonancia con la intención de fomentar vínculos entre distintos actores internacionales, surgió un documento titulado *Framework for NATO Industry Engagement*, el cual sustenta su origen en lo estipulado en los incisos de la Cumbre de Chicago, lo que pone de manifiesto la importancia de crear un vínculo entre la OTAN y la industria a fin de alcanzar de forma efectiva la ciberdefensa y la ciberseguridad.

LA DECLARACIÓN DE GALES

En septiembre de 2014, en Gales, Reino Unido, los países miembros de la OTAN se reunieron una vez más. En la declaración que surgió de esta cumbre se describen con especial severidad a los ciberataques y a las ciberamenazas, se sostiene que, al pasar los años, se vuelven cada vez más sofisticados, comunes y dañinos y que pueden llegar a un umbral capaz de amenazar la seguridad y la prosperidad de todas las naciones euroatlánticas. Esta situación ha llevado a establecer comparaciones con el daño que produce un ataque convencional a las sociedades (North Atlantic Treaty Organization, 2014).

También se dio a conocer la aprobación de una nueva política mejorada de ciberdefensa, que constituirá la contramedida al avance y al desarrollo de las ciberamenazas. La política tiene los siguientes objetivos:

- contribuir al cumplimiento de las tareas centrales de la Alianza Atlántica;
- reafirmar los principios de indivisibilidad de la seguridad aliada y de la prevención, la detección, la resiliencia, la recuperación y la defensa;
- destacar que los aliados deben brindar asistencia, con base en el espíritu de solidaridad y la responsabilidad, a fin de desarrollar las capacidades relevantes para la protección de las redes nacionales;
- reafirmar que la responsabilidad fundamental de la OTAN en este asunto es defender sus propias redes;
- reconocer que, tanto el derecho internacional, el derecho internacional humanitario y la Carta de las Naciones Unidas, son aplicables en el ciberespacio;
- afirmar que la ciberdefensa es un eje central de la defensa colectiva de la OTAN.

En relación con esto último, la Declaración de Gales, sostiene que el Consejo del Atlántico Norte es el encargado de decidir cuándo será posible la aplicación del artículo 5 de la Carta del Atlántico a raíz de un ciberataque.

Por otro lado, se destaca que la cooperación bilateral y multinacional son fundamentales a fin de mejorar las capacidades en ciberdefensa y que las alianzas son claves para afrontar las ciberamenazas. Por lo tanto, se reafirma el trabajo en conjunto con otras naciones y con organizaciones internacionales como la UE. Se propone intensificar los vínculos con la industria y el sector privado, lo que es fundamental para alcanzar los objetivos planteados en la nueva política de ciberdefensa (North Atlantic Treaty Organization, 2014).

Por último, pone foco también en la educación, el entrenamiento y el ejercicio de la OTAN en la ciberdefensa, cuyo órgano encargado es el CCDCOE.

LA CUMBRE DE VARSOVIA

En julio de 2016, los jefes de Estado y jefes de Gobierno de los países miembros de la OTAN reunidos en Polonia emitieron un texto en referencia a los avances logrados en Varsovia y las decisiones tomadas.

Varsovia dejó establecido que los ciberataques son un desafío a la seguridad de la OTAN y que podrían llegar a generar tanto daño como los ataques convencionales, al igual que se hizo en la Declaración de Gales. También reafirmó que la ciberdefensa es parte de la defensa colectiva de la Alianza y reconoció al ciberespacio como un dominio de operaciones más, tal como el aire, la tierra y el mar (North Atlantic Treaty Organization, 2016). Esto significa que se incluye al ciberespacio a la hora del planeamiento de la ejecución de medidas y contramedidas de tipo militar en pos de la seguridad y la defensa de la Alianza Atlántica, como de los aliados.

Además, la política que se adoptó en Gales se continuó aplicando con el propósito de fortalecer la ciberdefensa de la OTAN, lo que reafirmó el respeto por el derecho internacional público (DIP), el derecho internacional humanitario (DIH), la Carta de la ONU y los Derechos Humanos (DD. HH.), como así también mantener la paz, la seguridad y la estabilidad internacional en el ciberespacio (North Atlantic Treaty Organization, 2016).

Por otro lado, esta cumbre dejó como resultado la firma del Acuerdo Técnico entre la OTAN y la UE, la cual es una declaración conjunta firmada por el secretario general de la OTAN, Jens Stoltenberg, el presidente del Consejo Europeo, Donald Tusk, y el presidente de la Comisión Europea, Jean-Claude Juncker. Refleja el resultado de que las dos organizaciones se enfrentan a desafíos similares, por lo que es fundamental la protección de las redes contra el crecimiento de los ciberataques. El acuerdo se celebró entre el NCIRC y la CERT-EU, dos órganos técnicos conocidos como equipos de respuesta a incidentes informáticos respectivos de cada organización que intercambiarán información y compartirán las mejores prácticas a fin de evitar los ciberataques (North Atlantic Treaty Organization, 2016). "Para ello incluyen actividades de formación y ejercicios, así como la interacción con la industria a través de programas como el *Industry Cyber Partnership* de la OTAN" (De Espona, 2018).

Asimismo, también dejó como resultado la adopción de la *Cyber Defence Pledge*, que tiene como objetivo mejorar la ciberdefensa como asunto principal y primordial (North Atlantic Treaty Organization, 2016).

EL DERECHO INTERNACIONAL Y LOS CIBERATAQUES

El derecho internacional público (DIP) se define como "el conjunto de normas jurídicas que regulan las relaciones entre los sujetos de la comunidad internacional" (Moncayo, Vinuesa y Gutiérrez Posse, 1977:14). Esta definición se amplió a fin de incluir a los destinatarios a quienes van dirigidas las normas. Al tener en cuenta la temática de este trabajo, los sujetos no solo involucran a los Estados o las Organizaciones Internacionales (OI), sino a todo aquel que lleve a cabo acciones que tengan implicancias en la soberanía de otros sujetos internacionales.

Las normas preexistentes a los ciberatentados de Estonia sobre el DIP surgieron con el objetivo de condenar los delitos cibernéticos. Por ejemplo, aquellas normas se trataron de distintas resoluciones de la ONU, tales como la resolución 55/63 del año 2000, la resolución 56/121 de 2002, la 57/239 de 2002 y la 58/199 del año 2004, como así también el Convenio de Budapest por parte del Consejo de Europa, los cuales siempre destacaron el respeto por la Carta de la ONU, por los principios del DIP, por los DD. HH. y las convenciones referidas a ellos. No obstante, también manifestó que los avances de las tecnologías de la información tienen ventajas y desventajas, y es en estas últimas en

dónde centran su preocupación e instaron a los Estados a cooperar a fin de prevenir y combatir los delitos del ciberespacio.

Sin embargo, a partir del año 2009, debido a la iniciativa de la CCDCOE de invitar a un grupo de distinguidos profesionales y académicos del derecho internacional con el propósito de examinar cómo se aplicarían las normas jurídicas existentes a esta nueva forma de conflicto internacional (Schmitt, 2013: 17), se creó el *Manual sobre el derecho internacional* aplicable a la ciberguerra, o el "Manual del Tallin", el cual se publicó por la Universidad de Cambridge y lleva el nombre de la capital de Estonia, Tallin.

El manual no es un documento oficial de la OTAN, no representa las opiniones del CCDCOE, de los países miembros de la OTAN ni de ningún país u organización, sino que debe entenderse como el resultado del análisis de un grupo de expertos independientes que actuaron a título personal (Schmitt, 2013: 23). Por lo tanto, se pone de manifiesto una contradicción en sí mismo, ya que el CCDCOE impulsó el "Manual del Tallin" que a su vez la OTAN promovió y que nació como consecuencia de los ciberataques y la nueva política de la organización, pero que, en síntesis, no refleja la voluntad de los Estados partes.

El texto contiene en total dos partes, la primera se titula como "La seguridad del ciberespacio en el derecho internacional", mientras que la segunda parte "El derecho internacional en los ciberconflictos". El manual cuenta con siete capítulos y en total noventa y cinco reglas aplicables a la ciberguerra. El grupo de expertos se basó en diferentes fuentes a fin de redactar este texto, como por ejemplo las siguientes:

- el *Manual sobre el derecho de los conflictos armados no internacionales* (The NIAC Manual);
- el *Manual sobre el derecho internacional aplicable a la guerra aérea y a los misiles* (The AMW Manual);
- el estudio del derecho internacional humanitario del Comité Internacional de la Cruz Roja (The ICRC Customary IHL Study);
- los manuales militares de Alemania, Canadá, Estados Unidos y Reino Unido.
- la Convención de Ginebra y los protocolos adicionales;
- la opinión de la Corte Internacional de Justicia, donde afirmó que el Reglamento de La Haya de 1907 refleja el DIP.

Las noventa y cinco normas que contiene el manual se adoptaron por medio del consenso del grupo internacional de expertos (GIE), el cual tomó como referencia DIP, salvo que se indique lo contrario en los comentarios que acompañan y explican cada norma. El manual aplica la ley existente a la ciberguerra, es decir, examina la ley internacional que gobierna la ciberguerra, e incluye tanto el *ius ad bellum* (derecho de poder recurrir a la guerra) como el *ius in bello* (el derecho que regula la conducta en la guerra) (Schmitt, 2013: 19).

Los miembros del GIE realizaron un análisis de la aplicabilidad real del derecho internacional consuetudinario en el ciberespacio, como también de las normas contenidas en las Convenciones de Ginebra.

A continuación, se realizó un análisis sintetizado de las reglas más importantes a partir de los siguientes cinco ejes:

I. El respeto y la protección de NO ser objetivos de ciberataques a los siguientes sujetos:

- la población civil (regla 32);
- los bienes civiles (regla 37);
- el personal médico y religioso, las unidades y los transportes sanitarios (regla 70), como así también las computadoras, las redes informáticas y los datos que sean parte de la administración de las unidades o de los transportes sanitarios (regla 71);

- el personal, las instalaciones, el material (computadoras, redes informáticas, entre otras), las unidades y los vehículos de la ONU, como así aquellos que pertenezcan a una misión humanitaria o del mantenimiento de la paz (regla 4);
- los prisioneros de guerra, las personas protegidas internadas y otras personas detenidas (regla 75) ni su correspondencia (mantenida con familiares u otras personas civiles) (regla 76).;
- los periodistas civiles que participen en misiones profesionales caracterizadas como peligrosas en zonas de conflictos armados (regla 79);
- los bienes culturales (regla 82);
- el medio ambiente natural (regla 83);
- los archivos y las comunicaciones diplomáticas (regla 84);
- las personas protegidas en territorio ocupado (regla 87) .

II. Prohibición de actos tales como los siguientes:
- los ciberataques o las amenazas de ciberataques con el fin de sembrar terror (regla 36);
- el uso de medios o métodos de ciberguerra que causen daños superfluos o sufrimiento innecesario (regla 42);
- el uso de trampas cibernéticas (regla 44);
- hacer pasar hambre a la población civil como método de ciberguerra (regla 45);
- las represalias beligerantes contra los prisioneros de guerra; los civiles internados en territorio ocupado o en manos de una parte adversa al conflicto; aquellos que están fuera del combate; el personal, las instalaciones, los vehículos y los equipos médicos (regla 46), como así también contra la población civil, los bienes de carácter civil, los bienes culturales, los lugares de culto, el medio ambiente natural, las presas, los diques, las centrales eléctricas nucleares y los objetos fundamentales para la supervivencia de la población civil (regla 47, regla 81, regla 83);
- los ciberataques que no estén dirigidos contra un objetivo legítimo (regla 49);
- perfidia (regla 60);
- usar de forma indebida los emblemas, los símbolos o las señales protectoras que estén previstas en el *ius in bellum* como por ejemplo el emblema de la Cruz Roja, de la Media Luna Roja, Cristal Rojo (regla 62), como así también el emblema distintivo de la ONU (regla 63);
- usar de forma indebida las banderas, los emblemas militares, las insignias o uniformes tanto del enemigo mientras estén visibles durante un ataque, incluido un ciberataque (regla 64) como de Estados neutrales u otros Estados que no son parte del conflicto (regla 65);
- reclutar o alistar niños en las FFAA o permitirles participar en las ciberhostilidades (regla 78);
- castigar de forma colectiva a aquellas personas o grupos por actos que ellas no han cometido (regla 85);
- interferir de manera indebida en las acciones de asistencia humanitaria (regla 86);
- llevar a cabo acciones contra ciber infraestructuras neutrales (regla 91).

III. Precauciones tales como las siguientes:
- verificar y proteger a la población civil y a los bienes de carácter civil (regla 52 y 53), como así también de los efectos de los ciberataques (regla 59);
- tener precaución a la hora de la elección de los medios y métodos de ciberguerra a usar, con el fin de evitar daños incidentales a la población y a los bienes protegidos (regla 54);
- emitir advertencias con suficiente antelación de que sucederá un ciberataque que

pueda afectar a la población civil, siempre y cuando sea posible (regla 58);
- evitar que, al atacar presas, diques o instalaciones eléctricas nucleares, se liberen fuerzas peligrosas que atenten contra la vida de la población civil (regla 80).

IV. Acciones permitidas tales como las siguientes:
- el ciberespionaje (regla 66);
- hacer uso de medios y métodos de la ciberguerra a fin de mantener o hacer cumplir un bloqueo naval o aéreo (regla 67);
- hacer uso de ciberoperaciones legales con el fin de ejercer derechos en zonas establecidas (ya sea en tiempos de paz o en tiempos de guerra) (regla 69);
- levar a cabo medidas a fin de establecer o restablecer y garantizar, siempre y cuando sea posible, el orden y la seguridad en un territorio ocupado y respetar, siempre que sea posible, las leyes vigentes (regla 88), como así también tomar las medidas necesarias con el objetivo de garantizar la seguridad, la integridad y la confiabilidad de sus sistemas cibernéticos (regla 89).

V. Objetivos lícitos que podrán ser blancos de ciberataques tales como los siguientes:
- los miembros de las fuerzas armadas (FFAA) y los miembros de los grupos armados organizados (regla 34);
- los civiles que participan de manera directa en las hostilidades (regla 29 y regla 35);
- aquellos que deciden participar en un levantamiento masivo (en un conflicto armado internacional) (regla 27);
- los objetos con "doble uso" (civil/militar) (regla 39).

El "Manual del Tallin" analiza también la cuestión de la legítima defensa y sostiene que cuando "un Estado sea objetivo de una ciberoperación que alcance el nivel de un ataque armado, puede ejercer su derecho inherente a la legítima defensa" (Schmitt, 2013: 53). Por lo tanto, se remite al artículo 51 de la carta de la ONU, que reconoce también como derecho inherente de los Estados la legítima defensa. No obstante, para que un Estado víctima pueda ejercer el uso de su derecho a la legítima defensa, debe cumplir con ciertos requisitos tales como los que se mencionan a continuación:
- necesidad;
- proporcionalidad;
- inminencia;
- inmediatez.

Por otro lado, a la hora de llevar a cabo las acciones de legítima defensa es fundamental que el Estado víctima exija primero al Estado atacante (en caso de que sea un actor estatal) que cese con los ataques armados, pero pueden existir situaciones en las que no exista la posibilidad de hacer la petición y que se requiera una acción inmediata para repeler el ciberataque armado, para derrotarlo o para minimizar sus consecuencias, por lo que depende del contexto de la situación. Estas acciones pueden aplicarse desde el territorio del Estado víctima, de alta mar, del espacio aéreo internacional o inclusive desde el espacio ultraterrestre, pero siempre se debe tener en cuenta el principio de soberanía (Schmitt, 2013: 58).

El artículo 51 de la carta de la ONU también menciona la posibilidad de recurrir a la legítima defensa colectiva, y, en este caso, el Manual del Tallin reafirma que "el derecho de legítima defensa podrá ejercerse colectivamente. (...) solo podrá ejercerse a petición del Estado víctima (...)", en la regla 16 (Schmitt, 2013: 63). También se remarca que, a la hora de que un Estado asista a otro con el objetivo de hacer uso de la legítima defensa colectiva, debe primero haber recibido una solicitud de

asistencia y ambos deben estar seguros de la existencia inminente o en curso de un ataque armado (Schmitt, 2013: 63).

Se torna relevante retomar la última parte del artículo 51 de la Carta de la ONU, ya que el Manual establece en la regla 17 que todas las medidas que se tomarán en ejercicio del derecho de legítima defensa deben informarse al Consejo de Seguridad de la ONU. No cumplir con este deber significaría una violación al artículo 51 de la carta (Schmitt, 2013: 64).

CONCLUSIONES

En este trabajo se describieron las implicancias de los ciberatentados sucedidos en Estonia en 2007 y en las medidas adoptadas por la OTAN en su política de ciberdefensa. La importancia de realizar este trabajo radica en que el espacio cibernético no reconoce ni fronteras de ningún tipo ni autoridad ni norma alguna, por lo que tras lo sucedido en Estonia se generó un profundo impacto en la OTAN. A partir de entonces, inició el desarrollo de una política de ciberdefensa.

La Política de Ciberdefensa de la OTAN se entiende como una medida especial y extraordinaria creada a partir de la situación de peligro que atravesó la Alianza Atlántica y sus miembros. Inició su proceso de creación en la Cumbre de Bucarest, se adoptó en Chicago, se mejoró en Gales y buscó aumentar su implementación en Varsovia, con el fin de evitar, responder o disuadir nuevos ciberatentados.

Este trabajo demuestra cómo la organización desarrolló una política desde sus cimientos, a la que en la actualidad se considera una de las más emblemáticas y precursoras, lo que demostró la razón por la que la OTAN continúa siendo desde 1949 una de las organizaciones políticas-militares más importantes del mundo. Por lo tanto, se puede afirmar que la innovación en esta temática radica en la capacidad de mostrar cómo los ciberataques de 2007 impulsaron la creación y el desarrollo constante de la política de ciberdefensa de la OTAN.

REFERENCIAS BIBLIOGRÁFICAS

Cooperative Cyber Defense Center of Excellence. (n.d.-a). *About us*. https://ccdcoe.org/about-us/

Cooperative Cyber Defense Center of Excellence. (n.d.-b). *Exercises*. https://ccdcoe.org/exercises/

Cooperative Cyber Defense Center of Excellence. (n.d.-c). *North Atlantic Treaty Organisation*. https://ccdcoe.org/organisations/nato/

Council on Foreign Relations. (n.d.). *NATO's Trident Juncture Exercises: What to know*. https://www.cfr.org/in-brief/natos-trident-juncture-exercises-what-know

CybExer. (2020). *CybExer red-teaming capabilities deployed at NATO CCDCOE Crossed Swords 2020 exercise*. https://cybexer.com/news/crossed-swords-2020-exercise/

De Espona, R. J. (2018, mayo). *Guerra híbrida y capacidades estratégicas de la OTAN: aportaciones de Lituania, Letonia y Estonia*. Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO55-2018_GuerraHibrida_OTAN_Lit-Est-Let_RafaelJEspona.pdf

European Parliament. (n.d.). *Defending against cyber-attacks*. https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611natocyberattacks_/sede150611natocyberattacks_en.pdf

González de Cruz, C. (2008). *Curso de metodología de la investigación científica para las ciencias sociales*. Virtudes.

Healey, J., & Tothova, K. J. (2014, septiembre). *NATO's cyber capabilities: Yesterday, today and tomorrow*. Atlantic Council. https://www.atlan-

ticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf

Jordan, F., & Hallingstad, G. (n.d.). *Towards multi-national capability development in cyber defence. Information and Security: An International Journal.* https://procon.bg/system/files/27.09_Jordan.pdf

Joubert, V. (2012, mayo). *Five years after Estonia's cyber attacks: Lessons learned for NATO?* Research Paper No. 76.

Lonely Planet. (n.d.). *Historia de Estonia*. https://www.lonelyplanet.es/europa/estonia/historia

MC0571 North Atlantic Treaty Organization. (2012). *NATO cyber defence*. Citado por Centro Superior de Estudios de la Defensa Nacional. Ministerio de Defensa, Madrid.

Moncayo, G. R., Vinuesa, R. E., & Gutierrez Posse, H. (1977). *Derecho internacional público*. ZAVALIA.

Montoya Pino, F. (n.d.). *OTAN en Kosovo: La operación Fuerza Aliada vista desde los principios básicos del ius in bello*. https://publicaciones.eafit.edu.co/index.php/ejil/article/view/386/382

Moreira, J. (2010). *A implementação do conceito NATO Network-Enabled Capability (NNEC) em Portugal*.

North Atlantic Treaty Organization. (n.d.-a). ¿Qué es la OTAN? https://www.nato.int/nato-welcome/index_es.html

North Atlantic Treaty Organization. (2008). *Bucharest summit declaration*. https://www.nato.int/cps/en/natolive/official_texts_8443.htm

North Atlantic Treaty Organization. (n.d.-b). *Centres of Excellence*. https://www.nato.int/cps/en/natolive/topics_68372.htm

North Atlantic Treaty Organization. (2012). *Chicago summit declaration*. https://www.nato.int/cps/en/natolive/official_texts_87593.htm#deterrence

North Atlantic Treaty Organization. (2022). *Cyber defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm

North Atlantic Treaty Organization. (2009). *Declaration on Alliance Security*. https://www.nato.int/cps/en/natohq/news_52838.htm

North Atlantic Treaty Organization. (2022). *Kosovo Air Campaign (March–June 1999)*. https://www.nato.int/cps/en/natohq/topics_49602.htm

North Atlantic Treaty Organization. (2010, noviembre 20). *Lisbon summit declaration*. https://www.nato.int/cps/en/natolive/official_texts_68828.htm

North Atlantic Treaty Organization. (2016). *NATO and the European Union enhance cyber defence cooperation*. https://www.nato.int/cps/en/natohq/news_127836.htm

North Atlantic Treaty Organization. (2021, abril). *Nato Cyber Defence*. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

North Atlantic Treaty Organization. (n.d.-c). *NATO Defence Ministers adopt new cyber defence policy*. https://www.nato.int/cps/en/natohq/news_75195.htm

North Atlantic Treaty Organization. (2015). *NATO Network Enabled Capability (archived)*. https://www.nato.int/cps/en/natolive/topics_54644.htm

North Atlantic Treaty Organization. (n.d.-d). *NATO Rapid Reaction Team to fight cyber attack*. https://www.nato.int/cps/en/natolive/news_85161.htm

North Atlantic Treaty Organization. (2014). *NATO's cyber capabilities: Yesterday, today and tomorrow*. https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf

North Atlantic Treaty Organization. (2002). *Prague summit declaration*. https://www.nato.int/cps/en/natohq/official_texts_19552.htm

North Atlantic Treaty Organization. (2009). *Strasbourg/Kehl summit declaration*. https://www.nato.int/cps/en/natolive/news_52837.htm

North Atlantic Treaty Organization. (n.d.-e). *Strategic Concepts*. https://www.nato.int/cps/en/natohq/topics_56626.htm

North Atlantic Treaty Organization. (2012). *Summit declaration on defence capabilities: Toward NATO Forces 2020*. https://www.nato.int/cps/en/natohq/official_texts_87594.htm?mode=pressrelease

North Atlantic Treaty Organization. (2014). *Wales summit declaration*. https://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber

North Atlantic Treaty Organization. (2016). *Warsaw summit communiqué*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

North Atlantic Treaty Organization. (2010, noviembre). *Strategic concept for the defence and security of the members of the North Atlantic Treaty Organization*.

Pessino, M. (n.d.). *Las políticas en ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN) período 2008–2013*. Real Instituto El Cano. (2014, febrero). *La OTAN y la ciberdefensa*. https://www.realinstitutoelcano.org/blog/la-otan-y-la-ciberdefensa/

Schmitt, M. N. (Ed.). (2013). *The international law applicable to cyber warfare*. Cambridge University Press.

Verdes-Montenegro Escanez, F. J. (2015). Securitización: Agendas de investigación abiertas para el estudio de la seguridad. *Relaciones Internacionales*, (29), 111–131. https://revistas.uam.es/relacionesinternacionales/article/view/5273

María Virginia Rueda
Perfil Académico y Profesional: Licenciada en Relaciones Internacionales de la Universidad Católica de Salta (UCASAL). Miembro del Instituto de Relaciones Internacionales y Ciencias Políticas de la Universidad Católica de Salta.
mariavirginiarueda@gmail.com
ORCID: https://orcid.org/0009-0007-8281-6298