Currículum Vitae del TCnl Roberto Claudio Galizia

Es Oficial de Estado Mayor del Ejército Argentino y Diplomado en Altos Estudios Nacionales del Estado Plurinacional de Bolivia. Es Licenciado en Estrategia y Organización, Magister en Defensa, Desarrollo y Seguridad y Magister en Educación Superior. Se desempeñó como profesor en el Colegio Militar del Ejército "Cnl. Gualberto Villarroel" y en la Escuela Militar de Inteligencia "Gral. Ejto. Joaquín Zenteno Anaya" de Bolivia. Fue 2do Jefe de la Base Antártica Esperanza, Jefe de la Compañía de Comunicaciones Paracaidista 4 y Jefe del Batallón de Comunicaciones 141. Actualmente se desempeña como profesor en la Escuela Superior de Guerra.

Este artículo trata sobre el tratamiento de la Ciberdefensa desde el Derecho Internacional Público por parte de la OTAN a partir de la publicación en 2013 del "Tallin Manual on the International Law Applicable to Cyber Warfare", constituyéndose en la primera definición en materia de Derecho de los Conflictos Armados y por ende con incidencia en la Seguridad Internacional.

El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra

Autores: Dra. Claudia Elizabeth Fonseca, My (Aud.) Ivonne Luz Perdomo,

Lic. Miguel Arozarena Gratacos y Dr. Javier Ulises Ortiz

Proyecto de Investigación "Ciberdefensa" de la ESG

Propósito

Una apreciación del Manual de Tallin de la OTAN tanto estratégica como jurídica resulta necesaria para encuadrar las acciones ofensivas y defensivas de actores en el ciberespacio, lo que requiere un encuadramiento normativo de la dinámica de los conflictos en ese nuevo ambiente operacional signado por lo tecnológico, siendo esta la primera en su tipo.

Introducción

En un mundo cada vez más interrelacionado por el denominado proceso de globalización e incrementado por el "cuatro espacio" o el ciberespacio, las Políticas de Defensa de los Estados constituyen un factor preponderante para la materialización de alianzas y proyectos en conjunto que aseguren el desarrollo de las mismas acordes al nuevo escenario mundial. Así, las Políticas de Defensa comienzan a atender cada vez más al concepto de "fronteras virtuales" como una expresión normal para la interacción que se produce en el sistema internacional. La función de la Defensa es similar para las distintas naciones, tendiendo como objetivo prioritario mantener la Soberanía y la integridad territorial.

Así, cada Política de Defensa es una expresión de cómo la sociedad se organiza para el cumplimiento de la función anteriormente señalada, lo que depende de las características propias de cada Estado. Bajo esta premisa, la cultura, la historia, la situación geográfica de cada país y el sistema internacional en sus relaciones interestatales son fuentes para que cada país defina cuáles son sus necesidades específicas de Defensa. Asimismo, en los últimos años, comienza a cobrar más énfasis en el tratamiento de dichas políticas el impacto tecno-informacional en el campo de la Defensa y de la Seguridad Internacional en general.

Jeimy Cano, especialista en seguridad de redes, indica que "eventos recientes sobre fuga de información, las noticias de atacantes informáticos doblegando protocolos y tecnologías de seguridad, las fallas de seguridad que se han presentado tanto en el sector público como en el sector privado, son argumentos suficientes para evidenciar que estamos en un nuevo escenario de riesgos y amenazas, donde la información se convierte en un arma estratégica y táctica que cuestiona la gobernabilidad de una organización o la de una nación"[1].

María José Bejarano, analista del Instituto Español de Estudios Estratégicos (IEEE) resume claramente la situación al exponer que "en el mundo actual ha surgido una nueva dimensión donde pueden materializarse las amenazas: el ciberespacio. Si antes en el ámbito de la defensa estaba claro que nos movíamos en las tres dimensiones de tierra, mar y aire, ahora contamos con una dimensión adicional, y más intangible que las anteriores. (…) El ciberespacio no tiene fronteras, es un nuevo campo de batalla.[2]

Así, las Nuevas Amenazas y riesgos han hecho surgir una visión más amplia del problema abarcando todos los aspectos de la realidad de un país, la Defensa Nacional, así como aspectos económicos, tecnológicos y ambientales, ampliando los conceptos de Seguridad Internacional; donde los Estados siguen siendo los únicos actores internacionales dotados de capacidad de hacer uso legítimo de la fuerza en los conflictos Inter – Infra – Supra estatales, pero comienzan a integrarse en una agenda cada vez más cooperativa a regímenes de gobernabilidad regional como en respuesta ante la mayor demanda sobre operaciones de paz por parte de la Organizaciones de Naciones Unidas y en algunos casos frente a amenazas de alcance global.

Así, el surgimiento de la nueva amenaza de ciberataques a infraestructuras críticas que ponen en riesgo la libertad de acción de los Estados comienza a ser cada vez atendido en la agenda de amenazas asimétricas dando como respuesta la creación de organismos responsables para contrarrestarles en el marco de nuevas políticas de seguridad y defensa cibernética.

1 Cano, Jeimy. "Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global" N° 119 (abr-Jun. 2011) Revista Sistemas, Colombia, p. 4-7.

2 Bejarano, María José. "Alcances y ámbito de la seguridad nacional en el ciberespacio" Instituto Español de Estudios Estratégicos (IEEE). Cuaderno de estrategia N° 149. Pág. 51 2011

Como señala Cano, en este sentido, "el concepto de guerra tradicional, se transforma para darle una nueva función del Estado frente a la defensa de su soberanía en el espacio digital y la protección de los derechos de sus ciberciudadanos, ante las amenazas emergentes en el escenario de una vida más digital y gobernada por la información.(…) Es por ello que las reflexiones y decisiones sobre la seguridad tienen una renovada connotación."[3]

En los últimos años, se registraron los siguientes tres casos paradigmáticos de ciberataques:

- Los ciberataques a la infraestructura crítica tecnoinformacional en Estonia (2007).
- Los ciberataques en Georgia (2008), conocidos por ser el primer caso en el que las operaciones cibernéticas fueron iniciadas dos meses antes y luego conducidas conjuntamente con operaciones militares armadas, evidencian la significación de la amenaza cibernética[4].
- El virus Stuxnet que afectó el programa nuclear iraní (2010).

El caso de Estonia fue la primera vez que un país miembro solicitó apoyo a la OTAN por un ataque a sus sistemas de información y comunicaciones. En aquel momento la OTAN no disponía de un plan de acción para el caso de un ciberataque a un Estado miembro. El gobierno identificó con celeridad que estaban bajo un ataque de gran dimensión que podía derivar en una crisis de seguridad nacional. Formaron inmediatamente un equipo multifuncional para coordinar la respuesta; en el que se incluían expertos de la esfera técnica, política, militar, diplomática y jurídica.

El caso de Georgia, deliberadamente o no, los ciberataques debilitaron la capacidad de toma de decisiones del entorno político y militar de Georgia durante el conflicto; y debilitaron la capacidad de información y de comunicación entre el Gobierno y los ciudadanos, a la vez que, a través de la ciber propaganda, trataron de influenciar en la opinión pública hacia la postura defendida por Rusia, Osetia del Sur y Abjasia.

Más recientemente han proliferado las acusaciones por parte de Washington de haber recibido ciberataques provenientes de China. Asimismo, en otros recientes conflictos y operaciones militares han proliferado este tipo de ciberataques entre los contendientes.

3 Cano, Op, cit. Pag. 5

4 Artiles, Nestor. "La Situación de la ciberseguridad en el ámbito internacional y en la OTAN". Instituto Español de Estudios Estratégicos (IEEE). Cuaderno de Estrategia N° 149. Pág. 167 2011

Estos casos demostraron que la guerra tradicional, no solamente cambió, sino que ha evolucionado a un nuevo espacio virtual donde la soberanía y autonomía del Estado es cada vez más vulnerable por expertos de la tecnología.

Es a raíz de esta nueva concepción de amenaza se destacan como principales antecedentes que, necesariamente, obligaron a la OTAN a reestructurar sus capacidades y crear equipos de respuesta inmediata frente a ciberataques considerada como una Nueva Amenaza al orden internacional los casos de Estonia y Georgia.

Como consecuencia de estos ataques, se han desarrollado acuerdos de cooperación en la creación de instituciones y organismos dentro de la OTAN que permitan concentrar un conocimiento especializado en esta materia tendientes a generar áreas de ciberseguridad.[5]

La OTAN se enfrentó a este problema en la Cumbre de Bucarest de 2008, de cuya declaración se desprendían tres líneas de acción que consistían en medidas a adoptar:[6]

- Por la propia OTAN para mejorar su capacidad de ciberdefensa.
- Por las naciones para mejorar la protección de los sistemas de información crítica desplegados en sus territorios.
- Por ambas partes, OTAN y naciones, para mejorar la coordinación, intercambio de información y el apoyo mutuo.[7]

Nuevo Concepto Estratégico de Ciberdefensa de la OTAN

Con posterioridad a los sucesos de Estonia, en Septiembre de 2010, William J. Lynn, entonces Subecretario de Defensa de los Estados Unidos indicaba en oportunidad de una reunión de la OTAN que esta organización debía construir un "escudo de cibernético" para proteger la alianza transatlántica de cualquier amenaza a sus infraestructuras militares y económicas ya que la Alianza tiene un papel crucial que desempeñar en la ampliación de una malla de seguridad sobre nuestras redes". Lynn expresó que "la OTAN tiene un escudo nuclear, está construyendo un escudo de defensa y más fuerte, que necesita un ciber-escudo".

5 Este punto será desarrollado en la sección "Capacidades de Ciberdefensa"

6 Ministerio de Defensa. Op., cit

7 "La OTAN se mantiene comprometida con el fortalecimiento de los sistemas de información crítica de la Alianza contra ciberataques. Hemos adoptados recientemente la Política de Ciber Defensa, y estamos desarrollando las estructuras y autoridades para llevarla a cabo. Nuestra política en materia de Ciber Defensa subraya la necesidad de la OTAN y de las naciones miembros de proteger los sistemas de información crítica conforme con sus respectivas responsabilidades; compartir las mejores prácticas y establecer una capacidad de apoyo a las naciones, bajo petición, para contrarrestar un ciberataque. Continuamos con el desarrollo de las capacidades de ciberdefensa de la OTAN y con el fortalecimiento de los vínculos entre la OTAN y las autoridades nacionales" Declaración de Bucarest (2008), Sección 47.

A raíz de distintas reuniones llevadas a cabo por los Ministros de Defensa de la OTAN realizadas en el marco del Nuevo Concepto de Ciberdefensa de la Alianza[8] , la OTAN ha aprobado en 2011 una Política de Ciberdefensa y un plan de acción para su implementación[9]. El principal objetivo consiste en la protección de las redes informáticas de los Estados Miembros. Uno de los principios fundamentales de este Concepto es el de la cooperación como pilar fundamental para poder integrar las capacidades de otros Estados y organismos internacionales en el planeamiento de la Defensa de la OTAN frente a las ciberamenazas.[10]

Como objetivos, la OTAN implementará un enfoque coordinado de ciberdefensa para abarcar aspectos de planificación y desarrollo de capacidades junto con mecanismos de respuesta en caso de ciberataque. Asimismo, la Alianza incorporará e integrará las medidas de ciberdefensa en las misiones. Para lograr estos objetivos, la OTAN utilizará los procesos de planeamiento de la defensa para promover el desarrollo de las capacidades de ciberdefensa de los aliados, para ayudar a las naciones aliadas que lo soliciten y para optimizar la compartición de información, la colaboración y la interoperabilidad.[11]

Capacidades de Ciberdefensa

En este aspecto, se han creado organismos especializados en materia de ciberataques. Uno de ellos es el NCIRC[12] (Capacidad de respuesta ante incidentes informáticos de la OTAN), cuya misión principal, es la de repeler ataques en materia de ciberdelito. Al mismo tiempo, es la responsable de proteger todas las instalaciones informáticas de la OTAN, tanto civiles como militares. Para tal fin, cuenta con la logística y apoyo necesario que le brinda la organización para cumplir con tal fin.

Para aumentar las capacidades de la ciberdefensa, el Consejo de la OTAN firmó la Política de Ciberdefensa en enero de 2008[13] con el objetivo de aumentar la capacidad de la OTAN en respuesta a ciberataques, proteger los sistemas y redes de información y comunicaciones de valor crítico para la Alianza frente a los ciberataques; desarrollo del concepto de ciberdefensa[14]; proceso para conseguir una

8 Ministerio de Defensa. Dirección General de Relaciones Internacionales. Instituto Español de Estudios Estratégicos. Documento informativo del IEEE 09/2011. Nuevo concepto de Ciberdefensa de la OTAN (marzo 2011).

9 Ministerio de Defensa. Dirección General de Relaciones Internacionales. Instituto Español de Estudios Estratégicos Documento informativo del IEEE 37-2011. La Política de Ciberdefensa de la OTAN (octubre 2011)

10 A raíz de los ataques cibernéticos a Lituania, se decidió incorporar la ciberdefensa en las agendas políticas de la Alianza. Esto daría inicio al nacimiento de la política de Ciberdefensa de la Organización.

11 Ministerio de Defensa. Op., cit

12 NATO Computer Incidents Response Capability Technical Centre - CIRC

13 "NATO Policy on Cyber Defence", C-M(2007)0120.

14 "NATO Cyber Defence Concept, MC 0571, 4-2-2008.

capacidad operativa completa de respuesta ante incidentes informáticos-NCIRC.

Plan de Ciberdefensa

El principio que rige este plan es el "principio militar de mutua asistencia y defensa colectiva", el cual, establece que "cualquier nación miembro de la OTAN que sufra un ciberataque significativo podrá solicitar ayuda de la OTAN. La petición será considerada por el comité de gestión de ciberdefensa"

Ataques Más Sofisticados y Principales Actividades

Algunos de los tipos de ataques conocidos por los organismos especializados en materia de ciberseguridad figuran en las guías CCN-CERT son:[15]

- Virus: Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.
- Código dañino, también conocido como código malicioso, maligno o «malware» en su acepción inglesa: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial (42).
- Bomba lógica: Segmento de un programa que comprueba constantemente el cumplimiento de alguna condición lógica (por ejemplo, número de accesos a una parte del disco) o temporal (satisfacción de una cierta fecha). Cuando ello ocurre desencadenen a alguna acción no autorizada. En ocasiones, si la condición a verificar es una cierta fecha, la bomba se denomina temporal.
- Troyano: Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc.
- Gusano: Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.

Es importante destacar la "profesionalidad" con la que estos tipos de ataques son diseñados y ejecutados. Se requiere de un alto conocimientos en ciencias y tecnología y un alto nivel de organización para poder perpetuar en el tiempo. Las vulnerabilidades de los sistemas son el elemento fundamental de los ciberataques porque es la esencia de las capacidades ofensiva, defensiva y de inteligencia en el

15 Guía de seguridad de la STIC (CCN-STIC-401), Glosario y abreviaturas, 1 de febrero de 2010.

ciberespacio[16]- Asimismo, las amenazas enemigas de las infraestructuras críticas (IC) siempre han existido en tiempos de guerra o conflicto, pero los escenarios de amenazas incluyen ahora ataques en tiempos de paz por ciberatacantes anónimos.[17]

Así, teniendo en cuenta las características de estos ataques, la OTAN desarrollo el concepto de RRT: "Los expertos en ciberdefensa son responsables de asistir a los estados miembros que soliciten ayuda en el caso de un ataque de relevancia nacional"[18]. Para efectivizar este trabajo, han desarrollado diferentes actividades de coordinación y asesoramiento para que las autoridades políticas y expertos de las tecnologías puedan trabajar en conjunto con la colaboración de otros organismos internacionales como la Unión Europea. Estas actividades incluyen:

- Coordinación y asesoramiento en ciberdefensa.

  Esta actividad será desarrollada por el campo político, militar y científico-tecnológico de la Alianza. La **Cyber Defence Management Authority (CDMA)** es la encargada de llevar a cabo las coordinaciones y el asesoramiento a las unidades para repeler ciberamenazas y prevenir ataques cibernéticos, como así también, evaluar los riesgos de otros actores en infiltrar las estructuras críticas de la organización y repeler las vulnerabilidades que pongan en riesgo las actividades de la misma. Ante una emergencia en materia de ciberataque, se debe recurrir a este organismo.

- Asistencia a las naciones.

  La OTAN se rige por el principio de cooperación con otros socios regionales e internacionales puesto que la nueva modalidad de ataque permite que, desde cualquier computadora, pueda ejecutarse una infiltración a los sistemas de comunicación de los Estados Miembros. La OTAN, por tal motivo, promueve acuerdo, a través de medidas de confianza mutua con terceros para evitar riesgos o amenazas que pongan en riesgo la libertad de acción de la Alianza.

- Investigación y formación.

  Para el desarrollo de esta actividad, se ha creado el Centro de Excelencia OTAN de Ciberdefensa Cooperativa (Cooperative Cyber Defence Centre Of Excellence – CCDCOE) con el objetivo de llevar a cabo investigaciones en materia de ciberguerra y capacitar al personal en el conocimiento de este nuevo campo de la Defensa.

16 KEVIL COLEMAN, «The weaponry and strategies of digital conflict». Security and Intelligence Center at the Technolytics Institute, USA, 2010.

17 GEERS, KENNETH, «The Cyber Threat to National Critical Infrastructures: Beyond theory«. Information Security Journal: A global perspective, 18:1-7, 2009.

18 "Política de Ciberdefensa de la OTAN" – Reunión de Ministros de Defensa – Mayo 2011

- Cooperación con los socios.

  Se ha creado el Consejo para la Cooperación en Ciberdefensa con socios y organizaciones internacionales para fomentar mediadas de confianza mutua con la intención de mitigar y repeler ciberamenzas a los países de la Alianza.

Apreciación Estratégica Actual de la Ciberguerra por Parte de la Otan

El estudio sobre la apreciación estratégica de la OTAN brinda una importante experiencia ante la necesidad de un planeamiento estratégico que ha generado esta nueva modalidad de ataque para proteger los intereses vitales de una nación como así también la necesidad de fomentar la investigación y desarrollo en proyectos con capacidad de mitigar y repeler estas nuevas amenazas cibernéticas.

En la última cumbre de la OTAN, llevada a cabo los días 4 y 5 de septiembre de este año en Cardiff, Gales (RUGB)[19], que trató entre otros temas la crisis por la situación en Crimea, el organismo actualizó sus estándares de defensa de Europa por medio de un programa llamado "política de ciberdefensa reforzada" [20]. Las apreciaciones de las autoridades participantes de la cumbre centraron su atención en que durante el desarrollo de la crisis en Crimea, las fuerzas rusas tuvieron capacidad de integrar a sus acciones militares una eficaz estrategia "ciberofensiva", pudiendo interrumpir las comunicaciones de los Centros de Comando y Control de las fuerzas de Ucrania estacionadas en la península así como en otras zonas de Ucrania. De este modo la OTAN trató el aspecto ofensivo de la ciberguerra, extendiendo al ciberespacio todas las garantías del Tratado.

Así, cualquier ciberataque contra un país miembro será considerado como un ataque contra todos los miembros de la OTAN, o sea, equivalente a una agresión clásica. Esta situación fusiona el espacio "real" (terrestre, marítimo y aéreo) al ciberespacio. No obstante ello, Sorin Ducaru, Secretario Adjunto de la OTAN y encargado de los "desafíos emergentes" aclaró que el organismo se limitará a defenderse, no previéndose por el momento lanzar operaciones ciberofensivas, ya que son del dominio de cada país miembro.

Para asegurar estas capacidades los estados miembros proponen la necesidad de reforzar la Base Tecnológica e Industrial para la Defensa para sostener proyectos

19 "La cumbre galesa de la OTAN, continuidad y cambio", Jordi Marshall, Infodefensa, (22/09/2014) disponible en: http://www.infodefensa.com/es/2014/09/22/noticia-cumbre-galesa-continuidad-novedad.html

20 "Rusia y Occidente aceleran su ciberguerra", Eduaro Fabro, Diario Página 12, (28/09/2014) disponible en: http://www.pagina12.com.ar/diario/elmundo/4-256329-2014-09-28.html

de la denominada "Smart Defence" (defensa inteligente), que incluyan profundizar tres iniciativas: una dirigida al desarrollo de capacidades logísticas, protección ante ataques de destrucción masiva con el desarrollo de armamento de precisión y cuarteles generales desplegables; crear y mantener una fuerza expedicionaria y la sostener medios para la estabilización y reconstrucción.

Cabe destacar que Maxime Pinard, director de Ciberestrategia en el Instituto de Relaciones Internacionales y Estratégicas (IRIS) en relación a estas nuevas concepciones indicó que: "nos dirigimos hacia una militarización reforzada del ciberespacio con un riesgo certero de engranaje donde los cibernautas (simple usuarios) serán las principales víctimas" [21].

Para la OTAN, en todos los ámbitos del Poder Nacional: "la ciberguerra es asimétrica. El bajo coste de los equipos informáticos puede implicar que nuestros adversarios no tengan necesidad de fabricar armamento caro y sofisticado para suponer una amenaza significativa a nuestras capacidades militares. Unos cuantos programadores pueden, si encuentran una vulnerabilidad a explotar, amenazar nuestros sistemas logísticos, robar nuestro planeamiento operacional o cegar nuestros sistemas de inteligencia y de mando y control. Por este motivo, muchos ejércitos están desarrollando capacidades ofensivas en el ciberespacio y se estima que más de 100 servicios de inteligencia extranjeros llevan a cabo estas actividades."[22]

Así, la OTAN aprecia estar "inmersa en un proceso de transformación profunda de sus estructuras, procedimientos y capacidades, con el fin de conseguir unas fuerzas aliadas mejor dotadas, interoperables y capaces de actuar con la máxima eficacia. (…) Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar, aire y espacio, a través del ciberespacio"[23].

El Manual Otan de Tallin (2013) y la Aplicabilidad del Derecho Internacional Humanitario (dih) a los Ciberconflictos

Una guerra no deja de ser tal porque se libre en el ciberespacio en vez de los ambientes tradicionales de tierra, agua y contemporáneo del aire. Si consideramos al ciberespacio como un escenario más en el cual los estados a través de sus ejércitos participarían en guerras cibernéticas, cabe investigar si es posible aplicar el "ius ad bellum" (o el derecho que regula el recurso de la fuerza por parte de los Estados) y el "ius in bello" (derecho de la guerra o derecho internacional humanitario,

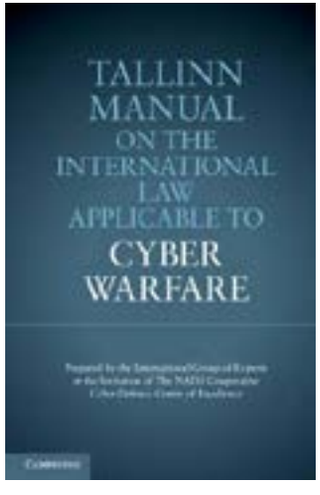
21 Ibídem 20.

22 www.reuters.com/article/idUSTRE69C5ED20101013

23 Diaz del Río Durán, Juan José. "La ciberseguridad en el ámbito militar" Instituto Español de Estudios estratégicos. Cuaderno de estrategia N° 149. Pág. 220

que regula el comportamiento durante el uso de la fuerza en un conflicto armado) a dicho contexto, siendo este uno de los mayores desafíos para los hombres del derecho. Hay diversas posturas jurídicas al respecto. Algunos autores dicen que se necesitaría un marco legal específico, otros autores opinan que todas las normas del DIH que rigen la conducción de las hostilidades serían adaptables y aplicables durante un conflicto armado cibernético, ya que en definitiva las normas a las que nos referimos tienen por objetivo proteger a la población y los bienes civiles contra los efectos de las hostilidades bélicas, por ello es que podemos incluir a los ataques cibernéticos.

Recientemente expertos en la materia han confeccionado una especie de corpus normativo del "Tallinn Manual on the International Law Applicable to Cyber Warfare"[24], denominado comúnmente "**Manual de Tallin", que lleva el nombre de la capital de Estonia, publicado en Abril de 2013, donde se compiló y perpetró el primer ataque cibernético de un país a otro. Se creó a pedido del Centro de Excelencia en la Defensa Cooperativa Cibernética de la OTAN.**



El manual de 282 páginas no es un cuerpo normativo oficial de la OTAN, pero es una guía importante para situaciones que se puedan plantear en el ciberespacio, toma normas vigentes de carácter internacional sobre conflictos armados como la Declaración de San Petersburgo de 1868 o las Convenciones de Ginebra de 1949, y las aplica adaptándolas al ciberespacio. El Manual es el resultado de un trabajo de tres años de análisis de las normas internacionales que pueden aplicarse para combatir los ataques de la guerra cibernética elaborado por un grupo de expertos independientes que emiten opiniones bajo su absoluta responsabilidad, pero crea

24 Disponible en varios sitios web como: http://nuclearenergy.ir/wp-content/uploads/2013/11/tallinn_manual.pdf

el primer cuerpo de ideas sobre a la materia.

Así, Marco Roscini, profesor de Derecho Internacional en la Universidad de Westminster, en Londres, dijo que el manual es el primer intento en su clase de mostrar que las leyes de guerra, algunas de las cuales datan del siglo XIX, son lo suficientemente flexibles para aceptar las nuevas realidades de los conflictos en el espacio cibernético. En el Manual se indica por primera vez el procedimiento a seguir por parte de los estados y las alianzas militares en caso de ciberataques masivos. En cierta medida, el objetivo de la publicación es apreciar que las actuales normas legales internacionales (sobre todo en derecho internacional humanitario) son aplicables también en el ciberespacio. Para el Manual, los (ciber) ataques desarrollados en ausencia de acciones militares pertenecen a la categoría de las "acciones en contra de la ley" por lo que la reacción a los mismos puede llevar al agresor ante ámbitos penales o tomar "contramedidas proporcionales".

Esto último depende de la envergadura del ciberataque y sus consecuencias (muertes, daños o destrucción de edificios), por lo que un (ciber) ataque en tiempos de paz podría llegar a ser equivalente al "uso de la fuerza" o a un "ataque armado". De este modo. El Estado agredido poseería el derecho a defenderse, permitiendo entre otras cosas el uso del armamento tradicional. Michael D. Schmitt, uno de los principales autores del Manual y profesor de la Escuela de Guerra Naval de Newport, EEUU, indicó que el ataque de virus Stuxnet, perpetrado contra las infaestructuras críticas de Irán en 2009, constituye en sí mismo un "acto de fuerza".

Críticas Rusas al Manual

Al conocerse el Manual, países como Rusia que aprecian la necesidad de nuevas leyes han indicado que el *documento sería la legitimación del propio concepto de las ciberguerras.*

En Rusia, Konstantín Peschanenko, representante del Ministerio de Defensa y Andréi Krutskij, enviado especial del Ministerio de Asuntos, han indicado que mientras Rusia intenta prevenir la militarización del ciberespacio, proponiendo a la comunidad internacional la aprobación de normas especiales de comportamiento, la OTAN estaría acordando normas de comportamiento durante las ciberguerras.

Por su parte, Alexander Bedritski, experto del Instituto Ruso de Investigaciones Estratégicas (RISI), Moscú en temas como "el proceso de una guerra interestatal en el ciberespacio", ha expuesto que por sobre las consideraciones del Manual y aunque es difícil el acuerdo, hay posibilidad de diálogo entre Washington y Moscú sobre estos asuntos. En el mismo sentido,

Oleg Demídov, experto del Centro de Investigaciones Políticas de Rusia, expone que: "si Rusia y sus aliados conciben su misión como el objetivo de no permitir los conflictos interestatales en el ciberespacio, así como hacer públicos estos fe-

nómenos ilegales en el terreno internacional, el 'Manual de Tallin' consistirá más en "¿Qué hacer si de todos modos se ha desatado un conflicto?", por lo que ambos enfoques podrían coincidir. Demídov, indica que si el Manual no posee el apoyo de ninguna norma internacional que mantenga a los estados alejados de la participación en las ciberguerras, puede realmente garantizar una legitimación de los ciberconflictos lo que propiciaría "la proliferación de este tipo de conflictos en el sistema de las relaciones internacionales del siglo XXI como un medio válido de cumplir los objetivos en política exterior y garantizar los intereses nacionales"[25].

Interrogantes Legales que Presenta El Manual

- ¿Una computadora puede ser considerada un arma?

  Si, efectivamente son consideradas armas, aunque no convencionales, por su capacidad para causar un daño tanto a un enemigo como a la población civil. En este punto se debe evaluar si pueden ser considerados sus efectos indiscriminados. Esta conceptualizacion es importante porque su uso podría estar prohibido por una Convención internacional.

- ¿Cómo definir al combatiente del ciberespacio?

  Cabe recordar que "combatiente" es todo miembro de las fuerzas armadas, excepto el personal sanitario y religioso. En una acción de combate los combatientes deben distinguirse de la población civil. Éstas se distinguen por su uniforme, un signo distintivo y armas a la vista. Un aspecto del ciberespacio que plantea dificultades es el anonimato tras el que se esconden quienes participan de las operaciones cibernéticas, por lo que hay dificultades para establecer si los participantes forman parte de las fuerzas armadas, son combatientes regulares o no, o son mercenarios de las mismas.

- ¿Han cambiado las amenazas en la guerra cibernética?

  Si, las amenazas han dejado de provenir de naciones identificadas y tienen múltiples orígenes en estados fallidos, grupos terroristas o incluso "solitarios", el recurso a los ciberataques supone un medio rápido, económico y ágil que, vulneran la seguridad de nuestros países de manera sensible. Cabe agregar que las operaciones de guerra convencional pueden estar acompañadas de operaciones en el ciberespacio.

- La definición de "objetivos militares" ¿es aplicable a estos conflictos?

  Si, considerándose como tal a las fuerzas armadas, los establecimientos y construcciones así como sus materiales, también otros bienes que por su

25 **"**Rusia teme que la OTAN haya desarrollado un documento para legitimar las ciberguerras" Elena Chernenko, Kommersant Vlast, Actualidad de Rusia (28/5/13)

naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a acción militar y cuya destrucción total o parcial, captura o neutralización tenga, en las circunstancias del caso, una concreta ventaja militar.Los convenios internacionales prohíben ataques contra "objetivos civiles".Cabe un interrogante, si cuando se habla de "objetivo" sea civil o militar, se alude también a "información" que se pudiera capturar o destruir. Es evidente que la información puede ser un "objetivo".

- ¿El empleo legítimo de la fuerza en respuesta a un ataque?

  La legítima defensa se encuentra normada en el artículo 51 de la Carta de la ONU, puede ser individual o colectiva, e indica: "ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales". Este artículo se aplicaría a la guerra cibernetica.

- ¿Cómo opera el concepto de neutralidad?

  Opera igual que en la guerra convencional, un país neutral debe abstenerse de participar de las hostilidades. Por otro lado, los contendientes deben tener en cuenta que lanzar un ataque desde la red informática de una nación neutral está prohibido, de la misma manera que ejércitos hostiles no pueden pasar por el territorio de un país neutral.

- ¿Cómo juegan los principios de distinción y proporcionalidad?

  El principio de distinción exige a las partes en conflicto que distingan entre civiles y combatientes, entre bienes civiles y militares. Solo son legítimos los ataques perpetrados contra combatientes u objetivos militares. Se prohíben los ataques indiscriminados, es decir no causar daños o víctimas excesivas en relación al resultado militar esperado. Por ejemplo un virus informático que se duplica constantemente que infecta redes militares y que por su interconexión también causa daños inestimables a infraestructura cibernética civil constituiría una infracción del DIH.Finalmente debemos recordar la Cláusula Martens, principio subsidiario aplicable al ciberespacio, que dice que en los casos no previstos por el derecho positivo, las personas civiles y los combatientes están bajo la protección y la autoridad de los principios del derecho internacional derivados de: la costumbre es-

tablecida, los principios de humanidad y la conciencia pública.

Problemas Específicos que se Plantean para La Ciberdefensa

En primer lugar, al examinar las respuestas legales a los efectos de la ciberdefensa, la situación varía entre los diferentes países y regiones, con diferente grado de desarrollo de las nuevas tecnologías y con diferente grado de desarrollo de sus legislaciones. Más de 45 países han firmado el Convenio de Ciberdelincuencia, tanto en el espacio del Consejo de Europa como Naciones Unidas. Sin embargo, hay distinta escala de operatividad del mismo, debida a múltiples circunstancias, entre ellas la efectiva incorporación a los ordenamientos nacionales de las disposiciones internacionales así como los grados de afectación por parte de los ciberataques. De ello se desprendería una diferencia conceptual entre ciberdefensa y ciberdelincuencia.

Cabe agregar que cuando se habla de la ciberdelincuencia se alude a delitos penales nacionales o transnacionales y no de ciberguerra, pese a que en ésta se desarrollen acciones iguales a los ciberdelitos. Muchos países permanecen absortos en sus prioridades y problemas internos. Esta actitud supone un desconocimiento de las ventajas globales de la cooperación y armonización internacional en ciberdefensa.

El convenio sobre ciberdelincuencia es altamente positivo, crea conciencia internacional sobre la evolución y magnitud de este problema, logrando consensos políticos aunque mínimos sobre las conductas a prohibir y de los mecanismos de persecución y colaboración jurisdiccional. Es un gran avance al propiciar definiciones legales estándar, posibilitar la extradición y fortalecer la cooperación policial y judicial entre Estados. Se debe avanzar hacia convenios internacionales sobre estrategias a adoptar también en materia de ciberdefensa.

Alcanzar consensos sobre ciertas definiciones legales tales como ciberguerra, ciberdefensa, ello, a los efectos de armonizar normativas de derecho internacional o convenios internacionales de diferentes estados, ello contribuye a articular una efectiva cooperación internacional. Si los países adhieren a convenciones internacionales sobre la materia, se pueden desarrollar adecuadamente procedimientos de extradición, intercambio de pruebas y toda clase de información. Un aspecto interesante es que la constante innovación tecnológica hace que los marcos normativos queden obsoletos, de allí la necesidad de una actualización constante.

Hacia una Ciberdefensa Regional

El desafío de integración asumido por los países de la región en la última década, especialmente con la creación de la Unión de Naciones Suramericanas (UNASUR), permitió plantear la defensa desde una perspectiva regional disuasiva y cooperativa, incluyendo la ciberdefensa.

En ese marco de cooperación y en la necesidad de enfrentar potenciales amenazas cibernéticas por medio del desarrollo de una estrategia regional de ciberdefensa se desarrolló en Buenos Aires del 14 al 16 de mayo del corriente año el Seminario Regional de Ciberdefensa, coorganizado por el ministerio de Defensa de Argentina y el Consejo de Defensa Sudamericano (CDS) de la UNASUR procurando la complementación de los avances alcanzados por los distintos países para disminuir las situaciones de vulnerabilidad, diseñar y contar con respuestas adecuada ante eventuales incidentes. La apertura del seminario estuvo a cargo del Ministro de Defensa Ing. Agustín Rossi, quien enmarcó el mismo en el Plan de Acción del CDS 2014 en lo referido a las capacidades en materia de cooperación frente a amenazas cibernéticas y desarrollo de tecnologías regionales para la protección de infraestructuras críticas, con el objetivo de que se jerarquice esta materia para la formulación de futuras políticas de defensa.

A tal efecto, en el CDS, se constituyó el Grupo de Trabajo de Ciberdefensa con el objetivo de conocer lo que cada país está realizando e informar sobre las capacidades desarrolladas para compartir y complementar las novedades en la materia, vinculando a expertos y referentes para incentivar el desarrollo de proyectos en el marco regional. El seminario, del cual participaron expertos de la región y a nivel internacional concluyó con la reunión del referido Grupo de Trabajo de Ciberdefensa y del Grupo de Trabajo de Telecomunicaciones del MERCOSUR con el objetivo de materializar la necesidad de enfrentar potenciales amenazas cibernéticas abre la posibilidad de plantear una estrategia regional de ciberdefensa.

Cibercomandos de Defensa en la Región

Diversos países han creado y se encuentran en previsión crear centros de Ciberdefensa. En tal sentido, por Resolución N° 343/14 del 14 de mayo, el Ministro de Defensa, Ing Agustín Rossi, dispuso la creación del Comando de Ciberdefensa dependiente del Estado Mayor Conjunto de las Fuerzas Armadas. Asimismo, el 16 de junio el Sr SubJefe del EMCFFAA, puso en funciones del Comandante Conjunto de Ciberdefensa.

En los considerandos de la Resolución, el nuevo Comando tendrá como misión "ejercer la conducción de las operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el planeamiento estratégico militar y desarrollar capacidades frente a los ciberataques contra las infraestructuras críticas de la información y

los activos del sistema de Defensa Nacional y de su Instrumento Militar. Asimismo se instruye a los Jefes de los Estados Mayores de las tres FFAA para desarrollar capacidades de ciberdefensa en orden a contribuir con el referido Comando.

Conclusiones

El estudio sobre la apreciación estratégica de la OTAN nos brinda una importante experiencia ante la necesidad de un planeamiento estratégico que ha generado esta nueva modalidad de ataque para proteger los intereses vitales de una nación como así también la necesidad de fomentar la investigación y desarrollo en proyectos con capacidad de mitigar y repeler estas nuevas amenazas cibernéticas.

Evidenciamos "que la Alianza Atlántica, que fue la primera en percibir la necesidad de acomodar las respuestas tradicionales al nuevo escenario estratégico, está inmersa en un proceso de transformación profunda de sus estructuras, procedimientos y capacidades, con el fin de conseguir unas fuerzas aliadas mejor dotadas, interoperables y capaces de actuar con la máxima eficacia. (…) Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar, aire y espacio, a través del ciberespacio"[26]

El Manual de Tallin demuestra los siguientes indicadores:

1. Mutación de la categoría jurídica de ciberdefensa.
2. Nos hallamos ante un nuevo escenario, el ciberespacio, en el ocurren crímenes y guerras.
3. El control del ciberespacio hace peligrar los valores del Estado de Derecho, especialmente en los derechos fundamentales.
4. Cibercrimen y ciberamenazas no son categorías equivalentes, existen ciberdelitos que no constituyen amenazas a la seguridad.

Alcanzar consensos sobre ciertas definiciones legales tales como ciberguerra, ciberdefensa, ello, a los efectos de armonizar normativas de derecho internacional o Convenios internacionales de diferentes estados, ello contribuye a articular una efectiva cooperación internacional.

Si los países adhieren a Convenciones internacionales sobre la materia, se pueden desarrollar adecuadamente procedimientos de extradición, intercambio de pruebas

26 Durán, Juan José Diaz. "La ciberseguridad en el ámbito militar" Instituto Español de Estudios estratégicos. Cuaderno de estrategia N° 149. Pág. 220

y toda clase de información. Un aspecto interesante es que la constante innovación tecnológica hace que los marcos normativos queden obsoletos, de allí la necesidad de una actualización constante.

Bibliografía

- Artiles, Nestor. "La Situación de la ciberseguridad en el ámbito internacional y en la OTAN". Instituto Español de Estudios Estratégicos (IEEE). Cuaderno de Estrategia N° 149.
- Cano, Jeimy. "Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global" N° 119 (abr-Jun. 2011) Revista Sistemas, Colombia.
- Durán, Juan José Diaz. "La ciberseguridad en el ámbito militar" Instituto Español de Estudios Estratégicos. Cuaderno de estrategia N° 149.
- Ministerio de Defensa (2010). Manual de Derecho Humanitario de los Conflictos Armados. Buenos Aires.Disponible en: http://www.mindef.gov.ar/publicaciones/pdf/Manual-de-derecho-humanitario-de-los-conflictos-armados.pdf
- Ministerio de Defensa de España (2013). XXXIII Curso de Defensa Nacional. Guerra Cibernática: Aspectos Organizativos. Disponible en: http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf
- Ministerio de Defensa de la República Argentina y Consejo de Defensa Sudamricano de la UNASUR (2014). "Seminario Regional de Ciberdefensa", Buenos Aires. Disponible en: http://www.youtube.com/watch?v=fd9X_xCQk50 y http://www.youtube.com/watch?v=XOwVV8RtQqg
- Ministerio de Defensa. Dirección General de Relaciones Internacionales. Instituto Español de Estudios Estratégicos Documento informativo del IEEE 37-2011. La Política de Ciberdefensa de la OTAN.
- Ministerio de Defensa. Dirección General de Relaciones Internacionales. Instituto Español de Estudios Estratégicos. Documento informativo del IEEE 09/2011. Nuevo concepto de Ciberdefensa de la OTAN.
- NATO Cooperative Cyber Defence Centre of Excellence (2013). "Tallinn Manual on the International Law Applicable to Cyber Warfare" (Tallinn Manual). Cambridge University Press.
- Mälksoo, Lauri (2013). The Tallinn Manual as an international event. Diploaatia. Estonia. Disponible en: http://www.diplomaatia.ee/en/article/the-tallinn-manual-as-an-international-event/

- Nguyen, Nam (2014). The International Humanitarian Law Implications of the 'Tallinn Manual. E-International Relations Students. RUGB. Disponible en: http://www.e-ir.info/2014/02/12/the-international-humanitarian-law-implications-of-the-tallinn-manual/
- 12. Healey, Jason (2013). Reason Finally Gets a Voice: The Tallinn Manual on Cyber War and International Law. EUA. Disponible en: http://www.atlanticcouncil.org/en/blogs/new-atlanticist/reason-finally-gets-a-voice-the-tallinn-manual-on-cyber-war-and-international-law
- Reyes Manzano, María Rosa (2013). "El ciberespacio como un nuevo reto del Derecho Internacional. La ciberguerra en el Derecho Internacional Humanitario". Tesis Master en Estudios Estratégicos y Seguridad Internacional, Universidad de Granada. España. Disponible en: http://www.academia.edu/5455118/_El_ciberespacio_como_un_nuevo_reto_del_Derecho_Internacional._La_ciberguerra_en_el_Derecho_Internacional_Humanitario_

Currículum Vitae de la Dra. Claudia Elizabeth Fonseca.

Doctora en Psicología Social y Licenciada en Ciencia Política por la Universidad Argentina John F. Kennedy (UAJFK). Docente la ESG-IUE y en postgrado en la UAJFK. Ex docente del Colegio Militar de la Nación y del Instituto Universitario de la PFA. Realizó el curso de Formación de Investigadores (ESG-IUE). Integra el Equipo de Investigación "Ciberdefensa" de la Secretaría de Investigación de la ESG.IUE.

Currículum Vitae de la My. Ivonne Luz Perdomo

Mayor Auditora del Ejército Argentino. Se desempeña en la Secretaría General del Ejército como Jefa del Departamento Asesoría. Abogada por la Universidad Católica de La Plata. Cursante de la Licenciatura en Relaciones Internacionales (ESG-IUE). Fue docente de la ESG. Es Profesora Universitaria por la UMSA. Integra el Equipo de Investigación "Ciberdefensa" de la Secretaría de Investigación de la ESG-IUE.

Currículum Vitae del Mg. Miguel Ansorena Gratacos

Licenciado y Profesor Universitario en Relaciones Internacionales por la Universidad Católica de Salta. Magíster en Defensa Nacional por el Instituto Universitario del Ejército. Egresado de la Escuela de Defensa Nacional. Docente en la ESG-IUE, en la ESG Conjunta y en la Escuela Superior de Guerra Aérea (ESGA). Realizó el curso de Formación de Investigadores (ESG-IUE). Integra el Equipo de Investigación "Ciberdefensa" de la Secretaría de Investigación de la ESG-IUE.

Currículum Vitae del Dr. Javier Ulises Ortiz

Doctor en Ciencia Política, Lic. en RRII y Profesor Universitario por la USAL. Postgraduado en Estrategia I y II (ESG-IESE). Investigador Cat. II (MinEduc.) e Investigador Principal (IiC3) acreditado por la Subsec. de Investigación Científica y Des. Tecnológico (MinDef). Docente ESG-IUE y ESGC. Director del Proyecto de Investigación "Ciberdefensa" (ESG). Autor de: "Estrategias de Defensa Cibernética en la Era de la Información", La Revista ESG N° 582 (2011); "Argentine: the challenge of IO" Iosphere, Kansas, EUA (2008) y "La necesidad de un nuevo pensamiento estratégico frente a la guerra de la información", La Revista ESG (2003).

En este artículo, la autora hace un análisis detallado de cómo era pensada la política al interior de las Sociedades de Tiro y en la Dirección General de Tiro durante los primeros años del Siglo XX

Discursos y Prácticas. La Política en las Sociedades de Tiro

Autora: Bárbara Raiter

"la institución guardará una prescindencia completa y absoluta en toda cuestión política, electoral y religiosa, ya sea nacional, provincial o local, siendo en consecuencia prohibida toda propaganda o discusión al respecto en el local de la sociedad"[1].

Estatutos del Tiro Federal San Francisco, 1903.

Introduccion

¿Cuál es el sentido de esta afirmación?, ¿cómo analizarla, pensarla y explicarla? Entre 1880-1920 en Argentina se experimentó una profunda transformación demográfica, económica, social y política. Dentro del conjunto de transformaciones, tres procesos concurrentes tuvieron lugar y operan como marco general y explicativo de esa afirmación.

En primer lugar tenemos que mencionar la organización estatal nacional, que desarrolla un conjunto de instituciones específicas para el ordenamiento administrativo, político, fiscal del país. En particular se destaca la construcción del Ejército Argentino, como institución militar y política, que en el período que nos ocupa está definiendo (y debatiendo) su forma institucional, a partir de la organización interna, la profesionalización de sus miembros y, también, la inclusión bajo bandera del conjunto de los ciudadanos a través del servicio militar obligatorio[2].

1 Tiro Federal San Francisco, *Estatutos*, Córdoba, 1903, mimeo

2 Cantón, Darío (1969), "Notas sobre las Fuerzas Armadas argentinas", en Di Tella, T. y Halperín Dongui, T., *Los fragmentos del poder*, Buenos Aires, Jorge Álvarez; Comando en jefe del Ejército (1971), *Reseña histórica y orgánica del Ejército Argentino*, Buenos Aires, Círculo Militar; Forte,