CARI /

Instituto de Seguridad Internacional y Asuntos Estratégicos

BOLETÍN DEL ISIAE

Septiembre 2015

Número 61

CARI
Consejo Argentino para las Relaciones Internacionales

Presidente
Adalberto Rodríguez Giavarini

ISIAE
Instituto de Seguridad Internacional y Asuntos Estratégicos

Director
Julio A. Hang

Secretario de Redacción
Lic. Alejo M. Ferrandi Aztiria

Contacto
difusionrdnisiae@gmail.com

Web
http://www.cari.org.ar/organos/isiae.html

Uruguay 1037, piso 1º
C1016ACA
Buenos Aires
Argentina
(5411) 4811-0071
www.cari.org.ar
@CARIconsejo

DEBATES EN TORNO A LA CIBERSEGURIDAD

SUMARIO

El Problema de la Ciber Atribución:
Aportes para una estrategia de Ciber Defensa

Prof. Dr. Roberto Uzal (*)

Introducción

La Ciber Atribución[1], la Ciber Anonimidad[2][3] y la Ciber Disuasión[4] constituyen las tres áreas esenciales de investigación y desarrollo, de adquisición y ejercicio de capacidades instrumentales y también de formación de Recursos Humanos, con un enfoque de mejora continua, en el ámbito de la Ciber Defensa.

En principio resulta imprescindible, para todo estado nación, poseer la capacidad de identificar y localizar a los responsables de Ciber Agresiones, especialmente aquellas dirigidas a afectar su Infraestructura Crítica[5]. Esto debe (y puede) lograrse con una muy alta probabilidad de éxito asociada, una muy baja tasa de falsos positivos y produciendo resultados casi en "tiempo real"[6][7][8][9]. Si un estado nación logra un alerta temprana de una Ciber Agresión, puede llegar a evitar que dicha Ciber Agresión cause daños pero, si no logra identificar y localizar al atacante, el éxito "defensivo" habrá sido parcial, casi mínimo. Al no identificar al Ciber Agresor, una importante oportunidad de posicionamiento positivo, en el contexto global de la Ciber Defensa, habrá sido desaprovechada.

Un estado nación, con una reconocida capacidad de Ciber Atribución será un estado tenido en cuenta en el proceso de toma de decisiones en la región y en el mundo. Casualmente, el foco de este trabajo está puesto en el denominado "Problema de la Ciber Atribución".

Por otro lado, referido ahora a la Ciber Anonimidad, se la puede asociar con la privacidad absoluta y con la reserva de la identidad de individuos y de organizaciones durante la interacción con la Red de Redes y otras redes que, directa o indirectamente, están vinculadas a Internet. La Ciber Anonimidad no necesariamente está orientada hacia fines o actividades maliciosos. Numerosas personas y organizaciones intentan diversos niveles de anonimidad como enfoque para incrementar la seguridad. Específicamente, en el ámbito de la Ciber Defensa, la Ciber Anonimidad ocupa un lugar de muy alta sensibilidad, tanto en operaciones defensivas como en las ofensivas.

Existen productos desarrollados con la intención declarada de incrementar la Anonimidad de los usuarios de Internet. Se citan como ejemplos a Anonabox[10] y Tor[11][12][13]. Este último es conocido por el acrónimo de "The Onion Router" (El Router Cebolla) aunque

[1] http://itlaw.wikia.com/wiki/Attribution_problem
[2] http://www.telegraph.co.uk/technology/internet-security/11422997/How-to-protect-your-anonymity-online.html
[3] http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
[4] http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/
[5] Una visión acerca de este tema: http://www.cfr.org/global/global-conflict-tracker/p32137#!/?marker=2
[6] https://www.iseclab.org/papers/disclosure.pdf
[7] http://sedici.unlp.edu.ar/bitstream/handle/10915/27537/Documento_completo.pdf?sequence=1
[8] http://desd.espe.edu.ec/wp-content/uploads/2015/06/Seminario-Defensa-Cibern%C3%A9tica-Dr-Uzal.pdf
[9] https://www.researchgate.net/publication/266652173_Trust_in_Cyberspace_New_Information_Security_Paradigm
[10] http://www.wired.com/2015/04/anonabox-recall/
[11] https://www.torproject.org/
[12] http://www.onion-router.net/
[13] https://www.youtube.com/watch?v=CmNWmdUXlLg

(*) Director del Doctorado en Ingeniería Informática de la Universidad Nacional de San Luis. Investigador Categoría I, Programa de Incentivo a la Investigación en Universidades Nacionales. Consultor en Ciber Defensa.

últimamente se lo reconoce como "Proyecto Tor". Tor, como herramienta para evitar la identificación de routers, comenzó a ser denominado con ese nombre a partir de 2004 aunque los primeros antecedentes de su desarrollo se remontan a 1995, cuando la "Office of Naval Research" de la Armada de Estados Unidos se fija el objetivo de a) proteger las redes militares de intrusiones no autorizadas, b) realizar una suerte de análisis de flujos de red y, c) lograr comunicaciones privadas protegiendo la anonimidad de los usuarios de la red.

De ninguna manera estas herramientas de incremento de la capacidad de Anonimidad constituyen impedimentos para lograr resultados de alta confiabilidad cuando se trabaja en Ciber Atribución; sólo incrementan la complejidad de la tarea. Adicionalmente, incorporar a las redes del área Defensa de distintos países productos de "Anonimidad" adquiridos en el exterior (países distintos a los usuarios), constituiría un acto de ingenuidad extrema.[14][15][16][17][18]

Pasando desde la Ciber Atribución a la Ciber Disuasión, se destaca que la Disuasión en general se manifiesta en casi todas las formas de relaciones humanas. Ha existido desde casi siempre en los vínculos entre grupos y por supuesto en la interacción entre estados naciones. A pesar de su importante incidencia en las relaciones internacionales, la disuasión no atrajo demasiado la atención de los estudiosos hasta después de finalizada a Segunda Guerra Mundial. Su auge como objeto de estudio y como herramienta política fue asociado, con frecuencia, a la disponibilidad, por parte de ciertos estados naciones, de armas de destrucción masiva. Cronológicamente se la ha vinculado fuertemente al contexto político mundial correspondiente al desarrollo de la Guerra Fría.

En el ámbito de la Disuasión están ampliamente reconocidos los aportes de William Weed Kaufmann[19][20], específicamente a la entonces denominada "Estrategia de la Disuasión Nuclear".

Debidamente adaptadas al entorno eminentemente asimétrico de la Ciber Defensa, algunas de las ideas fundamentales del Dr. William Kaufmann constituyen una importante contribución, como referencia, para quienes incursionan en el ámbito de la Ciber Disuasión. El desafío, en este caso, es el de compatibilizar/extrapolar/interpolar los aportes del Profesor Kaufmann a un contexto eminentemente asimétrico como lo es el de la Ciber Defensa.

La Ciber Disuasión se manifiesta mediante la percepción, por parte del oponente real o potencial, de a) la propia capacidad para identificar el origen de Ciber Ataques y b) la propia capacidad para ejercer en el Ciber Espacio el derecho que deriva del Artículo 51 de la Carta de las Naciones Unidas[21].

Ciber Disuación debería ser motivo de profundo análisis por parte de las autoridades nacionales. A juicio del autor, hace a los intereses de Argentina el que se consolide un consenso global que la reconozca como un país sólidamente posicionado como no-Ciber Agresor pero, al mismo tiempo, con el equipamiento y los Recursos Humanos necesarios que le posibiliten resolver la casi

[14] http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf

[15] http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

[16] http://www.cnet.com/news/nsa-has-backdoor-access-to-internet-companies-databases/

[17] http://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism

[18] http://www.ecommercetimes.com/story/81530.html

[19] http://www.washingtonpost.com/wp-dyn/content/article/2008/12/16/AR2008121602724.html

[20] Uno de los seguidores más notorios de William Weed Kaufmann lo es Richard A. Clarke, quien sirvió por treinta años en el gobierno de EEUU. Asistió a tres Presidentes de EEUU consecutivos. Sus últimos cargos en el gobierno lo fueron "Advisor to the President for Cyberspace" y "National Coordinator for Security and Counter-terrorism". Clarke enseño durante cinco años en la Harvard's Kennedy School of Government y escribió siete libros; entre ellos el ya clásico Cyber War, en este caso asistido por Robert K. Knake.

[21] http://www.un.org/es/documents/charter/chapter7.shtml#article51

totalidad de las variantes del Problema de la Ciber Atribución.

Lo señalado[22] debe ser acompañado con una amplia y robusta capacidad forense para efectuar presentaciones, sólidamente sustentadas, ante organismos internacionales.

La Ciber Disuasión requiere que, globalmente, se reconozca que Argentina cuenta con los recursos necesarios para ejercer plenamente, si fuere necesario, el derecho contemplado en el ya citado Artículo 51 de la Carta de las Naciones Unidas. Logrado el mencionado reconocimiento global, se minimizará la probabilidad de ser objeto de Ciber Agresiones provenientes de otros estados naciones y/o agentes estatales foráneos.

Viene al caso señalar que, frecuentemente, especialistas en Ciber Defensa pertenecientes a grandes potencias, le quitan importancia o aún niegan la existencia de una suerte de Ciber Disuasión; esto es entendible como componente comunicacional de una Ciber Estrategia. Eso sí, negar la capacidad potencial de Ciber Disuación a países medianos o pequeños es casi equivalente a negar el carácter asimétrico de la Ciber Defensa, es decir, es una postura difícilmente sustentable.

Aspectos específicos de la Ciber Atribución

Retomando el foco de esta contribución, es decir los aspectos vinculados con la Ciber Atribución, se destaca que la asociación de Ciber Agresiones a un responsable específico constituye un asunto no trivial. La complejidad de la solución del Problema de la Atribución ha sido utilizada, por determinados gobiernos, como sustento de importantes campañas comunicacionales destinadas a difundir el mito de la imposibilidad de solucionar el mencionado problema.

Curiosamente, la expansión del mito de la no-solución del Problema de la Atribución, ha recibido "ayudas" muy importantes y difícilmente explicables las que ameritan, por su carácter casi insólito, una seria investigación ad hoc[23].

En forma paradojal, la jurisprudencia y las opiniones de organismos internacionales que se han venido acumulando, establecen que un Ciber Ataque debe poder ser atribuido, con una muy alta probabilidad asociada, antes de que un contraataque del estado nación víctima pueda quedar claramente incluido en los términos del Artículo 51 de la Carta de las Naciones Unidas. Adicionalmente, un robusto y homologado enfoque forense debe respaldar la atribución (origen) de un Ciber Ataque[24][25][26][27]. La atribución de un Ciber Ataque a un estado nación o a un agente estatal es una pre condición sine qua non e internacionalmente requerida, para poder alegar legítima defensa

La Atribución en el Ciber Espacio es compleja; las identidades y localizaciones físicas de los Ciber Agresores pueden ser fácilmente disfrazadas o disimuladas. Sin embargo está claro que Argentina posee el potencial para para calificar entre los estados naciones líderes en este espacio de problema.[28][29][30][31][32][33][34]

[22] Se omiten referencias por lo sensitivo del tema.

[23] CCDCOE (NATO) Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy https://ccdcoe.org/publications/books/Peacetime-Regime.pdf

[24] CCDCOE - "Tallinn Manual on the International Law Applicable to Cyber Warfare". http://www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf

[25] http://digitalcommons.law.yale.edu/fss_papers/3852/

[26] http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1422&context=bjil

[27] https://journals.law.stanford.edu/stanford-law-policy-review

[28] http://argentina.afceachapters.org/wp-content/uploads/2013/07/presentacionDrUzal.pdf

[29] http://sedici.unlp.edu.ar/handle/10915/41932

[30] http://desd.espe.edu.ec/documentacion

[31] http://desd.espe.edu.ec/wp-content/uploads/2015/06/Taller-de-Defensa-Cibernética.pdf

[32] http://ciencia.espe.edu.ec/wp-content/uploads/2015/05/CICTE-SEGURIDAD-Y-DEFENSA.pdf

[33] http://www.sbseg2014.dcc.ufmg.br/programacao/

[34] http://content.netmundial.br/contribution/internet-roadmap-topics-freedom-and-security-in-cyberspace-a-cyber-defense-perspective/61

Como aspecto complementario de esta exposición, viene al caso mencionar que, un entonces recientemente graduado (año 2012), en el área "Law and Politics of International Security", de la Vrije Universiteit (Universidad Libre) de Amsterdam, llamado Dimitar Kostadinov, elaboró, en el año 2013, un muy relevante y acertado artículo sobre Ciber Atribución. Dicho artículo fue publicado en el tópico "hacking" de la página web del "Infosec Institute", una institución orientada a la formación de Recursos Humanos de nivel técnico localizada en Elmwood Park, Illinois, EEUU[35]. El artículo de Kostadinov (de origen búlgaro) sorprendió entonces (2013) por sus contenidos y mucho más sorprende ahora, al cobrar mayor relevancia sus aseveraciones por corresponderse con la experiencia académica y de campo que se ha adquirido, en este ámbito de estudio, en los dos años transcurridos desde su publicación.

El aporte de Kostadinov es una referencia importante de esta presentación; la diferencia esencial entre ambos escritos consiste en que este trabajo utiliza un enfoque sistémico al tratar las interrelaciones entre Ciber Atribución, Ciber Anonimidad y Ciber Disuasión, aunque con un fuerte énfasis en Ciber Atribución. Adicionalmente, otros aspectos esenciales en los que difieren el trabajo de Kostadinov y el presente son: La finalidad, el alcance y las conclusiones.

Retomando el hilo conductor prioritario de este artículo, se resalta que la Ciber Atribución requiere precisión y una consolidada seriedad profesional; si un atacante es erróneamente atribuido, existe un gran riesgo de dañar víctimas inocentes al tomar como blanco, en el ejercicio de la defensa propia, lugares o instalaciones equivocados. Una respuesta dirigida a un blanco equivocado afectará sistemas computacionales o instalaciones "inocentes", especialmente si el Ciber Ataque original ha sido ruteado a partir de alguno de los mencionados sistemas "inocentes" (falso origen del ataque).

Eventualmente podría darse que civiles fuera del control estatal lancen un Ciber Ataque. Esto podría o no tener consecuencias legales para ellos. De todas formas no procedería un ataque militar a gran escala como respuesta.

Se destaca que es también importante determinar, en la Ciber Atribución, cuándo un atacante es o no un actor estatal. Con el propósito de tener un marco adecuado, deberían examinarse primero a los actores no estatales

Los actores no estatales, tales como individuos, grupos organizados y organizaciones terroristas necesitan estar relacionados / vinculados a un estado de manera de que las Naciones Unidas (Consejo de Seguridad) tengan incumbencias en Ciber Conflictos originados por ellos (Artículo 24 de la Carta de las Naciones Unidas)[36]. Caso contrario, las acciones de actores no estatales quedan comprendidas en la legislación doméstica de los países en los que actúen.

La aplicación de "la letra" de los cuerpos legales, en general, dificulta el vincular a actores no estatales a alguna organización o estructura estatal. Es por esto que, mayoritariamente, individuos o pequeños grupos terminan frecuentemente siendo señalados como responsables de Ciber Ataques. Un buen ejemplo de ello es que Rusia sostiene (con bastante apoyo internacional) que fueron "patriotas rusos" quienes, individualmente, atacaron al gobierno de Estonia, a su sistema financiero, etc. Se suele argumentar que, en 2007, "indignados" por el traslado del "soldado de bronce", salieron por propia cuenta, a lavar el honor mancillado de "La Madre Rusia"[37][38]. Dado el incremento de las posibilidades tecnológicas para gestionar la Anonimidad,

[35] http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/

[36] http://www.un.org/es/documents/charter/chapter5.shtml

[37] https://blogs.law.harvard.edu/cyberwar43z/2012/12/21/estonia-ddos-attackrussian-nationalism/

[38] http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia

muchos estados prefieren poner el énfasis en medidas defensivas de carácter pasivo. Se estima que desechar a la Ciber Disuasión como componente esencial de la Ciber Defensa constituye un error conceptual profundo.

Algunas de las medidas "clásicas" para prevenir Ciber Ataques lo son los sistemas de detección de intrusos, firewalls, encriptado, etc. Estos enfoques no incluyen elementos que permitan, efectivamente, identificar y localizar al Ciber Agresor y/o el origen de la acción maliciosa. La claudicación respecto de trabajar para identificar al Ciber Agresor crea un círculo vicioso en el cual la Anonimidad impide la atribución del Ciber Ataque; esta carencia de capacidad de Ciber Atribución trae como consecuencia que los Ciber Agresores evadan la justicia, a la acción de respuesta y/o a las sanciones de organismos internacionales. Esto, a su vez, provoca la caída del nivel de la esencial "Ciber Disuasión"; sin el temor a ser identificados y penalizados, individuos, organizaciones y/o estados naciones continuarán, posiblemente en forma incremental, sus actividades maliciosas en el Ciberespacio.[39]

Ciber Atribución y Ciber Disuasión

Leon Panetta aportó positivamente en el ámbito que se está describiendo: "Los potenciales agresores deberían estar atentos a que los EEUU tienen la capacidad de identificarlos y de localizarlos cuando realicen acciones que impliquen algún tipo de daño, casualmente, a los EEUU"[40].

La expresión de Panetta, como un buen ejemplo de uso correcto de la Ciber Disuasión, está basada en que:

- Un arma cibernética puede producir efectos devastadores.
- Es posible y necesario detectar la autoría del desarrollo y de la utilización de armas cibernéticas.

Lo expresado por Panetta aplica perfectamente en Ciber Agresiones entre estados naciones; es bastante más difícil determinar/atribuir agresiones a organizaciones Ciber Terroristas o grupos de Activismo Hacker; la Ciber Disuasión y el temor a respuestas tienen en ellos efectos mucho menores.

En la Ciber Disuasión juega un rol negativo el mito/falacia de que un Ciber Ataque sofisticado eludirá cualquier tecnología o método de Ciber Atribución, sin importar cuán avanzado este método sea. La Ciber Atribución, en Ciber Defensa, es viable y también necesaria. Un pequeño grupo de Ciber Soldados, de muy alto nivel profesional, podrá resolver problemas de Ciber Atribución sumamente complejos. Se insiste: Ciber Defensa es un contexto eminentemente asimétrico.

Facilitando la Ciber Atribución en un territorio restringiendo la Ciber Anonimidad

Al respecto conviene mencionar que en China, en Egipto, en Siria, en Corea del Norte, en Birmania y en otros estados[41][42][43], existe un detallado control gubernamental y censura en el Ciberespacio en general y en Internet en particular. Los ciudadanos de algunos de esos países, que deseen tener acceso a Internet en forma privada, deben concurrir a una estación de policía, registrarse y adquirir una licencia de usuario de Internet.

La mayoría de los usuarios de Internet en China acceden desde cibercafés que obligatoriamente deben registrar en video toda la actividad allí realizada.

Los correspondientes registros (videos) deben ser almacenados por un tiempo bastante prolongado.

[39] http://www.thei3p.org/docs/publications/350.pdf
[40] http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136
[41] https://getyocrayon.wordpress.com/tag/neutralidad/
[42] https://www.eff.org/deeplinks/2011/12/week-censorship
[43] http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/#wrapper

La Policía de China administra una enorme base de datos en la que está registrada toda la información correspondiente a usuarios de Internet. Existen abundantes antecedentes de juicios y penas relacionadas con delitos cometidos en el Ciberespacio, por ejemplo, subversión.

Como resultado de estas medidas, donde toda China se comporta como una gran Intranet perfectamente monitoreada, el Problema de la Atribución, dentro de ese país, es muy sencillo de ser resuelto. Asimismo, los flujos de red, tanto entrantes como salientes (del país), están controlados por un esquema que funciona como un gran firewall (El Escudo Dorado); una verdadera y nueva Gran Muralla.[44][45][46][47]

Existen otros países que han incluido en su estrategia comunicacional que el Problema de la Atribución es inaplicable en democracia. Esto no es correcto, los flujos de red correspondientes a Ciber Agresiones pueden ser detectados mediante el estudio del comportamiento estadístico de los routers[48], sin violar derechos humanos básicos tales como la confidencialidad, la intimidad, etc.

Casualmente, dichos países han realizado inversiones gigantescas que les posibilitan realizar operaciones de espionaje / vigilancia masivos[49][50][51], casi en tiempo real, las que, o son equivalentes o superan, en sus resultados, a las correspondientes al Escudo Dorado de China.

[44] http://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html

[45] http://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/

[46] http://rendezvous.blogs.nytimes.com/2013/06/28/u-s-prism-meet-chinas-golden-shield/?_r=0

[47] http://www.forbes.com/fdc/welcome_mjx.shtml

[48] http://www.perfil.com/politica/Milani-ya-tiene-un-Centro-de-Ciberdefensa-para-sus-espias-20150201-0030.html

[49] http://www.theguardian.com/world/2013/jun/22/nsa-leaks-britain-us-surveillance

[50] http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11411759

[51] http://www.forbes.com/sites/katevinton/2015/06/30/nsa-will-continue-mass-surveillance-program-for-180-days-with-court-approval/

En otras palabras, buscan lograr, a nivel global, el control que China implantó en su territorio.

La importancia de la Ciber Atribución en el caso de estados naciones

Al tratar el tema de la Ciber Atribución, en el caso de los estados naciones y de los actores estatales, conviene citar a la Carta de las Naciones Unidas la que, en su Artículo 24 y otros, solo reconoce a los estados naciones, en determinadas situaciones, la legitimidad del uso de la fuerza. Las Ciber Agresiones quedan claramente comprendidas en la regulación mencionada.

Los actores estatales están comprendidos en esta categoría porque desarrollan sus actividades en nombre/representación de los estados. Actores estatales son, por ejemplo, las unidades militares de Ciber Defensa/Ciber Seguridad o individuos que trabajan para un gobierno de manera contractual.

Si el atacante es un estado nación, las contramedidas deben tener en cuenta las normas jus ad bellum y jus in bello, es decir las legítimas razones que un estado tiene para entrar en guerra y las prácticas aceptables mientras se está en guerra. Estas están reguladas por la Carta de las Naciones Unidas y por el Derecho Internacional.

Otro aspecto relevante de la Ciber Atribución es el de la "responsabilidad imputada". Cuando un estado nación desarrolla actividades en el Ciberespacio, la soberanía de otros estados necesita ser considerada. Esto es así debido a la naturaleza interconectada e interoperable del Ciberespacio. Operaciones que tengan como blanco la infraestructura TI de un país pueden tener efecto en otros países.

Citando el principio de soberanía y la doctrina de integridad territorial[52], los estados pueden y

[52] http://www.javeriana.edu.co/biblos/tesis/derecho/dere2/Tesis48.pdf

deben ejercitar el control integral de su territorio. En principio puede establecerse que los estados son responsables si desde su territorio se lanzan Cíber Ataques a otros estados naciones.

Enfoques alternativos de Cíber Atribución

Existe una tendencia creciente, por parte de los estados, de búsqueda de otros métodos de Atribución. Una alternativa que merece ser considerada es el concepto ya anticipado de "responsabilidad imputada". En este contexto, como se citó, un estado es responsable por cualquier Cíber Ataque que se origine desde su territorio, aún en el caso de que dichos Cíber Ataques sean lanzados por actores no estatales tales como organizaciones terroristas. De acuerdo con la evidente visión mayoritaria de la comunidad internacional, un estado no cumple con sus obligaciones cuando sus mecanismos legislativos y de procedimientos (protocolos), por una razón u otra, no conducen a los responsables de la Cíber Agresión a juicio y a las correspondientes sanciones.

Mención al caso de "estado santuario"

Merece especial tratamiento, en este trabajo, el caso de "estado santuario". Los conceptos de "santuario terrorista" y "santuario" están asociados a los siguientes escenarios:

1) Una parte o área en el territorio de un país es utilizada por un terrorista u organización terrorista para:

   a) llevar a cabo actividades terroristas, incluyendo entrenamiento, adquisición de recursos, financiamiento y reclutamiento o,

   b) como un territorio tránsito, y

2) El gobierno de dicha área territorial expresamente consciente, conoce, está en conocimiento, permite, tolera o se desentiende de dicho uso de su territorio.

Los gobiernos de estados naciones, que sean catalogados como "estados santuarios", deben responder por las actividades encuadrables en Cíber Terrorismo llevadas a cabo desde sus correspondientes territorios.

Sin embargo, se debe destacar que la justificación de la defensa y/o contraataque o respuesta a un Cíber Ataque proveniente de un "estado santuario", no es un tema del todo claro ni globalmente acordado; muchos estudiosos son partidarios de un enfoque más directo y concreto, especialmente cuando esté en juego la protección de la Infraestructura Crítica Nacional.

¿Límites a las responsabilidades de los estados naciones?

En principio se acepta que los estados no pueden ser señalados como responsables de actos ilegales cometidos por individuos sin que se haya probado que dichos individuos ejercen funciones públicas, es decir, actividades claramente relacionadas con el funcionamiento del gobierno estatal.

Esta aseveración, que deslinda responsabilidades del estado, luego del 9/11, ha sufrido cambios graduales. La tendencia es a establecer excepciones en el deslindar responsabilidades cuando haya evidente negligencia estatal o legislación evidentemente inadecuada según lo expresado por René Värk, opinión que ha alcanzado un amplio consenso internacional[53].

Adicionalmente, "efectivo control" es un estándar requerido a los estados según

[53] http://juridicainternational.eu/authors/14175/

jurisprudencia de la Corte Internacional de Justicia; caso Nicaragua, 1985[54].

Se entiende entonces que una acción de un actor no estatal podría ser atribuida a un estado si dicho estado está, directa o indirectamente involucrado en operaciones conducidas por actores no estatales[55].

Acotación importante: Si el daño a los Sistemas de Información ocasionados por un Ciber Ataque, trae aparejada la muerte o heridas en personas o la destrucción de objetos tangibles, al estado víctima se le presenta bastante claramente la oportunidad de regular su defensa de acuerdo con lo establecido por el Artículo 51 de la Carta de las Naciones Unidas[56].

Síntesis y conclusiones

Esta contribución amerita, en su parte final, una suerte de síntesis, conclusiones y propuestas del autor, que se exponen a continuación:

- Se reconoce que este documento admite numerosos y sustantivos aportes de los lectores para lograr una versión perfeccionada, consensuada y de mayor relevancia; sin embargo se remarca que, sin dudas, Ciber Atribución, Ciber Anonimidad y Ciber Disuasión constituyen conceptos, áreas de conocimiento y ámbitos de adquisición de capacidades instrumentales de muy alta prioridad y perentoriedad de la Gestión Gubernamental en general; no sólo del área Defensa.

- En el contexto apuntado por el párrafo anterior, Ciber Atribución se destaca por su innegable relevancia.

- Argentina no tiene limitaciones, en lo que hace a know how, para encarar un vigoroso programa que la posicione en un lugar de liderazgo en la región, en cuanto a conocimiento y a capacidades instrumentales, en lo que hace a Ciber Atribución .

- Los conocimientos y capacidades instrumentales que Argentina puede y debe adquirir en Ciber Atribución deberán ser homologadas mediante el concurso de organismos internacionales. Dicha homologación es la que le dará sustento a potenciales presentaciones que Argentina pueda efectuar, por ejemplo ante las Naciones Unidas, en el caso de ser víctima de un Ciber Ataque y/o para justificar el ejercicio del derecho reconocido en el Artículo 51 de la Carta de las Naciones Unidas.

- Lo expresado en los dos puntos anteriores es viable y, asimismo, es casi mandatorio. De lograrse lo señalado en los dos párrafos precedentes, se producirían efectos sinérgicos positivos en la relación de Argentina con los otros estados naciones de la región.

- Los recursos a ser destinados para llevar adelante los emprendimientos asociados a la adquisición de capacidades relevantes en Ciber Atribución implican montos razonables. La relación “costo / beneficio” de un proyecto integral en el ámbito citado resulta sumamente favorable a los intereses de Argentina, no restringidos, como se anticipó, al área Defensa.

- Este trabajo prioriza la Ciber Atribución; Sin embargo, Ciber Atribución, Ciber Anonimidad y Ciber Disuasión no constituyen conjuntos disjuntos. Las interacciones entre dichos tres ámbitos son extremadamente importantes. Todo trabajo que se emprenda, como consecuencia de las recomendaciones contenidas en este escrito, deberá tener permanentemente en consideración a la Teoría General de los Sistemas.

- Dada la formación y desarrollo profesional eminentemente ingenieril del autor, se espera que expertos en Relaciones Internacionales y/o Derecho Internacional propongan una versión superadora de los modestos aportes contenidos en esta presentación.

---

[54] https://books.google.com.ar/books?isbn=9682314984
[55] http://resources.infosecinstitute.com/invoking-article-51-of-un-charter-response-cyber-attacks-ii/
[56] https://www.usnwc.edu/getattachment/514e1c26-8117-4ce6-9bca-70afbe295d3d/International-Law-and-Cyber-Threats-from-Non-State.aspx

Una visión de las amenazas ciberespaciales y la defensa

Cnel. Héctor Rodolfo Flores(*)

Aquí está el problema – esto es 1946 en cibernética. Así que tenemos estas nuevas armas potentes, pero no tenemos todo el pensamiento conceptual y doctrinario que respalde a esas armas o cualquier tipo de disuasión. Peor aún, no son sólo los Estados Unidos y los soviéticos quienes tienen las armas – son millones y millones de personas alrededor del mundo que tienen estas armas.
James Mulvenon
President of the Cyber Conflict Studies Association

Tomando en consideración lo expresado por Mulvenon, que sintetiza su evaluación respecto al estado del tema en cuestión, y considerando que la misma es de carácter global, en este trabajo se profundizará y actualizará conceptos que se han desarrollado con antelación, a la luz de la actualización efectuada por el Poder Ejecutivo Nacional de la Directiva Política de Defensa Nacional y a la evolución de las amenazas que a la defensa de los Estados representa actores que emplean el ciberespacio.

Este artículo pretende ser una contribución académica desde y para la Argentina, que empleando criterios de validación y análisis seleccionados por el autor, sean de utilidad. Como parte de dicho proceso se inicia el desarrollo definiendo el *metalenguaje* empleado, así como los vínculos y límites del tema en cuestión.

¿De qué hablamos cuando hablamos de ciberespacio en defensa?

El primer aspecto es definir qué constituye el ciberespacio en relación a la defensa. Para ello, partiremos de la visión que la Directiva Política de Defensa Nacional de la Argentina (DPDN 2014) hace del mismo.

"[…] los usos militares de las novedosas tecnologías asociadas a la robótica, cibernética, sensores remotos, entre otros desarrollos en materia de ciencia y tecnología, han impulsado nuevas formas de librar la guerra que exhiben un salto cualitativo hacia un nuevo paradigma tecnológico. […]
Otro aspecto asociado al nuevo paradigma tecnológico y a las tecnologías de la información es la importancia que está adquiriendo el **ciberespacio** para el desarrollo de las operaciones militares. La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la 'guerra real' y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también el **ciberespacial. Éste no constituye un 'espacio en sí mismo'**, sino una dimensión que atraviesa a dichos espacios físicos, con medios y reglas propias".[57]

Lo resaltado en los párrafos de la DPDN tiene como objetivo efectuar algunas consideraciones que nos permitirán fijar una definición respecto a la naturaleza del ciberespacio, como nuevo espacio en sí mismo; en tal sentido:

- **Terminológicamente**, ha surgido la necesidad de crear una nueva palabra, y sus derivados, para definir al ciberespacio, ya que éste, de facto, se diferencia como un espacio nuevo donde se desarrollan operaciones de defensa y seguridad. La sola denominación de este nuevo espacio lo diferencia de hecho de los tres preexistentes.

- Los **medios** que se emplean en el ciberespacio son de reciente creación y para ser utilizados exclusivamente en este nuevo

[57] Ministerio de Defensa. República Argentina. Decreto 2645/2014. Directiva de Política de Defensa Nacional. Buenos Aires, 30/12/2014.

(*) Coronel (R) "VGM". Oficial de Estado Mayor del EA y del EMCO, licenciado en Estrategia y Organización, magíster en Políticas y Estrategia y doctor en Ciencia Política. Acreditado por la CONEAU como Experto en Ciencia Política. Calificado como Investigador tipo 1 por el SENESCYT (Ecuador). Actualmente se desempeña como profesor titular en la Escuela Superior de Guerra Conjunta y la Escuela de Defensa Nacional. Es miembro del ISIAE-CARI.

espacio. Poseen la particularidad de la cuasi libre disponibilidad y bajo costo, hechos que también lo diferencian de los espacios preexistentes. Pueden ser empleados por individuos aislados o grupos de estados, en simultaneidad y sin diferencias significativas.

- Por **esencia** (lo que hace que algo sea lo que es y no otra cosa), el ciberespacio es un espacio no físico, creado por el hombre a través de su evolución tecnológica, de allí que su naturaleza es, esencialmente, diferente y única, respecto a los otros tres de carácter físico y no creados por el hombre.

- La **materialización del poder** en este nuevo espacio, en nada se asemeja a la que las fuerzas físicas, en potencia o reales, otorgan a los actores en los tres espacios naturales. El alcance del poder proporcionado por los medios ciberespaciales es potencialmente global.

- La **libertad de acción** de los actores en el ciberespacio es de muchísima mayor autonomía, especialmente de los débiles, entre otros aspectos, por la disponibilidad libre de medios y globalización de los conocimientos. En los espacios naturales, las características mismas de los medios los restringen y limitan.

- La **naturaleza de los actores estratégicos** con impacto global es también esencialmente diferente. La aparición de este nuevo espacio permite el surgimiento de actores estaduales o no estaduales interactuando con una lógica fuerte-débil nueva y con alto grado de independencia con respecto a los otros tres: terrestre, marítimo y aeroespacial.

- Los **intereses de los actores estratégicos** en este nuevo espacio, teniendo en cuenta las características de los medios, son de impacto global, aunque se materialicen en un acotado y determinado espacio geográfico (local o regional).

- Las **oportunidades y amenazas** se potencian en este nuevo ambiente en forma generalizada, globalizada y transversal a los actores como nunca se vio en los otros tres espacios, en donde éstas se materializaban en espacios relativamente próximos, salvo para contados actores globales. Con el surgimiento del ciberespacio y la nueva lógica fuerte-débil, su materialización es totalmente diferente.

- El **balance de poder entre actores** en el ciberespacio requiere de herramientas de análisis y gestión que le son propias y diferentes al de los tres espacios naturales. Debe considerarse que, a diferencia de éstos, cuanto mayor sea el desarrollo y uso que del ciberespacio realice un actor, mayores pueden ser las consecuencias de proyección de poder que realice un actor débil. ¡La fortaleza del débil está en su debilidad!

- El **marco legal-normativo** de aplicación en el ciberespacio, en proceso de desarrollo, posee características que le son propias.

Por lo expuesto, se podría decir que cuando en Defensa hablamos de ciberespacio, hablamos de un espacio nuevo y diferente a los otros tres (terrestre, marítimo y aeroespacial) que, además, posee la característica particular de que, siendo creado por el hombre, impacta en los tres espacios naturales.

Debemos ser conscientes que el primer paso para dar soluciones nuevas a problemas nuevos es aprehender lo nuevo.

La lógica de los problemas y sus soluciones difiere de aquella que la antecedió. El criterio con el que los individuos, los Estados y los actores no estaduales interactúan en esta nueva realidad, global y transversal a todas las esferas, sean éstas públicas o privadas, estaduales o no estaduales, externas o internas, requiere aggiornarse[58] al nuevo paradigma que tipifica y distingue a esta nueva era.

[58] Del lunfardo: "actualizarse; ponerse al tanto de noticias, descubrimientos, avances y novedades referidos a una actividad específica o un ambiente determinado. (Del ital. *aggiornare*: poner al día)". Consultado el 20/07/2015, en: CONDE, Oscar, *Diccionario etimológico del lunfardo* https://books.google.com.ar/books?id=rvYQ5Aos3rcC&pg=PT38&lpg=PT38&dq=aggiornarse+diccionario&source=bl&ots=3Pw2hTSAJr&sig=Dn5oLkOoaYB3z3VFbx6jG9GDHX8&hl=es-419&sa=X&ved=0CDkQ6AEwBWoVChMIionw-cr0xgIViQqQCh3N6A8l#v=onepage&q=aggiornarse%20diccionario&f=false

Con la finalidad de simplificar la descripción del ambiente donde se enmarca sistémicamente este nuevo espacio, se podría modelizar a través de un proceso comparativo con un modelo anterior, señalando que nos encontraríamos en un período de inflexión similar al que ocurrió con el surgimiento de la imprenta en la sociedad de la edad media: la lecto-escritura cambió; los tiempos para la adquisición de conocimientos cambiaron; el proceso de adquisición, transformación y transmisión de información-conocimientos cambió la lógica para la toma de decisiones. En síntesis, cambió el mundo ¡y cambió mucho y rápido!, mucho más rápido que en períodos anteriores.

Como gran conclusión podemos decir que si las organizaciones con responsabilidad primaria en una de las funciones indelegables del Estado: la defensa-seguridad, no son rediseñadas, la entropía que se le generará internamente la harán inútiles, cual briosa y valiente, pero inútil, carga de caballería a caballos contra tanque. ¿Nos habremos olvidado de la invasión a Polonia en el ´39?

Ciberagresiones

Como se señaló en el apartado anterior, una de las funciones indelegables del Estado, como actor central que continúa siéndolo en el concierto de las relaciones internacionales, seguirá siendo la cuestión de la defensa-seguridad de quienes forman parte del mismo, y sus recursos.

En este marco normativo básico –siempre modelizando las descripciones como herramienta metodológica de este trabajo– cabría preguntarnos: ¿qué cambió y qué permanece estable desde que Aron, en su obra "Pensar la Guerra", entre otros, diferenció, a partir de constituir ambientes esencialmente distintos, la defensa y la seguridad, y en consecuencia la naturaleza de los medios a ser empleados en ellos?

Inicialmente, se identificará qué características tienen las agresiones-ataques que utiliza el ciberespacio para constituirse, eventualmente, en una amenaza a ser disuadida o repelida, en el marco de la defensa-seguridad, como responsabilidad de un Estado o grupos de Estados.

En el año 2009, el gobierno de EE.UU. convocó al National Research Council para estudiar ciberataques, en ese marco los definió como "acciones deliberadas para alterar, perturbar, engañar, degradar o destruir sistemas de computación o redes o la información y/o programas residentes o en tránsito por estos sistemas o redes".[59]

Esta primera aproximación nos permite extraer algunas conclusiones de las nuevas guerras en este nuevo espacio:

- Los medios a emplear en ciberataques no son esencialmente de carácter cinéticos, como sí lo son en los otros tres espacios. En el ciberespacio éstos son digitales y se desplazan a altísimas velocidades; no reconocen fronteras geográficas, ya que las atraviesan prácticamente sin interdicciones de los Estados; y pueden afectar a múltiples blancos en uno o varios Estados en forma simultánea.

- La afectación de los blancos atacados se realiza a través de los programas que sus ordenadores y redes ejecutan, incluso puede llegar a producir una posible destrucción física. Es el caso del ataque del gusano Stuxnet a la planta nuclear de Bushehr, Irán, en setiembre de 2010, donde se vieron afectados mil de las cinco mil centrifugadoras que posee la planta[60].

- Identificar a los actores y autores de los ataques se dificulta sensiblemente, esto es así porque tanto las redes y ordenadores, como los autores intelectuales de los virus se han globalizado. Este hecho se potencia porque una determinada red puede ser infectada y utilizada para incrementar el efecto de agresión buscado sin que su usuario sea partícipe de dicha decisión. El ataque a Estonia, en abril de 2007, es un ejemplo de ello.

El ciberataque a Estonia, uno de los más estudiados dentro de esta nueva tipología de ataques a Estados, nos permite citar hechos que corroboran las conclusiones efectuadas precedentemente:

---

[59] Singer, Peter Warren y Friedman, Allan, *Cybersecurity and Cyberwar*. New York, Oxford University Press, 2014, pág.68.

[60] Según algunos, como Snowden, marcó el nacimiento de la ciberguerra. Ver más en: http://www.qore.com/articulos/6560/Stuxnet-y-el-nacimiento-de-la-ciberguerra#sthash.FHceJl6s.dpuf

"[…] los atacantes, debido a la cooperación internacional, vieron que sus botnets[61] estaban siendo anuladas movieron sus redes a jurisdicciones con menos o ninguna disposición o capacidad a cooperar, es decir movían sus elementos de ataque a 'paraísos legales cibernéticos', como Egipto, Vietnam o Perú".[62]

"Fuimos atacados por 178 países, señaló Katrin Pargmae, portavoz del Centro de Informática de Estonia […]".[63]

La particularidad que se presenta en el análisis y evaluación de hechos como éste, efectuado desde el ámbito de la defensa de la Argentina, radica en que poseemos dos marcos legales que diferencian con leyes, cuasi excluyentes una de la otra, a la Seguridad Interior (sancionada en 1991) de la Defensa Nacional (sancionada en 1988). La reglamentación de la Ley de Defensa Nacional, efectuada a través del Decreto 727, del año 2006, ratificó y acotó el origen de los hechos a los que el sistema de defensa debe hacer frente, en particular aquellos que sean realizados por fuerzas que revistan el carácter de externo, estadual y militar.

En este marco normativo básico, el Presidente de la Nación emitió dos Directivas Políticas de Defensa Nacional (DPDN), la primera de ellas a través del Decreto N° 1714, del 10 de noviembre de 2009, y su actualización a través del Decreto 2645, del 30 de diciembre de 2014. En este último se señala:

"[…] Si bien las acciones de ciberguerra poseen su origen en el ámbito virtual de las redes de comunicación y sistemas informáticos, sus efectos impactan sobre el mundo físico, pudiendo afectar, por ejemplo, el tráfico aéreo y terrestre, el control de las infraestructuras críticas, el abastecimiento energético y de agua potable, entre otros. Dentro de la amplia gama de operaciones cibernéticas, sólo una porción de éstas afectan específicamente el ámbito de la Defensa Nacional. En efecto, en materia de ciberdefensa existen dificultades fácticas manifiestas para determinar a priori y ab initio si la afectación se trata de una agresión militar estatal externa. Por tal motivo, resulta necesario establecer dicha calificación a posteriori actuando como respuesta inmediata el Sistema de Defensa únicamente en aquellos casos que se persiguieron objetivos bajo protección de dicho sistema, es decir que poseen la intención de alterar e impedir el funcionamiento de sus capacidades".

De su lectura podríamos inicialmente preguntarnos: ¿toda infraestructura catalogada como crítica para el funcionamiento del Estado no debería estar protegida por el Sistema de Defensa? El conocimiento que hoy tenemos de casos como el de Estonia y las consecuencias que trajo para dicho Estado, así como para la OTAN, organización de la que es miembro, nos deben permitir definir los límites al empleo del propio Sistema, a fin de que éste diseñe y desarrolle capacidades para estar en aptitud de hacer frente a las guerras futuras y no a las pasadas.

Si bien este trabajo no es un estudio de casos, debemos señalar que existió otro suceso paradigmático: los ciberataques a Georgia, en el marco del conflicto con Rusia y Osetia del Sur, entre junio y agosto de 2008. En este episodio, dichos ataques, coordinados con operaciones militares clásicas llevadas a cabo por fuerzas rusas, permitieron debilitar el proceso de toma de decisiones político y militar, afectaron el suministro de servicios básicos y la comunicación con los ciudadanos. "Como en el caso Estonia, la participación del gobierno ruso no ha sido probada" (Ganuza Artiles, Néstor, p. 202).

Ante un eventual ciberataque, ¿podrá el Sistema de Defensa argentino identificar que la agresión puede ser de carácter militar estatal externa?; parecería difícil y quizás lo más peligroso será el tiempo de respuesta que el mismo puede requerir hasta tanto se lo califique como tal. En los casos mencionados es sabido que pese al apoyo internacional que recibieron Estonia y Georgia, los efectos fueron significativos para todo el Estado.

---

[61] "El término *bot* es el diminutivo de robot. Los delincuentes distribuyen software malintencionado (también conocido como *malware*) que puede convertir su equipo en un *bot* (también conocido como zombie). Cuando esto sucede, su equipo puede realizar tareas automatizadas a través de Internet sin que lo sepa. Los delincuentes suelen usar *bots* para infectar una gran cantidad de equipos. Estos equipos crean una red, también conocida como *botnet*. Los delincuentes usan *botnet* para enviar mensajes de correo electrónico no deseados, propagar virus, atacar equipos y servidores y cometer otros tipos de delitos y fraudes. Si su equipo forma parte de una *botnet*, el equipo puede volverse más lento y puede estar ayudando a los delincuentes sin darse cuenta". Consultado en: https://www.microsoft.com/es-es/security/resources/botnet-whatis.aspx

[62] Ganuza Artiles, Néstor, "La situación de la ciberseguridad en el ámbito internacional y en la OTAN", Universidad de La Rioja (España), *Cuadernos de estrategia,* N° 149, 2011, pág. 192.

[63] Consultado el 15/06/2015 en: http://balticbusinessnews.com/?PublicationId=b737410e-e519-4a36-885f-85b183cc3478

¿Qué se entiende como infraestructura crítica?, ¿qué cuestiones concretas incluye? El Consejo de la Unión Europea determinó en el año 2008, que "se entenderá por infraestructura crítica: elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones".[64]

En dicho marco supra estadual, España, a través de la sanción de la Ley 8/2011 de Protección de Infraestructuras Críticas (LPIC) y el posterior Real Decreto 704/2011[65] difundió el Reglamento de Protección de las Infraestructuras Críticas que, entre otras disposiciones, creó la Comisión Nacional para la Protección de las Infraestructuras Críticas a las que clasificó en doce sectores estratégicos, a saber:

- Administración
- Alimentación
- Energía
- Espacio
- Sistema Financiero y Tributario
- Agua
- Industria Nuclear
- Industria Química
- Instalaciones de Investigación
- Salud
- Tecnologías de la Información y las Comunicaciones
- Transporte

Esta clasificación nos permite inferir la complejidad de las operaciones necesarias para mantener el control de las mismas, tal como lo indica la DPDN 2014. También, debe señalarse que en su planeamiento surgirán los supuestos a partir de los cuales los planes a elaborar deberán permitir hacerle frente; es decir las misiones impuestas y deducidas, con responsabilidades primarias y secundarias; tiempos kronos y tiempos kairós para ejecutar acciones y coordinaciones para la protección de objetivos por parte de otros Sistemas distintos al de Defensa, etc.

La Argentina ha creado, a partir de la Resolución 580/2011, del 28 de julio de 2011, de la Jefatura de Gabinete de Ministros, el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad que se desarrolla en el ámbito de la Oficina Nacional de Tecnologías de Información dependiente de la Subsecretaria de Tecnologías de Gestión.

Complementando lo aquí expresado, debe destacarse que hay algunos consensos académicos, no absolutos ni protocolizados, para identificar diferentes grados y tipologías de acciones que haciendo uso del ciberespacio afectan a equipos y sistemas. En la publicación "*Los ámbitos terrestres en la guerra futura: ciberespacio"*[66], se efectuó una clasificación de las eventuales acciones hostiles, amenazas o agresiones que utilizan el ciberespacio, conceptos que actualizados son los siguientes:

- **Cibercrimen**: utilización del ciberespacio por parte de individuos o grupos no estaduales (a los que se denominan crackers, para diferenciarlos de los hackers), para cometer actos ilícitos en beneficio propio; en general estas acciones son reconocidas como delitos y de incumbencia policial. Por ejemplo: suplantación de identidad para acceder a cuentas bancarias.

- **Ciberterrorismo**: uso del ciberespacio por parte de individuos, grupos no estaduales y/o Estados, que buscan efectos sobre la psiquis global del blanco, los que pueden ser grupos de individuos, empresas e incluso Estados. Los instrumentos legales y medios materiales para hacer frente a estas acciones variarán según sea el Estado considerado.

- **Ciberguerra**: empleo del ciberespacio, generalmente junto al empleo de capacidades cinéticas tradicionales, normalmente por parte de un Estado o grupo de Estados que atacan la estructura

[64] Consejo de la Unión Europea. Directiva 2008/114/CE sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. 8 de diciembre de 2008. http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&type_doc=Directive&an_doc=2008&nu_doc=114&lg=es
Consulta: 30 septiembre 2011

[65] Boletín Oficial del Estado, 21/05/2011. Consultado en: http://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf.

[66] Flores, Héctor, *Los ámbitos no terrestres en la guerra futura: ciberespacio*, Madrid, CESDEN, 2011, pág. 12

funcional y/o decisional de otro u otros Estados u organismos no estaduales. Esta tipología sería aplicable al concepto de agresión establecido por la ONU (Resolución 3314, del 14 de diciembre de 1974), el que fue retenido como tal por el Decreto 727/2006 que reglamentó la Ley de Defensa Nacional de la Argentina.

Sólo a manera de ejemplo de la magnitud que estos hechos tienen en la lógica del siglo XXI, citaremos a Sergi Gil, responsable de CyberSOC Academy Deloitte, quien señala que "el cibercrimen mueve más dinero que el narcotráfico, el contrabando de armas y la prostitución; por eso las mafias no se quieren quedar atrás y lo que hacen es contratar a gente que se dedique exclusivamente a hacer ataques. Antes lo que hacían era tirar el virus en Internet y esperar la pesca de algún incauto. Pero hoy eso ha cambiado, y el 95% de los ataques es dirigido, es decir, que se ataca a una persona o una empresa con un objetivo muy concreto".[67]

También podemos citar a Adolfo Hernández, subdirector de THIBER (The Cybersecurity Think Tank), una organización que mensualmente difunde los principales hechos de operaciones cibercriminales; quien difundió que, entre los eventos de abril de 2015, "la aerolínea irlandesa de bajo coste Ryanair confirmó que unos 4,5 millones de € fueron extraídos fraudulentamente de una de sus cuentas bancarias a través de una operación efectuada desde un banco chino".[68]

Dentro de las acciones ofensivas propias del ciberterrorismo y la ciberguerra podríamos identificar algunas de las siguientes:

- Ataque de denegación de servicios (DoS). El mismo buscaría afectar fundamentalmente servicios básicos (luz, agua, salud, seguridad, bancarios, etc.) o infraestructura crítica en general. En el caso de Estonia, según algunos estudios, se produjeron alrededor de ciento veintiocho ataques de este tipo entre el 3 y el 11 de mayo de 2007.

- Ataques de desfiguración de sitios web (web site defacement). Este tipo de agresión tendría por finalidad modificar clandestinamente la presentación-visual del sitio a fin de llevar a engaño a usuarios. En Estonia se llevaron a cabo este tipo de ataques a páginas oficiales y personales de las máximas autoridades políticas.

- Ataques a servidores de sistemas de nombres de dominio. Estos tienen por finalidad poder redireccionar las capacidades de los equipos y redes que integran. Este tipo de acciones encubre a los autores y actores de eventuales ataques, tal y como ocurrió en Estonia y Georgia.

- Envío masivo de correo basura (spam). A través de estos envíos se busca recargar y paralizar las redes, las direcciones oficiales gubernamentales y las direcciones privadas de autoridades gubernamentales, tal como sucedió en Estonia.

En esta clasificación propuesta encontramos que una potencia militar global como los EE.UU., a través del documento DoD Cyber Strategy, difundido en abril del 2015 y que estará vigente hasta el 2018, señala expresamente que en los conflictos futuros deben "ser capaz de utilizar las ciberoperaciones para disrumpir[69] las redes de mando y control, infraestructuras críticas y sistemas de armas de los potenciales adversarios del país".[70]

Una vez más podemos observar que las infraestructuras críticas, más allá de las redes de mando y control propias del Sistema de Defensa del enemigo, son blancos reconocidos como tales en las guerras del siglo XXI. La fuerza cinética que utiliza el ciberespacio, como si fuera una bomba lanzada desde el aeroespacio, busca efectos violentos que podrían llegar a la destrucción del blanco a través de medios digitales.

Dicha irrupción es disruptiva, porque una de las características de los medios cibernéticos lo constituye la velocidad de los mismos, muy superior a la de los medios cinéticos y, tal como se ha señalado, se desplaza sin restricciones geográficas ni fronteras políticas.

---

[67] Consultado en: http://www.lanacion.com.ar/1813403-los-sherlock-holmes-del-siglo-xxi-trabajan-en-el-ciberespacio

[68] Consultado en: Ciber Elcano N° 3, "Análisis de los ciberataques". Madrid, mayo 2015, pág. 21.

[69] Interrumpir bruscamente; entrar violentamente a un lugar.

[70] Fojón Chamorro, Enrique, "La nueva estrategia ciber del Pentágono: innovar y potenciar la industria", en http://www.blog.rielcano.org/, 27/04/2015.

En general, los ataques disruptivos a través del ciberespacio afectan los datos disponibles en equipos y sistemas que archivan información e inteligencia propia para el funcionamiento de los mismos. En tal sentido, se debería poseer la capacidad de asegurar que la que sea de carácter sensible pueda ser preservada de una difusión no deseada aplicándole el principio de "necesidad de saber-confidencialidad"; debe poder ser empleada en oportunidad, al aplicar el principio de "oportunidad-disponibilidad"; y debe permitir el uso integral de la misma.

Al efectuar la evaluación de la disrupción, se debería poder determinar si fue un hacker, un cracker, un terrorista o el uso de fuerza por parte de un Estado o grupo de Estados. En tal sentido, el primer parámetro a considerar podría ser a través de sopesar el grado de daño provocado a fin de reaccionar bajo el criterio de proporcionalidad que determina la lógica del Derecho Internacional y el derecho positivo interno de los Estados en general.

Resulta interesante destacar que el efecto de destrucción a largo plazo, alcanzado hasta el presente por los medios cibernéticos es, en general, de mucho menor impacto y perdurabilidad que el uso de armas cinéticas, en especial de las nucleares. Por otro lado, los denominados efectos secundarios o bajas no deseadas también serían menores. Un aspecto que se encuentra en pleno proceso de evolución es poder direccionar puntualmente los efectos de un ciberataque. Actualmente, el eventual radio de acción de un virus-malware no es menos predecible que el de un proyectil cinético, aunque Stuxnet está señalando una mayor factibilidad de hacerlo.

Finalmente, y teniendo en cuenta que el artículo 2º de la Ley de Defensa Nacional prevé el empleo de las FF.AA., en forma efectiva o disuasiva, es en el ciberespacio en donde aplicar el concepto de disuasión resulta prácticamente nulo contra grupos no estatales o actores débiles, con escaza utilización de este espacio para su gestión interna, mientras que, "por supuesto, son los mayores jugadores en el ciberespacio" (Singer, p. 136); un aspecto más a considerar en la complejidad del planeamiento estratégico.

Ciberorganizaciones militares

A fin de contribuir en la difusión de aspectos organizacionales que, dentro del Sistema de Defensa de los Estados más avanzados en esta problemática, pudieran servir para identificar lo que Mintzberg señala como las partes de las organizaciones, se efectúan unas breves descripciones sobre algunos de los aspectos más trascendentes que caracterizan al Ciber Comando (CYBERCOM) de los EE.UU. Cabe destacar que el mismo "reúne todos los componentes militares de los EE.UU. que trabajan en cuestiones ciber, desde el Ninth Signal Command del Ejército hasta el Tenth Fleet de la Armada (el Comando Cibernético de la Flota). En total, la organización tiene una fuerza de ciber guerreros de un poco menos de 60.000 personas, con su comando localizado en Fort Meade, Maryland" (Singer, p. 134).

En el modelo de referencia, el general Keith Alexander fue designado Director de la NSA (Agencia Nacional de Seguridad) y, a su vez, Comandante del CYBERCOM. Este criterio fue objetado por algunos, mientras otros vieron esta dualidad como algo natural al considerar que ambas organizaciones poseen responsabilidades afines. Las críticas se fundamentaron, principalmente, en la preocupación que en algunos provoca el desdibujamiento de los límites entre lo interno y externo, como el que se produjo en los EE.UU. como consecuencia del ataque del 11 de septiembre de 2001.

En término simples y modelizados, podríamos decir que el CYBERCOM es un comando militar con las particularidades del nuevo espacio donde debe interactuar, mientras que la NSA se asemeja más a un organismo civil de inteligencia del Estado. En este orden de ideas, el soldado del futuro del CYBERCOM sigue llevando a cabo un combate abierto con ciertas particularidades o zonas grises aún no cubiertas o definidas claramente por las leyes que hoy enmarcan los conflictos armados (Derecho Internacional de los Conflictos Armados – DICA); en tanto que los integrantes de la NSA desarrollan sus actividades de inteligencia (obtener) y contrainteligencia (negar) por similitud a lo que hacía un espía del siglo XX.

El planeamiento público difundido por el CYBERCOM[71] permite observar que se centra en cinco objetivos:

[71] Consultado en: http://www.defense.gov/home/features/2015/0415_cyber-strategy/

- Tratar el ciberespacio como un dominio ("domain") operacional, como la tierra, el aire o el mar.

- Implementar nuevos conceptos de seguridad para tener éxito en ciberespacio.

- Colaborar con otras agencias y el sector privado.

- Construir relaciones con los socios internacionales.

- Desarrollar nuevos talentos para impulsar innovaciones en cómo el ejército puede luchar y ganar en este espacio.

La cibermisión principal del Departamento de Defensa (DoD) es:

- Defender las redes, sistemas e información del DoD.

- Defender el territorio de los EE.UU. y sus intereses nacionales contra ataques cibernéticos de importancia significativa.

- Proporcionar apoyo cibernético a los planes operativos y de contingencia militar.

Como parte de su misión, CYBERCOM está organizado en cuatro tipos de fuerzas:

- National Mission Teams: defenderán a los EE.UU. y sus intereses contra ciberataques de significativas consecuencias.

- Cyber Protection Teams: defenderán prioritariamente las redes y sistemas del Departamento de Defensa y ordenadores militares propios.

- Combat Mission Teams: apoyarán la misión de las tropas en el terreno, mediante la generación de efectos ciberespaciales integrados en apoyo de los planes operativos y las operaciones de contingencia.

- Support Teams: proporcionarán apoyo a la planificación de la Fuerza con misiones nacionales y la Fuerza con misiones de combate

Diseño de capacidades de defensa aplicables en el ciberespacio

La misión principal del Sistema de Defensa argentino es el criterio ordenador para el diseño de capacidades de defensa aplicables en el ciberespacio, lo corrobora la DPDN 2014 cuando señala:

"La Misión Principal asignada al Instrumento Militar (IM) consistente en asegurar la Defensa Nacional ante agresiones de origen externo perpetradas por Fuerzas Armadas pertenecientes a otros Estados constituye el criterio central y principio ordenador de su diseño, organización y funcionamiento. Se entenderá como 'agresión de origen externo' el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de nuestro país o en cualquier forma que sea incompatible con lo establecido por la Carta de la Organización de las Naciones Unidas (ONU)".

"[…] d) el desarrollo de capacidades operacionales en la dimensión ciberespacial con el objeto de adquirir competencias en los ambientes terrestre, naval y aéreo, así como de ciberseguridad de redes pertenecientes al Sistema de Defensa Nacional y respecto de los objetivos de valor estratégico que oportunamente sean definidos por el Nivel Estratégico Nacional".

Cabría ahora preguntarnos: ¿quién relacionaría los objetivos de valor estratégico que deberían estar bajo protección del Sistema de Defensa y el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, creado en el año 2011, encargado de diseñar y emplear los medios y capacidades para su seguridad? La respuesta la encontramos en la Directiva Política de Defensa Nacional 2014:

"9) El Ministerio de Defensa elaborará las normas para la creación de una instancia de naturaleza operacional en materia de Ciberdefensa, de acuerdo a lo previsto en el Plan de Capacidades Militares (PLANCAMIL 2011)".

En tal sentido, se conformó el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas, que es de naturaleza conjunta y depende del Estado Mayor Conjunto de las FF.AA. Posteriormente, la Decisión Administrativa 15/2015, publicada en el Boletín Oficial (BO) el 11/03/2015, creó, a su vez, la nueva

Dirección General de Ciberdefensa, cuyas misiones son:

1) Asistir en el planeamiento, diseño y elaboración de la política de ciberdefensa de acuerdo a lo establecido en el Ciclo de Planeamiento de la Defensa Nacional en coordinación con la Subsecretaría de Planeamiento Estratégico y Política Militar.

2) Entender en la coordinación con los organismos y autoridades de los distintos poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica.

3) Intervenir en la orientación, dirección y supervisión de las acciones en materia de ciberdefensa ejecutadas por el Nivel Estratégico Militar.

4) Ejercer el control funcional sobre el Comando Conjunto de Ciberdefensa de las FF.AA.

5) Intervenir en la evaluación y aprobación de los planes militares de desarrollo de capacidades de ciberdefensa, en la doctrina básica y en las publicaciones militares pertinentes, cualquiera sea su naturaleza.

6) Intervenir en el diseño de políticas, normas y procedimientos destinados a garantizar la seguridad de la información y a coordinar e integrar los centros de respuesta ante emergencias teleinformáticas.

7) Fomentar políticas de convocatoria, captación, incentivo y formación de recursos humanos para la ciberdefensa para mantener un plantel adecuado.

8) Promover vínculos sistemáticos de intercambio y cooperación en materia de ciberdefensa con los ámbitos académico, científico y empresarial.

9) Impulsar acuerdos de cooperación e intercambio en materia de investigación y asistencia técnica en ciberdefensa con organismos públicos y privados.

10) Asistir en el desarrollo doctrinario, en el diseño y fortalecimiento de capacidades y en la elaboración de la estrategia de ciberdefensa de conformidad a los lineamientos del Ciclo de Planeamiento de la Defensa Nacional.

La medida lleva la firma del jefe de Gabinete, Aníbal Fernández, y el ministro de Defensa, Agustín Rossi. "En función del marco normativo y doctrinario del Sistema de Defensa Nacional de la REPÚBLICA ARGENTINA, se entenderá por 'Ciberdefensa' a las acciones y capacidades desarrolladas por el IM en la dimensión ciberespacial de carácter transversal a los ambientes operacionales terrestre, naval y aéreo" (DPDN, 2014).

Sin lugar a dudas el ciberespacio es transversal a los otros espacios. Asimismo, las organizaciones que diseñe el IM deberán estar en capacidad de contribuir al cumplimiento de la misión principal del Sistema de Defensa; en tal sentido deberán ser empleados en forma efectiva o disuasiva.

Ya se han tratado, parcialmente, las restricciones que el empleo disuasivo tiene en el ciberespacio.

El concepto disuasivo nuclear, especialmente el de destrucción mutua asegurada[72] (DMA), busca alterar los cálculos de costo-beneficio para tender a la paz por el terror, que el empleo de los medios podría provocar. Otros conceptos disuasivos convencionales tales como: la Disuasión por Negación, por Conocimiento, No Provocativa o por el criterio de Puerta Giratoria, tienen como condición sine qua non saber a quién está dirigida, siendo la opinión del autor que no podrían ser de aplicación en el ciberespacio porque, fundamentalmente, como se ha señalado, en su diseño y posterior instrumentación habría que poder identificar claramente quién es el agresor eventual o real, y si los equipos, redes o sistemas que agreden al actor pertenecen al agresor o no. La naturaleza no física de las "ciber armas-malware" dificulta, sensiblemente, asignarle la atribución a una acción.

[72] La destrucción mutua asegurada (en inglés *mutual assured destruction* o MAD) es la doctrina concebida por John von Neumann de una situación en la cual cualquier uso de armamento nuclear por cualquiera de dos bandos opuestos podría resultar en la completa destrucción de ambos (atacante y defensor). Consultado en http://www.diclib.com/Destrucci%c3%b3n%20mutua%20asegurada/show/es/es_wiki_10/12879#ixzz3kPyehWDL

En el proceso de planeamiento de diseño se debe poder evaluar a las eventuales amenazas, especialmente en lo referido a la factibilidad de que éstas sean capaces de identificar y explotar las propias debilidades transformándolas en vulnerabilidades, determinando los posibles efectos a provocar, así como la voluntad del actor de materializar la amenaza. En este proceso, la evaluación de riesgos, así como la definición del peor escenario, es extremadamente compleja si no hay una reducción del flujo de la variedad[73] a través de la imposición de Objetivos Estratégicos por parte del Poder Ejecutivo Nacional que dé respuesta al interrogante "cómo", si es que no puede hacerlo al interrogante básico "quién".

En este marco, Argentina está en el puesto número 38 en el ranking de Estados más atacados, según el Cyberthreat Real-Time Map. Este hecho debería contribuir a permitirnos reducir el flujo de variedad.

El proceso de planeamiento, por el criterio de capacidades vigente, en su instrumentación por incertidumbre (sin hipótesis de conflicto), es la vía a través de la cual se debería poder aproximar una respuesta al cumplimiento de la misión principal en el ciberespacio. Ahora bien, no saber si se deberá estar en aptitud de hacerlo desde la lógica del fuerte o del débil tendrá un impacto mucho mayor que el que tiene en los otros espacios naturales. Por otra parte, según la opinión del autor, se podría orientar dicha reducción del flujo de la variedad sin llegar a definir contra quién (modelo de hipótesis de conflicto prevista en la Ley de Defensa) tal y como lo describió en el párrafo anterior, sustentado en el marco legal vigente que señala:

"c) Cuando las 'capacidades' que sean pertinentes poseer para enfrentar las formas genéricas de agresión que exige la Defensa Nacional carezcan de una demanda cuantitativamente objetiva, para el diseño de tales "capacidades" se apelará a la pauta de 'capacidad suficiente'. Por 'capacidad suficiente' debe entenderse al desarrollo de una 'fuerza activa sustancial' (mínima organización que en forma sistémica posee todos los atributos que le permiten desarrollar de manera autónoma todas las operaciones inherentes a la potencialidad de que se trate) con aptitud de expandirse o adecuarse según los requerimientos de respuesta operacional que se le presenten".[74]

Finalmente, hay actores que, como los EE.UU., han definido cual consideran que hoy constituye su mayor amenaza: "China […] es el más amenazante actor en el ciberespacio" (Singer, p. 138), esta sería una información relevante si lo relacionamos con la estación espacial de observación que dicho Estado está construyendo en nuestra Patagonia.

La lógica del fuerte y el débil en el ciberespacio

Mike Mc Connell, director de Inteligencia Nacional de los EE.UU., entre 2007 y 2009, testificó ante el Senado de ese país que "si la nación fuera a la guerra hoy, en una ciberguerra, nosotros perderíamos. Nosotros somos más vulnerables. Nosotros somos los más conectados. Nosotros tenemos mucho más que perder" (Singer, p. 151).

Esta afirmación se basa en que eventuales agresores, como Corea del Norte o el Estado Islámico, son sociedades y Estados que aún no ingresaron a la era de la información a pleno. Este hecho hace que el ciberespacio proporcione un criterio igualador de capacidades que los espacios naturales no proporcionan.

Como señalan Singer y Friedman, quien también corroboró esta afirmación fue el Jefe de la Inteligencia Militar de Israel al señalar que:

> *"…el ciberespacio proporciona a los pequeños países e individuos un poder que hasta ahora era preservado para los Estados grandes… creando "una extraña ironía de ciberguerra... Las naciones más hábiles en lanzamientos de cohetes viven en las grandes casas de cristal… (y los) grupos no estatales y Estados más débiles pueden ciertamente jugar ahora en el juego que estaba fuera de su alcance. Pero eso no significa que ellos tengan los mismos recursos para hacerse valer en él… pese a ello, Joseph Nye, ex funcionario del Pentágono y decano de la Harvard Kennedy*

[73] Respecto a la teoría en que se sustenta la reducción del flujo de la variedad puede consultarse el artículo: Flores, Héctor Rodolfo, "La sistemática del planeamiento estratégico militar sin hipótesis de conflicto y el control civil objetivo de las FFAA: caso argentino", en Revista Peruana de Ciencia Política, Vol. 1, Lima, 2012.pág. 9.

[74] República Argentina. Decreto 1691/2006 - Directiva sobre Organización y Funcionamiento de las Fuerzas Armadas. Buenos Aires, 22/11/2006 - B.O. 29/11/2006

> *School señaló: 'pero los perros pequeños muerden"* (Singer p. 151-2).

Esto es así porque, desde la lógica del débil, éstos pueden constituir ciber amenazas reales pero restringidas, ya que el desarrollo de gusanos como el Stuxnet requiere de capacidades que exceden a pequeños grupos o aquellos que carecen de fuertes centros de pensamientos.

Por similitud a períodos anteriores, la lógica del fuerte en el ciberespacio posee una característica común con sus predecesores: es él quien puede administrar el dominio de la escalada. Este concepto relaciona la capacidad de ciberdisuasión que poseen los actores fuertes para coordinarla, con las capacidades muy superiores que poseen en los otros espacios, en los cuales la lógica del fuerte y el débil continúan siendo las propias del balance de poder que por siglos rigió las relaciones entre Estados.

Un aspecto no menor en la nueva lógica del débil que se plantea, se refiere a que sus acciones en el ciberespacio, difíciles de identificar previamente y de incidir con represalias duras, proporcionan ventajas significativas al actor débil, de allí que las acciones ofensivas de éstos sobre blancos de interés crezcan a medida que transcurre el tiempo, aunque las mismas puedan realizarse sin utilizar conocimientos de punta que requerirían grandes esfuerzos de investigación. En sentido inverso, diseñar e instrumentar medidas defensivas, las que normalmente van a la zaga de las ofensivas, son en general más costosas.

"El Director de la Defense Advanced Research Project Agency (DARPA) señaló que 'las ciberdefensas han crecido exponencialmente en esfuerzo y complejidad, pero continúan siendo derrotadas por ataques que requieren mucho menos investigación por parte de los atacantes" (Singer, p. 154).

En la actualidad hay, indiscutiblemente, crecientes índices de ciberproliferación, tanto Estadual como no Estadual, público como privado; pese a ello, son pocos los Estados que poseen desarrollos propios avanzados aplicables en casos de ciberguerra.

Como se señaló, el impacto de acciones individuales tienden a ser menores en cuanto al conocimiento que emplean, ya que el desarrollo de eficientes malware normalmente requieren la cooperación de muchos expertos, especializados en variadas áreas pero no necesariamente son menores en cuanto al impacto que generan. Individuos aislados o pequeños grupos pueden potencialmente generar enormes consecuencias, y en él el hombre sigue siendo el escalón más débil de la cadena: Snowden es una muestra de ello.

El surgimiento de un mercado negro de creación y distribución de todo tipo de software, la mayoría de los cuales son plagios o no respetan los derechos de autor, entre los cuales los virus no están ajenos, constituye un nuevo tipo de mercado de cibercapacidades, que hacen de esta ciberproliferación una situación constante y preocupante para la seguridad.

Lo descripto en el párrafo anterior es también consecuencia de una característica tipificante del ciberespacio; en general, una vez que un determinado conocimiento es aplicado, en muy breve lapso de tiempo actores Estaduales y no Estaduales los duplican y difunden a un muy bajo costo en relación a los de su proceso investigativo, ejemplo de ello es lo ocurrido con el virus Stuxnet. En este orden de ideas, también podemos señalar que el tiempo para que se produzca el proceso descripto es mucho menor al requerido para las armas cinéticas en general y con menores posibilidades de control que el de las armas nucleares.

¿Una nueva visión de agresión y combatiente?

Si bien no es el motivo central de este artículo, de todos modos deseo dejar presentado dos problemas básicos referidos a la jurisprudencia de aplicación en la ciberdefensa por parte del sistema de defensa argentino:

El primero de ellos se refiere a poder determinar cuando estamos frente a una agresión que justifique el empleo de la fuerzas por parte del Estado agredido, en los término prescriptos por la ONU. Soy de opinión que nuestro marco normativo, apoyado en el Derecho Internacional no avanzó en la medida que el conocimiento lo ha hecho; al respecto cito lo que la publicación conjunta PC 00-02 define como Casus Belli:

"Término diplomático que indica que unas negociaciones o tensiones no sólo no han sido resueltas sino que se han enconado, no quedando otra solución que acudir a las armas para dirimir la

cuestión. Asimismo significa amenaza, acción u ofensa recibida que, por su alcance e importancia, es capaz de desencadenar un conflicto armado".[75]

El segundo de ellos es el referido al estatus de combatiente; el mismo refiere a:

"Todo miembro de las Fuerzas Armadas, excepto el personal sanitario y religioso. También los habitantes de un territorio no ocupado que, al acercarse el enemigo, tomen espontáneamente y en masa las armas para combatir contra las tropas invasoras sin haber tenido tiempo para constituirse en Fuerzas Armadas regulares; los mismos serán considerados como combatientes si llevan las armas a la vista y respetan el derecho de la guerra".[76]

En ambos casos, dichos conceptos vigentes en el Derecho Internacional considero que deben ser redefinidos producto de haberse producido una asincronía entre la realidad y la norma que la regula.

Conclusiones

Los desarrollos tecnológicos han impactado históricamente en los espacios en donde la seguridad y las relaciones entre los actores estratégicos interactuaban y dirimían sus espacios de poder, entendido éste como la capacidad de proyección del mismo por parte de un actor sobre otro.

En sus inicios el espacio terrestre fue donde se dirimió el poder, posteriormente se incorporó el marítimo y finalmente fue el aeroespacial, ya en el siglo XX. Hoy el ciberespacio surge como un nuevo espacio, creado por el hombre, de carácter transversal a los naturales preexistentes.

Ratifico mí postura respecto a que el ciberespacio constituye un nuevo espacio, diferente de los tres preexistentes y naturales (terrestre, marítimo y aeroespacial), fundamento la misma en al menos los siguientes criterios corroboradores:

- Su esencia es no cinética[77], lo que lo hace por naturaleza diferente a los otros tres.
- El poder y la libertad de acción en este espacio pueden ser independientes y autónomos del que se posea en los otros tres.
- Los intereses y amenazas de los actores pueden ser independientes de los otros espacios.
- El diseño de los medios y su empleo en el ciberespacio es de una especificidad que le es propio.
- La naturaleza de los actores que impactan en el mismo son diferentes, ya que pueden serlo desde un individuo, a organismos no Estaduales, Estados o un grupo de Estados.
- Los mecanismos de balance de poder entre actores son específicos de este ámbito.
- Permite aplicar una lógica propia y diferente a la geoespacial en la relación entre actores fuertes y débiles.
- Las reglas de juego o marco normativo, que se aplican en el mismo le son propias

Por último, este espacio nuevo plantea a los actores Estaduales la oportunidad de dinamizar, potenciar y consolidar sus industrias a partir del desarrollo de nichos de modernidad en ciberseguridad. Por otra parte, sólo así el Sistema de Defensa podría disponer de las capacidades necesarias (fortaleza) para mantener una cierta autonomía en el ciberespacio.

[75] EMCO. PC 00-02. Buenos Aires, 2010, p. C 7-43
[76] Ibídem p. C 23-43
[77] Cinética: energía que poseen los cuerpos en movimiento.

CARI/ Instituto de Seguridad Internacional y Asuntos Estratégicos

ESTIMADO LECTOR

Si desea suscribirse a esta publicación, lo invitamos a solicitarlo a la dirección difusionrdnisiae@gmail.com

Cordialmente,

Equipo de Redacción del RDN ISIAE

DEAR READER

If you want to subscribe to this publication, we invite you to send your request to difusionrdnisiae@gmail.com

Yours faithfully,

RDN ISIAE Editorial staff

ESTIMADO LEITOR

Se você deseja se inscrever a esta publicação, o convidamos a nos enviar a solicitação a difusionrdnisiae@gmail.com

Cordialmente,

O equipe editorial do RDN ISIAE

CARI

Consejo Argentino para las Relaciones Internacionales