VI Congreso de Relaciones Internacionales
21, 22 y 23 de noviembre de 2012

Defensa cibernética en América del Sur. Estrategias en la UNASUR ante ciberguerra y ciberdelito

Celia Romina Brúculo
Alejandro Gustavo Venczel

Resumen

Los desafíos que impulsa el alto crecimiento de las TICs en el mundo en general, y en la región latinoamericana en particular, trae consigo una complejización del sistema de seguridad y de los dispositivos que deban regular ese campo. Si bien cuando a primera vista el caso del cibercrimen, aparece como un área que se ve menos proclive a la regulación y a la capacidad de control y filtro por parte de los Estados, su importancia y versatilidad han producido la necesidad de contar con menos zonas grises de las que *a priori* presupone su naturaleza, por un mayor seguimiento y búsqueda de regulaciones que permitan volver más previsible sus aplicaciones. En ese marco se analizan las condiciones y estrategias de los países de la UNASUR, como el tratamiento regional en materia de defensa cibernética, siguiendo de cerca las políticas y legislación vigentes para hacer frente a las amenazas del cibercrimen, asumiendo que las características de transnacionalidad del espacio cibernético apuntan a las articulaciones regionales.

Introducción

En la actualidad el mundo se encuentra ligado a una alta dependencia de las tecnologías informáticas. Esto es así, ya que las mismas proporcionan un aumento en la eficiencia en materia organizacional y permite disminuir de forma considerable los costos operativos. Asimismo, en las últimas décadas, las organizaciones gubernamentales de todos los países del globo han confiado en las herramientas informáticas como facilitadoras y superadoras de algunas deficiencias administrativas.

En este sentido, el campo cibernético se ha posicionado como base de almacenamiento de información sensible de los Estados. Por lo tanto el espacio virtual, como contenedor de información pasa a cobrar una importancia crucial, tanto para el sector público, como para el sector privado. Y lo que anteriormente era una herramienta de modernización en las comunicaciones y en el sistema organizacional se convierte en una fuente de vulnerabilidad para aquellos organismos que lo adoptan.

La característica principal de este nuevo escenario es que no cuenta con fronteras de ningún tipo que permita delimitar la jurisdicción de un Estado. Por ende, cuando hablamos del ciberespacio, hablamos de un mundo sin límites y sin nacionalidades. Sin

embargo, las consecuencias afectan a objetivos específicos y bien delimitados, ya sea a nivel Estatal, empresarial o individual.

De esta manera, los gobiernos del mundo se encuentran ante un doble desafío: En primer lugar, deben implementar medidas para contrarrestar las posibilidades de ataque a sus sistemas informáticos, estableciendo un sistema de defensa que les permita trabajar en combinación con otros Estados dado el carácter transnacional de la amenaza en cuestión. Y en segundo lugar, el desafío más importante es el de alcanzar una legislación a nivel mundial para establecer las reglas de juego en orden de eliminar las "zonas grises" en el marco del crimen cibernético.

La ausencia de una legislación clara y concreta permite un accionar casi impune por parte de los criminales cibernéticos. Por el contario, un marco regulatorio bien aplicado se convierte en el principal factor de defensa, ya sea de la defensa de la información y de las estructuras públicas y privadas, como de los derechos y garantías de los individuos.

Aproximación a las nociones e implicancias de la seguridad y defensa cibernéticas

El carácter de las amenazas a la seguridad internacional se ha modificado producto de la complejidad que adquieren los medios de violencia masiva como los efectos diversos que éstos puedan acarrear. Para abordajes más efectivos, ante la mutación de los hechos se requiere de perspectivas multidisciplinares que analicen la diversidad de factores intervinientes. Puede considerarse en un sentido amplio a las amenazas como: "un conjunto de circunstancias que integradas constituyen un factor potencial de daño cierto y que bajo ciertas condiciones puede producirse"[1] (Laiño, 1991. P. 35). Tal concepción de las amenazas integra también la noción de "riesgo", distinta a la primera en la medida en que no requiere de la voluntad de daño[2] (Bartolomé, 2006. P.131).

En las últimas décadas se han incorporado nuevas amenazas y riesgos que atentan contra la seguridad internacional, por lo cual los Estados necesariamente debieron considerarlos en sus agendas tanto de seguridad como de defensa nacional. Entre las mismas se encuentran los delitos cibernéticos, cibercrimen y ciberguerra. A su vez, las acciones cibernéticas han evolucionado desde los primeros actos de piratería informática para acceder ilegalmente a información clasificada de empresas u organismos gubernamentales realizados por *hackers*[3] hasta el desarrollo de operaciones, ejecutadas por gobiernos estatales, para afectar las redes, sistemas informáticos e infraestructura crítica de un país[4] (Traina, 2012, 2). Paradojalmente, el sistema de redes fue utilizado en sus inicios para proteger la información sensible de los Estados Unidos ante un eventual ataque soviético durante la guerra fría. El objetivo era, ni más ni menos, multiplicar la

[1] LAÍÑO, Aníbal en Bartolomé, M. ""Una aproximación teórica al concepto de defensa", Mimeo, Ágora, Centro de Estudios Internacionales, BsAs, 1.991, p. 35.
[2] BARTOLOMÉ, Mariano, "La seguridad internacional post 11-S. Contenidos, debates y tendencias", Instituto de publicaciones navales, IPN Editores. Bs As, 2.006. p. 131.
3Hacker: término derivado del inglés hacking, irrumpir o entrar de forma forzada un sistema de computación o una red.
4TRAINA, Eduardo; Pendrives o Misiles, La Ciberguerra: una nueva variable en el nivel estratégico; Paper; Escuela Superior de Guerra Conjunta; 2012, pág. 2.

información en orden de evitar que la misma se encontrara almacenada en un solo lugar, evitando de esa manera que un único ataque destruyera los archivos clasificados del gobierno. En cambio, hoy en día lo que se quiere evitar es la copia sin control de esos datos. Ahora la amenaza no radica solamente en la destrucción de información sensible, sino en quien controla dicha información.
Desde el punto de vista del ciberespacio, queda claro que el principal objetivo a proteger es la información. Entendiendo a la información como "toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro." (Oficina Nacional de Tecnología de Información, 2005. P. 9)[5]. En este sentido la calidad de los actores involucrados en los ataques cibernéticos, definirá el tipo de acción ejecutada comenzando con un delito cibernético en el nivel más bajo y con una ciberguerra en su máxima expresión. Asimismo, la seguridad cibernética remite a la condición de preservación de los intereses nacionales amenazados por medios cibernéticos, mientras que la defensa cibernética hace alusión a las medidas, acciones y actitudes para impedir la disminución de la seguridad cibernética, ya sea en forma de disuasión o de acción concreta.

Tipos de ataques cibernéticos:
Para simplificar el análisis y la comprensión del fenómeno estudiado, hemos diferenciado los ataques cibernéticos en tres tipos puros:

1- El delito cibernético, como lo indica la palabra, es aquel delito cometido por un particular utilizando herramientas informáticas y que buscan el rédito personal. Son hechos ilícitos tales como la estafa, fraude bancario, robo de identidad, etc. Si bien el atacante es un particular, la víctima puede ser otro particular, una organización o el Estado.
2- El cibercrimen implica una intencionalidad diferente por parte de los ejecutantes de la acción. Ya no sólo se busca el rédito económico, sino que existe la intención de generar un determinado efecto en la víctima del ataque. El atacante puede ser un particular o una organización y los objetivos suelen ser otras organizaciones, grandes empresas o los Estados. Un claro ejemplo de esto es el caso de *Wikileaks*.
3- La ciberguerra puede definirse como un conflicto clásico entre Estados, en el que los actores se valen del campo de la tecnología informática para afectar las fuerzas armadas, infraestructura y/o sistema de comunicación de un Estado. En el conflicto entre Georgia y Rusia en 1993 se empleó la ciberguerra en conjunto con el aparato militar tradicional.

El concepto de ciberguerra plantea una doble problemática en el ámbito académico. De acuerdo a nuestra definición, para llamar ciberguerra a un ataque cibernético los actores deben ser estatales. Esto plantea una dificultad en cuanto al reconocimiento del hecho

[5] Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional; Oficina Nacional de Tecnología de Información, 2005. P. 9

por parte del Estado atacante, ya que la ventaja que plantea una acción de esta índole es la difícil vinculación entre el ataque y el atacante. Por lo que es mucho más común hablar de cibercrimenes, acusando a individuos nacionalistas como los generadores de ataques a objetivos estratégicos. Sin embargo, según los expertos, para desarrollar un arma cibernética que pueda golpear grandes objetivos es necesario el concurso de centenares de programadores y con gran cantidad de recursos económicos y tecnológicos, rompiendo con el mito de que un joven habilidoso pueda llevar a cabo semejantes acciones (Noro, 2012. P. 44)[6].

La otra cuestión surge en cuanto a si es correcto hablar de ciberguerra o guerra cibernética, en tanto a que se tiene la concepción de que en aquellas no se producen bajas, de acuerdo a una de las características planteadas por Clausewitz para definir a una guerra: y es que produce bajas (Nievas, 2006. P. 60)[7]. Como mencionamos anteriormente, se trata de una guerra clásica pero que tiene como medio el uso de herramientas informáticas. Por lo tanto, si puede ocasionar bajas. En el caso de un ataque a una central nuclear podría generar fallas en el funcionamiento de la misma pudiendo llegar a generar cuantiosos niveles de bajas en una población.

La relevancia de la ciberdefensa en el mundo contemporáneo

En 1993 cuando Georgia reprimió a la población de Osseria de origen ruso, el ejército ruso intervino con un ataque de blindados y lo acompaño con un ciber ataque que dejó aislado a Georgia del resto de Europa y los Estados Unidos (Noro Lauro, 2012. P. 46)[8].

Una serie de incidentes cibernéticos contra la Organización del Tratado del Atlántico Norte (OTAN) y gobiernos miembros ocurrieron durante el *ALLIED FORCE* en 1999 para forzar a las unidades militares serbias a que salieran de Kosovo. Estos incidentes incluyeron ataques de negación de servicio y desfiguraciones de páginas *web* del Cuartel General Supremo de las Fuerzas Aliadas Europeas mientras los militares norte-americanos asistieron a un triple ataque de desfiguración. Estos ataques fueron conducidos por *hackers* nacionalistas rusos, serbios y chinos (Healy, 2012)[9].

En junio de 2010, la empresa bielorusa VirusBlokAda descubrió el *worm* Stuxnet, capaz de alterar un control industrial. Dicho *worm* atacó de forma intensiva redes de Irán, tal como el reactor nuclear ubicado en Bushehr. Éste ha sido considerado el primer *worm* que tuvo como objetivo una infraestructura crítica industrial (Mac Millan, 2010)[10].

---

[6] Noro Lauro, en Revista DEF, Año VII, Nro. 84. Editorial Taeda. Pág. 44

[7] Nievas Flabián, *Aportes para una sociología de la guerra*, Proyecto Editorial, Buenos Aires, 2006. Pág. 60.

[8] Noro Lauro, en Revista DEF, Año VII, Nro. 84. Editorial Taeda. Pág. 46.

9HEALEY, J, VAN BOCHOVEN, L. NATO's Cyber Capabilities: Yesterday, Today and Tomorrow. OTAN, 2012. Disponible en http://www.acus.org/publication/natos-cyber-capabilities-yesterday-today-and-tomorrow, acceso en 20 de junio de 2012.

10 MAC MILLAN, R. SIEMENS: Stuxnet worm hit industrial systems. Computerworld, 14 de septiembre de 2010. Disponible en:
http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_
industrial_systems?taxonomyName=Network+Security&taxonomyId=142, acceso en: 11 de junio de 2012.

En noviembre de 2010 varios millares de documentos clasificados fueron publicados en el sitio *web* Wikileaks. Los documentos, en su mayoría, fueron robados por un soldado estadounidense que los entregó a las personas de dicho sitio (Mulazzani, 2011)[11].

En julio de 2009, con una serie de virus del tipo Botnet Corea del Norte hizo caer los sitios del departamento del Tesoro, del Servicio Secreto, la Comisión Federal del Comercio, entre otras entidades Norteamericanas (Noro, 2012 b. P. 45)[12].

Marcos regulatorios para el cibercrimen. Convenio sobre Cibercriminalidad

Los desafíos que impulsan el alto crecimiento de la TIC en el mundo en general, y en la región latinoamericana en particular, trae consigo una complejización del sistema de seguridad y de los dispositivos que deban regular ese campo. Si bien cuando a primera vista, el caso de las tecnologías de la información y comunicación aparezcan como un área que se ve menos proclive a la regulación y a la capacidad de control y filtro por parte de los Estados, su importancia y versatilidad han producido la necesidad de contar con menos zonas grises de las que *a priori* presupone su naturaleza, por un mayor seguimiento y búsqueda de regulaciones que permitan volver más previsible sus aplicaciones.

En general, los juristas internacionales y la doctrina del Derecho entienden a los cibercrímenes, en tres actividades delictivas fundamentales:

"… delitos en donde la computadora es el objetivo de la actividad delictual, delitos en donde la computadora es usada como herramienta para cometer un delito y delitos en donde el uso de la computadora es un aspecto accidental de la comisión del delito."(Clifford, 2006. P. 12)[13]

De tal modo, la *Convention on Cybercrime* (CETS 185), o el *Convenio sobre Cibercriminalidad* en español, conforma el único acuerdo bajo el modo de un tratado internacional que cubre -o intenta cubrir- las cuestiones más relevantes en materia de legislación internacional sobre el cibercrimen o ciberdelincuencia (tratando cuestiones de Derecho Penal, Derecho Procesal y Cooperación Judicial Internacional), considerando especialmente el tratamiento de una política penal contra la ciberdelincuencia.

Adoptado por el Comité de Ministros del Consejo de Europa en su sesión N° 109 del 8 de noviembre de 2001, se presentó a la firma en Budapest el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

11MULAZZANI, F., Sarcia, S.A. Cyber Security on Military Deployed Network. `CCD COE, 2011. Disponible en http://www.ccdcoe.org/publications/2011proceedings/CyberSecurityOnMilitaryDeployedNetworks-Mulazzani-Sarcia.pdf, acceso en 20 de junio de 2012.

12 Noro Lauro, en Revista DEF, Año VII, Nro. 84. Editorial Taeda. Pág. 45.

13 CLIFFORD, Ralph D. *Cybercrime: The Investigation, Prosecution and Defense of A Computer-Related Crime*, Second Edition, Carolina Academic Press, New England, 2006; p. 12.

"En abril de 2001 el Consejo Europeo publicó el proyecto destinado a armonizar las legislaciones en los estados miembros (47 miembros y 8 observadores al día de la fecha) y abierta a otros países como Australia, Japón, Canadá, Sudáfrica y los EE.UU. en noviembre de 2001 (...). Por ende, este Convenio es el único que se encarga de la seguridad de la información y trata los delitos contra la Confidencialidad, Integridad y Disponibilidad de los datos y los sistemas informáticos"[14].

Sin embargo, combatir la cibercriminalidad y consolidar un sistema de ciberdefensa que procure reprimir y salvaguardarse de los responsables es una tarea de extrema complejidad. Ello debido al uso dual que se puede realizar de cualquier sujeto ideal en tanto persona jurídica, ya sea organización civil, sociedad comercial, fundación, con fines cibercriminales. En este sentido, varios juristas ya han abogado por considerar una concreta responsabilidad penal que recae sobre la propia corporación como un actor colectivo y olvidarse así del modelo de sujetos físicos responsables que responden a una corporación criminal (Sánchez, 2006)[15].

Cabe destacar que la Convención de Budapest, es el primer acuerdo internacional que procura la cooperación entre países para luchar contra diversos crímenes informáticos, y es la primera que se ofrece a Estados no miembros de la Unión Europea.

Con ello, resulta relevante a la luz de la Convención de Budapest contra el Cibercrimen, observar su proyección hacia otros países, pues aparece como un precedente y una fuente de derecho internacional relevante en una materia tan joven.

Es menester destacar el lento avance del Convenio de Budapest en nuestra región, donde podemos observar en la grilla dispuesta oficialmente por la Comisión Europea la poca participación de los Estados de la UNASUR (siendo México un Estado observador de dicho proceso de integración regional):

Tabla 1 – Estados no Miembros de la Unión Europea pertenecientes a la UNASUR[16]

States	Signature	Ratification	Entry into forcé	Notes	R.	D.	A.	T.	C.	O.
Argentina										
Chile										
México										

14Segu-info. *¿Qué es el Convenio sobre Cibercriminalidad de Budapest?* en Segu-Info, marzo 25 de 2010. Disponible en: http://blog.segu-info.com.ar/2010/03/que-es-el-convenio-sobre.html#axzz1yIompzu7, acceso: junio 20 de 2012.

15SÁNCHEZ, Silvia, MARÍA, Jesús, "*La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre Cibercriminalidad"* en *Delincuencia informática 125*, CGPJ, 2002; -Gómez-Jara Diez, Carlos. *La culpabilidad penal de la empresa*, en *Delincuencia informática*, 179, 2006.

16 Disponible en: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=02/06/2010&CL=ENG

Tal como se observa en la grilla, para principios del año 2010 sólo tres Estados se encontraban en negociaciones abiertas para lograr la firma del Convenio, es decir, al comienzo de todo el largo camino para constituir obligaciones ante la comunidad jurídica internacional.

No obstante, en nuestra región latinoamericana es factible revisar el estado de situación en ese campo respecto de los Estados que integran la UNASUR, a los fines de poder visualizar tanto el nivel de armonía y compatibilidad, como los instrumentos y características con los que cuentan sus Estados Miembros, y así poder tener un panorama que nos permita observar algunos patrones a postular en la sub-región, en términos de contener y resolver ciberdelitos.

La regulación de la ciberdefensa en el ámbito de la OEA

En Latinoamérica, los países de la región no cuentan con una referencia común en materia de delitos informáticos, otro de los déficits son las diferencias conceptuales que hacen dificultosa la aplicación y la unificación de una tipología penal correspondiente con los delitos que se buscan reprimir. A esto se le suman ciertas inconsistencias en materia de recursos, tecnología y capacidad puesta al servicio de este campo.

En la región, la Asamblea General de la OEA, por medio de la Resolución 1939 del año 2003, conocida como Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética[17], reconoce lo siguiente:

> "…Es necesario desarrollar una estrategia integral para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario. La OEA está comprometida con el desarrollo e implementación de esta estrategia de seguridad cibernética y en respaldo a esto, celebró una Conferencia sobre Seguridad Cibernética…"[18]

Para ello se instrumentó diversos talleres y pautas de trabajo con instancias de asesoramiento a los Estados Miembros, a fin de que éstos incorporasen en sus legislaciones internas prescripciones de los delitos bajo algunos criterios comunes:

> "...La Estrategia Interamericana Integral de Seguridad Cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). La Estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus

17 Disponible en: http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf

18 Informe de la Conferencia sobre Seguridad Cibernética, documento OEA/Ser.L/X.5/ CICTE/CS/doc.2/03). Buenos Aires, Argentina, del 28 al 29 de julio de 2003.

funciones y responsabilidades con respecto a la seguridad a fin de crear una cultura de seguridad cibernética"[19].

No obstante ello, cabe reconocer los esfuerzos – aunque todavía aislados – por incorporar y tipificar los delitos informáticos, lo cual ha sido objeto de diferentes tratamientos según el país de la región y de la propia UNASUR en particular.

Avances en la regulación del cibercrimen en países de la región

Es dable observar ciertos avances efectivos en la última década en torno a la legislación interna de ciertos países de la UNASUR (Ver Anexo) que cubre – o intenta cubrir – esta materia, teniendo en cuenta leyes substantivas sobre delitos cibernéticos, buscando cumplimentar con las Recomendaciones para una Estrategia Interamericana Integral de Seguridad Cibernética[20] al obligar que "Todos los Estados Miembros deberán establecer prohibiciones de carácter penal y jurídico a los ataques contra la confidencialidad, integridad y seguridad de los sistemas informáticos", así como también "Leyes procesales para la recopilación de pruebas electrónicas".

Por su parte, el Estado Argentino avanzó en la regulación contra los ciberdelitos, incorporando normas que siguieron de cerca el modelo del Convenio de Budapest, teniendo en vista su adhesión formal y las negociaciones para la firma del Convenio de Budapest, el día 25 de marzo de 2010 en el marco de la Conferencia sobre Cooperación contra el Cibercrimen en la ciudad de Estrasburgo, no siendo específicamente la misma incorporada por su Congreso al Derecho Interno.

No obstante, en virtud de la Resolución Conjunta 866 y 1500 del año 2011[21] por parte de la Jefatura de Gabinete de Ministros y del Ministerio de Justicia se creó una Comisión Técnica Asesora en materia de Cibercrimen con los fines, según el Artículo 1, de "desarrollar y formular una propuesta en relación con aquellas cuestiones procesales que se requieran para hacer efectiva la lucha contra el cibercrimen y el tratamiento de la evidencia digital". Ello sin olvidar ciertas demostraciones de interés político, tal como fue el apoyo institucional al Congreso Internacional de Cibercrimen Cloud Summit 2010 por medio de la Resolución 157 de la Secretaría de Comunicaciones.

Así mismo, se realizó diversas modificaciones a la legislación argentina de fondo que ha adecuado la misma con los parámetros estipulados en la Convención de

19 Ibídem.

20 Recomendaciones para una Estrategia Interamericana Integral de Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética. Comisión de Seguridad Hemisférica del Consejo Permanente de la OEA, mayo 11 de 2004, p. 8 (Disponible en: http://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFEQFjAA&url=http%3A%2F%2Fscm.oas.org%2Fdoc_public%2FSPANISH%2FHIST_04%2FCP12902S04.DOC&ei=TVDhT7HAAob89QSa8tXFAw&usg=AFQjCNF9n_Khba__Os8OHIoy2VOYzJ7A2Q) (Acceso: junio 20 de 2012).

21 Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/188231/norma.htm

Budapest posibilitando el acceso a la misma. Estos fueron, entre otros, la Ley 26.388 por la cual se tipificó en el Código Penal un conjunto de acciones vinculadas con la criminalidad informática, agregándose además a su Artículo 77 términos técnicos utilizados en la Convención citada.

Esta clase de modificatorias al sistema normativo interno fue seguido por varios de los Estados de la región con más o menos especificidades pero, sin lugar a dudas, con los mismos parámetros alineados a la Convención de Budapest. En este sentido, una lista concreta de las normas que reprimen dichos delitos informáticos y que regulan situaciones conexas puede ser visualizada en el Anexo.

Por otra parte, en esta última década distintos acontecimientos han demostrado la flagrante vulnerabilidad de los sistemas informáticos de los Estados. En esta línea, es ejemplo a citar lo sucedido el 10 de mayo de 2008 en Chile, cuando un *hacker* autodenominado "Cobarde Anónimo" publicó en un *blog* (FayerWayer) información personal de más de seis millones de ciudadanos. Entre los datos expuestos se encontraban desde nombres y direcciones hasta teléfonos y calificaciones académicas, que se agregaban a la sensible información sobre el salario ingresado de cada individuo.

En este caso, el propio *hacker* explicaba que dicha información había sido sustraída de bases del Ministerio de Educación, de la Dirección Electoral, de las telefónicas y hasta de bases de datos de departamentos militares. Así, la intención principal del responsable era "mostrar qué pobre era la protección de datos en Chile"[22]. Situaciones de este tipo llevan, por ejemplo a Chile, a entender directamente al cibercrimen como una nueva amenaza para la seguridad hemisférica[23].

Todo ello, a pesar de que Chile haya sentado de alguna manera un precedente en la región al haber sido el primer Estado latinoamericano en tratar una ley contra delitos informáticos. Así en esta línea,

> "…la legislación que eventualmente se convirtió en la Ley de Privacidad de Chile comenzó como proyecto en el Senado en 1993 y no fue hasta octubre de 1999 cuando se aprobó por parte de una Comisión Mixta. (…) Sin embargo, no existió ningún tipo de participación significante de ningún grupo por fuera de la industria y el mercado de bases de datos..."[24].

Así, es evidenciado un vacío de la sociedad civil en este tipo de debates y, por ende, una vulnerabilidad concreta al momento de sancionar leyes que se adecuen a las necesidad defensivas de los sistemas informáticos utilizados por una sociedad.

La regulación de la ciberdefensa en la UNASUR

22MUÑOZ, D, ORELLAN, P. & SAAVEDRA, Ó. "Cibercrimen investiga filtration de bases de datos personates de seis millones de chilenos" en El Mercurio, mayo 11 de 2008.

23 Consejo Permanente de la Organización de los Estados Americanos, Comisión de Seguridad Hemisférica, OEA/Ser.G, CP/CSH-430/02 rev. 1, 1 octubre 2002 (disponible en: http://www.resdal.org.ar/ultimos-documentos/seg-hem-compendio.html) (Acceso: junio 20 de 2012).

24MENALDO, Nicola. *¿Viva la data protection? Chile as a touchstone for the future of information privacy,* en University of Miami International and Comparative Law Review, 191, 2011; pp. 228-229.

Por otra parte, en lo que refiere estrictamente a la UNASUR como bloque regional, tanto el cibercimen como su contraparte, la ciberdefensa, son objetos de interés y se vienen delineando estrategias para avanzar sobre tales campos.

En este sentido, el pasado 3 y 4 de mayo de 2012 se realizó una nueva Reunión de Ministros de Defensa de la UNASUR[25] en la ciudad colombiana de Cartagena buscando ante todo formular mecanismos de cooperación para hacer frente al crimen transnacional y a las nuevas amenazas en la región, incluyendo entre estas a los delitos cibernéticos. Tal como bien dijo el Presidente Pro Témpore de la UNASUR, Jorge Lara Castro, "la delincuencia organizada transnacional es una amenaza para los Estados Miembros de UNASUR (…) el delito cibernético, son algunos de esos desafíos"[26]. Y por su parte, el Ministro de Defensa de Colombia, Juan Carlos Pinzón, explicó en la sesión inaugural que

> "…el crimen no conoce fronteras y las tecnologías están al alcance de todos en el planeta por lo mismo las organizaciones criminales de distinta índole precisamente aprovecha esas tecnologías, esas facilidades que da el mundo moderno, este siglo 21 en el que nos encontramos para tomar ventaja para fortalecer su accionar criminal."[27]

Además por otra parte se firmó previamente un Acta de Reunión Preparatoria a la Reunión de Ministros de Defensa[28], por la cual a raíz de análisis del Centro de Estudios Estratégicos de Defensa la UNASUR (CEED) se disponía concretamente redoblar los esfuerzos para establecer un Consejo, en tanto instancia sectorial institucional, que trate específicamente contra Delincuencia Organizada Transnacional, con los ciberdelitos incluidos.

En esta misma línea, se observan acciones políticas que priorizan la ciberdefensa regional, siendo el Eje 1.f de las Políticas de Defensa del Plan de Acción 2012[29] del Consejo de Defensa Sudamericano (CDS): "Conformación de un Grupo de Trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa", tal comisión se encuentra en responsables de Perú.

Por otra parte, la cooperación binacional entre Estados ha incorporado también en su agenda de tareas esta temática. Es un ejemplo de ello la decisión por parte de los Ministros de Defensa de Brasil y Colombia el pasado 17 de enero de 2012 de crear "una

25 Ver http://www.unasursg.org/index.php?option=com_content&view=article&id=516:ultima-unasur-debate-cooperacion-regional-en-crimen-trasnacional-organizado-y-nuevas-amenazas&catid=66:noticias-unasur

26 Disponible en: http://www.unasursg.org/index.php?option=com_content&view=article&id=623:suramerica-debe-continuar-consolidandose-como-una-zona-de-paz-secretaria-de-unasur&catid=66:noticias-unasur

27 Disponible en: http://www.unasursg.org/images/file/DISCURSO-MINISTRO-DE-DEFENSA-REUNION-PREPARATORIA-UNASUR.pdf

28 Disponible en: http://www.unasursg.org/images/file/acta-febrero-16.pdf

29 Disponible en: http://www.unasurcds.org/index.php?option=com_content&view=article&id=486%3Aplan-de-accion-2012&catid=47%3Aplan-de-accion&Itemid=53&lang=es

Comisión Conjunta de técnicos de las Fuerzas Militares con el fin de revisar y precisar las capacidades de los UAV´S, Blindado y Defensa Cibernética" (Minuto30, 2012). Por su lado, es también otro ejemplo la reunión acaecida entre los Ministros de Brasil y Argentina el día 5 de septiembre de 2011, en donde se decidieron por la "Profundización de la cooperación en materia informática y de ciber-defensa"[30].

En definitiva, la situación actual de la legislación tanto internacional como interna no son merecedores de grandes congratulaciones. La no regulación jurídica significa impunidad delictual:

> "En nuestra Región, los ataques son altamente lucrativos y existe suficiente impunidad para que los cibercriminales continúen desempeñando este trabajo. El crecimiento en ataques es hoy de un 500% en los primeros meses de 2011, (…) un ciberatacante en la región iberoamericana invierte US$150 en desarrollar una botnet o robots (…). La ganancia final (…) está en el orden de los US$887, algo así como US$5 millones a la semana en ganancias."[31]

Así, en América Latina se ha dejado avanzar durante este último tiempo a los ciberdelincuentes y sólo recientemente se ha posicionado como objetivo consolidar los sistemas de defensa cibernética y establecer estas ciberacciones como tipos penales a reprimir como cualquier otro delito. Sin embargo, no debiera ni siquiera ser así, ya que estos ciberdelitos tienen una incidencia colectiva hacia todos los individuos y la peligrosidad social tanto para las personas como para los propios Estados es abismal. Así, adecuar las legislaciones internas a los estándares internacionales y fomentar proyectos de armonización jurídica entre los Estados de la UNASUR colaborarán a un mejor desarrollo de defensa en esta temática.

Conclusiones

Habiendo pasado revista sobre algunas nociones que nos introducen en una temática de reciente cuño en defensa y seguridad internacional, se ha procurado revisar el estado de situación y las estrategias de los países de la UNASUR para el tratamiento de las amenazas por parte de los delitos cibernéticos. Por todo lo expuesto, se entiende preciso explorar propuestas que los miembros de la UNASUR puedan desarrollar como acciones efectivas y autónomas para reducir tanto las inseguridades y falencias cibernéticas pero

30Ministerio de Defensa de la Nación Argentina. Resumen Semanal de Noticias, nº 52, septiembre 5 de 2011. Disponible en: http://www.ejercito.mil.ar/resumenes/2011/rsn_mindef_52.pdf, acceso: junio 20 de 2012.

31 SANTAMBROGIA, Clelia, "El Cibercrimen se mueve a sus anchas en Latinoamérica, en Computerworld", nº 7, año XXVI, 2011. Disponible en: http://www.cwv.com.ve/cwv7_1.pdf, acceso: junio 20 de 2012.

Secretaría de Gestión Pública de la Nación Argentina. Portal de Cibercrimen, disponible en http://www.sgp.gov.ar/contenidos/onti/Cuerpo1/paginas/2010/cibercrimen.html, acceso en 24 junio 2012; p. 14.

también la dependencia ante Estados extrarregionales que, debido a la creciente interdependencia, podrían exportar sus conflictos a nuestro interior.

Entre las directrices identificadas para desarrollar -siempre basados en los principios de voluntad política, regionalidad y asistencia- se pueden considerar los siguientes como pasos para un tratamiento consistente del tema en cuestión, tales como: Instaurar la autoridad de gerencia de Defensa Cibernética en Sudamérica, crear un organismo de cooperación de estudios, actuar en la prevención, la resiliencia y la defensa de activos cibernéticos críticos, incentivar la ratificación y entrada de los diferentes convenios sobre cibercrímenes y promover una Convención Interamericana, elaborar una política regional de Defensa Cibernética, establecer asociaciones con otras organizaciones internacionales, con el sector privado y con la academia, entre otras medidas.

.

En esta misma línea se puede concluir que los líderes sudamericanos deben abordar la amenaza de ataques cibernéticos estratégicos con las respuestas estratégicas a favor de la defensa cibernética. Por ello, los Estados Miembros de la UNASUR deben adoptar como acciones para mitigar la amenaza de ataque cibernético: la disuasión, el control de armas cibernéticas, la doctrina y la tecnología.

Las preocupaciones que hoy ocupan las agendas con respecto a la seguridad y defensa cibernéticas -particularmente con relación a las amenazas cibernéticas- no son infundadas y serán intensificadas en los próximos años. Sin embargo, no se debe volver el tratamiento una panacea de los tiempos modernos. Se deben valorar las visiones más equilibradas, que coloquen el espacio cibernético como un coadyuvante importante de los otros dominios operacionales, por veces decisivo, pero sin dar lugar a exageraciones en su tratamiento.

Cabe considerar que ante la complejidad y diversidad de los ciberdelitos y la factibilidad de la ciberguerra, hablamos de campos cuyas estrategias de abordajes por parte de los Estados de la UNASUR se encuentran en construcción. El debate sigue abierto pero las acciones que se vienen desarrollando dan cuenta de la necesaria logística y convergencia de políticas de defensa y seguridad que los signatarios del bloque en cuestión han considerado en la nutrida agenda regional y en la cual deben seguir avanzando de manera contundente.

Bibliografía

BARTOLOMÉ, Mariano, “La seguridad internacional post 11-S. Contenidos, debates y tendencias”, Instituto de publicaciones navales, IPN Editores. Bs As, 2.006. p. 131.

CLIFFORD, Ralph D. *Cybercrime: The Investigation, Prosecution and Defense of A Computer-Related Crime*, Second Edition, Carolina Academic Press, New England, 2006; p. 12.

HEALEY, J, VAN BOCHOVEN, L. NATO’s Cyber Capabilities: Yesterday, Today and Tomorrow. OTAN, 2012. Disponible en http://www.acus.org/publication/natos-cyber-capabilities-yesterday-today-and-tomorrow, acceso en 20 de junio de 2012.

MAC MILLAN, R. SIEMENS: Stuxnet worm hit industrial systems. Computerworld, 14 de septiembre de 2010. Disponible en: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142, acceso en: 11 de junio de 2012.

Ministerio de Defensa de la Nación Argentina. Resumen Semanal de Noticias, nº 52, septiembre 5 de 2011. Disponible en: http://www.ejercito.mil.ar/resumenes/2011/rsn_mindef_52.pdf, acceso: junio 20 de 2012.

MOUSSU, Nelly, LLOUQUET, Anne-Lise y CHAUMEI, Grégoi. (2011). *"Cyberespace le 5eme champ de Bataille*". Artículo Revista "Armees d'ajuord'hui – Dossier ". Nro. 365 Noviembre/Diciembre. Delegación de Información y Comunicación de la Defensa - Ministerio de Defensa. Francia. En Traina, Eduardo; *Pendrives o Misiles*, La Ciberguerra: una nueva variable en el nivel estratégico; Paper; Escuela Superior de Guerra Conjunta; 2012, pág. 2.

MULAZZANI, F., Sarcia, S.A. Cyber Security on Military Deployed Network. `CCD COE, 2011. Disponible en http://www.ccdcoe.org/publications/2011proceedings/CyberSecurityOnMilitaryDeployedNetworks-Mulazzani-Sarcia.pdf, acceso en 20 de junio de 2012.

MENALDO, Nicola. *¿Viva la data protection? Chile as a touchstone for the future of information privacy,* en University of Miami International and Comparative Law Review, 191, 2011; pp. 228-229
.
MUÑOZ, D, ORELLAN, P. & SAAVEDRA, Ó. "Cibercrimen investiga filtration de bases de datos personates de seis millones de chilenos" en El Mercurio, mayo 11 de 2008.

Segu-info. *¿Qué es el Convenio sobre Cibercriminalidad de Budapest?* en Segu-Info, marzo 25 de 2010. Disponible en: http://blog.segu-info.com.ar/2010/03/que-es-el-convenio-sobre.html#axzz1yIompzu7, acceso: junio 20 de 2012.

Recomendaciones para una Estrategia Interamericana Integral de Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética. Comisión de Seguridad Hemisférica del Consejo Permanente de la OEA, mayo 11 de 2004, p. 8 (Disponible en: http://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFEQFjAA&url=http%3A%2F%2Fscm.oas.org%2Fdoc_public%2FSPANISH%2FHIST_04%2FCP12902S04.DOC&ei=TVDhT7HAAob89QSa8tXFAw&usg=AFQjCNF9n_Khba__Os8OHIoy2VOYzJ7A2Q) (Acceso: junio 20 de 2012)

SÁNCHEZ, Silvia, MARÍA, Jesús, "*La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre Cibercriminalidad"* en *Delincuencia informática 125*, CGPJ, 2002; -Gómez-Jara Diez, Carlos. *La culpabilidad penal de la empresa*, en *Delincuencia informática*, 179, 2006.

SANTAMBROGIA, Clelia, “El Cibercrimen se mueve a sus anchas en Latinoamérica, en Computerworld”, nº 7, año XXVI, 2011. Disponible en: http://www.cwv.com.ve/cwv7_1.pdf, acceso: junio 20 de 2012.

Secretaría de Gestión Pública de la Nación Argentina. Portal de Cibercrimen, disponible en http://www.sgp.gov.ar/contenidos/onti/Cuerpo1/paginas/2010/cibercrimen.html, acceso en 24 junio 2012; p. 14.

TRAINA, Eduardo; Pendrives o Misiles, La Ciberguerra: una nueva variable en el nivel estratégico; Paper; Escuela Superior de Guerra Conjunta; 2012, pág. 2.

http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=02/06/2010&CL=EN http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf

Informe de la Conferencia sobre Seguridad Cibernética, documento OEA/Ser.L/X.5/CICTE/CS/doc.2/03). Buenos Aires, Argentina, del 28 al 29 de julio de 2003.

Consejo Permanente de la Organización de los Estados Americanos, Comisión de Seguridad Hemisférica, OEA/Ser.G, CP/CSH-430/02 rev. 1, 1 octubre 2002 (disponible en: http://www.resdal.org.ar/ultimos-documentos/seg-hem-compendio.html) (Acceso: junio 20 de 2012).