Consideraciones sobre la Ciberamenaza a la Seguridad Nacional

CONSIDERATIONS CYBER THREAT TO NATIONAL SECURITY

Recibido: 25 / 08 / 2015 *Aprobado: 09 / 11 / 2015*

Alejandro Amigo Tossi

Oficial de Estado Mayor, Ejército de Chile. Master of Arts in Security Studies, Georgetown University. Magister en Conducción Militar, Academia de Guerra, Ejército de Chile. Licenciado en Ciencias Militares, Escuela Militar. Autor del blog "Ciberestrategia" https://ciberestrategia.wordpress.com/. Actualmente es parte del Grupo de Planificación Estratégica de la Dirección de Operaciones del Ejército de Chile. alejandroamigotossi@gmail.com.

RESUMEN

La ciberamenaza es uno de los principales riesgos para la seguridad de los países desarrollados, como también de los Estados en vías de desarrollo como el nuestro. Este fenómeno es uno de los retos a la seguridad nacional que exige la adopción de un enfoque integral en su análisis, que contemple los aspectos que han transformado a los actores y acciones maliciosas de este ámbito en uno de los principales desafíos a la seguridad de organizaciones estatales y privadas en todo el mundo. Estados, hackers, hacktivistas y cibercriminales han sido protagonistas de diversos actos que han configurado una nueva dimensión para la seguridad nacional e internacional. El propósito de este artículo es proponer los tópicos que podrían incluirse en la apreciación nacional sobre la ciberamenaza a la seguridad nacional de Chile, basado en ciertas definiciones conceptuales, los ciberataques que han afectado a organismos del gobierno de Chile e instituciones de la defensa y por último, las consideraciones sobre la ciberamenaza incluidas en las Estrategias de Seguridad Nacional de ciertas potencias occidentales.

Palabras claves:

Seguridad nacional, defensa nacional, ciberespacio, ciberamenaza, planificación nacional.

ABSTRACT

The cyber threat is one of the major security risks in developed countries, as well as the developing States like ours. This phenomenon is one of the challenges to national security that calls for a comprehensive approach in its analysis that considers aspects that have transformed malicious actors and actions in this field in one of the main challenges to security organizations state and private worldwide. United, hackers, cybercriminals and hacktivists have been involved in various events that have shaped a new dimension to national and international security. The purpose of this paper is to propose topics for inclusion in the national assessment of the cyber threat to national security of Chile, based on certain conceptual definitions, cyber attacks that have affected agencies of the Chilean government and defense institutions and Finally, the cyber threat considerations included in the National Security Strategy of certain Western powers.

Keywords:

National defense, cyberspace, cyberthreat, national planning, national security

Introducción

La ciberamenaza forma parte de los riesgos a la seguridad nacional de los países desarrollados, pero también afecta a los Estados en vías de desarrollo, donde organizaciones estatales y empresas privadas han incorporado en sus procesos de funcionamiento las nuevas tecnologías que emplean el ciberespacio. Este último es el caso de Chile, donde el uso masivo de internet y redes informáticas es un aspecto fundamental en todos los ámbitos del quehacer nacional. El Estado chileno es el país latinoamericano con mayores avances en gobierno electrónico según la Encuesta de Desarrollo del Gobierno Electrónico de las Naciones Unidas.[1] Además, de acuerdo con el UN E-Government Development Survey, Chile es el país con la mayor evolución digital en la región.[2] Estos antecedentes hacen evidente que la ciberamenaza es parte de los retos a la seguridad nacional, exigiendo un análisis integral que defina los riesgos que en este dominio el país enfrentará en el corto y mediano plazo y que considere los últimos acontecimientos nacionales y la experiencia de ciertos países que están a la vanguardia en esta área.

El propósito de este artículo es desarrollar un breve análisis de la ciberamenaza a la seguridad nacional de Chile, teniendo como referencia ciertas nociones básicas sobre la temática, los ataques que han acaecido sobre objetivos nacionales y la apreciación estratégica de la amenaza procedente del ciberespacio por parte de tres potencias occidentales. A partir de esta revisión, se propone la consideración de ciertos temas en la apreciación que el Estado chileno debiera desarrollar sobre esta amenaza. El artículo se divide de la siguiente manera. En primer lugar, se desarrolla un breve marco teórico para conceptualizar los actores y fenómenos en el ámbito de la ciberamenaza que debieran considerarse para el análisis de la realidad nacional. En segundo lugar, se describen algunos ciberataques que han afectado a organismos del gobierno de Chile e instituciones de la defensa, como evidencias de la amenaza actual procedente del ciberespacio. En tercer lugar, se analiza el contenido sobre la ciberamenaza en las Estrategias de Seguridad Nacional de ciertas potencias occidentales que en el ámbito de la defensa podrían ser referentes para Chile. Por último, como conclusión, se proponen algunos aspectos que deberían ser contemplados en la evaluación de la ciberamenaza a la seguridad nacional.

1 http://unpan3.un.org/egovkb/datacenter/CountryView.aspx. Último acceso el 15 de abril del 2014.
2 Economist Intelligence Unit & IBM. "Digital economy rankings 2010: Beyond e-readiness". 2010. p. 4.

Conceptualización de la ciberamenaza

El ámbito donde se desarrollan y actúan las ciberamenazas es el ciberespacio, el cual entenderemos como un dominio interactivo compuesto por redes digitales que se utilizan para almacenar, modificar y comunicar información; incluyendo internet y otros sistemas de información que apoyan a las organizaciones, empresas, infraestructuras y servicios.[1] Por tanto, los ciberactores son aquellos elementos que llevan a cabo algunas de las acciones explicadas más adelante en el dominio del ciberespacio.

Los ciberactores que perpetran operaciones maliciosas contra Estados, sus instituciones y organizaciones privadas es posible separarlos en cinco grupos: actores estatales con cibercapacidades como parte de sus activos de defensa, terroristas, elementos del crimen organizado, hacktivistas[2] y hackers patriotas.[3] En el caso de los actores estatales, un ejemplo es el indicado por el reporte de la empresa norteamericana de ciberseguridad Mandiant que identifica como "APT-1" a un grupo situado en China que contaría con el apoyo del gobierno chino y posee diversas similitudes con una unidad del Ejército Popular Chino. Según este informe, esta unidad es capaz de desarrollar una avanzada y persistente amenaza a intereses norteamericanos.[4] Otro caso, es el ataque a los sistemas computacionales de la empresa Sony, supuestamente por parte del Estado Norcoreano según Estados Unidos, que incluso resultó en ciberataques de respuesta por parte de la potencia norteamericana.[5]

El ciberespacio es un dominio al cual los terroristas buscarán expandir las acciones de terror para el logro de sus objetivos políticos. El bloqueo de las emisiones del canal francés TV5 el mes de Abril pasado, por parte de un grupo que proclamó su lealtad al Estado Islámico, es un ejemplo de este tipo de hechos.[6] En cuanto al crimen organizado, un reporte de la empresa McAfee, señala que éste es un negocio ilícito donde los riesgos, que asumen los responsables, son bajos en comparación con las exorbitantes ganancias, y que sus operaciones implican pérdidas globales anuales aproximadas de $ 400 billones de dólares la economía mundial.[7]

Los hacktivistas como "Anonymous" llevan a cabo ataques a sitios web como protestar en defensa de ciertos derechos civiles en el contexto de conflictos intra-estatales o de tipo global. Nuestro país ha sido víctima de la acción de este último grupo, y algunos casos serán mencionados más adelante. Por último, los hackers patriotas han participado en el contexto de crisis inter-estatales, donde realizan ataques sin ninguna dirección o patrocinador, con el único fin de apoyar a sus respectivas naciones en la prosecución de los objetivos. [8] El rol de estos últimos en la agresión Rusa con-

1 - UK Government. "The UK Cyber Security Strategy". Noviembre 2011.
2 - Término utilizado para describir a los hackers que su principal objetivo es realizar activismo mediante acciones en redes y sistemas informáticos.
3 - Término utilizado para describir a los hackers que su principal objetivo es realizar activismo mediante acciones en redes y sistemas informáticos.
4 - Mandiant. "APT1 Exposing One of China's Cyber Espionage Units". Intelligence Report. 2014.
5 - http://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-to-sony-hack-lawmaker-says. Ultimo acceso el 19 de marzo de 2015.
6 - http://www.independent.co.uk/news/uk/home-news/bbc-says-feared-isis-cyber-attack-during-live-news-broadcast-was-actually-operational-error-10167537.html Último acceso el 02 de junio de 2015.
7 - McAfee & Center for Strategic and International Studies. "Net Losses: Estimating the global cost of Cybercrime". 2014.
8 - Carr, Jeffrey. "Inside Cyber Warfare". O'Reilly Media, Inc., 2010. p. 15.

tra Georgia en el año 2008, se concentró en ataque a sitios web gubernamentales e incluso superó el periodo de tiempo en que Rusia hizo uso de la fuerza.[9]

Es importante además mencionar la acción conjunta entre Estados y actores no estatales patrocinados por los primeros, donde la diferencia entre ambos se vuelve difusa. Algunos Estados han utilizado hackers de orientación nacionalista y hacktivistas para ocultar su responsabilidad y evitar la consiguiente atribución.[10] Estos actores no estatales con el apoyo financiero y técnico de un aparato estatal, aumentan sus capacidades y logran ejecutar acciones con altas probabilidades de infringir graves daños a objetivos más relevantes. Los casos de ataques atribuidos a China por parte de EE.UU. hacia organizaciones privadas y estamentos estatales de esa nación, son ejemplos recientes de este fenómeno.[11]

Otro punto son las técnicas que utilizan los ciberactores y los objetivos por alcanzar en el marco de sus acciones contra las redes y sistemas informáticos de organismos estatales y privados. Dentro de las técnicas encontramos la acción de virus o troyanos en sistemas informáticos, denegación del servicio en sitios web, robo de información sensible, fraude, eliminación de la información en computadores y bases de datos y la inutilización o control remoto de sistemas de control de infraestructura crítica. El ataque del virus Stuxnet, atribuido a EE.UU. e Israel, que destruyó entre 1.000 a 6.000 máquinas centrifugas que enriquecían uranio en plantas nucleares de Irán,[12] es una demostración de la última técnica señalada. En cuanto a los objetivos de los ciberataques, más allá de las actuales acciones en contra de redes computacionales, bases de datos y sistemas de correos corporativos, en un futuro previsible las acciones más riesgosas serán ataques contra infraestructuras civiles vitales (centrales nucleares, represas, sistemas de distribución de energía, servicios básicos, etc.) no necesariamente en el contexto de los conflictos armados, y acciones contra redes y/o sistemas de información de las Fuerzas Armadas durante crisis o conflictos.[13]

En cuanto a los métodos empleados para afectar los intereses de un país, es posible separarlos en dos tipos: la explotación de redes informáticas y ataques propiamente tal. La explotación corresponde a actividades de espionaje a redes del gobierno, industria de defensa y Fuerzas Armadas con el objetivo de alcanzar un dominio de la información desde tiempo de paz. Esta superioridad incluso podría otorgar a potenciales enemigos la ventaja de incrementar su preparación para enfrentar ciberataques de represalia. Adicionalmente, la explotación tendrá como propósito preparar futuros ataques contra redes informáticas o sistemas que controlan actividades industriales vitales en caso de crisis o conflictos de baja intensidad.

Los ciberataques corresponden a denegaciones de servicio, introducción de virus, malware y/o troyanos que causarán pérdida de información o impedirán el normal servicio de redes, servicios web y de correo, y sistemas informáticos. La evidencia internacional demuestra que los ataques más

9 - http://www.foxnews.com/story/2008/08/13/russian-hackers-attack-georgia-in-cyberspace/ Último acceso el 04 de junio del 2015.

10 Ibid. p. 115. Último acceso el 11 de agosto del 2014.

11 http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea1 4c099f9_story.html. Último acceso el 15 de agosto del 2014.

12 - http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. Último acceso el 22 de agosto del 2014.

13 - Clarke, Richard y Knake, Robert. "Cyber War, the next threat to National Security and what to do about it". Ecco Editorial, 2010. p. 107.

importantes son "denegación de servicio" contra redes gubernamentales y sitios web de empresas privadas para interrumpir o deshabilitar su funcionamiento normal; ataques destinados a borrar o destruir información vital en entidades privadas o estatales y ataques para degradar o alterar sistemas de control industriales. Además, los sistemas de mando y control y redes institucionales de las Fuerzas Armadas, serán vulnerables a ataques destinados a reducir la capacidad de la fuerza militar para dirigir y controlar las operaciones en los otros dominios de la guerra.

La complejidad de las acciones en el ciberespacio dificultan la defensa y disuasión contra estas operaciones. La atribución de un ataque va más allá de determinar el origen de los autores. La acción de identificar al o los responsables de un ciberataque debe relacionarse con el contexto de una crisis o con anteriores acciones similares. El caso del destructivo virus Shamoon en las redes informáticas de la petrolera estatal saudí Aramco y su consecuente atribución por parte de EE.UU. y Arabia Saudita al Estado de Irán[14] es un ejemplo donde un escenario estratégico de confrontación entre potencias regionales sirvió de base para especular sobre el supuesto responsable. Sin embargo, en caso de que la atribución sea correcta, será complejo ejecutar una acción de respuesta o procurar una sanción internacional, debido a la ausencia de normas reconocidas globalmente en el dominio del ciberconflicto. Además, la ambigüedad de la evaluación de un ciberataque como uso letal de la fuerza de acuerdo con el derecho internacional, significará un desafío adicional para que el Estado afectado planifique algún tipo de respuesta.

Por último, un aspecto relevante son los propios usuarios de los sistemas informáticos. Esta amenaza interna estará siempre presente a pesar del nivel de seguridad alcanzado en las propias redes, y podrá comportarse como un facilitador de un ataque o simplemente en ejecutor de acciones maliciosas. Los casos de Snowden y Manning, en la Agencia de Seguridad Nacional norteamericana y el Ejército de EE.UU. respectivamente, son ejemplos del alcance y daño que pueden provocar la acción de "insiders".

CHILE BAJO LA CIBERAMENAZA

Chile, en su condición de sociedad abierta, interconectada con el mundo y con un alto grado de avance digital, tiene una mayor exposición a los riesgos en el ámbito de las redes y sistemas informáticos, que previsiblemente se irán consolidando como parte de las amenazas que afectarán a la seguridad nacional. Por ejemplo, un evento organizado por Naciones Unidas sobre ciberseguridad y desarrollo entregó como conclusión que los países en vías de desarrollo como Chile tienen un mayor riesgo de ser blanco de ciberataques y que el impacto económico y consecuencias contra la infraestructura crítica, el sistema bancario, los sistemas nacionales de salud, el gobierno y bancos de datos de la industria y servicios podrían ser de alto impacto.[15] Es decir, un sostenido crecimiento económico, la adopción de tecnologías de informática y computación avanzadas y el creciente uso de internet son las condiciones ideales para un incremento de la ciberamenaza. Lo anterior, es respaldado por un informe de Kaspersky Lab, el cual se-

14 - http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_ r=2 Último acceso el 16 de septiembre del 2014.

15 - http://www.un.org/apps/newsstory.asp?Cr=cyber&NewsID=40692#.UXR-6xitAQW9. Último acceso 21 de abril del 2014.

ñala que Chile ocupa el puesto número uno de los países latinoamericanos que son víctimas de ciberataques.[16]

A la fecha, los principales ciberataques contra intereses nacionales han sido acciones de actores no estatales en apoyo a movimientos civiles de protesta, operaciones destinadas a robar información o cometer delitos y por último, espionaje de correos electrónicos de instituciones de la defensa nacional. Uno de los primeros episodios ocurrió en el año 1995, con el hackeo del sitio web de la "Cumbre de Presidentes de América", donde el dominio fue intervenido y reemplazado por propaganda en contra de la reunión internacional. [17] Luego, en 1996 fue saboteada la red informática del Servicio de Impuestos Internos y perturbado su funcionamiento, con el consiguiente daño en su nivel de confianza pública.[18]

Durante los últimos cinco años ha existido un incremento en los tres tipos de ataques mencionados en el párrafo anterior, lo que ha incrementado la atención pública sobre el tema. Con respecto a hacktivistas que han apoyado movimientos de protesta, el actor principal ha sido el actor no estatal "Anonymous Chile". Esta franquicia nacional ha sido responsable de ataques contra sitios web de organizaciones públicas y privadas, donde los dominios han sido víctimas de "denegación de servicio" y su contenido ha sido sustituido por propaganda contra políticas gubernamentales o empresas involucradas con cuestiones ambientales. Los principales ejemplos de estos casos son los siguientes: Junio del 2011, "Operación Andes libre" atribuida por Anonymous. En respuesta a la supervisión del Estado en el contenido de la web en territorio nacional. Sus acciones fueron la denegación de servicio de sitios web gubernamentales relacionados con el tema.[19]

Julio del 2012, "Operación Chile 2012" atribuida por Anonymous. Su objetivo fue la defensa de una serie de derechos cívicos y la denuncia de ciertas políticas ambientales del gobierno. Sus acciones fueron la denegación de servicio de sitios web del gobierno y empresas privadas relacionadas con proyectos hidroeléctricos.[20]

En relación a las acciones destinadas a robar información, éstas han correspondido a ataques contra sitios web del gobierno y actividades cibercriminales contra individuos. El principal ejemplo del primer caso, fue el robo de información privada de seis millones de personas desde las bases de datos de organismos públicos, que fueron subidos a internet el día siguiente. Los sitios web atacados fueron el Ministerio de Educación, la Dirección General de Movilización Nacional y el Servicio Electoral de Chile.[21]

En cuanto a ataques orientados a instituciones de la Defensa Nacional, durante el mes de Agosto del año 2014, se conoció una acción de hackers peruanos que vulneraron la ciberseguridad de la Fuerza Aérea de Chile y filtraron cientos de correos electrónicos de la institución. Dentro de la información revelada se encontraban detalles de nego-

16 - http://www.emol.com/noticias/tecnologia/2012/09/13/560281/chile-entre-los-paises-que-sufre-mas-ciberataques-en-america-latina.html. Último acceso 18 de abril del 2014.
17 - http://www.policia.cl/paginas/brigadas/bg-bricib/bg-bricib.htm. Último acceso el 14 de abril del 2013.
18 - Ibíd. Último acceso el 14 de abril del 2014.
19 - http://elcomercio.pe/actualidad/791354/noticia-anonymous-lanzara-ciberataques. Último acceso el 17 de abril del 2014.
20 - http://www.latercera.com/noticia/nacional/2012/07/680-475213-9-anonymous-lanzo-operacion-operacion-chile2012-contra-sitios-chilenos.shtml. Último acceso el 17 de Abril del 2014.
21 - http://news.bbc.co.uk/hi/spanish/latin_america/newsid_7395000/7395288.stm. Último acceso el 15 de abril del 2014.

ciaciones entre la institución y empresas de defensa para la compra de armamento, radares y el desarrollo de overhaul de sistemas de armas institucionales.[22]

LA CIBERAMENAZA SEGÚN LAS POTENCIAS OCCIDENTALES

La ciberamenaza representa un aspecto relevante en las estrategias de seguridad nacional de algunas de las principales potencias occidentales. Para demostrar lo anterior, se analizará brevemente las versiones de Estados Unidos, Reino Unido y Australia, con el objetivo de identificar aspectos que debiera considerar una apreciación sobre la ciberamenaza hacia los intereses de Chile. En general, estos documentos contienen una descripción general del fenómeno, que considera algunos tópicos que no forman parte del debate nacional, y plantean una interacción entre el tema en comento y otros fenómenos transnacionales. Aunque los textos reflejan la realidad de cada país en su dimensión nacional, regional e internacional, es importante que nuestra nación considere estas referencias para ser incluidas en nuestro escenario estratégico.

LA ESTRATEGIA DE SEGURIDAD NACIONAL DE EE.UU., 2010

La estrategia de EE.UU. en su versión 2010, consideró la ciberamenaza como parte de los retos a uno de sus principales intereses nacionales, la "seguridad". El documento declara que la ciberamenaza es uno de los más complejos desafíos para su estabilidad interna.[23] El texto describe claramente que las fortalezas de Estados Unidos en diversas áreas, son al mismo tiempo, su principal debilidad frente a ciberenemigos.

> *"…. nuestras redes gubernamentales son constantemente sondeadas por intrusos….. Adversarios podrían utilizar vulnerabilidades para interrumpir el suministro en una escala masiva. En el internet y comercio electrónico….. Cibercriminales generan cientos de millones de dólares de pérdidas a empresas y consumidores, como también el robo de valiosa propiedad intelectual."*[24]

Este párrafo contiene dos aspectos principales. Primero, para los EE.UU. la ciberamenaza se centra en la defensa nacional, la seguridad pública y la economía; ámbitos donde han ocurrido los principales acontecimientos en el ciberespacio. Segundo, confirma que cuanto más alto el nivel de desarrollo de un país, más peligrosa es la ciberamenaza en contra de sus intereses nacionales y la seguridad nacional.

Posteriormente, el documento norteamericano declara que sus ciberamenazas comprenden hackers individuales, grupos delictivos organizados, redes terroristas y Estados que disponen de avanzada tecnología en esta área;[25] incorporando a los grupos terroristas en los actores que operan activamente en el ciberespacio.

En resumen, el contenido de la estrategia estadounidense permite deducir algunos aspectos que deberían ser parte de la apreciación nacional sobre la temática. En primer

22 - http://www.elmostrador.cl/pais/2014/08/14/hackers-peruanos-vulneran-seguridad-de-la-fach-y-filtran-cientos-de-correos-electronicos-de-la-institucion. Último acceso el 15 de agosto del 2014.

23 - El Presidente de Estados Unidos. "The United States National Security Strategy", 2010. p. 27.

24 - Ibid. p. 27.

25 El Presidente de Estados Unidos. Op. Cit. 2010. p. 27.

lugar, la importancia de señalar claramente cuáles son los ámbitos del nivel nacional que podrían ser los principales objetivos de la ciberamenaza. En segundo lugar, la importancia de asumir que el avance del país hacia el desarrollo incrementará los riesgos en este ámbito. En tercer lugar, la necesidad de identificar los potenciales ciberactores según la realidad nacional.

ESTRATEGIA NACIONAL DE SEGURIDAD DEL REINO UNIDO, 2010

La Estrategia Nacional de Seguridad del Reino Unido contempla la ciberamenaza como uno de los riesgos prioritarios a su seguridad, en el mismo nivel del terrorismo, las crisis militares internacionales y los desastres naturales. El documento señala que la amenaza en cuestión no es un riesgo futuro, sino que en la actualidad el gobierno, el sector privado y los ciudadanos están bajo ataques sostenidos, por parte de Estados hostiles o de organizaciones criminales. [26]

La Estrategia en uno de sus párrafos declara lo siguiente:

> *"La actividad en el ciberespacio seguirá evolucionando como una amenaza directa a la seguridad y economía del país, mientras sigue perfeccionándose como un medio de espionaje y crimen, y continúa creciendo como un facilitador del terrorismo, así como un arma militar para uso de los Estados y, posiblemente, otros actores."* [27]

Esta declaración acerca de la ciberamenaza tiene dos aspectos relevantes. El Reino Unido la considera como uno de los activos de la defensa que serán empleados por actores estatales en caso de crisis o conflicto militar. Además, es evaluada como una herramienta disponible para las redes terroristas, que podrían atacar su territorio o intereses en el extranjero.

Por otra parte, el documento declara que los ataques en el ciberespacio podrían tener un efecto potencialmente devastador y que el gobierno, la fuerza militar, ciertos objetivos industriales y económicos (incluyendo los servicios críticos), podrían verse perturbados por adversarios que cuenten con la tecnología necesaria. [28]

En síntesis, la estrategia del Reino Unido contiene algunos puntos que sería significativo explicitar en el caso nacional. En primer lugar, la importancia de considerar la relación que existe entre redes terroristas y/o subversivas y el ciberespacio como un medio para influenciar las acciones del Estado de Chile. En segundo lugar, la ciberamenaza debe ser considerada como parte del inventario bélico que podría ser utilizado en el contexto de un conflicto. En tercer lugar, la importancia de asumir los efectos devastadores que un ciberataque podría tener en contra de bienes económicos vitales o servicios públicos en el futuro cercano.

LA ESTRATEGIA NACIONAL DE SEGURIDAD DE AUSTRALIA, 2012

Este documento, al igual que los otros dos casos, puntualiza a la ciberamenaza como uno de los principales riesgos para su seguridad. La estrategia afirma que la ciberactivi-

26 - HM Government. "The United Kingdom National Security Strategy", 2010. p. 29.

27- HM Government. Op. Cit. 2010. p. 29.

28 - Ibid. p. 30

dad maliciosa es una creciente, y siempre cambiante, amenaza a la seguridad nacional a través de actividades terroristas, el crimen organizado y el espionaje.[29] El documento australiano declara que si las acciones en el ciberespacio con intención de causar daños no se controlan, tienen el potencial de socavar la confianza en la estabilidad social y económica y la prosperidad de la nación.[30]

El texto además explica que la dependencia de internet y sistemas informáticos ha incrementado la exposición de Australia al ciberespionaje. El documento asume que las actividades de espionaje colocan una serie de intereses nacionales en riesgo, incluyendo: información gubernamental clasificada, información comercial con consecuencias directas para la economía, propiedad intelectual y datos privados de los ciudadanos.[31]

En otra sección se señalan otras actividades maliciosas en el ciberespacio tales como: servicios de inteligencia extranjeros que utilizan el internet para infiltrarse en los sistemas propios, coordinación de grupos extremistas y radicalización de nuevos reclutas y el internet como medio para promover el odio y la división entre grupos de la sociedad.[32]

En conclusión, el documento australiano contiene los siguientes temas que podrían incluirse en el proceso de análisis nacional. En primer lugar, la importancia de describir las consecuencias a largo plazo de que el país sea un objetivo permanente de los ciberataques. En segundo lugar, la importancia de evaluar en forma precisa los objetivos principales de las actividades de ciberespionaje. Finalmente, que la inclusión de otras actividades maliciosas en internet, además de los ciberataques, es relevante para una completa evaluación de la amenaza que en este dominio enfrentará el Estado chileno.

29 - Gobierno de Australia. "The Australian National Security Strategy". 2012. p. iii.
30 - Ibid. p. 11.
31- Ibid. p. 16.
32 - Gobierno de Australia. Op. Cit. 2012. p. 40.

CONCLUSIONES

La evaluación nacional de la ciberamenaza debe considerar como referencias, entre otros aspectos, el estado del arte sobre el tema, los acontecimientos nacionales e internacionales y la estimación de referentes internacionales. En cuanto al contenido, el documento al menos, debería referirse a los actores, objetivos, métodos, complejidad, inminencia y la multidimensionalidad del tema.

La defensa nacional debe definir con precisión la amenaza que Chile ya está enfrentando y la que probablemente afrontará en un futuro próximo. Aunque nuestros intereses nacionales y escenario estratégico poseen particularidades, si el Estado Chileno continúa avanzando hacia el desarrollo, la evidencia internacional permite asumir que enfrentará con mayor frecuencia la acción de algunos de los ciberactores mencionados.

La estimación de la ciberamenaza será la principal guía para planificar la respuesta nacional, por tanto ésta debería incluir los siguientes conceptos. En primer lugar, convendría considerar el amplio espectro de actores que han desarrollado acciones contra el Estado Chileno, principalmente hacktivistas y cibercriminales, y los que han protagonizado incidentes en el nivel internacional. Además, debería incorporar la interacción entre los diferentes actores, tanto la relación entre Estados y grupos no estatales y estos últimos con otras amenazas emergentes. En segundo lugar, correspondería analizar todos los métodos y objetivos que se han identificado en los últimos eventos y así permitir la

programación de distintas respuestas nacionales. Por último, se debe catalogar la ciberamenaza entre actividades de explotación de redes, ciberespionaje, cibercriminal y ataques propiamente tal a redes informáticas y/o sistemas de control industrial. Un enfoque integral que incluya todos estos aspectos, permitiría comprender la complejidad del fenómeno y los retos que plantea a nuestra Nación.

La apreciación tendría que ser priorizada conforme a la realidad nacional y su probable evolución. Es decir, los ciberataques o el espionaje que han afectado a organizaciones estatales y empresas privadas debieran ser considerados como los de mayor riesgo e inminencia. Asimismo, los acontecimientos que están ocurriendo en otras regiones del mundo deberían ser incluidos como potenciales peligros que pudieran materializarse en el futuro cercano.

Por último, sería relevante indicar los principales intereses nacionales que serían objetivos potenciales de acciones en el ámbito del ciberespacio, tanto en tiempo de paz como en crisis o conflicto. Además, señalar los efectos previsibles que la ciberamenaza podría tener contra activos económicos vitales y servicios públicos, con el objetivo de generar las medidas preventivas, de respuesta y remediales con respecto al tema.

Este breve análisis y consecuentes proposiciones buscan ser un aporte para desarrollar una evaluación actualizada y completa sobre la ciberamenaza que enfrenta y afrontará el Estado chileno. Una apreciación realista y contextualizada sobre este nuevo dominio en el escenario de seguridad nacional e internacional facilitaría la respuesta nacional. En el ciberespacio la ventaja está de lado del que ofende y los Estados deben ser previsores para disminuir esa brecha.

Referencias Bibliográficas

Carr, J. (2010). *Inside Cyber Warfare*. O'Reilly Media.

Clarke, R. y Knake, R. (2010). *Cyber War, the next threat to National Security and what to do about it*. Editorial Ecco.

Economist Intelligence Unit & IBM. (2010). *Digital economy rankings 2010: Beyond e-readiness*.

Gobierno de Australia. (2012). *The Australian National Security Strategy*.

Gobierno del Reino Unido. (2010). *The United Kingdom National Security Strategy*.

Gobierno del Reino Unido. (Nov. 2011). *The UK Cyber Security Strategy*.

Mandiant. (2014). *APT1 Exposing One of China's Cyber Espionage Units. Intelligence Report.*

McAfee & Center for Strategic and International Studies. (2014). *Net Losses: Estimating the global cost of Cybercrime*.

Ministerio de Defensa de Chile. (2012). *Estrategia Nacional de Seguridad y Defensa de Chile*.

Presidencia de Estados Unidos. (2010). *The United States National Security Strategy*.

http://diario.elmercurio.com/detalle/index.asp?id=%7B37c95938-4e8b-48d9-97e2-886d3d3668df%7D

http://elcomercio.pe/actualidad/791354/noticia-anonymous-lanzara-ciberataques.

http://news.bbc.co.uk/hi/spanish/latin_america/newsid_7395000/7395288.stm.

http://unpan3.un.org/egovkb/datacenter/CountryView.aspx

http://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-to-sony-hack-lawmaker-says.

http://www.elmostrador.cl/pais/2014/08/14/hackers-peruanos-vulneran-seguridad-de-la-fach-y-filtran-cientos-de-correos-electronicos-de-la-institucion/

http://www.emol.com/noticias/tecnologia/2012/09/13/560281/chile-entre-los-paises-que-sufre-mas-ciberataques-en-america-latina.html.

http://www.foxnews.com/story/2008/08/13/russian-hackers-attack-georgia-in-cyberspace/

http://www.independent.co.uk/news/uk/home-news/bbc-says-feared-isis-cyber-attack-during-live-news-broadcast-was-actually-operational-error-10167537.html

http://www.latercera.com/noticia/nacional/2012/07/680-475213-9-anonymous-lanzo-operacion-operacion-chile2012-contra-sitios-chilenos.shtml.

http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=2

http://www.policia.cl/paginas/brigadas/bg-bricib/bg-bricib.htm.

http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

http://www.un.org/apps/newsstory.asp?Cr=cyber&NewsID=40692#.UXR6xitAQW9.