Revista de Marina Nº 965, pp. 45-48
ISSN 0034-8511

CIBERSEGURIDAD Y CIBERDEFENSA: PRIORIDAD NACIONAL POSTERGADA

Óscar Aranda Mora*

Resumen

El autor -con experiencia profesional en el tema- hace una comparación entre los ataques físicos y cibernéticos para así definir la ciberseguridad y la ciberdefensa; en base a ellas reflexiona sobre las responsabilidades que caben a los distintos actores, desde los individuos hasta el Estado; profundiza luego sobre la vinculación entre la inteligencia y la cibernética y finalmente propone algunas soluciones al problema que estima como una prioridad nacional.

Palabras clave: cibernética, ciberseguridad, ciberdefensa, inteligencia, hackers, informática.

Aunque estamos advertidos del reciente robo informático ocurrido al Banco de Chile, igual que sus directores y clientes, probablemente nunca sabremos la cantidad real que fue robada. Quizás ni el mismo banco la conozca con exactitud. El banco acepta solamente un robo de 10 millones de dólares y resultaría comprensible que lo minimice: después de todo, la confianza de los depositantes es el atributo más preciado de un banco, porque ¿quién querría depositar sus ahorros en un banco inseguro?

Realmente, si sólo han sido robados los 10 millones que el Banco de Chile acepta, los directores quizás supongan que invirtiendo adicionalmente en ciberseguridad una fracción de lo robado, hubiesen evitado el robo. Esto, sin considerar -claro- que desde el año 2013 hay casos documentados a nivel mundial de robos SWIFT[1], empleando técnicas informáticas similares. Por eso, el caso del Banco de Chile deja al descubierto no sólo las falencias en ciberseguridad del propio banco, sino que además la carencia de una política efectiva de ciberseguridad a nivel nacional. Y es que, en Chile, hasta ahora, el Estado ha abdicado de brindarle ciberseguridad no sólo a sus ciudadanos, sino que -peor aún- a la infraestructura crítica nacional, como quiera que ésta se defina.

Lo que sucedió no es un fenómeno exclusivamente nacional. Según estimaciones internacionales, las pérdidas anuales por el cibercrimen oscilan entre el 0,8 y el 1% del PGB mundial y FORBES vaticina que para el 2019 el costo del cibercrimen mundial alcanzará 2.000 billones de dólares.

Ataques físicos y ataques cibernéticos: un paralelo

Existe un paralelo entre las medidas de seguridad anti-robos y la cibernética. En efecto, cada uno de nosotros ha adoptado medidas de

* Contraalmirante . Magíster en Ciencias Navales y Marítimas. (oscararandam@hotmail.com).
1. Entre los años 2015 y 2017 se reportaron ciber ataques similares a bancos en Bangladesh, Vietnam, Ecuador y Rusia, atribuidos a un grupo denominado Lazarus, posiblemente de origen estatal norcoreano. Para esto, se intervino el software SWIFT, que permite efectuar transacciones bancarias internacionales, generando transacciones en favor de cuentas de los atacantes e impidiendo que estas transacciones originen reportes, lo que las oculta.

seguridad para prevenir robos y así protegernos de la acción delictiva. Además, en nuestro hogar practicamos algunas medidas anti-delincuencia, como cerrar las puertas, no abrir a desconocidos, etc. Y aunque nosotros nos protegemos del robo mismo, esperamos que el Estado se encargue de perseguir a los ladrones. Pues bien, en el ámbito cibernético esta analogía es aplicable: cada cual es responsable de protegerse de los ciber-ataques. Esto es lo que se conoce como ciberseguridad y es de responsabilidad individual. Dentro de este ámbito están los antivirus, los *firewalls*, las buenas prácticas informáticas, etc. Sin embargo, esto no es suficiente. Alguien debe preocuparse de perseguir al criminal, en este caso al *hacker*, o como quiera que se denomine a quien pretenda vulnerar nuestra seguridad informática. El ámbito de dicha persecución además se relaciona con la diseminación a nivel nacional de alertas de amenazas, con el intercambio internacional de informaciones, con el análisis y neutralización de las técnicas empleadas y también con actuar proactivamente, para detectar oportunamente a los atacantes e incluso para disuadirlos. Atacar en Chile a un banco, a su Estado o a sus instituciones no debiera salirle gratis a nadie. Este es el ámbito de la ciberdefensa, que es -o mejor dicho, que debiese ser- una responsabilidad estatal. Sin descartar que la ciberdefensa también posee otro aspecto, relacionado con el empleo del ciberespacio con los propósitos propios de la defensa nacional, dentro de los que la protección de la infraestructura crítica no puede descartarse. Esperar en el siglo XXI que otro estado nos declare la guerra para emplear nuestras instituciones militares en la defensa de elementos vitales de Chile es -a lo menos- ingenuo.

La nueva cara del cibercrimen

Apenas se comenzó a emplear el ciberespacio -ese conjunto de terminales, de redes físicas y electromagnéticas, y de contenido informático- para propósitos sociales y económicos, surgió el cibercrimen, principalmente en tres expresiones: el cibercrimen financiero; el ciberabuso, principalmente infantil; y la intrusión en redes con propósitos tan variados como censurables. Sin embargo, por el ingreso de actores estatales por una parte y del crimen organizado por otra, hoy los ilícitos cibernéticos han mutado. Ya no debe pensarse que el autor del ilícito cibernético es un joven algo *nerd*, que come pizza y que desde su garage ataca al Pentágono, a usted o a

un banco. Hoy, algunos estados, los movimientos terroristas y poderosas organizaciones criminales trasnacionales emplean el ciberespacio para sus propósitos. Y estos propósitos incluyen el ataque financiero a gran escala (mucho más que los 10 millones de dólares que el Banco de Chile declara); influenciar a la opinión pública a través de las redes sociales; el traspaso oculto de grandes sumas de dinero para blanquear divisas o disponibilizarlas para el terrorismo; el espionaje industrial y militar, la pornografía infantil, etc. Estamos viviendo la etapa 2.0 de los ilícitos cibernéticos y ya no basta con que usted, que el Banco de Chile, o que yo mismo reforcemos nuestra ciberseguridad. El Estado, ese que nosotros financiamos, debe concurrir a nuestra protección.

Ciberdefensa: ¿quién y a qué?

Hecha la diferencia entre ciberseguridad y ciberdefensa, y comprendiendo el rol del Estado en esta última, conviene meditar respecto de quiénes son los actores comprometidos y cuáles los bienes a proteger. Lo primero que hay que proteger -sin duda- es lo vital, o crítico para el país. En otras palabras, aquello que requerimos, porque su interrupción puede dañarnos grave e inmediatamente. Dentro de esta categoría cae, por ejemplo, nuestra matriz energética y de agua potable; nuestros servicios hospitalarios (suponiendo que éstos hoy dependan vitalmente de las redes informáticas); nuestro sistema bancario; parte de nuestra red de telecomunicaciones y algunas cosas más. No muchos, quizás dos o tres docenas de sistemas y servicios, porque si pretendemos proteger todo, no protegeremos nada. Ellos constituyen la infraestructura crítica nacional y son el activo principal que defender por nuestro sistema nacional de ciberdefensa.

Luego vienen los sistemas y servicios importantes, aquellos cuya interrupción afecta grave pero no vitalmente a nuestras vidas: los medios de comunicación, el sistema de transportes, la industria productiva (que va quedando), etc. Este es un segundo nivel de protección, muchísimo más amplio, que debiera ser considerado por nuestra ciberdefensa, principalmente fijando estándares obligatorios de ciberseguridad y estableciendo protocolos de comunicación para alertarlos e intercambiar información con ellos. Por último, está el resto de los usuarios cibernéticos, que son beneficiados por la difusión de alertas informáticas y de buenas prácticas para establecer una cultura de ciberseguridad, que hoy debiese -al menos- inculcarse desde la educación primaria. En ese nivel estamos usted y yo, así como todas las actividades nacionales que empleen el ciberespacio.

Respecto de los actores estatales involucrados, es preciso separar aguas: por un lado, al Ministerio del Interior sin lugar a dudas le cabe un rol en el combate del cibercrimen, como otra forma más de delincuencia. La Agencia Nacional de Inteligencia, por ley también tiene un papel que jugar en este tema. Además, las FF.AA. poseen capacidades y un rol a jugar en ciberdefensa, para defendernos de otros actores estatales que empleen el ciberespacio con propósitos contrarios al interés nacional. Y en este aspecto, países tales como Corea del Norte, Rusia, China y otros, han sido reconocidos mundialmente por sus actividades ilícitas en el ciberespacio con propósitos de espionaje militar e industrial, de ataque a centros financieros y de influencia de la opinión pública a través de la red, ¡lo que no es una fake news, como pretende -a su conveniencia- el presidente Trump! Conjugar armoniosamente a estos actores junto al sector privado en el diseño de una arquitectura nacional de ciberdefensa y de ciberseguridad es el desafío que otros países como Estados Unidos, Israel y el Reino Unido han enfrentado, con soluciones ajustadas a cada realidad. Diseñar una para nuestro Chile es el desafío actual.

Inteligencia y cibernética

Existe, además, una estrecha relación entre la actividad de inteligencia y la cibernética. Mal que mal, en la naturaleza misma de ambas actividades reside el manejo de información. Por lo que el legislador, ya en la ley 19.974 de 2004, asignó a la Agencia Nacional de Inteligencia la función de "Proponer normas y procedimientos de protección de los sistemas de información crítica del Estado" (Ley 19.974, Art. 8° letra c)) ¡Todo un acierto de

nuestros legisladores! Además, el esfuerzo de ciberdefensa se beneficia de la recolección, del análisis y de la difusión de informaciones relacionadas con probables atacantes informáticos y sus procedimientos técnicos, lo que constituye una tarea de inteligencia. Esto, sin mencionar que las actividades clásicas de inteligencia: el espionaje, el sabotaje, la subversión y la insurgencia, se benefician de la cibernética, que ha potenciado a la inteligencia al brindarle un ciberespacio sin fronteras, con acceso directo a sus objetivos, y abundante información disponible.

¿Qué hacer?

Organizar la ciberdefensa a nivel nacional es un desafío urgente. Cabe mencionar que a la ciberdefensa le otorgamos un significado amplio, que excede el empleo militar del ciberespacio con los propósitos de la defensa nacional. La ciberdefensa del siglo XXI tiene que ver con la respuesta estatal a la amenaza cibernética sobre la estructura crítica nacional y sobre sus ciudadanos, amenaza desarrollada por actores poderosos, imposibles de enfrentar aisladamente por actores privados o estatales.

Sin embargo, no abogamos ni por la militarización de la ciberdefensa, encargándola a los militares exclusivamente, ni por la atomización de la ciberseguridad, reduciéndola a medidas pasivas aisladas, carentes de una coordinación central y sin actuar proactivamente, privándola así de efectividad y de la capacidad de disuasión de eventuales agresores.

Aprovechando la normativa legal y las capacidades existentes, debe propiciarse la creación de centros sectoriales de respuesta a incidentes informáticos (CIRT por su sigla del inglés Computer Incident Response Team), algunos privados y otros estatales. Los centros privados y estatales civiles, podrían coordinarse a través de un centro de seguridad informática (SOC por su sigla del inglés Segurity Operation Center) radicado en el Ministerio del Interior; mientras los militares, en otro SOC ubicado en el Ministerio de Defensa o alguna repartición dependiente. La Agencia Nacional de Inteligencia (ANI) podría, por ejemplo, poseer el centro de seguridad de operaciones informáticas del más alto nivel nacional, sirviendo de nexo entre lo militar y lo civil, efectuando contactos con agencias similares de otros países, y coordinando las actividades cibernéticas de defensa y de obtención de informaciones a nivel nacional. Así la ciberdefensa a nivel nacional se beneficiaría de la cooperación de los elementos de ciberseguridad civil, privada y militar existentes, podría actuar proactivamente y gozar del intercambio de informaciones y alertas entre ellos y con países aliados.

A manera de epílogo

El robo del Banco de Chile quizás tenga algún efecto positivo, ya que visibilizó una carencia nacional, que aunque parece haber sido detectada, tanto a nivel defensa como del Ministerio del Interior, no ha contado con la prioridad que merece. La ANI, que hoy busca redefinirse y modernizar el sistema de inteligencia, ahí tiene otro aspecto desatendido de sus funciones y relacionado con la inteligencia. Además, si pensamos en la rentabilidad social de un proyecto de ciberdefensa a nivel nacional, su costo es ínfimo considerando el retorno en términos de PIB. La contribución de la ciberdefensa a la seguridad de Chile, de sus habitantes y de su economía, bien vale la pena un esfuerzo, incluso en desmedro de otras formas convencionales de defensa.

Y, a decir verdad, el Banco de Chile no fue sólo víctima de sus probables fallas en ciberseguridad, sino de una deficiencia sistémica nacional en este aspecto. Esto, para que sirva de consuelo a su directorio, accionistas y ahorrantes, que hoy pagan el costo declarado de 10 millones de dólares.

* * *