DESCUBRIENDO LA AGENDA DE CIBERSEGURIDAD DE AMÉRICA LATINA. EL CASO DE ARGENTINA

PRIMERA ENTREGA

1

¿Qué entendemos por ciberseguridad?

ADC / Asociación por los Derechos Civiles

Área de Privacidad

ADC / Asociación por los Derechos Civiles

CYBER STEWARDS

Octubre de 2015

www.adc.org.ar

Fue realizado como parte del trabajo de la ADC en la Cyber Stewards Network, en el marco de un proyecto financiado por el International Development Research Centre, Ottawa, Canada.

creative commons

Fue publicado en octubre de 2015.

Índice

Descubriendo la agenda de ciberseguridad de América Latina: El caso de Argentina

Primera Entrega: ¿Qué entendemos por ciberseguridad?*

1. El Proyecto

Las discusiones acerca de Ciberseguridad se están desarrollando en contextos internacionales como el de la Organización de Estados Americanos (OEA) y sus programas, sin participación de la sociedad civil y sin considerar la perspectiva de protección de los derechos humanos. Por su parte, estas discusiones también están teniendo lugar en las agendas nacionales, con temas tales como la seguridad del Estado, los mecanismos de inteligencia y las prácticas de vigilancia.

Los trabajos de investigación que ha venido desarrollando ADC, Derechos Digitales y otras organizaciones civiles de la región sobre el tema nos permite describir el siguiente escenario: las prácticas de vigilancia en el Cono Sur, especialmente aquellas ligadas a actividades de inteligencia, no están alineadas con una perspectiva amplia de derechos humanos, no tienen adecuado control y son usualmente fuente de conductas ilegales que terminan violentando derechos de los ciudadanos o debilitando el sistema democrático y sus instituciones. Esto así pues hay países de Latinoamérica que cuentan con marcos legales que les permiten obtener información de sus ciudadanos en forma masiva y lo que es más grave, los organismos encargados de la recolección de esta información, de la interceptación de las comunicaciones, de las tareas de vigilancia y ciberseguridad son usualmente heredadas de gobiernos dictatoriales. Esta herencia por lo general significa métodos opacos, recolección desproporcionada de información, secreto excesivo, falta de transparencia y una larga experiencia en violaciones a derechos humanos que han quedado impunes.

Esta primera entrega corresponde a una serie de tres documentos que iremos publicando con frecuencia bimestral y se enmarca en un proyecto de investigación cuyo

*Este informe fue elaborado por el área de Privacidad de la ADC.

resultado final será publicado durante la segunda mitad de 2016 y que tiene por objetivo principal determinar la existencia y contenido de la agenda de ciberseguridad en Latinoamérica, con especial foco en el caso argentino, para determinar luego su correspondencia con estándares protectorios de derechos humanos y en su caso, efectuar las sugerencias o recomendaciones pertinentes.

2. Ciberseguridad: una primera aproximación

Antes de comenzar a desarrollar el panorama actual de la ciberseguridad en Argentina, nos hicimos esta primera pregunta: ¿Qué es ciberseguridad?

Así encaramos la búsqueda de una definición, en el entendimiento de que encontrarla nos daría el marco dentro del cual se desenvuelve la temática y nos facilitaría la interpretación -más restrictiva o más laxa- de sus alcances y de los diversos elementos que deben tenerse en cuenta al hablar de ciberseguridad.

Sin embargo no fue tan sencillo como podría parecer. En nuestro país no hay todavía una definición consensuada o adoptada unánimemente por los organismos estatales.

De tal suerte, cambiamos el enfoque y buscamos una definición de ciberseguridad en otros entornos nacionales e internacionales.

Pudimos advertir que si bien los intentos por acordar internacionalmente cuestiones relacionadas con Internet y la tecnología no son nuevos, con el debate de la ciberseguridad algunos problemas parecen haberse acentuado. Ello es así ya que los Estados tienen intereses distintos, ya sea sobre cómo debe regularse una actividad, sobre cuál debería ser su conceptualización y alcances, y sobre qué actividades podrían constituir delitos. Es por esto que llegar a un acuerdo sobre una definición resulta una tarea compleja, en la cual se deben considerar múltiples factores. El concepto de ciberseguridad parece estar en pleno desarrollo y una definición precisa ocultaría el hecho significativo de que el concepto, en sí, es objeto de disputas entre distintas miradas, perspectivas e intereses.

Por ello comenzamos a analizar algunos de estos factores y comparamos conceptos utilizados por varios países y por organismos internacionales, en el afán de establecer pautas de análisis que nos permitan comenzar a abordar y entender la agenda de ciberseguridad argentina, para luego establecer su adecuación con estándares protectorios de derechos humanos.

3. Factores que incidieron en su desarrollo

a. Del almacenamiento a bajo costo al lema "recolectar todo"

La tecnología en el campo del almacenamiento de datos ha dado en los últimos años pasos de gigante en su carrera por abaratar el costo de producción y del producto final. Así, a finales del año 2000, el costo promedio de 1 Gigabyte en almacenamiento era de 10 U$D; para el año 2005, el promedio había bajado a 1 USD y, actualmente, a finales de 2015, el promedio por GB es de menos de 5 centavos de dólar.

Las empresas y también los gobiernos comenzaron a darse cuenta que no era necesario deshacerse de toda la información que recolectaban de sus usuarios, con la excusa de nunca saber cuándo la necesitarían en el futuro y sobre todo porque ya no tenían que lidiar con altos costos de almacenamiento.

Los Estados también se vieron involucrados en este cambio de paradigma del almacenamiento de información, aún mediante el uso de prácticas que pueden ser consideradas netamente ilegales.

El caso más emblemático, y que se perfila como el más importante de la década, fue aquel denunciado por Edward Snowden (ex-analista de la NSA) en el año 2013, quien filtró miles de documentos que ponen de manifiesto los programas llevados a cabo por la Agencia Nacional de Seguridad (National Security Agency) de Estados Unidos y de la Oficina Central de Comunicaciones Gubernamentales (Government Communications Headquarters) que tienen como actividad primordial el almacenamiento masivo e indiscriminado de información, todos con plazos distintos. Por ejemplo, 3 días para el contenido de llamadas y emails bajo el programa XKEYSCORE; 1 año para el historial de navegación bajo el programa MARINA; y 5 años para los metadatos de llamadas telefónicas; todo esto sin olvidar que cuando un analista utiliza de alguna manera datos almacenados, su plazo de retención pasa a ser ilimitado. Este es el reflejo del lema de la NSA, "*Recolectarlo todo. Saberlo todo*".

b. Fácil adquisición de herramientas de vigilancia masiva

Sumado al factor sobre el almacenamiento de datos de los ciudadanos, encontramos a su vez que las herramientas de vigilancia masiva son cada vez más fáciles de adquirir, pues su desarrollo ha dejado de ser de exclusivo monopolio militar o estatal. El caso más reciente es el de la empresa italiana Hacking Team, conocida por vender software espía y utilidades para el acceso remoto a dispositivos electrónicos y que a partir del hackeo a sus bases de datos internas y la publicación de más de 400GB de información, pudo conocerse la existencia de relaciones comerciales de esta empresa con gobiernos de distintas regiones del mundo e incluso con regímenes autoritarios sancionados por la comunidad internacional. La presencia de Hacking Team en América Latina también

es muy fuerte, en países como México, Chile, Colombia, Ecuador, Honduras y Panamá, llegando además a sostener ciertas conversaciones en Argentina[1].

Pero Hacking Team es sólo una de las participantes dentro de un negocio mucho más grande y multimillonario dedicado a la comercialización de software de interceptación de comunicaciones y vigilancia. Así podemos nombrar a la empresa estadounidense Blue Coat, principal distribuidora de la NSA y también con presencia en Argentina; Gamma International, una empresa anglo-germana conocida por su solución de software FinFisher, también llamado FinSpy; la empresa francesa Vupen Security; la empresa israelí NSO Group, conocida competidora de Hacking Team, con su software Pegasus; y la empresa alemana Utimaco.

La facilidad al acceso de herramientas de vigilancia es una cuestión que debemos analizar como bidireccional. En este sentido, las agencias y dependencias gubernamentales, así como las corporaciones privadas, tienen la posibilidad de adquirir sin demasiados problemas burocráticos o barreras legales este tipo de productos, aún cuando los adquieran a precios que lejos están de ser irrisorios. Esta circunstancia también tiene incidencia en el esquema de relación entre estados "contrarios" para ilustrarlo, sirve el ejemplo USA - Rusia) y de las empresas privadas que compiten entre sí por esta "clientela".

Una de las consecuencias directas de este juego de relaciones generado por la facilidad en el acceso y adquisición de estas tecnologías es el alto riesgo para todas las partes involucradas.

Es en este escenario complejo en el que se evidencia el papel fundamental de la ciberseguridad en relación a la protección de las infraestructuras que manejan información y datos sensibles, entre otras.

4. Analizando el concepto de Ciberseguridad

Al analizar qué se entiende por ciberseguridad, descubrimos entonces tres aspectos en los cuales podríamos dividir el enfoque de la definición, que varían de acuerdo a los fines de quien hace uso del término.

- Ciberseguridad como la protección o defensa de las infraestructuras de un Estado, sus redes, datos y usuarios;
- Trabajo que realizan las fuerzas de seguridad en investigación, prevención y acción contra delitos en el ámbito digital (cibercrimen);
- Actividad de vigilancia llevada a cabo por los organismos de inteligencia.

[1] ADC Alerta: Software de interceptación y vulneración a los derechos humanos. Agosto 2015. Disponible en (PDF): *http://www.adc.org.ar/wp-content/uploads/2015/08/Software-de-interceptacion-y-DDHH.-Informe-ADC.pdf*

Podemos hacer esta triple distinción ya que aún no hay un concepto definido de lo que es ciberseguridad a nivel global, ni mucho menos a nivel regional en América Latina.

Aún así, organismos internacionales han avanzado en la discusión sobre el tema ensayando sus propias definiciones.

La Unión Internacional de Telecomunicaciones (UIT), organismo especializado de la Organización de las Naciones Unidas (ONU) para las tecnologías de la información y la comunicación, determinó una definición de ciberseguridad en la Recomendación UIT-T X.1205[2], luego aprobada con la Resolución 181[3], que establece (el resaltado es propio):

> "La ciberseguridad es el conjunto de *herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno*. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios y los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedias, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad".

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), de la Organización de los Estados Americanos (OEA), estableció en su publicación Libertad de expresión e Internet que "El concepto de ciberseguridad suele emplearse como un término amplio para referirse a diversos temas, desde la seguridad de la infraestructura nacional y de las redes a través de las cuales se provee el servicio de Internet, hasta la seguridad o integridad de los usuarios. No obstante, desarrollos posteriores sugieren la necesidad de limitar el concepto exclusivamente al resguardo de los sistemas y datos informáticos. (…) este enfoque acotado permite una mejor comprensión del problema así como una adecuada identificación de las soluciones necesarias para proteger las redes interdependientes y la infraestructura de la información"[4].

---

[2] UIT. Recomendación UIT-T X.1205. Abril de 2008. Disponible en: *https://www.itu.int/rec/T-REC-X.1205-200804-I/es*

[3] UIT. Resolución 181. Noviembre de 2010. Disponible en: *https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx*

[4] OEA. CIDH. Libertad de expresión e Internet. 31 de diciembre de 2013. Disponible en (PDF): *https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf*

Como también mencionó la Relatoría, lo que se busca evitar con un enfoque acotado en el concepto de ciberseguridad es la posible criminalización del uso de Internet, motivo por el cual "(…) la respuestas de los Estados en materia de seguridad en el ciberespacio debe ser limitada y proporcionada, y procurar cumplir con fines legales precisos, que no comprometan las virtudes democráticas que caracterizan a la red".

Cabe destacar que si bien la OEA tiene un Programa de Seguridad Cibernética, con el objetivo de -entre otras cosas- ayudar a los Estados miembros a adoptar estrategias nacionales de seguridad cibernética, no brindan un concepto propio de ciberseguridad, por más que sus informes desarrollan el tema en relación a buenas prácticas y reportes regionales sobre el estado de la ciberseguridad.

En el continente americano son varios los países que ya han implementado políticas nacionales de ciberseguridad o están trabajando en ellas. Canadá[5] plantea como eje para su estrategia de ciberseguridad no solo asegurar los sistemas de información gubernamentales y mantener alianzas que los ayudan a asegurar sistemas externos al gobierno, sino también ayudar a sus ciudadanos a navegar y hacer un uso seguro de Internet, dentro de lo cual incluyen pelear contra el cibercrimen, esto implica equipar a las fuerzas de seguridad con recursos modernos y obligar a los proveedores de Internet a que mantengan sistemas de intercepción para que se les pueda solicitar, mediante orden judicial, interceptar las comunicaciones de un determinado objetivo dentro del marco de una investigación, además de brindar información sobre sus usuarios.

Si vamos al caso de países europeos, Francia[6] por ejemplo también trabaja en base a un concepto amplio de ciberseguridad, ya que no solo está enfocado a la protección contra vulnerabilidades de aquellos sistemas que almacenan, procesan y transmiten datos, sino también a hacer uso de las técnicas de los sistemas de seguridad de la información para combatir el cibercrimen y establecer la ciberdefensa del país.

5. Concepto de Ciberseguridad en Argentina

Los primeros pasos dados en esta investigación nos mostraron que el término ciberseguridad aparece inserto en alguna normativa. Por ejemplo:

En el año 2011, la Jefatura de Gabinete de Ministros emitió la Resolución N° 580/11[7] mediante la cual creó el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC). Este fue el primer documento legislativo que invocó el

---

[5] Public Safety Canada. Cyber Security Strategy. Disponible en (PDF): *http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf*

[6] UIT. Estrategias Nacionales de Ciberseguridad. Francia. Disponible en (PDF): *http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/France_2011_2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf*

[7] Resolución 580/2011. Disponible en: *http://www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm*

término ciberseguridad, pero no brindó ni brinda ningún tipo de definición. A cuatro años de su creación, son varios los sectores del Estado que han trabajado en la implementación de lo que establece la normativa, pero como dicha resolución estableció solamente pautas orientadoras cada dependencia del Estado tiene la facultad de adoptarlas como mejor considere.

La repartición encargada del desarrollo del programa ICIC es la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad[8], dependiente de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad, que a su vez depende de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros.

Sin embargo, ni en las resoluciones y decretos que regulan ICIC, ni en su sitio oficial[9], se encuentra explicado qué concepto de ciberseguridad es utilizado como marco para el desarrollo de sus actividades, y a diferencia de los países mencionados previamente, Argentina no cuenta con una estrategia nacional de ciberseguridad documentada de tal forma que pueda accederse a ella públicamente.

Por su parte, el 6 de julio de 2015 se aprobó la Nueva Doctrina de Inteligencia Nacional a través del Decreto N° 1311/2015,[10] que estableció el marco normativo del Sistema Nacional de Inteligencia y fundamentalmente del funcionamiento de la Agencia Federal de Inteligencia (AFI).

En su segundo capítulo, referido a "Dimensiones y Actividades de la Inteligencia Nacional", la Doctrina estableció que la inteligencia criminal comprende la "producción de inteligencia referida a las problemáticas delictivas y, en particular, a aquellas problemáticas delictivas complejas de relevancia federal relativas al terrorismo, los atentados contra el orden constitucional y la vida democrática, la criminalidad organizada y los atentados contra la ciberseguridad".

Por otra parte, en la "Estructura Orgánica y Funcional de la Agencia Federal de Inteligencia", dentro de la misma Doctrina, el artículo 49 introdujo la Dirección Operacional de Inteligencia sobre Ciberseguridad, que "tiene a su cargo la producción de inteligencia orientada al conocimiento de las acciones que atenten contra la ciberseguridad en el marco de la defensa nacional o la seguridad interior, y de los grupos nacionales o extranjeros responsables de llevarlas a cabo" y está compuesta por la "Dirección de Inteligencia Informática" y "Dirección de Inteligencia sobre Delitos Informáticos".

Dicho artículo agregó finalmente que la Dirección Operacional de Inteligencia sobre Ciberseguridad está pensada para el desarrollo de actividades de recolección, gestión

---

[8] Decreto 1067/2015. Disponible en: *http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm*

[9] Cfr. http://www.icic.gob.ar/ consultado en 28/10/2015

[10] Decreto 1311/2015. Disponible en: *http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm*

y análisis de información, integrada por oficiales y analistas especializados en ciberseguridad.

Una vez más, y a pesar de las reiteradas menciones del término, el texto no contiene una definición ni concepto que establezca qué es ciberseguridad para el Sistema de Inteligencia Nacional.

6. Conclusiones parciales

Podemos resumir nuestras primeras reflexiones en las siguientes líneas:

- La dificultad y el desafío que supone establecer una definición de ciberseguridad. Esto se debe a que el concepto se encuentra en pleno desarrollo y disputado por diversas perspectivas e intereses.
- Las implicancias que para los derechos humanos podrían derivarse de la eventual adopción de una definición amplia o acotada del término ciberseguridad. En efecto, y de manera similar con lo que ocurre con el concepto de seguridad nacional, consideramos que las definiciones que eventualmente puedan adoptarse sobre el punto deberán partir de una perspectiva de derechos humanos.
- La falta de terminología clara, que ilumine y permita establecer alcances y limitaciones de las acciones del estado argentino en materia de ciberseguridad podría tener como desafortunadas derivaciones la superposición e incluso contradicción en criterios de implementación entre las diferentes reparticiones, la adopción de medidas discrecionales por parte de funcionarios de turno sin ningún tipo de control o supervisión, mantenimiento de prácticas opacas y falta de transparencia y, en definitiva, la generación de un escenario propicio para la vulneración de derechos humanos.

1

ADC / Asociación por los Derechos Civiles