ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

79/2015 24 de julio de 2015

*Paul-Edouard Martin**

INSEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA: LÍNEAS DE REFLEXIÓN PARA LA EVALUACIÓN DE RIESGOS

INSEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA: LÍNEAS DE REFLEXIÓN PARA LA EVALUACIÓN DE RIESGOS

Resumen:

En un contexto en el cuál se acentúa el carácter estratégico de la información, que concierne la atribución de mercados públicos, relaciones diplomáticas o la protección del capital inmaterial de las empresas, el control de la "información crítica" constituye un reto cada día más fundamental para las organizaciones. Entre los esfuerzos necesarios destaca la adaptación de las estrategias de seguridad en el momento de iniciar un proyecto de internacionalización, de la misma manera que con otros riesgos políticos vinculados a normas legales o fenómenos como movimientos sociales, clientelismo y corrupción o criminalidad organizada. Elaborar tales estrategias para cada tipo de organización necesita, como prerrequisito, un conocimiento del contexto. En el caso latinoamericano, este ejercicio aparece como muy complejo por una diversidad de razones entre las cuales la heterogeneidad de las situaciones nacionales y la escasez de información pública disponible.

Abstract:

In a context in which information is getting increasingly strategic, which can be observed in the award of public contracts, in diplomatic relations or in the protection of companies' intangible capital, it is getting more and more essential for organizations to control "critical information". Among the different fields in which effort should be made, security strategies should be particularly adapted when an internationalization project is about to be initiated, as it is done with other political risks linked to legal norms or phenomena like social movements, cronyism and corruption or organized crime. So as to develop such strategies for each organization case, some previous knowledge of the context is necessary. As for Latin America, such an exercise appears to be quite complex for a certain amount of reasons among which the extreme diversity of national situations and the shortage of available public information.

Palabras clave:

Ciberseguridad – América Latina – Organizaciones – Niveles de riesgo – Panorama.

Keywords:

Cybersecurity – Latin America – Organizations – Levels of risk – Panorama.

INTRODUCCIÓN

Este artículo busca proponer unos primeros pasos para la definición de niveles y características de riesgo informático en los países de América Latina desde el punto de vista de las organizaciones. La creciente importancia del ciberespacio como dimensión donde se plantean problemáticas de seguridad explica la multiplicación, en la literatura académica, por un lado de trabajos teóricos sobre las lógicas estratégicas aplicables al ciberespacio y, por otro lado, de panoramas o estudios de casos más específicos. Este texto se integra en esta segunda categoría con la ambición de participar en la concepción de una base común a partir de la cual se facilita la evaluación de riesgos de cada organización y el diseño de respuestas adecuadas.

Si es cierto que el ciberespacio presenta características "ambiguas" que marcan una ruptura con las fronteras tradicionales hacia una "universalidad de los riesgos"[1], no hay por lo tanto que concluir a una repartición homogénea de aquellos en su seno. Al contrario, opinamos que, para una mayoría de los actores, el terreno cibernético presenta diferencias notables de estructura que, a su vez, impactan las condiciones de su seguridad. Las disparidades entre continentes, países e incluso regiones constituyen entonces elementos pertinentes que tomar en cuenta.

Para analizar el panorama de riesgos del Continente Latinoamericano, nos centraremos en tres ejes principales de vulnerabilidad: los usuarios de Internet, la estructura y organización del acceso a la web y los contenidos de todo tipo que circulan y se comparten en ella, con el objetivo de contestar a la siguiente pregunta: ¿En qué medida se puede afirmar que América Latina es un continente cibernéticamente inseguro?

No se busca proponer allí una visión objetivamente exhaustiva sino una serie de conclusiones que se pueden sacar de las informaciones actualmente disponibles y una reflexión sobre lo que puede y no puede constituir un criterio válido para la medición de este tipo de riesgos en América Latina.

I – AMÉRICA LATINA, UN CONTINENTE DESIGUALMENTE CONECTADO

Los usuarios, penetración de Internet en América Latina

A pesar de la pertinencia de los argumentos que señalan que el concepto de penetración de Internet se puede estudiar según las categorías sociales, la intensidad del uso de Internet o el porcentaje de usuarios expertos, nos centraremos en el porcentaje de usuarios respecto a la población total de los países. En efecto, esta variable tiene la doble ventaja de constituir un punto de referencia común y de poder cifrarse objetiva y fácilmente.

[1] KEMPF, Olivier. *Introduction à la Cyberstratégie*. Paris, Broché, 2012.

Los principales países de América Latina se pueden repartir en 4 grupos, según su grado de penetración de Internet como lo señala el siguiente mapa:

Porcentaje de usuarios de Internet en los países de América Latina en 2013.

Fuente: Elaboración propia a partir de las cifras 2013 de la International Telecommunication Union (ITU)

Ya podemos comprobar una notable disparidad en cuanto al porcentaje de usuarios de Internet en los países latinoamericanos. Esta realidad constituye un elemento importante del contexto que se debe tomar en cuenta en la evaluación de los riesgos cibernéticos.

Sin embargo, más allá de una mera medición del fenómeno de conexión a Internet de América Latina y del impacto que puede tener en aspectos de desarrollo y vida política ¿cuáles pueden ser los efectos de estas disparidades sobre el nivel de riesgo cibernético?

Se podría fácilmente avanzar que los países menos conectados experimentan un riesgo estadísticamente menor en su amplitud que los dónde la penetración de Internet ya se encuentra bastante avanzada por el simple efecto de un número de víctimas potenciales menor. Sin embargo, en los países menos conectados, los grandes ausentes son los usuarios individuales, especialmente los que están ubicados en periferias de la red de infraestructuras de comunicación, como en zonas rurales y espacios de extrema pobreza. Tiene como efecto lógico una sobrerrepresentación de los ataques focalizados en contra de instituciones privadas y públicas. Al contrario, en países muy conectados, la población se encuentra directamente implicada en las problemáticas de seguridad y puede tener un efecto sobre las acciones llevadas a cabo a través de su comportamiento individual y de la expresión de una demanda política. Finalmente, no se debe olvidar que, en algunos países, la definición como objetivo prioritario del desarrollo de la cobertura territorial a través de infraestructuras de comunicación vinculadas a Internet – clave para la obtención de un reconocimiento internacional y político - puede ocultar límites importantes a un verdadero compromiso a favor de la calidad de estas infraestructuras y de su seguridad.

El grado de penetración de internet en los diferentes países de América Latina es entonces una variable interesante porque entrega indicaciones válidas para medir el fenómeno de su desarrollo en el continente y las disparidades existentes. Sin embargo, sus efectos sobre la seguridad informática son indirectos y, por lo tanto, plantean la necesidad de una interpretación detallada para cada país que no puede verse sistematizada[2].

En el mundo actual, la seguridad cibernética no se limita al uso tradicional de Internet

Ante todo, es importante definir correctamente la realidad que aquí se busca estudiar, recordando, por ejemplo, que Internet no es, en ningún caso, un equivalente al ciberespacio. La definición adoptada por el Departamento de Defensa Estadunidense lo señala bastante bien: "[El ciberespacio es] un dominio global dentro del entorno de la información,

[2] Sin embargo, la regla según la cual un país que experimenta un desarrollo rápido y masivo de su número de usuarios de internet tiende a experimentar también, *ceteris paribus,* una proporción más alta de ciberataques parece confirmarse.

compuesto por una infraestructura de redes de tecnologías de la información interdependientes, que incluye Internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores"[3].

Evaluar riesgos cibernéticos no se limita entonces a elaborar una tipología de las amenazas presentes en Internet. Implica la necesidad metodológica de ir más allá, interesándose por el intercambio de informaciones fuera de esta red, por las infraestructuras físicas vinculadas a las tecnologías de la información y por los usuarios de manera detallada, o sea caracterizando sus comportamientos. Estos elementos explican la estructura y el planteamiento elegidos para este artículo que, justamente, intenta identificar tendencias y niveles de riesgos específicos a un continente.

Las estadísticas de uso de internet, nacionales como regionales, permiten determinar una tendencia clara. Los principales usos de la red por parte de los usuarios corresponden a sus funciones tradicionales y principales: búsqueda de información, correspondencia por email y uso de las redes sociales.

Las organizaciones tienen que manejar las problemáticas de seguridad vinculadas a estos usos "tradicionales" de la tecnología pero también a otros relativamente nuevos del ciberespacio que pueden tener impactos notables, directamente o vía efectos en cascada sobre su actividad. Entre estas novedades que tienen efectos sobre la dimensión estratégica de la seguridad informática encontramos, por supuesto, la omnipresencia cotidiana de infraestructuras y aparatos conectados. Tendencia que se encuentra subrayada en un informe de la OEA, especialmente en su parte titulada "Preocupaciones sobre los sistemas de control industrial".[4] Es un buen ejemplo de situación en la cual la ciberseguridad no corresponde al uso tradicional de internet. Además de poner en tela de juicio las representaciones comunes sobre el perfil de los atacantes y el desarrollo de su acción, plantea de una nueva forma las problemáticas de gestión del activismo político violento o de la criminalidad organizada en el seno del ciberespacio y sus potenciales repercusiones en el mundo físico. Finalmente, pone las organizaciones frente a una necesidad de rediseño de su estructura hacia una orientación menos compartimentada de su concepción de la seguridad, reto muy difícil de conseguir en algunas configuraciones estratégicas internas. Se puede referir aquí a los aportes de Crozier y Friedberg[5], especialmente en el capítulo titulado "El

[3] Department of Defense. *Dictionary of Military and Associated Terms*. Noviembre de 2010. Disponible en línea: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf . Fecha de la consulta 12.02.2015.

[4] OEA. Tendencias en la Seguridad Cibernética en América Latina y el Caribe y respuestas de los gobiernos. 2013 Disponible en línea: www.oas.org/es/ssm/cyber/documents/oastrendmicrolac_spa.pdf Fecha de la consulta 12.02.2015.

[5] CROZIER, Michel y FRIEDBERG, Erhard. *El Actor y el Sistema*, Editions du Seuil, 1977.

problema de la toma de decisión" dónde analizan empíricamente dos procesos de toma de decisión.

No se trata en este artículo de arriesgarse a tomar posición en el intenso debate sobre cómo – y si es posible - evaluar el coste de los delitos cibernéticos. Si se trata ciertamente de un dato importante para determinar la "rentabilidad" de las medidas de seguridad – particularmente para las organizaciones - cabe reconocer que esta evaluación está generalmente llevada a cabo por actores que, siendo profesionales de este sector, tienen intereses en obtener cifras precisas cuyo aporte se centra más en su *marketing* que en una reflexión rigurosa sobre riesgos y amenazas. Además, este ejercicio siempre entrega resultados discutibles porque su centro de gravedad metodológico se encuentra, antes del cálculo y de la recolección de los datos, en la elección inicial de lo que se integra – o no – en los costes de la delincuencia cibernética[6]. Sin embargo, sin hacer la economía de un necesario espíritu crítico, parece interesante tener presente a lo menos una idea de escala en cuanto a la magnitud de estos fenómenos. Así, un informe del LACNIC señala que, para el solo comercio electrónico, se puede determinar "como el límite inferior del monto del fraude un monto de 430 millones de dólares US." A lo largo del año 2011. Este monto llega hasta 1.100 millones de dólares de pérdidas por robos de identidad llevados a cabo a través de Internet[7].

Ejemplos de ataques en contra de infraestructuras se pueden encontrar en la actualidad latinoamericana, las más preocupantes siendo por supuesto las que implican vulnerabilidades mayores en la disponibilidad de energía, servicios de comunicación, recursos necesarios en el proceso productivo, etc. Aunque las infraestructuras de los países latinoamericanos presentan numerosos fallos de seguridad - algunas ni siquiera están protegidas por una contraseña[8] - este tipo de incidentes no son muy comunes. Sin embargo, existen antecedentes de tales ataques, como por ejemplo, las de gran magnitud que afectaron la red eléctrica de Paraguay en 2012. La multiplicación de los objetos conectados refuerza el carácter determinante de la seguridad cibernética, incluyendo progresivamente inmuebles, automóviles y hasta dispositivos domésticos.

[6] O sea, se debate la pertinencia de integrar solamente las pérdidas y el coste de las reparaciones y soluciones o también precauciones posteriores que se traducen por inversiones públicas como privadas, el efecto de baja del incentivo al consumo, evaluaciones de magnitud de los ataques no detectados, etc…

[7] LACNIC. Ciberdelito en América Latina y el Caribe – Una visión desde la sociedad civil. 2013. 150-153 Disponible en línea: http://tinyurl.com/l4p76j4 Fecha de la consulta 12.02.2015.

[8] OEA, opus citatum, 6.

Existen entonces por un lado ataques bien conocidos llevados a cabo a través o en contra de los usos "tradicionales" de los sistemas de la información y, por otro, ataques menos numerosos, pero que pueden tener impactos determinantes por efectos en cascada. Lo que lleva a interesarse de manera más especial por el estado de las infraestructuras de acceso a Internet en el continente.

Estado de las infraestructuras de acceso a Internet en el continente

Dado que este trabajo corresponde a un panorama general con escala continental, nos centramos en los equipamientos de mayor amplitud. Es, sin embargo, importante señalar que infraestructuras más locales pueden tener una gran importancia en la conexión de los países a Internet y en las problemáticas de seguridad experimentadas por los diferentes actores[9]

Entre los equipamientos más sensibles, se encuentran los cables de comunicación submarinos y sus puntos de aterrizaje. Generalmente, los operadores son los que deciden de la instalación de estas "autopistas de la información". Lo hacen en función de la evolución de los flujos de comunicación y sin necesariamente centrar sus proyectos en las implicaciones estratégicas para cada Estado de la configuración estas infraestructuras.

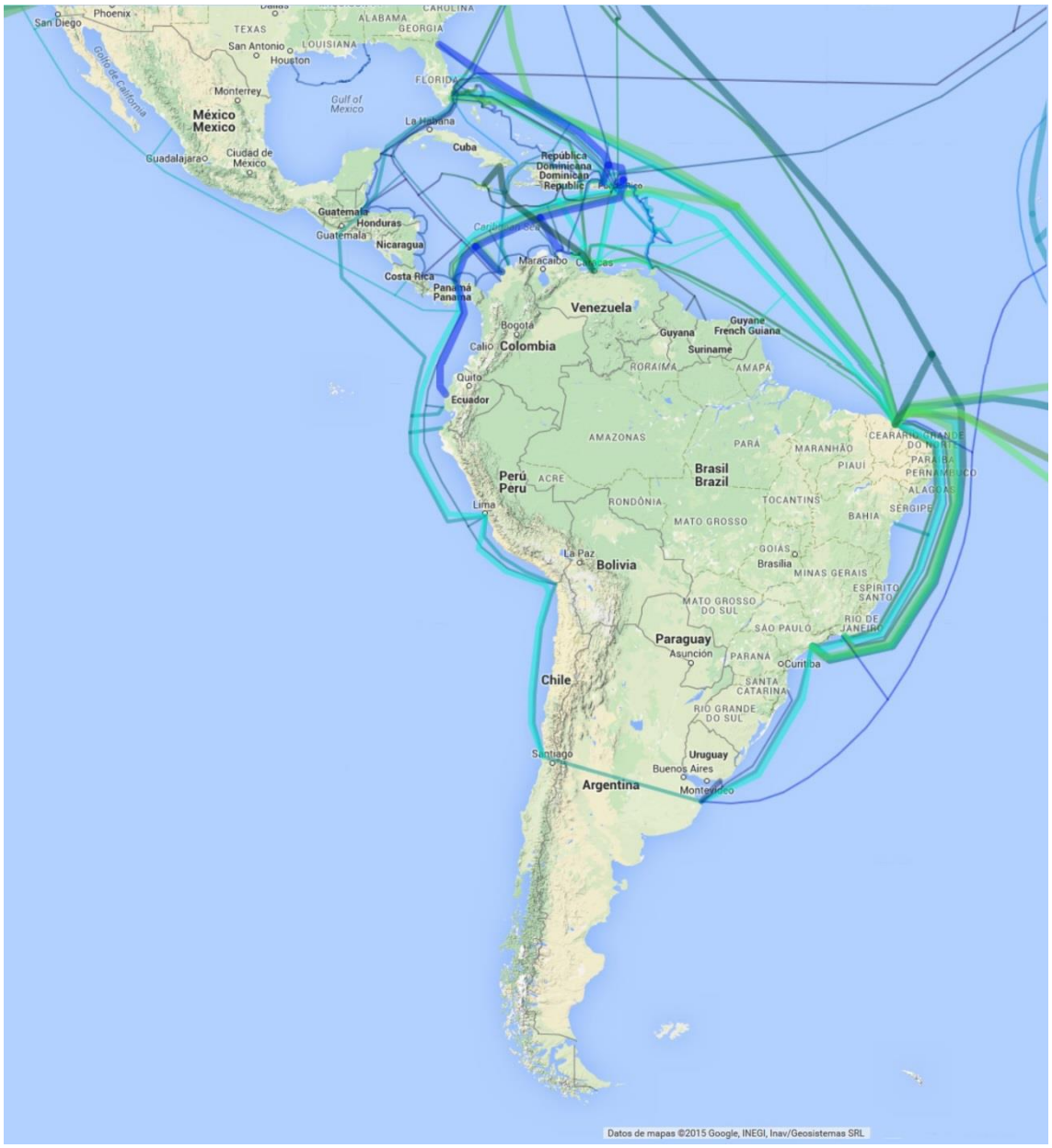
Cabe recordar que, a pesar de las numerosas precauciones de seguridad, varios casos de accidentes poco conocidos del público se registraron a lo largo de los últimos años[10]. Generan un riesgo de suspensión del acceso que se encuentra entonces multiplicado – en probabilidad y gravedad – en las zonas del planeta menos conectadas a esta red de cables. En el caso latinoamericano, estos equipamientos[11] conectan el continente en una configuración "en serie" – especialmente su costa Pacífica – como se puede comprobar en el siguiente mapa.

[9] Así, en 2012 se detectó en Brasil una serie de ataques llevados a cabo a través de módems contaminados. Faltas de precauciones por parte de los proveedores de acceso y de los usuarios permitieron la corrupción de más de 4,5 millones de box según el CERT brasileño. Si es verdad que se solucionaron varias de los fraudes iniciadas a partir de esta vulnerabilidad, el mantenimiento en servicio de módems infectados es muy probable, implicando preocupaciones de seguridad para el acceso a Internet a partir de redes públicas o desconocidas.

[10] Se puede, por ejemplo, aludir a los accidentes ocurridos en Taiwán en 2006, y más recientemente en Alexandria y Dubái en 2008, que han causado una suspensión prolongada del acceso a Internet para millones de usuarios.

[11] Concretamente, los principales cables submarinos, actualmente en uso, que permiten la conexión de América del Sur a Internet se conocen bajo los nombres de "SAm-1", "LAN", "PAN-AM", "GlobeNet" y "Atlantis 2".

Situación de América Latina respecto a los cables submarinos de telecomunicación.



Fuente: Extracto del mapa interactivo realizado por Greg Mahlknecht[12].

La cuestión de los cables submarinos es fundamental, porque plantea las problemáticas tradicionales de la organización de las infraestructuras de comunicación en América Latina y su vínculo con una serie de riesgos importantes. Como se puede averiguar en el mapa, la configuración actual de este tipo de equipamientos a la escala del continente hace aparecer nudos de comunicación y una disparidad geográfica notable. Así, especialmente en los países

[12] MAHLKNECHT, Greg. *Open Source Submarine Cables Map*. 2014. Disponible en línea : http://www.cablemap.info/ . Fecha de la consulta 18.02.2015.

más conectados del Cono Sur, las infraestructuras nacionales de conexión a Internet dependen de cables poco numerosos y, todos, provenientes de países ubicados en el norte. En caso de incidente "río arriba", las consecuencias sobre el acceso de los usuarios de estas zonas a la web serían importantes y causarían numerosos efectos en cascada.

La capacidad de interceptación de datos es otra de las cosas que están en juego cuando se evocan las redes de cables submarinos de telecomunicación, sus itinerarios y puntos de aterrizaje. Es interesante recordar que la instalación de nuevos cables submarinos es una de las medidas anunciadas por las autoridades brasileñas en respuesta a las "revelaciones" de Edward Snowden respecto a la existencia de operaciones de inteligencia enfocadas sobre sectores económicos y políticos del país. Es innegable que, en actividades estratégicas, este tipo de prácticas por parte de los Estados, es una variable que puede tener un impacto negativo sobre los resultados de las empresas y sobre la confidencialidad de sus informaciones. Por lo tanto, constituye también un riesgo en sí, para una variedad de organizaciones, que tienen que tomarlo en cuenta.

Sin embargo notamos que, más allá de la sola reacción brasileña, varios proyectos de mejoramiento de esta red – a través de nuevas conexiones – están diseñándose. Significa que, a medio plazo, el riesgo de un accidente que causaría una pérdida de conexión masiva y daños en cascada está destinado a atenuarse.

II – LOS ACTORES DE LA ZONA INVOLUCRADOS EN EL MEJORAMIENTO DE LA SEGURIDAD CIBERNÉTICA. ACTORES REGIONALES

De manera a facilitar la armonización y coherencia de los marcos legales diseñados para enfrentar los riesgos transversales del ciberespacio, es evidente que hacen falta iniciativas de cooperación internacional. En esta parte consagrada a los actores regionales dedicados a tareas de ciberseguridad, nos interesamos por la visión y las capacidades de los que aparecen como los tres actores principales en término de efectos: la OEA, AMERIPOL y el LACNIC.

La Organización de los Estados Americanos considera la constitución de estadísticas y de análisis de calidad como condiciones esenciales a la elaboración de políticas públicas y estrategias de seguridad cibernética eficaces por parte de las organizaciones públicas como privadas. Es cierto que la incertidumbre actual genera dificultades en el momento de elaborar un diagnóstico fiable de los riesgos cibernéticos del continente. Frente a esta situación, la institución promueve concretamente una estrategia progresiva cuya primera etapa es la instauración de Equipos Nacionales de Respuesta a Incidentes de Seguridad Cibernética - o CSIRTs - combinados con campañas de sensibilización que favorezcan una verdadera toma de conciencia en cuanto a la gravedad de estos temas (OEA, 2012). La OEA

dispone además de una institución especializada a través de la Comisión Interamericana de Telecomunicaciones.

En un informe del año 2012, la OEA presenta un "estado del panorama de las amenazas". Sin negar unos aportes interesantes, cabe destacar que su contenido está muy vinculado con la estrategia progresiva adoptada por la institución. Este planteamiento, junto con la colaboración directa de los Estados obliga el observador a poner en tela de juicio su contenido, como en cualquier caso de evaluación llevada a cabo por actores que, por su involucramiento en el proceso, son, a la vez, jueces y partes. Así, presenta una visión limitada de las amenazas, diseñada para convencer a los gobiernos de la validez de la estrategia de la OEA. Sin embargo, tiene la virtud de reflejar un hecho fundamental: que América Latina experimenta riesgos diferentes – en naturaleza y amplitud – respecto a otras regiones del planeta. Además, la toma en cuenta de los riesgos cibernéticos en aspectos de desarrollo y de negocios comunes es un hecho positivo.

En el ámbito de la lucha contra los actos de ciberdelincuencia en su sentido más estricto, existe también en América Latina un marco activo de cooperación a través de AMERIPOL, la Comunidad de Policías de América.

Según sus estatutos, "AMERIPOL, es un mecanismo de cooperación hemisférico, integrado y coordinado, cuyo propósito es promover y fortalecer la cooperación policial en materia técnico científica, de capacitación, así como para dinamizar y hacer más efectivo el intercambio de información con fines de inteligencia. De igual forma tiene como propósito coordinar y potenciar acciones sostenidas de investigación criminal y asistencia judicial (…) para que se traduzcan en la consolidación de la doctrina y filosofía policial, así como en la prevención y neutralización del delito". Anunció, el 7 de Agosto de 2014, la creación de un Centro de Ciberseguridad. Este órgano contaría con el apoyo de la Policía Nacional Española a través de asesoría en su funcionamiento y de formaciones en el marco de la Escuela Iberoamericana de Policía. Si se trata claramente de una iniciativa que, en el futuro, facilitará las investigaciones de los diferentes cuerpos policiales, no tiene por lo tanto la capacidad de mejorar las respuestas ante amenazas globales en el estado actual de la situación. Además, cabe señalar como otro límite a la acción de AMERIPOL que los Estados, a pesar de este involucramiento en un mecanismo de cooperación, no suelen entregar la totalidad de sus informaciones respecto a amenazas o a sus estrategias y medios, como bien lo señala Kyra Gurney en su artículo[13].

Finalmente, el *Latin America and Carribean Network Information Center* (LACNIC) asigna y administra las direcciones IP de América Latina. Trabaja en colaboración con los CISRT de los países del continente latinoamericano y con la OEA, participa en la reflexión regional respecto de la seguridad de la red. También publica un reporte anual y estadísticas por

[13] GURNEY, Kyra. "Can Ameripol Center Effectively Combat Cyber Crime?" in *InSight Crime*. Agosto de 2014, disponible en: http://www.insightcrime.org/news-briefs/can-ameripol-center-effectively-combat-cyber-crime . Fecha de la consulta 12.02.2015.

países. El principal eje de la acción del LACNIC en materia de seguridad, más allá de certificaciones de propiedad de direcciones IP, se conoce bajo el nombre de "Proyecto Amparo". Iniciado en 2009, consiste en un apoyo al trabajo de los CSIRT nacionales, en iniciativas de mejora de la seguridad de los DNS y en la organización de formaciones y congresos.

Actores nacionales

Un análisis sencillo de las administraciones de los países de América Latina permite constatar que instituciones especializadas en la lucha contra la ciberdelincuencia generalmente existen. Sin embargo, experiencias pasadas han demostrado que este hecho no es suficiente para afirmar que tienen los recursos suficientes para cumplir misiones de ciberseguridad eficaces o que no se centran exclusivamente en la protección de sistemas públicos, descuidando al sector privado en su acción. El número de instituciones por país tampoco puede elegirse como un criterio adecuado, considerando que se deben tomar también en cuenta sus efectivos y su capacidad de comunicación o de trabajo conjunto.

El contexto nacional en el cual actúan estos servicios públicos tampoco se puede eludir, especialmente en las zonas donde la criminalidad organizada ha conseguido afirmarse como un actor que entra en concurrencia directa con el Estado. La actividad cibernética de los grupos criminales se concibe primero como un instrumento al servicio de las actividades "tradicionales" de las redes criminales. En términos concretos, el acceso indebido a sistemas de información y su eventual alteración constituyen una manera de contrarrestar las medidas tomadas por el Estado y de anticiparlas. Sin embargo, existen evidencias de que varias redes de criminalidad organizada también han elegido la opción estratégica de multiplicar sus fuentes de ingresos, perpetrando delitos en línea tales como fraudes, robo de informaciones, chantaje y producción o difusión de contenidos de pornografía infantil.

La cuestión del marco legal

El estado del marco legal y de los controles en un país refleja también la calidad de los instrumentos con los cuales el Estado intenta limitar los delitos informáticos. La adopción, estos últimos años, de varias legislaciones específicas a la seguridad informática tiende a concluir a una mejora general del marco legal en este ámbito en el continente y a una progresiva toma de conciencia. Sin embargo, para ir más allá de los efectos de anuncio, a su estudio formal se debe añadir una evaluación de resultados y del impacto concreto de las instituciones encargadas de aplicarle. Además, estos marcos legales no pueden ser eficaces sin ser actualizados en varias ocasiones de manera a mantenerse en plena coherencia con las evoluciones tecnológicas que afectan el ciberespacio en permanencia.

Así, por ejemplo, se puede considerar que un país en el cual existen espacios y redes de venta bien conocidos de informaciones robadas no tiene un compromiso prioritario con las problemáticas de ciberseguridad empresarial y ciudadana – o fracasó en sus intentos. Igualmente, se plantea la cuestión de la adaptación de estas normas a medios tecnológicos

en permanente evolución que determina directamente la capacidad del Estado en fiscalizar los casos detectados y sancionar a sus autores. Desde este punto de vista, el análisis de la actualización de los marcos legales nacionales y del número de acciones en justicia lleva a matizar fuertemente la calidad de los marcos legales vigentes en América Latina. Cabe destacar que estos obstáculos enfrentados por los actores que se dedican a la disminución de la inseguridad cibernética corresponden a problemáticas más generales de credibilidad de los Estados latinoamericanos, en varios asuntos en total desfase con las declaraciones voluntaristas de los gobiernos.

III – AMÉRICA LATINA, UNA "ZONA GRIS" EN MATERIA DE SEGURIDAD CIBERNÉTICA

Componentes ideales de un panorama de riesgos cibernéticos

En un continente que presenta un grado de penetración de internet importante, que posee infraestructuras propias y tiene intereses económicos mayores vinculados al ciberespacio, el riesgo cibernético se debe incluir entre las variables de una evaluación de riesgos integral.

En el momento de elaborar sus estrategias, las organizaciones intentan diseñar medidas que les permitan gestionar los riesgos más presentes en su sector de actividad. Más que una lógica de prudencia, se trata de un imperativo esencial para un proceso de decisión racional. Este trabajo consiste en dos pasos sucesivos e inseparables: obtener informaciones y analizarlas. Sin embargo, cabe destacar que un trabajo de análisis que no esté respaldado por informaciones válidas se convierte en un ejercicio de adivinación basado en la interpretación de señales anecdóticas.

Un panorama ideal de riesgos cibernéticos tendría entonces que integrar estadísticas públicas creíbles sobre tipos, gravedad y duración de ataques o incidentes detectados en los países y las organizaciones. El detalle de los contenidos implicados en los ataques, de manera directa o como vectores[14], permite definir *patterns* y entonces tendencias.

Sin embargo, hay que tener conciencia que este componente esencial no es, en ningún caso, suficiente, primero considerando que no indica las respuestas dadas a estos ataques y, sobre todo, porque se trata de un panorama en un momento dado, que no se repite de forma automática.

Así, las características según el tipo de amenazas constituyen un buen indicador para la elaboración de una estrategia defensiva a corto plazo. Sin embargo es también cierto que los vectores y tipos de amenazas en América Latina parecen experimentar una volatilidad muy fuerte y entonces, no se pueden generalizar a un horizonte de tiempo más largo. Además, las estadísticas de amenazas informáticas publicadas por las instituciones estatales en América Latina presentan dos problemas. Se centran en ataques pasados, sin

[14] Para una tipología de delitos informáticos detallada y no reservada a los especialistas de las tecnologías de la información, se puede referir al informe de la ITU publicado en 2009 y titulado *El ciberdelito: guía para los países en desarrollo*.

necesariamente proponer respuestas que les solucionen y, por supuesto, ignoran los ataques que no se detectaron. Por consecuente hay que ser muy prudente en el momento de usar estas cifras que, mal interpretadas, pueden introducir sesgos y efectos contra-intuitivos mayores.

Uno de los casos más claros tiene que ver con la capacidad de detección de los ataques. Un país puede detectar menos incidentes que la media, por no tener una dotación suficiente en instrumentos o personales y, por falta de una metodología común, no se puede diferenciarlo de un país realmente menos inseguro. En tales casos de ausencia de información sobre la metodología empleada o de incoherencias evidentes[15], aquellas cifras no se pueden utilizar como criterio válido de una evaluación de riesgo.

La incertidumbre como principal fuente de riesgo

De esta constatación, se puede concluir que la incertidumbre generada por la ausencia de informaciones públicas de calidad sobre las amenazas y las medidas de los Estados genera efectos problemáticos. Así, impide que las organizaciones puedan llevar a cabo un proceso de toma de decisiones de calidad en cuanto a su seguridad, ahuyenta a las inversiones en sectores sensibles y da a actores privados que proponen soluciones de protección de la información la oportunidad de publicar cifras que valoran su necesidad, sin necesariamente reflejar la realidad de manera fidedigna.

Ocurre que justamente se trata de una problemática particularmente presente en América Latina. Del informe de la OEA, se puede recordar la siguiente frase, que subraya de manera muy correcta estas dificultades "El conocimiento de que se dispone sobre el panorama general de las amenazas cibernéticas en la región es incompleto. Gran parte de lo que se conoce sobre el panorama de las amenazas cibernéticas en la región se basa en informes noticiosos esporádicos y sin fundamentos sólidos"[16].

Una conclusión muy acertada pero que pocos estados miembros de la Organización han sido dispuestos a reconocer. Se añade entonces a las dificultades clásicas de evaluación - características de los temas de seguridad cibernética - obstáculos específicos al continente latinoamericano.

Un desfase entre las medidas impulsadas y el estado de la lucha contra la cibercriminalidad

¿En qué se centran entonces las iniciativas públicas en torno a la protección de los sistemas de la información en América Latina? Las medidas, en la mayoría de los casos, están exclusivamente centradas en la protección de los sistemas informáticos de los órganos del

[15] Así, por ejemplo, varios países latinoamericanos indican no haber detectado ningún ataque vinculado al SPAM durante un periodo de un año, dato poco creíble.

[16] OEA, opus citatum, 1.

Estado. Varios gobiernos presentan los resultados de su acción en defensa de sus instituciones como si fueran equivalentes a una política pública integral de seguridad cibernética que debería estar también orientada hacia las necesidades de la sociedad civil.

Como detallado en la segunda parte, a pesar de los discursos oficiales, brechas mayores de seguridad siguen existiendo en las "infraestructuras críticas" del continente. Más allá de este hecho, parece interesante poner en tela de juicio la definición de este concepto. En efecto, se podría avanzar que tales "infraestructuras críticas" no se pueden, en el contexto actual, limitar a una serie de infraestructuras de abastecimiento básico. La tendencia a la omnipresencia tecnológica y a la conexión de objetos "inteligentes" tiende a multiplicar el número de infraestructuras claves y a intensificar las consecuencias potenciales de los riesgos que les afectan. Un cambio de mentalidad es entonces necesario para reconocer que, en el ciberespacio, ninguna infraestructura es neutral y el grado de criticidad no es absoluto sino que depende de un planteamiento que prioriza a ciertos actores específicos.

Una buena ilustración de esta realidad y de las acciones que han podido desarrollarse en este contexto de incertidumbre y de inseguridad cibernética en varios países de América Latina es el caso de la "operación Careto".

Activa durante 7 años, consistió en un ataque complejo en contra de un número muy limitado de usuarios. Las víctimas fueron ministerios, representaciones diplomáticas, grupos de investigación, pero también empresas privadas del sector de las materias primas y de la energía. Esta operación se descubrió solamente en 2014. Mientras tanto, todas las comunicaciones de estas instituciones víctimas fueron interceptadas por los atacantes[17]. El grado de profesionalismo – en los instrumentos como en los métodos de cierre de las infraestructuras utilizadas en Argentina – es tal que parece poco creíble que se eligió la ubicación física de la operación por casualidad.

CONCLUSIÓN

Los diferentes aspectos desarrollados en este trabajo permiten ilustrar la complejidad actual del ejercicio de medición de riesgo cibernético para América Latina. Si no constituye un análisis exhaustivo de las amenazas y riesgos presentes en el ciberespacio, permite poner de relieve una incertidumbre que solamente se puede traducir en una evaluación por un riesgo alto.

Por supuesto, las organizaciones deben dar orientaciones a sus estrategias de seguridad, incluso en este contexto de escasez de información. Para cumplir con esta necesidad pueden dirigirse a fuentes alternativas o indirectas que, a pesar de no ser necesariamente representativas, indican tendencias e índices sobre las amenazas o la actitud de los poderes públicos. Tales fuentes se pueden encontrar en informes de empresas privadas de seguridad,

[17] Kaspersky Lab. *Unveiling "Careto" - The Masked APT*. 2014.

en artículos de prensa que reportan detenciones o la existencia de redes de venta de informaciones robadas. Así, según el informe de la OEA, estos espacios de venta se camuflan en páginas de intercambio en línea como IRCs o redes sociales tradicionales. Por ejemplo, el documento indica que la red social Orkut sería una de las principales plataformas de venta de informaciones robadas y de programas maliciosos en América Latina[18]. Los informes anuales de gigantes de la web como Facebook que publica, cada año, estadísticas por países que reflejan el número de solicitudes de información sobre páginas o perfiles de usuarios y sobre el grado de éxito de estas demandas tienen mucho interés.

Más allá de estas alternativas insatisfactorias, parece interesante recordar que la seguridad informática no es más que una variante de la seguridad en general. Y por lo tanto, cabe destacar la importancia del factor humano en la mayoría de los fallos de seguridad informáticos a través del uso de *keyloggers*, de métodos de *social engineering*, del robo de ordenadores, etc.

En esta situación, la sensibilización y formación de los usuarios a procedimientos básicos de seguridad informática parece la opción que podría potencialmente dar los mejores resultados, por un esfuerzo reducido. La emisión de "informes de asombro" internos es una de estas prácticas que, poco a poco, pueden llevar los usuarios a considerar menos los sistemas de la información como una "caja negra" y permiten una mejora inmediata del grado de seguridad de una organización.

Igualmente, parece muy importante insistir sobre la necesidad para cualquiera organización de formar sus miembros a usar con precaución las conexiones a Internet, en particular en lugares públicos. Una compartimentación estricta de las informaciones de la empresa entre dispositivos fijos y móviles, profesionales y personales es otra de las medidas importante que permiten limitar los riesgos de fuga de información, de fraude o de ataque. En un contexto de omnipresencia de las redes sociales, el control de la información pública de las organizaciones constituye un reto determinante que plantea problemáticas complejas de fronteras entre vida privada y profesional, entre información crítica y datos personales que cada persona está en derecho de compartir.

Añadiremos, por fin, que para ir más lejos y matizar las conclusiones del presente análisis sobre "la seguridad cibernética en América Latina", sería preciso examinar detenida y separadamente la situación específica presentada por cada zona geográfica del continente latinoamericano.

i

*Paul-Edouard Martin**
Máster Estrategia, Inteligencia y Gestión Riesgos Sciences Po Lille
Máster Estudios Latinoamericanos Instituto Iberoamérica USAL
pauledouard.m@gmail.com

[18] OEA, opus citatum, 15.

BIBLIOGRAFIA:

-CROZIER, Michel y FRIEDBERG, Erhard. *L'Acteur et le système*, Editions du Seuil, 1977.
-International Telecommunication Union (ITU) Agencia de las Naciones Unidas: www.itu.int
-International Telecommunication Union (ITU) – *El ciberdelito: guía para los países en desarrollo*. 2009.
-Indicadores del Desarrollo Mundial - Información y comunicación: wdi.worldbank.org/table/5.12
-Kaspersky Lab Informe (en inglés) « Unveiling "Careto" - The Masked APT »
-KEMPF, Olivier. *Introduction à la Cyberstratégie*. Economica. 2012.
-Organización de los Estados Latinoamericanos – *Tendencias en la Seguridad Cibernética en América Latina y el Caribe y respuestas de los gobiernos.* 2012 Disponible en línea: www.oas.org/es/ssm/cyber/documents/oastrendmicrolac_spa.pdf
-Organización de los Estados latinoamericanos – *Estrategia Interamericana Integral de Seguridad Cibernética*. 2004
-Página Web del portal de informaciones sobre crimen organizado en América: www.insightcrime.org
-TeleGeography. Mapa interactivo de las redes de cables submarinos de telecomunicación. Consultable en línea : www.submarinecablemap.com/
-TeleGeography – *Lista de cables submarinos*. Disponible en línea: www.telegeography.com