Seguridad de las Redes y Sistemas de Telecomunicaciones Críticos

Por Carlos Silva Ponce de León, Director de Servicios Empresariales de Lusacell y Secretario del Instituto del Derecho de las Telecomunicaciones

Este artículo es una versión editada del original publicado en *AHCIET Revista de Telecomunicaciones*, año XXVI, no. 116 (octubre-diciembre/2008): 12-18. La Secretaría de Información de AHCIET cedió amablemente sus derechos.

Introducción

La infraestructura crítica de todos los Estados Miembros, sus economías y sociedades dependerán de la seguridad de la Infraestructura Crítica de Redes de Telecomunicaciones durante el siglo XXI —del inglés, *Critical Network Infrastructure* (CNI)—. La infraestructura crítica en términos generales abarca los siguientes segmentos: información y comunicaciones, generación y transporte de energéticos y energía, sistemas bancarios y financieros, transportación, agua, alimentos, servicios de salud pública, sistemas de emergencia y operaciones de manufactura relevantes.

La Infraestructura Crítica de Redes de Telecomunicaciones se refiere al conjunto de redes y computadoras interconectadas que transportan información relevante a la seguridad de un país o de alto valor financiero, también se refiere a las redes que soportan las operaciones de algún otro tipo de infraestructura crítica. Físicamente, la CNI puede identificarse como la totalidad de una red o las porciones de la red que intercambian información de alto significado.

Las amenazas a la CNI están incrementándose en su frecuencia y severidad, y potencialmente pueden afectar todos los aspectos de la sociedad. La carencia de conciencia, análisis, intervención, acción preventiva y despliegue de estrategias para aminorar los posibles efectos, deja a las sociedades vulnerables a eventos potencialmente catastróficos. Tales eventos pueden dañar seriamente economías, minar la actividad económica, desestabilizar gobiernos y directamente afectar la seguridad de los ciudadanos.

La globalización del comercio, del intercambio de información y de las actividades humanas en general es tal, que la seguridad de la CNI no puede ser lograda por las acciones de estados individuales por su cuenta. Por lo tanto, se requiere de una apreciación colectiva de las amenazas así como acciones de colaboración para atender tales temas. Esta colaboración debe incluir a todas las partes interesadas.

Tendencias tecnológicas de las CNI

La rápida evolución tecnológica en las redes de telecomunicaciones ha creado nuevas oportunidades de desarrollo de la misma forma que genera nuevos retos a la seguridad de la CNI en su conjunto. En particular, las tendencias expuestas en los siguientes párrafos deben analizarse con la finalidad de apreciar la complejidad de los temas asociados con su seguridad.

Redes sin marcadas jerarquías: la Red Telefónica Pública Conmutada tiene un cierto nivel de seguridad intrínseca al existir una brecha importante entre los usuarios y los operadores de la red en función de la estructura jerárquica de la infraestructura. Tal separación entre usuario y operador virtualmente desaparece en la arquitectura de Internet, la cual es plana por naturaleza, con usuarios prácticamente indistinguibles de los operadores en términos del acceso a los componentes de la red tales como concentradores, conmutadores y enrutadores. La convergencia entre la RTPC e Internet ha incrementado la vulnerabilidad potencial de la infraestructura de telecomunicaciones en su conjunto. Esta tendencia continuará incrementándose una vez que la infraestructura de telecomunicaciones continúe su gradual migración a tecnología basada en paquetes y más parecida a Internet.

Más inteligencia en las puntas terminales de la red: hablar de redes que evolucionan para asemejarse cada vez más a Internet, puede describirse también como la tendencia a migrar más inteligencia del núcleo de la red a sus puntas terminales, donde los usuarios individuales son responsables por la configuración, mantenimiento y protección de sus equipos. Al carecerse de una entidad centralizada responsable por la configuración de los dispositivos conectados a la red, aumentan las posibilidades de que tal proceso se lleve a cabo con deficiencias provocando que los dispositivos se vuelvan plataformas potenciales para lanzar ataques al núcleo de la red.

Multiplicidad de operadores: el ambiente tradicional de proveedores monopolísticos delimitaba un escenario con relativamente pocos actores que colaboraban cercanamente en asuntos críticos y que establecían relaciones de mutua confianza en sus operaciones. En la actualidad, con mercados abiertos a la competencia y nuevos operadores en todos los niveles, las nuevas redes de telecomunicaciones replantean sus premisas básicas de operación. El servicio típico de acceso a Internet, por ejemplo, requiere la interconexión con múltiples operadores pares para la infraestructura básica y la interoperabilidad con proveedores de valor agregado para servicios complementarios que son accesibles sobre la misma red. La tendencia a la convergencia de servicios sólo refuerza al escenario anterior y hace imposible poder asignar la responsabilidad de la seguridad de la red a una sola entidad, ya sea privada o, incluso, al nivel de un estado individual. Ante este panorama, si se desea garantizar la provisión de servicios de forma continua, será indispensable la coordinación de esfuerzos multilaterales para la protección de las redes y los sistemas en su conjunto.

Más control en manos de los usuarios: el usuario de redes de telecomunicacio-nes del siglo XXI y, en particular, aquellos que usan activamente la Internet, cuenta con más poder en término de acceso a los recursos de la red que los usuarios de la RTPC tradicional. Este cambio en el balance de poder a favor de los usuarios de la red podría verse idealmente como un suceso positivo que permite a los usuarios configurar la red a sus propios requerimientos, logrando nuevas eficiencias y explotando nuevas oportunidades. Sin embargo, tal evolución en las redes permite, también, la oportunidad para la explotación de vulnerabilidades para dañar la infraestructura y provocar interrupciones a los servicios al resto de los usuarios.

Nuevos servicios: la disponibilidad de cada vez mayores anchos de banda en servicios fijos, así como la rápida evolución de servicios inalámbricos tales como la telefonía celular y nuevas tecnologías como WiFi y WiMax, hacen posible el acceso a las telecomunicaciones en mayores capacidades, desde más localidades y en situaciones más diversas. Si bien lo anterior juega en beneficio del usuario y puede tener enormes impactos positivos en la sociedad en su conjunto, también incrementa significativamente el potencial para violaciones a la seguridad en la infraestructura de telecomunicaciones.

Sobre los riesgos de ataques a la CNI

Las CNI en general son redes vulnerables a ataques. Este aspecto es particularmente grave en las nuevas redes como Internet que no consideraron en su diseño original aspectos de seguridad. Si bien se han dedicado cuantiosos esfuerzos en el diseño de protocolos y redes seguras, es un hecho que estos van acompañados de rutinarios reportes de nuevas vulnerabilidades en los sistemas más frecuentemente utilizados.

Dado que una porción cada vez mayor de la actividad económica global depende de la CNI, su protección —muchas veces referida como la protección de la infraestructura física del ciberespacio— es crucial para mantener y garantizar el desarrollo y el bienestar social. Esto la hace un elemento importante de infraestructura crítica la cual debe ser protegida con alta prioridad. Se debe prestar especial atención a la lucha contra el terrorismo, que amenaza la paz y seguridad de estados y pueblos.

El Borrador de la Convención de Stanford para Ampliar la Protección contra el Ciber-crimen y el Terrorismo es un documento preparado como un ejercicio académico con miras a la creación de una agencia internacional con tales fines. El documento define un cibercrimen como las siguientes acciones cuando son realizadas sin autoridad o permiso legal:

- La acción de crear o usar programas que provoquen que un sistema de cómputo deje de operar en la forma como fue concebido o realice funciones no contempladas por su dueño legítimo.
- La acción de crear, modificar, borrar o manipular datos en un sistema de cómputo con la intención de proveer información falsa para causar daños a las personas o a las propiedades.
- Obtener acceso a un sistema restringido.
- Usar un sistema de cómputo como factor material para la comisión de un acto penado por las diversas convenciones en materia aeronáutica, marítima, de actos terroristas y narcotráfico.

Los ataques cibernéticos más conocidos en Internet son los virus, caballos de troya y "gusanos", entre otros. Las motivaciones de estos ataques tienen que ver más con el reto intelectual y la emoción que en sí mismo representan para sus ejecutantes. Por lo anterior, estos ataques son típicamente transitorios y no son concebidos como parte de un plan estructurado con objetivos que trasciendan al ataque individual.

El riesgo a futuro debe considerarse desde una perspectiva más amplia, una vez que la ubicuidad de las CNI también permite a un potencial ciberterrorista o ciber-criminal infringir daños relevantes a sus blancos desde cualquier parte del mundo sin el miedo a poder ser detenido o impedido por defensas físicas.

Por otro lado, es vital diferenciar entre el ataque aislado y ocasional provocado por individuos no profesionales, de aquellas acciones instrumentadas como parte de planes más extensos y que constituyen verdaderas amenazas estratégicas. En el Taller sobre la Creación de Confianza en Infraestructuras de Red Críticas, las siguientes fueron expuestas como características de una amenaza estratégica:

- Es estructurada, de forma tal que la fuente de una amenaza es una organización y no un individuo aislado.
- Está bien financiada, de forma que cuenta con equipo, tecnología y personal necesarios para operar un ataque de gran escala desde múltiples localidades.
- Es un actor hostil al tener fines antagónicos con los de la parte atacada. Tiene objetivos de ataque bien definidos y estándares específicos de operación.

- Protege a su personal, haciéndolo difícil de identificar, localizar y aprehender.
- La estructura hostil es respaldada por una o varias agencias de inteligencia, permitiendo la infiltración de agentes que puedan tener acceso de primera mano a la operación de la CNI o información relevante a esta.
- Puede compartir información con otras organizaciones afines a sus intereses políticos.

Aspectos de colaboración internacional

El sitio de la UIT comenta que "los defensores necesitan defenderse contra todos los ataques posibles mientras un atacante solo necesita encontrar y explotar una falla única. Por ello es deseable contar no con una sino con varias líneas de defensa yuxtapuestas que incluyan estrategias nacionales e internacionales, esfuerzos públicos y privados, canales formales e informales de comunicación así como cooperación bilateral y multilateral". Es necesario un esquema de cooperación que permita crear relaciones de confianza entre los estados, de forma que estos puedan confiar en que cuando una o más defensas fallen, otras entrarían en efecto para detener el ataque, contener el daño o evitar que el ataque se repita.

Existen otros aspectos que hacen deseable la colaboración multilateral una vez que esta:

- Puede ser un factor para reducir los costos, lo cual se espera en todos los casos por la magnitud de los esfuerzos requeridos, pero en el caso de naciones pequeñas puede ser un requisito indispensable.
- Puede incrementar el rango de opciones estratégicas que una nación puede considerar implantar.
- Labores particulares, como dar de baja a sistemas atacantes o localizar y extraditar a los individuos atacantes, pueden ser imposibles tanto técnica como legalmente sino existen acuerdos formales.

Lograr acuerdos internacionales es una labor compleja, una vez que se requiere no sólo la intervención de los gobiernos sino además a los proveedores de tecnología del sector privado, a los dueños y usuarios de la infraestructura y a las múltiples agencias de regulación y policíacas de un mismo Estado.

Las metas particulares que puede tener un esquema de colaboración internacional son:

- Compartir infraestructura necesaria para el esfuerzo y coordinar, a nivel internacional, la acumulación de inteligencia.
- Coordinar internacionalmente la aplicación de leyes, instrumentar acciones para prevenir, investigar y perseguir el crimen.
- Definir indicadores de desempeño.
- Mejorar la cooperación internacional para desarrollar estándares internacionales de cómputo y de seguridad de las redes.
- Hacer conciencia entre los involucrados vía esfuerzos de educación.
- Permitir la colaboración para la investigación en la industria, la academia y los gobiernos.
- Facilitar alianzas entre el sector público y el privado.
- Asegurar la transparencia y el acceso a la información.

Los esquemas de colaboración internacional pueden clasificarse según el grado de formalidad y el número de Estados involucrados.

Un acuerdo informal se logra cuando las partes han establecido una relación y han desarrollado un nivel de confianza mutua que les permite colaborar en su interés común. Tal confianza crea una expectativa de confidencialidad y reciprocidad pero sin ninguna obligación legal. La principal ventaja de los convenios informales, dada la sencillez de sus métodos de comunicación, puede ser la eficiencia para responder de manera rápida ante amenazas, especialmente aquellas cuya naturaleza no está bien identificada. Su desventaja primordial es, sin duda, su opacidad al no haber registro formal del intercambio de información.

En un acuerdo formal se establece oficialmente una agencia o foro con roles y responsabilidades asignados para su operación. Tal consenso involucra frecuentemente un instrumento legal acordado entre representantes de los gobiernos y que requiere ratificación por la entidad legislativa, por lo mismo su concreción puede ser bastante compleja. Algunas de las ventajas de un acuerdo formal pueden ser:

- Permitir con más facilidad que el convenio crezca para incluir, posteriormente, a más naciones. Si bien el establecer procesos formales puede retrasar la rapidez de la respuesta, puede ser la forma más efectiva de manejar volúmenes mayores de transacciones de información.
- Servir como el mejor marco para negociar esquemas de costos y uso de infraestructura compartida para proyectos grandes.
- Ofrecer mayor confianza una vez que cada parte está obligada legalmente a cumplir con los términos del contrato.

Además de ser relativamente sencillos de negociar, los acuerdos bilaterales pueden ser un excelente marco de referencia previo a la cooperación multilateral. Permiten, asimismo, la cooperación de modo flexible según el grado de confianza mutua de las partes.

Los acuerdos multilaterales son deseables una vez que pueden ser más consistentes que una colección de múltiples acuerdos bilaterales no relacionados. Al congregar a un mayor número de naciones, su instrumentación puede hacer una acumulación mayor de recursos reduciendo la aportación individual de cada parte. La determinación de la cantidad de recursos a aportar en función del tamaño relativo de las economías participantes puede ser un gran incen-

tivo para la participación de países pequeños.

Todas las naciones tienen el incentivo de participar en acuerdos universales donde todos los participantes se beneficien del conocimiento generado colectivamente. El logro de un consenso casi universal permite que quienes cometen un crimen no puedan beneficiarse de potenciales paraísos criminales. Un acuerdo multilateral sin alcance casi universal, por otro lado, puede generar externalidades de las cuales se beneficien aquellos estados que no comprometieron recursos en él.

El éxito de la instrumentación de un acuerdo casi universal dependerá de la efectividad para definir principios generales de forma consensuada en los temas de:

- Adopción de los principios del acuerdo multilateral en las leyes domésticas.
- La definición de las acciones que constituyen un crimen.
- La definición de las jurisdicciones de cada estado participante.
- La asistencia legal mutua para identificar y rastrear sistemas atacantes, identificar y tomar declaraciones de personas, realizar búsquedas y aseguramiento por medios electrónicos, examinar dispositivos y sitios, asegurar e intercambiar información y transferir personas en custodia.
- La asistencia a países en desarrollo, especialmente a los más pequeños.
- La creación de una agencia internacional especializada.
- El respeto a los Derechos Humanos, particularmente en el tema de privacidad.
- Mecanismos de auditoría y de acceso a la información.
- La definición de comités técnicos donde participen activamente los operadores de la infraestructura así como los proveedores de la tecnología de equipamiento y software. En tales comités deberían estudiarse los temas de la protección de datos, la detección de usuarios y programas intrusos, la verificación y prueba de vulnerabilidades así como la comunicación y distribución de parches que corrijan vulnerabilidades conocidas.
- Esquemas formales para el desarrollo de estándares. Este tema es vital una vez que los estándares existentes son solo "recomendaciones" cuya aplicación queda a la discreción de los proveedores y de los usuarios de la infraestructura. El problema es frecuentemente agravado por los proveedores que lanzan al mercado "estándares" que compiten entre sí.
- Garantizar el rápido restablecimiento de los servicios en caso de desastres naturales, definiendo estándares operativos para los proveedores así como esquemas de cooperación entre agencias gubernamentales, cuando se presenten daños a la infraestructura crítica trasnacional.
- Definir mecanismos que incentiven la participación y que definan la relación con los Estados no miembros.

La lista anterior centra la discusión en la esfera de la CNI propiamente dicha, dejando de lado aquellos aspectos polémicos tales como la motivación política de los posibles crímenes, la regulación de contenidos y la protección a la propiedad intelectual.

Aspectos de reglamentación doméstica

En el camino a un acuerdo multilateral, casi universal para la creación de una nueva agencia en el tema de protección a la CNI, existe en paralelo una gran lista de tareas que los entes reguladores deben atender en sus mercados domésticos. Más aún, la experiencia doméstica acumulada debe ser un recurso fundamental que soporte las posturas de los estados hacia el consenso internacional.

La tendencia hacia la adopción masiva de servicios de banda ancha tanto fijos como móviles significa que nuevas y más aplicaciones podrán ejecutarse sobre la infraestructura de telecomunicaciones. Esto incrementará la necesidad de que los proveedores de servicios tengan estrategias de mitigación del riesgo bien calculadas, objetivos de servicio para respuesta y recuperación en caso de ciber-ataques y catástrofes naturales. En tales casos, es responsabilidad del regulador definir recomendaciones o, incluso, estándares formales de operación que garanticen la provisión del servicio sin interrupciones.

El ente regulador debe hacer una selección detallada de aquellos parámetros de calidad que sean relevantes en su mercado para posteriormente solicitar a los operadores el reporte periódico de los mismos. La recopilación de información estadística es vital para poder determinar las potenciales vulnerabilidades de las redes a nivel de un sistema nacional.

La definición de estándares o recomendaciones debe llevarse a cabo atendiendo al interés común y su esencia como norma debe considerar un rol complementario a los criterios primordialmente técnicos y económicos de los diseños de los operadores. Algunos temas que pueden considerarse como sujetos a ser requeridos por el ente regulador:

- Parámetros de disponibilidad, tiempo de conexión al servicio y calidad de la transmisión de los servicios dentro de rangos aceptables de forma general para los usuarios.
- Existencia de planes de contingencia documentados para la restauración del servicio por parte de los operadores en caso de interrupciones mayores, así como la coordinación entre operadores y las agencias de gobierno en caso de catástrofes naturales.

◆ La inclusión de características de redundancia incluidas en el diseño de porciones de la red que son críticas para la totalidad de la red de uno o de varios operadores.

El regulador debe también incrementar la conciencia sobre la necesidad de la seguridad de la Infraestructura Crítica de Redes de Telecomunicaciones, diseminando información relevante para el consumidor y el usuario de negocios acerca de prácticas recomendables en el uso y configuración de los dispositivos de red. La colaboración con los sectores privado y académico debe considerarse como ingrediente esencial para el logro de tales objetivos.