La guerra mundial en el ciberespacio está teniendo lugar. Ejércitos de hackers, espías informáticos y ciberdelincuentes conforman las fuerzas contrincantes; no hay distinción, los adversarios son naciones desarrolladas o en vías de desarrollo así como grupos e individuos al margen de la ley. Generalmente no hay víctimas mortales ni heridos; pero los daños económicos son inconmensurables. Naciones Unidas y la OEA en particular, han tomado el reto de enfrentar esta nueva amenaza mediante la defensa cooperativa; sin embargo, sin embargo, en el ámbito regional, es poco lo que se ha hecho.

La ciberseguridad y el contexto actual

Fuente: T21 Noticias

The world war in cyberspace is taking place. Armies of hackers, computer spies and cybercriminals form the opposing forces; there is no distinction, adversaries are developed or developing nations as well as groups and individuals outside the law. Generally there are no fatalities or injuries; but the economic damages are immeasurable. The United Nations and the OAS in particular have taken up the challenge of confronting this new threat through cooperative defense; however, fundamentally at the regional level, little has been done.

Coronel EP
Roberto Vizcardo
Benavides

Coronel Ejército del Perú (R) del arma de Artillería. Magister en Economía por la Universidad San Martín de Porres-Lima. Doctor en Ciencia Política y Relaciones Internacionales por la Universidad Ricardo Palma-Lima. Graduado en Desarrollo y Defensa Nacional por el Centro de Altos Estudios Nacionales - CAEN. Ha realizado estudios en Argentina, EEUU, Corea del Sur, China y Taiwán. Actualmente ejerce la docencia en universidades e instituciones militares de nivel superior del Perú y el extranjero.

"Con la llegada de ciberamenazas ejecutadas por nuevos o distintos delincuentes o estados, es posible que observemos más ataques basados en hardware destinados a generar caos o producir la denegación de servicio a una organización".

Steven Grobman, Director de Tecnología - INTEL

INTRODUCCIÓN

Desde los albores de la creación, el ser humano se ha visto en la necesidad de comunicar sus ideas, para ello tuvo que buscar una "herramienta tecnológica" que le permitiese controlar y disponer de la información con el propósito de crear, preservar y compartir sus pensamientos con sus congéneres, herramientas tales como los mensajes en piedra (petroglifos), papiro, varas de bambú, vitela, papel, imprenta, máquinas de escribir, telégrafo, teléfono, fax, computadora, y actualmente, mediante la internet; cada una de estas "herramientas tecnológicas" ha significado un impacto trascendental en la sociedad a lo largo de la historia de la humanidad; constatamos así que el desarrollo de la sociedad humana, desde sus orígenes, ha sido determinado por las herramientas de la información y comunicación.

Se aprecia que estos avances se han dado con mayor rapidez que los anteriores, y han afectado las formas tradicionales de generar y aprovechar el valor socioeconómico de los pueblos. En especial destaca la Internet, que permite que individuos y organizaciones compartan información, desarrollen y estructuren el conocimiento en una dimensión totalmente nueva. La Internet ha permitido establecer relaciones organizacionales que eran consideradas como imposibles hace sólo algunas décadas.

Sin embargo, ese salto cuántico revolucionario también ha creado una nueva dimensión en la problemática mundial. Así, a la par de estos avances en la tecnología informática y de comunicación, también han aparecido nuevos desafíos para la humanidad, tales como la brecha digital, el ciber terrorismo y la excesiva dependencia en esta tecnología, por citar tres.

PALABRAS CLAVE: GUERRA MUNDIAL, CIBERESPACIO, HACKERS, NACIONES UNIDAS, OEA, AMENAZA, DAÑO ECONÓMICO.
KEYWORDS: WORLD WAR, CYBERSPACE, HACKERS, UNITED NATIONS, OAS, THREATEN, ECONOMIC DAMAGE.

De manera que los últimos cincuenta años de desarrollo de la humanidad, tal vez sean los más sorprendentes e impresionantes en comparación con otros períodos de la historia, a juzgar por la velocidad de los desarrollos científicos, sociales, humanísticos y políticos que la era de la globalización ha traído consigo. Se puede constatar además que, a este punto de la globalización, queda claro y ratificado que el hombre jamás perderá esa característica intrínseca que lo diferencia como ser humano: el conflicto. La historia nos documenta de manera recurrente y casi cotidiana la ocurrencia de conflictos por casi todo el planeta, ¿existe alguna isla de paz?, desde la creación hasta nuestros días; conflictos que van desde las riñas domésticas, enfrentamientos tribales, combates, guerras mundiales, batallas terrestres, marítimas y aéreas y, en nuestros tiempos, la ciberguerra o ciberconflicto.

La construcción de ingenios aéreos capaces de romper dos veces la barrera del sonido; submarinos guiados a propulsión atómica, transbordadores espaciales, aviones diseñados para transportar 800 personas en un vuelo continuo de 18 horas, son desarrollos verdaderamente impresionantes. Hoy en día, un desarrollo tecnológico relativamente reciente, como lo es el teléfono celular, se innova cada año, y en cada presentación o lanzamiento de la nueva versión de un equipo, se incrementan las prestaciones y las características, habiéndose convertido en un accesorio fundamental para la vida diaria.

Se estima que para el año 2025, el número de usuarios de los llamados teléfonos celulares "Smart" o teléfonos inteligentes, alcanzará la cifra de ocho mil millones en todo el mundo. Signo del vertiginoso avance de la tecnología, además de representar un indicador de la calidad de vida.

En ese mismo sentido, la era de la "Internet de las cosas" (IoT) ya está entre nosotros y es muy probable que en poco menos que el mediano plazo se masifique o generalice su uso; es decir la automatización de la vida diaria pasando por el e-commerce, la telemedicina, las operaciones financieras desde el teléfono celular y la construcción, a gran escala, de los vehículos sin conductor.

Todo lo descrito, aparentemente se ha diseñado para facilitar la vida de los ciudadanos, de hecho, esa es la intención por ejemplo, de las impresoras "3D", revolucionario invento que permite construir o replicar prácticamente todo, lo cual constituye una maravillosa innovación tecnológica. En fin, sería larga la lista de las aplicaciones, usos y bondades que la tecnología informática nos permite en la vida coti-

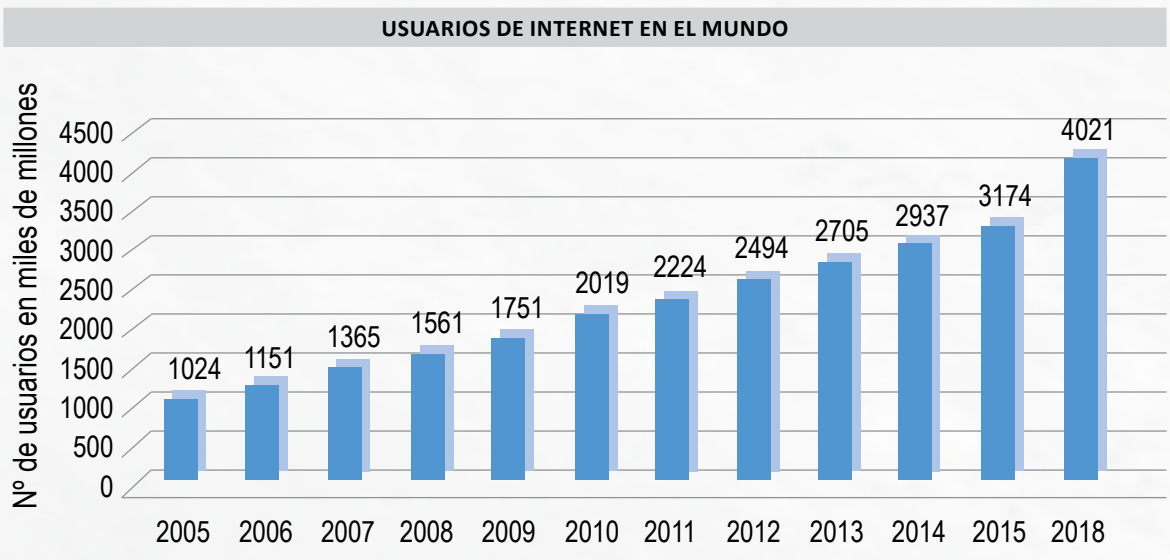

Figura N° 1. Usuarios de internet en el mundo. Fuente: International Telecommunications Union – ITU. Elaboración: Roberto Vizcardo

diana, en la ciencia y el desarrollo humano, acceder a niveles de comunicación, interrelación y soluciones nunca antes vistos en la historia de la humanidad. Pues en buena hora, el ingenio humano, gracias a Dios, no tiene límite.

Solo en el campo de las aplicaciones (App) informáticas, que se cuentan por miles, podríamos decir metafóricamente que somos "app dependientes" (si vale la pena acuñar un neologismo), pues en el caso de los "Smartphone", o teléfonos celulares "Smart", estos pequeños ingenios tecnológicos, contienen todo tipo de aplicaciones que facilitan o coadyuvan a la vida diaria; las hay para todos los usos, están aquellas diseñadas para medir la presión arterial, para el "jogging", para determinar la ubicación con relación al globo terrestre, reconocer al usuario, realizar complejas operaciones matemáticas, llevar la agenda diaria, practicar idiomas, entre muchas otras.

El escenario es más elevado si de alta tecnología (high tech) se trata. Pues esta se aplica a las centrales nucleares, satélites, sistema financiero, y todo tipo de actividades que se inscriben dentro del campo de los secretos de Estado, como aquellos programas de desarrollo de nuevos equipos para la defensa, el ámbito industrial o de las patentes denominadas críticas.

Igualmente los distintos idiomas se han visto "enriquecidos", a consecuencia de la nueva tecnología, con términos y acrónimos hasta hace poco desconocidos, tales como ramsonware, DDOS, phishing, malware, trojans, hacker, hacktivismo (que pueden ser aplicativos maliciosos utilizados por personas, estados o mafias), etc. todos ellos asociados a la cibercriminalidad, al delito informático y que configuran un amplio espectro de modalidades como la multiplicación de las prácticas de extorsión, el chantaje, la intrusión en los correos electrónicos de las personas e instituciones, robo de información de las bases de datos, modificación maliciosa del software de las infraestructuras críticas, etc.; pues bien, a todo lo anterior habría que agregar la posibilidad de ejecutar estas acciones a distancia, tan remotas como aquellas de continente a continente o tan cercanas como el vecindario.

Claro está entonces que, consecuente con lo anterior, existen personas (Hacker, piratas, etc.), Estados (como Corea del Norte y otros) y grupos organizados, que por razones pecuniarias, ideológicas o simplemente por lograr notoriedad, se han constituido como las amenazas modernas del Siglo XXI, capaces de causar daños de magnitudes tales que podrían paralizar el funcionamiento de una empresa, las actividades de una persona (key person), Estado o grupos de interés. Entonces aparecen el ciber crimen, el ciber terrorismo, los ciberataques, dejando atrás el enfrentamiento armado en el terreno de los campos de batalla. Un ciberataque en masa, podría destruir un Estado y someterlo, sin necesidad de un enfrentamiento armado.

Con mucha frecuencia se conoce de los múltiples ataques cibernéticos a los que son sometidos las empresas en todo el mundo, así como las personas (aunque hay gran cantidad de incidentes que no se dan a conocer, sea por preservar la imagen, el prestigio, o simplemente por no incrementar el daño ocasionado); se pueden señalar como ejemplos el publicitado, notorio y escandaloso ataque que el año 2015 sufrió la transnacional Sony, cuya autoría se llegó a determinar proveniente de un Estado; la exposición pública de la información supuestamente "confidencial" de los miembros del portal de citas Ashley Madison; las continuas exposiciones públicas de las fotografías "íntimas" de actrices de Hollywood; o el último escándalo de alcance global de los llamados "Panamá papers", que involucra a políticos, empresarios, actores, deportistas, etc. En el año 2014, el banco norteamericano JP Morgan Chase informó a sus clientes (unos 70 millones de personas y 7 millones de pequeños negocios) que la información cliente-banco se había visto comprometida a causa de un ataque cibernético. Recientemente el gigante tecnológico Yahoo, informó a sus clientes de todo el mundo que los datos de sus usuarios habían sido expuestos.

Otros casos emblemáticos y relativamente recientes, que ilustran la capacidad del ciberatacante (hacker o Estado) sobre blancos determinados deliberadamente son: el ataque DDOS (distributed denial of service), contra un Estado: Estonia, producido el 27 de abril al 18 de mayo del 2009 (21 diasiiii),

sobre la estructura del gobierno, bancos, portales y páginas web corporativas. El daño causado produjo la paralización del 97% de las transacciones por internet; inoperatividad de la infraestructura gubernamental, sistema bancario, medios de comunicación, etc., ocasionando decenas de millones de dólares americanos en pérdidas.

En Julio del año 2010 se descubrió la "infección" viral a las plantas nucleares del Estado de Irán, ocasionando daño a las usinas de enriquecimiento de uranio de Natanz (ciudad ubicada al sureste de Teherán); se paralizaron 1000 centrifugadoras nucleares que a la postre significaron el alargamiento del Programa Nuclear Iraní a por lo menos 5 años más. Extraoficialmente se atribuyó la responsabilidad a dos Estados.

El caso del exempleado de la CIA Edward Snowden que desveló numerosos programas de vigilancia a líderes mundiales y gobiernos aliados de EEUU, constituye un caso de uso de la cibernética tanto como de la vulnerabilidad y desafección del elemento humano.

En diciembre del año 2012, se descubrió la fuga de información de 110 millones de operaciones de pago de una famosa cadena norteamericana de retail; nombres de los clientes, número de tarjeta de crédito, fecha de expiración, CVC/CVV. El método utilizado por los ciberdelincuentes fue el malware kaptoxa, proveniente de un hacker ruso que había logrado "infectar" el POS (point of sale), es decir el punto de venta donde se registra el pago con tarjeta de crédito. El daño aproximado: 18 mil millones de dólares considerando los daños colaterales.

El 23 de diciembre del año 2015, en lo que se podría considerar el primer apagón de gran magnitud causado por un ciberataque, las plantas de energía de Ucrania dejaron de funcionar dejando a más de 225,000 habitantes en la oscuridad. El ciberataque fue conducido a distancia mediante un "reconocimiento extensivo" para identificar las redes de energía, sustraer las credenciales de los operadores y conocer la manera en que se operan los controles de apagado de las plantas. Funcionarios de Ucrania responsabilizaron del hecho a un país vecino. Este incidente causó gran alarma en Estados Unidos, al punto que la administración del Presidente Obama, cursó una circular de preventiva a los operadores norteamericanos de plantas generadoras de energía y agua, a fin de que tomen las debidas precauciones.

Recientemente un vocero de la empresa norteamericana Varonis, cuyo core business es brindar soluciones de seguridad de la información y diseño de aplicaciones informáticas, aseguró que si un hacker o pirata cibernético interviniese las bases de

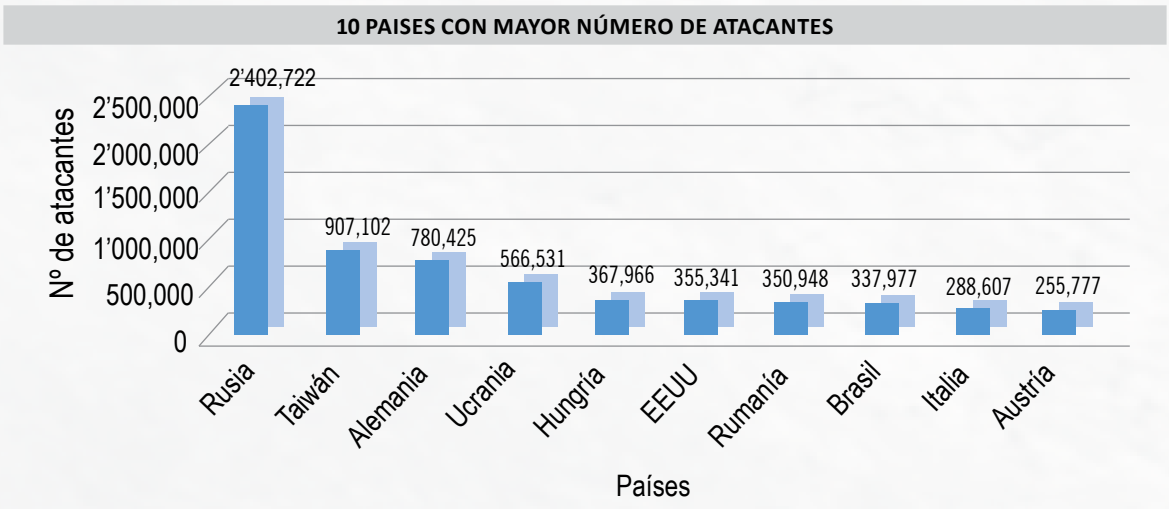

Figura N° 2. Países con mayor número de atacantes. Fuente: DIGIWARE. Elaboración: Roberto Vizcardo

datos o la información almacenada en los teléfonos inteligentes de los aspirantes (y sus entornos) a la Presidencia de los EEUU de NA, las consecuencias serían desastrosas: expondría las estrategias de campaña, donantes, número de tarjetas de crédito, etc. Pues bien, la advertencia devino en realidad con ocasión del último proceso electoral en ese país. Hay una investigación en curso.

En febrero de 2016, se llevó a cabo la Cumbre sobre Ciberseguridad y Protección del Consumidor en la Casa Blanca, Washington DC, organizada por la Universidad de Stanford; en dicho evento el Presidente Barack Obama firmó un Decreto por el cual se dispone compartir información e inteligencia entre todas agencias norteamericanas incluyendo al sector privado, a fin de detectar y actuar rápidamente ante los ciberataques.

EVOLUCIÓN TECNOLÓGICA DE LA DEFENSA

En lo que concierne al campo de la Defensa, los avances tecnológicos son también impresionantes, la "guerra de las galaxias" traída a la realidad; los misiles "inteligentes" y el uso de "drones", han reemplazado a las armas y complejos militares tradicionales, que paradójicamente, ha dado lugar a la ciberguerra y el ciberespionaje.

En relación a este último aspecto, premonitoriamente uno de los más importantes diarios del planeta comentó lo siguiente:

> *"…en el día de hoy, Estados Unidos se asemeja inconfortablemente a Goliat, arrogante en su poderío, armado hasta los dientes e ignorante de su debilidad. En una guerra informática, Goliat podría ser derribado con una honda de alta tecnología.."* (New York Times, edición nov. 1°, 1998).

Como es de suponer sin temor a errar, el blanco más atacado es la zona de Silicon Valley (California) y alrededores, donde se ubican las grandes empresas tecnológicas estadounidenses. También se constata ataques densos en la zona noroeste de la Costa del Pacífico, donde se concentra gran parte de su industria aeronáutica y militar norteamericana.

Situación actual ante la amenaza

Ciberguerra, ciberconflicto, cibercrimen, ciberespionaje, etc., sobre el tema aún está pendiente homogenizar los conceptos. Lo cierto es que estamos frente a una amenaza real que desafía a la sociedad en su conjunto, sin ninguna clase de distinciones; de una manera general estamos hablando de ataques a sistemas e infraestructuras críticas que dependen justamente de la cibernética, que se encuentran en el campo industrial, comercial, militar, espacial, gubernamental, etc., ataques a los que debemos enfrentar.

Se conoce que más de 100 países en el mundo han implementado sistemas de ciberseguridad, incluyendo en la mayoría de ellos, los comandos cibernéticos; de otro lado, existe ya un cuerpo doctrinario desarrollado por los países líderes en ciberseguridad, como Israel, Corea del Sur, etc. En América Latina, la mayoría de naciones han establecido los llamados CERT (Computer Emergency Response Team – Equipos de Respuesta ante Emergencias Informáticas) que son centros de respuesta a incidentes de seguridad cibernética que afecten los sistemas informáticos; operados por expertos en tecnologías de la información. Los CERT tienen por función implementar las medidas preventivas y de respuesta ante incidentes cibernéticos; también, de acuerdo con la magnitud y nivel de equipamiento de la infraestructura, puede proporcionar alertas relativas a amenazas y vulnerabilidades que puedan constituir peligros potenciales a la infraestructura crítica y la información tanto pública como privada.

Sin embargo, es posible que la euforia por la tecnología no nos haga ver que así como la internet y la PC, la tableta o el teléfono inteligente han revolucionado la vida moderna, al mismo tiempo se ha desarrollado todo un cuerpo de riesgos potenciales (se estima que existen unas 280,000 aplicaciones maliciosas) que afectan la cultura, la política, la economía, el gobierno, las empresas y los ciudadanos, y que en nuestras realidades, es una verdad insoslayable que no le concedemos la importancia que debería dársele, no obstante que el mundo ha sido y es testigo de la guerra silenciosa que en estos momentos se viene librando en el ciberespacio, que como se ha indicado anteriormente es una guerra

permanente, de larga duración con beligerantes que no dan la cara.

Hace unos años, el hacker más famoso del mundo Kevin Mitnick, a quien se le recuerda por haberse introducido de manera ilegítima en los sistemas informáticos de empresas como Motorola, Novell, Nokia y Sun Microsystems, para realizar llamadas de larga distancia y obtener información secreta a través de archivos almacenados en servidores, finalmente fue descubierto y condenado a 3 años de prisión; ya en libertad, actualmente Mitnick es un hombre reformado y dedicado a enseñar a empresas y expertos en informática las técnicas de cómo protegerse de la ingeniería social (se denomina así, en el contexto de la ciberseguridad, al arte de la manipulación de personas para que realicen acciones o divulguen información confidencial –en la mayoría de los casos, el atacante nunca conoce a las víctimas).

De momento ya existe una agenda global para enfrentar el problema; esta se refleja en los siguientes tópicos: normatividad de ciberseguridad; medidas de confianza y capacidad de respuesta.

Para el desarrollo de esta agenda se han constituido cuatro foros: el Grupo de Expertos Gubernamentales de Naciones Unidas (UN-GGE); la Organización Europea para la Cooperación en Seguridad (OSCE); el Foro Regional de ASEAN (ARF) y el Foro de la Organización de Estados Americanos (OAS). Está claro que el trabajo que desarrolla la UN-GGE tiene implicancias en todas las regiones del mundo hasta el nivel nacional. Para el caso de la región latinoamericana, el último reporte emitido por el Observatorio de Ciberseguridad de la OEA y el BID, recomienda que "Los gobiernos necesitan establecer organismos de ciberseguridad que incluyan como mínimo un equipo CERT (Computer Emergency Response Team), y una policía especializada en ciberdelitos.." (James A. Lewis: Observatorio de Ciberseguridad – Reporte 2016, pág. 5)

Por cierto, a nivel regional, enfrentar el reto requiere de la cooperación internacional, porque si algo se ha aprendido es que ningún país por sí mismo, actualmente, posee la capacidad de asegurar sus redes. La cooperación es esencial.

LA DIMENSIÓN ECONÓMICA DE LA CIBERSEGURIDAD

En el pasado la culminación de los mega conflictos como la I y II Guerra Mundial, la Guerra de la Península Coreana, de Vietnam, el Golfo o las varias guerras árabe-israelíes, trajeron como consecuencia etapas de depresión económica, principalmente para el bando perdedor y en general para la economía global.

Es muy ilustrativo el caso de la península de Corea. Cuando en 1953 concluye la guerra fratricida con la división del territorio, Corea del Sur inició el proceso de reconstrucción nacional desde las cenizas. Enormes sacrificios tuvieron que ser asumidos por el pueblo coreano ante la devastación y pobreza generada por el conflicto. Es digno y admirable reconocer el grado de resiliencia de esta cultura que actualmente es uno de los paradigmas del desarrollo y la tecnología, fundamentalmente en los campos de la electrónica y la informática, habiendo alcanzado la categoría de líder global en ciberseguridad.

Pues bien, hace ya varios años que asistimos al fin del conflicto en su versión tradicional, de ocupación y devastación de territorios enemigos (ciudades y pueblos) y destrucción de la infraestructura crítica ocasionando sufrimientos y dolor en poblaciones enteras. La recuperación y reconstrucción suponía grandes sacrificios económicos y por largo tiempo, muy aparte de las reparaciones económicas impuestas al perdedor. El beneficio económico que se irrogaba el vencedor generalmente estaba asociado a la captura de recursos y territorios estratégicos vía la ocupación o anexión geográfica; onerosas indemnizaciones pecuniarias entre otras condiciones humillantes.

Al parecer con el advenimiento de la era digital, asistimos a una notoria disminución del factor violento de la guerra, lo cual ha revolucionado la teoría del conflicto en tiempos de paz, tanto como la teo-

ría de los asuntos militares. La destrucción física se ha reducido ostensiblemente al igual que el derramamiento de sangre y el número de víctimas fatales directas e indirectas. A los escenarios terrestres, marítimos, aéreos y espaciales se ha sobrepuesto el escenario cibernético con sus características aquí expuestas.

Sin embargo, lo que no ha desaparecido, con el advenimiento del quinto escenario del conflicto - el ciberespacio - son las consecuencias económicas que se desprenden de un enfrentamiento o de un ataque cibernético sea cual fuera la modalidad empleada: invasión electrónica, ciberespionaje, ransomware, etc. El daño económico que se puede ocasionar puede superar al de una guerra convencional, con el añadido de que se enfrenta a un enemigo invisible, difícil de ubicar (al menos que se cuente con la tecnología más avanzada) y de sancionar obviamente.

Pero, ¿qué motivaciones pueden esgrimir el o los atacantes cibernéticos?. Pues hay muchas. Van desde las motivaciones estrictamente comerciales, industriales y de seguridad nacional (sustracción de información privilegiada, confidencial, propiedad intelectual, desarrollos estratégicos y secretos así como conocer y vigilar los movimientos del competidor u oponente); también están las motivaciones ideológicas, aquellas llevadas a cabo por personas o grupos terroristas, fundamentalmente ligados a doctrinas violentas.

Todo ello supone un enorme costo económico, empezando por la implementación de las estrategias preventivas para proteger todo aquello que se encuentra digitalizado en todos los campos de la actividad humana: gobierno, industria, energía, banca, comercio, educación, salud, seguridad, defensa, propiedad intelectual, propiedad privada, información personal, etc. Todo lo cual supone una organicidad o estructura relevante.

LA CIBERSEGURIDAD Y LA LEY

Las características del ciberespacio se pueden resumir en tres variables: tiempo (siempre disponible); espacio (sin límites ni fronteras); y, objeto (multicomunicación). En este contexto, para entender el marco legal de la ciberseguridad se tiene que considerar el efecto negativo de internet en nuestras vidas, la sociedad en su conjunto y la comunidad global. El hecho de que las comunicaciones por esta vía muchas veces no implican una relación cara a cara, ha generado desconfianza y la consecuente aparición del cibercrimen, la guerra cibernética, la invasión de la privacidad y el correo electrónico no deseado.

De acuerdo con el estado o nivel de ciberdefensa alcanzado por una organización o nación, los efectos negativos de internet o tecnología de la información, en su vertiente criminal, puede ocasionar: en el usuario: daño mental y financiero; en la empresa: pérdida de productividad y a nivel país, declive de la competitividad.

De ahí la necesidad de contar con un Sistema Legal de Ciberseguridad, el cual debería proporcionar las medidas de protección de los objetivos o infraestructuras críticas y los activos de información. Este cuerpo legal debe ser aplicable a los sistemas, redes, hardware e información; en el caso de las personas se aplica a todo el recurso humano que forma parte del sistema de redes, incluyendo los terminales, la gestión técnica de los procesos de manejo de información y las medidas de seguridad.

En el ámbito del derecho internacional, existe consenso que el jus ad bellum (derecho sobre el empleo de la fuerza) y el jus in bello (derecho de la guerra), se aplican al escenario del ciberespacio. Diversas resoluciones de Naciones Unidas han sido emitidas con la finalidad de crear una cultura global de ciberseguridad.

Otro importante marco de referencia legal sobre el cibercrimen está constituido por el Tratado 185 del Consejo Europeo (CoE) sobre el cibercrimen, producto de la Convención de Budapest del año 2001 y puesto en vigor en el 2004. Este marco legal tiene como objetivo la protección de la comunidad contra el cibercrimen, estableciendo procedimientos y políticas comunes para enfrentarlo; es de libre adhesión por los países que

reúnan ciertos requisitos. Al momento, se conoce que unos 130 países alrededor del mundo lo han utilizado como guía para establecer sus propias estrategias.

CONCLUSIONES

El vertiginoso desarrollo de las comunicaciones a partir de la era de internet, ha revolucionado el acceso a la información así como a la tecnología que la sustenta. Desde la creación de los primeros programas operativos para las computadoras, el software parece no tener límites; hoy en día se crean para toda necesidad de la vida diaria, desde los aspectos más domésticos hasta los de alta seguridad de las personas, empresas o Estados. Desde luego, hay también software creado especialmente con fines delictivos para cometer fraude en el sistema financiero, robar información, bloquear sistemas o simplemente lograr notoriedad. Es cada vez más frecuente en el mundo el llamado Cibercrimen, asunto que Naciones Unidas ya ha asumido como amenaza a la seguridad.

El rápido desarrollo de la tecnología de la información y comunicaciones va a la par con la expansión del cibercrimen; a su vez la innovación tecnológica crea nuevas vulnerabilidades en todo orden de cosas, en el IoT de los hogares, las empresas, el gobierno, la defensa nacional; de una manera general en todos los campos de actividad humana, sin distinguir si los blancos corresponden a una empresa grande o pequeña, a un Estado o nación desarrollada o en vías de desarrollo, o simplemente a un ciudadano. Una característica transversal a todo ello es la falta de toma de conciencia de la amenaza, en todo nivel.

La guerra mundial en el ciberespacio está teniendo lugar, las consecuencias potenciales pueden ser desastrosas y enfrentar poderes que deterioren las relaciones internacionales y ocasionen inconmensurables pérdidas económicas a los beligerantes. De otro lado, el fraude, robo de información y de bases de datos protegidas, la extorsión y la amenaza, teniendo como protagonistas desde una persona o mafia organizada para el delito, tienen un impacto tremendo sobre la confianza y moral del blanco atacado.

A nivel regional, todavía no se ha homogenizado una plataforma común para enfrentar la amenaza; los esfuerzos que los países vienen realizando, son todavía dispersos. Si bien es cierto la ONU y la OEA han tomado la iniciativa para hacer frente a esta amenaza, la agenda está cargada de temas pendientes, como por ejemplo la legislación ad-hoc (una buena base constituye los lineamientos de la Convención de Budapest), tanto como la implementación de la infraestructura adecuada que permita asumir la tarea de brindar ciberseguridad a la nación.

Está claro que la ciberseguridad contribuye al crecimiento y al desarrollo de un país, su descuido puede acarrear graves consecuencias al gobierno, el aparato productivo, la generación de energía y agua, la operación de aeropuertos, puertos, la bolsa de valores, el sistema financiero, la propiedad intelectual, los secretos militares o de Estado, y a los ciudadanos en general. No olvidemos que en el ciberespacio hay francotiradores (piratas, hackers, etc.), ejércitos bien apertrechados (bandas criminales dedicadas al ciberdelito), países competidores y beligerantes. Afortunadamente, por otro lado, también existen cada vez más herramientas para enfrentar estas amenazas.

BIBLIOGRAFÍA

- MacAfee Labs. 2016. Predicciones sobre amenazas 2016. Intel Security. EEUU.
- Mitnick, William. 2002. The art of deception, Controling the human element of security. Ed. John Willey and Sons. EEUU.
- OEA – BID. Cibersecurity, are we ready in Latin America and the Caribbean?. Inter American Development Bank. Washington. 2016
- Wegener, Henning. 2015. Riesgos Económicos de la Ciberguerra. Capítulo V. Cuadernos de Estrategia. IEEE. España.