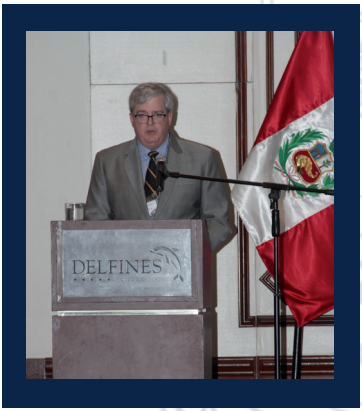
II SIMPOSIO INTERNACIONAL
DE SEGURIDAD Y DEFENSA
PERÚ 2015

CIBERESPACIO, CIBERSEGURIDAD Y CIBERGUERRA

Ph. D. Kevin Newmeyer



Ph.D. Kevin Newmeyer

El Dr. Kevin P. Newmeyer, de nacionalidad estadounidense, es el actual Director de Operaciones Senior de CREATE, Departamento del Programa de Modernización de Cómputo de Alta Performance para la Defensa dedicado al desarrollo de software de modelamiento avanzado utilizado en los programas de adquisiciones del Departamento de Defensa de los Estados Unidos.

Doctor en Filosofía, Política Pública y Administración por la Universidad de Walden, Minnesota. Políticas de Ciberseguridad en naciones en desarrollo con maestrías en Administración de Negocios por la Universidad George Mason, en Fairfax, Virginia; y en Relaciones Internacionales, por el Instituto Universitario Ortega y Gasset de España.

Experto en temas sobre Ciberseguridad y Defensa Nacional. Es docente de Prácticas en Asuntos de Seguridad Nacional en el Centro para Estudios Hemisféricos William J. Perry, de la Universidad Nacional de Defensa. Es diseñador y Director del Curso de Ciberseguridad para la Seguridad Nacional e Internacional. Fue Director a nivel global, para la Seguridad Estratégica y Contra Terrorismo en la corporación UNYSIS en los años 2006-2009. Estuvo a cargo del Planeamiento Estratégico en la oficina del Jefe de Operaciones Navales, en el Pentágono.

Entre sus publicaciones se puede destacar: El reto de Ciberseguridad para el Caribe: Funcionará el modelo americano?; ¿Quién deberá guiar los esfuerzos Americanos en Ciberseguridad?

INTRODUCCIÓN

Desde su aparición, algo nublada, entre la Segunda Guerra Mundial y la década del 60 y de la década de los 80 en adelante, la palabra "cyber" ha dominado las discusiones en un sin número de campos. Una búsqueda con Google proporcionó 323 millones de accesos en menos de un segundo. Haciendo la búsqueda con el vocablo hispano "ciber" brindó 15.3 millones de accesos en menos de medio segundo. La palabra china, equivalente Wangluo, generó aún más accesos que el vocablo inglés con 504 millones en 0.36 segundos. El vocablo "Ciber" está asociado, normalmente, a casi todas las palabras conforme la vida moderna se vuelve más dependiente de lo digital. Hoy en día, las personas portan normalmente en sus bolsillos una capacidad de cómputo que hace treinta años era considerado el ordenador existente más poderoso. La pregunta que surge ahora es: ¿Se ha mantenido la habilidad para desarrollar e implementar políticas a la par con la tecnología?

La tecnología moderna de la información y de las comunicaciones permite que cualquier persona pueda publicar sus ideas y compartirlas globalmente. Ya sea la joven estudiante paquistaní Malala Yousafazi, opinando sobre la educación de las jóvenes o sobre las violentas imágenes del Estado islámico. La tecnología digital está forjando nuevos medios para moldear la opinión pública. Los teléfonos celulares han permitido un crecimiento explosivo del número de personas que accesa a la red. La página Internet Live Stats (www.internetlivestats.com), estima que el 40% de la población mundial; es decir, más de 3 mil millones de personas hacen uso del Internet. En 1995, era menos del 1%. Con la finalidad de expandir el acceso a Internet y su mercado al 4.5 mil millones de personas restante, Google ha empleado globos aerostáticos (Geier, 2015). Si tan solo una fracción de estas personas entrara en línea vía proyecto LOON, Google recibiría miles de millones en ingresos anualmente. ¿Cómo podría alterar la economía o la seguridad del Perú, el acceso a internet de bajo costo en la Amazonía? ¿Tienen las leyes para regir y regularlo?

Titulares de noticieros recientes dan a conocer que continúan los ciberataques, así como que evolucionan constantemente. Los ataques han progresado desde simple alteraciones de las páginas web; pasando al espectro criminal de simples fraudes, hasta complejas actividades de espionajes. Stuxnet demostró que las herramientas cibernéticas pueden ser empleadas, no sólo para causar daños a los datos, sino tener también efectos físicos.

El ataque a Sony Pictures a fines del año 2014 demostró cómo la ingeniería social simple puede ser empleada para ingresar al núcleo del patrimonio intelectual de una compañía, así como un medio para generar políticas de respuesta. Los hackers de Sony manifestaron haber sustraído 100 Terabitios (1014 bitios) en información, incluyendo correos, películas de presentación y futuros guiones (Raile, 2014). Estos son solo algunos de los ejemplos entorno del Ciberespacio, Ciberseguridad y Ciberdefensa. Las definiciones, normas de comportamiento y las posibles actividades en el ámbito del bien y del mal, están aún en pleno desarrollo. En esta exposición vamos a explorar varios de los retos a las políticas que enfrentan los profesionales en el campo de la Seguridad y Defensa; así como presentar recomendaciones prácticas, para mejorar la Ciberseguridad. Es muy probable que nos conduzca a más interrogantes, sin embargo, esto es lo que hace que el mundo cibernético sea tan interesante.

DEFINICIONES

a. Ciberespacio: originario en el libro Neuromancer del escritor de ciencia ficción William Gobson, ha sufrido cambios desde la "alucinación consensual" hasta la definición que da el Departamento de Defensa de los Estados Unidos en la Publicación Conjunta 1 o" el dominio global dentro del entorno

de la información, que consiste en infraestructura para la información tecnológica; lo que esencialmente, vienen a ser todas las máquinas conectadas a internet y a la red que enlaza". La definición del Departamento de Defensa no incluye lo explícitamente la información residente dentro del sistema, a diferencia de la Unión Europea que sí incluye. (Ottis & Lorents, 2010)

Parece artificial separar la información de la infraestructura. En el Cibercrimen y Ciberespionaje, el blanco del ataque es generalmente la información. La información por sí misma tiene un valor. Personalmente prefiero una definición más inclusiva. Ciberespacio es el conjunto de dispositivos tecnológicos de comunicaciones para la información, la infraestructura de redes que los conecta, la información producida, redes y datos. En términos de Defensa y Seguridad, el Ciberespacio es un dominio comparable con los dominios tradicionales del poder militar como son el mar, aire, tierra y espacio (Kuehl, 2009)

A diferencia de los otros dominios, en los cuales prevalece una potencial posibilidad de conflicto, el Ciberespacio ha sido moldeado completamente por el hombre con fronteras inciertas y algunas normas para la política de Gobernación. El Ciberespacio solo promete crecer, como por ejemplo, conectar desde un refrigerador hasta un automóvil con el universo de cosas de internet.

b. Ciberseguridad: Nuevamente, no existe un consenso internacional en lo que constituye Ciberseguridad. Las definiciones nacionales, cuando existen, reflejan normalmente el cómo percibe una Nación la naturaleza de la amenaza del Ciberespacio (Lehto, Huhtinen & Jantunen, 2011). La amenaza puede provenir de la tecnología, o en varias naciones no occidentales, el contenido podrá ser transportado por las redes. Hansen y Nissenbaum (2009), trazaron los orígenes de la Ciberseguridad hasta discusiones por ordenadores de científicos en la década del 90, acerca de la debilidad en los sistemas de redes. La discusión sobre ataques, a la infraestructura crítica, y del rápido crecimiento del Cibercrimen en los últimos 20 y 25 años no hace sino complicarlo. Para el presente propósito, definamos la Ciberseguridad como el conjunto de prácticas políticas, de entrenamiento y tecnología, diseñada para proteger el entorno cibernético con la finalidad de asegurar la integridad de la información y habilidad de conectar dispositivos para que operen según diseño.

c. Ciberdefensa: De los tres términos anteriores, Ciberdefensa es probablemente el más fácil de definir y de entender. Muchas definiciones de Ciberdefensa consideran la adopción de tecnologías, prácticas y estrategias que buscan contrarrestar los ataques sobre los sistemas tecnológicos de información y data. Es una industria multimillonaria con mercados en los sectores militares, públicos y privados. Mientras que Ciberseguridad, es generalmente considerada en términos pasivos, como los cortafuegos y cifrado. La Ciberdefensa incorpora un espectro de componentes activos y pasivos. El paso de una medida pasiva a una activa es tal vez el nivel de política más desafiante. ¿En qué momento, si es que lo hay, conviene devolver el hackeo? Una vez más, esta es un área sin definiciones claras. Mientras que la defensa pasiva en Ciberdefensa puede ser entendida como la adopción en el mejor de los sentidos como por ejemplo, el mantener los parches del sistema actualizados, hacer uso de fuertes contraseñas e identificaciones multifactores; uso de programas anti malware, la defensa activa es algo diferente. La Ciberdefensa activa es más reciente y responde a una amenaza más significativa, la amenaza avanzada persistente o Amenaza Persistente Avanzada (APT) por sus siglas en inglés (ver Lachow, 2013). Originalmente definida por el Departamento de Defensa de los Estados Unidos en el Departamento de Defensa Estratégica para Operaciones en el Ciberespacio (2011, pág.7), la Ciberdefensa activa es:

La capacidad sincronizada del Departamento de Defensa, capacidad para descubrir en tiempo real, detectar, analizar y mitigar amenazas y vulnerabilidades. Se basa en aproximaciones tradicionales para defender las redes y sistemas del Departamento de Defensa, supliendo las buenas prácticas con nuevos conceptos operacionales. Opera a la velocidad de la red mediante el empleo de sensores, software

e inteligencia para detectar y parar la actividad maliciosa antes que pueda afectar las redes y sistemas del Departamento de Defensa. Toda vez que no se puede parar siempre a los intrusos en los límites de las redes. El Departamento de Defensa habrá de continuar operando y mejorando sus sensores avanzados para detectar, descubrir, mapear y mitigar la actividad maliciosa sobre las redes. El elemento importante en el concepto de Defensa activo es el de asumir que los malos actores están en capacidad de penetrar los sistemas tradicionales de Ciberegurídad. La Defensa activa involucra el constante monitoreo de los sistemas para hallar alguna actividad inusual.

Las Amenazas Persistentes Avanzadas merecen alguna definición. Las APT´s se diferencian de los bien conocidos ataques negados al servicio, desfasamientos de las redes y del tipo de crimen que aplasta y coge, en el cual los archivos de datos son robados y empleados para fines criminales. Los APT´s son eventos de larga duración, pensemos en meses y hasta años, donde el intruso permanece sin ser detectado al interior de la red, robando información. Con frecuencia se estima que la actividad es respaldada por Estados Naciones como herramientas de espionaje con la finalidad de robar datos militares (ver el informe de Mandiant en el APT1 en http://intelreport.mandiant.com). Existe un evidente incremento en el que las instituciones comerciales tales como los bancos que están siendo blanco de actividades criminales APT. Kaspersky anunció en febrero de 2015 de que un grupo criminal había penetrado aproximadamente 100 bancos en 30 países (Robinson, 2015). Los hackers pudieron monitorear por largo tiempo, las operaciones de los bancos víctimas. Luego, empleando metodología estándar de los bancos, los criminales efectuaron transferencias fraudulentas de dinero hacia cuentas controladas, robando $ 100 millones por banco, sumando en total $ 1 Billón.

RETOS A LAS POLÍTICAS CIBERNÉTICAS

a. Soberanía

El mundo Cibernético presenta los retos al conocimiento tradicional de Soberanía. Sin embargo, esto no significa que las naciones dejen de jugar un rol importante. Las leyes internacionales, así como los principios legales tradicionales, le otorgan al Estado Nación el monopolio de la fuerza coercitiva y la habilidad para hacer cumplir las leyes y reglamentos dentro de su territorio. Aun cuando el Ciberespacio es frecuentemente referido como un entorno sin fronteras, que existe dentro de una dimensión. Todos los ordenadores, servidores, switches y el cableado permiten al Internet que exista en un espacio físico. El espacio físico está sujeto a las leyes y reglamentos de la Nación que lo acoge. En forma análoga, las señales que viajan de un Estado a otro, están igualmente sujetas a las leyes y reglamentaciones de los países por los cuales cruza. Uno de los retos es el correspondiente a que la ruta no es necesariamente fija. La información en su totalidad, no requiere seguir el mismo camino y el Estado podrá no tener la capacidad técnica para ver y entender lo que está cruzando por su territorio. Si no se cuenta con el capital humano entrenado correctamente y el equipamiento técnico, ¿podrá un Estado ejercer su soberanía?

b. Estructuras Legales Internacionales

Si el Estado cuenta con la capacidad técnica, así como con el personal entrenado, entonces tendrá la estructura legal y las políticas apropiadas para actuar. Cuando el Hacker filipino lanzó el virus I LOVE-YOU, el 05 de mayo del año 2000, este se diseminó hacia Occidente, siguiendo los días laborales alrededor del mundo. El virus causó miles de millones de dólares en pérdidas productivas, y miles más en su eliminación. Los autores de los virus fueron identificados en el transcurrir de algunos días y arrestados. Luego fueron liberados y los cargos desechados toda vez que en las leyes filipinas no está

tipificado y por lo tanto, no constituye un delito escribir y lanzar un virus. Como los autores se encontraban en Manila al momento de lanzar el virus, no pudieron ser extraditados a los Estados Unidos u otra parte, por no cumplir con el requisito de la dualidad del crimen, para que proceda la extradición de acuerdo a los tratados. Sprinkel (2001) pudo notar los efectos de este caso sobre el desarrollo del Tratado Internacional con respecto al Cibercrimen.

El Concilio de la Convención Europea sobre el Cibercrimen (2001), proporcionó la primera y hasta ahora el único Tratado, que rige los esfuerzos internacionales sobre el Ciberespacio. El Tratado proporcionó la definición para varios cibernéticos relacionados con la data y sistemas, incluidos los correspondientes al acceso ilegal, interferencia de datos, interceptación ilegal de datos y empleo ilegal de los dispositivos. El Tratado, también define los crímenes relacionados a los ordenadores, tales como falsificación y fraude. La convención también penaliza la producción, almacenamiento y distribución por computadora de pornografía infantil y alberga medidas para proteger la propiedad intelectual. También sirve como un Tratado de extradición entre los países partes de la convención y posee medidas para el apoyo legal mutuo para aquellos que retengan y obtengan dispositivos electrónicos. Sin embargo, posee limitaciones.

Solamente 45 Estados forman parte del Tratado, de los cuales seis integrantes se encuentran fuera de Europa, al mes de marzo de 2015. En Latinoamérica, sólo República Dominicana y Panamá son miembros, mientras que Perú, Colombia, México, Costa Rica, Argentina y Chile han sostenido discusiones sobre la conveniencia de incorporarse. Cabe resaltar que varias potencias cibernéticas no se han incorporado al Tratado; como son China, Rusia, India y Brasil. Este último ha propuesto que las Naciones Unidas desarrolle un nuevo Tratado que contenga más aportaciones de los países emergentes.

Otros esfuerzos internacionales dirigidos a establecer tratados sobre el Cibercrimen y Ciberseguridad, permanecen estancados. El occidente desarrollado, ha rechazado los esfuerzos para establecer que la Unión Internacional de las Telecomunicaciones (UIT), sea la Autoridad Internacional responsable de la Ciberseguridad (Downes, 2012). Mientras tanto, continúan los debates con respecto a la definición de Ciberseguridad. Los Estados Unidos, Europa Occidental, Japón y sus Aliados, concentran el debate de Seguridad sobre amenazas a las operaciones e integridad de las redes y datos. China, Rusia y varios países del Medio Oriente así como sus Aliados, van tras una interpretación más profunda que, analice el contenido del material en línea, bajo una postura más amplia de seguridad de la información, (Lindsay, 2015; Ministerio de Asuntos Exteriores de la República Popular de China, 2011) sobre la diferencia de libertad de expresión, que enfrentan los límites de Seguridad, que restringen la posibilidad de cualquier acuerdo internacional sobre Ciberseguridad.

El área donde aparentemente crece el Consenso Internacional sobre las leyes cibernéticas es aquel correspondiente a la aplicabilidad de las leyes sobre los conflictos armados hasta el del dominio Cibernético. A través de trabajos tales como el Manual Tallín (2013), así como el esfuerzo del Comité Internacional de la Cruz Roja y otros, los conceptos sobre las leyes internacionales humanitarias, se consideran aplicables a la Internet. El reto estiba en la aplicación, particularmente sobre actores que no son Estados y que no han estado sujetos a las leyes humanitarias internacionales. Los incidentes cibernéticos, que salen del espectro de los conflictos de las Fuerzas Armadas, pueden tener efectos directos sobre poblaciones protegidas.

c. Retos Domésticos

Adicionalmente a los retos de nivel internacional, las naciones deben enfrentar la dificultad de los retos de políticas domésticas, correspondientes a los Cibercrímenes y Ciberinseguridad. En los últimos diez años, numerosos Estados han publicado Estrategias Nacionales sobre Ciberseguridad y políticas diseñadas para mejorar sus defensas contra la Ciberamenaza y posicionarse mejor para acceder a las oportunidades creadas por el desarrollo de la Tecnología de la Información (Falessi, Gavrila, Klenstrup,& Moulinos, 2012; Luiijf, Besseling & Graaf, 2013).

Estas políticas han sido diseñadas para referirse a las áreas deficientes de estructuras legales, vigilancia gubernamental, protección de infraestructuras críticas, educación y comunicaciones público-privadas que obstaculizan la habilidad del Estado y la del sector privado para responder a los problemas en el Ciberespacio. No es que solamente el mundo desarrollado esté buscando mejorar la Ciberseguridad (Newmeyer, 2014). Las naciones emergentes tales como Panamá, Colombia, Trinidad y Tobago y apenas este año Jamaica; se han unido junto con Sudáfrica, Malasia y otros, en la facilitación de políticas públicas. De cómo orientan su seguridad; aplicación de la ley, educación y en algunos casos, la mejora de los sectores privados en su habilidad para responder a las amenazas y el apalancamiento de las oportunidades económicas en el Ciberespacio.

Un elemento clave en la respuesta doméstica a los retos cibernéticos corresponde al desarrollo de una infraestructura nacional y organización que se encargue de recolectar la información y de organizar la respuesta. El desarrollo de un Equipo de Respuesta a Incidentes de Ciberseguridad Nacional CSIRTs o Equipos de Respuesta de Emergencias Informáticas (CERTs) son una de las principales recomendaciones a los Estados, a fin de mejorar la Ciberseguridad. Esto ha sido por décadas, el elemento clave en el programa de Ciberseguridad de la Organización del Comité Interamericano de los Estados Americanos contra el Terrorismo (CICTE). Un CERT provee un punto focal para la información de Ciberseguridad y Ciberdefensa. La investigación conducida por Microsoft, ha demostrado que las naciones con políticas sobre Ciberseguridad, organizaciones CERT, y leyes estrictas de protección a la propiedad intelectual; han tenido pocos incidentes de Malware (Klieiner, Nicholás & Sullivan, 2013).

d. ¿Seguridad o Defensa?

Las políticas nacionales sobre ciberseguridad pueden establecer las responsabilidades entre las agencias de defensa y de seguridad. Qué agencias son responsables de responder ante qué amenaza? Los retos incluyen determinar el origen y/o el objetivo de la amenaza. Es el ciberataque sobre una empresa utilitaria un esfuerzo que busca extorsionar? Una venganza por una acción personal negativa? O un intento por inutilizar un radar o la alarma de un banco que viene siendo alimentada desde una subestación determinada? Tienen ustedes los medios para detectar el ataque?

e. Cibercrimen

Aun cuando se considera mínima la respuesta militar ante la amenaza de un Ciberataque, es una preocupación permanente. Un informe reciente del Centro de Estudios Estratégicos e Internacionales (CSIS), ha estimado las pérdidas debido a Cibercrímenes en $ 445 mil millones para el año 2013.

Muchas de las pérdidas involucran el robo de la propiedad intelectual. enfocada en secretos militares y corporativos. Una cantidad considerable de Cibercrímenes están directamente dirigidos a las ganancias financieras. Los Hackers han penetrado compañías como por ejemplo la Sony y muchas otras, con la

finalidad de sustraerles información de tarjetas de crédito, para luego emplearlas con fines fraudulentos. Los ataques a los cajeros automáticos han generado pérdidas por $ 2.4 millones de dólares en 24 horas en la ciudad de Nueva York, durante el mes de febrero de 2013 (Bray, 2013). Esto fue parte de un ataque del crimen organizado a nivel global, que afectó a 36,000 máquinas ATM en 20 países en los cinco continentes; causando pérdidas por $ 40 millones.

En febrero de 2015, Kaspersky publicó un reporte sobre el Cibercrimen perpetrado por el grupo Carbanak, el mismo que en una serie de robos cerca de 100 bancos, sustrajeron aproximadamente $ 1 billón de dólares alrededor del mundo. Estos criminales explotaron las debilidades del sistema de seguridad y de la naturaleza humana, para penetrar al interior de las mayores instituciones, y permanecer en éstas durante un largo período de tiempo. Estos ataques a largo plazo permitieron a los criminales introducir registros y transacciones fraudulentas, las que aparentaban ser normales para los bancos; por lo que no fueron detectadas por los sistemas antifraude. Las herramientas criminales pueden ser adquiridas en Internet o aprendidas en YouTube. Los esfuerzos de la ley, inadecuadamente financiados, hacen que el esfuerzo para perseguir a los criminales no sea efectivo; sino hasta imposible, aún cuando los crímenes son detectados.

Poder determinar el blanco y las intenciones de un ataque Cibernético, está estrechamente relacionado con el problema de la asignación de funciones en los asuntos cibernéticos. Los protocolos operacionales subyacentes, encargados de controlar la transferencia de información por Internet, han sido diseñados para maximizar la probabilidad de que la información llegue hasta su destino. En estos protocolos no se consideró la incorporación de artilugios de seguridad. Es fácil dirigir la información a través de múltiples países y encubrir así su origen. Las prácticas de seguridad pobres permiten que los ordenadores sean capturados por terceros y empleados para lanzar correos no deseados (spam), diseminar virus o unirse a ataques que nieguen el servicio.

La negación del servicio es fácil de crear. La dificultad en las atribuciones impone limitaciones a los encargados del planeamiento de políticas y de ejecutar acciones en respuesta. A diferencia de los ataques militares históricos, la estela de un cohete Cibernético, no deja trazos que marquen el punto de lanzamiento. La habilidad de un actor que no sea un Estado para perpetrar un Ciberataque, complica aún más la respuesta que un Estado puede dar a esta agresión (Tsagourias, 2012).

OPCIONES DE RESPUESTA

Luego de reconocer los retos ¿cuáles habrán de ser opciones de respuesta viables para el Estado, organizaciones e individuos? ¿Es la Ciberdefensa una respuesta activa o pasiva? ¿podrán ser ambas? Un estudio llevado a cabo en los últimos años, indica que existen medidas prudentes que las personas individuales, organizaciones y las naciones pueden implementar a fin de mejorar su Ciberseguridad. Estas buenas prácticas nos llevan a las cuatro áreas vulnerables a las incursiones cibernéticas:

- Programas (Software),
- Equipamiento (Hardware),
- Políticas
- Personas

El instituto SANS y el Departamento Australiano del Directorado de Defensa de Señales (ASD) han publicado un listado de buenas prácticas para la Ciberseguridad. Los dos listados contienen recomendaciones similares con ligera diferencia de terminología. La lista del SANS conteniendo los Controles de Seguridad Críticos considera 20 recomendaciones. (http://www.sans.org/critical -security-controls/). El listado australiano considera por su parte 35 recomendaciones (http://www.asd.gov.au/infosec/mitiga-

tionstrategies.htm). Las recomendaciones son básicamente las mismas y sirven como una lista de verificación conveniente para que las autoridades superiores; que no poseen el conocimiento profundo sobre el dominio cibernético, puedan llevar a cabo una vigilancia.

Estas medidas no son particularmente difíciles de implementar tecnológicamente. Los australianos hallaron que con tan solo implementar las primeras cuatro recomendaciones se logra evitar el 85% de los ataques. Estas cuatro recomendaciones son:

a. Aplicación del listado blanco: Esta permite que solo las aplicaciones autorizadas corran en el sistema y evita que Malware y programas no autorizados sean ejecutados.

b. Parchado de las aplicaciones y sistemas operativos: Mantener los programas actualizados con los últimos cambios evita que se exploten los defectos conocidos. Los ataques pueden generarse para explotar debilidades publicitadas en tan solo 8 horas y ciertamente dentro de los 2 días.

c. Correr sólo las últimas versiones del sistema operativo: El riesgo de que un parche nuevo quiebre el sistema es relativamente bajo. Ya que toma dos semanas para probar completamente un parche; genera que el sistema quede muy vulnerable y ser aprovechado por los adversarios.

d. Restricción de los privilegios administrativos: Los bandidos apuntan hacia los usuarios con administración de privilegios, ya que estos cuentan con acceso de alto nivel a los Sistemas Tecnológicos de la Información y Comunicaciones (ICT) de una organización. Si una cuenta administrativa ICT se ve comprometida, es muy sencillo para el adversario enmascararse y continuar con la explotación.

Estos mecanismos afectan a muchos programas, hardware y políticas emitidas entorno a la Ciberseguridad. Sin embargo, éstas no van a evitar todos los intentos de explotación. El personal se ubica como el eslabón más débil en la cadena de Ciberseguridad. La Defensa en profundidad de los cortafuegos (firewalls), los antivirus y las contraseñas más complejas pueden ser by paseadas por un ejecutivo pobremente entrenado o por un determinado intruso.

La "pesca" (fishing) y la "pesca con arpón" (spear fishing), permiten al hacker saltarse todos los mecanismos defensivos de la organización. Los ataques por pesca permiten sustraer la propiedad intelectual, comprometer los sistemas bancarios y dañar la Seguridad Nacional (Hong, 2012). Estos ataques pueden ser altamente sofisticados, pero con frecuencia, sólo requieren algo de ingeniería social para ser exitoso. La mínima alteración del nombre de un dominio, como de paypal.com hacia paypal1.com; va a lograr frecuentemente, que la víctima cliquee sobre el enlace que va a introducir Malware en el ordenador víctima.

Un falso correo del vicepresidente de una compañía, puede tentar a un subordinado a abrir un archivo adjunto infectado. Una vez dentro de la máquina, el Hacker puede instalarse y explorar las redes de la víctima; los enlaces con los compañeros de la compañía y sustraer información a voluntad. Aunque algunas políticas como la inhabilitación de ciertas características de los navegadores y el filtrado avanzado de los correos que ingresan reducen los riesgos, es necesario entrenar a los individuos para que estén atentos a las técnicas de ingeniería social así como a emplear las mejores prácticas.

La amenaza del intruso es tal vez la más difícil de enfrentar. Tradicionalmente las medidas individuales de seguridad, permiten el acceso a información de apoyo sensible; pero como el caso de los WikiLeaks y de Snowden demostraron, estas medidas están lejos de ser efectivas. Limitando el acceso del

administrador es el primer componente de una Defensa. Sin embargo, el elemento más importante es el monitoreo activo de lo que está ocurriendo al interior de las redes (Park, Yim & Hallahan, 2013). El acceso a la información requiere de un estrecho vínculo con el empleo. ¿Por qué habría de hurgar un cocinero en archivos de un médico? La apertura de puertos de acceso a internet inusuales, deberá ser investigada e identificada. La Amenaza Persistente Avanzada (APT), típico de actividades criminales y espionaje avanzadas, requiere que los operadores entiendan lo que sus redes deben estar haciendo, a fin de detectar la actividad anómala que está ocurriendo.

La medida defensiva final, a ser considerada, corresponde al tópico emergente de Defensa Activa o "devolviendo el hackeo". Dittrich y Himma (2005) describen la Respuesta Activa Continuum (RAC) como el espectro de respuestas que van desde las de uso pasivo, como son los programas anti Malware; hasta el traqueo y ataque a las redes del intruso. Los modelos de negocios nuevos se enfocan sobre el final agresivo del continum; sin embargo, las consecuencias legales y técnicas distan de ser claras.

El problema de atribución se mantiene, por lo que es difícil de determinar la fuente real del ataque o intrusión después de los dos o tres saltos. Los conceptos tradicionales de autodefensa limitan la magnitud de la respuesta al nivel necesario para detener la amenaza. La definición de esta capacidad en términos cibernéticos dista de ser exacta. Sin embargo, los pasos intermedios en la Respuesta Activa Continum (RAC), proporcionan el espacio suficiente para que actúen los defensores cibernéticos entrenados.

Cuando las defensas se asocian con el monitoreo activo, es posible que se puedan calibrar los ajustes de las defensas de la red; modificar los programas y colectar información acerca de los métodos de ataque. Si es coherente con el marco legal, la defensa podrá iniciar también el acopio de información contra los agresores o aperturar el diálogo con las fuerzas del orden, o socios industriales, para optar por medidas de respuesta cooperativas.

CONCLUSIONES

Queda claro que las amenazas Cibernéticas se encuentran en franco incremento. El rango de éstas va desde la actividad criminal tradicional del hurto y fraude, hasta el espionaje avanzado y daño a la información y el equipamiento. La Defensa Cibernética requiere de un esfuerzo político coordinado, a fin de establecer las estructuras legales, programas educacionales y de la capacidad institucional para responder a los acontecimientos que se presenten a lo largo del espectro de amenazas. El reto no es insuperable, pero requiere que las instituciones, empresarios y el gobierno inviertan tiempo y dinero. Muchos de los riesgos pueden ser reducidos significativamente, mediante la adopción e implementación rigurosa de algunas buenas prácticas. La tarea para los líderes está en reconocer los riesgos y disponer las acciones convenientes.

PANELISTAS

C. DE N. ENRIQUE CUBEIRO

Capitán de Navío de la Armada española. Actualmente preside el Grupo de Trabajo de Implantación de la Ciberdefensa en el ámbito marítimo, que deriva de la Estrategia de Seguridad Marítima Nacional. Estuvo al mando del buque Patiño en la Operación Atalanta (2012), donde se produjo el apresamiento de los primeros piratas juzgados y condenados en España por el delito de piratería. Se ha especializado en: Sistema Meroka Naval (E.T.A.N. Janer, Cádiz); Comunicaciones (E.T.E.A., Vigo), Link-11 (CPT-CIA, Rota); Oficial de Acción Táctica (Escuela de Guerra Naval, Madrid); Curso de Técnicas Pedagógicas (EMCE, Madrid); NATO COMSEC Officer Course (NCISS Latina); EMFAS (ESFAS. Madrid); Derecho Internacional Humanitario (Cruz Roja Internacional). Se destaca en su haber premios como Defensa 2002, y por la monografía "Sistemas de mando y control: una visión histórico-prospectiva". Así también con el mérito al primer Premio Revista General de Marina 2013, por el artículo "Aaba, Maxaa Nahay Kalluumaysato", sobre la piratería en Somalia. Cuenta con reconocimientos, por mencionar algunos como: 5 Cruces del Mérito Naval.

CNEL. FAC MARTHA SANCHEZ

Oficial de la Fuerza Aérea colombiana, profesional en Ingeniería de Sistemas. Es Coordinadora del Programa Académico e Investigación de Ciberdefensa, desde el 2012 en el Ministerio de Defensa- Escuela Superior de Guerra de Colombia (ESDEGUE). Asimismo, cuenta con maestrías en Administración de empresas y en Seguridad y Defensa Nacional. Es Especialista en Sistema de la de Información y de Gerencia Técnica de Telecomunicaciones. Entre sus logros se destaca: El Desarrollo de los primeros juegos cibernéticos del sector defensa; preparación e incorporación de la cátedra de Ciberguerra en el pensum de la ESDEGUE. Desarrolló varios seminarios en Ciberdefensa y Ciberterrrorismo como impacto a la Seguridad Nacional, en colaboración con el Grupo Militar EE.UU 2013; "Cyber Threats to National Security", dirigido al CAEM y líderes del sector, en colaboración con el Grupo Militar EE.UU 2014. Tuvo a su cargo la creación de la maestría de Seguridad y Defensa Cibernética de la Escuela Superior de Guerra de Colombia.

PANELISTAS

CALM. (r) OSCAR ANDERSON

Óscar Anderson Machado, Contralmirante en retiro. Actualmente es Subdirector del Centro de Estudios Estratégicos y Marítimos de la Escuela Superior de Guerra Naval del Perú.
Es especialista en Defensa Nacional por el Centro de Altos Estudios Nacionales (CAEN); en Seguridad Naval por la Dirección de Inteligencia; Guerra Electrónica Básica, estudios realizados en Dam Neck Virginia - Estados Unidos de Norteamérica; especialista en Electrónica, estudios realizados en la República Federal de Alemania.
Fue inspector interno de la Dirección de Telemática y encargado del Proyecto del Sistema de Comando y Control. Ha tenido a su cargo la Subdirección de Telemática y encargado del Proyecto del Sistema de Comando y Control de la Marina de Guerra del Perú. Fue Director de Política y Estrategia en el Ministerio de Defensa. Asimismo fue Jefe de Comunicaciones y Guerra Electrónica de la Comandancia de Operaciones Navales.

C. de N. Enrique Cubeiro

El título de mi presentación como pueden ver es "Ciberespacio, nuevo campo de batalla". Durante los próximos minutos lo que pretendo es intentar explicarles por qué y para qué hemos llegado los militares al Ciberespacio y para ello me van a permitir que hagamos un pequeño recorrido histórico a través de la evolución de los dominios de la guerra.

Desde el principio de los tiempos, el hombre ha combatido sobre el terreno, a lo largo de los siglos se han ido perfeccionando las armas y las técnicas de combate. Primero se incorporó la caballería, las armas de fuego, la artillería; aparecieron las armas químicas, los vehículos blindados, el apoyo aéreo y armamento cada vez más preciso y sofisticado.

El mar fue el segundo dominio de la guerra. Al principio se empleaban naves que combatían al abordaje. Posteriormente llegó la propulsión a vela y ya en la Edad Media, la artillería naval. En el siglo XIX aparece la propulsión a vapor, que es una auténtica revolución para este ámbito. En el siglo XX el submarino se convierte en un arma decisiva y la táctica, así como la estrategia naval ha de evolucionar continuamente con la aparición sucesiva de la Aviación Naval; los misiles, las comunicaciones por satélite, la propulsión nuclear y las tecnologías externas. Hay que esperar hasta el siglo XX para apreciar cómo el aire se convierte en un campo de batalla que hasta entonces tampoco había sido utilizado. Tan solo se había empleado para aumentar el horizonte de opciones generales, para ver la disposición y los movimientos del enemigo sobre el campo de batalla. Como en los casos anteriores, la revolución tecnológica obliga continuamente a revisar conceptos doctrinarios, los que se originan en combate. En otra relación el radar, los misiles, las aeronaves no tripuladas. A finales del siglo XX el espacio pasa a ser también objeto del interés militar. Las operaciones militares se apoyan cada vez más en las comunicaciones vía satélite como medio vital para el ejercicio de mando y control de los satélites de observación para las operaciones del Ejército. Las potencias más avanzadas desarrollan capacidades para impedir el uso de estos medios al enemigo. Ya en la frontera en el siglo XX y XXI aparece el quinto dominio de la guerra: el Ciberespacio. Un dominio en donde, como los anteriormente mencionados, se puede combatir y en donde hay que defender los intereses; los intereses propios de las fauces del enemigo. Un dominio que puede llegar a tener enorme influencia sobre los otros cuatro y que tienen unas peculiaridades que van en completa diferencia a todos los anteriores. Como hemos podido ver, durante la práctica y totalidad del estudio de la humanidad han existido tan solo dos dominios de la guerra. En el último siglo han aparecido otros más. Todos productos de la función tecnológica. Por lo tanto, no es descabellado pensar que en los próximos años veremos aparecer otros dominios de la guerra.

¿Y qué tiene de especial este nuevo dominio que nos acaba de llega? pues tiene mucho. Se trata de un dominio prácticamente infinito, parecido al dominio del espacio. Un dominio en que las fronteras están muy poco claras, muy poco definidas. No existe la claridad que hay en otros ámbitos en los que se utilizan unas armas y unas técnicas de combate completamente diferentes a las anteriores, o las que se han utilizado hasta ahora en los campos de batalla tradicionales. Un dominio en que no existe ningún tipo de control armamentístico y en el que además existen mucho más actores que en el resto de dominios. En el mar, en la tierra, en el aire; el armamento está normalmente en poder de los ejércitos o de las fuerzas y cuerpos de seguridad del Estado. En el Ciberespacio el armamento está prácticamente en poder de toda la humanidad. A ello se suma un entorno legal y complejo y si ya no es muy complejo; el ámbito del cibercrimen la cosa se complica todavía mucho más, cuando lo trasladamos al campo militar. Es muy difícil trasladar conceptos hasta ahora conocidos como ataque armado, como autodefensa, como acto hostil, como intento hostil al espacio. Podemos decir en cierto modo que el Ciberespacio es una especie de estado fallido, en el que esta autoridad favorece como siempre al agresor.

Por otra parte, es un dominio al que no es ajena ninguna actividad del Estado. Prácticamente, por no decir todas las actividades del Estado que apoyan de alguna u otra manera en el Ciberespacio como es el: transporte, economía, banca, energía incluso el ocio se apoya en el Ciberespacio. Y por último, quizá lo más importante de todo, se trata de un dominio en el que por primera vez se pone el corazón de la Nación en primera línea de combate. Un dominio además en el que existe una intensa actividad en todo momento. Desde el tiempo de paz, al tiempo de crisis y en tiempo de conflicto. Podemos hablar que existe una permanente e intensa actividad soterrada al Ciberespacio. Un dominio en que tratamos como en el resto, de explotar las vulnerabilidades del adversario, al mismo tiempo defendemos las propias relacionadas al enemigo.

Las hay de tipo físico; errores de diseño, errores estructurales; las hay de tipo lógico, fallas de programación y de tipo humano; es decir, la indolencia de los usuarios. El no seguimiento de políticas en seguridad o como ha dicho el profesor Newmeyer, los ensayos que son una auténtica amenaza porque es cuando el enemigo tiene el acceso privilegiado a nuestros sistemas. Un dominio a través del cual es posible acceder a una gran variedad de objetivos, no solo a la información, o a los sistemas de información atentando a la integridad, a la confiabilidad o a la disponibilidad de información y a la propia integridad de los sistemas; sino también a un dominio en que está demostrado se puede atentar contra las infraestructuras y en el que también las personas son objetivo. Cada vez más hemos aumentado en la superficie y a defender en los últimos años de manera exponencial con la presión del almacenamiento de la nube, expresamente en la nube, los Smart phones, cada vez más potentes y la proliferación de las redes sociales en donde muchas veces se publica información confidencial o altamente sensible.

Y ¿de qué y o de quién tenemos que defendernos en el Ciberespacio? Con la diapositiva tengo una pequeña muestra de los niveles de los agresores potenciales y de las capacidades de aquellos que energía en el espacio. Y lo más bajo de su estrato en el ecosistema, pues encontramos a personas que simplemente lo utilizan como armas descargables perfectamente fáciles elaborar gratuitamente en Internet y que son capaces de hacer pequeñas cosas como robarle la contraseña. A partir de allí, a medida que tienen las capacidades técnicas como agresores, forman grupos organizados lo que va a permitir llevar a cabo ataques cada vez más complejos. En los últimos años en la cúspide del ecosistema aparecen las APTs. De lo que ha hablado también el profesor Newmeyer, que son equipos multidisciplinares, capaces de llevar ataques muy complejos, muy difíciles de detectar y que pueden mantenerse mucho tiempo sin ser detectados por la víctima. Y ¿con qué, cómo y de qué nos tenemos que defender? Los militares en el Ciberespacio normalmente no cuentan con ninguna técnica, herramienta o arma que no sea la que usan contra la delincuencia, contra el espionaje o contra el hackeismo. Son las mismas que se emplean en cualquiera de estos ámbitos en el mundo militar.

El siguiente esquema trata de representar las diferentes modalidades y acciones en el Ciberespacio en función de su finalidad y efecto. En general las acciones ofensivas son más fáciles de detectar, obviamente siempre y cuando conozcamos sus efectos. Si bien una cosa muy diferente es la detección, la trazabilidad y aún más difícil, la capacidad de atribución. Si bien hay unas pautas fijas, un ataque complejo puede requerir la combinación y un buen número de técnicas iniciándose por regla general, con la recopilación de datos y objetivos, mediante técnicas de inteligencia. Inteligencia digital que permita posteriormente la infiltración o infección. Siendo el propio objetivo algún otro elemento que pudiéramos identificar como ciberataque, que busca la obtención o la alteración de la información; la negación o eliminación de algún servicio del adversario, incluso su propia destrucción física como se ha demostrado en casos anteriores. Como digo los ataques son cada vez más sofisticados y pueden llegar a encadenar todas las modalidades vistas en la diapositiva anterior. Es el caso de las APTs (Advanced Persistent Threats). Un ataque cada vez más común cuya metodología típica es la que tienen en la diapositiva. El primer paso es el compromiso inicial realizado mediante el uso conveniente de las técnicas

de inteligencia y de infiltración. Esto permite al atacante la obtención de un punto de apoyo mediante la implantación a la víctima de algún software de administración remota y la creación de puertas traseras y túneles que permitan el acceso sigiloso a nuestra estructura.

El siguiente paso se apoya en el uso de displays y técnicas de descifrado y contraseñas, con el fin de adquirir privilegios en administración sobre la computadora víctima y ampliarlo a las cuentas de administración de dominio, lo que posibilita la recopilación de información sobre la estructura circundante, las relaciones de confianza y la estructura de dominio. Mediante un movimiento lateral el control se amplía a otras estaciones de trabajo, servidores y elementos de la infraestructura de la red. Es una ventaja la persistencia manteniendo una presencia continuada que permita el control sobre los canales y acceso; credenciales adquiridas en los pasos anteriores.

Y por último en cumplimiento de la misión según sea el objetivo perseguido; la filtración de información, la delegación de servicios o la descripción de alguna infraestructura. Es importante entender que hay algunas fases de este proceso que pueden durar meses y cuyos efectos pueden ser mantenidos durante años sin que la víctima sepa que está siendo atacada. En la actualidad en la práctica, la totalidad de naciones avanzadas cuentan con unidades especializadas en su defensa. Por regla general, el ámbito de actuación de estas unidades en sistemas militares, aunque algunos casos y circunstancias se amplían estos sistemas relacionados con infraestructuras críticas. Se enfoca prioritariamente hacia la protección de la defensa de los sistemas. Sus capacidades suelen adaptar también lo que se denomina inteligencia y amenazas a las operaciones de respuesta a un ataque. Sin embargo y a pesar que un buen número de naciones han redactado y publicado sus estrategias nacionales de la Seguridad de la Defensa, todavía no se ha logrado una visión clara sobre cuestiones estratégicas fundamentales, a lo que contribuye un origen de número de factores.

Aquí les presento algunos de ellos y es probablemente el más importante, dadas las habilidades de la defensa de la que ya les hablé antes y que afecta a todas actividades del Estado. Pero hay muchos más, la situación legal de la que también he hablado. La ausencia de normativa común impredecible de los ataques y su alcance, la cada vez más compleja y superficie a defender, la fragmentación de las responsabilidades, la volatilidad tecnológica que nos obliga continuamente a adaptarnos a las nuevas tecnologías y a renovar máquinas, a renovar sistemas operativos, a actualizar software. Las dificultades y atribución de la disuasión. Ahora mismo creemos que no hay ninguna Nación en el mundo con capacidad de disuasión en el Ciberespacio. También la existencia de un control en el armamento, la difícil gestión de la crisis de la determinada ambigüedad intrínseca a muchas de las posibles acciones en el Ciberespacio. Por otra parte a excepción de eventos puntuales, hasta el momento no ha acontecido en la historia del mundo ningún conflicto armado en el que el Ciberespacio haya jugado un papel preponderante. Esto convierte cualquier pensamiento en este campo en un ejercicio especulativo que tendrá que afinarse con la experiencia. Pues bien, para finalizar, en ese contexto uno tiene que pasar los retos a los que se enfrenta en la mayoría de las naciones con temas militares; en esta integración para la Defensa, en el proceso de Planeamiento Operativo. A fin de alcanzar un nivel adecuado de coordinación y sincronización con el resto de acciones militares y convencionales.

Esta tarea no es nada fácil y gran parte de la dificultad radica nuevamente en la versatilidad de la autodefensa, al afectar no solo las comunicaciones en su interior; sino también, operaciones, inteligencia, logística, planes y formación pública e incluso personal. En ello estamos.

Coronel FAC Martha Sánchez

Bueno, empezamos con una frase en la cual, ya con lo que nos acaban de contar, la guerra va cambiando; o sea ya la guerra no va a ser ganada solamente por quien posea un arsenal militar crítico, sino Cibernético. Se podrá ganar una guerra sin disparar una sola bala en el futuro. Esto que suene bonito porque realmente puede destruir y dejar países sin energía, dejar países sin transporte, y causar una crisis nacional. Y ¿por qué el problema? ¿Lo voy hablaré de modo más sencillo. En el mundo tenemos 7.2 mil millones de personas, actualmente a junio de 2015. Esto lo tomo de una página donde cada 3 meses están actualizando la información y más de 3 mil millones de personas están en Internet. O sea, el 42% de las personas se encuentran en este medio. Allí tenemos nosotros los índices a nivel mundial y obviamente hay otros índices de penetración de cuántos teléfonos móviles existen. Hay más de 3.6 mil millones de telefonía móvil. Como decía el Doctor Kevin, países como Estados Unidos tienen el 80% de penetración, así como otros países de Europa y aunque sea una buena cifra, entre más colectividad exista, vamos a ver que hay más vulnerabilidad. En consecuencia, estos países son los más atacados por los cibernautas. ¿Y qué pasa? Que la población al año va creciendo en un1.6% anual, pero las conexiones a Internet están creciendo en un 21% anual. O sea que dentro de poco vamos a tener más conexiones que personas. Por eso se dice que es una ola que va creciendo día a día y que ha surgido con el problema. Si hablamos del Ciberespacio estamos hablando de conexiones, de computadores, de errores, de todos estos sistemas de información que no solamente maneja el Estado, sino que maneja en su mayoría el sector privado y personas comunes.

Tal como lo dijo el Capitán de Navío Cubeiro los dominios de la guerra han venido cambiando y evolucionando. Tenemos unos puntos que vamos a ver rápidamente, pero realmente, la guerra como decía Chomsky es el motor de la transformación de los Estados. La guerra nos ha llevado a conectarnos con la tecnología y la tecnología nos ha llevado a ver a como cambia la forma de la guerra. Pues esto es un ciclo que cada vez vamos viendo crecer y nos ha demostrado que seguirán apareciendo dominios como hemos visto anteriormente. ¿Qué va a pasar en el futuro? La primera Batalla Naval documentada donde el Imperio Hitita combate contra una Flota Naval de Chipre. Asimismo, con la llegada de los navieros y toda esta tecnología, llega la Guerra Naval. Después, la guerra aérea donde ya los primeros dirigibles y aeroplanos tuvieron lugar en la guerra de Libia. Además, vemos cómo Italia bombardea diferentes posiciones turcas con el componente aéreo. En este tema, se desarrolló como ustedes saben, toda la potencia aérea para la II Guerra Mundial. Después llegamos a la II Guerra Mundial y vemos cómo la necesidad de descifrar esos mensajes en Alemania con su máquina enigma hace que los británicos y los americanos empiecen a desarrollar sistemas o tecnologías inicialmente electromecánicas, para poder descifrar esos códigos. Lo que para una persona normal le podía tomar cientos de años, una máquina lo podía hacer en cuestión de horas. Cuando viene la máquina de Turing y empieza a mejorar la comunicación. Comienzan a salir los ordenadores. Empieza a mejorar el procesamiento y luego, viene la carrera espacial. Pues sin la velocidad de procesamiento no hubiese sido posible llegar al espacio. Es conocida, la Guerra

Fría entre Rusia y Estados Unidos por desarrollar equipos espaciales y comienzan a desarrollar sus computadoras. Con esta era espacial fue más desarrollada la informática y las telecomunicaciones. Estados unidos y Alemania empiezan a desarrollar sus computadores y en 1941 Alemania es pionera en elaborar una computadora, luego en 1944, Estados Unidos saca su primera computadora. Como lo decíamos eran muy grandes y esto nos lleva a que el sector Defensa empezara a querer comunicarse con esas máquinas de forma segura y empieza el proyecto DARPA, de allí es donde sale Internet y es donde se va complicando más la historia de la tecnología. Surge la primera Guerra Cibernética durante la Guerra Fría, que sucedió durante el tiempo de convivencia pacífica que tuvieron Estados Unidos y la

URSS. Comparten tecnología y con el tema de espionaje y contraespionaje, Estados Unidos permite que la URSS le robe unos programas que contenían virus, y estamos 1982. La URSS hace explotar un gaseoducto muy grande que atraviesa toda la Siberia y otra vez EEUU se deja robar un software con un virus que hizo que se active y estalle el gaseoducto en 1982. O sea que eso, como si estallarán tres kilotones de TNT. Los daños realmente fueron económicos y el impacto fue internacional.

En consecuencia, empieza el tema de la Guerra Cibernética. Una Guerra Cibernética sucede cuando un país quiere atacar a otro país. Estamos hablando de hackers tratando de robarnos datos. Un país que recibiría duras críticas de otro país. Existen muchos casos, aparte del caso de Rusia. Como consecuencia empiezan todos los ataques cibernéticos de país a país. En el caso de las Fuerzas Armadas, tenemos que protegerlas.
Un caso de un país cibernético fue el de Estonia en 2007. Por ser un país altamente tecnificado fue el primer país que pudo invertir en una votación electrónica. Contaban con una cédula digital donde todo el mundo tenía un código. Era el país y el paraíso de la tecnología, pero obviamente con tanta tecnología, si los dejaban sin Internet significaba dejarlos sin bancos, sin luz, sin transporte, sin comunicaciones. Por tanto, fue el colapso de Estonia durante una semana con amenazas persistentes; en consecuencia bloquearon el país. No está documentado, ya que no se sabe si Rusia lo hizo. Quizás surge a raíz del problema geopolítico que tiene Rusia con sus vecinos Estonia y Georgia, los cuales son países atacados permanentemente por Rusia.

Asimismo, más ataques han surgido. Actualmente se vive el problema con el caso de Rusia y Ucrania que la Península de Crimea. Rusia baja a los DRONES por medio de una Guerra Cibernética. Para esto se necesita saber cómo han hecho los DRONES, pues ahí se está robando propiedad intelectual. De ahí que se empiezan a desarrollar armas cibernéticas. Y ¿qué es un arma cibernética? Es un desarrollo de software, pues se filtra en unas redes y que puede causar severos daños.

Por tanto, después de tener una estrategia de Seguridad Nacional, debemos tener una estrategia de Seguridad y Defensa Cibernética y empezar a hacer planes de protección de infraestructura pública. En el caso de Colombia, existe una política de Defensa y Seguridad Cibernética que tenemos desde el 2011. Creamos unas infraestructuras en la Policía, en el Ejército en el ministerio de Defensa, del Comando General. Existen Comandos Cibernéticos Operativos que están dedicados, ya desde hace unos años, a a implementar toda esta capacidad. De pronto, ustedes saben que violaron el correo del presidente Santos, este es un blanco como digamos apetitoso por los hackers. Cuyo objetivo era hackear la presidencia o los correos o el teléfono del presidente quien, a su vez, manifestó que estábamos en pañales. Y empezamos a implementar y a pensar cuáles son nuestras capacidades del futuro de nuestras fuerzas públicas. Y analizamos cuáles eran nuestras capacidades para el futuro; para la transformación era necesario adquirir una política de Seguridad y Ciberdefensa. En nuestro último Plan de Desarrollo planteamos el Ciberespacio como el quinto dominio de la guerra, y esto como aprecian en el título es de interés nacional. O sea, no solo las Fuerzas militares pero lo vamos a hacer. Hay que formar programas de capacitación y concientización formalmente para que la gente vaya retomando el tema, teniendo en cuenta la importancia que esos escenarios de interacción son propicios para todos, así nuestros países y las personas que interactúan en el tema. Y obviamente la debilidad jurídica que tenemos todos los países. No hay un país que pueda regir o que proteja las Operaciones Cibernéticas. Las Fuerzas militares siempre vamos a estar en una línea de no saber, si vamos a tener una protección cuando queremos interceptar los datos a terroristas o enemigos de la Nación. Todavía no hay un escenario en que podamos actuar libremente. Yo termino con una frase de Maquiavelo: no hay nada más difícil de emprender, ni más peligroso de llevar a cabo y más incierto que la tomar la iniciativa de un nuevo orden de cosas. Los invito a que pensemos en este tema nuevamente aquí en Perú y que en unión con todos los países, logremos también una estrategia internacional.

Calm. (r) Óscar Anderson

Buenas tardes damas y caballeros, me toca tratar el escenario del Ciberespacio, Ciberseguridad y Ciberguerra. Mis antecesores me han dejado un escenario bastante complicado. Ya lo más fino lo han expuesto ustedes, sin embargo voy a tratar de complementar la información expuesta con algunas ideas. Voy a sintetizar un poco lo expuesto y a aportar sobre lo que está ocurriendo en nuestro entorno. La información es la primera línea de defensa de cualquier Estado, palabras de Gordon Thomas, autor del libro "Mossad: La Historia Secreta".

Si no disponemos de suficiente información no se puede conducir una guerra, un negocio o por lo menos no se puede pretender ganarla, o tener éxito en una empresa salvo que uno tenga mucha suerte. ¿Qué buscan los principales ciberactores? Obviamente obtener y robar información, tenemos los ejemplos de Snowden, Asshange. Todos sustraen información, todos han sustraído información y obviamente desde el interior de las principales dependencias en las cuales se encontraban laborando. La principal amenaza no está afuera, está dentro de las empresas, el 70% o 75% de la sustracción de información viene de dentro de las propias empresas o dentro de las propias dependencias. Pensar en acciones como la de James Bond quedó en el pasado. Obviamente, se requieren agentes encubiertos.

Se van a seguir empleando, pero es mucho más fácil meterse en la red y sustraer toda una librería, toda una biblioteca con información que estar fotografiando página por página y pensar en sustraerla con seguridad. ¿Qué debemos hacer' Proteger esta información evitando que información de importancia sea sustraída. ¿Qué buscan algunos protagonistas internacionales' Obviamente resaltar en la opinión pública, llevar a cabo acciones que burlen la autoridad, por ejemplo es solamente un caso utópico, ¿por qué no pensar que el avión de Malasia Airlines fue capturado en el aire y llevado por algunos ciberpiratas a un punto desconocido y se perdió? Hoy en día se puede pensar en estas acciones. La semana pasada en El Comercio se publicó que los ciberpiratas estaban pensando secuestrar aeronaves, infiltrándose en los sistemas para llegar a los ordenadores de abordo. Todo es posible, los blancos son el Gobierno, el sector privado y los ciudadanos.

¿Por qué proliferan los ataques? Los cibercrímenes son de bajo costo, fácil encubrimiento y ejecución; efectivo y de alto impacto, bajo riesgo para el atacante. Vamos a ver algunos ejemplos de los intereses que existen para obtener información. Tienen ustedes en pantalla la base de la Real Fuerza Aérea de Menwith Hill allí se encuentra materializada ECRAS una organización de escucha de análisis y procesamiento electrónica creada posterior a la Segunda Guerra Mundial a inicios de la década del 60. Inicialmente integrado por Estados Unidos y Gran Bretaña, a los que se incorporaron posteriormente en el año de 1981: Canadá, Australia y Nueva Zelanda contando en la actualidad con más de 120 estaciones de escucha e interceptación en tierra y en el espacio. ¿Qué analizan? Señales de radio, satélites, teléfonos, faxes y correos electrónicos, a razón de tres mil millones por día; más o menos equivalente al 90% de las comunicaciones diarias. La planta de personal es de quinientos mil empleados aproximadamente de los cuales 120,000 están en Estados Unidos y el resto repartido en los países integrantes.

Otro esfuerzo PROVIS. Es otro centro moderno para la información. Desde 1967 el experto William Hamilton retornó a Estados Unidos de Vietnam donde había desarrollado una red de puntos de escucha electrónica con lo que monitoreaba a los VietCom. Entró a trabajar en la Agencia Nacional de Seguridad en la universidad, con sus siglas en inglés y dado que era la época del desarrollo de los ordenadores, desarrolló el FACE (Free Air Concentration Enrichment) igualmente por sus siglas en inglés que equivale a sistemas de análisis facial por comparación y eliminación. Esto revolucionó el proceso de identificación de personas. Este programa podía analizar 15 millones de rostros por segundo. Ha-

milton vio el potencial de su programa y decidió desarrollar un programa que se relacione con la base de datos de los bancos, logrando interconectarse así con otros sistemas; sin que estos se percataran de ello. En 1981 bautizó el programa como PROMISE.

Algunas agencias de inteligencia tomaron conocimiento de este programa y lo obtuvieron, logrando con la ayuda de este, ubicar y neutralizar a líderes enemigos terroristas, sin hacer uso de inteligencia humana sino de la electrónica. El programa fue mejorado logrando insertar puertas falsas en los programas, a fin de permitir el acceso a la información de las computadoras.

Hoy en día podemos plantearnos la pregunta ¿Quién no navega por internet? Desde la casa lo hacemos todos, en la oficina o en tránsito hacia algún lugar. Sin embargo, acaso somos conscientes de los riesgos que corremos al hacerlo aparte de tener un accidente automovilístico por marcar un número o estar leyendo un mensaje recibido. Habremos tomado las precauciones para que la información en nuestro equipo esté seguro contra los intrusos e infiltraciones no deseadas que además pueden modificar o sustraernos la información, sin que seamos conscientes de esto.

Necesitamos seguridad, todos estamos expuestos a los ataques cibernéticos y dependiendo de la información que se afecte, esto podrá generar daños personales a la empresa y a la Nación. Es de vital importancia hacer uso de las tecnologías de las comunicaciones, las mismas que han evolucionado y continúan haciéndolo en forma vertiginosa para fomentar el cambio en la sociedad. Internet ha maquillado los procesos sociales de cambio y ha logrado quebrar dos dimensiones, estas son el espacio y el tiempo. Ha generado un fenómeno social que requiere que las estructuras jurídicas, políticas, educativas y comerciales de protección y seguridad se actualicen de forma dinámica, conforme se desarrolla el Internet, a fin de evitar que las ciberamenazas o la ciberdelincuencia nos ganen la partida en la conciencia de la ciberseguridad. La conciencia en la protección debe abarcar todos los aspectos de los sistemas informáticos y de comunicaciones y principalmente, sobre todo, el ser humano. Toda vez que este es el eslabón más débil de la cadena de seguridad, del que pueden aprovecharse tres características inherentes: el miedo, la confianza y la inconciencia.

¿Qué se requiere para crear una conciencia nacional de ciberseguridad? Hay tres vías: La educación, la enseñanza y la concientización. ¿Qué requerimos para alcanzar un ciberespacio seguro? Capacidad de colaboración y coordinación entre los distintos organismos del Estado con las instituciones privadas y actores internacionales y sobre todo, desarrollo de nuevas tecnologías que permitan prevenir y reaccionar ante las amenazas.

Tenemos en pantalla los primeros transistores en la parte superior, los que fueron desarrollados en los laboratorios Bell el año 1945 y en la parte inferior un chip, un circuito integrado más o menos moderno. ¿Por qué los presento? Podemos considerar que en la década de los 70 más o menos habían 2,300 transistores en cada chip y de acuerdo a la ley de Moore cada dos años debía duplicarse este número de integrados. Sin embargo, Moore se equivocó, cada 18 meses se duplican el número de transistores en los integrados. A la fecha debemos tener más o menos unos 5,000 millones de transistores en cada chip de media pulgada cuadrada. ¿Por qué traigo a colación esta información? Por la miniaturización, la alta densidad en los circuitos integrados, la volatilidad tecnológica que se hizo mención. Permiten a los países generadores y exportadores de tecnología en equipamiento militar, científico y administrativo poder incorporar circuitos en los equipos exportados que permitan saber dónde están ubicados estos equipos y adicionalmente desactivarlos, a voluntad; a interés o que actúen como bomba lógica, destruyendo el equipo. ¿Qué pueden planear estos ciberataques?

Como ya se ha mencionado anteriormente, colapso del sistema bancario, interrupción del suministro eléctrico, inoperatividad de los sistemas de Defensa, corte de los suministros de combustible, colapso de los sistemas de transporte y muchos otros. Todo esto sin conocer la identidad y la ubicación del atacante. El centro cooperativo por excelencia de ciberdefensa, en Tallin, Estonia, ha publicado la relación de países con políticas de ciberseguridad al 18 de marzo del presente año. 59 países de los 194 que hay en el mundo, o sea casi el 30% tienen políticas de ciberseguridad. Ya es hora de que los países empiecen a hablar del control de las armas cibernéticas. A lo largo de la historia las nuevas tecnologías han revolucionado las guerras, algunas veces en forma abrupta, otras solo gradualmente. Los ordenadores y el Internet han transformado las economías y le han dado grandes ventajas a los efectos occidentales, tales como poder enviar aviones no tripulados a diferentes puntos del globo para obtener información o atacar objetivos, pero la difusión de la tecnología digital tiene su costo, expone a los ejércitos y a la sociedad a los ataques digitales.

¿Cómo estamos en el Perú? Puede haber habido más eventos pero voy a nombrar, voy a citar los dos más resaltantes. Ha habido dos actividades en la empresa ISSA (Information System Security Association) en abril del 2012, un conversatorio, un evento sobre Ciberseguridad. Presentaron al final de este las propuestas políticas y estrategias nacionales de Ciberseguridad para el Perú. Durante el presente año, entre el 20 y 22 de enero se llevó a cabo la reunión de especialistas de Ciberseguridad de especialistas de las Fuerzas Armadas entre el Perú y Estados Unidos y se plantearon los retos de crear una doctrina para estandarizar estrategias y metodologías de Ciberdefensa y Ciberseguridad; implementar un comando operacional de Ciberespacio e implementar un centro de respuesta ante incidentes informáticos. Un aporte podría ser el presente organigrama, donde la cabeza del sistema de Ciberseguridad está presidida por el presidente de la República e inmediatamente después, estaría el presidente del Consejo de Ministros, quien tendría a su cargo el COSENA El Consejo de Seguridad Electrónica Nacional.

A cargo del COSENA estaría un director del sistema y a orden de este tendríamos dos pilares: uno el ministerio de Defensa, que tendría a su cargo el dominio (.mil) y el ministerio del Interior, que tendría a su cargo el dominio (.gob). El resto de instituciones, tanto el ministerio Público, como la banca, como los representantes de la industria, y la Cancillería, tendrían que estar obviamente considerados para poder articular los sistemas de Defensa. ¿Qué actividades deben desarrollar para una estrategia de Ciberseguridad? Establecer los principios rectores, los objetivos y las líneas de acciones y lo más importante el Estado, las instituciones y el sector empresarial deben invertir tiempo y dinero en forma coordinada.