Ciberseguridad: Un reto para la Defensa Nacional en entornos intangibles

CYBERSECURITY: A CHALLENGE FOR NATIONAL DEFENSE AT INTANGIBLE ENVIRONMENTS

Recibido: 20/09/2017 ***Aprobado: 17/11/2017***

Coronel
Nelton Baralt Blanco,
Ejército República
Dominicana

El autor es Coronel del Ejército República Dominicana y tiene una Maestría en Defensa y Seguridad Nacional de la Universidad Nacional para la Defensa (UNADE), Escuela de Altos Estudios, un Máster Internacional en Gestión Universitaria de la Universidad de Alcalá de Henares, España, Especialidad en Comando y Estado Mayor del Instituto Militar de Estudios Superiores, Licenciado en Administración de Empresas, UTESA, Oficial de Infantería (Cadete) en la Academia Aérea "Gral. de Brigada Piloto Frank Feliz Miranda, FARD", Curso Superior de DDHH y DIH, Instituto Militar de DDHH y DIH, Curso de Altos Estudios Estratégicos para oficiales Iberoamericanos, España; entre otros. Actualmente es el Vicerrector Académico del INSUDE. Escritor de la unidad I: La Inteligencia Militar. (Libro "Inteligencia Aplicada a la Seguridad del SIGLO XXI" julio 2016) con la Universidad Nebrija/INSUDE. nelton.baralt@gmail.com

RESUMEN

La participación de las fuerzas militares encargados de la Defensa Nacional en un nuevo espacio de batalla, emplea la ciberdefensa pone todos los recursos disponibles y unidades especializadas de las Fuerzas Armadas de la nación, para enfrentar las actividades delictivas en los ambientes cibernéticos que puedan afectar la infraestructura critica, las instituciones públicas, los servicios de salud y la banca privada, tomando acciones preventivas, al tiempo que realizan actividades que permiten restaurar los servicios que fueren afectados en el menor tiempo posible.

Palabras clave:

Amenaza, ciberseguridad, ciberdefensa, cloud computer. malware, ingeniería social y riesgo, vulnerabilidad.

ABSTRACT

The use of the military forces in charge of National Defense in a new battle space, using cyber defense, puts all available resources and specialized units of the Armed Forces of the nation, to face the criminal activities in cyber environments that may affect the critical infrastructure, public institutions, health services and private banking, taking preventive action while performing activities that restore the services that become affected in the shortest possible time.

Keywords:

Threat, cybersecurity, cyber-defense, cloud computer, malware, social engineering and risk, vulnerability.

Introducción

La Seguridad está definida como la necesidad que tienen los seres humanos de sentirse sin riesgo o en absoluta confianza con su habitat. La tecnología ha ido creciendo hasta tal punto que lo que antes era percibido como parte de una fábula de ciencia ficción, hoy día son una realidad y a todas luces evidencian nuevos paradigmas en cuanto al concepto de seguridad tradicional.

En términos de la Defensa, todos los recursos son debidamente organizados para garantizar los la permanencia o la consecución de los intereses vitales de las Naciones-Estado, especialmente condicionados con la geografía así como la libertad de sus ciudadanos, sin embargo la aparición de ambientes híbridos entre lo virtual y físico, propicio el establecimiento de un nuevo concepto del espacio de batalla para las fuerzas militares, donde priman los ambientes intangibles y el enemigo en la mayoría de los casos prefiere una asimetría en el conflicto aprovechando que no pueda ser fácilmente descubierto, perseguido o legalmente sometido.

La dependencia de la conexión a internet o de servicios "In Cloud" o en la nube, aumenta la probabilidad de riesgos causados por ciberdelincuentes aislados, estatales o empresariales, que utilizan una tecnología de fácil conexión e interacción, con acceso global, bajo costo y especialmente bajos niveles de exposición, frente a grandes beneficios morales o económicos.

Los países deben enfocar los recursos de Defensa a la construcción de infraestructuras y equipos de respuesta ante ataques informáticos, a los fines de retomar el control una vez colapsen los servicios afectados por acciones maliciosas, malware, accidentes o desconocimiento de los operarios de un sistema de infraestructuras críticas que puede ser afectado.

Desarrollo del tema

Desde las historias narradas por Julio Verne en sus impactantes trabajos relacionados con la ciencia ficción, donde gracias a su estilo único, logro imprimir una cierta experiencia visionaria, de temas que en el momento de su redacción presumían de ser algo fantástico que era posible imaginar que alguna vez se tratare de algo real, nos marcó una base inspiradora en nuestras infancias, al tratar de identificar a través de las letras como se realizaban viajes extraordinarios como el realizado hacia el centro de la tierra (1864), a lo más profundo del mar con "20,000 leguas de viaje submarino" (1870) y por qué no, la inimaginable exploración del universo, con su obra "De la tierra a la Luna" (1870).

Pero a pesar de la fascinación evidenciada por estos viajes fantásticos, lo que muchos no se percataron era la existencia y uso de maquinarias de carácter futurista como individuos autómatas (robots), vehículos con cierta autonomía y pilotos automáticos y sobre todo la existencia de algo que solo iba a ser descubierto en el siguiente siglo con la aparición de las computadoras.

Descritas como máquinas electrónicas capaces de recibir y procesar datos, superaron en diversas formas las capacidades matemáticas y de procesamiento que las mentes más brillantes de la humanidad pudieron alcanzar. Visto así las informaciones ingresan a la máquina, que procesa la información y pone a disposición del usuario de un recurso o información que puede ser utilizada por este para los fines que requiera.

Bajo este mismo principio la Inteligencia militar o en cualquiera de sus denominaciones, trato de identificar o descubrir nueva información a partir de esa capacidad única de los seres humanos, para conocer, escudriñar, y razonar cosas para con ello elegir una opción a partir de las ideas que fueron surgiendo, venciendo así en cierta forma cualquier rastro de incertidumbre (Baralt, 2013, pág. 9).

Las Cumbres de Ministros de Defensa celebradas en Bariloche, Chile, en octubre del 1996 y la de Cartagena de Indias, Colombia en noviembre del 1998 habrían definido de común acuerdo la necesidad de los países de cooperar para enfrentar las nuevas dimensiones de la seguridad hemisférica, nuevos roles y perfiles de las fuerzas militares así como la implementación de un Sistema de Seguridad Hemisférica (Bolivia, 2010).

Son estas nuevas amenazas consideradas en su mayoría no tradicionales o asimétricas, elevan la complejidad de llevar a cabo la gestión de la seguridad y la defensa, obligando en cierta forma a transformar todos los modelos doctrinales para las operaciones militares hacia otros un tanto novedosos y sin ningún tipo de norma de aplicación general. Las actividades como la Inteligencia se enfocaban en determinar informaciones para generar conocimiento a partir de enfoques político social y económico o militar,

de países que fueran sus adversarios reales o potenciales (Milano, 2003).

Sin embargo el uso de nuevas tecnologías de naturaleza no militar con propósitos orientados a la producción de terror, sabotajes secuestros, actividades criminales internacionales, hizo posible que estas acciones se enmascararan en un tipo de acciones no tradicionales que han podido causar graves daños a la estabilidad de los países.

No obstante la discusión resulta interesante ya que ahora tenemos que enfrentarnos a algo que parecería formar parte de estas viejas novelas de ciencia ficción, o que estamos viviendo en vida propia un largo metraje, donde se exhibe la astucia de un agente secreto con autoridad para matar en nombre de un servicio de inteligencia de un país como un agente de los denominado 00 o mejor conocido como James Bond, o con la visión futurista sacada de una de las versiones de la "Guerra de las Galaxias" de George Lucas.

En nuestra realidad, las computadoras han escalado niveles de participación en la vida de los seres humanos, donde iniciaron su presencia en las empresas mayoritarias, luego en las medianas empresas para culminar dentro de las casas de las personas, donde somos cada día dependientes y es por esto que definimos que uno de los factores fundamentales de la ciberseguridad implica proteger activos, de las amenazas externas o internas que pueden afectarlo, inutilizarlo o usarlo para otros fines que no fueron concebidos (Beltrán, 2017).

En este contexto hemos pasado de actividades muy centralizadas en instituciones gubernamentales, empresas multinacionales, empresas de capital privado y desarrolladores de softwares, a una actividad donde cada vez estamos más expuestos en nuestra privacidad, y donde ya inclusive programas permiten identificar en función a su experiencia pasada pueden predecir incluso que bienes y servicios puede adquirir o que lugares pudiera visitar en sus próximos viajes.

Sin embargo en el aspecto divertido de la vida, resulta cómico ver cuando el programa hace esto, y si transportamos esta experiencia a la posibilidad de que las máquinas puedan ser controladas o manipuladas desde el exterior, o peor aún que se activen de manera autónoma. Seguro que alguien pudiera manipular a su antojo cómo funcionan instalaciones de infraestructuras críticas, aeronaves y equipo militar, equipos de navegación aérea y marítima o instituciones e información bancaria.

No podemos vivir encerrados en una burbuja, por esto al determinar la seguridad que necesita un país para que todos las fuentes del poder nacional (Recursos con los que cuenta) y los Instrumentos del poder nacional (Elementos de que dispone para preservar o conseguir alcanzar sus intereses nacionales) (Ministerio de Defensa, 2007).

Los principios que rigen la ciberseguridad en actuales momentos, establecen que la "***Seguridad completa no existe***", no podemos seguir con el concepto de poner dentro de una muralla todas nuestras instalaciones y recursos, mien-

tras tenemos que mantener la flexibilidad y la capacidad de interconexión hacia el mundo exterior.

Tanto la Política de Defensa Nacional como en las misiones y funciones de las FFAA, ha sido concebido un especial interés para dotar al país de todos los recursos necesarios para asumir los riesgos y enfrentar las amenazas (Ministerio de Defensa, 2007).

Asimismo fue evidenciado en el Anteproyecto para la Ley de Seguridad y Defensa (2017) que se encuentra en proceso de revisión de la Comisión de Seguridad y Defensa del Congreso Nacional de la República Dominicana, donde se define el riesgo: acción de exponerse a la contingencia de recibir un cierto daño en algún área o aspecto de interés, que se transforma en amenaza cuando existe baja o ninguna capacidad de reacción y a la vez un adversario real o potencial tiene capacidad de explotar la situación en su provecho (Congreso Nacional, 2017).

En este sentido este mismo documento establece que la ciberseguridad es el conjunto de políticas, estrategias, métodos de gestión de riesgos, acciones preventivas y seguros tecnológicos que sirven para proteger el ciberespacio de una nación, su patrimonio y los usuarios del ciberentorno, enfocados en la protección de la información digital en los sistemas interconectados.

Pero entonces como definimos la ciberseguridad y la ciberdefensa, y como afectan a los ciudadanos de un país y a las capacidades de respuesta en cada nivel, y para los componentes de las fuerzas militares de una nación. De allí que al revisar las documentaciones redactadas a través de la Agencia Europea de Seguridad de las redes y de la información (ENISA) creada en el 2004 para luchar contra las violaciones de la seguridad de las redes y los sistemas de información, para la cual constituye su principal objetivo es mejorar las capacidades de prevención y reacción ante cualquier evento real o sospechoso.

En la estrategia desarrollada (ENISA, 2017) se destaca que dado el impulso que han evidenciado las Tecnologías de la Información y las Comunicaciones (TIC), logrando reducir al mínimo las distancias, usos de recurso y tiempo para las operaciones, y el riesgo a que se exponen los operarios, se entiende que proporcionan un entorno dinámico que permite manejar diferentes infraestructura o llevar a cabo operaciones a distancia.

Esto hace posible que el esfuerzo mayor que debemos observar estará en conocer cuáles son las principales amenazas y riesgos a la seguridad de la información y la creación de diferentes instrumentos para la detección, defensa, investigación, recuperación de los sistemas y respuesta a los ataques de personas mal intencionadas, actos terrorista o acciones de países o competidores comerciales.

De esto surge una gran interrogante ¿cómo podemos hacer frente a estas amenazas, y estar preparados para estas contingencias, si desconocemos desde donde provendría el ataque? La respuesta obligatoria debe estar relacionada con la Inteligencia en una primera etapa, y pudiéramos estar generando algún tipo de nuevo concepto como la Inteligencia cibernética o la ciberinteligencia, pero en

cualquiera de los escenarios debemos estar listos para enfrentarlos de algún modo. Así vemos cómo afecta significativamente este concepto a partir de estos elementos:

RIESGO	AMENAZA	VULNERABILIDAD	IMPACTO EN ORGANIZACION

Participación de los Cuerpos de Defensa en la prevención del crimen y el delito

Una de las implicaciones que para los Cuerpos de Defensa, tienen como sus nuevos roles constituye el apoyo a los Cuerpos de Seguridad y servicios policiales. En este sentido cada país y especialmente los de Hispanoamérica, ha experimentado cada vez más, el empleo de sus Fuerzas Armadas en actividades de naturaleza de seguridad o en el despliegue de sus efectivos y equipos en otras operaciones no militares.

La prevención del crimen y el delito ha pasado a formar parte de las agendas de todos los países en cuanto a actividades que van desde la persecución de la criminalidad común, el uso y abuso de drogas, el tráfico internacional de drogas y armas, así como el terrorismo. Sin embargo esto ha ido aumentando en una compleja relación de los actores involucrados. El efecto de la globalización no solo ha impactado en el crecimiento y proliferación de estas actividades sino que también genera nuevas formas de actividad criminal.

Durante la celebración del 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, llevado a cabo en Doha (ONU, 2015), se estableció un enfoque amplio para prevenir y afrontar nuevas formas emergentes de delincuencia transnacional.

En esto se estableció que las actividades criminales y delictivas tenían motivaciones aun fueran diferentes, tenían modos de operación comunes, además de que se veían influenciadas por la globalización, la pobreza extrema, los conflictos y fragilidad de las estructuras del estado, así como el surgimiento de nuevas tecnologías, y como la corrupción ayudaba al crecimiento de los grupos.

A estas actividades sumaron unos nuevos delitos como la piratería marítima y la falsificación, el abuso y explotación de niños, trata y tráfico de personas, y la ciberdelincuencia, donde estos fueron definidos como no tan nuevos sino que habían experimentado una evolución a nuevas formas y medios para la comisión de delitos ya tipificados.

Al definir el problema de la ciberdelincuencia en el documento de las Naciones Unidas, titulado "Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos", Revista Internacional de Política Criminal, donde se estableció que el potencial de la proliferación de la delincuencia informática era tan amplio como el propio desarrollo de las comunicaciones. De esta visión se hace evidente que la capacidad de que estos actos tengan un carácter transnacional es ilimitada.

Estas acciones son complejizadas al momento de que ya no se trata de las acciones que se llevan a cabo con fines económicos como el robo de información bancaria o la falsificación de credenciales para acceder a determinados lugares o claves para instalación de software, con la intención de dañar o estafar a otras personas. Lo peor es que los países enfrentan a organizaciones, personas externas que no tienen la más mínima idea de donde se encuentran o que fines persiguen, o con los propios empleados que pueden hacer o no sus labores correctamente o pueden ser víctimas de actos provocados por la propia naturaleza.

Otro caso resulta de las acciones judiciales, de cómo identificar un sospechoso que está a miles de kilómetros, que no tiene un móvil o motivación, más que el simple hecho de que ha logrado intervenir en una instalación protegida o que solo persigue las claves de un software original en su PC, o que pretende fisgonear dentro de los correos electrónicos de alguien, pretendiendo enterarse al menos de lo que realiza en su ámbito privado o personal. Un nuevo peligro surge al momento de que este Intruso logra bajo una técnica denominada "Man in the Midle" conectarse en medio de dos ordenadores mientras realizan una comunicación que para ellos es segura. Es en este punto que todo el mundo se plantea que el problema viene desde fuera, sin embargo en la mayoría de los casos la brecha en la seguridad proviene desde dentro.

De acuerdo a la organización Open Information Security Foundation (OISF) una organización formada por entusiastas de la seguridad de la información, estableció que la mayoría de los eventos eran producto de un descuido o causa de seres humanos (Foundation, 2017). Los humanos dirigen el Sistema de seguridad pero no son máquinas, y tienen sentimientos, pasiones o afinidades con amigos o compañeros de trabajo (Beltrán, 2017).

Se entiende que este proceso de captar información de las personas es lo que se conoce como ingeniería social, permitiendo con esto sacar datos de las personas, y estas no se dan cuenta ni siquiera de que fue el mismo quien proporcionó toda la información necesaria para ser víctima de un ataque informático. El que se dedica a la ingeniería social entiende que en la cadena de seguridad el ser humano es el eslabón más débil.

Kevin Mitnick reconocido como un famoso Hacker de Ingeniería social, solía expresar, que no importaba cuantos equipos de seguridad, sistemas, tecnologías, dispositivos biométricos, si podía hacer una llamada a un empleado desprevenido que le proporcionara información valiosa y le diera acceso al sistema.

Así se entiende que es tanta la información que proporcionamos que desconocemos que puede hacer quien busca conocer de nosotros, como puede ser evidenciado en algunos ejemplos:

- Los datos proporcionados en un diskete llevaron a la detención del asesino en serie de Wichita en EUA, en el 2005, ya que el documento en Word tenía información valiosa de los lugares que había frecuentado

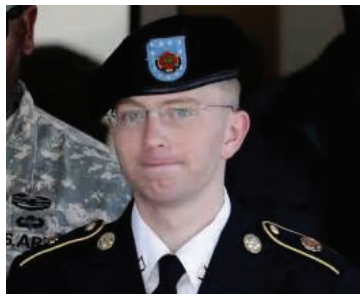
y donde había redactado el texto. Fue acusado de la muerte de 10 personas entre 1974 y 1991.

- En el 2015 las Fuerzas Militares de EUA bombardearon un cuartel del Estado Islámico (EI) en vista de la información que proporcionó una SELFIE que publicara uno de los miembros de esa organización.

Es por esto que las Fuerzas de Defensa cada vez más son un tanto rígidos en su protocolos de seguridad, ya que cualquier información que proporcione un soldado o uno de los comandantes, pudiera comprometer las misiones, o poner en riesgo la infraestructura del sistema de Defensa o los equipos de alta tecnología, como drones, radares, cohetes de largo alcance o satélites.

El Sistema de Ciberdefensa y de Ciberseguridad proporciona medidas para protegerse de ataques externos como estos, sin embargo la mayor amenaza que los cuerpos de Defensa enfrentan está en los **Malicious Insider** los cuales funcionan como un Enemigo dentro de la casa, donde no solo por descuidos a causa de ingeniería social o ganas de ser buen amigo de sus compañeros de trabajo, dado sus niveles de inconformidad por el puesto, la insensibilidad por su trabajo o bien porque su ambición le permite corromperse ante el pago recibido por alguna fuerza externa.

Casos como el de **Edward Snowden**, que siendo Consultor y empleado de la CIA y la Agencia Nacional de Seguridad filtró algunos documentos de estas agencias incluyendo los programas de vigilancia masiva PRISM y XKeyscore, o el de **Bradley Manning**, que siendo soldado y analista de inteligencia del ejército de Estados Unidos que en 2010 filtró a Wikileaks miles de documentos clasificados de las guerras de Afganistán e Irak, incluyendo cables diplomáticos de varias embajadas estadounidenses, pone un nuevo elemento en las agendas de seguridad y los servicios de cada agencia de Inteligencia y las Fuerzas Armadas de cada país.



INTERNET: Conexión global o acceso a la vulnerabilidad

Se ha hablado mucho de las ventajas que ofrecen el internet y la conexión masiva de los equipos a una conexión global, bajo la premisa de mantenerse siempre conectado y con soporte para las mejoras o actualizaciones de software. Este crecimiento también ha traído consigo nuevos entornos vulnerables gracias a esta conectividad.

En principio Internet de las máquinas protegíamos dentro de una muralla.

Luego vino el Internet de las personas donde son mejores que en la Compañía.

Por último el Internet de las cosas (IOT) Conexión de Internet con más cosas u objetos.

De acuerdo al Informe de las Naciones Unidas el acceso al internet en la actualidad ronda el 40% de la población mundial, pero se estima que para el 2018 el número de dispositivos conectados a internet alcanzará al menos el doble de la población mundial (ONU, 2015).

La dependencia por lo digital y la conexión a internet está creciendo pero las medidas para garantizar la seguridad no, lo que aumenta además el crecimiento de la capacidad delictiva. Softwares maliciosos pueden infectar todos nuestros sistemas y permanecer allí latentes hasta tanto sea dado la orden de activación y toda la actividad de Defensa, Seguridad, transporte, salud, bolsas de valores y bancos entre otros pueden colapsar en solo unos segundos en todo el mundo.

La tecnología de la información ha pasado del internet de las máquinas, a las personas y ahora el mundo se encuentra frente al internet de las cosas, haciendo posible que todos los equipos se conecten por si solos a la red y proporcionen infinidad de informaciones referentes a los individuos, sin que estos lo sepan, donde están, que les gusta, que compran, lugares que visitan y frecuencia incluso los viajes en avión, tren o barcos, ya resulta casi imposible que un ser humano pueda hacer nada sin que lo sepan los sistemas computarizados.

Sin embargo no están fácil descubrir en realidad lo que los usuarios pueden realizar, ya que alguien estando en el mismo país puede simular una conexión por internet que va pasando de un servidor a otro y aparentar realiza un ataque informático desde cualquier país en otro continente, borrando los rastros originales de la conexión, o suplantando identidades, o haciendo posible que una PC en cualquier lugar del mundo ejecute un comando o acción a distancia y será difícil descubrir el caso antes de que provoque el daño, que puede tener implicaciones financieras, de robo de tecnología o incluso acciones tipificadas como terroristas.

Estos eventos establecen el marco referencial para un nuevo campo de batalla, donde al salir del convencionalismo de la guerra en cualquiera de sus acepciones, plantea una CIBERGUERRA que involucra no solo a los cuerpos de Seguridad, los Cuerpos de Defensa, a las instituciones de cada país, sino que involucra a todas las naciones.

En este contexto la Organización del Tratado del Atlántico Norte, mejor conocida por sus siglas como OTAN realizó una cumbre de Ministros de Defensa de los miembros de su organización para conocer las implicaciones de los ataques cibernéticos a las infraestructuras de los países, donde aprobaron (marzo del 2011), el Nuevo Concepto de Ciberdefensa de la Alianza, el cual define la protección de las redes de la OTAN como una responsabilidad fundamental de los aliados además de sentar las bases para una política de ciberdefensa (IEEE, 2011).

La OTAN propuso utilizar los procesos del Planeamiento de Defensa para ayudar en el desarrollo de las capacidades de los aliados y aquellas naciones que lo solicitaran, trabajando de la mano con la Organización de las Naciones Unidas (ONU) y la Unión Europea (EU). Las actividades llevadas a cabo incluyen: coordinación y asesoramiento en

ciberdefensa; asistencia a las naciones; investigación y formación; y cooperación con los socios.

En la Coordinación la OTAN consideró la creación de dos estructuras: La Autoridad para la Gestión de la Ciberdefensa-CDMA (NATO Cyberdefence Management Authority-CDMA) que se encarga de la gestión del riesgo de seguridad; la valoración de las vulnerabilidades, y la operatividad de los sistemas de información y comunicaciones críticos para el funcionamiento de la alianza y del Consejo de Gestión de Ciberdefensa-CDMB (NATO CyberDefence Management Board-CDMB) que está integrada por los comités político, militar, operacional y técnico de la OTAN con responsabilidades en ciberdefensa. En ambas instancias se asegura de evaluar las capacidades y revisar la capacidad de respuesta ante un evento.

En cuanto a asistencia en temas de ciberseguridad, aunque cada país debe proporcionarse sus propias capacidades de protección, dispone de equipos multidisciplinados de respuesta rápida, para atender países afectados. Las capacidades de entrenamiento e investigación se llevan a cabo a través del Centro de Excelencia OTAN de Ciberdefensa Cooperativa (Cooperative CyberDefence Centre of Excellence -CCDCOE) en Tallinn, Estonia fue acreditado en 2008 y se encarga de la formación en ciberguerra con personal experto de los diez países que lo patrocinan (Estonia como país anfitrión, Alemania, Eslovaquia, España, EEUU, Hungría, Italia, Letonia, Lituania y Turquía). Persiguen mejorar las capacidades en Ciberdefensa a través de programas y proyectos que involucran la investigación, el desarrollo y la inteligencia.

Esta configuración de la OTAN de acuerdo a María José Caro Bejarano, analista principal del Instituto Español de Estudios Estratégicos (IEEE) hace importantes aportes en cuanto a una necesidad emergente de los países frente a la ciberdefensa, al reconocer las implicaciones de la amenaza, generar un nuevo concepto, el abordaje común entre los organismos de carácter regional o mundial, y el desarrollo de políticas conjuntas para enfrentarlos (IEEE, 2011, pág. 5).

Nuevos riesgos y amenazas cibernéticas a la Seguridad y la Defensa

El avance de las tecnologías de información y comunicaciones, su fácil acceso, bajo costo y alcance a todos los estratos sociales, han proporcionado grandes beneficios para el desarrollo político, social, económico, con un denominador común: El hombre, que conecta todas las estructuras desde los gobiernos, las empresas e industria, la educación, transporte, comunicaciones, poblaciones y familias, a través del internet, sus redes sociales y el propio internet de las cosas que le permiten estar

interconectado y comunicado en todo momento y lugar (Digital, 2015).

Este aumento de actividad de las personas y las cosas en un ambiente ciber aumenta la exposición a los riesgos y amenazas dado que lo mismo que le favorece debe tomarse en cuenta para la prevención. Estos riesgos en ciberseguridad pueden ser advertidos en los siguientes puntos:

- **Tienen acceso global**. El ataque puede ir o venir desde y hacia cualquier persona, institución u organización conectada a las redes.
- **Generan impacto.** Ya que están conectados a más personas y pueden afectar a infraestructuras críticas, transporte o sistemas de defensa.
- **Son difíciles de predecir**. Ya que la comunicación es tan rápida que resulta imposible detectar con efectividad los ataques.
- **Evolucionan muy rápido.** Es previsible que muchos virus informáticos y troyanos tienen capacidad de mutar en sí mismos como vida inteligente o con vida propia.
- **Usan tecnología barata.** Se destaca que la mayoría de estos ataques provienen de equipos de moderado costo y en algún caso de los denominados CLOUD COMPUTING que se basa en que todos los recursos están en la red y el usuario solo necesita acceder a internet por cualquier vía con un teclado.

Es quizás el último de estos aspectos que ha motivado a que cada día más personas se sumen a la participación en los delitos en contra de la ciberseguridad y la ciberdefensa, ya que pueden cometer acciones con un bajo nivel de inversión o costo, con un relativo anonimato y beneficios económicos grandes, los hackers, terroristas, activistas, pero también empresas y gobierno realizan estas acciones denominadas ciberataques que no son más que acciones perpetradas a través de internet para destruir, afectar o comprometer los sistemas informáticos de una entidad, infraestructuras o gobierno, con el acceso masivo ilegal que proporciona interrupciones en el servicio y acceso a datos sensibles o personal es aprovechando el poco conocimiento o el descuido de los usuarios ante una amenaza.

Por esto la ciberseguridad y todas las ramificaciones que se asocien al término constituye una prioridad para los gobiernos, las empresas y por qué no, las personas. Solo basta identificar el colapso de servicios como Facebook, whatsapp, twitter entre otros, como puede afectar la vida de los usuarios, que no pueden siquiera decidir las cosas que deben realizar en su vida diaria, para entender que pasa a nivel gubernamental o de la empresa cuando por denegaciones de servicio los demandantes de un servicio como energía, transporte, comunicaciones o algún bien, pueden generar infinidad de reclamos y paralizaciones en los estados incluso provocar la muerte de muchas vidas o la destrucción de instalaciones denominadas críticas para la existencia misma de los estados.

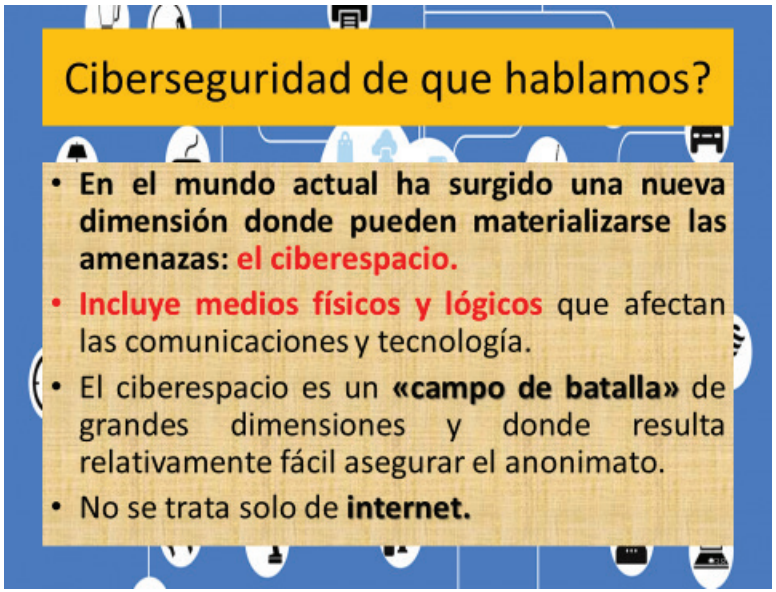
Ya los ciberdelitos dejaron de ser una actividad exclusiva de los hackers ya cualquiera puede obtener el conocimiento y participar en una lucrativa acción, que si les va del todo bien pueden continuar con una carrera rentable. Es por esto que en el 2014 durante una conferencia del entonces Ministro del Interior Español Jorge Fernández Díaz, puso de manifiesto que esta actividad ya ocupaba un tercer lugar de las actividades delictivas y criminales a nivel mundial y que esto es de conocimiento de las Fuerzas Militares y de Seguridad.

A esto se suma la cantidad creciente de eventos de a través del denominado Man in the Midlle o Janus que permite que un atacante interfiera en un segmento de la red, e interfiere las comunicaciones entre dos equipos. Esto puede hacerse muy claramente pero también puede realizarse sin que los intervenidos se den cuenta prácticamente haciendo una interferencia en el router o distribuidor de internet.

En otro lado las denegaciones de servicios (DoS) son los ataques que más preocupan a las organizaciones ya que inundan con software maliciosos o bonnets como especies de robots a los servidores. Este tipo de resultado ha demostrado generar importantes pérdidas económicas y dañar significativamente la reputación de las organizaciones en diferentes sectores. Junto con las brechas de datos, son probablemente las amenazas que más preocupan en la actualidad. Si esto es utilizado para entorpecer los servidores de unidades de primera respuesta o atención a emergencias, se produciría un impacto significativo que puede afectar los que requieren estos servicios.

La estructura piramidal de estos ataques hace que se multiplique de manera exponencial el efecto del ataque, y reduce las posibilidades de respuesta, ya que los computadores, interpretan están respondiendo a un número de usuarios que aumenta en cada clic o botón de entrada.

Esto permite enfocarnos en algunos aspectos interesantes ya tratados y a modo de resumen, de que podemos esperar para los próximos años. La ciberseguridad y ciberdefensa han surgido como nuevas dimensiones a la seguridad, que bien haría repensar las teorías de Abraham Maslow en la estructura de las necesidades humanas que este sugirió y que luego de haber completado las llamadas fisiológicas o primarias, el ser humano quería seguridad. Pero de qué seguridad hablamos cuando ya no solo abarca lo que vemos.

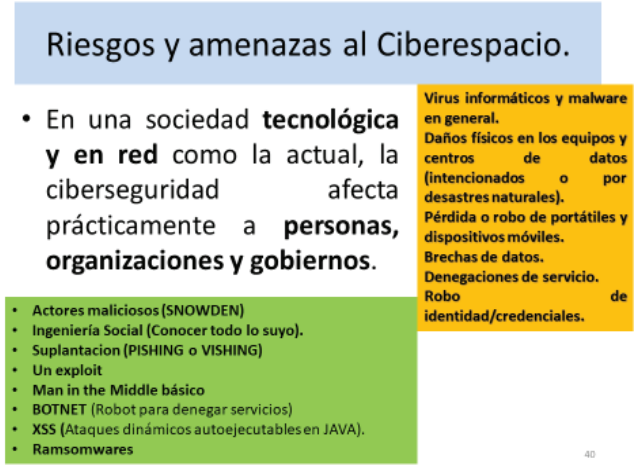


Este ciberespacio incluye medios físicos y lógicos que se interrelacionan y hacen posible la vida del hombre de manera cotidiana como un gran eslabón que une al siguiente, y que si fallan afectan sensiblemente las comunicaciones y la tecnología. Esto nos permite entender que las Fuerzas Militares y los organismos de Defensa y Seguridad se encuentran frente a un nuevo "Campo de Batalla" de grandes dimensiones y donde resulta muy fácil actuar desde la clandestinidad, sin grandes recursos y con conocimiento prácticamente rudimentario, técnico, vocacional, por lo que no se trata solo de Internet esto asegura otros alcances.

En la conferencia virtual del grupo Internet Society "Ciberseguridad o Ciberdefensa" no se trata del Ciberinteligencia, el expositor Enrique Ávila Gómez, hablando en torno a la estrategia de Seguridad Nacional de España, (Gómez, 2017), habla de que el dominio del ciberespacio implica más que lo tangible o físico. El dominio ciber está caracterizándose como el viejo oeste norteamericano, y no existen leyes suficientes para enfrentar esto y posiblemente tomará años para que pueda ser definido.

En un esfuerzo del Centro Criptologico Nacional en su glosario establecen las definiciones de ciberdefensa, ciberseguridad y ciberinteligencia, pero estas han quedado obsoletas, debido a que plantean un espacio de batalla de tres dimensiones terrestres, navales o aéreas, y sin embargo esto marca un aspecto nuevo con infinidad de intangibles pero capaz de provocar daños inimaginables.

Sufrimos de una dependencia tecnológica, ya que nuestro modelo productivo se enmarca en esto, donde incluso los gobiernos están dejando de ser importantes y dan paso a otros modelos económicos no tradicionales. Esta dependencia afecta mucho más de lo que creemos ya que nuestra vida, nuestra cadena logística y nuestro futuro dependen ampliamente de ello.



Al observar cómo se desarrolla la pesca o la agricultura en la actualidad, no está siendo llevada por la libre o por la naturaleza, sino que está siendo definido en base a un patrón o laboratorio, pero vale la pena preguntar ¿qué nos pasaría si todo esto falla? Hay pocas posibilidades de aplicar la ley en la seguridad interior y la defensa cuando hablamos del ciberespacio. El problema de la territorialidad como el territorio, la población la ciudadanía será reelaborado como ciberciudadania, ya que habría que desarrollar un modelo de derecho internacional que permita aplicar las leyes en el ciberespacio.

El problema de la identidad como solucionarlo tecnológicamente, internet se diseña como un sistema que se desarrolla en la defensa de EUA en caso de la destrucción por un ataque nuclear, entre nodos que se conocen. Esto trasciende el ámbito militar y es inadecuado para asegurar la identidad de quien define un aspecto de índole penal o civil, o jurídico. Cuando hablamos del Internet de las Cosas (IOT) estos equipos tienen 3 capacidades: almacenamiento, cómputo y comunicación, los cuales realizan estas actividades aun sin nuestro consentimiento previo y se están introduciendo en nuestro dominio del ciberespacio, sin criterios, porque lo se persigue es el bajo costo y buena conectividad.

La inteligencia artificial que se genera es más que una fábula, es un problema grave, ya que si no podemos regular estos dispositivos estaremos hablando de ataques hacia infraestructuras críticas, hay que tomar decisiones en tiempo real y no se dispone de tal capacidad. Estamos perdiendo capacidades como seres humanos, capacidad de pensar, de hacer análisis profundos, de generación de conocimiento epistemológico, ya no recordamos siquiera los números de teléfono o utilizamos GPS en vez de mirar el mapa y referenciar nuestra ubicación, ya no buscamos una información en libros sino en Google,

El libro de **Jeremy Rifkin** titulado La sociedad de coste marginal cero, hace una reflexión en cuanto al Internet de las Cosas (IOT) donde establece que esta red conectará a todas las cosas con todas las personas en una red mundial integrada. Esto incluirá personas, máquinas, recursos naturales, cadenas de producción, redes de logística, hábitos de consumo y cualquier otra información que será enviada en tiempo real afectara a todos en función de buscar mejores respuestas y economía de esfuerzos de los seres humanos además de la velocidad en responder a la demanda de manera automática.

Si esto lo asociamos al sector defensa, imaginemos que todos los sistemas de armas estarían controlados mediante computadoras con habilidad del IOT y con respuesta automática, estos equipos estaría georreferenciados y se sabría dónde están en todo momento, además de que pudieran ser intervenidos y propiciar ataques entre aliados o para provocar conflictos con otras naciones, o quedar inutilizados al momento que fueran requeridos ante una amenaza.

¿Están los Cuerpos de Defensa en capacidad para atender los retos y desafíos que la ciberseguridad?

Al revisar el Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe como parte de una gestión de colaboración conjunta entre el Banco Inte-

ramericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) para presentar una imagen completa y actualizada del estado de la seguridad cibernética de los países de América Latina y el Caribe, se puede establecer que la situación los países situados en el hemisferio occidental apunta en opinión de James Andrew Lewis Director y Miembro Senior, Programa Estratégico de Tecnologías Centro de Estudios Estratégicos e Internacionales, que ha habido un buen avance entre los países, pero aun los gobiernos ignoran la seguridad cibernética, y esto sera catastrófico en la medida que la tecnología adquiera un mayor nivel.

Propone que para esta iniciativa y en el marco de la OEA sean tomadas en cuenta al menos cuatro pasos o tendencias fundamentales a seguir para desarrollar una cultura de ciberseguridad no solo en los gobiernos, lo cual debe incluir sus Fuerzas Armadas, sino que además debe aglutinar a comunidades académicas y grupos empresariales.

Pasos para impulsar una cultura de ciberseguridad en América y Caribe:

Primer paso: Propiciar el esfuerzo en una legislación que regule el delito cibernético conforme a la Convención de Budapest sobre el delito cibernético.

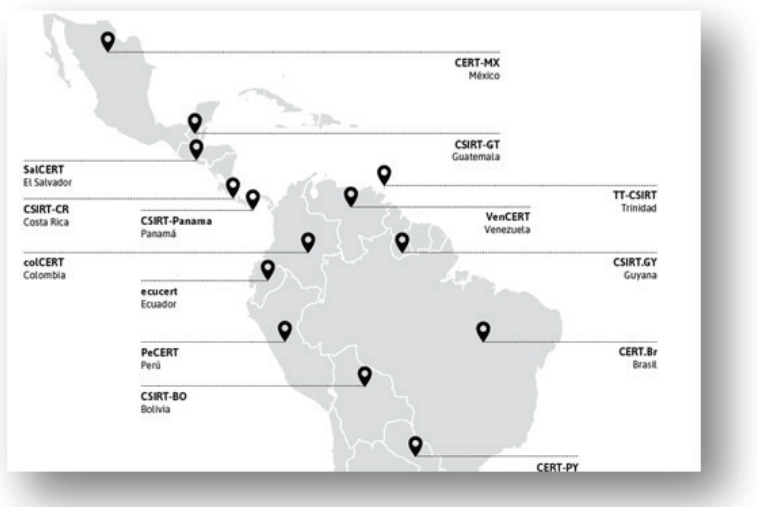
Segundo paso: Definir un modelo común de infraestructuras críticas y judicializar las actividades que puedan afectar (transporte, salud, energía, comunicaciones, instalaciones militares y policiales).

Tercer paso: Fomento a un sistema de confianza de carácter regional, atendiendo a que lo que nos afecta, luego de nuestras fronteras afectará a nuestros vecinos.

Cuarto paso: Formulación de una estrategia nacional de seguridad cibernética donde se definan los roles de colaboración. Los gobiernos nacionales necesitan organizaciones de seguridad cibernética adecuadamente atendida que incluyan como mínimo un CERT nacional y policía cibernéticamente capaz.

La Creación de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) debe ser una prioridad para los países. El CSIRT se define como un equipo o una entidad dentro de una agencia que proporciona servicios y apoyo a un grupo particular (la comunidad de destino) con el fin de prevenir, manejar y responder a los incidentes de seguridad de la información.

El CSIRT se compone de especialistas multidisciplinarios que actúan de acuerdo con los procedimientos y políticas predefinidos para responder rápida y eficazmente a los incidentes des eguridad y para reducir el riesgo de ataques cibernéticos. La existencia de estos permite en cierta forma que los países miembros hablen en el mismo idioma y puedan atender a eventos o ataques a la seguridad o los organismos de defensa de cada país de manera conjunta. Pero cuando realizamos una panorámica nos damos cuenta que el Caribe parece ausente de estas iniciativas frente a los demás países del continente Americano.



Como dato curioso la 2013, República Dominicana se convirtió en el primer país de América Latina que se adhirió al Convenio de Budapest. La Ley 53-07 de 2007 transpuso las disposiciones del tratado al derecho interno, no solo en lo que respecta a la ley sustantiva,sino también a la ley procesal. Lo anterior es una situación atípica en América Latina, donde se prefiere que los poderes procesales sean aplicados a la evidencia electrónica por analogía (OEA, BID, 2016).

Esto se señala porque aunque no tiene ninguna estrategia nacional de seguridad cibernética, ni una política coordinada de defensa cibernética, un número de entidades trabajan conjuntamente para abordar las cuestiones de seguridad cibernéticaen virtud de la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT). A pesar de la participación de las agencias en la CICDAT, el nivel de sensibilización sobre la seguridad cibernética dentro del gobierno es generalmente bajo. Recién ahora están comenzando los operadores de Infraestructura Crítica Nacional (ICN) a adherirse a los estándares internacionales de tecnologías de información (TI) y a adoptar tecnologías de seguridad.

Como nota final se entiende que son los Cuerpos de Defensa quienes por estar comprometidos con la Defensa del territorio y sus nacionales, debe ser el elemento impulsor y de carácter permanente que haga posible el funcionamiento de cada uno de estos estamentos.

De acuerdo al Mando Conjunto de la Ciberdefensa del Reino de España, se define la Ciberdefensa militar como el Conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control de las Fuerzas Armadas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas necesarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos (Ministerio de Defensa, 2017).

Dado que históricamente las guerras son el comportamiento resultante del conflicto armado, por las diferencias entre seres humanos que persiguen alcanzar sus intereses y propósitos nacionales, además de satisfacer sus necesidades humanas, es un concepto que ha sido asociado a los militares, que se ha desarrollado en ambientes terrestres, navales y aéreos, así cada adversario cuenta con una necesidad para dominar el espacio de batalla (Feliu, 2017).

En función de esto cada país establece una Estrategia de Seguridad y Defensa para enfrentar las amenazas reales y potenciales, es por esto que ante eventos que puedan afectar el ciberespacio deberá existir una ciberdefensa que garantice la ciberseguridad. El diccionario de RAE de la lengua define al Ciberespacio como "ámbito artificial creado por medios informáticos". Otros autores como E. Fojón y Sanz Ángel dicen que Ciberespacio es el conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos (CIS).

La Estrategia Española de Seguridad es más explícita y lo define como " el espacio virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas web, foros, servicios de internet y otras redes. El Estado Mayor de la Defensa mejor conocido por sus siglas de EMAD, en su Concepto de Ciberdefensa Militar lo define como "un dominio global y dinámico dentro del entorno de la información, compuesto por una infraestructura de redes, de tecnologías de información y telecomunicaciones interdependientes, que incluye Internet, los sistemas de información y los controladores y procesadores integrados, junto con sus usuarios y operadores" (Feliu, 2017).

Conclusión

Visto de esta forma el Ciberespacio es un espacio único de grandes dimensiones que no tiene ni límites, fronteras o propiedad, por lo que se requiere una nueva definición del concepto de soberanía, territorio, alcances, y como se establece la posesión. Desde el punto de vista militar cuando hablamos de los contribuyentes para la superioridad de información, dejamos claro que la misma puede ser alcanzada cuando tiene acceso.

En todo esto se requiere además de lo expuesto para la creación de infraestructuras dependientes de los ministerios de defensa o de los componentes de Fuerza (terrestres, navales, aéreas) ante potenciales eventos capaces de causar daños en los entornos ciber, se requiere primero definir una política clara, instrumentos legales para su persecución, un marco legal de actuación para los militares, estructuras del tipo CERT o un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés), con sistemas de respaldo para restaurar la operatividad del entorno en casos de un ataque, destrucción, denegación de servicio o la anulación de los sistemas.

En una reflexión final, vale más estar preparados para los eventos que indefectiblemente ocurrirán y reducir el tiempo en que podrán ser reestablecidos todos los servicios, además de cómo proteger los recursos definidos como infraestructuras criticas de posibles ataques que los afecten o garantizando la pronta recuperación, es por esto que debe completarse una conciencia colectiva en cuanto a la seguridad informática especialmente en el sector Defensa que cuenta con un carácter permanente junto con el Estado-Nación.

REFERENCIAS BIBLIOGRÁFICAS

(IEEE), M. D. (2011). Nuevo concepto de ciberdefensa de la OTAN. *Documento informativo del IEEE 09/2011*. Madrid: Minsiterio de Defensa, p. 5.

Beltran, P. (marzo de 2017). Curso de Ciberseguridad. *Conceptos básicos y contexto actual de la ciberseguridad.*

Bolivia, M. D. (1 de mayo de 2010). *IX Conferencia de Ministros de Defensa de las Americas*. Recuperado de http://www.somossur.net/documentos/boletinconferencia.pdf.pdf

Congreso Nacional. (1 de septiembre de 2017). *Anteproyecto de Ley de Seguridad y Defensa Nacional.* Santo Domingo, República Dominicana.

Digital, C. U. (2015). *Estado de la ciberseguridad.* Madrid.

ENISA. (14 de septiembre de 2017). *ENISA*. Recuperado de https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf

Foundation, O. I. (16 de septiembre de 2017). *Open Information Security Foundation*. Recuperado de https://oisf.net/

Gómez, E. A. (3 de septiembre de 2017). *Ciberseguridad o ciberdefensa no se trata de ciberinteligencia.* (Security, Entrevistador)

Milano, C. C. (2003). Los nuevos desafíos de la inteligencia estratégica frente a las nuevas amenazas. *Center for Hemispheric Defense Studies: Redes 2003*, 3-5.

Ministerio de Defensa (20 de septiembre de 2017). intelipage. Recuperado de intelipage: https://www.intelpage.info/mando-conjunto-de-ciberdefensa-de-las-fuerzas-armadas.html

Ministerio de Defensa (2007). *Manual de Doctrina Conjunta*. Santo Domingo, República Dominicana: Edita Libros.

OEA, BID. (2016). Ciberseguridad *¿Estamos preparados en América y el Caribe?* OEA, BID.

ONU. (29 de abril de 2015). 13º Congreso de las Naciones Unidas Sobre la Prevencion del Delito y Justicia Penal. *El fortalecimiento de las respuestas de prevención del delito y justicia penal.* Doha: Naciones Unidas.