ISSN: 2413-869X
ISSN-CD: 2613-8832
e-ISSN: 2636-2309

INSTITUTO SUPERIOR PARA LA DEFENSA
"GENERAL JUAN PABLO DUARTE Y DIEZ"
(INSUDE)

SEGURIDAD, CIENCIA & DEFENSA

REVISTA CIENTÍFICA

CIBERSEGURIDAD, CIBERDEFENSA "LAS AMENAZAS EN EL CIBERESPACIO"

AÑO V • NO. 5 • 2019

MINISTERIO DE DEFENSA

INSTITUTO SUPERIOR PARA LA DEFENSA
"GENERAL JUAN PABLO DUARTE Y DIEZ"
(INSUDE)

SEGURIDAD, CIENCIA & DEFENSA

CIBERSEGURIDAD, CIBERDEFENSA "LAS AMENAZAS EN EL CIBERESPACIO"

Santo Domingo, Distrito Nacional,
República Dominicana

Año V, No.5, 2019

Declaración de privacidad:
Los nombres y las direcciones de correo electrónico introducidos en esta revista se usarán exclusivamente para los fines establecidos en ella y no se proporcionarán a terceros o para su uso con otros fines.

INFORMACIÓN GENERAL

Título	Seguridad, Ciencia y Defensa
País	República Dominicana
Situación	Vigente
Año de inicio	2015
Frecuencia	Anual
Tipo de publicación	Publicación periódica
Soporte	Impreso en papel, sitio web
Idioma	Español
ISSN	2416-869X
Sitio web de difusión	www.insude.mil.do / http://revista.insude.mil.do/index.php/rscd
Temas	Ciencias Sociales
Subtemas	Defensa y seguridad
Clasificación Dewey	350
Organismo responsable	Ministerio de Defensa
Editorial	Instituto Superior para la Defensa "General Juan Pablo Duarte y Díez" (INSUDE)
Naturaleza de la publicación	Revista de investigación científica
Naturaleza de la organización	Institución educativa
Notas	Fuente: Año , No. 1 2015 (impresa en marzo de 2016)
Revista arbitrada	Si

La Revista Científica Seguridad, Ciencia & Defensa, es el órgano de divulgación científica y de publicación anual del Instituto Superior para la Defensa "General Juan Pablo Duarte y Díez" (INSUDE), como Instituto Especializado de la Educación Superior Militar. Coordinada por la Vicerrectoría de Investigación, Extensión y Educación Continua y publicada por el Departamento de Investigación del INSUDE.

Inscribe su quehacer en la naturaleza y misión de la institución al desarrollar las estructuras y procesos académicos necesarios para garantizar la educación superior en la carrera militar. Y ser así, una institución dirigida a promover y difundir la investigación científica, cuyos resultados responden a las necesidades de las Fuerzas Armadas dominicanas en el ámbito de la seguridad y defensa nacional.

CONTENIDO

PRESENTACIÓN DEL MINISTRO

El escenario estratégico del siglo XXI se caracteriza porque, junto a las tradicionales amenazas (simétricas y asimétricas), riesgos y vulnerabilidades para la seguridad, la estabilidad, la paz y el equilibrio armónico de la sociedad, han emergido nuevos modelos de amenazas transnacionales, como por ejemplo el terrorismo con alcance global, con gran capacidad de ocasionar daño indiscriminadamente, así como las diferentes modalidades de ataques que se pueden producir a través del ciberespacio. La lucha contra estas nuevas amenazas es clave en la estrategia de las organizaciones internacionales de seguridad y defensa.

El tener una alta dependencia tecnológica en el seno de nuestra sociedad ya es una realidad constatable, siendo imprescindible para el buen funcionamiento de los Estados, sus Fuerzas Armadas, los cuerpos de seguridad y sus infraestructuras críticas. En menos de una generación, las Tics en el ámbito castrense, han evolucionado desde una simple herramienta para mejorar la productividad administrativa, hasta convertirse en un medio estratégico.

Por tal circunstancia en mi condición de **Ministro de Defensa**, constituye motivo de orgullo presentar el V Volumen de la **Revista Científica "Seguridad, Ciencia & Defensa"**, una publicación que inició sus pasos en el año 2015 y que ya hoy, marca un hito al estar incluida en el catálogo de revistas científicas en línea indexadas por LATINDEX, lo que la convierte en el órgano de difusión académica destinado al estudio científico de la seguridad y la defensa.

Oportuno es manifestar que gracias al esfuerzo denodado del equipo de trabajo del **Instituto Superior para la Defensa "General Juan Pablo Duarte y Díez" (INSUDE)**, se ha podido consolidar esta labor educativa, la cual promueve la investigación al más alto nivel, por la divulgación de artículos de interés y de actualidad, para la sociedad nacional e internacional, motivados estos temas en que los conflictos modernos han asumido formas de confrontación asimétrica, por lo que es cada vez más necesario, usar sistemas tecnológicos en ciberseguridad y ciberdefensa, requeridos dentro de la estructura de las Fuerzas Armadas, a fin de garantizar la trascendencia en los resultados de las operaciones militares (terrestres, navales y aéreas), con el objetivo de mantener la seguridad y la defensa de la nación.

Nos complace hacer la entrega de este quinto volumen, intitulado **Ciberseguridad & Ciberdefensa "Las Amenazas en el Ciberespacio"**, donde se demuestran el alcance y transcendencia de sus autores nacionales e internacionales, quienes evidencian sus conocimientos desglosados en estas páginas, que sirven para proyectar la unión de esfuerzos en el campo del ciberespacio, en aras de lograr mayor seguridad y defensa.

Sea oportuna la ocasión para continuar el proceso de consolidación de las relaciones entre la comunidad científica y la militar, un vínculo que se entrelaza a través de la estrategia y la operatividad de las Fuerzas Armadas, dentro de un mundo globalizado, flexible y versátil.

Ante los nuevos escenarios, la revista científica **Seguridad Ciencia & Defensa** del INSUDE nos obliga a demandar la continuación de la construcción de una nueva cultura de seguridad y defensa.

Éxitos y felicidades a todos los participantes en este gran esfuerzo editorial.

PRÓLOGO

Recorrer un laberinto temático de tanta trascendencia resulta ser una tarea muy ardua, aun para los más acuciosos prologuistas de obras literarias; sobre todo, por la tediosidad de su contenido.

El lenguaje cibernético, en su precisión científica, requiere de profundos análisis por ser tan sofisticada la metodología para encontrar soluciones adecuadas, en lo referente al logro de sus objetivos en materia de seguridad, defensa y amenazas en el ciberespacio.

Bastaría tan solo enfocar de cerca cuán diversas son las técnicas aplicadas por los que propugnan entronizar sus actitudes hostiles. Por ejemplo, uno de los factores que más incidencia tiene en el plano de su combate radica en la dificultad de controlar las grandes amenazas del ciberespacio, por carecer de suficientes recursos para dar al traste con los inminentes desafíos que de manera persistente, se mantienen activos al asecho de las aeronaves que surcan los espacios, muy especialmente en el área correspondiente al Cono Sur.

Ciertamente, la ciberdelincuencia ha ganado un amplio terreno para mantener en zozobra todos los entornos en los ámbitos industriales, laborales y hasta en el desarrollo de la vida privada.

Con mucha facilidad, se han abierto brechas estratégicas en tiempo real y sin importar las distancias insalvables llevar a cabo su accionar delictivo, y viven causando daños sin que sus fechorías tengan que recurrir a equipos de cómputos sofisticados.

El Ministerio de Defensa de República Dominicana ha de emplear su marco de acción de la defensa fronteriza y de los intereses de la nación, según esta consignado en la Constitución, para enfrentar el nuevo reto planteado en el campo virtual, que viene incrementando de forma alarmante, acciones criminales por los agentes ciberdelincuenciales.

De ahí que sea necesario desarrollar una intensa labor para tales fines, y no se puede concluir este prólogo, sin dejar constancia del elogio que merecen todos y cada uno de los exponentes que han plasmado con tinta indeleble sus aportes intelectuales, con mucha maestría y profesionalidad, artículos que han servido para confeccionar el V Volumen de la Revista Científica del Instituto Superior para la Defensa, General Juan Pablo Duarte y Díez (INSUDE), el cual lleva por título: Ciberseguridad, Ciberdefensa "Las Amenazas en el Ciberespacio". Esto, sin duda alguna, abrirá un surco que habrá que recibir la semilla de la concienciación en las diferentes ramas de los institutos castrenses.

PREFACIO DEL RECTOR

En mi calidad de **Rector del Instituto Superior de la Defensa, "General Juan Pablo Duarte y Diez" (INSUDE)**, constituye motivo de gran satisfacción haber logrado el V Volumen de la **Revista Científica: "Seguridad, Ciencia & Defensa"**, una publicación que ha marcado un hito, al convertirse en el órgano de difusión académica destinado al estudio científico de la Seguridad y la Defensa. Con este nuevo volumen de la Revista Científica, el INSUDE se consolida como una institución de educación superior que promueve la investigación de alto nivel, con temas de actualidad y de supremo interés para la comunidad educativa del país.

La Revista Científica del INSUDE nace en el año 2015, fruto del trabajo de un equipo de alto desempeño académico, compuesto por maestros, escritores, asesores, investigadores y colaboradores del INSUDE, que con grandes esfuerzos lograron desarrollar este importante órgano de divulgación, reconocido e indexado por LATINDEX, actualmente evaluada de forma positiva e integrada en el Catálogo de Revistas Científicas indexadas en Línea.

Este nuevo producto del INSUDE, con el título de: **Ciberseguridad & Ciberdefensa "Las Amenazas en el Ciberespacio"**., ha sido elaborado por articulistas nacionales e internacionales, conectados con los avances de las ciencias para la seguridad y la defensa y que encuentran su clímax en la cuarta revolución industrial y en la manera como las tecnologías disruptivas y exponenciales incidirán en la protección de los ciudadanos e infraestructuras criticas como forma de garantizar la paz y la armonía que la sociedad demanda para soportar los procesos de desarrollo social y económico.

Desde la difusión del primer número, nuestra aspiración era que esta herramienta académica se convirtiera en un instrumento destinado a motivar a quienes lean lo complejo que encierra el mundo de la Seguridad y Defensa, a fin de que los artículos publicados permitiera introducir a esas personas hábidas de conocimiento en estas materias tan especializadas, pretendiendo crear una cadena de debates a nivel nacional e internacional sobre temas que proyecten el futuro. Al leer los artículos de este V número, podemos decir con orgullo que lo hemos logrado.

Sea esta la oportunidad para continuar con el proceso de consolidación de las relaciones entre la comunidad científica y la militar, un vínculo que se entrelaza a través de las ciencias militares, navales y aeronáuticas, así como su aplicación en el campo de la estrategia y la operatividad de las Fuerzas Armadas, dentro de un mundo globalizado, elástico y cambiante.

Es evidente que todos estos aspectos nos demandan la continuación de la construcción de una nueva cultura de Seguridad y Defensa. Ante los nuevos escenario y con nuestra Revista Científica: **Seguridad Ciencia & Defensa**, el INSUDE continua en su ruta hacia la excelencia: ***"Desarrollando las capacidades militares y civiles de la defensa nacional"***.

EDITORIAL

La Revista Científica "Seguridad, Ciencia & Defensa" como herramienta de divulgación científica y de publicación anual, se inscribe su quehacer en la filosofía institucional, necesaria para garantizar que las investigaciones dentro de la educación superior militar, persigue que los resultados obtenidos estén vinculadas a las necesidades de las Fuerzas Armadas dominicanas en el ámbito de la Seguridad y Defensa Nacional.

En ese contexto, el desarrollo de este V Volumen, estará relacionado con la **Ciberseguridad, Ciberdefensa "Las Amenazas en el Ciberespacio"**. Ahora bien, la implantación de una cultura de ciberseguridad sólida permitirá crear una conciencia a los miembros de las Fuerzas Armadas y la Policía Nacional, profesionales y empresas de seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento y de la sociedad dominicana, dispuestos para atender los retos que generen los Ciberataques y en donde República Dominicana no escapa de esas amenazas.

Para tratar el tema de **Ciberseguridad, Ciberdefensa "Las Amenazas en el Ciberespacio"**, debemos de hablar sobre la configuración de un ciberespacio seguro, el que dependerá de la capacidad de colaboración entre las distintas agencias gubernamentales, los actores internacionales (tanto públicos como privados), el desarrollo de nuevas tecnologías para prevenir y reaccionar ante dichas amenazas y la capacitación suficiente para afrontarlas. El establecimiento de medidas de persecución real y efectiva de los actores maliciosos, es urgente y se ha convertido en un objetivo de todas las organizaciones nacionales e internacionales en la lucha contra este tipo de ataques.

Ahora bien, la sociedad dominicana ha estado expuesta a ciberataques, que no solo generan elevados costes económicos, sino también y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad resultan críticos para el normal funcionamiento de la sociedad; razón por la cual el Gobierno dominicano ha diseñado mediante el **Decreto No. 230-18, de fecha 19 de junio del 2018**, una Estrategia Nacional de Ciberseguridad 2018-2021, para fortalecer las respuestas y las líneas de acción frente a cualquier ataque, desastre natural u otra emergencia.

En ese tenor, es interesante preguntarnos: ¿Por qué una conciencia nacional de Ciberseguridad y Ciberdefensa? La compilación de los temas que componen este volumen, ha sido un verdadero reto especialmente por los contenidos, alcance y trascendencia que ellos generan, ha sido un trabajo de altísimo nivel profesional acorde con los articulistas invitados. Entender la realidad social en nuestros días pasa ineludiblemente por analizar las circunstancias que rodean a los ciudadanos. Dentro de estos últimos, la tecnología, una vez más, se ha convertido en un disparador de las modificaciones sustanciales y por ende, de las reglas del juego que significan el poder defendernos de una Ciberataque, modificando así, los modelos de relación sociedad-Tic.

A la hora de abordar el V Volumen, consideramos todas las ponencias, basándonos en los actores de estos temas por lo que ningún aspecto ha quedado sin considerar. Por ello, partiendo no solo de las Tic, sino de las Lot, ellas se han convertido en un fenómeno de revolución social, que posibilita cambios y fuerza la acomodación de estructuras tanto jurídicas como políticas, para la protección y seguridad personal y estatales, donde aparecen nuevos riesgos, amenazas, oportunidades, internet y su medio natural **"el Ciberespacio"**, convirtiéndose en un nuevo ecosistema donde todos hemos empezado a convivir. Las iniciativas sobre materias de ciberseguridad que están siendo desarrolladas en todos los países ante este entorno de cambio y en el ciberespacio configuran un reto de entendimiento.

Como el lector ha podido comprobar, nuestros articulistas despertarán la curiosidad ante una situación de candente actualidad y también el conocimiento en esta materia, por el trabajo cuidadoso, bien conducido y documentado que han llevado a cabo, en interesantes tópicos del ámbito del Ciberespacio; artículos de gran interés los que, sin lugar a dudas, su lectura y estudio contribuirán al aprendizaje del lector, al desarrollo de sus competencias profesionales, al reforzamiento de un interés perenne por los hallazgos científicos y por prácticas novedosas de eficacia comprobada. Por último y no menos importante, queremos manifestarle a la comunidad educativa del INSUDE y a la sociedad en general, y muy especialmente al gremio de científicos, que los motivamos a redactar sus trabajos para el volumen Nº VI de nuestra Revista Científica, el cual llevará por nombre: **"Sociedad, Seguridad y Defensa"**.

Disfruten de su lectura.


301

"INFRAESTRUCTURAS CRITICAS Y CIBERSEGURIDAD EN LAS FUERZAS ARMADAS DOMINICANAS"

Critical Infrastructures and Cyber Security in the Dominican Armed Forces

Recibido: 02 / 09 / 2019 Aprobado: 31 / 10 / 2019

Coronel
Nelton Baralt Blanco
Ejército de República Dominicana

El autor es Coronel del Ejército República Dominicana es Doctorando en Métodos de Investigación en Ciencias de la Educación en la Universidad de Cordova, España, tiene una Maestría en Seguridad y Defensa de la Universidad Antonio de Nebrija, España, 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 Director de la Escuela de Graduados de Altos Estudios Estratégicos (EGAEE). Escritor de la unidad I: La Inteligencia Militar. (Libro "Inteligencia Aplicada a la Seguridad del SIGLO XXI" julio 2016) con la Universidad Nebrija/INSUDE. neltonbaralt@egae.mil.do, nelton.baralt@gmail.com

RESUMEN

La seguridad siempre ha sido el aspecto clave en la existencia del hombre a partir del uso de la razón y su capacidad cognitiva, como forma de enfrentar las amenazas. El surgimiento de la tecnología como forma de simplificar procesos complejos y ayudar en la solución de problemas cotidianos también trajo consigo el paso de maquinarias inmensas hasta llegar a procesadores minúsculos con capacidad de desarrollar infinidad de operaciones.

Hoy en día la dependencia a los sistemas computarizados hace pensar que resultaría imposible desarrollar actividad alguna actividad por simple que parezca. Es por esto por lo que la exposición a los entornos virtuales ha aumentado el número de amenazas de carácter cibernético en los entornos industriales, laborales o hasta de la vida privada, abriendo nuevos debates en cuanto a la seguridad cibernética entre la exposición o el riesgo asumido.

La misma facilidad con la que se puede acceder a cualquier sistema en tiempo real y sin importar la distancia, también es la misma vía utilizada por ciberdelincuentes, criminales o terroristas para poder acceder a infraestructuras y sistemas consideradas críticas, como forma de emprender acciones en su beneficio o para causar daños, sin que se requiera para ello, equipos de cómputos sofisticados.

La misión de las Fuerzas Armadas de República Dominicana, consagrada por la Constitución, establece que además del resguardo de las fronteras y los intereses de la nación, implica en este nuevo espacio virtual un nuevo escenario donde seguramente se desarrollaran los nuevos combates del futuro. Se requiere entonces repensar las acciones, roles y misiones y por qué no mejorar la capacidad de respuesta ante estos eventos, dada la dependencia en materia de Tecnología de Información y Comunicación, de los sistemas de defensa nacional.

La creación de centros de atención a emergencias o incidentes cibernéticos, mejor conocidos como CERT o CSIRT, para el sector defensa es forma parte de las agendas nacionales e internacionales, como forma de responder de manera oportuna a las amenazas del entorno ciber, y dotar de las capacidades de resiliencia que permitan restaurar los sistemas en el menor tiempo y con el menor nivel de daño.

Palabras clave:
Amenaza, CERT, CSIRT, ciberseguridad, infraestructura critica, riesgo, seguridad, vulnerabilidad.

ABSTRACT

Safety has always been the key aspect of man's existence from the use of reason and cognitive ability, as a way to deal with threats. The emergence of technology as a way of simplifying complex processes and assisting in the solution of everyday problems also led to from huge machinery to small microprocessors with the ability to develop innumerable Operations.

Today, dependence on computer systems suggests that it would be impossible to develop any activity, however simple it may seem. This is why exposure to virtual environments has increased the number of cyber threats in industrial, work or even private life environments, opening up new debates on cybersecurity between exposure and risk assumed.

The same facility with which you can access any system in real time and regardless of distance, is also the same path used by cybercriminals, criminals or terrorists to be able to access infrastructures and systems considered critical, such as how to take action to your advantage or to cause damage, without requiring sophisticated computing equipment.

The mission of Dominican Republic Armed Forces established in the Constitution, states that in addition to the safeguarding of borders and interests of the nation, it implies in this new virtual space a new scenario where the new fights of the future. It is then necessary to rethink actions, roles and missions and why not, improve the responsiveness to these events, given the dependence on Information and Communication Technology, on national defense systems.

The creation of Cyber Incident or Emergency Care Centers, better known as CERT or CSIRT, for the defense sector is part of national and international agendas, as a way of responding in a timely manner to cyber environment threats, and provide resiliency capabilities to restore systems in the shortest time and with the lowest level of damage.

Keywords:
Threat, CERT, CSIRT, cybersecurity, critical infrastructure, risk, security, vulnerability.

INTRODUCCIÓN

Desde el origen de la humanidad y a partir de lo señalado como la revolución cognitiva donde los seres humanos mediante un proceso de transformación orgánica pudieron diferenciarse del resto de los organismos vivientes en la tierra, surgió como base de este entendimiento la necesidad de sentirse seguros ante las agresiones del ambiente y otros animales, iniciando desde allí nuevas capacidades para enfrentarlas. Esta necesidad de estar seguros para garantizar su propia existencia se ha mantenido hasta nuestros días.

Al hablar de la seguridad en términos integrales, pueden ser asociados algunos conceptos relacionados como: "La ausencia de amenazas", "La reducción del riesgo", o la "reducción de los factores que se asocian a una vulnerabilidad" asumiendo esta última como cualquier persona, actividad o cosa que puede causar un daño.

En estos contextos, la seguridad se asocia a una sensación que, si bien es cierto que se relaciona con el riesgo, las amenazas y la vulnerabilidad, no es menos importante considerar que influyen factores internos en los individuos que valoran indistintamente la sensación de que algo puede afectarlos. Es posiblemente el instinto de supervivencia, lo que más nos ha impulsado a actuar, ante determinadas agresiones, y es por esto por lo que el hombre en sociedad se ha unido para reclamar las garantías que les hagan ser más seguro.

Este enfoque tradicional de la seguridad está relacionado con la propia naturaleza de las fuerzas militares, que en ámbitos de la defensa ha sentado las bases de los planteamientos para generar entornos seguros estableciendo controles de seguridad perimétrica, así como por la fortificación de instalaciones y estructuras como forma de brindar a la sociedad una sensación de seguridad que permita el desarrollo humano.

El diccionario de la Real Academia Española establece que el término Seguridad proviene del latín securĭtas, -ātis, y se asocia a la cualidad de seguro o a la ausencia de amenazas, mientras que el término ciber proviene del inglés cyber-, acort. de cybernetic 'cibernético', y se asocia a las redes informáticas (RAE, 2019), por lo que pudiéramos asociar ambos conceptos y expresar que la Ciberseguridad se refiere a la seguridad en las redes informáticas.
Este modelo tradicional de la seguridad debió transformarse en el momento en que la implementación de medios tecnológicos y la cada vez más marcada influencia de la tecnología en los sistemas funcionales se hizo evidente, complejizo este aspecto al visualizar un mundo físico y su tránsito hacia un mundo lógico, logrando un puente imaginario entre lo tangible y lo intangible.

Esto es algo de lo que nos explica Yuval Noah Harari (sapiens, 2014), cuando establece que a pesar de que en el aspecto orgánico no somos tan diferentes a otros animales, es nuestra capacidad de actuar colectivamente de manera flexible y en masa lo que marca la diferencia.

Este tipo de acciones ha permitido que sea desarrollada una actualización de los conceptos de seguridad y defensa debido a la modificación de los conceptos de riesgo amenaza y vulnerabilidad, además de la aparición de nuevos actores estatales o no, vinculados al ambiente militar o no, así como la multiplicidad de afectados, seres humanos, maquinarias, infraestructuras y softwares (Gamón, 2017).

De lo anterior se entiende que nos mantenemos ante una disyuntiva del modelo tradicional de la Defensa y la Seguridad frente a un nuevo modelo que debe aceptar algunos riesgos y que debe operar en un entorno vulnerable, pero que se asocia también al crecimiento de nuevas amenazas en un entorno virtual e intangible.

PARADIGMAS DE SEGURIDAD Y DEFENSA FRENTE A LA TECNOLOGÍA

Amparados bajo el principio de la legítima defensa y de la búsqueda, protección y preservación de los intereses nacionales, y habiendo sigo testigos de los eventos del 11 de septiembre del 2001 en los Estados Unidos de Norteamérica y el 11 de marzo del 2004 en Madrid, España, evidenciaron nuevos elementos a ser considerados como amenazas y como las actividades cotidianas, podían colapsar, lo cual hizo posible un cambio en las estrategias de Defensa y Seguridad de todos los organismos. Este Siglo XXI promete estar plagado de una serie de acciones o ataques desde diferentes lugares, incluso aprovechando los entornos virtuales lo que ha obligado a la creación de los Cibercomandos.

Conforme a la legislación europea las infraestructuras críticas son definidas como:

"Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros. http://europa.eu/scadplus/leg/es/lvb/l33259.htm (CCNSTIC-401:2007)".

Con esto se destaca que las infraestructuras estratégicas del estado son las que garantizan el desarrollo de las actividades cotidianas y mantiene un equilibrio entre el desarrollo, el uso aplicado de la tecnología y el estado, brindando estabilidad y paz a sus ciudadanos.

Constituye un grave problema de Defensa y Seguridad de los países, poder contar con una organización con las competencias necesarias para garantizar la protección de las infraestructuras críticas y su clasificación, sean estas vistas del modo estratégico, vitales, operativas, funcionales, de defensa y seguridad o de transporte. Así como los correspondientes elementos, instituciones, agencias y marcos legales o de acción para poder actuar en momento determinado. Esto último porque algunas instalaciones pueden formar parte de la iniciativa privada o de empresas, pero pueden afectar a la colectividad de la nación en caso de fallas, así como estas pudieran cambiar de clasificación en un momento determinado, lo cual implicaría un cambio en los roles de control, dirección o administración del recurso.

De acuerdo a un artículo del Dr. Vicente Pons Gamón, publicado en la Revista URVIO (Gamón, 2017), se afirma que el incremento de usuarios de internet es uno de los mayores fenómenos, que ha dado pasos agigantados desde el 1969 hasta la fecha, donde existe una dependencia casi total de los sistemas informáticos, se atribuye junto al crecimiento del internet a un nuevo espacio delictivo, para criminales y terroristas.

Es por esto, que podemos identificar que esto produjo dos cambios significativos en cuanto a los países a partir del marco legal regulatorio para perseguir estos delitos, crímenes y acciones terroristas vinculadas al ciberespacio, y la creación de nuevas estructuras o cuerpos de seguridad para enfrentarlas, perseguirlas o prevenir sus acciones.

Basado en estos criterios se ha podido observar como el desarrollo tecnológico de la humanidad, ha provocado cambios que se asocian a la naturaleza de la guerra. En nuestra intervención durante el Simposio Ciber Seguridad/Defensa 2019 celebrado por el Instituto Superior para la Defensa (INSUDE) se pudo ponderar que asumiendo los cambios paradigmáticos en ciclos de cada 20 años a partir de la Segunda Guerra Mundial (1945) y con ello fueron identificadas acciones militares desarrolladas a gran escala frente a los adelantos y usos de nuevas tecnologías, dejando abierto este esquema para el año 2025, donde con el Big Data, la Inteligencia artificial, las tecnologías disruptivas y exponenciales, sumado a la investigación y desarrollo de equipos cada vez más rápidos y mejores vías de interconexión, no cabe dudas que estaremos frente a nuevos eventos. (Baralt, 2019).

NUEVOS ESQUEMAS PARA LA DEFENSA Y LA SEGURIDAD

La seguridad Informática había sido tratada en un principio sobre la base de mecanismos de restricciones físicas, murallas o controles de acceso, sin embargo, con la proliferación de los equipos informáticos y la mejora de la tecnología, que propiciaron su cambio de tamaño, estos equipos fueron más accesibles, con más capacidad y mejor desempeño que los equipos tradicionales lo que hizo posible que los empleados utilizaran sus propios equipos o desde su hogar.

La protección de las infraestructuras criticas abarca no solo la protección física o material contra posibles ataques, sino otras vin-

culadas con el entorno virtual, además de definir las respuestas correspondientes, así como la normativa de coordinación entre las agencias o instituciones actuantes.

Factores como el terrorismo, la delincuencia organizada, la interconexión de los sistemas críticos, y cada vez más dependientes de la interconexión a través de sistemas de cómputos o instalaciones de carácter privado que no están bajo el control del estado, son algunos de los potenciadores de esta identificación de las infraestructuras, así como los protocolos de acción y marco regulatorio para cada uno de los casos.

Existen tres aspectos se asocian a que la seguridad de información basada en la norma ISO2700 (Glosario de términos) consiste en la preservación de la confidencialidad, integridad y la disponibilidad de la información.

La seguridad Informática como una disciplina que involucra técnicas, aplicaciones y dispositivos que aseguran la autenticidad y privacidad de las informaciones contenidas en los sistemas informáticos, dividiendo está en dos tipos: a) seguridad lógica: De las herramientas informáticas de control de acceso a los sistemas informáticos y b) La seguridad física: Aquella que se especializa en proteger los dispositivos del ambiente externo a causa de factores externos (ataques, incendios, inundaciones etc.).

Las infraestructuras críticas están expuestas a las amenazas internas y externas que pueden afectar no solo a los ambientes lógicos, sino que además pueden afectar los ambientes físicos o una combinación de ambos. A esto se suma el factor humano, que bien puede además afectar ambos ambientes en función al daño provocado con intencionalidad o no, pero que al final tiene un costo similar.

Las infraestructuras deben ser clasificadas y para ello existen diferentes métodos para evaluar las infraestructuras, y para esto se precisa establecer un listado que bien puede estar relacionado con las siguientes categorías:

Energía	*Industria Nuclear Y manufacturera*	*Tecnología de información y comunicaciones*	*Recursos Hídricos*
Alimentación	Salud	Sistema financiero	Transporte
Industria química	Espacio	Investigación	Administración

Tabla 1: Tomado de: Sectores estratégicos conforme a la Ley 8/2011 de Infraestructuras Críticas de España.

De esta lista son consideradas para su evaluación en función de:

- Cantidad de personas afectadas en función del número de víctimas mortales o heridos o consecuencias para la salud pública.
- Impacto económico de las perdidas.
- Impacto medioambiental.
- Impacto público y social (alteración de la vida cotidiana o perdida de los servicios esenciales).

La Constitución de República Dominicana establece las garantías en cuanto al respeto a la dignidad humana y los derechos fundamentales, así como la protección efectiva de su persona, su dignidad a la vez que proporciona los medios para que los ciudadanos puedan perfeccionarse de modo equitativo y progresista lo cual se evidencia en los artículos 7 y 8. (República Dominicana, 2015).

Artículo 7.- Estado Social y Democrático de Derecho. La República Dominicana es un Estado Social y Democrático de Derecho, organizado en forma de República unitaria, fundado en el respeto de la dignidad humana, los derechos fundamentales, el trabajo, la soberanía popular y la separación e independencia de los poderes públicos.

Artículo 8.- Función esencial del Estado. Es la protección efectiva de los derechos de la persona, el respeto de su dignidad y la obtención de los medios que le permitan perfeccionarse de forma igualitaria, equitativa y progresiva, dentro de un marco de libertad individual y de justicia social, compatible con el orden público, el bienestar general y los derechos de todos y todas.

Con el Decreto Presidencial número 230-18, de la Estrategia Nacional de Ciberseguridad la República Dominicana asume su compromiso de garantizar la seguridad de los sistemas de información, así como de las infraestructuras críticas (Gobierno dominicano, 2018).

El objeto de su creación persigue establecer y regular la estrategia nacional de Ciberseguridad del 2018-2021, con la misión de establecer los mecanismos necesarios para la protección del estado, sus habitantes y el aseguramiento del desarrollo y seguridad nacional, además de procurar en su visión, establecerse al 2021 como un país más seguro en cuanto al ciberespacio y las actividades de sus ciudadanos.

Distribuido su accionar a través de 4 pilares, se plantea brindar respuesta en los ámbitos de: 1.- Marco legal y fortalecimiento institucional, 2.- Protección de infraestructuras Críticas e Infraestructuras TI del Estado, 3.- Educación y cultura nacional en ciberseguridad, 4.- Alianzas nacionales e internacionales.

Las Fuerzas Armadas dominicanas, como parte de la estructura del estado, deben emplear sus recursos para provocar un cambio en la naturaleza de las funciones y roles tradicionales, y sumar sus propias iniciativas que permitan ayudar a completar las acciones de esta directiva, y promover la creación de entornos sectoriales seguros.

Nota: Las líneas de acción y objetivos superan los dispuestos, aquí fueron señalados los que afectan al Ministerio de Defensa y la Policía Nacional como instituciones encargadas de preservar la Defensa y la Seguridad Nacional.

PILAR	Objetivo especifico	Lineas de acción
I Marco legal y fortalecimiento institucional	1: Fortalecer el marco jurídico que facilite un ciberespacio seguro en RD.	1.1 Desarrollar un plan de actualización y reforma del marco jurídico. 1.2 Establecer un plan de actualización del marco regulatorio dados los cambios.
	2: Fortalecer las capacidades de los órganos de investigación de crímenes y delitos de alta tecnología.	2.1. Realizar una evaluación de las capacidades de los cuerpos de investigación. 2.2. Incluir en el plan de estudios programas de investigación y seguimiento a evidencias. 2.3 Fortalecer la relación de la policía con la ciudadanía en la mejora de la confianza para hacer denuncias.
2.- Protección de Infraestructuras Criticas e Infraestructuras TI del Estado	1.- Identificar las infraestructuras criticas y de TI de la nación.	1.- Establecer los criterios para la evaluación. 2.- Catalogar las Infraestructuras Criticas y de TI. 3.- Efectuar el análisis de riesgo de las infraestructuras criticas y de TI e identificar su vulnerabilidad.
	2.- Elaborar y poner en ejecución un plan para robustecer la seguridad de la infraestructura crítica.	1.- Considerará las mejores prácticas en ciberseguridad. 2.- Analizar y mejorar las normas emitidas en ciberseguridad.
	3.- Mejorar la Coordinación intersectorial	1.- Establecer un equipo se respuesta ante incidentes cibernéticos (CSIRT-RD) 2.- Promover la creación de equipos sectoriales de respuestas a incidentes cibernéticos y ayudar al CSIRT-RD. 3.- Definir y aplicar un protocolo de comunicación entre los equipos sectoriales y el CSIRT-RD 4.- Hacer cumplir los requisitos mínimos de seguridad y recuperación de las infraestructuras criticas y de TI del Estado.
	4.- Elaborar un plan de respuesta ante incidentes	1.- Identificar las entidades relevantes para la actuación. 2.- Definir el protocolo de activación y actuación de las instituciones ante incidentes de ciberseguridad. 3.- Coordinar y monitorear las actividades de recuperación de incidentes hasta la normalidad. 4.- Crear un plan de ejercicios periódicos y prácticas en incidencias cibernéticas del estado y del sector privado.
Pilar 3: Educación y cultura nacional en ciberseguridad	1.- Incorporar el manejo de los temas fundamentales en seguridad informática.	1.- Incluir planes de capacitación en materia de ciberseguridad al personal docente del nivel básico y media escuela públicas. 2.- Adecuar los planes de estudio de educación básica y media.
	2.-Adecuar los planes de estudio básica, grado y postgrado a ciberseguridad y cibercivismo.	1.- Planes de capacitación a docentes de grado y posgrado en ciberseguridad.
	3.- Crear un marco de coordinación académica en ciberseguridad.	1.- Propiciar la investigación en ciberseguridad. 2.- Desarrollar un programa de caza talentos en ciberseguridad. 3.- Establecer un programa de formación continua para los servidores públicos. 4.- Sensibilizar a la población civil.
Pilar 4: Alianzas Nacionales e Internacionales	Fomentar mecanismos de cooperación nacional con los sectores público, privado y sociedad civil.	1.- Establecer alianzas para la creación de una plataforma de seguimiento conjunta. 2.- Asegurar la participación de República Dominicana en foros y eventos internacionales en materia de ciberseguridad. 3.- Fomentar el intercambio de información nacional e internacional.

Tabla 2: Identificación por pilares de las vinculaciones de las FFAA a la Estrategia de Ciberseguridad RD 2018-2021. Elaboración propia.

Al producirse los cambios en este mundo global en cuanto a este espacio virtual intangible surgen nuevas actividades como la Cibercriminalidad y la Ciberguerra. Ambos conceptos se definen de acuerdo al Diccionario LID de Inteligencia y Seguridad, (Díaz, Cabré, Marcelino, Gómez, 2013) del modo siguiente:

Cibercriminalidad: Modalidad delictiva contra la confidencialidad, la integridad, y la disponibilidad de los datos y los sistemas informáticos. Incluye aquellos delitos relacionados con fraudes informáticos o falsificaciones informáticas, delitos relacionados con la venta o distribución de pornografía infantil a través de internet y delitos que infringen el derecho de la propiedad intelectual o derechos afines. La práctica de actividades relacionadas con la cibercriminalidad ha crecido desde el mismo momento en que apareció internet. Muchos ciberdelitos son perpetrados por delincuentes aislados, pero otros son obra de grupos criminales internacionales.

Por su parte la ciberguerra ha sido definida en el referido diccionario como:

Acción ejecutada por un Estado con la finalidad de penetrar en los ordenadores o redes informáticas de otro, con el objeto de causar daños o interrupción de servicios. El Pentágono reconoció, en 2009, al espacio cibernético como un potencial territorio donde podría librarse un ataque de otros Estados, que podría ir dirigido a infraestructuras críticas, pudiendo así bloquear servicios esenciales como agua, electricidad o transporte; causar daños económicos importantes, e interrumpir actividades cotidianas de ciudadanos, empresas y administraciones. Tras los ciberataques que sufrió Estonia en 2007, muchos países han establecido departamentos de guerra electrónica y han reforzado la protección de sus infraestructuras críticas.

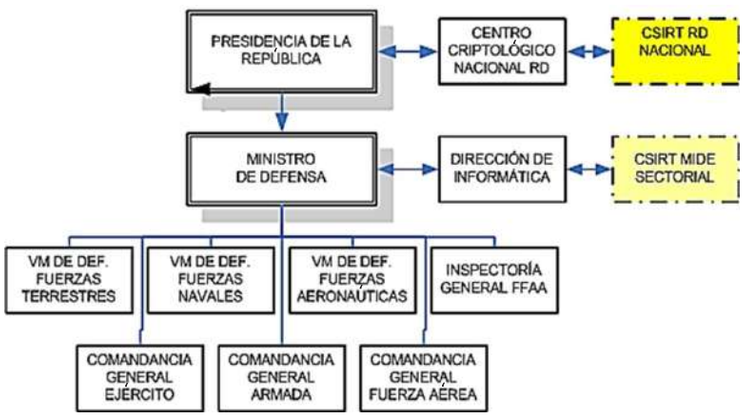
En todas estas definiciones, arrojan nuevamente la necesidad de los estados de generar las estructuras y los instrumentos necesarios para la protección de la vida y bienes de sus ciudadanos, así como la inminente implicación de que los países podían ser afectados por otros a través del espacio cibernético, dirigiendo ataques a las infraestructuras críticas, así como a recursos vitales de cada nación. Esto demanda una estructura defensiva que permita responder a una crisis y que por demás permita restaurar los sistemas en la brevedad posible para su funcionamiento.

LA CREACIÓN DE UN CERT O CSIRT SECTORIAL PARA EL MINISTERIO DE DEFENSA DE REPÚBLICA DOMINICANA

En atención a la Estrategia Nacional de Ciberseguridad las instituciones del estado tendrán CSIRT Sectoriales, los cuales obedecen a instituciones afines. El MIDE puede transformar su Dirección de Informática en el CSIRT-MIDE.

Ante estos nuevos roles que afectarán a las FFAA se propone la creación de un CERT o CSIRT del Ministerio de Defensa de la República Dominicana, utilizando para ello en vista de la experiencia favorable de otros países como el Reino de España, de donde fueron tomados como ejemplos los documentos fundamentales para su diseño y configuración el Producto WP2006/5.1 (CERT-D1/D2) titulado "Cómo crear un CSIRT paso a paso" de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, 2019) y la Guía de Creación de un CERT/CSIRT (CCN-STIC-810) del Centro Criptográfico Nacional del Ministerio de Defensa de España.

Cabe destacar que el proceso de creación de los CERT o CSIRT, se refiere en primera instancia a que la organización ya cuenta con un Sistema de Seguridad de la Información, que ha cumplido con el proceso prudente para su maduración y cuenta ya con la estructura básica de recursos humanos, económicos, instalaciones, infraestructura, protocolos de actuación, un marco legal regulatorio y competencias, aprovechando para ello la estructura existente en la Dirección de Informática en un nuevo esquema.



Propuesta para la creación de un CSIRT para el Ministerio de Defensa de República Dominicana. (Elaboración propia).

Tomando en cuenta los servicios que ofrecería el mismo, dado que cada país tiene sus propias capacidades, recursos y necesidades, para prestar los mismos servicios conforme a la lista de los servicios de los CSIRT del CERT/CC: recuperado de: http://www.cert.org/csirts/services.html, estos pueden ser identificados de acuerdo a su naturaleza, alcance, tamaño y disponibilidad de recursos (ENISA, 2019).

De lo anterior se describen las actividades que el CERT o CSIRT del MIDE deberá ofrecer como servicios de donde los reactivos y proactivos, reflejan una gama importante en cuanto a las actividades, los primeros para responder y mitigar los incidentes y los segundos para prevenir la ocurrencia de incidentes. Todas estas acciones deberán conectar con el accionar del CSIRT-RD o Nacional.

Este, al estar conectado con el Centro Nacional de Ciberseguridad podrá proveer capacidades de información, prevención, mitigación y respuesta adecuada ante cualquier incidencia de carácter cibernético, así como las capacidades de resiliencia ante eventos que puedan ser catastróficos o que afecten las infraestructuras críticas.

Servicios reactivos	Servicios proactivos
✓ Alertas y advertencias	✓ Comunicados
✓ Tratamiento de incidentes	✓ Observatorio de tecnología
✓ Análisis de incidentes	✓ Evaluaciones o auditorías de la seguridad
✓ Apoyo a la respuesta a incidentes	✓ Configuración y mantenimiento de la seguridad
✓ Coordinación de la respuesta a incidentes	✓ Desarrollo de herramientas de seguridad
✓ Respuesta a incidentes in situ	✓ Servicios de detección de intrusos
✓ Tratamiento, análisis y respuesta a la vulnerabilidad	✓ Difusión de información relacionada con la seguridad

Gráfica servicios a ofrecer en el CSIRT del MIDE. (Elaboración propia basado en el documento fuente).

NUEVO PARADIGMA HACIA EL AÑO 2030 DE LAS INFRAESTRUCTURAS CRÍTICAS EN CUANTO A LA SEGURIDAD Y DEFENSA

Los escenarios actuales permiten evidenciar que estaremos en el 2030, en un aumento de la tecnología en cuanto a la cantidad, calidad y uso, por lo tanto se precisa establecer que para las Fuerzas Armadas serán nuevos roles a emplear y nuevos escenarios que dan sentido a la guerra vista no solo desde el punto de vista militar, sino de cómo enfrentar las acciones que puedan generar daños contra la vida y bienes de los ciudadanos.

Visto así la Ciberguerra y los conflictos en escenarios virtuales son una realidad, solo basta definir como la enfrentaremos, y como serán empleadas las medidas para adaptarnos cuando esto ocurra. El desarrollo de políticas públicas para garantizar la ciberseguridad y las infraestructuras críticas, sumado a la educación y concientización en temas ciber, deberán ser la prioridad para los próximos años, en virtud del aumento de la dependencia de los sistemas informáticos y los efectos domino o cascada que pueden producirse en algún momento al colapsar uno de los sistemas prioritarios.

En pocas palabras tendremos que adaptarnos, desaprender, aprender y reaprender, porque cada día van en aumento los sistemas y cambian nuestras capacidades de reacción y no existen las de prevención ante eventos de nueva aparición.

Peor aún, las máquinas dotadas de inteligencia artificial y los programas que pueden tener estas capacidades, permiten evidenciar que nos enfrentaremos a un nuevo enemigo que ha aprendido con nosotros, que podrá anticipar las respuestas y contramedidas, o que de algún modo podrá condicionar nuestra respuesta ante estos eventos.

CONCLUSIÓN

• Estamos frente a un nuevo paradigma que debe ser enfrentado y al que debemos adaptarnos. ¿Estamos preparados para ello?

• Debemos dejar atrás el pasado y estar listos a desaprender para aprender lo nuevo.

• Las amenazas no solo están dentro o fuera de nuestras oficinas o en nuestros hogares, están en todas partes, en todo lo que hacemos o pretendemos hacer.

• Se requiere una formación especializada, cambiante y retadora, que cada día sufre mutaciones y hace muchas cosas.

• Los individuos y las instituciones solos no pueden avanzar, se necesita la cooperación en la sociedad, instituciones públicas y privadas, así como la cooperación internacional y especializada.

• Pero sobre todo, prepararnos no para no caer, sino prepararnos para levantarnos y restaurar los sistemas y servicios que brindan nuestras infraestructuras, cuando por razón de cualquier naturaleza.

REFERENCIAS

Centro Criptológico Nacional. (2015). *Guía de seguridad (ccn-stic-401) glosario y abreviaturas.* Madrid, España: Centro Criptológico Nacional.

Constitución de la República Dominicana. (2015). Santo Domingo, República Dominicana: Congreso Nacional.

Decreto 230-18. (2018). *Estrategia nacional de ciberseguridad 2018-2021.* Santo Domingo, República Dominicana: Presidencia de la República.

Díaz Fernández, A., Cabré, M.T., Elosa, M. y Gómez Enterria, J. (2013). *Diccionario LID de inteligencia y seguridad.* Madrid: LID Editorial Empresarial.

ENISA. (2019). *Como crear un CSIRT paso a paso. Producto WP2006/5.1* (CERT-D1/D2). ENISA. Recuperado de https://www.enisa.europa.eu/publications#c5=2009&c5=2019&c5=-false&c2=publicationDate&reversed=on&b_start=20&c10=C-SIRTs+in+Europe&c8=CSIRTs

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Urvio: Revista Latinoamericana de Estudios de Seguridad,* 15. dx.doi.org/10.17141/urvio.20.2017.2563

Gobierno de España_CCN. (2019). *Guía de seguridad (CCN-STIC-810). Guía de creación de un CERT / CSIRT.* Recuperado de https://www.ccncert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

Obama, B. (2008). *La iniciativa nacional de seguridad cibernética integral.* Recuperado de https://obamawhitehouse.archives.gov/issues/foreignpolicy/cybersecurity/national-initiative

RAE. (2019). *Seguridad.* Diccionario de la Real Academia Española. Recuperado de https://dle.rae.es/

"Tecnología e Infraestructura Crítica para las Operaciones de Defensa Aérea de la Fuerza Aérea de República Dominicana".

Technology and critical infrastructure for air defense operations of the Air Force of Dominican Republic.

Recibido: 23 / 08 / 2019 Aprobado: 31 / 10 / 2019

Coronel
Carlos Febrillet Rodríguez
Fuerza Aérea de República Dominicana

El autor es Coronel técnico de aviación de la Fuerza Aérea de República Dominicana, Diplomado de Comando y Estado Mayor, Master en Defensa Geoestratégica y Dinámica Industrial en la Universidad Pantheon-Sorbone Paris Francia, Maestría en Relaciones Internacionales en el Centro de Estudios Diplomático y Estratégico (CDES), Paris, Francia. Altos Estudios para la Defensa y Seguridad Nacional (IHDEN), Regional (Martinica, Guadalupe, Guayanas y Brasil). Ingeniero Electromecánico Mención Electrónica en la Universidad Autónoma de Santo Domingo. Actualmente es el Director del Taller de Mantenimiento Aéreo y Maestro del Bachillerato Técnico Aeronáutico del Colegio de la FARD. carlosfebrillet@gmail.com

RESUMEN

Hoy en día nuestra sociedad está viviendo una increíble revolución tecnológica, la encontramos en cada área, el gran cambio de análogo a digital desde nuestras aeronaves en su evolución de modernización a través de nuevas tecnologías hasta infraestructuras, nuestra institución la Fuerza Aérea de República Dominicana (FARD), y todo tipo de servicios prestados han provocando una aceleración exponencial de ciberataques. Todas estas nuevas tecnologías, amenazas informáticas a través de la Web en internet y las telecomunicaciones, han evolucionado al pasar de los tiempos convirtiéndose en una gran preocupación de la FARD al igual que otras instituciones, empresas e individuos que necesitan mantener a salvo sus dispositivos para proteger informaciones y datos que están expuestas a pérdidas o filtraciones, debido a esta nueva amenaza y riesgo sobre la seguridad de la información, la cual se ha convertido en una prioridad dentro de la institución, con protocolos de seguridad en áreas vitales e infraestructuras críticas para ser menos vulnerables a estos ataques.

Palabras clave:
Capacitación, comunicación, información, innovación, protección.

ABSTRACT

Today our society is experiencing an incredible technological revolution, we find it in every area, the great change from analogue to digital from our aircraft in its evolution of modernization through new technologies to infrastructures, our Dominican Republic Air Force (FARD) and all kinds of services have led to an exponential acceleration of cyberattacks. All these new technologies, computer threats through the Web , Internet and telecommunications, have evolved over time becoming a major concern for the FARD as well as other institutions, companies and individuals that need to keep their devices safe to protect information and data that is exposed to loss or leakage due to this new threat and risk to information security, which has become a priority within the institution, with security protocols in vital areas and critical infrastructure to be less vulnerable to these attacks.

Keywords:
Training, communication, information, innovation and protection.

INTRODUCCIÓN

Como parte del simposio de Ciberseguridad, Ciberdefensa, las amenazas en el Ciberespacio, manifestamos en nuestra ponencia las actividades en el ciberespacio por parte de terceros que buscan producir una afectación concreta a las infraestructuras críticas dentro de las Innovaciones Tecnológicas de la Fuerza Aérea de República Dominicana y por ende, de la Nación, por lo que resulta hoy, una práctica que aparece como muy difundida entre países desarrollados siendo los muy importantes en el concierto internacional los que sufren estas acciones por parte de actores de menor rango jerárquico en el escenario mundial.

En virtud a lo antes citado, describiremos en el presente trabajo de investigación tres bloques o áreas, la primera será las innovaciones tecnológicas dentro de la Fuerza Aérea de República Dominicana, la segunda será sobre infraestructuras críticas y, por último, las operaciones de defensa aérea.

Partiendo de nuestro título Tecnología e Infraestructura Crítica para las Operaciones de Defensa Aérea en la Fuerza Aérea de República Dominicana, daremos unas pinceladas de cada bloque o áreas y al mismo tiempo se introducirá las latentes amenazas y sistemas de protección.

INNOVACIONES TECNOLÓGICAS DENTRO DE LA FUERZA AÉREA DE REPÚBLICA DOMINICANA

Partiendo del vocablo Tecnología: que es una palabra de origen griego, τεχνολογία, formada por téchnē (τέχνη, arte, técnica u oficio, que puede ser traducido como destreza) y logía (λογία, el estudio de algo), es decir, el estudio de las destrezas para realizar arte, técnica u oficio.

Estas destrezas de las diferentes áreas llegan a nuestra institución por una disposición del alto mando filtrada a través de una comisión aeronáutica seleccionada por nuestro Comandante General dentro de la estructura orgánica de las distintas direcciones de la FARD, la cual vela por todos los proyectos tecnológicos en el sector Aeronáutico. Algunos de estos proyectos tecnológicos vienen de la Dirección de Educación, Capacitación y Entrenamiento (DECEFARD) con sus diferentes escuelas bajo su mando, realizados por los oficiales, cadetes y estudiantes, donde los mejores trabajos científicos son evaluados, desarrollados y puestos en ejecución de ser aprobado para la mejor operatividad y servicio de la institución.

Dentro del Colegio Nuestra Señora del Perpetuo Socorro, FARD encontramos el Laboratorio Aeronáutico con el Departamento de Innovación Tecnológica, allí nuestros jóvenes estudiantes trabajan por competencias adquiriendo la capacidad, destreza y habilidades para realizar las operaciones de mantenimiento preventivo y correctivo de las aeronaves, de sus componentes y sistemas, asegurando la calidad y seguridad, cumpliendo con las normas de gestión de riesgos profesionales y medioambientales vigentes, las regulaciones nacionales, los procedimientos establecidos en las publicaciones de mantenimiento del fabricante y en el Manual de control de mantenimiento de la organización en la que trabajé, siempre bajo la supervisión de un(a) Técnico(a) de Mantenimiento de Aeronaves certificado(a) con licencia y, por ende, con capacidad de certificación del sistema que se trabaje (Grupo Motor, Grupo Estructura, Aviónica).

Dentro del Laboratorio encontramos una aeronave de ala fija y otra de ala rotatoria, trasmisiones, motores de diferentes aeronaves, repuestos y partes de aeronaves, impresora 3D, caja de herramientas, computadoras, tornos, routers, simuladores de vuelo, con la finalidad de que el estudiantes para adquirir conocimiento y destrezas en el sector aeronáutico, con visitas guiadas a los aeropuertos nacionales e internacionales, visitas al órgano de supervisión y control de la Aviación Civil Dominicana (IDAC), el cual promueve el desarrollo sostenible de la aviación civil asegurando la seguridad operacional, visitas a la Academia Superior de Ciencias Aeronáuticas donde los laureados reciben becas para continuar sus estudios superiores al finalizar su ciclo escolar de bachiller. Algunos de estos jóvenes estudiantes ingresan a la institución a través de la Academia Aérea General Piloto Frank Feliz Miranda FARD y la escuela Técnica de Aviación de la FARD.

En su ciclo de enseñanza-aprendizaje por competencias, experimentan la magnífica y grandiosa ocasión de volar en una aeronave de ala fija y una aeronave de alas rotatorias de la FARD.

Al finalizar sus estudios deben desarrollar un proyecto con la creación y fabricación de un artilugio capaz de despegar y aterrizar, navegar por la atmósfera. Estas aeronaves R/C, ya sean

aviones, alas deltas, helicópteros o drones la FARD los modifica, alterando sus capacidades tanto de software como otros dispositivos para poder usarla en el proyecto de observación de video vigilancia como es el caso del VSP, vehículo de seguridad perimétrica, Este es un prototipo de vehículo que se construyó con la finalidad de dar soporte a la seguridad perimétrica de la Base Aérea de San Isidro. Es de construcción ligera de tubos de aluminio con tola metálica, 4 neumáticos de 12 pulgadas con las gomas tubulares, tamaño 2 mts por 1.5 mts, con cámara FHD de 1080p en la parte superior frontal y una cámara lateral para verificar la salida del drone, el cual se encuentra dentro del VSP y posee una plataforma móvil la cual saca el drone de su alojamiento, tiene de autonomía de 3 horas a una velocidad de 60 km /h, su rango de acción es de 7 km. Capacidad de almacenamiento de 3 gls de gasolina, motor de 2 tiempos de 50cc, software FPV. El Drone es un cuadricopter 350, autonomía de vuelo 20 minutos, rango de acción 2km. Este prototipo su primera aparición fue en el desfile militar del 30 de Marzo 2017.

Encontramos infinitas aplicaciones en los drones como son la gestión de la calidad del aire, seguridad vial, seguimiento de especies en peligro de extinción, prevención y extinción de incendios, control meteorológico, publicidad, grabación de eventos deportivos, búsqueda y rescate de personas etc. Pero dónde realmente ofrecen mayores posibilidades para nuestras operaciones de la FARD es a la hora de desempeñar funciones de seguridad y video vigilancia.

Hasta ahora, el uso de drones con video vigilancia está muy extendido en control de fronteras, en la supervisión y protección de grandes espacios como lo es la base aérea y especialmente a nivel militar y en funciones de espionaje.

La video vigilancia a través de nuestros drones modificados está indicada para la protección y seguridad perimetral. Es una solución de video-vigilancia fiable, eficaz y en alta resolución. Nuestros drones están equipados con cámaras de seguridad de alta resolución FHD 1080p, con estabilizador de imagen que garantiza imágenes de gran nitidez y neutraliza los movimientos del dron. Las imágenes se transmiten en tiempo real de forma inalámbrica a un grabador de video-vigilancia que garantiza la integridad de las imágenes.

El drone puede programarse para que despegue a las horas establecidas, de manera que realice tareas de seguridad al manejarse en remoto por un operador y reconocimiento del terreno de forma automática. Los drones, están equipados con cámaras de vigilancia de alta resolución y visión nocturna (cámaras de vigilancia infrarrojas), sensores térmicos, GPS (para programar sus vuelos) e incluso los más avanzados disponen de funciones de reconocimiento facial que les permite identificar usuarios y detectar intrusos y accesos no autorizados.

Los drones con cámaras de vigilancia incorporada, se pueden programar para que en diferentes horas realicen rondas de video-vigilancia. Las rutas y duración de las rondas se pueden definir previamente y el drone sobrevolará los puntos establecidos gracias a la localización GPS. De esta manera, se puede programar para que el drone despegue y realice rondas nocturnas cada hora, comprobando los accesos y el perímetro del espacio a proteger, de la misma manera que lo haría un vigilante físico.

El último proyecto en fase es el proyecto CUYAYA, consiste en un avión hecho en la impresora 3D en pliegos de 2 pies ensamblado y posteriormente armado, su longitud es de 4 mts y envergadura del ala es de 5 mts. Tiene una cámara FHD de 1080p infrarroja, con sistema de amortiguadores en su base para darle estabilidad en la filmación o tomas fotográficas aéreas, poseen un motor de 2 tiempo 200cc.de gasolina convencional 89 octano, almacenamiento de 2 galones de combustible, con capacidad de permanecer 2 horas de vuelo, 40 kilómetros de radio de acción, 80 Km/h de velocidad con GPS, sistema FPV para su control y navegación aérea.

En cuanto al nivel de tecnología aeronáutica del Comando Aéreo, éste se divide en tres escuadrones de vuelo, el Escuadrón de Combate, Escuadrón de Rescate y Escuadrón de Trasporte.

1. El Escuadrón de Combate posee estaciones de trabajo, las cuales utilizan informaciones pertinentes de las aeronaves, además de guardar informaciones precisas de las misiones que se realizan, estas se encuentran desconectadas de toda red de informática para evitar un ataque por medio a esta vía, solo se conecta para actualización de software. Las computadoras de trabajo se conectan a una red privada de la FARD, Entranet donde se puede conectar a una base de datos y al Internet con su seguridad y dispositivos de Firewall de protección.

- En las estaciones de trabajo tenemos el MDS (Mission Debriefing Station) Offline. En este podemos realizar debriefings de misiones, almacenar los datos de misiones y visualizar la trayectoria de las aeronaves sobre un mapa, visualizando en 3D el desplazamiento y las maniobras.
- MPS (Mission Planning Station) (Offline), se planifican las trayectorias de las aeronaves en misión, se calculan las capacidades de las aeronaves según la configuración, se calcula el tiempo de duración de la misión.
- Simuladores de vuelo (Offline), se realizan vuelos rutinarios de práctica y refrescamientos para tener a los pilotos en condiciones de vuelos óptimos.
- Aeronaves A-29B tiene la capacidad de utilizar Flir, infrarrojo de barrido frontal, la cual es una tecnología de imagen que detecta la radiación infrarroja.
- Dentro del equipo de vuelo del escuadrón de Combate tienen los trajes Anti-G y visores nocturnos. Sus pilotos se capacitan tanto en el territorio nacional como en el extranjero, además realizan ejercicios con otras naciones extranjeras, hasta el día de hoy tienen 10 ejercicios Cielo Soberanos (Estados Unidos de América). Y 7 ejercicios Caribe (Colombia).

2. El Escuadrón de Rescate, posee simuladores de vuelo para la capacitación y entrenamiento de los pilotos de fallas de emergencia que solo se practican en simuladores.

- Algunas de las aeronaves de rescate poseen sistema de navegación satelital G-500H, Display de GTN permitiendo la vista en 3D (visión sintética).
- GTN-750H son GPS con características para aviación y el GTN-650 (WAAS) este cada 28 día hay que actualizarlo, estos sistemas de posicionamiento global nos dan la ubicación exacta de los vuelos, tiempo, distancia, cantidad de combustible, altura, etc.
- Algunas de estas aeronaves poseen radar meteorológico donde monitoreamos el clima en tiempo real.

3. El Escuadrón de Transporte posee también su simulador de vuelo en el cual pueden variar de elección del modelo de aeronave de trasporte a volar y capacitarse y entrenarse desde inicial a realizar cursos recurrentes.

- Las aeronaves del Escuadrón de Trasporte poseen trasponedores MODES y ADSB, estos integran el radar y reciben informaciones de los tráficos a las que estén equipadas con el sistema TIS, (Sistema de Información de Tráfico) el ADSB este posee la capacidad de entrar los radares, los satélites y las aeronaves entre todos y brindar información de los tráficos y condiciones meteorológicas, esta información es brindada aun habiendo interferencia del terreno.
- PLB (Personal Locator Beacom) este es un localizador portátil individual que puede ser trasportado a cualquier aeronave.
- ELT (Emergency location transmitter) es una radiobaliza de emergencia para localizar una aeronave que se encuentra en peligro, al activarse manda señales intermitentes de datos que permiten enviar las coordenadas exactas para localizar una aeronave para rescatarla. El emisor tiene una potencia de 350mW a una frecuencia de 121.5 MHz la modulación de amplitud de la emisión de frecuencia corresponde a un barrido de 700Hz. Se activa automáticamente después de un impacto.

Otros explotadores de tecnología, encontramos la Dirección de Defensa Aérea la cual detallaremos en la tercera parte de la exposición, el Comando de Mantenimiento Aeronáutico y el Taller de Mantenimiento Aeronáutico (TAMA).

Estas dos direcciones poseen herramientas modernas de última generación, así como talleres computarizados para el correcto mantenimiento de las aeronaves tanto militares como civiles que llegan a repararse en el Taller de Mantenimiento Aeronáutico. Posee Unidades Móviles listas para salir al socorro de cualquier aeronave que no haya podido retornar a la Base Aérea, con equipo de herramientas especiales para reparar y dar mantenimiento de primera y segunda línea a nuestras aeronaves que tenga una discrepancia de incidente o accidente, contamos software y aplicaciones que nos comunican en tiempo real con el constructor donde ellos nos monitorean cualquier proceso de mantenimiento con el celular o una tablet con cámara, indicándonos los pasos a seguir . Todos los manuales de mantenimiento los encontramos en formato digital y cada 6 meses a un año se actualizan o en caso de una emisión de modificación, AD (Airworthiness Directives), boletines de alerta del constructor y/o de la FAA (Federal Aviation Administration). Tenemos nuestros Hangares de Mantenimiento que poseen estaciones de trabajos computarizadas para poder realizar cualquier trabajo de mantenimiento, conectadas a la red

interna con password de seguridad y monitoreado por el centro de cómputos de la institución los cuales poseen sus protocolos de seguridad para disminuir las posibilidades de un ciberataque, en el peor de los casos que nos aislemos del sistema digital por un eventual hackeo o interrupción de este sistema, se cuenta con documentación física en la biblioteca técnica, la cual es actualizada todos los años permitiendo seguir trabajando sin ninguna novedad.

Unas de las prioridades de nuestra institución es la capacitación y entrenamiento, los cuales nuestro personal técnico realiza cursos recurrentes tanto físicamente en nuestra escuela de formación y capacitación al igual que en el extranjero, además contamos con una plataforma digital para realizar cursos online avalados por el constructor.

En cuanto a la Dirección de Informática y sus adelantos tecnológicos tenemos que han cableado en fibra óptica más de 16,520 metros para la interconectividad de todas las edificaciones de la Base Aérea de San Isidro, poseen un amplio módulo de sistemas administrativos que soportan la infraestructura crítica. Un moderno Data Center con todas las normas TIA, (Telecommunications Insfrastructure Standard for Data Center). Sala de monitoreo C-2, y una plataforma nacional de comunicaciones (PNC). Diferentes Software de aplicaciones para el sistema de abastecimiento, logística, contraloría y finanzas, mantenimiento de vehículos, mantenimiento de aeronaves ICARO, sistema administrativos de personal, armamento, administrativo del hospital.

Existen múltiples ciberataques en cada caso diferente al que estamos expuesto a diario en la Dirección de Informática de nuestra institución al igual que otras empresas somos vulnerables a ataques informáticos como son Troyano, Malware, Worms, Adware, Keyloggers, Ransomme, Virus y unas de las primeras precauciones es conocer al enemigo, para poder enfrentar cada ciberataque, ya que posee diferentes características y cada caso se debe estudiar de forma aislada, la Ciberseguridad posee procedimientos necesarios para asegurar que, con los sistemas que se disponen puedan proteger adecuadamente la información almacenada, los datos y comunicaciones, utilizando las estrategias necesarias para la protección de contra-ataque de la Ciberdefensa que es una parte esencial de la Ciberseguridad.

INFRAESTRUCTURAS CRÍTICAS DENTRO DE LA FUERZA AÉREA DE REPÚBLICA DOMINICANA

Infraestructura Crítica: Término usado por los gobiernos para describir activos que son esenciales para el funcionamiento de una sociedad y su economía.

Ejemplos de Infraestructuras Críticas (IC):

1. Sistema Eléctrico Nacional Interconectado (SENI): Es el conjunto de centrales de generación eléctrica y sistemas de distribución que se encuentran interconectados entre sí. La programación y operación integrada del SENI está a cargo del Centro Nacional de Despacho de Carga (CNDC).
2. Sistema Financiero de República Dominicana: Su función principal consiste en servir como un vínculo o intermediario entre las personas (físicas o jurídicas) que desean ahorrar y aquellas personas que tienen necesidades de recursos, ya sea para consumir o emprender algún proyecto de inversión.
3. Servicio de telecomunicaciones: Uso eficiente del dominio público del espectro radioeléctrico y el desarrollo de las telecomunicaciones.
4. Servicio de radio ayudas a la navegación aérea, los servicios de emergencia, el suministro de agua, los diferentes sistemas de transporte, organismos de Seguridad del Estado, entre otros.

Uso de las IC en Operaciones de Defensa Aérea:

1. Alimentación eléctrica de instalaciones: Militares, Sensores, Centros de Mando y Control, etc.
2. Monitorización del flujo de los recursos e inteligencia financiera en apoyo a operaciones de interdicción.
3. Guerra Electrónica (Sensores y Comunicaciones), especialmente lo relativo a Inteligencia Electrónica.
4. Ciberdefensa.
5. Uso de Big Data para análisis de los corredores aéreos utilizados por estructuras criminales.

Amenazas a las IC para las operaciones de Defensa Aérea:

1. Sabotaje del SENI,
2. Ataques electrónicos
3. Ataques Cibernéticos,
4. Contrainteligencia (aplicación de Inteligencia electrónica en contra de sensores propios).

En nuestra Base Aérea de San Isidro tenemos el Comando de Fuerzas Especiales, el cual una de sus misiones es velar por la central del sistema eléctrico que se encuentra frente a este comando, en caso de una interrupción ya sea por ataque cibernético o climático tenemos plantas de emergencia en las principales dependencias de la institución para suministrar dicha energía, además que poseen como otra medida de seguridad inversores con baterías de reservas para seguir supliendo esta necesidad hasta que vuelva a funcionar el servicio normal.

En cuanto al suministro de agua, la Base Aérea estratégicamente posee tomas independientes de agua suplida por comunidades diferentes y cuenta con destacamentos para protección, no obstante, en la actualidad se realiza la adecuación de la conexión del Acueducto de Santo Domingo Este, como otra medida de protección al suministro de agua para la Base Aérea y los barrios que se encuentran dentro de ésta.

Los servicios de radio ayudan para la navegación de las aeronaves son señales radioeléctricas que son enviadas desde tierra a nuestras aeronaves para guiarse. La torre de control dirige el tráfico aéreo dando asistencia a todas las aeronaves que se encuentren en su zona de control, existen diferentes radios ayudas como son VOR, ADF, ILS, NDB, DME. Las aeronaves cuentan con un sistema de radio independiente con canales de emergencia para su comunicación, en algunas aeronaves dependiendo la misión pueden llevar un teléfono satelital además de sus celulares y comunicación por el Wifi que se tiene a bordo de la aeronave. Radio Harris: provee comunicación en HF para la comunicación con las aeronaves con radios de HF. También provee un mecanismo de encriptación de tercera generación con otros radios Harris, con dicha característica. Actualmente existe una red de radios Harris mantenida por la Armada, en la cual están incluidos, además de la Armada, el Ministerio de Defensa, la DNCD y la FARD. Radio ICOM: Provee comunicación VHF para el monitoreo del tránsito aéreo. Radio Motorola UHF: Provee un enlace repetidor con Alto Bandera para las operaciones de la Fuerza Aérea, el cual a su vez retransmite en VHZ en la frecuencia de operaciones de la FARD con alcance nacional.

LAS OPERACIONES DE DEFENSA AÉREA

Rápidamente se relatará los orígenes, antecedentes, leyes, tecnología y operaciones de defensa aérea de República Dominicana.

1955 Adquisición de Radares de Vigilancia.
1977 Operación Pico (Cuba-RD).
1990 Constantes violaciones al espacio aéreo.
2006 Inicio Servicio de Vigilancia.
2009 Llegada Aeronaves A-29B.
2010, Egresan los primeros 2 Oficiales Controladores de Armas Aéreas (OCA), capacitados en Colombia, por la FAC.
Adquisición del primer radar militar 3D.

La creación de la Dirección de Defensa Aérea, mediante Orden General No.44 del 2012, y efectivo el 1ro. de agosto del mismo año como parte del Estado Mayor Especial, la Dirección de Defensa Aérea tiene sus orígenes en el establecimiento del Servicio de Vigilancia Radar en los Aeropuertos Internacional de Las Américas e Internacional de Punta Cana, a principios de abril del año 2006, como respuesta del Estado ante las constantes violaciones al espacio aéreo nacional por parte del narcotráfico por vía aérea.

La normativa que regula nuestra defensa aérea se encuentra en:

1. La Constitución de República Dominicana en el Artículo 9. Territorio nacional.

2. Ley 491-06, sobre Aviación Civil. Artículo 6.

3. Ley 188-11, sobre la Seguridad Aeroportuaria y de la Aviación Civil. Título IV del Sistema Nacional de Seguridad y Defensa del Espacio Aéreo. Capítulo I, de la creación del Sistema Nacional de Seguridad y Defensa del Espacio Aéreo. Artículo 29. Se crea el "Sistema Nacional de Seguridad y Defensa del Espacio Aéreo".

4. Ley 139-13, Ley Orgánica de las FF. AA.: Artículo 10. Misión de la Fuerza Aérea de República Dominicana (FARD), del Artículo 9 de la presente ley.

5. Reglamento Orgánico de la FARD, donde "establece la misión de defender la Independencia e integridad de la República, proteger la soberanía del espacio aéreo, garantizar el tránsito y comercio por la vía aérea, así como combatir la piratería y la contravención a las leyes y disposiciones sobre navegación aérea".

Podemos definir como defensa aérea: Aquellas operaciones activas y acciones pasivas que se conducen para prevenir, contrarrestar, neutralizar o minimizar los daños que pueda causar un ataque procedente del aire contra los centros vitales de la Nación, la población civil, sus recursos y las fuerzas militares, para negar el empleo ilícito del espacio aéreo.

Las funciones de Defensa Aérea de la FARD son: Detectar aviones incursores que se aproximen a las fronteras del país y penetren en su espacio aéreo, rastrear los aviones incursores, evaluar la amenaza que representan estos aviones, asignar las armas para interceptar y neutralizar con éxito la amenaza, coordinar e integrar los elementos de Defensa Aérea en un sistema único de enlace, desarrollar las actividades de Comando y Control, bajo la dirección de los Centros de Vigilancia y Defensa Aérea e identificar los aviones rastreados.

Los medios utilizados por la Defensa Aérea son la Red de Vigilancia y Detección y Alerta Temprana, el Sistemas de Armas, la Red de Comunicaciones y Procedimientos Operativos de Comando y Control.

Herramientas de vigilancia e identificación:

1. Sistema CSII:
CSII: Es un sistema proporcionado por el Comando Sur de los Estados Unidos para la vigilancia del espacio aéreo, éste además provee las trazas.

2. Sistema Top-Sky:
Top-Sky: Es un terminal radar que nos provee el IDAC para ver en tiempo real las trazas de todos los radares del IDAC de forma directa. Mecanismo de seguridad.

3. Sistema NTRD:
NTRD (New Technologies Radar Display): Es un sistema de sensores remotos en tiempo real el cual visualiza las trazas detectadas por los radares del IDAC sobre el espacio aéreo de República Dominicana. Mecanismo de seguridad: Circuito cerrado (túnel encriptado entre Defensa Aérea y los servidores de Comando Sur).

4. Red AMHS: Consultar planes de vuelo.

5. Red APAN:
Es una red integral de colaboración interagencial de varios países amigos con el fin de compartir información sensible sobre trazas sospechosas salientes o entrantes. Provee un medio de comunicación entre agencias nacionales e internacionales para la cooperación de la vigilancia del espacio aéreo para agencias unidas al CSII.

6. ROTH (Radar Over The Horizon)
No son capturadas por los radares convencionales del IDAC ya sea porque esté fuera del alcance o por vuelos rasantes. Mecanismo de seguridad, doble autenticación con Password y Token, protocolo encriptado https. Estos radares que usan la ionósfera para proyectar sus señales de radio frecuencia tal como hacen los radios HF, solo que en este caso es para la detección de objetivo que sobre vuelen la superficie terrestre. La frecuencia de trabajo va de 3 a 30 MHZ, la frecuencia puede variar dentro de ese rango debido a los cambios de la ionósfera a causa de la actividad solar y otras condiciones atmosféricas. El mismo radar tiene un mecanismo de retroalimentación en tiempo real.

7. RS3:
Es un sistema que nos permite grabar todas las trazas dentro del espacio aéreo de República Dominicana, esto puede ser exportado a formato KML para su futura investigación para casos interesados. Mecanismo de seguridad, circuito cerrado (túnel encriptado entre Defensa Aérea y los servidores de Comando Sur).

8. Teléfono Internacional:
Llamadas nacionales e internacionales (Contacto con las dependencias adyacentes, JIAFTSOUTH, Colombia.)

9. FRAN RELAY: Comunicación con los distintos aeropuertos nacionales.

10. Flota: Contacto vía llamada y Whatsapp con los distintos incumbentes en el proceso operacional.

11. Línea Caliente: Comunicación con JIAFTSOUTH para mantenimiento y funcionamiento de los sistemas que proveen.

Clasificación de las Trazas

Detección: Es la observación que permiten los sensores de radar al establecer la ubicación, velocidad, altura, rumbo de una aeronave. También se podría tener información de detección visual por parte de plataformas aéreas de alerta temprana.

Identificación: A continuación de la fase anterior se procede con el registro de la aeronave y su matrícula. Esto se realiza contactando la autoridad que conoce del plan de vuelo, monitoreando la frecuencia de control de vuelo apropiado, o mediante la observación directa de la aeronave sospechosa, por una aeronave militar.

Clasificación: La clasificación y validación de las trazas puede realizarse de la siguiente manera:

1. Traza Amiga (TA): Toda traza que cumpla con los requisitos de aeronavegación emitidos por el Instituto Dominicano de Aviación Civil.

2. Traza Desconocida (TD): Es la traza que se detecta en un espacio aéreo fuera del Territorio Nacional, con código transpondedor activado y sobre la cual no es posible alcanzar su identificación.

3. Traza de Interés (TI): Es la traza observada dentro del espacio aéreo dominicano que por sus características de vuelo presenta una situación especial que requiere una identificación y seguimiento hasta establecer su estado de legalidad y que puede contemplar una o varias de las siguientes condiciones a saber:

a. Se encuentra volando fuera de una aerovía o por fuera de la ruta de vuelo establecida entre dos puntos conocidos.
b. No se le escucha transmitir por ninguna frecuencia ATS.
c. Se registran cambios erráticos de velocidad y/o altura y/o rumbo.
d. Se registra en una ruta de baja utilización, en especial cuando se trata de salida/ingreso al espacio aéreo nacional.
e. Que su plan de vuelo propuesto involucre aeródromos no controlados y sobre áreas de interés.
f. No tiene activado el equipo transpondedor.
g. Cambios injustificados de plan de vuelo en desarrollo de la inicial propuestos sobre áreas de interés.

4. Traza de Interés Desconocida (TID):

a. Es la traza observada fuera del espacio aéreo nacional que no puede ser identificada, la cual por sus características de vuelo representa interés para el control y seguridad del Espacio Aéreo y demanda la ejecución de una acción inmediata para alertar los medios con que cuenta la Defensa Aérea.
b. Se encuentra volando fuera de una aerovía o de la ruta de vuelo establecida entre dos puntos en áreas fronterizas fuera de territorio dominicano.
c. Se encuentra volando en un área de interés previamente establecida.
d. Se registran cambios erráticos de velocidad y/o altura y/o rumbo.
e. Se registra en una ruta de baja utilización en especial cuando se trata de salida/ingreso al espacio aéreo nacional.
f. Se detecta fuera del Espacio Aéreo Nacional, pero se presume que su origen o destino se dio en territorio dominicano.
g. No tiene activado equipo transpondedor.
h. Cambio injustificado del plan de vuelo en desarrollo de la inicial propuesto sobre áreas de interés.

5. Traza Sospechosa (TS): Es la traza que por sus características de vuelo se encuentra fuera de las normas o reglas de aeronavegación o de Seguridad Nacional. Puede contemplar una o varias de las siguientes condiciones a saber:

a. Una traza que este volando a bajo nivel (menor a 3,000 pies) en un radio menor o igual a 60 millas náuticas del radar y/o de una Base Aérea, sin identificar.
b. Una aeronave que vuele el espacio aéreo nacional sin la debida autorización de plan de vuelo ante la Autoridad ATS competente.
c. Una aeronave que ingrese a una área restringida sin autorización.
d. Una aeronave que aterrice y/o despegue desde un aeródromo no autorizado.
e. Una aeronave sobre la cual, a pesar de agotar las medidas de coordinación con las dependencias de tránsito aéreo, no se logra su identificación.
f. Que incumpla sin causa justificada los procedimientos especiales dictados para las áreas restringidas, entrando o saliendo de ellas, aun mediando autorización de sobrevuelo.

6. Traza Hostil (TH): Una aeronave se considera hostil cuando se encuentra violando el espacio aéreo nacional, dentro de las 12 millas náuticas próximas a la línea de costa y que luego de ser identificada e interceptada como aeronave sospechosa, no atiende las normas y procedimientos indicados por su interceptor. Puede contemplar una o varias de las siguientes condiciones a saber:

a. Aeronave militar extranjera que ingrese al espacio aéreo de República Dominicana sin autorización.
b. Una aeronave que esté volando a un nivel menor de 3.000 pies en un radio menor o igual a 40 millas náuticas del radar y/o de una Base Aérea, sin identificar.
c. La aeronave que una vez interceptada no atiende las instrucciones del interceptor o registre una actitud de agresión o de ataque.
d. Aeronave que se encuentre aterrizada en un aeródromo ilegal sin autorización de la Fuerza Aérea Dominicana, Instituto Dominicano de Aviación Civil o el Departamento Aeroportuario.
e. Aeronave efectuando operaciones nocturnas desde pistas no autorizadas o sin plan de vuelo.
f. Aeronave que una vez interceptada, arroje objetos o elementos y que de forma sistemática desatienda las instrucciones de la aeronave interceptora.
g. Aeronave que sobrevuele sin autorización a una altura inferior a 3000 pies cualquier instalación militar.
h. Si existen razones suficientes que indiquen que la aeronave representa una amenaza inminente para personas fuera de la misma y se concluya que el reporte de interferencia ilícita está siendo utilizado como engaño para evitar el uso de la fuerza por parte de la FARD, por lo que no se aceptará la declaración por parte del piloto de la aeronave interceptada, en situación de emergencia por interferencia ilícita (secuestro) o por motivos técnicos, después de realizada una interceptación.

CONCLUSIÓN

Podríamos concluir uniendo los tres bloques del desglose de la exposición en:

Las Tecnologías e Infraestructuras Críticas para las Operaciones de Defensa Aérea son el estudio del empleo de activos esenciales para el funcionamiento de la sociedad, su economía, sus recursos, para negar el empleo ilícito del espacio aéreo, espacial y ciberespacial en operaciones activas y acciones pasivas que se conducen para prevenir, contrarrestar, neutralizar o minimizar los daños que pueda causar un ataque procedente del aire, espacio o ciberespacio.

REFERENCIAS

Bermejo Higuera, J. (2019). *ITM, Introducción a la Ciberdefensa.* EDITA y MAQUETA: Fundación In-Nova Castilla La Mancha. Recuperado de http://campus.in-nova.org formacion@in-nova.org

Fuerza Aérea de República Dominicana. Dirección de Defensa Aérea. (s.f.) *Manual de doctrina operacional.* Santo Domingo. FARD.

Pérez Martínez, F., García Otero, M. (2019). *PTD guerra electrónica.* EDITA y MAQUETA: Fundación In-Nova Castilla La Mancha. Recuperado de http://campus.in-nova.org formacion@in-nova.org

Pichardo, J. (2019). *Ciberseguridad e infraestructuras críticas (parte I).* Recuperado de https://cncs.gob.do/articulos/ciberseguridad-e-infraestructuras-criticas-parte-i/

Tecnología (2020). *Wikipedia, La enciclopedia libre.* Recuperado de https://es.wikipedia.org/wiki/Tecnolog%C3%ADa

"Costo económico de los Ciberataques no tipificados en las leyes dominicanas"

Economic cost of the cyberattackes not typed in Dominican laws

Recibido: 18 / 09 / 2019 Aprobado: 31 / 10 / 2019

Capitán de Navío
Rocío Santana Gozález
Armada de República Dominicana

La autora es Capitán de Navío, Armada de República Dominicana, Ingeniera en Sistemas. Graduada en la Universidad Iberoamericana (UNIBE). Especialista de Estado Mayor Naval de la Escuela de Graduados de Comando y Estado Mayor Naval, con Maestría en Defensa y Seguridad Nacional, Escuela de Graduados de Altos Estudios Estratégicos del Instituto Superior para la Defensa (INSUDE), con doble titulación con la Universidad Antonio de Nebrija, España. Actualmente doctorando en proyectos con la Universidad Internacional Iberoamericana (UNINI, México).omphsantana@gmail.com

RESUMEN

El ciberespacio es declarado ámbito de seguridad en el 2016 por la OTAN y se caracteriza por su intangibilidad, un mundo no físico, flexible, el cual no tiene límites, sin fronteras, donde cualquier persona puede estar interconectada únicamente con una conexión a la red, de tal manera que pueda interactuar con el mundo entero sin barreras, identificándose o en el anonimato. Es en este espacio donde las economías de muchos Estados han percibido crecimientos muy notables debido a las innovaciones en tecnologías de la información, los procesos económicos y la comunicación, pero eso nos ha dejado más vulnerables al uso ilegal de estas mismas ventajas que, por falta de normativas y leyes adecuadas, República Dominicana no es la excepción en este punto, han generado pérdidas cuantiosa y una sensación de desprotección, en vista de las prontas actualizaciones delictivas empleadas en los Ciberataques, superior a los correctivos especificados en las leyes existentes, evidenciando el vacío legal, en vista de la necesidad de regular el uso, el derecho y la protección en el ciberespacio a fin de encontrar el equilibrio entre seguridad y la "libertad" que se percibe en el mismo.

Palabras clave:
Ciberespacio, economía, ciberdelito, ciberataque, leyes.

ABSTRACT

Cyberspace is declared a security field in 2016 by NATO and is characterized by its intangibility, a non-physical, flexible world, which has no limits, without borders, where anyone can be interconnected only with a network connection, in such a way that it can interact with the entire world without barriers, identifying itself or in anonymity. It is in this space where the economies of many States have perceived very notable growth due to innovations in information technologies, economic processes and communication, but that has left us more vulnerable to the illegal use of these same advantages that, due to lack of adequate regulations and laws, the Dominican Republic is no exception at this point, they have generated substantial losses and a sense of lack of protection, in view of the early criminal updates used in the Cyber-attacks, superior to the corrective measures specified in the existing laws, evidencing the legal vacuum, in view of the need to regulate the use, the right and the protection in cyberspace in order to find the balance between security and the "freedom" that is perceived in it.

Keywords:
Cyberspace, economy, cybercrime, cyber attack, laws.

INTRODUCCIÓN

¿Sabes cuánto dinero pierde el sector público y privado de un Estado en promedio por ataques cibernéticos? ¿Qué le ha costado a República Dominicana? ¿La ausencia de fronteras físicas y la dificultad de encontrar a los responsables en el ciberespacio tienen algo que ver con estas pérdidas económicas? ¿Están las regulaciones cónsonas con la novedad del fenómeno y los avances tan rápidos que se producen en el ciberespacio?

Después de la aceleración de la década de los noventas y en términos de seguridad, los ajustes realizados después del 11 de septiembre del 2001, el 2017 fue un año donde los ataques cibernéticos tuvieron papeles protagónicos, mostrando ciertas ventajas frente a las autoridades y dejando una gran tarea de revisión de las leyes que protegen a los ciudadanos víctimas en el ciberespacio.

El aumento del acceso al internet y el riesgo de abuso en torno a su apertura se han convertido en uno de los temas más apremiantes de nuestro tiempo. No hay duda de que esta híper-conectividad es una poderosa herramienta de desarrollo que debe permanecer abierta y accesible. Funciona como motor de crecimiento y una oportunidad para gobiernos, empresas y personas por igual. Sin embargo, esta apertura y accesibilidad vienen con riesgos.

COSTO OPERACIONAL DE LA CIBERSEGURIDAD

La compañía analista Gartner[1] pronosticó que para el año 2020 habrá 20.400 millones de dispositivos conectados. La atención a este dato debe estar en si cada una de esas conexiones conllevan a la concientización del usuario final acerca de la comprensión de las políticas de privacidad y de los derechos que lo amparan antes de aceptar. Es necesaria la concientización de la población de que la seguridad es asunto de todos, que a todos nos compete, y que un ciberespacio más confiable redunda en su beneficio.

Las amenazas, riesgos y vulnerabilidades van en aumento exponencial y no es paranoia, un ciber-delito podría originarse desde cualquier lugar y pasar por una serie de computadoras comprometidas por piratas informáticos de todo el mundo antes de alcanzar su objetivo previsto. Este es solo un ejemplo de cómo el ciberespacio complica el concepto de tiempo, distancia y jurisdicción.

Como sabemos, el desarrollo tecnológico ha transformado las operaciones de las empresas e instituciones y la forma en cómo interactúan las personas, pero a la vez han traído riesgos y dificultades en cuanto a la seguridad de la información. En un mundo híper conectado y con todo lo positivo de estos avances e innovaciones tecnológicas, las comunicaciones también han permitido y fortalecido las redes del crimen…quienes están protegidos de un ciberataque, la respuesta es una: nadie.

Según el Informe sobre Riesgos Globales para 2016 del Foro Económico Mundial[2], los ataques cibernéticos se han considerado como uno de los principales riesgos globales entre los más probables de ocurrir y con mayores consecuencias. En los últimos años han aumentado rápidamente, atacando a los negocios en todo tipo de sectores empresariales, y con ellos al ciudadano. Por lo tanto, se necesitará implementar nuevas directivas que garanticen la seguridad, minimizando los riesgos de ataques cibernéticos.

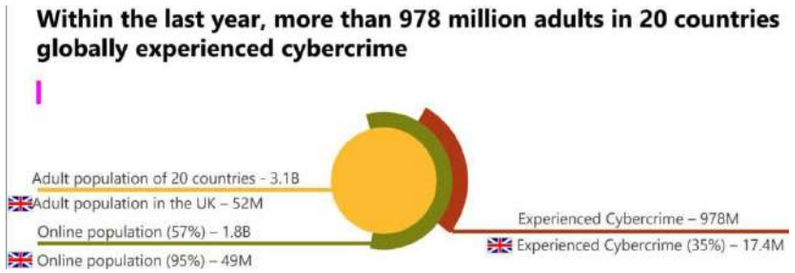
Si bien es cierto que es a partir de la década de los 90, que estos conceptos de seguridad aplicados a la ciberseguridad, comienzan a tener protagonismo y a incrementar su uso y su importancia, como consecuencia de la aceleración mundial que ha generado la tecnología en todos los ámbitos de poder, también es cierto que la delincuencia da la apariencia que lleva unos pasos más adelante que la comprensión y ajustes en torno a los nuevos conceptos y las normativas que los ampara.

En el año 2017, quedó de manifiesto la evolución de los cibercriminales y sus nuevas formas de delinquir de manera creativa con los robos millonarios de criptomonedas y ataques como los ocasionados por Wannacry y Petya que dejan gran preocupación en las autoridades referente al tema de la seguridad en línea.

[1]Gartner, Inc. es una empresa consultora y de investigación de las tecnologías de la información con sede en Stamford, Connecticut, Estados Unidos.

[2]La versión número 46 de la Asamblea Anual del Foro Económico Mundial en Davos, Suiza, tuvo como tema principal "los desafíos de la cuarta revolución industrial". Más de 2,500 participantes, entre jefes de estado, empresarios, líderes de organizaciones mundiales y regionales y sociedad civil conversaron sobre la situación económica internacional caracterizada por el aumento de los intercambios y sobre las soluciones a los retos que imponen las nuevas tecnologías y modelos empresariales.

Según el informe de Norton Cyber Security Insights en el año 2017, el robo en línea ascendió a unos 172,000 millones de dólares estadounidenses, que afectaron a 978 millones de consumidores en 20 países.



En los primeros siete meses de 2017 se totalizaron 677 millones de ciberataques. Colombia y México son de las naciones de habla hispana que más ciberataques recibe. En relación con el anterior año 2016, este problema experimentó un incremento de 59%.

Dentro de los países que conforman América Latina se han estimado pérdidas por noventa mil millones de dólares estadounidenses, según un estudio realizado por Net Scout Arbor, "Tendencias en Ciberseguridad en Latinoamérica". Un caso muy notorio fue el que experimentó Venezuela en agosto de 2017 y que dejó sin telefonía celular a siete millones de usuarios.

En República Dominicana, desde enero a julio de 2017 se produjeron 24 millones de ciberataques , siendo los servicios financieros, los récords médicos del sector salud, el sector educativo y las universidades los más afectados. Además de secuestrar información de empresas a través de virus como Wannacry, muchos de los ciberataques[3] en República Dominicana tienen por objeto, obtener información confidencial de algún cliente y amenazar con publicarla, comprometiendo así a la empresa que debe resguardar esa información, por lo que se ve en la obligación de pagar a los ciberdelincuentes que se dedican a eso. Se puede observar gráficamente este proceso.

Fuente:TendMicro /Carbon Black

De acuerdo con el reporte anual de ciberseguridad de Cisco 2018 "La sofisticación de los programas maliciosos está creciendo a medida que los ciberpiratas comienzan a incorporar los servicios en la nube y aluden la detección a través de cifrados, utilizándolos como herramienta para ocultar la actividad de comando y control".

Los Estados son los responsables de la Seguridad Nacional y disponen de medios e instituciones para alcanzarla y mantenerla, solo que en este nuevo ámbito se da la sensación de limitación. Las amenazas procedentes del ciberespacio se presentan, como se ha visto en los ejemplos anteriores, como un conjunto variado y continuamente cambiante de elementos, cuyo objeto es atentar a la seguridad de las personas y de las infraestructuras, tomando en cuenta que la información tiene un valor por sí misma. Por lo tanto, es una gran responsabilidad y reto para los Estados diseñar estrategias que garanticen la eficientización de los recursos disponibles, ya que, en cuanto al poder político, económico, social y militar, mientras mayor sea la eficacia con que sean manejados, mayores serán los beneficios.

La Seguridad Nacional debe garantizarse en todos, y desde todos los diversos ámbitos o espacios estratégicos, establecerse su defensa y conseguir y mantener sus objetivos; se debe estar preparado para las confrontaciones, conflictos o incidentes con otros adver-

[3]https://www.eldiaº.com.do/el-60-operaciones-bancarias-en-el-pais-se-hace-via-electronica/

sarios, cuyos objetivos sean incompatibles con los propios, y también, por otro lado, se pueden mantener acuerdos de cooperación con otros países.

El Lic. Carlos E. Pimentel Florenzán[4] expresa que la seguridad nacional en el marco institucional de un Estado de Derecho, proporciona las garantías necesarias a la nación para la vigencia de sus intereses y objetivos nacionales frente a cualquier amenaza, que en el caso de República Dominicana son multidimensionales, vinculadas a factores de orden público, entre ellas, la inmigración ilegal, el tráfico ilícito de armas, lavado de activos, trata de personas, corrupción, narcotráfico y la penetración del crimen organizado, entre otras.

También es un hecho reconocido a nivel mundial, que la delincuencia cibernética es una amenaza real y presente para la estabilidad de cualquier sociedad y República Dominicana no es la excepción. La escala y la sofisticación de la delincuencia informática ha hecho que muchos gobiernos replanteen su estrategia para la protección de sus ciudadanos en una economía mundial cada vez más impulsada por, y dependiente de la tecnología.

Garantizar la ciberseguridad es una de las prioridades de la agenda de los países del hemisferio. La Organización de los Estados Americanos (OEA) está trabajando en el desarrollo de una agenda sobre seguridad cibernética en las Américas con el objetivo de que las estrategias presentadas contribuyan notablemente a conseguir un espacio cibernético más seguro para ciudadanos, empresas y administración de pública los diferentes países.

Los delincuentes cibernéticos suelen tener objetivos claros cuando se lanzan a sus actividades ilícitas. Ellos saben cuál es la información que están buscando o los resultados que quieren lograr, y además del camino que deben tomar para alcanzar esos objetivos. Estos criminales le dedicarán un tiempo importante a la investigación de sus objetivos, a menudo a través de la información a disposición del público en las redes sociales, y planean sus acciones cuidadosamente. Asimismo, el interés de muchos de estos ataques maliciosos ha sido exponer y/o explotar información sensible y confidencial, que puede tener efectos perjudiciales para los agentes gubernamentales y la infraestructura crítica.

Existe la idea de que los usuarios de Internet deben asumir que no se puede ni se debe confiar en nada en el mundo cibernético. Sin embargo, las organizaciones de los sectores público y privado, así como las personas, todavía desean tener la seguridad de que se puede confiar en las tecnologías de las que dependen cotidianamente.

En los últimos años, las empresas han ido generando cada vez mayores cantidades de datos personales y sensibles, tales como nombres, direcciones e información de tarjetas de crédito. Además, cada vez más empresas almacenan datos personales y sensibles en plataformas en línea o en otros medios de comunicación electrónicos. A medida que se van volviendo más accesibles grandes cantidades de datos, estos se han convertido en productos básicos de gran valor para los delincuentes cibernéticos, ya que pueden ser vendidos a otros actores maliciosos. En consecuencia, los individuos, empresas y gobiernos por igual, deben tomar las precauciones adecuadas para proteger sus datos.

Las tendencias mundiales en delitos cibernéticos demuestran que el sector financiero es el sector más atacado por los delincuentes cibernéticos. Sus actividades incluyen el phishing, robo de identidad y la creación de aplicaciones bancarias falsas.

Es por todo esto que se debe robustecer el marco normativo, pero, para esto, primero se debe saber con qué se cuenta para poder mejorar y ajustar las leyes, las instituciones y los organismos de respuesta y, en virtud de ello, a continuación se describirán las normas legales vigentes sobre la materia:

- **Constitución de República Dominicana.**

  De acuerdo con el Artículo No. 44 de la Constitución de República Dominicana del 2015, en su numeral 2, que dice "toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad,

[4]Carlos E. Pimentel Florenzán, abogado, con experiencia profesional en los ámbitos de la transparencia en la administración pública, Miembro Fundador / Oficina de Asesorías, Consultorías e Investigaciones. (OACI).

licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos".

Asimismo, en el numeral 3, de dicho artículo hace referencia a que "se reconoce la inviolabilidad de la correspondencia, documentos o mensajes es privados en formato físicos, digitales, electrónicos, o de todo tipo".

• Ley No. 155-17. Ley contra el Lavado de Activos y el Financiamiento del Terrorismo.

Esta Ley sustituye y deroga la Ley No.72-02, sobre el Lavado de Activos Provenientes del Tráfico Ilícito de Drogas, del 26 de abril de 2002.

• Ley No. 310-14. Que Regula el Envío de Correos Electrónicos Comerciales No Solicitados (SPAM).

Tiene por objeto "regular el envío de comunicaciones comerciales, publicitarias o promocionales no solicitadas, realizadas vía correos electrónicos, sin perjuicio de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor".

• Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología.

Tiene por objeto "la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra estos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en dicha ley."

• Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales.

Tiene por objeto "brindar el soporte normativo sobre todo lo relativo al uso de nuevas tecnologías informáticas, aplicado al comercio electrónico y al uso de nuevas técnicas para la elaboración, transmisión y autenticación de documentos y mensajes por medios digitales e informáticos".

Esta ley es aplicable a todo tipo de información en forma de documento digital o mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado dominicano en virtud de convenios o tratados internacionales.

b) En las advertencias escritas que, por disposiciones legales, deban ir necesariamente impresas en ciertos tipos de productos en razón al riesgo que implica su comercialización, uso o consumo.

• Decreto No.230-18, que Establece y Regula la Estrategia Nacional de Ciberseguridad 2018-2021.

Mediante el Decreto No. 230-18 se aprobó la Estrategia Nacional de Ciberseguridad de República Dominicana 2018-2021. Según el gobierno, este documento ha surgido de la voluntad del Estado dominicano de hacer frente a las amenazas cibernéticas y como mecanismo para crear un ciberespacio más seguro.

Algunas de las instituciones primordiales para el combate de la ciberdelincuencia:

• Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), que es una dependencia de la Policía Nacional y tiene como misión combatir el crimen de alta tecnología dentro del territorio nacional. Se encarga de realizar las investigaciones de todas las denuncias de crímenes y delitos considerados de alta tecnología. Responder sobre la base de capacidad investigativa a todas las amenazas y ataques a las infraestructuras críticas nacionales. Desarrollar análisis estratégicos de amenazas informáticas y desarrollar inteligencia.

• División de Investigaciones de Delitos Informáticos, es una dependencia de la Dirección Nacional de Investigaciones (DNI). Su principal misión es velar por el fiel cumplimiento de la Ley No. 53-07. Esta división se encarga de investigar los crímenes contra la humanidad; crímenes y delitos contra la Nación, el Estado y la Paz pública; amenazas contra el Estado dominicano, la Seguridad Nacional. Trabaja entrelazada con

el DICAT, el Ministerio de Defensa y la Dirección Nacional de Control de Drogas.

Otras instituciones que trabajan y ayudan a informar acerca de las actividades del cibercrimen, los riesgos que estas implican, así como la implementación de las buenas prácticas, incluyen las siguientes:

- Instituto Dominicano de Telecomunicaciones (INDOTEL), junto con la Procuraduría General de la República, coordinan acciones contra el cibercrimen y promueven las políticas de ciberseguridad en el país.

- Instituto Tecnológico de Santo Domingo (INTEC), universidad con la cual el gobierno realizó un pacto para que sirva de base en las certificaciones del personal de seguridad de la información.

El país mantiene una cooperación bilateral con los gobiernos de España y Colombia y con otros países como Estado Parte del Convenio de Budapest[5] y como miembro de la red 24/7 del G8, de la INTERPOL y la OEA. De igual forma la República Dominicana obtiene información de los proveedores y operadores de servicios de internet desde los Estados Unidos.

CONCLUSIÓN

No existen leyes o normas que atiendan la problemática de manera integral. Cabe destacar que la Ley No. 53-07 ha sido un paso de avance respecto al anterior estado de cosas existente en República Dominicana en la materia y también lo ha sido la Estrategia Nacional de Ciberseguridad. Sin embargo, conforme avanza la tecnología, se presentan nuevas maneras de delinquir en el ciberespacio.

El marco legal aplicativo a la ciberseguridad no va al ritmo de las mejoradas formas de los ciberataques, por lo tanto, la práctica es ajustar soluciones con normas preexistentes, como contingencia o respuestas a situaciones que se presentan. Es importante que se creen mecanismos o medidas preventivas, conscientes de que modificar las normas toma un tiempo considerable.

Es a través de la educación y de la buena información que se pueden ir reduciendo los potenciales daños. Es importante la preparación de un personal calificado y experto en estos temas, así como seguir contando con el apoyo del Estado dominicano, que debe colocar a la ciberseguridad como prioridad en la agenda gubernamental, creando las instancias necesarias capaces de emitir y diseñar resoluciones que contribuyan a cubrir las faltas legislativas.

REFERENCIAS

Constitución de la República Dominicana. *Gaceta Oficial* núm. 10805. 13 julio del 2015. (2019). Recuperado de https://poderjudicial.gob.do/documentos/PDF/constitucion/Constitucion.pdf

Decreto No.230-18. (2018). *Establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021*. Santo Domingo, República Dominicana. Recuperado de https://es.scribd.com/document/382100584/Decreto-230-18

Fallas, S. (2019). *Lo más destacado del reporte de ciberseguridad CISCO* 2018. Recuperado de https://gblogs.cisco.com/la/sg-stfallas-lo-mas-destacado-del-reporte-de-ciberseguridad-cisco-2018/

Gartner (empresa). (2019). *Wikipedia, La Enciclopedia Libre*. Recuperado de https://es.wikipedia.org/wiki/Gartner_(empresa).

Global Partner Programs | Trend Micro. (2019). Recuperado de https://www.trendmicro.com/en_us/partners.html

Ley No. 126-02. (2002). *Sobre comercio electrónico, documentos y firma digital.* Santo Domingo, República Dominicana.(2019). Recupe- rado de https://www.indotel.gob.do/media/1060/agenda-regulatoria.pdf

Ley No.53-07. (2007). *Contra crímenes y delitos de alta tecnología*, de fecha 23 de abril del año 2007. Santo Domingo, República Dominicana.

[5]Hasta ahora el documento que sirve como guía en la materia a nivel internacional es el Convenio de Budapest, celebrado en 2001. Sólo 54 países lo han firmado, ratificándolo 42, y 17 reglamentándolo en su derecho interno. En América Latina y el Caribe sólo Panamá y República Dominicana lo hicieron, aunque hay otros en vías de suscribir, como México, El Salvador, Argentina, Costa Rica, Uruguay y Chile.

Ley No. 310-14. (2014). *Que regula el envío de correos electrónicos comerciales no solicitados (SPAM).* Santo Domingo, República Dominicana. Recuperado de https://indotel.gob.do/media/6187/ley-310-14-2.pdf

Ley No.155-17. (2017). *Ley contra el lavado de activos y el financiamiento del terrorismo que busca sustituir y derogar la Ley No.72-02, sobre el lavado de activos provenientes del tráfico ilícito de drogas,* del 7 de junio de 2002. Análisis de la Ley 155-17, Contra lavado de activo y el financiamiento del terrorismo | Respuesta Procesal. Recuperado de https://respuestaprocesal.com.do/analisis-de-la-ley-155-17-contra-lavado-de-activo-y-el-financiamiento-del-terrorismo/

Pimentel, C. (2013). *Una iniciativa: gobierno abierto.* Recuperado de https://acento.com.do/author/cpimentel/

Symantec - Global Leader In Next-Generation Cyber Security | Symantec. (2019). Recuperado de https://www.symantec.com/

Vargas, J. (2017) *El 60 % operaciones bancarias en el país se hace vía electrónica.* Recuperado de https://www.eldia.com.do/el-60-operaciones-bancarias-en-el-pais-se-hace-via-electronica/

"Análisis Sistemático de Metodologías y Modelos para la Gestión del Riesgo en las Operaciones Navales y Costeras de República Dominicana"

Systematic Analysis of Methodologies and Models for Risk Management in Naval and Coastal Operations of Dominican Republic

Recibido: 26 / 08 / 2019 Aprobado: 31 / 10 / 2019

Capitán de Fragata
Fausto R. Richardson H.
Armada de República Dominicana

En la actualidad el autor está en la fase de defensa de la tesis de un Doctorado en Proyectos con la Universidad Internacional Iberoamericana (UNINI – México). Asimismo, está cursando una Maestría en Ciberseguridad con triple titulación, del IMF Business School, la Universidad Camilo José Cela y la Universidad de Nebrija. Obtuvo su formación inicial con una Licenciatura en Informática en la Universidad Pedro Henríquez Ureña (UNPHU), en el año 2003. Ha fortalecido sus conocimientos a través de la titulación de Máster en Gestión Universitaria con la Universidad de Alcalá, España, en el año 2015; y una Maestría en Sistemas de Información mención Gestión de la Información con el Stevens Institute of Technology, USA, para el año 2011. También cuenta con diversas especialidades, entre ellas: Especialidad en Derechos Humanos y Derecho Internacional Humanitario (2011) y una especialización en Seguridad Nacional relacionada a la Ciberseguridad (2018). En su formación técnica profesional domina aspectos de Ingeniería de Software, las Redes y la Ciberseguridad. faustorichardson@gmail.com

RESUMEN

Con la llegada del siglo XXI, y el auge que ha tomado la adopción del uso de las Tecnologías de la Información y Comunicación (TIC) en todos los escenarios de la vida diaria de las naciones, las Fuerzas Armadas han llevado sus operaciones a un nuevo escenario de conflicto armado el cual viene acompañado de amenazas que pretenden vulnerar la Seguridad y Defensa Nacional. Este nuevo escenario es el ciberespacio. En ese sentido, las operaciones navales y costeras no han quedado exentas de ser un blanco de ataque de las ciberamenazas que se convierten en un desafío para las fuerzas militares que se encargan de velar de cualquier intento o situación que ponga en riesgo la soberanía nacional. Por lo que el presente artículo pretende analizar de manera sistemática las diferentes metodologías y modelos existentes, como buenas prácticas, para gestionar el tratamiento a los diferentes riesgos cibernéticos que pudieran impactar de manera negativa en el buen desenvolvimiento de las operaciones navales y costeras de República Dominicana.

Palabras clave:
Operaciones navales, riesgos cibernéticos, análisis de riesgos, ciberseguridad.

ABSTRACT

With the arrival of the 21st century, and the boom of the use of Information and Communication Technologies (ICT) in all scenarios in the daily life, the Armed Forces have carried out their operations to a new scenario of armed conflict which is accompanied by threats intended to violate National Security and Defense. This new scenario is cyberspace. In that sense, naval and coastal operations have not been exempt from being a target of cyber threats that become a challenge for military forces that are responsible for overseeing any attempt or situation that jeopardizes national sovereignty. Therefore, this article intends to systematically analyze the different methodologies and models that exist as good practices, to manage the treatment of the different cyber risks that have a negative impact on the smooth development of naval and coastal operations in Dominican Republic.

Keywords:
Naval operations, cyber risk, risk analysis, cybersecurity.

INTRODUCCIÓN

En los últimos años, los diferentes escenarios de la guerra han sido conquistados por un nuevo enfoque o dimensión, gobernado por bits (cero y uno), conocido como ciberespacio. Esta nueva (y para muchas naciones vieja) dimensión se ha convertido en un gran desafío para los Estados, dado su rápida evolución, y la necesidad imperante del uso de herramientas tecnológicas para la automatización de procesos que permiten ser más competentes a las naciones en un mundo gobernado por la globalización.

En ese sentido, ante este nuevo escenario de conflicto armado, donde accionan actores estatales y no estatales, tal como señala Giudici (2013, p.1), estos pueden valerse de los medios electrónicos disponibles, para poner en riesgo la defensa y seguridad de una nación, atacando las vulnerabilidades de las plataformas tecnológicas e infraestructuras críticas de un Estado.

Las operaciones navales y costeras no han estado exentas de los ataques cibernéticos que se han llevado a cabo, por lo que es una necesidad adoptar las buenas prácticas que permitan garantizar la defensa y seguridad de República Dominicana en los aspectos tratados en este artículo.

Por tal motivo, para poder lograr las garantías al más mínimo riesgo residual aceptado en operaciones navales y costeras, es muy importante aplicar los controles de la seguridad tecnológica que permitan conocer y gestionar los riesgos cibernéticos a los que puedan estar sometidos las operaciones marítimas.

Por lo que el presente artículo, tiene como objetivo analizar las diferentes metodologías existentes para el tratamiento de los riesgos cibernéticos en operaciones navales y costeras, y recomendar las buenas prácticas para el diseño y adopción de un marco de referencia (framework) que se adapte a las particularidades de República Dominicana.

METODOLOGÍAS PARA LA GESTIÓN DE RIESGO EN OPERACIONES NAVALES Y COSTERAS

De acuerdo a la OMI[1] (2017), las tecnologías cibernéticas se han convertido en herramientas esenciales que permiten el funcionamiento y la gestión de los numerosos sistemas cruciales para la gestión de la seguridad y protección del transporte marítimo y del medio marino.

En ese sentido, y de acuerdo al criterio del autor de este artículo, en las operaciones navales y costeras aplican los tres (3) ejes sobre los que están basadas las metas de la ciberseguridad: i) Confidencialidad que no sean reveladas informaciones por usuarios no autorizados; ii) Integridad que no sean alterados los datos e informaciones; y la iii) Disponibilidad que los sistemas estén funcionales en todo momento.

El riesgo cibernético, según varios autores (Santos et al., 2012, Giudici, 2013; Wegener, 2013; Martín, 2015; Parada, 2018), es la probabilidad de que una amenaza explote una o varias vulnerabilidades resultando en consecuencias indeseables. Según estos mismos autores, una vulnerabilidad es una debilidad en el software / hardware, que puede ser explotada por una amenaza.

Asimismo, una amenaza es la probabilidad de que un evento explote una vulnerabilidad y provoque que sean comprometidos la confidencialidad, integridad y disponibilidad de la información.

Aunque los sistemas tecnológicos utilizados para las operaciones navales y costeras deben cumplir las normas internacionales y las establecidas como buenas prácticas de seguridad por las administraciones de abanderamiento, las vulnerabilidades generadas por el acceso, la interconexión o el establecimiento de redes entre estos sistemas, dan lugar a cualquier tipo de probabilidad de que estos sean impactados por los riesgos cibernéticos a los que están expuestos. OMI (2017) los enumera en los siguientes: a) Los sistemas del puente; b) los sistemas de manipulación de carga; c) los sistemas de propulsión y gestión de la máquina y de control de suministro eléctrico; d) los sistemas de control de acceso; e) los sistemas de servicio a los pasajeros y de organización de los mismos; f) las redes públicas para los pasajeros; g) los sistemas administra-

[1]Organización Marítima Internacional.

tivos y de bienestar de la tripulación; y h) los sistemas de comunicación (pp. 1-2).

Para establecer las buenas prácticas que permitan gestionar los riesgos cibernéticos asociados a los sistemas tecnológicos utilizados en operaciones navales y costeras, es necesario analizar las metodologías existentes, y cómo abordan cada una de estas, la gestión de los riesgos marítimos.

METODOLOGÍAS PARA LA GESTIÓN DEL RIESGO CIBERNÉTICO EN OPERACIONES NAVALES Y COSTERAS

Como órgano rector de las operaciones marítimas internacionales, se analizarán a primera instancia las directrices sobre la gestión de los riesgos cibernéticos marítimos de la Organización Marítima Internacional (OMI), a partir de las cuales se deberán sustentar las buenas prácticas para gestionar los riesgos cibernéticos marítimos.

Directriz sobre la gestión de los riesgos cibernéticos marítimos de la Organización Marítima Internacional (OMI)

De acuerdo a la OMI (2017), sus directrices presentan cinco (5) elementos funcionales que tributan al objetivo de gestionar de manera efectiva los riesgos cibernéticos.

La OMI define los elementos de la siguiente manera:

> a. Identificación. Donde se definen las funciones y responsabilidades del personal en la gestión del riesgo cibernético, se identifican los sistemas, activos, datos y otras capacidades tecnológicas, que de ser interrumpida su funcionamiento, generarán un riesgo para las operaciones de los buques.
> b. Proteger. Es donde se implementan los procedimientos y medidas para el control de los riesgos, al igual que la planificación de los planes de contingencias, con la finalidad de proteger los activos ante cualquier evento que signifique la posibilidad de ocurrencia de un riesgo cibernético y garantizar la continuidad de las operaciones del transporte marítimo.
> c. Detectar. Se crean las actividades necesarias para detectar cualquier suceso cibernético de manera oportuna.
> d. *Responder*. Donde se crean e implementan actividades y planes para dar resiliencia y restaurar los sistemas necesarios para las operaciones o servicios del transporte marítimo que hayan sido afectados por cualquier tipo de suceso cibernético.
> e. Recuperar. Es donde se determinan las medidas para copiar y restaurar sistemas cibernéticos necesarios para las operaciones de transporte marítimo que hayan sido sujeto de un suceso cibernético. (2017, p.4).

Sin embargo, de acuerdo al criterio del autor de este artículo, las directrices fundamentadas por OMI (2017) son elementos insuficientes para lograr implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que vincule los cinco (5) elementos funcionales definidos. Es por tal razón, que la OMI, señala normas adicionales que tributan a las mejores prácticas para implementar la gestión de los riesgos cibernéticos, como una referencia de información más detallada a los usuarios de sus directrices.

De acuerdo a OMI (2017, p. 5), estas normas son:

> a. Directrices sobre ciberseguridad a bordo de los buques elaboradas y apoyadas por BIMCO, CLIA, ICS, INTERCARGO e INTERTANKO (mejor conocidas como normas BIMCO de ciberseguridad).
>
> b. Normas ISO / IEC 27001: Gestión de la Seguridad de la Información. Publicada por la Organización Internacional de Normalización (ISO por sus siglas en inglés).
>
> c. Marco de mejora de la ciberseguridad de las infraestructuras críticas del Instituto Nacional de Normas y Tecnologías (NIST por sus siglas en inglés) de los Estados Unidos. (2017, p. 5).

El autor de este artículo es de opinión que, independientemente se hiciera referencia a la norma ISO 27001 sobre la implementación de un SGSI, también debió hacerse referencia a la norma ISO 27005 sobre Gestión de Riesgos en la directiva de la OMI, debido a que esta es la guía que tiene las recomendaciones de cómo gestionar los riesgos de seguridad de la información que pudieran comprometer a las organizaciones, para el caso de este artículo, las operaciones marítimas.

Otro aspecto que observa el autor de este artículo, es que la directiva sobre la gestión de riesgos cibernéticos marítimos de la OMI, su alcance es concerniente a la seguridad cibernética en los buques.

Sin embargo, en las operaciones navales y costeras, existen otros elementos que integran tecnología cibernética, como por ejemplo los sensores que utilizan las boyas, entre otros, que pudieran afectar las operaciones navales y costeras, de no tomarse en consideración el salvaguardar estas tecnologías de cualquier incidente cibernético que ponga en riesgo el buen funcionamiento de los mismos.

Directrices sobre ciberseguridad a bordo de los buques elaboradas y apoyadas por BIMCO[2], CLIA, ICS, INTERCARGO e INTERTANKO (Guía BIMCO)

La guía BIMCO, de acuerdo a Erawat (2016), es el primer enfoque sistemático para la gestión de riesgos de ciberseguridad en buques. Esta directiva está compuesta por un enfoque para la gestión del riesgo establecido en seis (6) procesos, que de acuerdo a BIMCO (2018), son:

a. Identificación de las amenazas, donde se deben comprender las amenazas cibernéticas externas al buque.

b. Identificar las vulnerabilidades, proceso en el cual se realizan los inventarios de los sistemas a bordo del buque, con enlaces de conexión directa e indirecta a redes de comunicación.

c. Evaluación de la exposición al riesgo, donde se determina la probabilidad de que una vulnerabilidad sea explotada por amenazas externas.

d. Desarrollar medidas de protección y detección, lo que permite reducir la probabilidad de que las vulnerabilidades sean explotadas, y esto permite reducir el impacto en caso contrario.

e. Establecer planes de contingencia, en donde se diseña y prioriza los planes de contingencias para mitigar cualquier riesgo cibernético potencial identificado.

f. Responder y recuperarse de un incidente de ciberseguridad, este proceso se logra utilizando las buenas prácticas definidas en los planes de contingencia.

[2]Consejo Marítimo Internacional del Báltico (BIMCO por sus siglas en inglés).

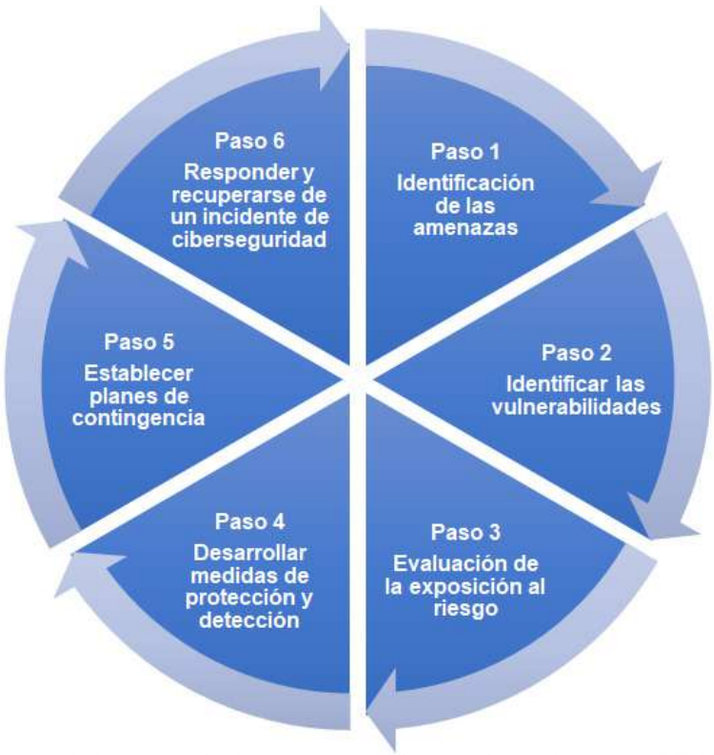


Figura 1. Enfoque gestión del riesgo cibernético según las directrices BIMCO. Fuente: Recreado de Guías BIMCO (2018, p. 4).

Asimismo, el autor de este artículo es del criterio de que la guía BIMCO ofrece un listado más detallado que el definido por la directiva de la OMI (2017) de los sistemas, equipos y tecnologías a bordo de un buque que pueden ser objeto de ataques cibernéticos. Estos quedan agrupados en el mismo contexto de categorías establecidos por la directiva OMI.

Sistema de Gestión de Seguridad de la Información – Normas ISO / IEC 27001

Es del criterio del autor de este artículo, que las normas ISO / IEC 27001 son un estándar mundial de buenas prácticas para establecer un sistema de gestión de la seguridad de la información, y por tanto, aunque estas no están directamente orientadas al sector marítimo, su metodología puede ser utilizada para ser aplicada en la gestión de riesgos cibernéticos en operaciones navales y costeras, acompañado del estándar ISO / IEC 27005 de las mismas normas, pero orientado a la gestión de riesgos.

En ese mismo sentido opina Erawat (2016), cuando señala que las normas ISO 27000 son un estándar aplicable a todo tipo de organizaciones y que son guías reconocidas en el ámbito de la ciberseguridad.

De acuerdo al ISO 27000 (2018), este estándar está compuesto por las siguientes publicaciones principales que conforman un SGSI:

a. ISO / IEC 27001, es la certificación que deben de obtener las organizaciones y que contiene las especificaciones para la implementación de un SGSI.

b. ISO / IEC 27002, es la norma que contiene las buenas prácticas para la gestión de la seguridad de la información.

c. ISO / IEC 27003, esta norma es el soporte de la ISO / IEC 27001, ya que contiene las directrices para la implementación de un SGSI.

d. ISO / IEC 27004, establece las métricas para la gestión de la seguridad de la información.
e. ISO / IEC 27005, contiene las buenas prácticas sobre la gestión de riesgos para la seguridad de la información.

Marco de mejora de la ciberseguridad de las infraestructuras críticas del Instituto Nacional de Normas y Tecnologías de los Estados Unidos (NIST Cybersecurity Framework CSF)

De acuerdo a Erawat (2016), la guía NIST se publicó en el año 2014 por el Instituto Nacional de Estándares y Tecnologías de Estados Unidos y es de libre consulta y aplicación. De acuerdo al criterio de este autor, esta guía posee un enfoque bastante adecuado para gestionar la ciberseguridad en infraestructuras críticas, por lo que considera, puede ser adoptado en el sector del transporte marítimo.

En ese mismo sentido, Erawat señala que los cinco elementos que presenta la OMI (2017, p. 4) en su directiva, son los mismos indicados por la guía NIST CSF.

Función	Identificador función	Identificador categoría y descripción
ID	Identificar	ID.AM Gestión de activos
		ID.BE Entorno del negcoio
		ID.GV Gobierno
		ID.RA Análisis de riesgos
		ID.RM Estrategia gestión de riesgos
PR	Proteger	PR.AC Control de accesos
		PR.AT Concienciación y formación
		PR.DS Seguridad de datos
		PR.IP Procesos y procedimientos para protección de información
		PR.MA Mantenimiento
		PR.PT Tecnologías de protección
DE	Detectar	DE.AE Anomalías y eventos
		DE.CM Monitorización continua de la seguridad
		DE.DP Procesos de detección
RS	Responder	RS.RP Planificación de la respuesta
		RS.CO Comunicaciones
		RS.AN Analisis
		RS.MI Mitigación
		RS.IM Mejoras
RC	Recuperar	RC.RP Planificación de la recuperación
		RC.IM Mejoras
		RC.CO Comunicaciones

Figura 2. Funciones y categorías del Marco de Referencia NIST CSF. Fuente: Recuperado de Erawat (2016).

De acuerdo a la Figura 2 se puede visualizar que, dentro de este marco de referencia diseñado por la NIST, se pueden encontrar para cada uno de los cinco elementos funcionales de la guía OMI, las categorías y subcategorías de los controles de ciberseguridad que pueden ser utilizados para aplicar a cada elemento funcional, y cuyos controles están identificados por un código como se muestra en la figura indicada.

CONCLUSIÓN

Visto lo analizado en el presente artículo, el autor concluye con lo siguiente:

a. Con la publicación de la directiva sobre la gestión de riesgos cibernéticos marítimos de la OMI, queda claramente evidenciado el criterio del autor de este artículo, respecto a que las

operaciones navales y costeras no escapan a los ataques de la guerra cibernética.

b. Es necesario diseñar e implementar, sustentado en las directrices / marcos de referencias establecidos por la OMI y analizadas sus principales características en este artículo, un Sistema de Gestión de Seguridad de la Información (SGSI) que se adapte a las particularidades de las Operaciones Navales y Costeras de República Dominicana, y que permita dar respuesta efectiva a la gestión de riesgos cibernéticos en este sector.

c. Se deberá considerar, el diseño del SGSI a proponer, como un estándar militar que vincule las dependencias del Ministerio de Defensa que deben salvaguardar la soberanía nacional en actividades relacionadas a las operaciones navales y costeras.

d. El diseño del SGSI a proponer, deberá de considerar la gestión de riesgos cibernéticos en todo lo que se relaciona con las operaciones navales y costeras, y no solo enfocado a la protección de la tecnología en buques, como lo establecen las directivas de la OMI y la guía BIMCO.

REFERENCIAS

BIMCO. (2018). *Directrices sobre la seguridad cibernética a bordo de buques.* Recuperado de https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/cyber-security-guidelines-2018.ashx

Erawat. (2016). *Guía OMI ciber riesgo y buenas prácticas ciberseguridad* [Mensaje en un blog]. Recuperado de http://erawat.es/es/guia-omi-ciber-riesgo

Giudici, D. E. (2013). *Lineamientos para la seguridad cibernética en Teatro de Operaciones.* Recuperado de http://190.12.101.91:80/jspui/handle/123456789/176

Martín, P. E. (2015). Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos. *Instituto Español de Estudios Estratégicos, 8.* Recuperado de http://www.ieee.es/

Organización Marítima Internacional – OMI. (2017). *Directrices sobre la gestión de los riesgos cibernéticos marítimos.* Recuperado de http://www.imo.org/es/ourwork/security/guide_to_maritime_security/paginas/cyber-security.aspx

Parada, D. J., Flórez, A., y Gómez, U. E. (2018). Análisis de los componentes de la seguridad desde una perspectiva sistémica de la dinámica de sistemas. *Información Tecnológica, 29*(1), 27-38. doc: http://dx.doi.org/10.4067/S0718-07642018000100027

Santos-Olmo, L. A., Fernández-Medina, E., y Piattini, M. (2012). *Revisión sistemática de metodologías y modelos para el análisis y gestión de riesgos asociativos y jerárquicos para PYMES.* Recuperado de https://www.researchgate.net

Wegener, H. (2013). Los riesgos económicos de la ciberguerra. *Cuadernos de Estrategia, 162, 177-227.* Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4276097

"REDES SOCIALES Y GESTIÓN DE CRISIS, EN ENTORNOS DE CIBERSEGURIDAD Y CIBERDEFENSA"

Social Networks and crisis management, in Cybersecurity and Cyberdefense environments

Recibido: 12 / 09 / 2019 Aprobado: 31 / 10 / 2019

Licenciada
Ceinett Sánchez Quintero
República Dominicana

La autora es Periodista y Máster Gestión Seguridad, Crisis y Emergencias, por el Instituto Global de Altos Estudios (IGLOBAL) Instituto Ortega y Gasset, en Madrid, España (2014). Licda. Comunicación Social Mención "Periodismo, Universidad Bicentenaria de Aragua, Edo. Aragua, Venezuela, 1.997-2.002. Gerencia de la Seguridad, William J. Perry Centro de Estudios Hemisférico de Defensa, Washington Agosto 2014. Conferencista de diversas instituciones. Directora Revista Guarnición del Ejército de República Dominicana. Asesora en Comunicaciones Estratégicas del Ministerio de Defensa (J5), la Escuela de Graduados de Altos Estudios Estratégicos (Docente en talleres de comunicación estratégica y encargada de Redes Sociales). Autora de los libros "Comunicación, Emergencias y Desastres" y "#SoyPreventivo: Redes sociales, seguridad y emergencias"; también dirige revistas especializadas en Defensa y Seguridad. Coordinadora académica de capacitaciones en "Comunicación Estratégica para la Defensa y Seguridad nacional". Fue reportera y editora de CDN Canal 37 y desde el año 2010 imparte conferencias locales e internacionales sobre comunicación en emergencias y desastres. Ponente en diversos talleres, seminarios y Congresos. ceinett@yahoo.com

RESUMEN

Estudiar las dinámicas de cómo se teje la opinión pública y se gestionan las crisis mediáticas desde las redes sociales, en entornos de ciberseguridad y ciberdefensa en República Dominicana, resulta fascinante y despierta la curiosidad, sobre todo en estos tiempos donde el poder fáctico de estos medios de comunicación digital, marcan pautas y viralizan en cuestión de segundos, informaciones sensibles y de alto interés para las sociedades, en momentos determinados.

Palabras clave:
Comunicación estratégica, redes sociales, opinión pública, ciberseguridad, ciberdefensa.

ABSTRACT

Studying the dynamics of how public opinion is weaved and media crises are managed from social networks, in cybersecurity and cyberdefense environments in the Dominican Republic, is fascinating and arouses curiosity, especially in these times where the factual power of these digital media, set guidelines and viralize in a matter of seconds, sensitive information and high interest to societies, at certain times.

Keywords:
Strategic communication, social networks, public opinion, cybersecurity, cyberdefense.

INTRODUCCIÓN

Es evidente que en los últimos años, las Fuerzas Armadas dominicanas así como las instituciones que velan por la seguridad del Estado dominicano, han cambiado radicalmente la manera que comunican su gestión pública y gestionan las crisis, en especial desde las redes sociales y sobre todo, desde los entornos donde ahora se libran las guerras mediáticas en los ciberespacios. Pensar y actuar para garantizar la ciberseguridad y ciberdefensa, ha obligado tomar mucho más en cuenta la planificación estratégica y hasta la estética de los contenidos informativos, al momento de colarlos y exponerlos frente a la opinión pública.

Con esto, no sólo demuestran sus muy meritorias capacidades militares y el desarrollo que sobreviene de la interpretación de la intención del mando político, sino que además, exponen frente al escrutinio y corren las cortinas de sus instituciones castrenses y de seguridad, para sumergirse y salir a flote magistralmente por ejemplo, ante las turbulencias y amenazas de los fakenews (o falsas noticias), abrirse y atreverse al diálogo constante a través de las redes sociales y mostrarse como entes flexibles, transparentes pero sin dejar de actuar acorde a lo que establecen las leyes, cuando así lo amerita la ocasión.

Por tanto, la comunicación estratégica digital, ha sido considerada en tiempos recientes como una herramienta de planificación e integración de las capacidades de información que en el caso de las Fuerzas Armadas dominicanas y de sus instituciones, contribuye significativamente en el alcance de sus objetivos militares, acorde con las políticas públicas de defensa y seguridad establecidas en el país que incluyen por supuesto con el Decreto Presidencial número 230-18, de la Estrategia Nacional de Ciberseguridad de República Dominicana, el cual hace alusión al Programa República Digital, creado mediante Decreto número 258-16 del 16 de septiembre de 2016, y concebido como el conjunto de políticas y acciones que promueven la inclusión de las tecnologías de información y comunicación en los procesos educativos, gubernamentales y servicios ciudadanos.

LAS REDES SOCIALES Y LA GESTIÓN POR CRISIS MEDIATICAS

Tal y como se ha introducido el presente artículo, el Decreto Presidencial número 230-18, de la Estrategia Nacional de Ciberseguridad de República Dominicana, marca la pauta de los entornos virtuales no sólo para Fuerzas Armadas dominicanas, sino también para las demás instituciones públicas del Estado dominicano. Este hace alusión al Programa República Digital, creado mediante Decreto número 258-16 del 16 de septiembre de 2016, y concebido como el conjunto de políticas y acciones que promueven la inclusión de las tecnologías de información y comunicación en los procesos educativos, gubernamentales y los servicios ciudadanos.

Adicionalmente, el marco legal nacional que direcciona las acciones de las fuerzas castrenses y los cuerpos especializados de seguridad en el país, tales como la Constitución dominicana vigente, la Ley 1-12 Estrategia Nacional de Desarrollo 2030 y la misión de las FF.AA, aluden a la defensa de la integridad territorial, la soberanía, el mantenimiento de la paz y el orden público, en aras de crear un clima de máxima seguridad.

Al revisar los seis objetivos estratégicos de FF.AA., en apoyo a los objetivos nacionales que deben alcanzarse antes del 2030, se determina el interés por lograr: 1) Unas FF.AA., que garanticen la Seguridad y Defensa Nacional; 2) Que promuevan el bienestar de sus miembros con igualdad de derechos; 3) Que contribuyan con su accionar al desarrollo nacional; 4) Que garanticen la protección de la población, medio ambiente, recursos naturales y promuevan con eficiencia la gestión del riesgo y la adaptación al cambio climático; 5) Que protejan eficientemente las infraestructuras vitales y las instituciones públicas nacionales, y 6) Que promuevan el bienestar de sus miembros a través del mejoramiento de la educación, capacitación, entrenamiento, desarrollo integral, profesional, deporte y cultural.

Así que, en la práctica es evidente entre las instituciones del Estado dominicano lideradas por la Presidencia de República Dominicana, -entre las cuales se encuentran las fuerzas castrenses-, que existe una marcada tendencia a dinamizar y a modernizar las estrategias comunicacionales cuidando la imagen, reputación, percepción y conocimiento público de sus iniciativas, para construir no sólo una opinión pública favorable, sino que esta pueda

acompañarse de sanas e interactivas relaciones con las audiencias dentro del marco legal establecido.

Esto ha llevado de alguna manera, a la inclusión progresiva de jóvenes civiles y militares, que con sus talentos aportan a las Direcciones de Asuntos Cívico-Militares y de Relaciones Públicas (como se conocen dentro de la guardia), capaces de elaborar, narrativas y contenidos en formatos atractivos, modernos y de fuerte carga audiovisual, que son difundidos con inmediatez y alta frecuencia en las redes sociales y sus portales.

La inclusión de estos equipos multidisciplinarios, felizmente ha permitido que al margen de las publicaciones institucionales referidas a sus actividades rutinarias y cotidianas, también en situaciones de crisis, las decisiones sobre qué, cómo y cuándo reaccionar ante lo inesperado, facilite la entrega sin tantas burocracias de contenidos oportunos, dinámicos y con un lenguaje digital sencillo, digerible y amigable (o "friendly" como les llaman los "milleniums"), sin apartarse de la formalidad y el respeto a lo que establecen las leyes en temas tan delicados como la defensa y la seguridad nacional.

Comunicar y reaccionar a tiempo, ante eventos que se viralizan en las redes sociales, facilitan las aclaratorias y la defensa de la institucionalidad, antes de que se armen incendios ante la opinión pública, se trata de decisiones que evidencian un buen manejo de la comunicación estratégica.

Es así como dentro del amplio campo de investigación de la "Comunicación Estratégica", un término ante el cual aún no existe una definición consensuada dentro de la comunidad científica, existe el interés por demostrar que su empleo como herramienta de planificación e integración de las capacidades de información de las Fuerzas Armadas dominicanas, contribuye significativamente en el alcance de sus objetivos militares, acorde con las políticas públicas de defensa y seguridad de República Dominicana.

Hoy en día, es necesario entender que los escenarios donde se están librando las "batallas mediáticas", son sumamente complejos, cambiantes y volátiles. Se debe tener en cuenta los hábitos de conducta de los individuos, sus formas de comunicarse entre ellos, cambian constantemente así como muta el uso de las herramientas tecnológicas y de información en un espacio virtual hiperconectado.

No basta con establecer un escalón de propaganda al máximo nivel con la introducción de narrativas que emerjan desde las autoridades al inicio de las actividades de las instituciones estatales que representan incluyendo a las FF.AA., porque ahora hay que vincularlas rápidamente con la difusión de contenidos atractivos, multimedia, que sean breves, bien pensados, con una alta dosis de persuasión, para lograr que en el mejor de las casos, los mismos ciudadanos y medios de comunicación decidan contribuir de forma instintiva y los distribuyan en tiempo real como relatos propios.

El uso de videos e historias en Instagram, conmueven y hacen llegar mensajes de una manera más atractiva y directa, con lo cual se logra un mejor y mayor acercamiento con los públicos, en especial de la clase civil.

Expuesto esto, cabe preguntar primero si existen estructuras formales de direcciones o departamentos de "Comunicación Estratégica" y si no existen, evaluar cómo se está planificando la creación y difusión de informaciones desde el máximo nivel de las organizaciones militares; verificar si están utilizando los códigos de los potenciales difusores para dirigir los mensajes a un público, de manera que se mantengan en el tiempo mensajes potentes, integrados con las acciones en el plano militar y que al mismo tiempo, puedan ir mitigando por ejemplo, opiniones desfavorables en contra de los esfuerzos que se realizan para combatir las principales amenazas a la seguridad nacional como las migraciones ilegales, el narcotráfico, el contrabando y los daños al medio ambiente.

En este caso, habría que revisar si la concepción tradicional de direcciones de prensa y relaciones públicas, están evolucionando en su estructura operativa y evaluación de desempeño de sus integrantes, para garantizar el manejo de la información para la gestión de crisis dentro de las Fuerzas Armadas y con cuáles criterios se hace.

En el caso de los Departamentos Socialmedia dentro de las instituciones militares, dedicadas exclusivamente a la creación de contenidos creativos y mutlimedia, sería interesante indagar hasta qué punto han logrado el acercamiento entre las instituciones militares y los públicos, creando una sinergia de crecimiento y desarrollo o contribuyendo cuando hay que apagar incendios de opinión pública.

También sería interesante determinar, el alcance de los mensajes que se generen desde estas estructuras dedicadas a la comunicación de las instituciones castrenses, están actuando en favor del trabajo de prevención de la población frente a emergencias causadas por la dinámica propia de la naturaleza (terremotos, huracanes, inundaciones, etc.) o de origen antropogénico (incendios provocados, explosiones, derrames químicos).

Estas interrogantes se plantean así, ya que es una realidad que las redes sociales y la conexión permanente de los usuarios al internet, son los elementos que más han modificado los parámetros de la comunicación en los últimos tiempos. Como el modo en que recibimos la información ha cambiado radicalmente, la introducción del receptor como posible emisor de la misma información que la fuerza castrense genera, sería oportuno también averiguar hasta qué punto desde la opinión pública "los fans" o "seguidores", se encargan de generar matrices de opinión pública favorables a los intereses de las FF.AA., en medio de campañas mediáticas organizadas o a través de iniciativas como concursos periodísticos y la realización de programas de formación dirigida a comunicadores sociales o "influencers".

Una vez realizadas todas estas pesquisas sustentadas en teorías de la comunicación, la opinión pública, estudios similares previos y utilizadas las técnicas de investigación más oportunas, será posible proponer nuevas formas que puedan justificar la importancia de la comunicación estratégica como ancla vital de planificación y herramienta integradora de capacidades en el máximo nivel de unas Fuerzas Armadas que ciertamente por lo que ordena la Constitución y su Ley Orgánica no deliberan, pero que sin dudas, sí saben comunicar y que hoy día más que nunca, tienen todas las herramientas disponibles a su favor y cada vez que lo requieran.

El pasado 12 de septiembre del 2019, un "fakenews" se convirtió en tendencia en las redes sociales y gracias a un desmentido oportuno y consensuado entre las instituciones castrenses involucradas, fue posible que el descrédito no se apoderara de la buena imagen y reputación de las FF.AA., así como del trabajo que realizan.

COMUNICACIÓN ACERTADA: PIEDRA ANGULAR EN LA GESTIÓN DE CRISIS

Sin dudas, se encuentra en un sitial de importancia en la escala de valores de cada individuo por razones de supervivencia, desde que existe sobre la faz de la tierra. Así como la comunicación y la inteligencia van unidas, como van unidas al pensamiento, hoy día como elemento fundamental de desarrollo humano, social y obviamente en el plano político, militar, diplomático y empresarial, cada vez adquiere mayor importancia como vehículo imprescindible de posicionamiento, reputación, influencia, venta y transmisión de valores.

Ahora bien, el término estrategia procede del griego stratégós, que significa "General de un Ejército", de modo que el empleo del concepto "comunicación estratégica" en sí mismo, aunque no cuenta con un significado consensuado y es objeto de múltiples interpretaciones, obedece sin dudas al espíritu de pensamiento previo, planificación y elaboración de herramientas óptimas para librar y ganar batallas en las llamadas "guerras mediáticas". Así que no dista en lo absoluto de la naturaleza y la razón que justifica la creación y existencia de las propias Fuerzas Armadas.

Múltiples teorías e investigaciones en el campo de la "Comunicación Estratégica" (CE) avalan su facultad integradora por encima incluso de su capacidad de coordinación, y en el ámbito militar cobra mucha más importancia porque en terrenos de operaciones, abarca la búsqueda de influencia sobre la población local o sobre el enemigo que realiza acciones como operaciones sicológicas, cooperaciones y acciones cívico-militares, servicios de inteligencia, etc.

Tomando en cuenta algunas referencias, podría considerarse que la CE es el proceso mediante el cual, se trazan las líneas sobre las cuales debe transcurrir la comunicación del día a día acorde con la filosofía de la empresa u organización; debe nacer del máximo nivel y desde el comienzo de la toma de decisiones de una organización para ser parte del proceso que consiga alcanzar los objetivos marcados por la autoridad.

Al mismo tiempo, ha de ejercer una función integradora y de coordinación de los diferentes elementos que intervienen en la comunicación y de las herramientas a través de las cuales se llevarán a cabo, con especial interés en las redes sociales; debiendo ser capaz de afrontar los nuevos retos, especialmente la medición del impacto real de su ejercicio y su posicionamiento definitivo en las organizaciones como elemento de capital importancia y acorde al interés del mando.

El uso de infografías y elementos gráficos atractivos, permiten a través de las redes sociales, presentar informaciones formales por medio de un lenguaje más digerible, lo cual se ha convertido en una tendencia de la comunicación estratégica en el mundo.

De acuerdo a algunos expertos, el nivel donde se ubica la unidad responsable de la comunicación es de suma importancia. Donde tiene que tener acceso directo al nivel de decisión, tomando parte del mismo y con posibilidad real mediante el asesoramiento al Comandante General o al mando militar de lugar, de condicionar su proceso. Por tanto, es necesario que antes de la acción, haya un planeamiento de comunicación, un paso previo que convierta la acción en una comunicación en sí misma y la comunicación esté presente antes, durante y después para intentar evitar la distorsión del mensaje, donde el emisor en origen quiere trasladar al receptor y no se pierda en el camino.

Es así como los responsables de gestionar las comunicaciones institucionales, deben de coordinar e integrar como responsabilidad principal, la facilitación de las interacciones entre las fuerzas militares y los actores que generan opinión pública, asegurando la coherencia con la estrategia previamente marcada, en el escalón superior y su integración en el planeamiento y conducción de las operaciones.

La comunicación debe estar implicada en el más alto nivel, en la fase de decisión de cara no solo a responder fielmente a su carácter de estratégica, en sintonía con las líneas marcadas desde el nivel político o empresarial más alto, sino también de cara a prevenir

crisis posteriores. Por tanto, aquí cobra mayor fuerza el "más vale prevenir que lamentar" y donde la planificación previa, evita muchas veces tener que hacer una comunicación reactiva.

Durante el año 2019, el Ejército de República Dominicana organizó un Concurso de Periodismo donde participaron más de 80 periodistas, que cursaron en FF.AA., a través del INSUDE y la EGAEE, talleres de Comunicación Estratégica enfocada en temas de defensa y seguridad fronteriza, lo que permitió un acercamiento con las instituciones castrenses dominicanas y con ello, un cambio en la opinión pública sobre estos temas.

Al revisar un sin número de publicaciones referidas al tema, se logra determinar que el término de CE nace con la Organización de los Países del Atlántico Norte (OTAN) y que por razones de seguridad y algunas políticas de gobierno que se detallarán más adelante, fue el Departamento de Estado de los Estados Unidos que decidió colocarlo en desuso. Sin embargo, en el tiempo ha quedado demostrado que lo que no se cuenta no existe y que siendo la comunicación una necesidad de primer orden también para las organizaciones militares, su aplicación y buen manejo es necesario para evitar incluso desastres militares o de tipo político que puedan ser irreparables.

En el caso de República Dominicana, la ya referida Ley 1-12 Estrategia Nacional de Desarrollo 2030 como doctrina del Estado dominicano en el largo plazo, en su cuarto eje estratégico contempla: "la intención de alcanzar para sus habitantes los resultados de una eficaz gestión de riesgos y minimizar pérdidas humanas, económicas y ambientales a partir de la activa participación de las comunidades y gobiernos locales, la reducción al máximo posible de los daños y la posibilidad de recuperación rápida y sostenible de las áreas o poblaciones afectadas".

Esta visión estratégica necesariamente hay que asociarla con la realidad que hay en la región del Caribe durante cada temporada ciclónica; las coordinaciones logísticas y operativas en momentos críticos, requieren de la información inmediata para salvar vidas y salvaguardar bienes materiales. Es por eso que los mensajes de anticipación y soluciones, se convierten en una gran ayuda, especialmente donde las catástrofes tienen un carácter cíclico y pueden preverse por medios científicos y de comunicación digitales.

Cuando la situación de crisis es inminente o ya se ha desencadenado por la evolución de huracanes o cualquier otro evento, las estrategias de seguridad de los estados se sustentan en mensajes de alerta y pre alerta, así como de las recomendaciones que los acompaña. Esto es, para que la información llegue a los ciudadanos y se reduzcan lo máximo posible los riesgos ante el probable impacto de los acontecimientos y se maneje oportunamente la percepción de seguridad ante la opinión pública.

En este mismo orden, la llamada Teoría de "Los seis grados de separación" de Stanley Miller" (1953), a través de la cual explica en términos sencillos el cómo operan las redes sociales para conectar a conocidos y desconocidos en el planeta, se sustenta en la hipótesis que intenta probar que "cualquiera en la tierra puede estar conectado a cualquier otra persona del planeta a través de una cadena de conocidos que no tiene más de cinco intermediarios (conectando a ambas personas con sólo seis enlaces)".

El concepto está basado en la idea de que "el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera". Esta teoría también está contenida en el libro "Six Degrees: The Science of a Connected Age" del sociólogo Duncan Watts (2003) y que asegura que "es posible acceder a cualquier persona del planeta en tan sólo seis "saltos", a través de una suerte de efecto contagioso que se activa cuando somos conscientes del poder de las redes y se entiende cómo podemos influir en el otro".

Ahora bien, en el caso de la Teoría de la Complejidad y Organizaciones, también llamada Estrategia de la Complejidad u Organización Compleja Adaptativa, es el uso de la teoría de la complejidad en el campo de la gestión estratégica y los estudios organizacionales. Las áreas de aplicación incluyen la comprensión

de cómo las organizaciones o empresas se adaptan a su entorno y cómo hacen frente a situaciones de incertidumbre. La estructura es compleja, debido a que son redes dinámicas de interacciones, y sus relaciones no son resultado de la agregación de las entidades estáticas individuales. Son adaptativos, porque los comportamientos individuales y colectivos mutan y se auto organizan en respuesta a los cambios iniciales de los micro eventos o el conjunto total de eventos.

Así que tomando en cuenta que la Comunicación Estratégica puede ser la ventana por la que instituciones, ejércitos y gobiernos se muestran al mundo y que podría definirse como el empleo planificado e integrado de todas las capacidades y medios de comunicación que tiene a su disposición el emisor en apoyo de sus objetivos estratégicos, sean estos políticos, diplomáticos, económicos o militares y en la búsqueda de una mejora de imagen, reputación, percepción o conocimiento por parte del receptor, la suscrita propone entre otras cosas:

1. La formalización dentro de FF.AA., de estructuras orgánicas de Comunicación Estratégica, que les permita a los encargados de departamentos de relaciones públicas dirigidas por oficiales militares y equipos multidisciplinarios, planificar, ejecutar y evaluar sus tácticas de prensa, relaciones públicas, comunicaciones digitales y gestionar crisis ante la opinión pública.

2. Sacar un mayor provecho a sus recursos informativos y medios de comunicación institucionales, planificando sus contenidos de manera estratégica y constituyendo equipos con roles bien definidos para las áreas de prensa, relaciones públicas, socialmedia y gestión de crisis.

3. Prestar una mayor importancia al monitoreo y a la evaluación de los niveles de alcance, influencia y exposición de los mensajes, así como al desarrollo constante de capacitaciones a periodistas y profesionales de la comunicación en distintas áreas, en temas de defensa y seguridad, también en ciberdefensa y ciberseguridad, de manera que faciliten la multiplicación de los esfuerzos que desde FF.AA., se realizan.

CONCLUSIÓN

Demostrar que el empleo de la Comunicación Estratégica como herramienta de planificación e integración de las capacidades de información de las Fuerzas Armadas dominicanas, contribuye significativamente en el alcance de sus objetivos militares, acorde con las políticas públicas de Defensa y Seguridad de República Dominicana, sigue siendo un reto para el cual se está trabajando.

En el tiempo, se han venido dando de manera paulatina, algunos pasos para estructurar y dar formalidad a la conformación de equipos que se dedican en la práctica, exclusivamente a las Comunicaciones Estratégicas dentro de Fuerzas Armadas dominicanas, con ciertas capacidades de planificar y elaborar contenidos que les permiten mostrarse ante la opinión pública, ante las situaciones más adversas.

El uso continuo de recursos informativos y medios de comunicación institucionales de manera planificada, para la consecución de los objetivos estratégicos institucionales de las Fuerzas Armadas dominicanas, les ha permitido un sitial de importancia frente a la percepción de la sociedad dominicana sobre el gran trabajo que desarrollan sus autoridades y los miembros que las conforman, no obstante, sería interesante determinar si FFAA, está midiendo el alcance de sus campañas educativas y de sus estrategias comunicacionales, de tal modo que les permita reinventar sus tácticas informativas.

Sería interesante del mismo modo, seguir promoviendo programas de formación dirigidos a profesionales de la comunicación e influencers de manera continua, a través de sus academias y escuelas de graduados, fuerzas castrenses, policial y cuerpos especializados de seguridad, con el norte de desarrollar habilidades y obtener resultados tangibles en favor de la imagen organizacional ante la opinión pública y del alcance de sus objetivos estratégicos y militares.

REFERENCIAS

Constitución de la República Dominicana (2015). Santo Domingo: Asamblea Nacional de República Dominicana.

De la Torre, H. (1996). Comunicaciones eficaces. [Libro en línea]. Conceptos y herramientas de managment. *(Cuadernos No. 7).* Recuperado de www.mercadeo.com.ar [2019, mayo 15].

Decreto No. 230-18. (2018). *Estrategia Nacional de Ciberseguridad la República Dominicana. Gaceta Oficial.* Santo Domingo, República Dominicana, 19 de junio del 2018, núm. 10912.

Decreto No. 361-01. (2001). Creación Comisión Nacional de Emergencias. *Gaceta Oficial.* Santo Domingo, República Dominicana. 14 de marzo del 2001, núm. 10076.

Fowler J. y Espert, R. (2013). El poder de las redes sociales. Entrevista a James Fowler Universidad de California [en línea]. Recuperado de http://www.dailymotion.com/video/xhyz4y_el-poder-de-las-redes-sociales-james-fowler_school.

Ley No. 139-13. (2013). Ley Orgánica de las Fuerzas Armadas de República Dominicana. *Gaceta Oficial.* Santo Domingo, República Dominicana, 13 de septiembre del 2013, núm. 10728.

Ley No. 147-02. (2002). Ley sobre gestión de riesgos y su reglamento de aplicación. *Gaceta Oficial.* Santo Domingo, República Dominicana. 22 de septiembre del 2002, núm. 10172. 45-69.

Mc Luhan, M. (1989). *La aldea global.* Barcelona: Editorial Gedisa.

Nicolás, M. y Grandío, M. (2012). *Estrategias de comunicación en redes sociales: Usuarios, aplicaciones y contenidos.* España: Gedisa.

Pacheco, J. (2011). *La facultad predictiva del lenguaje: De la comunicación celular a la comunicación digital.* Colombia: Editorial Uniautónoma.

Pintado, R. (2013). *Las redes sociales y la defensa. Un análisis DAFO. Instituto Español de Estudios Estratégicos.* [en línea]. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO119-2013_redesSociales_CesarPintado.pdf

Sánchez, C. (2012). *Comunicación, emergencias y desastres: Periodismo ciudadano digital.* Santo Domingo, República Dominicana: Ediciones UNICARIBE.

Sánchez, C. (2013). *Proyecto para la creación de una coordinación social media que articule las estrategias de comunicación digital preventivas.* Santo Domingo, República Dominicana. Comisión Nacional de Emergencias/Defensa Civil Dominicana.

Sánchez, C. (2014). *#SoyPreventivo: Redes sociales, seguridad y emergencias.* Santo Domingo, República Dominicana: Ediciones UNICARIBE.

Watts, D. (2004). *Six Degrees: The science of a connected age.* Estados Unidos: W.W Norton

"TECNOLOGÍAS DIGITALES Y LOS RIESGOS DE LA CIBERNÉTICA EN LA SEGURIDAD NACIONAL"

Digital Technologies and the Risks of Cybernetics in National Security

Recibido: 06 / 08 / 2019 Aprobado: 31 / 10 / 2019

Coronel
Ángel Gómez de Ágreda
España

El autor es Coronel del Ejército del Aire, Diplomado de Estado Mayor, Máster en Terrorismo y Anti-terrorismo por la Universidad de la Rioja, y Doctorando en Ingeniería en la Universidad Politécnica de Madrid. Ha sido profesor del Departamento de Estrategia y Relaciones Internacionales en el CESEDEN, y jefe de la Sección de Cooperación del Estado Mayor del Mando Conjunto de Ciberdefensa. Actualmente es el jefe del Área de Análisis Geopolítico de la División de Coordinación y Estudios de Seguridad y Defensa de la Secretaría General de Política de Defensa (SEGENPOL). Es piloto militar de transporte, paracaidista y diplomado en Seguridad de Vuelo por el Ejército del Aire, la US Air Force y por la Universidad del Sur de California. Ha participado en cuatro misiones internacionales en la antigua Yugoslavia, Afganistán y el Sahel. Ha publicado un centenar de artículos y participaciones en libros. Es autor de "Mundo Orwell. Manual de supervivencia para un mundo hiperconectado" agomde@ea.mde.es

RESUMEN

Internet, esa herramienta que empleamos a diario para las más diversas actividades, es también un ecosistema en el que convivimos y en el que nos relacionamos. Fruto de esa actividad social y política, la guerra está también presente en el ciberespacio. El mundo digital trae consigo modos más eficientes de gestionar los conflictos y cambia sus características al alterar el escenario en el que tienen lugar. Sin embargo, más allá de las nuevas formas de amenaza que surgen de las redes, la principal alteración que se está produciendo es la desintermediación entre los productos y los consumidores. Esto supone un desafío al modelo de gobernanza en su conjunto y no solo a la estabilidad de gobiernos concretos.

Palabras clave:
Seguridad, libertad, desintermediación, narrativa, desinformación, influencia, afectos, guerra en la gente.

ABSTRACT

Internet, the tool we used daily for the most diverse tasks, is also an ecosystem in which we live and in which we relate to one another. As a result of that social and political activity, warfare is also present in cyberspace. The digital world brings along more efficient ways to manage conflict and changes their characteristics by altering the scenario in which they take place. Nonetheless, beyond these new threats emanating from the networks, the main alteration taking place is the disintermediation between products and consumers. This poses a challenge to the governance model as a whole and not only to the stability of specific governments.

Keywords:
Security, safety, freedom, disintermediation, narrative, disinformation, influence, affection, war within the people.

INTRODUCCIÓN

Lo digital se visualiza desde dos ópticas opuestas. Por un lado, como herramienta cotidiana, aparece como algo ubicuo en nuestras vidas y en nuestro trabajo. Por otro, como tecnología, se percibe como algo sobre lo que no tenemos control directo, algo casi sobrenatural ante cuyo poder no cabe más que plegarse. Por lo tanto, terminamos por asumir como natural llevar un celular en nuestro bolso o nuestro bolsillo sabiendo que, de alguna manera, controla todos nuestros movimientos y palabras.

Porque, hace apenas unos pocos años podíamos todavía argumentar que los riesgos de la cibernética eran asuntos de ciencia ficción o de conspiraciones más o menos increíbles. Ya no es el caso, han salido a la luz suficientes ejemplos de cómo las redes sociales o las tecnologías digitales en general comercian y juegan con nuestros datos como para que no nos quede ninguna duda al respecto.

Sin embargo, pese a saber que nuestra seguridad está en entredicho si no limitamos el acceso de estos aparatos a nuestras vidas, pese a saber que nuestra libertad para elegir está siendo condicionada por el conocimiento casi total que se acumula en las bases de datos sobre cada aspecto de nuestras vidas, pese a todo eso, seguimos aferrados a celulares y servicios digitales como un náufrago a una tabla de salvación.

En el viejo debate entre la libertad y la seguridad, en el contrato social que proponía Rousseau, hemos elegido perder ambas a cambio de la comodidad, la inmediatez y la aparente gratuidad de unos servicios que no sabíamos que requeríamos hasta hace apenas unos meses. Hemos regalado nuestros datos sin ser conscientes de que son nosotros, de que en el mundo digital, son la materia de la que estamos hechos igual que la carne y los huesos nos dan forma en el mundo físico.

Y hemos abrazado estas tecnologías particularmente nocivas desde la consciencia de que son, en muy buena parte, fruto de un estudio sociológico que nos genera una dependencia similar a la de las drogas, el tabaco o el alcohol. Al igual que el paquete de cigarrillos es lo primero que prepara el fumador, nuestro teléfono de bolsillo es lo último que querríamos dejarnos olvidado al salir de casa.

En su novela "1984", George Orwell describía cómo el Estado colocaba una cámara en cada estancia de las casas de los ciudadanos para tener absoluto control sobre sus actividades. En 2019, todos y cada uno de nosotros lleva no ya una, sino dos cámaras de alta resolución permanentemente sobre él y se asegura de que no le falte la batería en ningún momento.

INTERNET, HERRAMIENTA PARA GESTIONAR NUEVAS AMENAZAS

El ciberespacio, ese entorno en el que convivimos compartiendo información a través de equipos informáticos, y la inteligencia artificial se han convertido, como dice Andrew Ng, en la electricidad del siglo XXI. Siguen existiendo "cosas" que no son "smart", que no están conectadas, pero son reliquias de un siglo XX que nos parece a todos ya muy lejano.

Porque la clave es precisamente, que internet, que el ciberespacio, no es solo una herramienta que utilizamos en nuestras vidas. Muy lejos de eso, se trata sobre todo de un entorno en el cual estamos desarrollando nuestra actividad. Vivimos a través de nuestros avatares, en las redes informáticas. Pero nuestros avatares, nuestro correo electrónico, nuestro usuario de cualquier plataforma, no dejan de ser también nosotros. Hemos volcado nuestras vidas en ellos y hemos aprendido a creernos la realidad que se nos presenta a su través.

La realidad, la verdad, se han convertido en una abstracción, en algo imposible de aprehender. Vivimos en un mundo global con implicaciones planetarias. ¿Cómo vamos a poder abarcar todos los múltiples aspectos que presenta?, ¿cómo vamos a estar al día de las últimas evoluciones que se producen, o de las últimas noticias?

Afortunadamente, tenemos una ventana que nos acerca instantáneamente a la realidad de cualquier tema en cualquier parte del mundo. Una ventana abierta de forma instantánea a la situación en tiempo real, a lo más reciente que haya ocurrido. Somos dueños absolutos del tiempo y del espacio con solo teclear tres "w" o señalar con el dedo o con el ratón un enlace en una pantalla.

El problema, sin embargo, es que la realidad que se nos presenta a través de la pantalla está separada de la que existe verdaderamente en muchos grados de magnitud. Es una realidad construida en función de lo que esa misma ventana deja ver de nosotros mismos. Percibimos una realidad hecha a nuestra medida, customizada, tuneada para que sigamos enganchados a ella. Y esa percepción es nuestro mundo hasta el punto de que, si la realidad física desafía el relato que nos llega a través de la pantalla, dudamos antes de nuestros ojos que del criterio de Google.

Esa realidad percibida juega con lo más preciado que nos queda. Regalados nuestros datos, solo nos queda nuestro tiempo y nuestra atención. La economía de la atención busca esclavizar nuestra voluntad a una determinada plataforma o a un medio concreto para que se convierta en referencia y para que su capacidad de influencia sobre nosotros pueda monetizarse por parte de media docena de grandes corporaciones.

Más allá de las "fake news", las mismas noticias que los medios nos hacen llegar cada día tienen una carga ideológica y, sobre todo, sentimental, que se adapta a nuestros prejuicios. Si nos gusta un color, todo se volverá de distintos tonos del mismo.

Grandísima y potentísima herramienta esa que permite a la más marginal de las personas encontrar un alma gemela mucho más allá del limitado alcance de su aldea o de su país. Por muy excéntrica o absurda que sea una idea, seguro que habrá alguien entre 4.000 millones de internautas que la comparta. Sobre todo, porque no tendrá que venir asociada a ningún otro relato. Será una idea aislada. No tendrá que aceptar ni amar a la persona completa, sino solo a una de sus ideas. Para las otras, ya encontraremos a otros candidatos a compartirlas. Ya no existe la marginación porque hemos ampliado el alcance de nuestra comunidad al mundo completo.

Pero tampoco existe la limitación. Ya no tenemos tampoco que negociar con nuestros vecinos, con nuestra pandilla, con el grupo social en el que vivimos ningún aspecto de nuestras vidas. ¿Quién necesita sujetarse a la disciplina de un grupo cuando puede individualizar sus emociones, sus sentimientos y sus creencias? Eso, claro, genera egoísmo, individualismo, radicalización y un sinfín de efectos perversos. Pero, por otro lado, alimenta aquella parte de nosotros que siempre está dispuesta a aceptar una taza más: el ego.

Y volvemos así a las cámaras de los celulares, a las que sirven para hacer fotos de nosotros mismos. Vámonos de viaje a los confines del universo a obtener un primer plano de nuestra cara contra el fondo de tal o cual monumento o atracción. Dejada constancia social de la importancia de nuestro ego, pasemos al siguiente estadio.

Hablábamos de que la ventana nos daba acceso a todo el mundo y también de que lo hacía en tiempo real. Y ahí es donde entra en juego el segundo pecado capital de nuestra vida digital. La adicción a lo último se vuelve obscena. Repasamos una y mil veces los titulares de las noticias recogidas en Twitter sin leer ni una sola de ellas más allá de los 280 caracteres que preceden al enlace.

De hecho, la prensa se convierte en un mero diseñador de titulares que resulten lo suficientemente atractivos para que las redes sociales los recojan y generen tráfico en la página web. El contenido completo de la noticia es más o menos irrelevante porque los "clicks" nacen de los titulares. Al final, es un círculo vicioso en el que nadie lee noticias vacías que no se rellenan porque solo se leen los titulares. Los medios son incapaces de romper la dinámica dando información más allá del encabezado, el público se contenta con una cita de consumo rápido siempre que ésta cambie cada vez que revisa su Tablet o su celular, y el Estado se ve incapacitado para regular este mercadeo con la atención de sus ciudadanos.

Es fácil argumentar que siempre ha habido medios de comunicación que eran capaces de influir en las percepciones del público. Y no faltará razón al hacerlo. En los Estados Unidos de finales del siglo XIX, de hecho, había dos grandes medios dominantes: el de Pulitzer y el de Hearst. Este último, "el ciudadano Kane", demostró su capacidad de manipulación propiciando una guerra contra España que terminó con la presencia española en Cuba.

Sin embargo, por muy sesgado que pudiera ser un medio, por muy limitada que pudiera ser la oferta informativa, existía un discurso. Lo ideal sería que hubiera suficientes medios y que estos fueran independientes de los poderes políticos y económicos. Nuestro problema actual no es la cantidad de medios de hecho, cualquier se convierte hoy en una fuente de "información" y de "noticias" a través de las redes sociales. Nuestro problema es con la independencia y con la calidad de esa información.

Esa misma inmediatez que exigimos, unida a la necesidad constante de novedades, degrada la consistencia de la información que

procesamos. Nada es realmente relevante porque mañana habrá sido sustituido por otro asunto. Además, la sospecha permanente sobre la independencia y solvencia de la información nos hace poner toda ella en cuarentena. De este modo, hemos pasado de tener un par de discursos interesados que generaban un relato coherente para sus lectores a tener una miríada de medios que alimentan una cadena de producción en serie de noticias inconexas que no terminan de encajarse entre ellas para formar un relato. Hemos llegado a un mundo sin narrativas, sin verdades y sin interés porque las haya.

Hasta aquí no hemos hablado siquiera de seguridad nacional, de ejércitos, de defensa, ni siquiera de tecnología como tal. No obstante, hemos llegado a un punto en el que lo que se está cuestionando no es la continuidad de un gobierno, de un dirigente o de una idea, sino la misma esencia del poder tal y cómo lo concebimos, los sistemas de gobierno según los conocemos.

La democracia no se concibe sin capacidad para elegir y la libertad se basa en el acceso a la verdad. A algún tipo de verdad -no nos vamos a poner filosóficos en este punto-. El Estado moderno, desde la Paz de Wesphalia en 1648, se basa en el monopolio que los estados ejercen sobre el uso de la fuerza, sobre su capacidad para proporcionar seguridad -y ejercer coacción- sobre sus habitantes. Todo eso salta por los aires cuando lo hacen las fronteras del ciberespacio y cuando las grandes corporaciones compiten por garantizar privacidad o libertad con los mismos gobiernos.

Todo esto ya ha sucedido antes. Las compañías de Indias holandesa o británica eran tan grandes o mayores que la mayor parte de los países de la época en cuanto a su poder económico e, incluso, militar. Y, a pesar de todo, no dejaban de ser empresas nacionales como lo eran Oil Standard o la Bell Company. Grandes monopolios nacionales sujetos a la regulación del Estado en el que tenían su sede y ejercían su actividad. No es un caso similar a los oligopolios mundiales de la era digital.

Es casi imposible hablar de soberanía en la actualidad sin incluir en el concepto la capacidad para actuar en el mundo de la información y en el ámbito digital. Retener el control de las fronteras físicas se antoja del todo insuficiente cuando los recursos y los activos se mueven en el ciberespacio y en el entorno de lo cognitivo. La acción del Estado tiene que ser capaz de ejercer su autoridad también en esos ámbitos para ser realmente eficaz.

No obstante, una de las características que define al ciberespacio es su naturaleza artificial. Ha sido diseñado, construido y mantenido por el hombre. Concretamente, en su inmensa mayoría, por empresas privadas con ánimo de lucro. Es decir, no podemos hablar, como hacen muchos, de un Global Common en sentido estricto porque toda infraestructura está sujeta, no solo a la jurisdicción de un Estado, sino también a la propiedad de una empresa o particular.

Este carácter artificial supone, por lo tanto, una propiedad sobre las características que tiene la arquitectura y la composición de los sistemas digitales. No existe una terra nullius, un territorio sin dueño sobre el que se pueda ejercer soberanía, sino que estamos empleando medios particulares sobre los cuáles construimos nuestra vida digital. Muchas veces, esta infraestructura convertida en un ecosistema mantiene una agenda propia y genera beneficios en paralelo a los servicios que proporciona.

¿Quién hubiera podido intuir siquiera que una parte casi mayoritaria de la población mundial iba a "habitar" parcialmente en un universo diseñado por una compañía? Y, sin embargo, Google es ese ecosistema en el cual estamos interactuando. Es el equivalente a una estación espacial o a una estación en Marte que hubiera sido diseñada por una empresa y en la cual estableciéramos nuestra residencia. Sujetos todavía a algunas restricciones legales derivadas de la residencia fiscal de la empresa, en todo lo demás estaríamos sujetos a las leyes "físicas" imperantes en la estación según su diseño.

Hemos visto que esas condiciones, los términos de uso de las plataformas, pueden incluir cláusulas tan abusivas como aquella por la que se cedía nuestra "alma inmortal" al prestatario de un servicio al acceder al mismo. El requisito no dejaba de ser una mezcla de broma y de demostración de que nadie presta atención a estos documentos deliberadamente engorrosos, cambiantes y oscuros.

Una segunda consecuencia de la naturaleza artificial del ciberespacio es su intrínseca falibilidad. Como toda creación humana, internet no deja de ser algo imperfecto, pero también es un diseño que siempre tenderá a optimizar el beneficio de su diseñador frente a la seguridad de sus operadores. Internet siempre tuvo como prioridad la usabilidad, incluso cuando John Perry Barlow lanzaba

la Declaración de Independencia del Ciberespacio[1], en el fondo una súplica para que los poderes estatales se mantuvieran al margen de un mundo idealizado en el que todos realizarían aportaciones puramente positivas.

La internet es vulnerable igual como son los vehículos que conducimos o las viviendas en las que habitamos. No por eso dejamos de hacer uso de cualquiera de las tres cosas. La única diferencia entre ellas es de alcance. Mientras que las vulnerabilidades de los vehículos o las casas pueden afectar a un usuario o a un número muy limitado de ellos, internet es el habitáculo y el vehículo de miles de millones de personas -y de cosas- que transitan por ella muchas veces sin la menor consciencia de su fragilidad. ¡Es tan fácil sentirse seguro detrás de una pantalla!

Se puede afirmar que la toma de conciencia de los Estados respecto de esa vulnerabilidad llegó en 2007 con el ataque de denegación de servicio distribuido (DDoS, por sus siglas en inglés) que sufrió Estonia. Este pequeño país báltico llevaba siendo independiente poco más de tres lustros. Se había escindido de la Unión Soviética, pero mantenía una importante población rusa entre sus habitantes. A falta de una posibilidad más atractiva, centró su modelo de desarrollo económico en la generación de una industria digital y en el aprovechamiento de las posibilidades que ofrecía un todavía incipiente ciberespacio.

El ataque consistió en la saturación de la capacidad de respuesta de las páginas web del dominio estonio (.ee) durante más de dos semanas. Se lanzaron visitas a los servicios de hospitales, transportes, bancos y demás hasta que sus páginas dejaron de responder. Un país que había fiado todo a lo digital quedó, repentinamente, paralizado. Es fácil imaginar los efectos que una agresión similar -o una mera caída del servicio de internet- podría suponer hoy, doce años después.

El ataque procedía, en último extremo, de Rusia. Parece lógico pensar que se trató de una agresión institucional organizada desde el Kremlin, pero a día de hoy, sigue sin poder probarse. Todo lo que le podríamos achacar a Rusia es que no atendiese a su deber de diligencia debida de desactivar el ataque una vez que se estaba produciendo. Incluso, de haber tomado todas las medidas posibles para evitar que se produjese. Sin embargo, en 2007, pocos países se sentían moralmente autorizados a exigir a otro que tuviese en marcha mecanismos para la lucha contra este tipo de actividades.

España no publicó su primera Estrategia de Ciberseguridad Nacional hasta seis años más tarde, fue de los primeros países en hacerlo. El mundo no era consciente de la dependencia que tenía de la tecnología digital. Hoy, cuando esa dependencia es mucho mayor, esa consciencia apenas se ha incrementado mínimamente.

Estonia aprendió la lección y promovió la creación del Centro de Excelencia para la Cooperación en Ciberseguridad de la OTAN (CCD-CoE)[2], que se situó a pocos metros del lugar al que fue trasladada la estatua del soldado soviético que dio lugar al ataque. También estableció embajadas digitales para situar fuera de su territorio copias de todos los datos críticos de su administración. La idea subyacente era desconcentrar la información para hacer más difícil su acceso a un posible agresor.

La solución, que puede ser viable en el caso de Estonia y sus 1,3 millones de habitantes, supone retos difíciles de abarcar para países más grandes. Y tampoco termina de solucionar el problema de la independencia o la soberanía nacional, sino que lo difiere a aliados con los que, en un momento dado, existe buena sintonía y afinidad.

No asegurar los activos digitales de un país equivale a no hacerlo con las fronteras físicas o con la vida de sus ciudadanos en el mundo físico. No hay alternativa para un Estado funcionante a la asunción de sus responsabilidades en el ciberespacio. Las limitaciones serán muchas en el caso de que no existan desarrollos y plataformas propias, en cuanto no existan redes autóctonas, y siempre que los dispositivos que se utilicen procedan de terceros países, pero no puede dejar de poner todos los medios al alcance de las autoridades nacionales para retener el control sobre los mismos.

Dos son los principales ámbitos en los que se tienen que centrar los esfuerzos de cualquier administración: la protección de sus infraestructuras y servicios críticos, y el aseguramiento de los datos de y generados por sus ciudadanos. Mientras que el primer aspec-

[1]El texto de la declaración puede leerse completo en https://www.eff.org/cyberspace-independence

[2]https://ccdcoe.org/

to debería contribuir a la supervivencia de la nación, el segundo permite la de sus ciudadanos y establece las bases para el desarrollo económico y el bienestar de los mismos. Sin una adecuada defensa del conocimiento como tal no existe posibilidad de progreso social ni económico.

Queda, en fin, hablar de la utilización del ciberespacio en provecho propio. La protección de las redes es un primer paso necesario para poder emplearlas, pero no es suficiente.

Decíamos que internet había nacido y se había desarrollado con la usabilidad como bandera. En nuestro afán por mantener las redes seguras no podemos descuidar la verdadera razón de su existencia. Siendo, como recordábamos más arriba, una creación humana no tendría sentido mantenerla si no proporcionase unas ventajas superiores a los costes de su implantación y mantenimiento.

Es evidente que las tecnologías digitales han cambiado el mundo. Lo han hecho profundamente con los medios de comunicación, están siendo disruptivos en la banca y las finanzas, y podrían -como hemos visto- hacer otro tanto con los Estados y las formas tradicionales de gobernanza. Pero, más allá de esas utilidades en cuanto a la desintermediación entre la noticia y el público, entre el dinero y el cliente, o entre el gobernante y el gobernado, internet nos ofrece posibilidades directas de uso en el mundo de la seguridad y la defensa. Y mucho más sin entramos en el ámbito de la inteligencia artificial que, por ahora, dejaremos en simple mención.

La conectividad, inmediatez y capacidad de procesamiento de información cambian el campo de batalla, concebido desde el punto de vista de las operaciones militares como de las policiales. De hecho, una de las primeras distinciones que elimina el ciberespacio es la que existía entre la seguridad interior y la internacional.

No merece la pena entrar en los detalles de qué significa en la práctica el hecho de que podamos mantener una conexión de datos con cualquier miembro de nuestro equipo esté donde esté en el teatro de operaciones. También parece superfluo deletrear las ventajas que introduce en el planeamiento de las operaciones, en las labores logísticas, en la recopilación y tratamiento de la información y su transformación en inteligencia.

En muchas de estas facetas, internet simplemente proporciona una vía optimizada para llevar a cabo aquello que ya se venía haciendo en el mundo analógico. Un ideal olímpico aplicado a lo físico, podemos hacer lo mismo, pero más alto, más lejos y más fuerte. Sin embargo, siendo importante la contribución que hace en estos campos, no es lo fundamental.

Lo realmente disruptivo, allá donde se encuentra el valor añadido del ciberespacio, son aquellas tareas que configuran un nuevo paradigma de seguridad y de defensa. Igual que digitalizar una empresa no significa hacer en formato MSWord o .pdf lo que antes hacíamos a bolígrafo o con dos copias de calco en la máquina de escribir, tampoco digitalizar el campo de batalla consiste en cambiar el mapa enrollable desplegado en la pared o sobre la mesa por un videowall interactivo. Es el fondo de la guerra lo que cambia, no sólo la forma.

Por eso, lo importante del ciberespacio es que su alcance, interactividad e inmediatez nos permiten -y permiten al adversario- llevar la guerra a la gente. Las grandes explanadas donde se congregaban infantes y jinetes para la batalla dejaron paso a una guerra mucho más cercana. Los terroristas y los guerrilleros trajeron la guerra entre la gente; a nuestras casas, a nuestras calles. El ciberespacio se cuela dentro de nosotros y nos convierte, a cada uno -combatiente o no-, en campo de batalla, en arma y en objetivo al mismo tiempo.

Las redes neuronales del ciberespacio se confunden con las de nuestras mentes para llevar hasta ellas las percepciones de la realidad, para alterar nuestra voluntad apelando a nuestros sentimientos y para vencer -como aconsejaba Sun-Tzu- cada batalla sin llegar a combatir.[3]

Son operaciones que no pretenden destruir físicamente más que en la medida en que esa destrucción envíe un mensaje. No son operaciones basadas en los efectos cinéticos, operativos o logísticos, sino en los afectos y en los sentimientos como precursores de las voluntades.

Esa es la verdadera naturaleza disruptiva del ciberespacio y de las tecnologías digitales, su capacidad para hacer la guerra en la gente. De forma sutil, siguiendo doctrinas antiguas como "la muerte

[3]El libro de Sun-Tzu puede consultarse en https://suntzusaid.com/

por los mil cortes" en la que ninguna agresión es letal ni justifica una respuesta, pero todas debilitan y merman nuestra capacidad de respuesta. Siguiendo doctrinas modernas como la "guerra sin restricciones", en la que todo contribuye al objetivo final, en la que no hay periodos de paz ni de guerra, sino un conflicto permanente de constante cooperación y competición.

CONCLUSIÓN

La consideración del ciberespacio como entorno en el que desarrollamos nuestra actividad trae consigo implicaciones importantes. Al cambiar el escenario, cambia necesariamente la obra representada, nuestra vida entera se ve afectada por las características del medio. Sus características claves son la ubicuidad, la interactividad y la inmediatez, y las tres tienen implicaciones importantes en sus vertientes positiva y negativa.

Si bien la posibilidad de comunicarse con cualquier punto del planeta y con cualquier persona ofrece unas enormes posibilidades que muchas veces no somos conscientes de utilizar a diario, también es cierto que esa falta de limitación respecto de dónde encontrar apoyo a nuestros puntos de vista reduce la autocrítica y la capacidad de crecimiento. Si la interactividad es mucho más poderosa a la hora de comunicar ideas, también lo es cuando se trata de manipular mentes. Si la inmediatez permite una mayor eficiencia en los negocios o en las transacciones, también termina por incrementar la obsolescencia de las noticias hasta convertirlas en carentes de contenido.

La promesa de comodidad y conveniencia que traen consigo los servicios digitales adormecen el afán de lucha y superación tanto del humano como individuo como de la especie como conjunto. Esto genera sociedades de valores poco profundos y nada proclives, por lo tanto a su defensa. Las desigualdades se incrementan y las castas se estratifican, muchas veces en función del acceso dispar a la tecnología y de la comprensión de sus implicaciones.

La guerra, como fenómeno sociológico y político, se vuelve igualmente ubicua e instantánea. Vivimos en un permanente estado de competición, gestionando conflictos en una "zona gris" que se mueve bajo el umbral que generaría una respuesta por parte del adversario. La guerra en este nuevo ámbito se traslada al interior de la gente, a los sentimientos. Son operaciones basadas en afectos en las que no se juega tanto con la realidad como con las percepciones y los relatos. En las que no es necesario alterar lo físico porque se puede presentar distorsionado al público objetivo. Una suerte de realidad aumentada narrada en la que somos capaces de superponer conceptos e interpretaciones sobre una capa de medias verdades.

Es cierto que la seguridad nacional requiere de una defensa de la capa tecnológica, de seguridad de las redes. No obstante, la ciberseguridad, la seguridad del ciberespacio tiene que abordar también a los humanos que viven dentro de él y avanzar hasta la explotación de las posibilidades que se presentan en el mismo como una forma más de preservarnos. En un mundo en el que puedes correr, pero no esconderte, será preciso estar en los puestos de cabeza para siquiera conocer los riesgos antes de que se materialicen.

Todo ello va a suponer la necesidad de formar una y otra vez a un nutrido grupo de profesionales, y de concienciar y formar al resto de la población, que queda subsumida en la guerra como escenario, arma y víctima de la misma.

REFERENCIAS

Allen, T. S., & Moore, A. J. (2018). Victory without casualties: Russia's information operations. *Parameters, 48*(1), 59–71.

Botsman, R. (2015). The changing rules of trust in the digital age. *Harvard Business Review Digital Articles, 2–4*. Recuperado de http://search.ebscohost.com/login.aspx?direct=true%7B&%7Ddb=bth%7B&%7DAN=118685348%7B&%7Dsite=ehost-live

Del-Fresno-García, M. (2019). Desórdenes informativos: sobreexpuestos e infrainformados en la era de la posverdad. *El Profesional de La Información, 28*(3), 1–11. Recuperado de https://doi.org/10.3145/epi.2019.may.02

Fischer-Lescano, A. (2016). Struggles for a global internet constitution: protecting global communication structures against surveillance measures. *Global Constitutionalism*, 5(02), 145–172. https://doi.org/10.1017/S204538171600006X

Gómez de Ágreda, Á. (2014). El ciberespacio como escenario del conflicto. Identificación de las amenazas. En Centro de Estudios de la Defensa Nacional. El ciberespacio: Nuevo escenario de confronta- ción. Madrid, España: Ministerio de Defensa. pp. 863–868.

Gómez de Ágreda, Á. (2016). De Irak a Irak. Evolución del pensamiento militar contemporáneo. *Tiempo Devorado,* (3), 2–6.

Gómez de Ágreda, Á. (2018a). Falsas noticias, no noticias falsas | Telos Fundación Teléfonica. *TELOS*, 109. Recuperado de https://telos.fundaciontelefonica.com/telos-109-asuntos-de-comunicacion-falsas-noticias-no-noticias-falsas/

Gómez de Ágreda, Á. (2018b). Vencer convenciendo o, si es preciso, combatiendo. *TELOS*, 109. Recuperado de https://telos.fundaciontelefonica.com/una-nueva-doctrina-para-la-guerra-del-siglo-xxi-vencer-convenciendo-o-si-es-preciso-combatiendo/

Gómez de Ágreda, Á. (2019a). La guerra en la gente. *IEEE*., 14, 1–14.

Gómez de Ágreda, Á. (2019b). Mundo Orwell. *Manual de supervivencia para un mundo hiperconectado* (1st ed.). Barcelona: Ariel.

Gómez de Ágreda, Á., & Robles Carrillo, M. (2016). Tecnología y derecho: El FBI contra Apple. En *JNIC*.

Lewis, J. A. (2018). *Cognitive effect and state conflict in cyberspace.* (September). Recuperado de https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace

Liang, Q., y Xiangsui, W. (1999). Unrestricted Warfare. *Unrestricted Warfare*. (February), 1–228.

Ng, A. (2017). *Artificial intelligence is the new electricity.* Medium. Recuperado de https://medium.com/syncedreview/artificial-intelligence-is-the-new-electricity-andrew-ng-cc132ea6264

Prier, J. (2017). Commanding the Trend : Social Media as Information Warfare, 51–86.

Reino de España. (2013). *Estrategia de ciberseguridad nacional 2013,* 55.

Rugge, F. (2018). Mind hacking: information warfare in the cyber age. *ISPI, 20*(319), 1–8.

Sociología y redes sociales. (2010). *La economía de la atención.* Recuperado de http://sociologiayredessociales.com/2010/03/economia-de-la-atencion/

Voiklis, J., Kim, B., Cusimano, C., & Malle, B. F. (2016). Moral judgments of human vs. robot agents. IEEE pp. 775-780. doi:org/10.1109/ROMAN.2016.7745207

"CIBERSEGURIDAD: HACIA UNA RESPUESTA Y DISUASIÓN EFECTIVA"

CYBERSECURITY: TOWARDS AN EFFECTIVE RESPONSE AND DETERRENCE

RECIBIDO: 10 / 04 / 2019 APROBADO: 31 / 10 / 2019

Coronel
Javier Candau
España

El autor es Coronel de Artillería. Ingeniero Industrial con especialidad en electrónica y automática. Actualmente se desempeña como Jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional y responsable de la Capacidad de Respuesta ante Incidentes gubernamental (CCN-CERT). Es Especialista criptólogo. Dispone de diversas certificaciones de especialización en seguridad de las TIC (ISS, SANS, CRAMM, Curso de Auditoría del INAP, Cursos CCN-STIC, etc.). Los principales cometidos de su actividad son la formación del personal especialista en seguridad de la Administración, el desarrollo de normativa del CCN (elaboración de políticas, directrices y guías de seguridad de las TIC para la Administración Pública - Series CCN-STIC), desarrollo de la herramienta de análisis de riesgos PILAR, la supervisión de acreditación de sistemas y la realización de auditorías de seguridad. Tiene más de 18 años de experiencia en todas estas actividades.

RESUMEN

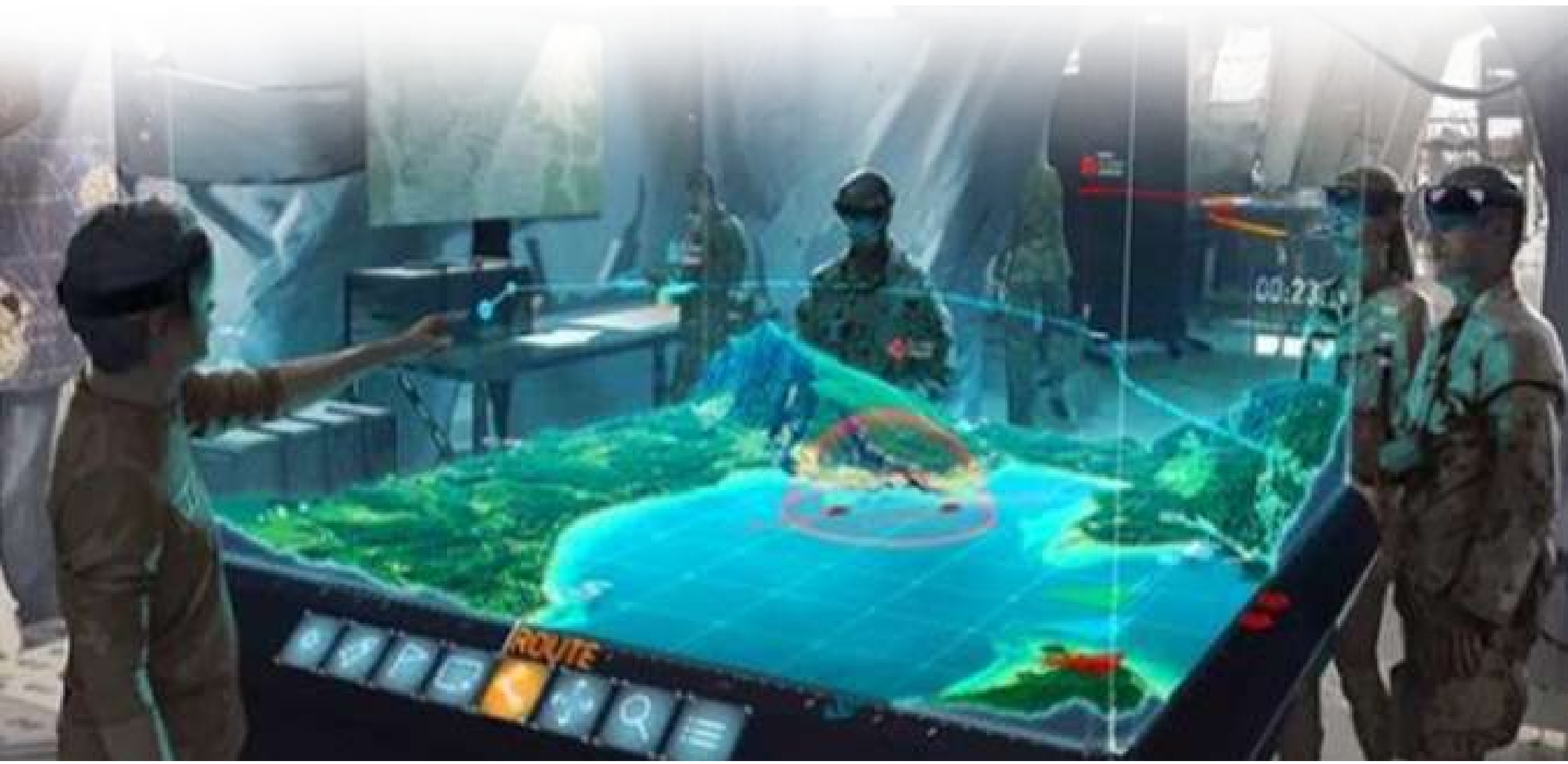
Garantizar e implementar la seguridad en el ciberespacio es un reto extraordinario que exige mejorar las capacidades de detección, monitorización y vigilancia, y conocer las vulnerabilidades y las amenazas a las que se enfrenta la tecnología, con el fin de ofrecer una respuesta oportuna a los nuevos desafíos. La adaptación a este escenario tiene una meta clara: convertir a las organizaciones en objetivos cada vez más difíciles de atacar.

Palabras clave:
Ciberseguridad, ciberamenaza, prevención, detección, respuesta, ciberespacio.

ABSTRACT

Ensuring and implementing cyberspace security is an extraordinary challenge that requires improving detection, monitoring and surveillance capabilities, and knowing the vulnerabilities and threats that technology faces, to offer a timely response to the new challenges. Adapting to this scenario has a clear goal: to turn organizations into increasingly difficult targets to attack.

Keywords:
Cybersecurity, cyberthreat, monitoring, cyberspace, surveillance, response, cyberspace,.



INTRODUCCIÓN

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el Art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

EL RETO DE LA SEGURIDAD EN EL CIBERESPACIO

El avance de las Tecnologías de la Información y la Comunicación (TIC) presenta un nuevo paradigma. La expansión de internet, con más de 4.000 millones de usuarios en todo el mundo, ha impulsado una profunda transformación de las estructuras mundiales. Los servicios públicos, la educación, el ocio, el transporte, la cultura o las relaciones personales han experimentado un proceso de cambio absoluto, debido a la influencia que la tecnología ejerce sobre la sociedad. Tanto es así que existe incluso una nueva realidad: el ciberespacio.

Este entorno global plantea un escenario de oportunidades económicas y sociales de gran alcance. Sin embargo, también conlleva una serie de riesgos, que se incrementan día a día. Las amenazas del ciberespacio, favorecidas por la rentabilidad económica o política, el bajo coste de las herramientas empleadas y la posibilidad de actuar desde cualquier lugar del mundo de manera anónima, se dirigen y afectan transversalmente a los sectores públicos y privado, así como a los ciudadanos.

En este contexto, los ciberdelincuentes, los hacktivistas o los propios Estados, son capaces de explotar las vulnerabilidades tecnológicas con el objetivo de recabar información, sustraer activos de gran valor y amenazar servicios básicos para el normal funcionamiento de un país. Asimismo, la utilización de las técnicas de aprendizaje automático (machine learning) o el uso de modelos de inteligencia artificial (IA) son cada vez más frecuentes y sofisticados, evidenciando un creciente potencial para amplificar los riesgos existentes o crear nuevos riesgos; especialmente cuando Internet de las Cosas (IoT) es capaz de conectar cientos de millones de dispositivos.

Así pues, garantizar e implementar seguridad en el ciberespacio, al tiempo que se respeta la privacidad y la libertad, se ha convertido en una de las prioridades estratégicas de los países más desarrollados, debido a su impacto directo en la seguridad nacional, en la competitividad de las empresas y en la prosperidad de la sociedad en su conjunto. El mundo ciber exige un compromiso constante ante la evolución tecnológica y la creciente sofisticación de los ataques.

La adaptación a este escenario pone de manifiesto la necesidad de implementar seguridad, a través de la mejora de las capacidades de prevención, detección y respuesta ante las posibles amenazas.

PREVENCIÓN: NECESIDAD DE IMPLEMENTAR CIBERSEGURIDAD

La ciberseguridad, con el paso de los años se ha introducido entre las prioridades de un gran número de gobiernos, considerada ahora un asunto de seguridad nacional y eje fundamental de la sociedad y de sus sistemas económicos.

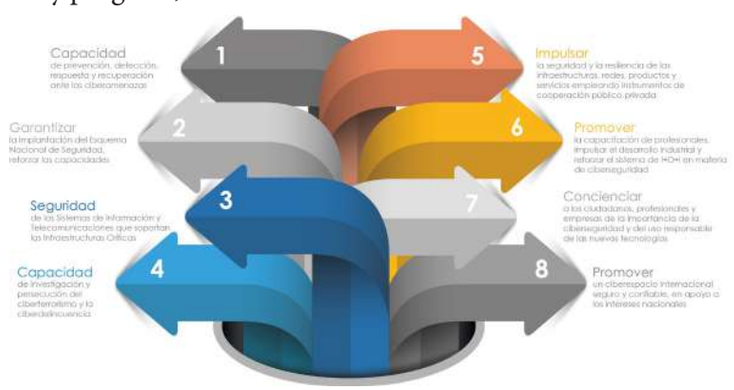
El desarrollo de un marco regulatorio y reglamentario posibilita, el establecimiento de una normativa y legislación en materia de ciberseguridad son el pilar fundamental de la prevención, pues actúan como catalizadores del sector y favorecen la creación, el crecimiento y el fortalecimiento de la actividad.

Todo eso ha justificado la necesidad de disponer de estrategias de ciberseguridad nacionales que permiten enmarcar los objetivos y las medidas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información de los Estados.

En Estados Unidos, en el 2009 el Departamento de Defensa creó el US Cyber Command (CYBERCOM) para controlar las capacidades de ciberdefensa y ciberguerra del Ejército y, en el 2011 publicó su Estrategia. En Europa, la Agencia Europa de Ciberseguridad (ENISA) elaboró una Guía de Buenas Prácticas en Estrategias Nacionales de Ciberseguridad.

Del mismo modo, la Organización de Estados Americanos (OEA) desarrolló varios programas para promover la Estrategia Iberoamericana con el objetivo de combatir las Amenazas de la Seguridad Cibernética, y en el 2011 Colombia presentó su Estrategia de Ciberseguridad y Ciberdefensa del Estado Colombiano.

Así pues, en España también se hizo evidente la necesidad de desarrollar un sistema nacional de ciberseguridad que fomentara la integración de todos los actores e instrumentos públicos y privados, con el fin de preservar el ciberespacio de todo tipo de riesgos y ataques, por tanto, defender los intereses nacionales y contribuir al desarrollo de la Sociedad Digital. Un modelo de ciberseguridad integrado que dirigido por el gobierno, garantizara al país su seguridad y progreso, a través de la adecuada coordinación de todas las



Administraciones Públicas entre sí, con el sector privado y con los ciudadanos; y que canalizase las iniciativas y esfuerzos internacionales en defensa del ciberespacio.

De este modo, y después de varios años de intenso trabajo a través de diferentes grupos y organismos, en diciembre de 2013 se publicó en España la Estrategia de Ciberseguridad Nacional (actualizada en 2017).

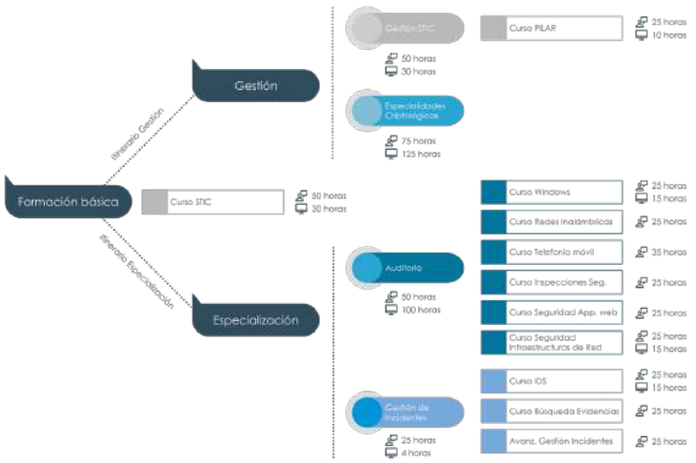
El cuerpo de leyes, decretos, órdenes ministeriales y reglamentos por los que se gobierna en materia de ciberseguridad debe ser ágil y aprovechar las situaciones existentes para conseguir un ciberespacio más seguro y confiable.

En el caso de España, existe el Código de Derecho de la Ciberseguridad, publicado en el Boletín Oficial del Estado, que cita las principales normas a tener en cuenta con relación a la protección del ciberespacio y para velar por la mencionada ciberseguridad. Del mismo modo, la Ley 11/2002 del 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, del 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en el sector público. Su mandato esencial es que todo el sector disponga de una política que garantice el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de datos e informaciones, sentando las bases necesarias para promover la confianza de los ciudadanos en la utilización de los medios electrónicos.

Asimismo, para implementar ciberseguridad de una manera más clara y como medida de fortalecimiento de las capacidades de prevención, es necesario analizar los procedimientos y medidas de seguridad aplicadas a los sistemas de información de organismos, entidades y organizaciones. Para ello, resulta conveniente realizar auditorías de seguridad, que tienen como fin la obtención de evidencias y su evaluación de modo que se pueda determinar el grado de conformidad con la política de seguridad del sistema de información auditado y las necesidades de mejora y corrección de este. Para desarrollar estas acciones preventivas es imprescindible fomentar y desarrollar perfiles profesionales cualificados, así como concienciar y sensibilizar a los ciudadanos de los riesgos derivados de este nuevo paradigma. La prevención de los riesgos solo es

posible si la sociedad es consciente de las consecuencias derivadas de un incidente de seguridad.

Ante esta necesidad, el Centro Criptológico Nacional ha desarrollado un Plan de Formación adaptado a las tendencias en la gestión de incidentes y a la evolución de la superficie de exposición ante las posibles deficiencias de los requerimientos establecidos por la política de Seguridad de los Sistemas. Este nuevo escenario ha quedado reflejado en un diseño curricular, que da respuesta a las necesidades planteadas por su comunidad de referencia.



DETECCIÓN, LA CLAVE DE LA ACCIÓN PREVENTIVA

Para garantizar un nivel de seguridad adecuado en los sistemas, es necesario actuar antes de que produzca un incidente o, por lo menos, reducir su impacto y alcance una vez se ha detectado.

Por este motivo, desde el año 2008 el CCN-CERT ha desarrollado un Sistema de Alerta Temprana (SAT) para la detección rápida de incidentes y anomalías, que permite realizar acciones preventivas, correctivas y de contención. Su principal función, por lo tanto, es la detección temprana de un incidente para que puedan aplicarse las medidas necesarias de eliminación de la amenaza y poder evitar que el intento de ataque sea fructífero o, en su caso, minimizar el posible impacto.

Este sistema cuenta con tres (3) vertientes: SAT-SARA, monitorización de la Intranet de la Administración; SAT-INET, monitorización de las salidas de internet de los organismos adscritos al servicio; y SAT-ICS, para la detección en tiempo real de las amenazas e incidentes existentes en las redes de control y supervisión industrial del organismo adscrito.

A través de este servicio, el organismo adscrito tiene capacidad de detectar multitud de tipo de ataques, evitar su expansión, responder de forma rápida ante el incidente detectado y generar normas de actuación que eviten futuros incidentes. Al mismo tiempo y gracias al almacenamiento de un número progresivo de eventos, es posible contar con una panorámica completa y veraz de la situación de los sistemas, que posibilita una acción preventiva frente a las amenazas que sobre ellas se ciernen.

El Sistema de Alerta Temprana permite automatizar y reducir los tiempos de respuesta ante ataques e incidentes de todo tipo, incluida la detección avanzada interdominio, es decir, la detección temprana de un incidente replicado en otros dominios monitorizados. En este sentido, la integración de las capacidades de Security Information and Event Management (SIEM), notificación de incidentes y ciberinteligencia se hacen especialmente necesarias para la mejora de las técnicas de correlación compleja de eventos y gestión de incidentes.

HACIA UNA RESPUESTA Y DISUASIÓN EFECTIVA

En 1988, y ante lo que se consideró el primer gran ataque de la historia conocido como el gusano Morris, el Departamento de Defensa de Estados Unidos encargó a la Universidad Carnegie Mellon, en Pittsburg, la creación de un equipo capaz de hacer frente a este nuevo tipo de amenazas. El resultado fue la constitución del denominado Computer Emergency Response Team (CERT).

Bajos estas mismas siglas comenzaron a formarse otros grupos en distintas universidades norteamericanas, encargados de estudiar la seguridad de las redes y ordenadores para proporcionar servicios de respuesta ante incidentes víctimas de ataques, publicar alertas relativas a amenazas y vulnerabilidades y ofrecer información que ayudara a mejorar la seguridad de estos sistemas.

Teniendo en cuenta el continuo incremento de las amenazas y vulnerabilidades sobre los sistemas de información de todo el mundo, en el año 2004 se afianzó lo que sería el CERT Gubernamental Na-

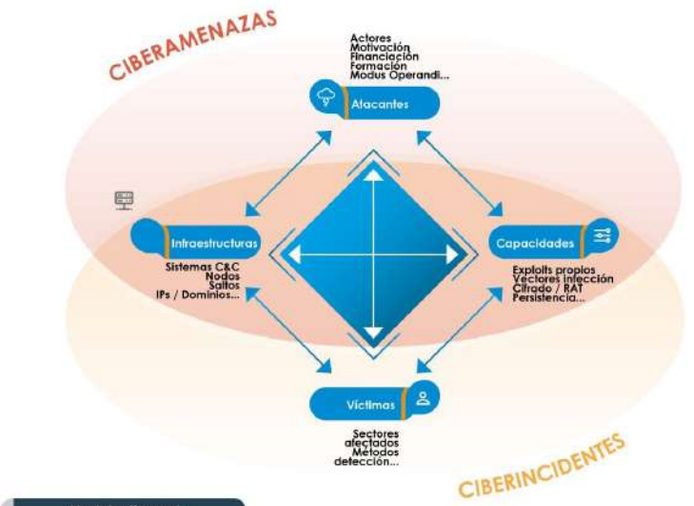
cional español. Así, y tras dos años de intenso trabajo, se presentó la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, (CCN-CERT), organismo cuya misión es contribuir a la mejora del nivel de seguridad de los sistemas de información de las Administraciones Públicas españolas y que coopera y ayuda al sector público a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir, para afrontar de forma activa las nuevas amenazas.

Estas amenazas han demostrado ser globales y su resolución solo puede llevarse a cabo mediante una respuesta conjunta, que debe implicar un mayor grado de coordinación y cooperación. Por un lado, a nivel nacional, entre los niveles de la Administración del Estado y las empresas privadas; y por otro, a nivel internacional, con otros países y organizaciones multilaterales.

Cualquier mecanismo utilizado para la gobernanza será verdaderamente eficaz si todos los participantes disponen de información fidedigna que les permita actuar. Esta capacidad de actuación es especialmente relevante en el caso de los gobiernos, a los que compete garantizar la seguridad y el bienestar de los ciudadanos.

En el ámbito nacional resulta imprescindible disponer de un modelo basado en el intercambio de información entre organismos públicos y privados, proveniente tanto del análisis de ciberamenazas como de ciberincidentes, con el objetivo de mejorar y agilizar la detección y actuación frente a los ataques.

Este intercambio siempre es más efectivo a través de la confianza entre las partes que por imposición normativa. Dicha confianza permitirá que todos los agentes implicados consideren beneficioso invertir su tiempo en foros y sistemas de intercambio y, asimismo, que se produzca una actuación recíproca en la que la información aportada esté a la par que la obtenida para optimizar sus defensas. Para que este modelo funcione, las aportaciones respecto a ciberamenazas y ciberincidentes deben estar compensadas, pues es necesaria tanto la información del atacante, relativo a sus capacidades e infraestructuras, como la de la víctima, en relación con el procedimiento de ataque, el impacto sufrido y las técnicas de detección y resolución. De este modo, se podrán cubrir todos los vértices del modelo de diamante y conocer las técnicas, tácticas y procedimientos (TTP) del atacante.



Modelo diamante

La industria de la ciberseguridad nacional debe actuar como catalizador de esta compartición de información de valor, con especial énfasis en el factor humano y a la formación de un equipo de analistas e investigadores, que aporten conocimiento y sean capaces de interpretar la información.

En esta tarea, el CCN-CERT ofrece dos de sus soluciones más destacadas: LUCÍA y REYES. La primera de ellas, para la notificación de incidentes y contextualización de la amenaza; la segunda, para el conocimiento y parametrización de la amenaza, permitiendo la elaboración de ciberinteligencia.

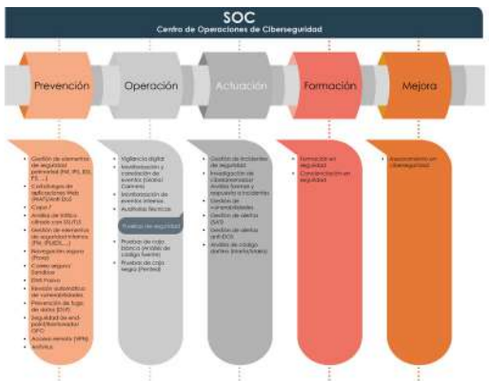
Junto a la cooperación nacional, resulta fundamental que cualquier equipo de respuesta a incidentes mantenga contacto en caso de ataque, con otros equipos del resto del mundo y asegure así las fuentes de información fiables. De ahí, la importancia de participar en los distintos foros internacionales existentes.

Del mismo modo, el constante aumento de los ciberataques, unido a las posibles consecuencias que para un país tendría que un incidente de seguridad afectase a sus sistemas, conlleva la necesidad de incrementar y mejorar las capacidades de prevención, monitorización, vigilancia y respuesta.

Todo ello es posible a través de los Centros de Operaciones de Ciberseguridad (SOC), cuya finalidad es la prestación de servicios

horizontales de ciberseguridad que permiten aumentar la capacidad de vigilancia y detección en la operación diaria de los sistemas de información y comunicación, así como mejorar su capacidad de respuesta ante cualquier ataque.

Su objetivo final es aumentar las capacidades existentes de vigilancia y detección de amenazas en la operación diaria, así como su capacidad de respuesta ante cualquier ataque, siendo prioritarios la monitorización y evaluación de manera continua de las medidas de seguridad, la actuación de manera proactiva ampliando las capacidades de vigilancia y reacción ante incidentes, y la parametrización de la amenaza mediante inteligencia de ciberseguridad, que permita integrar la información, para lo que resulta imprescindible mejorar la notificación de incidentes e incrementar el intercambio sobre la amenaza.



De esta manera, la evaluación continua constituye uno de los objetivos principales que persigue un Centro de Operaciones de Ciberseguridad, al permitir a lo largo del tiempo el seguimiento del grado de exposición a potenciales atacantes.

Asimismo, la cibervigilancia juega un papel primordial al comprender las acciones destinadas a vigilar el ciberespacio. Por tanto, la misión de un sistema de cibervigilancia es emitir informes y alertas sobre amenazas, de forma que la inteligencia obtenida pueda ser empleada para desplegar capacidades de respuesta en pro de desactivar, contener, mitigar o anular la posible acción dañina.

CONCLUSIÓN

El tiempo que media entre la primera acción hostil hasta el compromiso de un activo se mide, frecuentemente, en términos de segundos o minutos. Sin embargo, el plazo para su descubrimiento o detección, que depende en gran medida del tipo de ataque, suele expresarse en días, semanas o meses.

Estos datos reflejan la necesidad de continuar invirtiendo recursos materiales y, sobre todo humanos, para mejorar la protección del ciberespacio ante la imparable evolución de las tecnologías y la creciente sofisticación de los ataques. De igual modo, es necesario incrementar y mejorar las capacidades de inteligencia para la identificación de los atacantes, la determinación de sus objetivos y, sobre todo, la formación y concienciación de las personas para que los mecanismos de protección sean eficientes.

Por eso, el Centro Criptológico Nacional trabaja para dar respuesta al gran desafío que supone preservar el ciberespacio español, mejorando y adaptando sus soluciones a las necesidades presentes y futuras, para afianzar su papel como centro de referencia, tanto a nivel nacional como internacional, en materia de ciberseguridad.

REFERENCIAS

Capacidad de respuesta a incidentes del Centro Criptológico Nacional. (2007). www.ccn-cert.cni.es

Centro Criptológico Nacional (2018, junio). *Aproximación española a la ciberseguridad.* Decálogo CCN-CERT. Recuperado de https://www.ccn.cni.es/index.php/es/menu-ccn-es/aproximacion-espanola-a-la-ciberseguridad

Estrategia Nacional de Ciberseguridad. (2013). Recuperado de https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

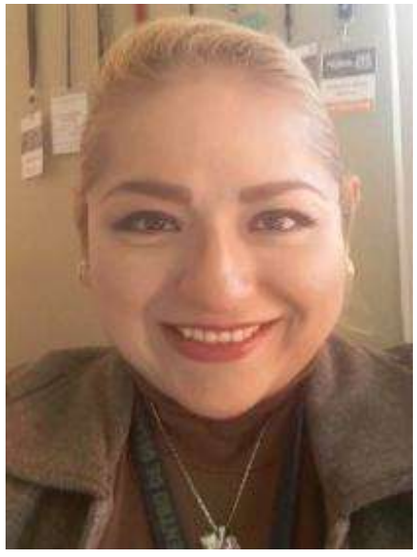
Europea Union Agency for Network and Information Security. (2016). *NCSS Good Practice Guide*. Recuperado de https://www.enisa.europa.eu/publications/ncss-good-practice-guide

We are social (2018). *Global Digital Report.* Recuperado de https://digitalreport.wearesocial.com/

"CIBERSEGURIDAD: APRENDIZAJE DISRUPTIVO EN LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y LA SEGURIDAD NACIONAL "

Cybersecurity: Disruptive learning in the protection of Critical Infrastructures and National Security

Recibido: 06 / 08 / 2019 Aprobado: 31 / 10 / 2019



Licenciada
Alejandra Morán Espinosa
México

Licenciada en Derecho, Licenciada en Derecho por la Facultad de Estudios Superiores Acatlán, candidata a Maestra en Política Criminal, Diplomada en Criminalística con formación docente en la UNAM y diversas universidades privadas, conferencista, articulista e instructora en temas jurídicos relacionados con: seguridad informática, derecho informático, ciberdelitos, TIC, protección de datos personales, informática forense y Ciberespionaje entre otros. Ponente y conferencista en temas jurídicos relacionados con la seguridad informática y los delitos informáticos, docente de la materia de Derecho Informático en la FES Acatlán para alumnos y para profesores en el área de Tecnologías de la Información y Comunicación aplicables al Derecho, recientemente responsable del primer proyecto institucional de Investigación en Derecho Informático (IUSTICS) en la FES Acatlán. Es asesora de desarrolladores de software independientes e integrante de la comisión especializada de evaluadores de aspirantes a peritos auxiliares en el área de informática forense del Tribunal Superior de Justicia del Distrito Federal con sede en FES Acatlán (Áreas de evaluación: Derecho informático y Auditoria Informática), y responsable del único proyecto de Investigación, docencia y difusión en Derecho Informático y la Ciberseguridad en la UNAM denominado IUSTICS, con sede en FES Acatlán. Invitada como sector académico a eventos con la Estrategia Digital Nacional, así como, recientemente integrante y ponente del "5to. Encuentro Latinoamericano sobre: Ciberseguridad, Delitos Cibernéticos e Informática Forense" que literalmente incorpora a la UNAM, como una de las 15 instituciones del sector académico más importantes en la conformación de la actual Estrategia Nacional de Ciberseguridad. amoran@unam.mx y amoran@iustics.tech

RESUMEN

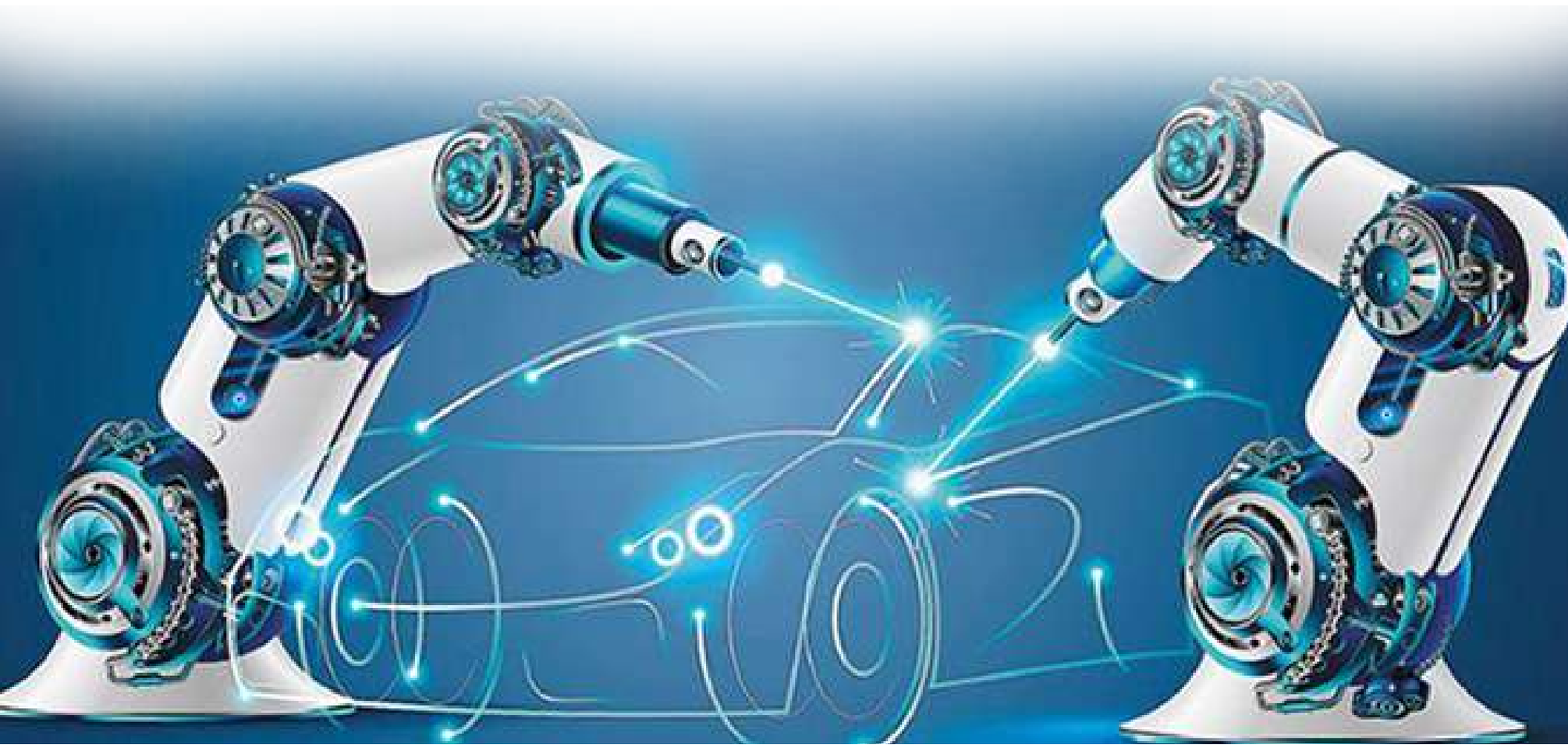
Ante la creciente posibilidad de un ataque cibernético a las infraestructuras críticas de un país, no bastan la seguridad cibernética o la seguridad nacional, debe evolucionarse decididamente a un modelo de protección que implique todos los aspectos, que sume a los avances en la ciberdefensa de los países; con un cambio del modelo de pensamiento, a uno complejo, multifactorial y radical e invariablemente integral, aquel que modifique la forma tradicional de proteger, debe atenderse como un todo a la Ciberseguridad.

Palabras clave:
Ciberseguridad, infraestructuras críticas, seguridad nacional, disrupción, estrategia nacional de ciberseguridad.

ABSTRACT

Given the growing possibility of a cyber attack on a country's critical infrastructures, cybersecurity or national security are not enough; there must be a decided evolution to a protection model that involves all aspects, which adds to the advances in the cyber defense of the countries. With a change of the thinking model, a complex, multifactorial and radical and invariably integral one, that modifies the traditional way of protecting, Cybersecurity should be understood as a whole.

Keywords:
Cybersecurity, critical infrastructures, national security, disruption, national cybersecurity strategy.



INTRODUCCIÓN

Mucho se ha dicho de la era digital y altamente tecnológica en la cual vivimos, pero nunca será suficiente, cada cosa dicha, cada frase acuñada, cada curso impartido, cada medida tomada, cada regulación creada y cada nota informativa publicada aportan mucho al tema, propiamente al de la cultura de la seguridad, pero ya es insuficiente, hay muchas cosas que proteger que van más allá de la cartera, el auto o la casa… notas informativas cotidianas reportan diariamente un apartado incluso específico, de aquellos incidentes o delitos cometidos a través de la tecnología o teniendo a ésta como objetivo, lo cual ya lo hace muy grave dado que ¡se está clasificando a la inseguridad misma!, y por tanto a los actos delictivos que le caracterizan, por tipo o gravedad de los mismos; lo cual no sería posible si no fuera tan variada, de hecho, podría sucederle a cualquier persona, empresa o gobierno y sucede no recientemente.

Hablar de inseguridad es cotidiano en cualquier lugar del mundo, ya que, en el momento histórico actual, con sus variadas y robustas herramientas tecnológicas, informatización generalizada, innovación y nuevos negocios y el excesivo flujo e intercambio transfronterizo de información por minuto, se realiza, pero sin saber mucho de la protección de la información y sin importar quién es el destinatario final, por un lado; por otro, si bien el momento y la propia tecnología con sus cada vez más variados entornos "Ciber", presenta un escenario de nuevas e impactantes oportunidades, implica a la vez nuevos retos y claramente nuevos riesgos, transformando tal cúmulo imparable de oportunidades que la conectividad y la interconexión[1] ofrecen, en un potencial imparable de riesgos y amenazas en el ciberespacio[2] y recientemente denominado ciberentorno[3], lo que es motivo suficiente para entender[4], informarse, atender, prevenir y proteger los activos de información y crear o actualizar la regulación jurídica necesaria que determine la responsabilidad de quien actúe lesivamente, tal como sucede en la vida cotidiana; incluido un cambio radical de pensamiento que supere los conceptos tradicionales de seguridad y por supuesto de inseguridad, para lo que la expresión Ciberseguridad es ideal, ya que contiene todos los campos de conocimiento necesarios para elevar al máximo, el nivel de seguridad que pueda tenerse y que nunca será ni perfecto, ni absoluto.

La necesidad de Ciberseguridad debe convertirse en una inclusión obligada legalmente en el tema, desde los aspectos introductorios hasta la aplicación y monitoreo de la situación y avances actuales. Incluso la creación de un observatorio internacional que facilite el aprendizaje, la generación de recursos humanos, materiales, herramientas, profundización en cifrado, y temas selectos de ciberdefensa para cuerpos especiales, generación de leyes modelo, homologación de definiciones, que de preferencia estuviera relacionada con algún tratado existente o nuevo, que facilite en la región los parámetros actuales de Ciberseguridad de todos, para todos dado el impacto masivo peligroso que tendría un ciberataque para cualquier país, ello facilitaría la protección de las distintas infraestructuras de un país; algo así como la ONU de la Ciberseguridad, lo más viable para un avance común en la protección de problemas comunes para la comunidad de países contra los ciberdelincuentes[5].

[1]Interconexión: Conexión física o virtual, lógica y funcional entre redes públicas de telecomunicaciones que permite la conducción de tráfico entre dichas redes y/o entre servicios de telecomunicaciones prestados a través de las mismas, de manera que los usuarios de una de las redes públicas de telecomunicaciones puedan conectarse e intercambiar tráfico con los usuarios de otra red pública de telecomunicaciones y viceversa, o bien permite a los usuarios de una red pública de telecomunicaciones la utilización de servicios de telecomunicaciones provistos por o a través de otra red pública de telecomunicaciones.

[2]Ámbito artificial o lugar virtual donde usuarios de la red interactúan a través de un lenguaje, expresado en sentido de textos, imágenes, gráficos, sonidos etc., entendiendo dicha red como un tejido de computadoras interconectadas que guardan bases de datos y fuentes de información, a las cuales los usuarios pueden acceder. Genera situaciones de derecho reales a pesar de romper el ámbito espacial, es decir, se puede caer en una determinada situación sin importar la distancia de las mismas, dicha situación sigue generando consecuencias de derecho a pesar de que no se realicen en un plano físicamente tangible.

[3]Esto incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes o en dispositivos o la información que éstos generan. Las instalaciones y edificios donde residen los dispositivos también forman parte del Ciberentorno…"

[4] Los diferentes vocablos que han surgido y que continuarán surgiendo a partir de que, a cada conducta nueva se le asigne tal prefijo para diferenciarla de la conducta en la vida cotidiana, ejemplos de ello pueden ser las siguientes expresiones: Cibernauta, Ciberguerra, Cibernética, Ciberarmamento, Ciberataque, Cibernegocio, Ciberdelincuencia, Ciberconciencia, Cibertolerancia, Ciberinteligencia, Ciberaliados, Cibertratado o por qué no…Ciberpaz.

[5] Aquella persona (s), entidad y/o organización, interna o externa al sujeto pasivo o agraviado, que dolosa e ilícitamente realiza cualquier acto considerado hostil, directo o indirecto de cualquier intensidad, nivel, tipo y por cualquier medio contra la comunidad global de personas o naciones, contra su información, procesos, datos, infraestructura, sitios web, equipos o redes con cualquier fin, protegida o no, logre o no su objetivo. (Definición propia).

A manera de referente, el panorama señalado por el informe de la OEA (2014), "Tendencias de Seguridad Cibernética en América Latina y el Caribe", en América Latina y el Caribe este tipo de delitos cuesta alrededor de US$90,000 millones al año. Por su parte para tener como referente más actual, el propio informe de la OEA (2016), "¿Estamos preparados en América Latina y el Caribe?", que señala que en su calidad de cibercrimen, éste le costaba cada año al mundo hasta US$575,000, 2 millones al año, 0.5 por ciento del producto interno bruto global, lo que representa casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional, baste decir. (ENC:2017)

Ante un panorama nada esperanzador -como si no fueran suficientes las amenazas ya existentes-: por lo que es urgente, adecuar nuevas definiciones hasta cambiar la forma de pensamiento sobre la forma de proporcionar seguridad a la información y a las infraestructuras nacionales, ya que la seguridad tradicional debe adecuarse y mejorar permanentemente, ya que no solo se trata de proteger además de delincuentes comunes con delitos tradicionales, hasta protegerse ante la presencia ilícita, impactante y global de un relativamente nuevo tipo de delincuencia; sin duda alguna esto a través del aprendizaje obligado de la Ciberseguridad como nuevo modelo de protección de las infraestructuras de los países y a propósito de las conocidas ventajas que conlleva el trabajo conjunto de éstos, lo que justifica inequívocamente su aprendizaje y lo que parece la única manera de enfrentar, exitosamente, a la nada menos que ¡Delincuencia informática organizada!

SEGURIDAD CIBERNÉTICA A LAS INFRAESTRUCTURAS CRÍTICAS

El tema esencial para vivir con cierta tranquilidad y paz en la sociedad actual de cualquier lugar del mundo, es el tema de la seguridad, pública, personal o nacional, y recientemente de la seguridad de la información, término perfeccionado en su definición y aplicabilidad, y que en algunos años se ha dado en denominar Ciberseguridad, misma a la que se puede definir así:

ENC (2017) (México): "Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación."

UIT–T X.1205 (2010): "La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno… Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad, integridad, que puede incluir la autenticidad y el no repudio; confidencialidad."

Definiciones necesarias que implican atender y elevar el nivel de seguridad de la información, ya que de ser accesada, vulnerada, atacada, expuesta o copiada, puede incluso poner en entredicho la reputación, el trabajo, la seguridad personal y familiar y en el caso de los estados y sus gobiernos, ¡la continuidad de los servicios públicos que prestan a los ciudadanos, necesarios para la continuidad de la vida misma de las personas!, en el peor de los casos el gravísimo colapso de éstos. Es aquí donde aparecen las diversas infraestructuras de los estados, ya que son precisamente éstas a través de las cuales se prestan esos servicios y existen en todos los países, lo que justifica su importancia global.

Se trata de proteger y salvaguardar los bienes más preciados en el momento social actual -activos que usuarios, empresas y gobiernos poseen-, donde el enemigo, el riesgo o el atacante, es: anónimo, especializado e invisible, ¡casi nada!, de ahí que el tema sea tan importante, porque las potenciales víctimas (los estados), no saben necesariamente, que deben prepararse para protegerse de personas, gobiernos, analfabetismo digital, desobediencia profesional, incumplimiento laboral, la obsolescencia jurídica o la continuidad de su aplicación cuando existe la normativa, donde el ideal sería la existencia de la propia Estrategia Nacional de Ciberseguridad para todos los países, porque los riesgos existen y seguirán existiendo, tan sencillo y tan confuso ya que se trata de protegerse de algo que podría o no, atacar; nada parecido a la vida cotidiana donde la mayoría es consciente para enfrentar de alguna manera a la delincuencia -que denomino solo para efectos didácticos- "tradicional", si se permite la expresión.

En principio, no entender que la seguridad absoluta no existe[6], poca atención provoca en los gobernantes respecto de la seguridad física, de la información de personas y gobiernos, la protección de todo tipo de recursos, de información, sistemas, de fronteras, comunicaciones, de los aspectos físicos, geográficos e informáticos, tan necesarios de proteger (hasta años recientes); lo que en sí mismo es una vulnerabilidad[7], donde la definición que se use para explicar el nivel de seguridad y atención que se tenga de ésta, depende de la óptica de estudio o de la autoridad que la defina, y lo que por ella debe entenderse para concientizar, aplicar y proteger, y en el peor de los casos defender.

Dados los argumentos vertidos, es que se convierte en cuestionable la poca atención al tema por algunos gobiernos, atendiéndose más veces solo por cuestiones políticas del gobierno en funciones –políticas, presupuestos, agenda, planes de desarrollo, etc.-, que con un programa o normativa permanente de protección de las funciones de salvaguarda de la seguridad nacional y sus infraestructuras, podría mantenerse eficiente, eficaz y fuerte; superando así, los planes de trabajo y plataforma política de los cambios de gobierno, la apatía por los temas de trabajo del gobierno anterior, planificación presupuestal o la propia brecha digital/generacional; lo que es justo, necesario, responsable y jurídicamente exigible. Con independencia del país, solo algunos gobiernos se han preocupado por informatizar algunos de sus servicios a través de la implementación de figuras como la del gobierno electrónico o e-gobierno[8] por ejemplo, que, si bien cumple cabalmente con el derecho humano de acceso a la información[9], no implica acciones de Ciberseguridad y menos aun involucra la protección cibernética de las infraestructuras del estado, y la poca atención es en su mayoría verdaderamente insuficiente, de forma que al accesarse ilícitamente a datos e información, ésta es considerada vulnerada y/o expuesta y ello puede suceder en un sin fin de ocasiones, donde el esfuerzo por continuar direccionando y facilitando las funciones de seguridad ciudadana y seguridad nacional del estado, así como la falta de acciones específicas, no necesariamente facilitan la protección de la información.

Ante tal escenario deben sumarse las amenazas existentes, –que no son precisamente lo que se conoce como "tradicionales"- lo que deja, permite visualizar un escenario a decir lo menos preocupante y urgente no solo para la seguridad de la información, literalmente para la propia seguridad nacional, como lo refiere excelentemente Baralt (2017), en su trabajo intitulado "Un reto para la Defensa Nacional en entornos intangibles", expresión que aplica perfectamente al presente trabajo, donde se particulariza en las infraestructuras críticas del estado y cuya inminente necesidad de protección, se corrobora con los innumerables trabajos realizados a nivel internacional que en diversidad de eventos y foros de intercambio de experiencias incluidas por supuesto, la diversas fuerzas de defensa y militares de los países participantes, son quienes encabezan la función protectora y defensora del estado, como en cualquier país, aportando a la comunidad internacional de países, información e investigación relevante de su experiencia, donde sin embargo, nunca son suficientes espacios de intercambio o siempre naciones ausentes.

Dadas primeramente las amenazas[10] existentes (riesgos, desastres naturales[11], conflictos sociales, ciberataques, entre otros tipos de incidentes de seguridad), en segundo lugar las debilidades[12] (p.e.

[6]El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de Titanio, encerrado en un búnker de concreto, rodeado por gas venenoso y cuidado por guardias muy armados y muy bien pagados. Aun así, no apostaría mi vida por él.

[7]Las debilidades identificadas en la ciberseguridad dentro de las dependencias o entidades de la APF, los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las empresas productivas del Estado, los Gobiernos Estatales, Municipales y Delegacionales, así como los particulares que potencialmente permiten que una amenaza afecte los activos de TIC, a la Infraestructura Información Esencial, así como a los Activos de Información.

[8]El gobierno electrónico es la aplicación de las tecnologías de la información y la comunicación (TIC) al funcionamiento del sector Público, con el objetivo de incrementar la eficiencia, la trasparencia y la participación ciudadana que tiene el gobierno de un país con sus gobernados".

[9]…la Corte Interamericana de Derechos Humanos ha señalado … "el concepto de orden público reclama que, dentro de una sociedad democrática, se garanticen las mayores posibilidades de circulación de noticias, ideas y opiniones, así como el más amplio acceso a la información por parte de la sociedad en su conjunto..."

[10]Amenaza: cualquier elemento, conducta, actividad, proceso, automático o manual, de cualquier índole, que aprovecha una vulnerabilidad generada o existente, para atentar contra la seguridad de un activo de información o de alguno de sus componentes y/o equipos y/o sistemas y/o procesos y/o software y/o redes y/o sitio web, comprometiendo la continuidad de la operación de la infraestructura y/o del servicio público prestado, se logre o no el objetivo de la amenaza.

[11]Aquéllos sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta: fuego y/o rayo), daños por agua (desbordamiento de un rio), otros desastres naturales (tornados o temblores).

[12]Debilidad: que puede poner en peligro la información, operación o infraestructura y alguno de sus componentes y/o equipos y/o sistemas y/o procesos y/o software y/o redes y/o sitio web, comprometiendo la continuidad de la operación de la infraestructura y/o del servicio público prestado, que provoque una afectación o daño grave y/o inmediato y/o general para el país o a alguno de los estados que lo conformen.

la falta de presupuesto o de concienciación o concientización[13]), en tercer lugar los riesgos[14] inminentes (ransomware, espionaje, terrorismo, ataques dirigidos o intencionados[15], y las correspondientes actividades "Cyber" de los ciberataques en general–conocidos también como defensa activa-), en cuarto lugar la escasa atención al desarrollo del tema en las agendas de algunos Estados[16] se suman nuevos entornos de riesgo como son: uso indiscriminado de Apps contaminadas, plataformas informáticas alojadas en otros países, las nubes o entorno cloud, la expansión de centros de datos (datacenters), el necesario flujo de datos transfronterizos, el internet de las cosas (IoT), la videovigilancia, los radares civiles y militares, las WiFi o redes abiertas; la falta de protocolos particularizados, los actos cotidianos de ciberespionaje, el analfabetismo tecnológico y la ausencia legislativa –que son un riesgo en sí mismos-, puede asegurarse que el panorama no es alentador y si muy atemorizante y urgente.

Lo anterior, sin considerar que exista un tipo penal ideal, garante y protector de las infraestructuras del estado y la información y procesos que contengan, y que podría presentar sus propios problemas ya que los elementos de la conducta típica no suelen reunirse en su totalidad ni fácilmente, ya que muchas veces la información no fue accesada u obtenida inmediatamente, los atacantes suelen estar presentes desde muchos meses antes, por lo que no se conoce mucho del proceso del ataque ni del dominio exacto de información que poseen, lo que dificulta la investigación y la correlativa relación con la tipificación criminal, en su caso, todo ello sin siquiera precisar el necesario contexto legal que debe aplicarse, -de existir éste-, lo que representa un grave problema de seguridad nacional por supuesto, ya que la ausencia o la obsolescencia normativa, solo dejan como resultado, pérdidas, daños e impunidad y provocan un estado de indefensión permanente.

Tratándose de tecnología y para el caso de estados y sus gobiernos, es que el hablar de Ciberseguridad se convierte en determinante dada la alta y necesaria dependencia tecnológica de éstos, lo que justifica fundadamente la protección de sus entidades públicas, misma que está considerada en la propia recomendación UIT Rec. UIT-T X.1205 (04/2008:2), por eso, proteger su seguridad perimetral, seguridad de la información y la de todos sus tipos de infraestructuras es primordial, prioritario y deseable, ya que avanzar en el modelo de madurez del uso y protección de la tecnología, no es nada fácil donde muchas veces los procesos de sucesión presidencial que se vive en cada país en algún momento producen la interrupción de los trabajos y funciones de protección, gestando cambios en políticas públicas, agendas, estrategias o el abandono de éstas, lo que es contrario al modelo de continuidad que sobre la protección de las infraestructuras esenciales y las infraestructuras críticas debe existir, por ello, el cambio de pensamiento es esencial, de ahí la presente propuesta denominada "Ciberseguridad: Aprendizaje disruptivo en la protección de Infraestructuras Críticas y la Seguridad Nacional", entendiéndose como disruptivo el hecho de que gracias a la aplicación directa de la Ciberseguridad, se produzca necesariamente una ruptura simbólica en la forma de trabajo y protección que brindan algunos Estados a sus infraestructuras críticas, superando significativamente la protección tradicional. Cambio determinante para la continuidad de los servicios públicos prestados a través de aquéllas, ante los riesgos propios o las vulnerabilidades del ciberentorno.

Al hacer referencia a una entidad pública como objeto de protección, se alude a las instituciones, dependencias y en general a cualquier secretaría, área, departamento, institución, dependencia, oficina, instancia, etc., que forma parte de la organización de la ad-

[13]Errores de los usuarios, del administrador o de configuración, deficiencias en la organización, alteración de la información, introducción de información incorrecta, degradación o destrucción de información, divulgación de ésta, falta de actualización de sistemas y programas.

[14] Riesgo : aquél que puede poner en peligro la información confidencial o sensible de personas, grupos vulnerables, financiera, presupuestal, identificativa, de salud, proveedores, de procesos, servidores públicos, expedientes judiciales, empleados, funcionamiento, investigaciones criminales, investigaciones científicas sobre la salud, operativos de seguridad ciudadana o pública, procedimientos internos, control y acceso de sistemas informáticos, de vigilancia, funcionamiento o distribución, etc. Comprometiendo la continuidad de un servicio o exponiendo información aún no firme o definitiva, de carácter estrictamente confidencial y de alta seguridad, incluso seguridad nacional.

[15] Manipulación de la configuración, suplantación de la identidad, abuso de privilegios de acceso, acceso no autorizado, interceptación de información (escucha), modificación de la información, denegación de servicio (ataque Dos o DDos). Debe precisarse que cuando un riesgo se vuelve real, causa invariablemente un incidente.

[16] Información fundamentada en otros materiales, como en los hallazgos que indican que analizados los datos de 191 entidades bancarias de toda la región de Latinoamérica, el 49% de las entidades bancarias aún no están implementando herramientas, controles o procesos usando Tecnologías Digitales Emergentes, tales como Big Data, Machine Learning o Inteligencia Artificial, las cuales resultan muy importantes a la hora de prevenir ciberataques, (OEA:2018), por ejemplo; lo que indica por simple sentido común, que si los sistemas financieros que son un sector de lo más interesante para los criminales (véase: Harán J.M.:2018), no tiene la protección suficiente que aporta la ciberseguridad, entonces queda claro el porqué, no es posible encontrar mayor interés en la protección de las diversas infraestructuras de los países.

ministración pública de un país, para el caso de México, ejemplos de entidad pública serían las siguientes: la Oficina de la Presidencia de la República, las Secretarías de Estado, la Consejería Jurídica del Ejecutivo Federal, los Órganos Reguladores Coordinados en Materia Energética, entre otros, lo cual significa que prácticamente toda la administración pública de un país, debe estar incluida en la categoría de dependencia pública y por ende ser sujeto de protección.

Por otro lado, cuando se habla de infraestructuras críticas, claramente se hace alusión a un solo tipo de éstas, sin embargo, existen claras definiciones que diferencian el tipo de infraestructura (s) que puede existir en un país, a saber:

Infraestructuras estratégicas: Ley 8 (2011) (España), Artículo 2, inciso d): "las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales."

Infraestructuras críticas: ENC (2017:21) (México): "… acciones encaminadas a establecer las acciones y mecanismos necesarios para minimizar la probabilidad de riesgos y vulnerabilidades inherentes en el uso de las TIC para la gestión de infraestructuras críticas, así como para fortalecer la capacidad de resiliencia[17] para mantener la estabilidad y continuidad de los servicios en caso de sufrir un incidente de ciberseguridad."

Ley 8 (2011) (España): Artículo 2, incisos: "**e)** Las instalaciones, redes, servicios y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre dichos servicios … **k)** Protección de infraestructuras críticas: el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia."

Directiva 2008/114/CE del Consejo (Unión Europea): "Artículo 2, inciso a): "El elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;"

Como se desprende de las definiciones referidas, la diferencia entre los tipos de infraestructura es determinante para saber el nivel de protección que estas necesitan y el impacto que podría desencadenarse si fueran expuestas o atacadas y cualquiera de ellas claramente forma parte de alguno o de todos los órdenes de gobierno y muchas de ellas, son componente indispensable para la prestación de un servicio público esencial y en el caso más grave, inhabilitar el servicio o proporcionarlo pero integrar en él un elemento adicional que afecte directamente a toda la población que lo recibe, donde el servicio es el vehículo utilizado para ocasionar la afectación lo que permite clasificar en afectación directa de la infraestructura, teniendo a ésta como objetivo o usando a esta como medio para la comisión de un daño, por supuesto en el caso de la infraestructura critica sería más grave la afectación ya que se trata de aquellas que son de vital importancia para el mantenimiento del Estado o la seguridad nacional, incluso para la supervivencia de la vida.

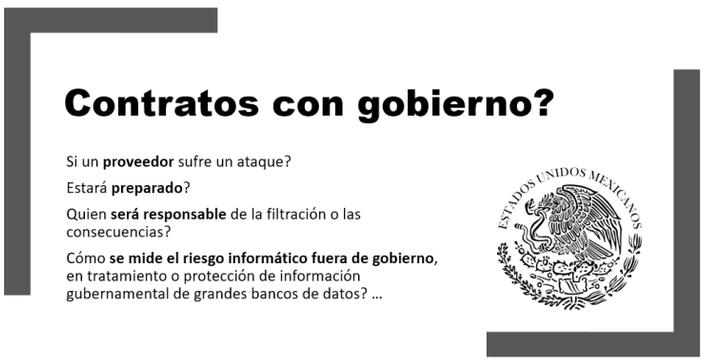
Los principales riesgos y amenazas a un país podrían involucrar alguno o varios de los aspectos que formen parte de la estructura funcional, jerárquica u organizativa de los siguientes servicios proporcionados por un estado:

1. Administración (servicios básicos, instalaciones, redes de información, principales activos y monumentos del patrimonio nacional)
2. Instalaciones espaciales; Industria Química y Centrales Nucleares (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, biológicos, radiológicos, etc.)

[17]Ciber resiliencia puede entenderse como lo define Carrasco (2015) al decir: "…se ha definido partiendo de la definición de resiliencia y restringiendo las posibles fuentes de crisis a eventos tecnológicos y procedentes del ciberespacio, o también se ha definido limitando la dimensión afectada de la empresa a lo que son sus sistemas de proceso de datos y sus comunicaciones. Dada la complejidad de las organizaciones, y la interdependencia entre los distintos elementos que las forman: personal, entorno social, suministros, infraestructura TIC, procesos, ...; no se puede trazar una línea divisoria clara entre lo que supone la resiliencia de la misma y la ciber-resiliencia de sus sistemas. Una y otra están íntimamente relacionadas, es más, son un mismo concepto. No se puede crear una infraestructura tecnológica ciber-resiliente si la organización en sí no es resiliente."

3. Agua (embalses, presas, almacenamiento, tratamiento y redes de distribución)
4. Centrales y Redes de energía (producción y distribución)
5. Gasoductos (extracción, almacenamiento y distribución)
6. Tecnologías de la Información y las Comunicaciones (las existentes, independiente del nivel de reducción de la brecha digital)
7. Salud (sector e infraestructura sanitaria hasta su usuario final)
8. Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico, logística, etc.)
9. Alimentación (producción, almacenamiento y distribución)
10. Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones)
11. Infraestructuras defensivas nacionales (militares, aéreas y navales, oficiales, encubiertas y de contrainteligencia).

Además del listado anterior, deben reconocerse otro tipo de peligros, como el de la subcontratación o descentralización en la prestación de un servicio público, es tema de particular atención ya que existe mucha probabilidad de que la empresa privada que controle la prestación del servicio público estatal, no tenga la Ciberseguridad necesaria para proteger muchos aspectos la actividad adecuadamente.



Considerando que difícilmente existen protocolos de supervisión a terceros, un buen ejemplo de esto es el sucedido en 2018 con Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día, donde los temas centrales se relacionaron con acusaciones de robo de datos, interferencia política, chantajes y la adquisición indebida de información de por lo menos 50 millones de usuarios, solamente en Estados Unidos. Si hipotéticamente colocáramos a cualquier gobierno en el lugar de Facebook y a una empresa privada trabajando para éste la prestación de algún servicio público (conocido como descentralización), podría suceder lo mismo, el que un estado esté preparado -en el mejor de los casos- en Ciberseguridad, no asegura que quienes trabajen legalmente para éstos, estén tan preparados como el estado contratante.

Los servicios públicos referidos, se encuentran relacionados directa o indirectamente con la seguridad nacional o su información, entendiéndose esta en lo expresado por la Ley de Seguridad Nacional (2005) (Mexicana), Artículo 6, fracción 5 como: "…los datos personales otorgados a una instancia por servidores públicos, así como los datos personales proporcionados al Estado Mexicano para determinar o prevenir una amenaza a la Seguridad Nacional", de manera que es una de las funciones primordiales y prioritarias de cualquier estado, solamente realizado por su ejército, fuerza armada, la marina y/o la fuerza aérea, independientes o en conjunto, como en México que en éste último caso se le conoce como "Fuerza armada permanente" y que en términos de la ley referida indica: "Artículo 3.- Para efectos de esta Ley, por Seguridad Nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a:

I. La protección de la nación… frente a las amenazas y riesgos…;
II. La preservación de la soberanía e independencia nacionales y la defensa del territorio;…
V. La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional,…"

Adicionalmente y de forma clara especifica también: "Artículo 5.- Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:

I. Actos tendientes a consumar espionaje, sabotaje, terrorismo, … en contra de los Estados Unidos Mexicanos dentro del territorio nacional;
II. Actos de interferencia extranjera en los asuntos nacionales;…
V. Actos tendentes a obstaculizar… operaciones militares o navales…;

VI. Actos en contra de la seguridad de la aviación;
VII. Actos que atenten en contra del personal diplomático;…
IX. Actos ilícitos en contra de la navegación marítima;…
XI. Actos tendentes a obstaculizar… actividades de inteligencia o contrainteligencia, y
XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico… para la provisión de bienes o servicios públicos."

Normativa que considerando que existen diversos actos posibles y que de cualquier forma puedan afectar a la seguridad nacional, serán invariablemente considerados como una amenaza a ésta, estableciéndose en la última fracción precisamente el tema que nos ocupa, refiriendo a los dos tipos de infraestructura más importantes, la infraestructura estratégica y aquella propiamente critica, dado lo cual en México cualquier ataque a este tipo de infraestructuras es considerado un ataque a la seguridad nacional, donde el cambio disruptivo no seria de orden normativo en principio, sino de continuidad de los trabajos realizados desde hace ya poco más de seis años.

Debe tenerse presente que, desde una óptica jurídica y de derecho internacional, es todo un reto el uso de tecnología para tres figuras del Derecho Internacional relacionadas con el conflicto y que aun en la actualidad generan polémica, siendo éstas: a) Uso de la fuerza (ataques armados con la aplicación de la tecnología conocidos como ciberataques), b) El espionaje o el ciberespionaje y c) El terrorismo o ciberterrorismo; temas difíciles y sensibles para la comunidad internacional de países, ya que representan muchas dificultades legales principalmente, desde la falta de precisión territorial (jurisdicción), hasta el problema de las definiciones homogéneas. Sin embargo, hay que recordar que para muchos estados, los principios del Derecho Internacional sí le aplican, ya que solo son nuevas herramientas en caso de conflicto internacional, pero ello no cambia el conflicto, solo lo diferencia de territorio y de armamento, y para responder precisamente a ese problema, se encuentra el Derecho Internacional, que provoca a su vez otros cambios en diversas ramas del mismo, como lo son el Derecho Humanitario Internacional y el Derecho de Guerra principalmente. (Morán:2013)

De esta manera es como el ciberespacio -contrario a lo que pudiera pensarse-, no es una zona totalmente libre de leyes donde cualquiera puede llevar a cabo todo tipo de actividades y conductas, incluyendo las hostiles; paulatinamente se aprecia que la norma jurídica tiende a regular conductas y aspectos de dicho entorno, solo que este proceso es bastante lento dado que no se esperaba la variedad y cantidad de amenazas que ahora se sabe que existen y de las cuales se han desprendido incalculables daños financieros en diversos países del mundo. Lamentablemente los aspectos regulatorios, llevan mucho trabajo y tiempo, ya que éstos se establecen precisamente en función de la aparición de los ciberataques -situación que precisamente propone este trabajo a contrario sensu para no esperar a que sucedan-, considerando que es un hecho cierto la comisión de éstos actos humanos o conductas que han sido inequívocamente hostiles y que pese a los esfuerzos de los atacantes por evitar ser localizados e identificados, suele conocerse en breve su estrategia, tiempo de ejecución y cuantificación aproximada de daños; donde el problema principal radica en el orden jurídico aplicable, debido a que para la determinación de la responsabilidad y su respectiva sanción, -como en cualquier otro delito-, deben identificarse con precisión los principios jurídicos aplicables a las circunstancias incluyendo la comisión de otras conductas delictivas, con ello determinar la norma jurídica adecuada y la jurisdicción que corresponda, sin embargo no siempre sucede, debe recordarse que si bien el Derecho Internacional es aplicable en una gran parte del territorio internacional, es precisamente en los territorios sujetos a excepción, donde los verdaderos ataques se organizan, atentando pública y cínicamente contra todo ordenamiento o tratado internacional que exista y su aplicación.

Debe decirse al respecto que en ciertas circunstancias, las actividades en el ciberespacio pueden ser consideradas como uso de la fuerza nacional o internacional, eso con base en el Artículo 2 párrafo 4 de la Carta de las Naciones Unidas (ONU:1945), que manifiesta: "Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas." Dicha Carta también establece que un estado puede responder a un ataque por internet -lo que ahora denominamos el Ciberespacio-, ejerciendo su derecho de legítima defensa en el caso de que el ataque sea equivalente a un ataque armado, ello con base en el Artículo 51 del mismo documento que establece: "Ninguna disposición de esta Carta menoscabará el derecho inminente de legítima defensa, individual o

colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales."

Es de esta forma como la propia Carta de las Naciones Unidas usa el término ataque armado para describir los actos contra los cuales está permitido el uso de la fuerza a través del derecho de legítima defensa, como se analizaba de la pr opia Ley de Seguridad Nacional en el caso de México, sin embargo, es innegable la relación entre los conceptos de agresión[18] y ataque armado, es decir, por ele- mental inteligencia y mínimo sentido común, es claro que todos los ataques armados se pueden equiparar a una agresión directa, pero también debe recordarse que la expresión "ataque armado" no está definida por ninguna convención y su significado está abierto a la interpretación de los Estados, de ahí que deba aplaudirse el esfuerzo de las regulaciones jurídicas de los países que si definen éstos preceptos.

Paralelamente, debe destacarse la propuesta de Feffrey (2012), quien explica los modelos utilizados para identificar si un ciberataque es un ataque armado: "El primer modelo es … basado en el enfoque, que comprueba si el daño causado por un nuevo método de ataque anteriormente podría haber sido logrado sólo con un ataque cinético. El segundo es … basado en los efectos… consecuencia, en la que la similitud del ataque a un ataque cinético es irrelevante y la atención se centra en el efecto general … estos tienen como víctima al Estado. El tercero es … de responsabilidad estricta, en la que los ciberataques contra infraestructuras críticas son tratados automáticamente como ataques armados, debido a las graves consecuencias que pueden derivarse de la desactivación de los sistemas."

Tal y como se ha venido identificando y con base en la clasificación de enfoques del autor, el ciberataque a una infraestructura crítica puede ser equiparado a un ataque armado, debiendo precisar que a este criterio también le son aplicables la consideración de los daños económicos causados, ya que el derecho internacional establece que los ataques económicos también son aplicables a la legítima defensa o autodefensa; daños que innumerables comunicados oficiales demuestran han existido y han sido consecuencia directa de ciberataques. Como si no fuera suficiente, debe sumarse a los criterios analizados y como refuerzo de éstos, lo establecido por Jens Stoltenberg, secretario general de la alianza militar de ministros de Defensa de la OTAN en 2017, dijo que la alianza estaba "…en el proceso de establecer al ciberespacio", como un dominio junto con la tierra, el mar y el aire, lo que significa que un ataque cibernético teóricamente podría accionar el Artículo 5 del tratado que está relacionado con la defensa colectiva, lo que significa que la OTAN, establece el ciberespacio como un dominio militar legítimo, donde se consideraría un ciberataque a una nación miembro como si afectara a los 29 aliados de la organización.

En la asignación de responsabilidad en la comisión de ciberataques, hay que remarcar que los Estados son legalmente responsables por las actividades de sus órganos, personas o instituciones siempre que actúen bajo su control, por tanto, hay responsabilidad internacional inmediata en esta materia. Por otra parte, en cuanto al tema de la intensidad de la autodefensa, se encuentra relacionada con los principios de distinción y de proporcionalidad, de tal forma que no contribuya a preservar el esfuerzo de guerra, de forma que la autodefensa debe ser proporcional al daño recibido y la acción debe darse para evadir un daño mayor sin afán de castigo o venganza. Lo que significa que el ciberespacio es oficialmente un territorio más donde desencadenar una guerra con tal de proteger los bienes jurídicos[19] de todos, tarea muy complicada si se tiene presente que el ciberdelito va en aumento año con año.

Quedan en el tintero algunos otros aspectos, dado que día a día la Ciberseguridad se vuelve más importante, como se comprueba

[18]Agresión: "…es cualquier uso ilegal de la fuerza, cualquier uso … que no sea legítima defensa contra un ataque armado o acción coercitiva por las Naciones Unidas.

[19]Bien jurídico, es de origen jurídico doctrinal y se refiere, en palabras de la Universidad de Navarra (s.f.), ".. a .. aquella realidad valorada socialmente por su vinculación con la persona y su desarrollo. Vida, salud, integridad, libertad, indemnidad, patrimonio… son bienes jurídicos. Pero también lo son la Administración pública, entendida como conjunto de circunstancias de funcionamiento de la Administración que posibilitan el desarrollo de las personas; también la Administración de Justicia, el medio ambiente, la salud pública…", tratándose de los bienes que debe proteger cualquier estado.

con su inclusión desde videojuegos hasta miniseries televisivas, por ello solo se enuncia uno de los pendientes más importantes: el problema de la inversión financiera (unos para protegerse y otros para atacar).

CONCLUSIÓN

En la actualidad el mundo globalizado, ampliamente informatizado e hiperconectado exige Ciberseguridad, ya que hace frente a riesgos y vulnerabilidades propias. Ello presenta un claro escenario de retos y desafíos en el tema, que además de fortalecerse deba transformarse y mejorar permanentemente, sumando el trabajo transdisciplinario que sea necesario para disminuir el riesgo latente al que todos los sectores -personas, empresas y gobiernos- estamos expuestos, evitando que al sumar las vulnerabilidades propias, se llegue a en peligroso estado de indefensión. A manera de conclusiones, se enlistan cuatro rubros que justifican realizar el pensamiento disruptivo que considere la aplicación de la Ciberseguridad como aprendizaje necesario e ideal en la protección de las Infraestructuras Críticas existentes y la Seguridad Nacional de nuestros países, basadas en un enfoque integral, a saber:

Técnicas: Uso de cifrado obligatorio; dobles autenticaciones (incluidas biométricas); crear "estándar modelo" único de gestión de riesgos, inclusión de diagnósticos de vulnerabilidades; realización de cibersimulacros, creación de alerta nacional; creación de centros de sensibilización y concienciación; auditorías integrales aleatorias (interconectadas entre instancias gubernamentales y con los CERT existentes); diseñar y considerar a la resiliencia cibernética en los procesos internos; diseño de herramientas, metodologías y operarios propios.

Sociales: Potenciar el aprendizaje en ciberseguridad incluido uso ético y responsable de la tecnología; fortalecer la cooperación con entes privados para mejora continua y desistimiento voluntario de conductas de sabotaje (eslabón más débil). Concientizar a los ciudadanos que la tecnología es una herramienta, no un arma.

Económicas: Priorizar la inversión estatal en ciberseguridad; atender acciones de Inversión en capacitación, investigación y formación en Ciberseguridad.

Jurídicas: Homologar definiciones generales útiles para las normas jurídicas, catalogar específicamente las infraestructuras críticas del país incluyendo al internet como una de éstas; sumarse o crear un tratado específico de Ciberseguridad que procure la cooperación e investigación internacional de delitos en las infraestructuras estratégicas y críticas[20]; sustituir las estrategias nacionales por legislación especial; convertir a la Ciberseguridad como objetivo común; incremento y reforzamiento permanente, de la capacidad táctica, operativa, de inteligencia y contrainteligencia (ciberdefensa) nacionales, con un equilibrio respetuoso de capacidades, jerarquía y funciones en ciberseguridad, evitando la militarización del ciberespacio y evitando llegar a los excesos, homologando el concepto real y jurídico de soberanía nacional digital, sin alimentar la ciberguerra que se dice hace tiempo ya comenzó.

Siendo los riesgos actuales desde el malware, la inteligencia artificial, los riesgos del Big Data, la videovigilancia, las nuevas redes (5G), hasta las Fake News que ocasionan riesgos por el impacto y movilidad social que generan, estos son los razonamientos, razones y motivos suficientes, para proponer y apostar por una cultura general y obligada de la Ciberseguridad como una prioridad de Seguridad Nacional en la política de los estados, que debe sucederse desde la disrupción del pensamiento tradicional de protección de las infraestructuras críticas, para superar la constante de aprender, desarrollar y aplicar Ciberseguridad solo hasta después de que suceda algún incidente.

[20]Como el caso de la Unión Europea que el 17 de mayo de este 2019, anunció que ya se aprobó un régimen para sancionar los ciberataques y se encuentra trabajado conjuntamente en el proceso de atribución de éstos a algún país, ya que la Unión no posee esa facultad.

REFERENCIAS

Abril, C. G. (2010). *El cuarto bios. Estudios sobre comunicación e información.* Madrid, España: Editorial Complutense.

Baralt B. N. (2017). Ciberseguridad: Un reto para la Defensa Nacional en entornos intangibles. *Revista Seguridad, Ciencia & Defensa. 3* (3): 53-71. Recuperado de www.insude.mil.do

Carrasco, L. de S. (2015). Ciber-resiliencia, documento de opinión en web, 15 p.p. *IEEE.ES.* Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf

CNDH. (2015). *Derecho humano de acceso a la información.* Instituto Nacional de Estudios Históricos de las Revoluciones de México. Recuperado de http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/foll_DHAccesoinformacion.pdf

Critifense. (2018). *Critical infrastructure cyber attack timeline*. Recuperado de http://www.critifence.com/papers/attack-timeline/files/SCADA%20Cyber%20Attacks%20Timeline

Directiva 2008/114/CE del Consejo (Unión Europea) (2008). *Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.* Siario oficial de la Unión Europea. Recuperado de https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

Estrategia Nacional de Ciberseguridad México (ENC). (2017). 31 p.p., México. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Feffrey C. (2012). *Inside Cyber Warfare.* Second edition. United States of America: O'reilly Media.

Harán J.M. (2018). Los ciberataques dirigidos a bancos más importantes de los últimos tiempos. ESET, welivesecurity. Recuperado de https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/

Ley 8. (2011). Medidas para la protección de las infraestructuras críticas. 11p.p., Jefatura del Estado, «*BOE*» núm. 102, de 29 de abril, Referencia: BOE-A-2011-7630, España. Recuperada de https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

Ley de Seguridad Nacional. (2005). México. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf

Ley Federal de Telecomunicaciones y Radiodifusión. (2014). México. Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_311017.pdf

Ley Orgánica de la Administración Pública Federal. (1976). México. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/153_120419.pdf

Morán E. A., Servín C. A. y Alquicira G. O. (2013). TIC (internet) y ciberterrorismo. Artículo digital, I, II y III, a través de la revista. *Seguridad*, UNAM, México. Recuperado de https://revista.seguridad.unam.mx/numero23/tic-internet-y-ci- berterrorismo

OEA. (2010). *Definición de e-gobierno*. Recuperado de http://portal.oas.org/Portal/Sector/SAP/DepartamentoparalaGesti%C3%B3nP%C3%BAblicaEfectiva/NPA/SobreProgramadeeGobierno/tabid/811/Default.aspx

OEA. (2014). *Tendencias de seguridad cibernética en América Latina y el Caribe.* Recuperado de https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

OEA. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?.* Informe Ciberseguridad 2016. Banco Interamericano de Desarrollo. Observatorio de la Ciberseguridad en América Latina y el Caribe. Recuperado de https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

OEA. (2018). *Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe.* Recuperado de https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

ONU. (1945). Carta de las Naciones Unidas. Recuperada de http://www.un.org/es/documents/charter/

Pádinger G. (2018). *Ciberataques a bancos latinoamericanos y el fantasma norcoreano: los afectados en 2018 y las amenazas para 2019.* Infobae, España. Recuperado de https://www.infobae.com/america/tecno/2018/12/22/ciber-ataques-a-bancos-latinoamericanos-y-el-fantasma-norcoreano-los-afectados-en-2018-y-las-amenazas-para-2019/

UIT-T X.1205. (2008). *Seguridad en el ciberespacio – Ciberseguridad, aspectos generales de la ciberseguridad, Sector de Normalización de las Telecomunicaciones de la UIT.* Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad Recomendación UIT-T X.1205. Recuperada de https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-S&type=items

UIT–T X.1205. (2010). *Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. Actualidades de la UIT. Decisiones de Guadalajara*. Recuperado de https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

Vicioso H. J. (2015). La sanidad se prepara para un ataque terrorista. *Revista Médica,* España. Recuperado de http://www.rmedica.es/edicion/260/la-sanidad-se-prepara-para-un-ataque-terrorista

"CIBERDEFENSA AEROESPACIAL"

Aerospace cyber defense

Recibido: 21 / 08 / 2019 Aprobado: 31 / 10 / 2019

Comandante
José Igancio Pérez Benítez
España

El autor es comandante del Cuerpo General del Ejército del Aire Español. Actualmente Jefe de la Sección de Defensa del Centro de Apoyo Técnico Avanzado del Ejército del Aire. Oficial especialista en Informática y Controlador de Tránsito Aéreo. Ingeniero Técnico en Informática de Gestión por la Universidad Carlos III de Madrid. Supervisor de Seguridad de Sistemas con formación avanzada en ciberdefensa y específica en sistemas medios. Tiene experiencia en Control de Tránsito Aéreo, gestión de seguridad de las TIC, acreditación y conformidad de Sistemas, gestión INFOSEC/COMSEC, gestión de proyectos de desarrollo de software embarcado, análisis de riesgos y administración de sistemas. Entre sus destinos, el Centro Corporativo de Explotación de Apoyo, el Centro Superior de Estudios de la Defensa Nacional, NATO E-3A Component, el Centro de Informática de Gestión y la Dirección de Ciberdefensa del Ejército del Aire.

RESUMEN

Las amenazas cibernéticas en la aviación civil y militar son una realidad en un ámbito global cada vez más tecnificado. Algunas de ellas son compartidas con otros sectores de la industria, pero otras son específicas de la aviación. Esas amenazas pueden afectar a la seguridad en vuelo creando problemas en el control de tráfico, provocando maniobras anticolisión, distracciones, incremento de la carga de trabajo de pilotos y controladores, desconfianza en el sistema afectado y en las tripulaciones o, en el peor de los casos, un accidente aéreo. Los investigadores han demostrado vulnerabilidades en distintas tecnologías inalámbricas muy usadas por las aeronaves que carecen de los mecanismos básicos de ciberseguridad. Con la disponibilidad creciente de avanzados medios técnicos a bajo coste, surge una nueva amenaza. La necesaria interconectividad de los sistemas incrementa considerablemente el riesgo en un ámbito donde los efectos disruptivos pueden ser devastadores.

Palabras clave:
Amenaza, aeroespacial, malware, análisis de riesgos, impacto, ADS-B, GPWS, TCAS, ILS, seguridad en vuelo.

ABSTRACT

Cyber threats in civil and military aviation represent a reality in a global scope more and more technified. Some of them are shared among different industry sectors but others are specific to aviation. These threats can affect flight safety by creating traffic control problems. These threats can affect flight safety by creating traffic control problems, causing anti-collision maneuvers, distractions, increased workload of pilots and controllers, distrust of the affected system and crews or, in the worst cases, a plane crash. Researchers have demonstrated vulnerabilities in different wireless technologies widely used by aircraft that lack the basic cybersecurity mechanisms. With the increasing availability of advanced technical means at low cost, a new threat has emerged. The necessary interconnectivity of the systems considerably increases the risk in an area where disruptive effects can be devastating.

Keywords:
Threat, aerospace, malware, risk analysis, impact, ADS-B, GPWS, TCAS, ILS, safety.

INTRODUCCIÓN

Todavía parece existir la creencia de que el "Air gap" hace que una aeronave sea inmune a un ciberataque. Nada más lejos de la realidad. Se trata de un entorno en el que el ritmo de adopción tecnológica crece exponencialmente y donde los sistemas en tierra y en vuelo deben en algún momento, estar conectados de forma directa o indirecta y donde las comunicaciones inalámbricas presentan vulnerabilidades evidentes.

Una simple búsqueda en Google arroja resultados preocupantes: exfiltración de datos, multas millonarias a compañías aéreas, investigaciones que demuestran la posibilidad real de un ataque cibernético, accidentes o incidentes indirectamente provocados por malware presente en sistemas, código fuente con vulnerabilidades, hackeo de drones, etc. Todas estas noticias hay que tratarlas con la precaución que merece toda información que llega de medios no contrastados, pensando que hay muchos intereses en juego. Los fabricantes y las aerolíneas querrán mantener su reputación intacta y probablemente harán lo posible por desmentir o negar todo aquello que afecte negativamente al sector. Los gobiernos se preocuparán por mantener la credibilidad de sus capacidades de defensa a toda costa y es posible que no permitan que se conozcan fallos de seguridad en sus sistemas de armas. Por el lado contrario, los investigadores intentarán demostrar que existe un riesgo real y que es necesario actuar. En cualquier caso, a nadie le interesa mantener los riesgos por encima del umbral aceptable, especialmente en el ámbito aeroespacial.

En este ámbito las principales vulnerabilidades provienen de la condición de espacio global común, donde las amenazas pueden venir desde dentro y fuera de los espacios de soberanía. También de la elevada tecnificación y complejidad. Una aeronave moderna implica muchos sistemas embarcados con millones de líneas de código. Este incremento de complejidad supone más dificultad en todas las fases del ciclo de vida e incrementa considerablemente el riesgo de fallo lógico en cualquiera de sus componentes.

En definitiva, estamos ante un entorno complejo altamente tecnificado, interconectado y de ámbito global, donde hay que proteger no solo las aeronaves y sus sistemas embarcados, sino también los sistemas de navegación, las estaciones de control y seguimiento de satélites, los sistemas de control aéreo, los sistemas meteorológicos, las instalaciones aeroportuarias con todos sus sistemas de información asociados, los sistemas de mantenimiento y de gestión logística, los entornos de desarrollo, los canales de distribución del software, los procedimientos de actualización, la organización de la ciberseguridad, las estructuras de mando y control, etc. Se necesita una aproximación integral que permita generar la necesaria confianza a los usuarios, a los gobiernos y a las empresas.

LAS AMENAZAS CIBERNÉTICAS A LA AVIACIÓN MILITAR Y CIVIL

La evolución tecnológica ha hecho que alcanzar ese nivel deseado de ciberseguridad no resulte fácil. Un problema que destaca y que resulta inevitable en el entorno aeronáutico es el de la obsolescencia.

La obsolescencia puede definirse como la pérdida real o inminente de la capacidad de conseguir tecnología de su fabricante original. Afecta al hardware, software, firmware, drivers, interfaces o algoritmos en uso por un sistema CIS[1].

El problema radica en los ciclos de vida de los sistemas de información, es decir, del tiempo que transcurre desde que surge la necesidad del sistema hasta que otro lo sustituye. Hay sistemas aéreos diseñados para estar en servicio 30 años o más, sin embargo, los sistemas que lo soportan especialmente si usan COTS[2], tienen ciclos de vida considerablemente más cortos. Un hardware COTS tiene una vida media de 18 meses y un software COTS de 5 años, lo que puede dar una idea de la dimensión del problema.

Si nos vamos a los tiempos de diseño, podríamos decir que un sistema de armas necesita de unos 10 años en fase de diseño y desarrollo. Un sistema CIS puede necesitar entre 2 y 6 años en dichas fases, lo que significa que en ocasiones, algunos sistemas CIS ya están obsoletos antes de entrar en servicio como parte del sistema de armas que corresponda.

Existen dos tipos de obsolescencia: funcional y tecnológica.

[1]Sistemas de Información y Comunicaciones (en inglés, Communications and Information Systems)
[2]Sistemas comerciales disponibles para el público en general (en inglés, Commercial Off-The-Shelf)

La obsolescencia funcional se produce cuando cualquier elemento de un sistema no realiza la función para la que fue diseñado debido a cambios en otra parte del sistema.

La obsolescencia tecnológica se produce cuando el fabricante no da soporte al elemento por falta de continuidad, el mismo fabricante ya no existe como empresa, no se permite la distribución por guerras tecnológicas, existe falta de disponibilidad en el mercado o aparecen tecnologías disruptivas.

Un sistema obsoleto, sin la capacidad de actualización constante, pasa a ser vulnerable por definición. A partir de aquí, ninguna otra medida de seguridad tiene sentido. Solamente en un esquema de seguridad en profundidad se pueden buscar estrategias para dotar de seguridad capas sobre las que todavía se tiene control tecnológico. La obsolescencia afecta al mantenimiento, a la acreditación o reacreditación de los sistemas, es decir, a su posibilidad legal de manejar o no información clasificada, a las posibles interacciones no contempladas safety/security, etc. Es un problema muy difícil de gestionar, por lo que hay que tratar de evitarla a toda costa.

Otro problema importante es el de la cadena de suministro. Resulta lógico pensar que los fabricantes recurran a otras empresas y países para reducir costes y terminar proyectos más rápidamente. Cualquier sistema formado por subsistemas ensamblados y no fabricados va a presentar este problema. Se trata de conseguir que los canales de distribución sean seguros desde su origen. Los proveedores deberían ser capaces de aplicar las mismas medidas de seguridad a sus sistemas que se aplican en los sistemas propios, así como que la información, clasificada o no, se maneje adecuadamente y con garantías.

Si un subsistema, sistema o producto está comprometido en origen, ya sea por vulnerabilidades no tratadas, por malware, o por cualquier otro motivo, el problema se va a trasladar al producto final. Esto puede hacer que las vulnerabilidades queden latentes durante meses o incluso años esperando ser explotadas. En cualquier caso, si no se toman las medidas adecuadas, es probable que algún punto de la cadena se vea afectado por algún ataque viéndose comprometido el producto final. El problema surge cuando un fabricante de aeronaves actúa como integrador tecnológico que trabaja con proveedores que poseen limitadas capacidades de ciberseguridad, lo cual se traslada al producto final.

Resulta difícil, por no decir imposible, hacer un seguimiento de quien accede a cada sistema en todo momento, los proveedores deberán establecer relaciones de confianza basadas en marcos regulatorios y tecnológicos comunes.

Si nos centramos en el plano técnico existen múltiples vectores de ataque: actualizaciones de software de misión, de las bolsas electrónicas de vuelo, los interfaces de cabina, contenidos infectados en sistemas multimedia, falta de aislamiento efectivo entre sistemas vitales y no vitales para el vuelo, falta de supervisión de puntos de acceso y conexión, etc. Pero si hubiese que elegir uno, sin duda sería el de las comunicaciones inalámbricas.

Resulta chocante descubrir que muchos sistemas de comunicaciones inalámbricas de las aeronaves carecen de mecanismos básicos de seguridad, dejándolos expuestos a ataques. Hay que tener en cuenta que muchos de estos sistemas entran en servicio cuando la seguridad no estaba en la mente de los diseñadores. El auge de las radios definidas software[3] tiene incidencia directa en el incremento de la posibilidad de ataques a este tipo de sistemas a un coste muy bajo.

En concreto, se ha demostrado que en la mayoría de los casos, será suficiente una radio definida software, un ordenador de bajo coste, una antena, un amplificador de señal y software open-source de libre acceso para que un atacante con conocimientos y presupuesto moderados sea capaz de desarrollar ataques remotos a este tipo de tecnologías.

Los ataques pueden ser pasivos o activos. Los pasivos, en principio, no representan una amenaza real, solamente escuchan. Los fines pueden ser observación sin más agregación de datos o vigilancia y como mucho, afectan a la confidencialidad, lo cual en sí no es un riesgo directo para la seguridad ya que no interfieren con el sistema. Sin embargo, no debemos olvidar que todo ataque activo empieza por uno pasivo y puede terminar en un ataque dirigido.

[3]Radio definida por software o SDR (del inglés Software Defined Radio) es un sistema de radiocomunicaciones donde varios de los componentes típicamente implementados en hardware (mezcladores, filtros, moduladores/demoduladores, detectores, etc) son implementados en software, utilizando un ordenador personal u otros dispositivos de computación. De Wikipedia.

Se podría decir que actualmente hemos pasado de ataques de denegación tipo "jamming"[4], a ataques de falsificación tipo "spoofing"[5] mucho más peligrosos y complicados de detectar, por ejemplo, en sistemas de navegación como el GPS.

En cualquier caso, vamos a repasar algunos de estos sistemas, empezando por el ADS-B (Automatic Dependent Surveillance Broadcast).

El ADS-B es un sistema que determina la posición de la aeronave mediante navegación vía satélite y periódicamente la emite de forma inalámbrica, permitiendo que pueda usarse por otras aeronaves o por el control de tránsito aéreo y visualizar su posición y altitud en las pantallas sin necesidad de radar.

Este sistema ofrece numerosas ventajas, mejor control de tránsito aéreo, menor coste que el radar primario y secundario, mejor visualización, mejor cobertura, más precisión, etc. Es un sistema que se usa en un alto porcentaje de los aviones comerciales y con previsión de seguir haciéndolo. De hecho, un mandato de la FAA[6] requiere la instalación de un transpondedor "ADS-B Out" no más tarde del 1 de enero del 2020. Otro mandato similar de la Unión Europea entraría en vigor algo más tarde, el 7 de junio de 2020.

Este sistema emite mucha información, identificación del vuelo, identificación del avión, posición (latitud/longitud), altitudes, régimen de ascenso/descenso, ángulos y velocidad sobre el terreno, indicaciones de emergencia (cuando se selecciona algún código), etc., todo ello sobre enlaces sin cifrar, sin ningún tipo de autenticación o integridad, lo que permite manipularla o hacer spoofing [7] anto de aeronaves como de las estaciones de control en tierra.

Los ataques pasivos al ADS-B pueden hacerse, además de con los medios descritos anteriormente, adquiriendo un receptor ADS-B o acudiendo a uno de los múltiples servicios en internet que proporcionan datos ADS-B en tiempo real. Sin embargo, no son estos ataques los que preocupan.

Un ataque activo tipo sería la generación de un avión fantasma. Mediante la emisión de nuevos mensajes ADS-B de un avión inexistente (fantasma), los sistemas los van a interpretar como una aeronave real, lo cual puede llegar a forzar a realizar maniobras innecesarias para evitar una colisión.

Otro ataque sería la denegación de servicio. Usando la técnica anterior, inundar los sistemas con múltiples aviones fantasma con la intención de que los sistemas de vigilancia, de los aeropuertos o de las propias aeronaves no se puedan utilizar.

Existen otras posibilidades de ataque activo como modificación de trayectorias, generación de falsas alarmas, aeronaves desaparecidas o spoofing de aeronaves, siempre generando, eliminando o manipulando mensajes de forma aislada o en combinación con otras técnicas como manipulando transpondedores en cabina para modificar la dirección ICAO[8] y simular ser otra aeronave distinta.

Otro sistema vulnerable es el ACARS (Aircraft Communications Addressing and Reporting System), ampliamente utilizado. Se trata de un sistema del año 1978. Existe un cifrado estándar para este sistema, pero no se ha implantado de forma generalizada. Se utiliza para la transmisión de mensajes cortos entre el avión y las estaciones de tierra con distintos fines como informes de rendimiento, comunicaciones interactivas con la tripulación, planes de vuelo antes del despegue, incidencias técnicas o de otro tipo, etc.

Los ataques activos al sistema ACARS consisten en la inyección, modificación o borrado de mensajes, que puede usarse para provocar, por ejemplo, actualizaciones falsas de planes de vuelo, información meteorológica falsa, alertas innecesarias, etc.

Algunas aeronaves tienen el sistema ACARS conectado al FMS[9] lo cual incrementa considerablemente el riesgo. En concreto, en la conferencia "Hack in the Box 2013" en Amsterdam se demostró que con equipos comprados en ebay se pueden ver y manipular los mensajes y enviar código malicioso al FMS. En primer lugar, se

[4]Creando interferencias o altos niveles de ruido.
[5] Uso de técnicas a través de las cuales un atacante, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
[6] La Administración Federal de Aviación (en inglés, Federal Aviation Administration, FAA) es la entidad gubernamental responsable de la regulación de todos los aspectos de la aviación civil en los Estados Unidos.
[7]Uso de técnicas a través de las cuales un atacante, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
[8]Código de 24-bits que identifica de forma unívoca a la aeronave.
[9] Sistema de gestión de vuelo (del inglés, Flight Management System)

localiza el avión con ADS-B, luego se usan mensajes ACARS para subir malware al FMS y posteriormente manipular el sistema cambiando planes de vuelo, predicciones meteorológicas, información del avión, o incluso controlar el avión si el piloto automático está conectado.

ADS-B y ACARS son los sistemas que parecen acumular más literatura en relación con comunicaciones inalámbricas no protegidas, pero no son los únicos. El GPWS (Ground Proximity Warning System) es otro ejemplo a considerar.

El GPWS es un sistema que alerta a los pilotos sobre la proximidad del terreno, que comenzó su vida a finales de los años 60. Usa un radioaltímetro para calcular la distancia al terreno que sigue patrones estándar de frecuencia de emisión y barrido. Se usa el cambio de frecuencia y el tiempo de ida y vuelta de la señal emitida para calcular la altura sobre el terreno.

Un posible ataque consistiría en emitir una ráfaga de frecuencias simulando la señal de vuelta en el rango y momento adecuados. De esta forma se puede simular que el terreno se aproxima rápidamente. Con este tipo de ataque no se espera provocar un accidente, sino más bien una maniobra para evitar una colisión. También se podría anular el sistema mediante una denegación de servicio, que el sistema no es capaz de detectar y con ello, aumentar la posibilidad de un accidente.

Para materializar este ataque será necesario utilizar antenas direccionales que se situarían bajo la trayectoria de aproximación para transmitir las señales al radioaltímetro de la aeronave. La capacidad de despliegue dependerá de la seguridad física del aeródromo/aeropuerto y su perímetro.

Algo similar ocurre con el TCAS (Traffic Collision Avoidance System). Un Sistema de los años 80 que, con independencia de equipos en tierra, proporciona resolución de conflictos y alertas ante una amenaza de colisión aérea entre aeronaves.

El TCAS también utiliza canales de comunicación sin autenticación. En este caso, un requisito a resolver para un potencial atacante sería el alcance, ya que la velocidad de una aeronave hace que rápidamente quede fuera del mismo. Esto puede solucionarse desplegando múltiples antenas con la separación física adecuada.

En cualquier caso, la intención del atacante es emitir señales de alerta de proximidad de una aeronave inexistente para provocar maniobras innecesarias.

Un último ejemplo de comunicaciones no protegidas sería el ILS (Instrument Landing System). El ILS es un sistema de aterrizaje por instrumentos que permite que un avión sea guiado y aterrizado con precisión durante la aproximación a la pista de aterrizaje, incluso en condiciones de baja visibilidad.

El ILS se compone de equipos en tierra, que emiten las señales y equipos a bordo del avión, que las procesa y permite guiar al piloto horizontal (localizador) y verticalmente (senda de planeo) hasta la pista de aterrizaje.

Un atacante pretenderá generar lóbulos de señal falsos que repliquen los legítimos del sistema con la intención de desencadenar múltiples aproximaciones frustradas, causar que el avión toque la pista antes de lo previsto o que la sobrevuele por completo.

Lo que más dificulta este posible ataque serían las limitaciones físicas, ya que habría que situar el equipamiento próximo a la pista de aterrizaje. Es algo difícil, pero no imposible. No obstante, una vez que el avión está en el localizador, se puede generar una senda de planeo falsa, emitiendo un lóbulo con más potencia y a cierta distancia del aeropuerto, lo que es más sencillo ya que estaría fuera de la zona de protección física.

En este artículo sólo se han tratado posibles ataques a sistemas específicos. Un escenario más complejo y efectivo para un potencial hacker consistiría en combinar ataques simultáneos a distintas tecnologías.

Hemos visto que, en el plano técnico y de forma relativamente sencilla, se pueden utilizar medios accesibles para materializar distintos tipos de ataques.

Entonces, ¿qué se puede hacer para resolver o mitigar estas amenazas? ¿se puede hacer algo? La respuesta no es sencilla.

Podríamos pensar inicialmente que con aplicar medidas técnicas adecuadas ya sería suficiente. Por ejemplo, podríamos dar seguridad a las comunicaciones inalámbricas, incorporando autenti-

cación y cifrado, también podríamos pensar en utilizar siempre sistemas redundantes, es decir, duplicando sistemas para que en caso de fallo siempre haya otro disponible; resistentes, que soporten condiciones de temperatura y presión extremas, pero que también sean capaces de resistir ataques físicos o eléctricos y resilientes, que utilicen distintas tecnologías para realizar la misma función y, de esta forma minimizar los efectos de ataques dirigidos a tecnologías concretas.

Todas estas medidas técnicas aportan seguridad, pero ¿qué ocurre si el jefe de mantenimiento no registra los incidentes mecánicos? ¿Y si se actualiza el software embarcado siguiendo un procedimiento no escrito? ¿O si un técnico utiliza la memoria USB de su ordenador particular infectado para trasferir datos de misión a un sistema embarcado? ¿Y si un contrato de mantenimiento no cubre la posible incorporación de nuevas funcionalidades, o se alcanza obsolescencia funcional porque el mantenimiento no contempla la posibilidad de adaptarse a un nuevo entorno actualizado?

Podríamos empezar por mejorar los contratos de mantenimiento de los sistemas. Tradicionalmente el mantenimiento podía ser: preventivo, con revisiones periódicas se pretende identificar y detectar fallos latentes y correctivo, identificando y eliminando defectos o corrigiendo errores reales. Sin embargo, es necesario pensar en un mantenimiento adaptativo, que permita adaptar un entorno determinado a las actualizaciones de sistemas que le puedan afectar, predictivo, que permita evaluar el flujo de ejecución para anticiparse a posibles fallos y estudiar la situación actual para programar el siguiente mantenimiento en función de la situación, perfectivo, que permita incorporar nuevas funcionalidades o capacidades, mejoras de rendimiento, dependencias o mantenibilidad y evolutivo, para estar actualizado y no permitir la obsolescencia.

Vemos que además de las medidas técnicas, la revisión de los contratos también aporta seguridad. Aunque hay muchas otras áreas de mejora. En cualquier caso, lo que está claro es que hay que actuar desde distintos frentes buscando una aproximación integral. Las medidas técnicas no lo son todo, hay que pensar en normativa, organización, procedimientos, acuerdos comerciales, canales de distribución, concienciación, etc.

En este punto podríamos hacernos varias preguntas: ¿no estamos ante un problema demasiado complejo? ¿no hay una forma de tratar todos los problemas de manera holística? ¿por dónde empezamos?…

La respuesta a gran parte de todas estas preguntas la encontramos en la gestión y el análisis de riesgos.

Pero ¿qué es el riesgo? El riesgo es una estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños o perjuicios a la organización. Es decir, es una combinación del impacto que supone la pérdida total o parcial del activo y la probabilidad de que esto ocurra.

RIESGO = PROBABILIDAD * IMPACTO

Esta fórmula es importante ya que el riesgo será alto si el impacto es alto, si la probabilidad de que ocurra es alta, o si la combinación de ambos factores es alta. Por ejemplo, la probabilidad de que un sistema crítico del avión sea hackeado por personal de mantenimiento utilizando una bolsa electrónica de vuelo puede ser baja, sin embargo, el impacto producido si se materializa esta amenaza sería muy alto, por lo tanto, el riesgo será alto.

El primer paso sería hacer un análisis, ver cómo estamos para poder tomar decisiones que supondrán un coste. Esto es lo que proporciona el análisis de riesgos. Es decir, es una actividad básica cuyo resultado es un mapa de riesgos que da una idea de lo que se puede perder si se materializa cualquier amenaza.

Una vez se tiene el análisis, hay que pasar por una evaluación, para que la dirección coteje el riesgo estimado contra los criterios de la organización y priorizar las medidas que deberán adoptarse para mantener dicho riesgo bajo umbrales aceptables. Esto derivará en el correspondiente “plan de seguridad” que llevará a la práctica todo lo decidido en forma de proyectos, desarrollos y contrataciones y, como cualquier otro proyecto deberá tratar tareas, tiempos y recursos.

Algunos ejemplos de salvaguardas a aplicar podrían ser:

- Aislar funciones críticas desde la fase de diseño.
- Sistemas redundantes, resistentes y resilientes.

- Refinar los contratos con los proveedores, con respecto a:
  - Responsabilidades bien definidas.
  - Habilitaciones de seguridad[10].
  - Incorporar todos los tipos de mantenimiento.
- Realizar inspecciones de calidad.
- Elaborar un plan de concienciación.
- Incorporar autenticación y cifrado en las comunicaciones inalámbricas.
- Incorporar infraestructura de clave pública en la entrada de datos a sistemas críticos.
- Etc.

Entonces ¿ya está? ¿tenemos la solución en nuestras manos? ¿hemos encontrado la forma de abordar de forma holística la amenaza ciber en el entorno aeronáutico? De nuevo la respuesta no es sencilla.

En primer lugar, siempre conviene acudir a metodologías internacionalmente reconocidas. Entre ellas podemos citar MAGERIT, OCTAVE, CRAMM, MEHARI o SP800-30 entre otras.

Será necesario contar con herramientas que faciliten el trabajo. El análisis de riesgos es una actividad compleja, metódica y cíclica. El análisis debe hacerse tanto en la fase de especificación, como en la de desarrollo y, por supuesto, durante la operación del sistema. El problema es que no hay herramientas que traten los riesgos aeronáuticos de forma específica, o al menos el autor de este artículo no las ha encontrado. ENISA (European Union Agency for Cybersecurity) publica un inventario de metodologías[11] y herramientas[12] con plantillas de atributos que describen en detalle dichas metodologías y herramientas.

Lo cierto es que el entorno aeronáutico se enfrenta a riesgos específicos, por ejemplo, actividades interrumpidas por dependencias SAFETY/SECURITY no previstas, datos radares corruptos, saturación de procesamiento por obsolescencia de sistemas, sistemas de mantenimiento comprometidos, falta de resiliencia, resistencia o redundancia en los sistemas, uso de COTS, etc. Estos factores deben ser incorporados a herramientas específicas.

CONCLUSIÓN

Estamos ante un escenario complejo y cada vez más tecnificado donde muchos actores e intereses entran en juego. La amenaza cibernética es una realidad y representa un riesgo importante en el entorno aeronáutico.

Es de esperar que los sistemas en este ámbito sufran fallos y ataques cibernéticos. Es necesario conseguir detectar intrusiones e implementar una adecuada defensa activa y en profundidad.

Los ciberataques vienen sin aviso previo y pueden afectar a múltiples sistemas simultáneamente. Una adecuada concienciación y entrenamiento del personal implicado resulta fundamental.

Las medidas técnicas aportan seguridad, pero es necesario seguir una aproximación integral que cubra otras áreas de actuación.

Los análisis de riesgos se presentan como una herramienta básica de apoyo a la decisión. Es un primer punto de partida que permite saber que salvaguardas habría que aplicar, ya sean organizativas, procedimentales o técnicas. Es importante usar una metodología reconocida para evitar arbitrariedades.

[10]Permisos otorgados por la autoridad nacional cuando se requiera manejar, almacenar o generar información clasificada en las instalaciones del proveedor.
[11]https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods
[12]https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools

REFERENCIAS

Air Line Pilots Association, Int'l. (2017). *Aircraft cybersecurity: the pilot's perspective.* Recuperado de http://www.alpa.org/-/media/ALPA/Files/pdfs/news-events/white-papers/white-paper-cybersecurity.pdf?la=en

Berges, P. M. (2019). *Exploring the vulnerabilities of traffic co- llision avoidance systems (TCAS) through software defined radio (SDR) exploitation.* (Tesis de master). Faculty of the Virginia Polytechnic Institute and State University. Recuperado de https://vtechworks.lib.vt.edu/handle/10919/90165

Cohen, N. (2019). *When an aircraft landing system is made to enter the spoofing zone [weblog].* Recuperado de https://techxplore.com/news/2019-05-aircraft-spoofing-zone.html

Costin, A. y Francillon, A. (2012). *Ghost in the air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices (Informe técnico).* Recuperado de https://www.researchgate.net/publication/267557712_Ghost_in_the_AirTraffic_On_insecurity_of_ADS-B_protocol_and_practical_attacks_on_ADS-B_devices

EASA. (2018). *Impact assessment of cybersecurity threats (IACT) (proyecto de investigación).* Recuperado de https://www.easa.europa.eu/document-library/research-projects/easarepresea20161

Geister, R., Buch, J-P., Niedermeier, D., Gamba, G., Canzian, L. y Pozzobon, O. (2018). *Impact study on cyber threats to GNSS and FMS systems (trabajo de conferencia).* Recuperado de https://www.icas.org/ICAS_ARCHIVE/ICAS2018/data/papers/ICAS2018_0249_paper.pdf

LTG Wyche, L. y Pieratt, G. (2017). *Securing the Army's weapon systems and supply chain against cyber attack. association of the United States Army.* Recuperado de https://www.ausa.org/publications/securing-armys-weapon-systems-and-supply-chain-against-cyber-attack

Mandelbaum, J., Patterson, C., Brown, R. (2017). *The evolution of DMSMS management in DOD – there's still room for improvement.* Recuperado de https://www.ida.org/research-and-publications/publications/all/t/th/the-evolution-of-dmsms-management-in-dod-theres-still-room-for-improvement

Ro, S. (2013). *Boeing's 787 Dreamliner is made of parts from all over the world.* Recuperado de https://www.insider.com/boeing-787-dreamliner-structure-suppliers-2013-10

Sathaye, H., Schepers, D., Ranganathan, A. and Noubir, G., Northeastern University. (2019). *Wireless attacks on aircraft instrument landing systems (trabajo de conferencia.)* Recuperado de https://www.usenix.org/system/files/sec19-sathaye.pdf

Schäfer M., Lenders V., Martinovic I. (2013). *Experimental analysis of attacks on next generation air traffic communication (trabajo de conferencia).* Recuperado de https://link.springer.com/chapter/10.1007/978-3-642-38980-1_16

Smith, M., Strohmeier, M., Harman J., Lenders, V. y Martinovic, I. (2019). *Safety vs. security: attacking avionic systems with humans in the loop.* (Department of computer science, University of Oxford). Recuperado de https://arxiv.org/pdf/1905.08039.pdf

Strohmeier, M., Smith, M., Schäfer, M., Lenders, V. y Martinovic, I. (2016). Assessing the impact of aviation security on cyber power. 2016 8th International Conference on Cyber Conflict (CyCon). Recuperado de https://ieeexplore.ieee.org/abstract/document/7529437

Wolf, M., Minzlaff, M. y Moser, M. (2014). *Information technology security threats to modern e-enabled aircraft: a cautionary note.* doi:org/10.2514/1.I010156

"MANDO Y CONTROL EN EL CIBERESPACIO: MÁS ALLÁ DE LOS PUROS DATOS TÉCNICOS"

Command And Control In Cyber Space: Beyond Pure Technical Data

Recibido: 02 / 09 / 2019 Aprobado: 30 / 10 / 2019

Doctor
José R. Coz Fernández
España

José Ramón Coz Fernández es Auditor Interno Cyber en el Centro Europeo de Investigación y Tecnología Espacial (ESTEC), en Keplerlaan 1, 2201 AZ Noordwijk. de la Agencia Espacial Europea (ESA). Es Doctor en Economía por la Universidad Complutense de Madrid y Doctor en Ingeniería Informática por la UNED. Además, es Licenciado en Ciencias Físicas por la Universidad de Cantabria, Grado Máster en Economía, Graduado Especialista en Gestión Pública y Máster en Dirección de Tecnologías de la Información por el IDE-CESEM. Posee más de una docena de certificaciones internacionales en Tecnologías de la Información como CISA, CISM, CGEIT, CRISC, PRINCE, MSP, TOGAF o ITIL y varios postgrados en Telecomunicaciones. Tiene más de veinte años de experiencia en el campo de la Auditoría y la Ciberseguridad. Es, además, profesor e investigador en varias instituciones, universidades y escuelas de negocio. Ha realizado multitud de publicaciones científicas y de tecnología, es revisor de varias revistas de ciencia y tecnología internacionales, y es miembro de varias comisiones y asociaciones de auditoría y tecnologías de la información.jose.ramon.coz@esa.int.

Ingeniero
Vicente J. Pastor Pérez
España

Vicente José Pastor Pérez es Analista Principal (Compartición de Información Estratégica) y Jefe de la Sección de Soporte de Conciencia Situacional del Centro de Operaciones del Ciberespacio de la OTAN, en 7010 SHAPE, Bélgica, siendo uno de los miembros fundadores del CyOC (Cyberspace Operations Centre).También fue uno de los miembros fundadores de la Capacidad de Respuesta a Incidentes de Seguridad de la OTAN (NCIRC - NATO Computer Incident Response Capability) en la que trabajó durante casi 12 años.Es Ingeniero en Informática por la UNED y posee el Diploma de Estudios Avanzados. Se graduó en el programa de desarrollo de ejecutivos de la OTAN (NATO-wide Executive Development Programme - NEDP) en 2012. Posee diversos diplomas de posgrado entre los que podemos destacar Experto en Seguridad de la Información y Redes de Ordenadores por la UNED, Experto en la Dirección y Gestión de la Información y sus Tecnologías por la Universidad de Alcalá y Experto Profesional en la Gestión de Servicios TI mediante ITIL e ISO 20000 por la UNED. En cuanto a certificaciones, Vicente es, entre otros, Certified Information Systems Security Professional (CISSP), GIAC Certified Forensic Analyst (GCFA) y GIAC Certified Incident-Handler (GCIH). Además, Vicente es Auditor SGSI, Especialista Implantador de SGSI y Experto en Seguridad de la Información por AENOR. Entre otras organizaciones, Vicente es miembro del IEEE, la Computer Society, ISOC y el Colegio Profesional de Ingenieros en Informática de Madrid. En la actualidad se encuentra realizando una tesis doctoral relacionada con sistemas multiagente y su aplicación a la ciberdefensa para mejorar su control centralizado y la conciencia situacional vpastor3@alumno.uned.es, vicente.pastor@ieee.org.

RESUMEN

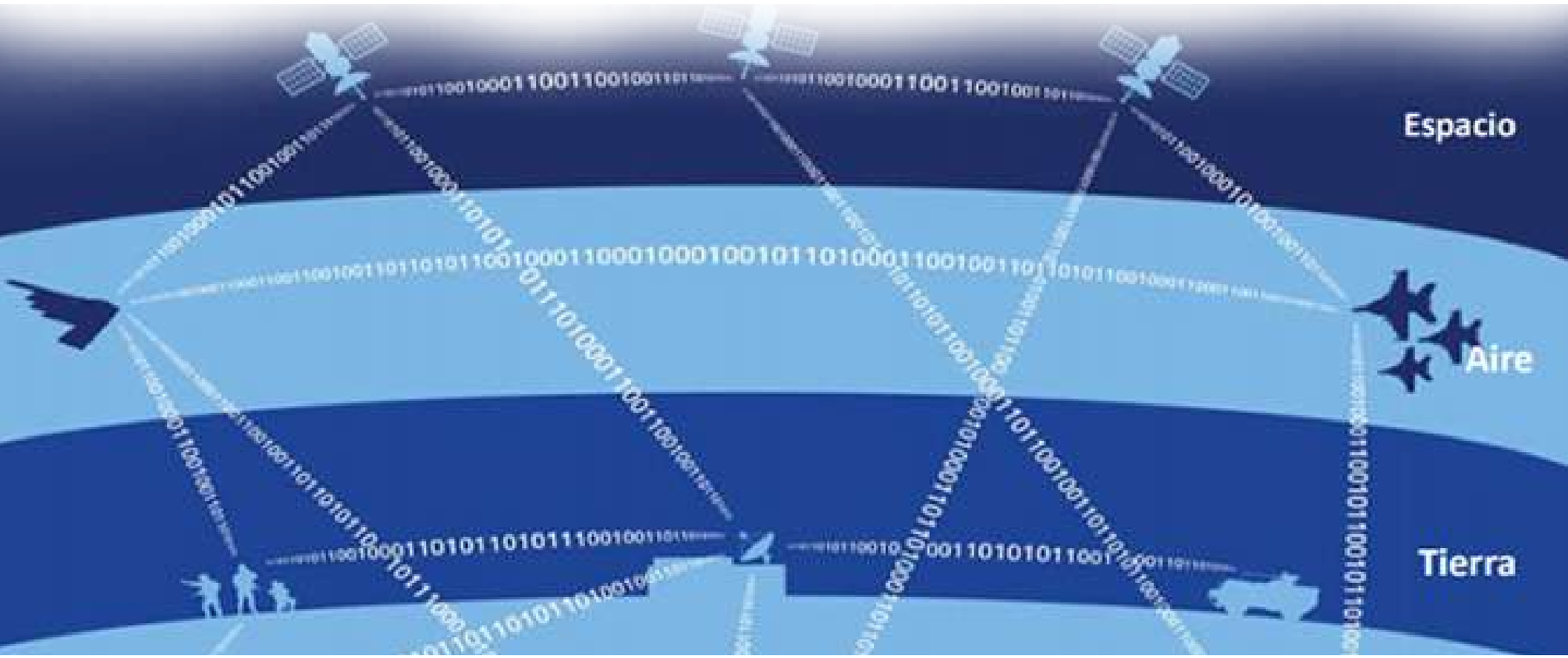
Ríos de tinta han corrido a la hora de describir los requisitos y necesidades para lograr la tan necesitada conciencia situacional en el ciberespacio. Sin el conocimiento adecuado de la situación no es posible conocer las debilidades y las vulnerabilidades presentes y tampoco es posible entender el impacto que sobre las operaciones pueden tener los incidentes accidentales o intencionados. En definitiva, se hace imposible la toma de decisiones a la velocidad adecuada y, por lo tanto, un mando y control adecuado en el ciberespacio. Los autores explican que la ciberseguridad se ha tratado como un silo aislado y, además, se ha estudiado más en profundidad la parte técnica que las dependencias existentes que son las que, en realidad, permiten una toma de decisiones adecuada.

Palabras clave:
Ciberespacio, ciberdefensa, conciencia situacional, gestión del riesgo, mando y control.

ABSTRACT

Rivers of ink have run to describe the requirements and needs to achieve the much-needed situational awareness in cyberspace. Without proper knowledge of the situation, it is not possible to know the actual weaknesses and vulnerabilities and it is also not possible to understand the impact that accidental or intentional incidents may have on operations. Finally, it is impossible to make decisions at the right speed and, therefore, an adequate command and control in cyberspace. The authors explain that cybersecurity has been treated as an isolated silo and, in addition, the technical part has been studied more in depth than the existing dependencies that are the ones that allow for adequate decision making.

Keywords:
Cyberspace, cyber defence, situational awareness, risk management, command and control.



INTRODUCCIÓN

Una vez que el ciberespacio ha sido considerado un dominio más de las operaciones militares, todo lo que hemos hecho hasta ahora en el área de la ciberseguridad y del aseguramiento de la información, se queda muy pequeño para los requisitos que aparecen en este momento. Se trata no sólo de defenderse de posibles ataques técnicos con mayor o menor impacto en las operaciones en los demás dominios, sino también de combatir dentro del ciberespacio y causar efectos en el adversario mediante acciones iniciadas en o realizadas a través del ciberespacio.

Esto hace que si los clásicos en los que se ha movido el mundo cíber, deban ahora desaparecer para entender lo que sucede en el ciberespacio como una parte de un todo mucho mayor. Los responsables de los mandos militares deben entender perfectamente las consecuencias de sus decisiones relacionadas con la parte tecnológica en todas las fases del planeamiento de sus operaciones, algo que ya se hacía hasta el momento. Pero ahora, además, tienen que entender su evolución y el cambio en el valor de los riesgos calculados durante la ejecución de las operaciones, en muchos casos debido a eventos inesperados o descubrimientos sobre las debilidades y vulnerabilidades propias o sobre las capacidades del adversario posteriores a esa fase de planeamiento.

Dos son los retos principales para poder operar en este nuevo entorno. El primero, la velocidad con la que ocurren los cambios, se conocen esos eventos o se descubren nuevas vulnerabilidades o debilidades y la necesidad de conseguir que la ventana de oportunidad del adversario sea lo más pequeña posible. El segundo reto es conseguir crear un conocimiento y, en un paso posterior, un entendimiento del ciberespacio idealmente completo pero que nosotros calificaremos de suficientemente amplio. La complejidad en este dominio creado por el hombre y que cambia a una velocidad nunca vista harán que esta tarea sea muy difícil de abordar y sus objetivos muy duros de alcanzar si no dedicamos los recursos necesarios y si no somos lo suficientemente disciplinados como para seguir unos procesos marcados de antemano.

Una vez conseguido ese entendimiento de la situación, empezando por nuestros propios sistemas y dependencias, pero luego extendido potencialmente a los del adversario, podremos entonces pasar a una siguiente fase, la de proyección de lo entendido hasta el momento para intentar predecir lo que ocurrirá y minimizar los posibles efectos. Es justo después de realizar esa proyección, cuándo estaremos en condiciones de realizar la toma de decisiones necesaria en todos estos casos.

Hasta aquí nos hemos enfocado en lo que llamaremos relaciones verticales que van desde un nivel inferior, el técnico, pasando por el nivel militar (táctico, operativo, estratégico) y llegando al nivel político. Claro que esto no es suficiente si no tenemos en cuenta lo que llamaremos relaciones horizontales, y si dejamos que el ciberespacio como nuevo dominio de las operaciones militares exista desconectado del resto de los dominios cuando la realidad es muy diferente.

Todos los dominios tienen más y más dependencia de los servicios técnicos proporcionados por las telecomunicaciones y los sistemas de información. Por esto, debemos ampliar nuestro modelo para entender esas dependencias y calcular los riesgos y sus variaciones.

La única forma de ejercer un mando y control efectivo, es tener esa visión holística que permita a nuestros comandantes militares entender las consecuencias reales de esos eventos y cambios técnicos que hemos comentado, en términos que les permitan tomar las decisiones adecuadas de acuerdo con la misión. Y es ahora el foco de todo este esfuerzo, el aseguramiento de la misión, la ejecución de acciones militares y también en el ciberespacio.

En el presente artículo, los autores tratan diversos aspectos relacionados con la ciberseguridad, comenzando por elaborar el concepto de conciencia situacional, clave para entender el resto de los procesos; posteriormente, analizando los elementos que son indispensables para su apropiada gestión; a continuación, se analizan las relaciones entre las diferentes partes, y, por último, se exponen las principales conclusiones.

LOS TRES ELEMENTOS DE LA CONCIENCIA SITUACIONAL: REDES, AMENAZAS Y OPERACIONES

El factor clave que determina la calidad del resultado de la toma de decisiones en cualquier campo es la conciencia situacional. En el ciberespacio, pese a que conceptualmente podamos estar ante un proceso maduro, su implantación no lo es del todo (Coz y Pastor, SIC F13), pues se trata principalmente de ser plenamente conscientes de la situación en la que nos encontramos y de las conse-

cuencias absolutas y relativas de cada una de las opciones frente a nosotros.

En el caso de algunos países y organizaciones internacionales, se opta por un uso holístico que aglutina multitud de capacidades, que incluyen entre otras la monitorización continua, la gestión de los problemas, los eventos y logs, los riesgos, los contenidos, las licencias, las vulnerabilidades y los parches, la protección perimetral, el aseguramiento del software y las auditorias, la gestión de la informática forense, los equipos de gestión de la respuesta y la propia gestión de la seguridad de la información (Coz y Pastor, SIC A13). Todo ello debe estar orientado a un proceso de gestión del conocimiento de los activos de información y las amenazas, y para ello es clave dotar de una compartición adecuada de la información que nos permita el intercambio de los datos y la información necesaria con diversos foros públicos y privados (Coz y Pastor, SIC N14).

Desde el Mando Aliado de Operaciones de la Organización del Tratado del Atlántico Norte (OTAN) se ha desarrollado un marco que permite caracterizar esta conciencia situacional en el ciberespacio a través de la identificación de tres elementos clave para su gestión. Estos elementos, que se pueden observar en la figura siguiente, engloban las amenazas, la situación de las redes y sistemas, y la situación de las misiones, actividades y operaciones (Ali, 2016). A continuación, en los siguientes sub-apartados, expondremos las principales características de cada uno de estos elementos. Por último, mencionaremos algunas iniciativas internacionales para el intercambio de información.

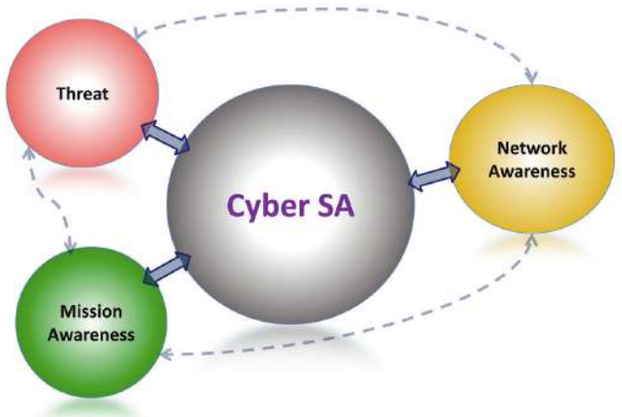


Figura 1: Marco de Conciencia Situacional del Ciberespacio de la OTAN.

LA GESTIÓN DE LAS AMENAZAS EN LA CONCIENCIA SITUACIONAL

En el caso de la gestión de las amenazas, hay que considerar diversos actores que participan, tanto dentro de las estructuras de los Estados, como fuera de ellas, incluyendo las principales fuentes de amenazas como los criminales, los activistas (en ocasiones extremistas), el personal infiltrado y los terroristas. Al hablar de ciberamenazas, normalmente se mencionan los resultados relacionados con capacidades o tácticas tecnológicas para alcanzar un determinado objetivo, pero a nivel estratégico, una de las principales metas es el conocimiento de quién está detrás de esos procedimientos técnicos, qué intentan conseguir y por qué.

Las fuentes que se pueden utilizar para obtener información sobre las potenciales amenazas son múltiples. Nosotros vamos a destacar cuatro de ellas, representadas en la figura dos:

1) Información de fuentes abiertas, tales como informes de prensa, análisis académicos o cualquier otra accesible al público en general, incluyendo la puesta en funcionamiento de herramientas de inteligencia asociadas al análisis de fuentes abiertas tipo OSINT (Open Source Intelligence), bien desarrolladas o parametrizadas ad hoc, en base a las necesidades específicas de la organización, o bien haciendo uso de herramientas o servicios comerciales dispuestas a tal fin.

2) Informes de situación y de amenazas realizados específicamente por la industria, incluyendo herramientas al efecto proporcionadas por las empresas o servicios específicos a medida, en base a las necesidades de la organización. En la mayor parte de los casos, disponer de estos informes requiere un contrato previo para su acceso. Existen multitud de opciones en el mercado en función de las necesidades.

3) Informes clasificados de inteligencia producidos en la propia organización, como pueda ser el caso de organizaciones militares o gubernamentales, que tienen sus propias capacidades para realizar esta tarea, o proporcionados por organizaciones de otros estados o fuentes públicas. En el caso de los informes elaborados por entidades estatales, en la mayor parte de los países existen Centros de Respuesta a Incidentes (CERT) que publican regularmente este tipo de informes. Incluso, en

el caso de Infraestructuras Criticas, existe una legislación, normativas y guías en muchos países y organizaciones, como en la Unión Europea, que abogan por este tipo de intercambio de información (Directiva 2008/114/CE).

4) A través de procesos de intercambio de información entre la propia organización y otros actores. Por ejemplo, en el caso de la OTAN podemos hacer hincapié en la importancia del intercambio de información a nivel militar de cada uno de los Estados miembros de la OTAN, entre sí de forma bilateral o multilateral, o mediante un modelo centralizado en el que se comparte información con la Organización para que la procese y vuelva a compartir el resultado de sus análisis con todos los Estados miembros. Unos modelos similares de compartición de la información existen también a un nivel superior (el nivel político) y a un nivel inferior (el nivel técnico). Como algunos de estos acuerdos podemos destacar la Asociación OTAN-Industria para la Ciberdefensa (NATO-Industry Cyber Partnership – NICP 2019).

Figura 2: Fuentes de información para la gestión de amenazas.

LA SITUACIÓN DE REDES Y SISTEMAS EN LA CONCIENCIA SITUACIONAL

El segundo elemento clave de la conciencia situacional, es la situación de las redes y sistemas. Lo idóneo sería la disposición de un "mapa" de todo el ciberespacio donde pudiéramos consultar los distintos parámetros de interés a nivel técnico para poder, en nuestro modelo, interrelacionar lo observado a este nivel con lo que nos interesa para nuestra misión y con las potenciales amenazas detectadas (Coz y Pastor, SIC M15).

Sin embargo, un conocimiento completo y exhaustivo del ciberespacio es un objetivo que podemos catalogar como inalcanzable. Una forma de aproximar este complejo mapa es ir recopilando toda la información disponible en diferentes "anillos" que representan nuestra distancia a cada uno de los activos (servicios, procesos y los activos de información que soportan los diferentes sistemas que los componen), de acuerdo con nuestro grado de influencia sobre ellos.

En la mayor parte de las organizaciones el "anillo" más cercano es el de los servicios y los sistemas de información que están bajo responsabilidad de la propia organización. Así que siguiendo el aforismo griego de "conócete a ti mismo", se trataría de llevar a cabo un proceso de adquisición del conocimiento de los activos propios, sus interrelaciones, las dependencias a la hora de proporcionar los servicios, procesos y la contribución de estos servicios y procesos a los objetivos globales del negocio. A modo de operación, se trataría del "reconocimiento" del ciberespacio propio organizativo, que sería el terreno más cercano a nosotros.

Por ejemplo, en el caso de la OTAN se deben de tener en cuenta "anillos" que representan los siguientes niveles: redes, sistemas y servicios propios de la Organización, de los Estados miembros, de los Estados Asociados, de las Organizaciones no Gubernamentales, de otras Organizaciones Internacionales, Internet y el total del ciberespacio.

A los adversarios, en principio esperamos encontrarlos únicamente en cualquiera de los dos anillos exteriores, pero la experiencia nos dice que asumir que esto es así está lejos de la realidad y que el adversario en multitud de ocasiones, se encuentra ya dentro de esos perímetros definidos anteriormente. Está claro que estas zonas no son círculos concéntricos, sus límites son difíciles de definir y que incluso hay solapes entre la mismas, pero aun así es una aproximación a la hora de intentar definir las diferentes áreas de responsabilidad.

Dentro del tipo de información que nos interesa conocer relacionado con las redes, sistemas y servicios deberíamos incluir el estado de disponibilidad y rendimiento de los servicios en tiempo real (lo que podríamos llamar "salud de la red"), las vulnerabilidades que sean susceptibles de ser explotadas y su impacto potencial sobre la disponibilidad, confidencialidad e integridad de la información que gestionan nuestros servicios, los eventos, los

incidentes y los ataques, con su impacto asociado, y las posibilidades que tenemos de retorno a la situación normal, la posible duración de la interrupción o el alcance de la acción llevada a cabo por el adversario. Toda esta información debemos obtenerla de las redes, sistemas, procesos y servicios propios, y de las de los demás "anillos" especificados anteriormente en la medida de lo posible.

EL ESTADO DE LAS MISIONES, ACTIVIDADES Y OPERACIONES EN LA CONCIENCIA SITUACIONAL

El último elemento clave de la conciencia situacional y probablemente el más importante, es el conocimiento en tiempo real de la situación de las misiones, actividades y operaciones que nuestra organización lleva a cabo. Generalmente los servicios de inteligencia se centran en el primer elemento (amenazas) y los servicios técnicos en el segundo elemento (técnico). Sin embargo, este elemento es el que en realidad es más necesario a nivel estratégico, y debería ser el objetivo principal de la conciencia situacional. Se trata de unir, integrar y relacionar todo lo que hemos observado en el ciberespacio con las misiones, operaciones y actividades que estamos realizando y con lo que ocurre en los demás dominios, para tener una visión lo más holística posible de la situación y poder tomar las decisiones más adecuadas en cada momento.

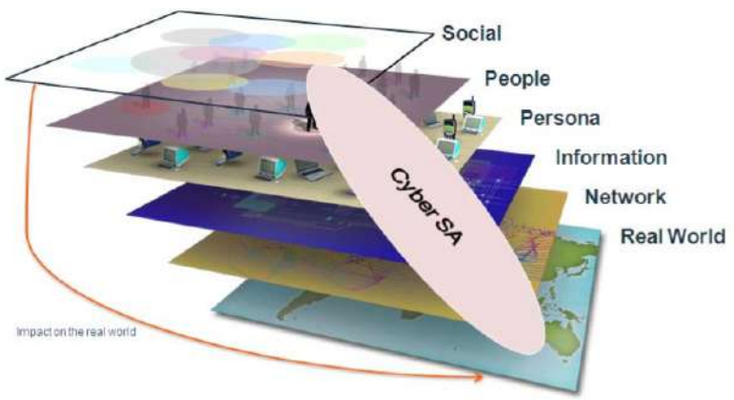


Figura 3: Lo que ocurre en el mundo virtual tiene impacto en el mundo real.

A la hora de implementar capacidades que nos permitan soportar esta visión holística, nos encontramos que la mayoría de los sistemas y herramientas disponibles que proporcionan la información de base no son interoperables entre sí, y los fabricantes de este tipo de herramientas y sistemas no proporcionan una vía nada fácil para integrar todos los productos. Es más, a nivel industrial y de competitividad, se considera como una gran desventaja abrir los datos y el código fuente de sus sistemas a la explotación por parte de terceros (Coz y Pastor, SIC F13).

No obstante, podemos destacar que existen multitud de esfuerzos por estandarizar como los realizados por la Corporación Mitre, que estructura las diferentes iniciativas de estandarización en grandes bloques: Registros, Formatos/Lenguajes, Utilización Estandarizada y Procesos Estandarizados. También hay que destacar el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de los EE.UU y sus Publicaciones Especiales, principalmente la serie 800 (SIC 113).

Por otro lado, para poder disponer de dicho conocimiento, es necesario desplegar variados sensores en muy diversos escenarios y algunas veces dispersas, localizaciones que puedan obtener todo lo que sucede en ellas y centralicen posteriormente esa información para su análisis. Ese análisis, que debería realizarse en tiempo real, supondría un acceso muy rápido a grandes volúmenes de datos, lo cual es un gran reto al que las nuevas propuestas de big data, todavía inmaduras, están intentando dar solución. Además, la recolección de los datos relevantes necesarios debería ser obtenida con un grado de fiabilidad alto, en entornos donde su configuración suele ser cambiante de manera continua. Por otro lado, también es bastante complejo el desarrollo de unas métricas que sean las adecuadas y que especifiquen claramente los umbrales a partir de los cuáles se debe o no tomar las diferentes acciones.

LA CONCIENCIA SITUACIONAL Y ALGUNAS INICIATIVAS INTERNACIONALES

Existen a nivel internacional, diversas iniciativas que tratan de minimizar los riesgos asociados a la gestión de la conciencia situacional, poniendo a disposición información muy útil sobre amenazas y otros aspectos técnicos como el Collaborative ResearchInto Threats - Investigación Colaborativa de las Amenazas (CRIT 2019). Se trata de un repositorio de información sobre malware y amenazas, basado en software abierto y soportado por una herramienta unificada para analistas y expertos en Ciberdefensa.

Por otro lado, tenemos el Collective Intelligence Framework - Marco de Inteligencia Colectiva (CIF 2019), que es un sistema de gestión de inteligencia de ciberamenazas que proporciona diversa información sobre amenazas maliciosas conocidas de diversas fuentes y su utilización para la identificación, detección y mitigación. También destacamos el Framework Mantis (análisis basado en modelos de fuentes de inteligencia de amenazas), (Mantis 2019) que apoya la gestión de la inteligencia cibernética aglutinando diversos estándares tales como: STIX, CYBOX, OPENIOC e IODEF. Finalmente, mencionaremos la Plataforma para la compartición de información sobre malware coordinada por la OTAN (MISP 2019), que reúne a diversos CERT gubernamentales.

Pero además de este tipo de iniciativas, que podemos considerar más de tipo técnico, existen otras a nivel más organizativo o estratégico como los conocidos Centros de Intercambio y Análisis de la Información (ISAC), que nacieron en Estados Unidos como consecuencia de la Directiva Presidencial 63, firmada en mayo de 1998, que reconocía el potencial dañino de los ataques tanto físicos como cibernéticos a las Infraestructuras Críticas de los Estados Unidos, y que dichos ataques podían poner en gran riesgo no sólo a la economía del país, sino también a su potencia militar. Desde entonces los ISAC se han convertido en la base de la gestión del conocimiento para la gestión de Ciberincidentes relacionados con las infraestructuras críticas públicas y privadas, no sólo en Estados Unidos, sino en todo el mundo (Coz y Pastor, SIC M15).

EL NIVEL TÉCNICO: ¿QUÉ ELEMENTOS SON INDISPENSABLES?

Como hemos comentado, el nivel técnico es en el que más hincapié se ha hecho, obviando en muchos casos el hecho de que los comandantes militares no pueden consumir la información técnica tal cual. El jefe militar necesita una imagen orientada al problema, a su nivel y los informes existentes mantienen la información escondida en extensos campos con datos no estructurados o no está lo suficientemente elaborada para que él/ella pueda entender las implicaciones de lo que está leyendo o está siendo reportado.

Uno de los problemas en el ámbito técnico es que no se dispone de datos continuos como sería de desear para una toma de decisiones casi en tiempo real, sino que únicamente recibimos informes periódicos en los que la información es inherentemente incompleta y confusa. Los flujos de información no contienen todos los datos, o parte de ellos no están contrastados y conllevan ciertas malinterpretaciones que conducen a una toma de decisiones no adecuada.

La comunicación entre partes de la organización o entre organizaciones es inconsistente e incompleta. Los sistemas y los procesos no están adecuadamente diseñados para permitir una compartición efectiva y eficiente de la información lo que hace que se creen burbujas de información que no contribuyen a esa visión global necesaria en la construcción de la conciencia situacional.

Es cierto que tampoco es fácil para los operadores técnicos que han de introducir los datos y la información a bajo nivel y que no entienden las implicaciones de no hacerlo de la manera adecuada. Pero sin una base adecuada es prácticamente imposible construir el conocimiento necesario. Sin información no hay conocimiento.

Si suponemos que partimos de una situación ideal, de cero y que no hay ningún sistema y servicio existente, los datos que son necesarios son los siguientes:

1. **Conocimiento inicial.** ¿Cómo es el diseño del sistema que necesitamos? ¿Para qué lo utilizamos? ¿Cuáles son las dependencias conocidas? Lo que estamos construyendo aquí es nuestra parte preventiva. No tocamos aún nuestra parte reactiva. Este conocimiento inicial incluye:

   a. El diseño inicial de los sistemas y servicios tanto en las fases iniciales de proyecto como en las finales de implementación, es decir, como debería ser el sistema y/o servicio.
   b. Riesgos iniciales calculados, vulnerabilidades y debilidades esperadas, gestión consciente de esos riesgos y riesgos residuales (datos teóricospara cumplir con nuestros propios requisitos de seguridad).
   c. Planes. En este caso nos referimos a la parte de explotación de esos sistemas y servicios técnicos por parte de los usuarios. Si se trata de servicios que utilizamos en el día a día, ¿para qué los usamos? ¿qué dependencia tienen nuestras actividades de esos servicios? ¿Cuál es su resiliencia? Exactamente lo mismo es aplicable a los Planes de Operaciones,

pero con los requisitos elevados que tiene una Operación Militar y teniendo en cuenta el análisis de riesgos de su nivel. En ambos casos, es necesario un conocimiento profundo de las dependencias para entender las consecuencias en cada nivel. Es necesario desarrollar ya en estas fases iniciales un plan de continuidad (de negocio, de las operaciones) con sus correspondientes planes de recuperación de desastres.
d. En esta fase inicial, necesitamos establecer nuestros sistemas de monitorización a nivel técnico, tanto los que nos reportarán sobre la disponibilidad y el rendimiento de los servicios, como los que nos alertarán de posibles incidentes de seguridad. Ambos han de ser diseñados conjuntamente, no por separado.

2. Conocimiento real. A pesar de todo nuestro cuidado en seguir nuestros propios diseños y nuestras propias políticas, la realidad nos dice que las organizaciones son imperfectas en la implementación de éstas. Eso hace forzoso disponer de un conocimiento de la realidad tal y cómo es, no cómo nos gustaría que fuese. En este apartado, estamos interesados en disponer del delta entre cómo debería ser y cómo es en realidad. Estos son los elementos esenciales:

a. Vulnerabilidades y debilidades todavía existentes a pesar de haber sido tenidas en cuenta en la fase inicial. En este punto debemos indefectiblemente realizar las correspondientes auditorías y análisis de vulnerabilidades, así como tomar las medidas correctoras necesarias y proceder a su seguimiento para cerrar el hueco entre lo real y lo planificado.
b. Control y gestión de cambios y configuraciones. Desde que diseñamos nuestras redes, sistemas y servicios, estos se encuentran en continuo cambio por motivos diversos. ¿Tiene la organización un conocimiento claro de estos cambios y de sus posibles implicaciones? El conocimiento de la situación requiere también de esta información.

3. **Conocimiento de los eventos adversos.** Una vez que conocemos la situación, digamos normal, sin influencias externas tenemos que tener en cuenta en el siguiente nivel los eventos adversos. Aquí ya estaríamos en la parte reactiva del proceso. Queremos resaltar tres tipos de estos eventos:

a. Incidentes accidentales, es decir en los que no hay intervención por parte del adversario. Son los típicos incidentes de los que se encarga la gestión de servicios de tecnologías de información. Se trata de problemas inesperados en los equipos u otro tipo de adversidades que influyen en la disponibilidad y el rendimiento de los servicios y que, por lo tanto, pueden tener un impacto notable sobre nuestras actividades.
b. La aparición de nuevas vulnerabilidades o debilidades desconocidas hasta el momento y que, por ello, no fueron tenidas en cuenta en ninguna de las dos fases anteriores. Es necesario un recálculo completo del nivel de riesgo y una toma de decisiones rápida que evite que la ventana de oportunidad sea muy grande y dé más tiempo al adversario para aprovecharla.
c. Los incidentes intencionados, los ataques, en los que es fundamental entender no sólo las implicaciones técnicas sino el objetivo final del adversario uniendo la información con la correspondiente a la amenaza y nuestra propia misión. Quizá uno de los más difíciles de entender ya que tenemos que ser capaces de reconstruir el plan del adversario con unas pocas piezas de información.

La falta de un conocimiento adecuado de la información inicial descrita en el punto 1, hace que no quede más remedio que tomar una actitud reactiva muy ineficiente y en muchos casos, también poco o nada efectiva. Cuando recibimos nueva información, digamos sobre un incidente, si el conocimiento inicial descrito es deficiente, utilizaremos la mayor parte de nuestro tiempo en intentar entender el impacto real de los eventos detectados y posiblemente jamás hallaremos qué es lo que está tratando de hacer globalmente nuestro adversario, al menos no desde la información de un simple evento.

Tenemos que saber que hemos descrito una situación ideal en la que partíamos diseñando todo desde cero. En realidad, ninguno estamos en esta situación, sino que tenemos una infinidad de sistemas y servicios ya existentes. En multitud de casos, tendremos que realizar ingeniería inversa para entender nuestras propias redes, nuestros sistemas y servicios y todas sus dependencias. Y no se trata en absoluto de tarea fácil. La complejidad es muy elevada únicamente teniendo en cuenta el nivel técnico y, si tenemos en cuenta las interdependencias con las actividades correspondientes a las misiones, la complejidad es incluso mucho mayor.

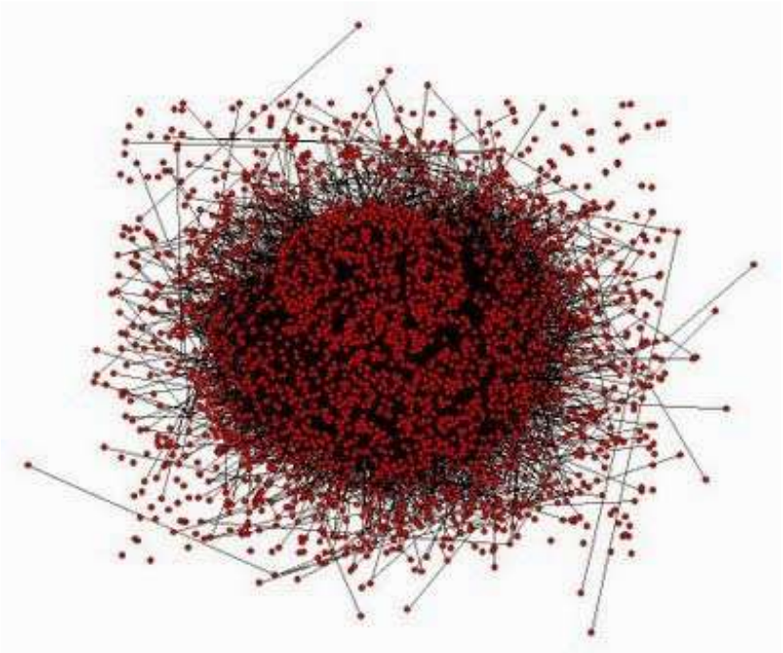


Figura 4: La complejidad dentro del nivel técnico es muy elevada.

Otro factor para tener en cuenta es la naturaleza cambiante del ciberespacio. Incluso después de realizar el esfuerzo de esa ingeniería inversa para entender nuestro entorno, eso no basta. Es indispensable mantener esa información actualizada a medida que ocurren esos cambios. Este es uno de los puntos en los que la mayoría de las organizaciones falla. La información desactualizada no sólo pierde su valor con el tiempo, sino que además puede llevarnos a una toma de decisiones deficiente e incluso peligrosa debido a que la información de la que se dispone es errónea y nuestra conciencia situacional es incompleta.

Un aspecto añadido en el que las organizaciones tienen también retos que resolver es en el seguimiento y realimentación de las acciones tomadas tras la aparición de un nuevo evento. Por ejemplo, si se determina que, tras aparecer una determinada nueva vulnerabilidad, nuestro curso de acción consiste en instalar un determinado parche, o cambiar la arquitectura del sistema o reducir la dependencia de la misión del servicio afectado, posteriormente hay que realizar un seguimiento de la compleción de esas acciones, así como recibir la realimentación respecto a la efectividad de la acción que se ha decidido tomar. De otro modo no seríamos capaces de retornar esa información para seguir construyendo el nuevo conocimiento de la situación. Se trata de un proceso continuo, cada nueva decisión y el resultado de esta influyen en una nueva instancia de la conciencia situacional.

Está claro que, sin esta conciencia situacional, que llamaremos de nivel técnico, no es posible una toma de decisiones adecuada. No obstante, el conocimiento a nivel técnico por sí mismo no es suficiente para operar en el ciberespacio. Se hace necesario un conocimiento claro de las interdependencias entre los niveles verticales de nuestra organización y una adecuada comunicación de unos con otros en ambas direcciones de manera que funcionen al unísono y sean percibidos como una sola unidad externamente.

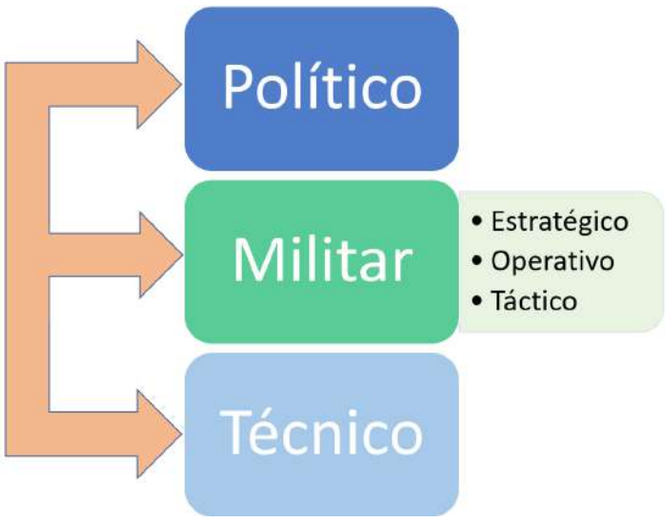


Figura 5: Relaciones verticales entre niveles para la conciencia situacional en el ciberespacio.

Cada uno de los equipos en cada uno de esos niveles dispone de un grado de conciencia situacional que ese equipo necesita para realizar su propio trabajo. Esto incluye el hecho de que los miembros de esos equipos que trabajan en el mismo nivel necesitan una conciencia situacional particular (digamos una porción de la conciencia situacional de su nivel) relativa a su cometido. El mismo escenario ocurre en cada uno de los niveles y los equipos que trabajan en un nivel diferente requieren también de su conciencia situacional particular para realizar su trabajo o conseguir su objetivo.

A esto lo llamaremos conciencia situacional de equipo. Por ejemplo, en el nivel técnico, el equipo de detección de intrusiones maneja una porción de la conciencia situacional de nivel técnico diferente a la que maneja el equipo de gestión de vulnerabilidades. Sin embargo, es necesario un conocimiento de la situación técnica único y completo para tomar decisiones adecuadas que afecten a varios equipos. En los otros niveles ocurre de manera similar.

Sin embargo, la toma de decisiones en el ciberespacio, necesita de una conciencia situacional compartida en la que las interdependencias entre los diferentes niveles sean explícitas y exista un conocimiento de la situación que permita una coordinación efectiva de las tareas entre ellos. De lo que se trata es de alcanzar un único entendimiento de la situación por medio de una comunicación efectiva y la comprensión de las interdependencias entre niveles. Es necesario unir esas conciencias situacionales de equipo en una única conciencia situacional global compartida.

EL CIBERESPACIO COMO DOMINIO DE LAS OPERACIONES MILITARES

La declaración del ciberespacio como dominio de las operaciones militares por parte de varias naciones de manera explícita, abre nuevos retos a la hora de coordinar los diferentes dominios de la guerra. Y es que, a pesar de que la mayor parte de las representaciones que encontramos, colocan los dominios uno al costado del otro, esta imagen sugiere que no hay interdependencias entre ellos y esto no es en absoluto así.

El problema es aún mayor si tenemos en cuenta la transversalidad del ciberespacio. Este dominio existe en todos los demás y requiere de una coordinación aún mayor que a la que los mandos militares estaban acostumbrados hasta ahora en las operaciones conjuntas. Así mismo, dada la naturaleza global del ciberespacio, se complica la gestión de las operaciones combinadas y se hace necesaria una colaboración con los aliados de manera continua a niveles de detalle antes reservados únicamente a crisis declaradas también en períodos donde no existe ese nivel de crisis.

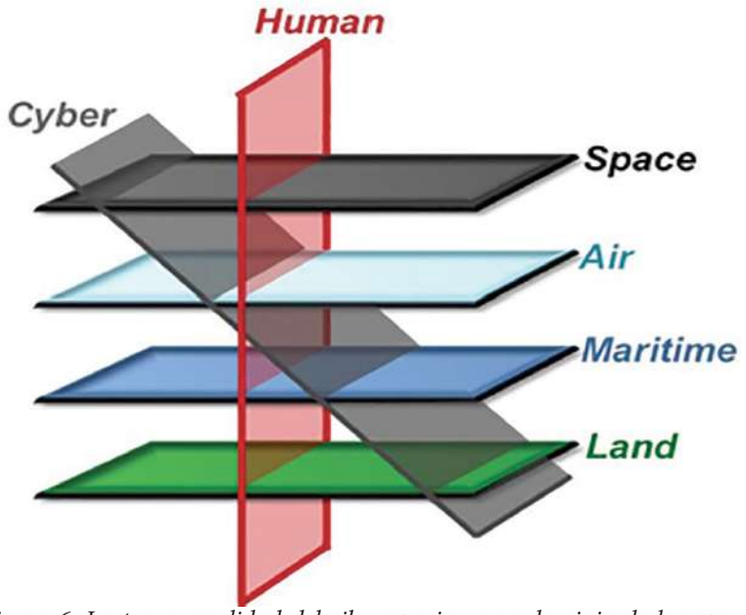


Figura 6: La transversalidad del ciberespacio como dominio de las operaciones militares.

Es por lo tanto necesario que la conciencia situacional del ciberespacio sea a la vez alimentada por la información procedente de los demás dominios y además compartida entre todos ellos, para conseguir ese único entendimiento de la situación por el que abogábamos en el apartado anterior cuando hablábamos de las relaciones verticales entre niveles.

En este caso es aún más crítico. Pensemos que la evaluación de la situación, como hemos reiterado, no puede esperar a investigar sobre partes de la información que deben estar disponibles instantáneamente. Surgen por tanto preguntas inter-dominio cuando sucede, por ejemplo, un incidente en el ciberespacio:

- ¿Se trata de un acto intencionado o un evento accidental?
- ¿Cuál es el impacto en mi dominio de operaciones?
- ¿Cuál es el impacto global en la misión?
- ¿Cuál es la situación actual?
- ¿Qué se ha hecho hasta el momento?
- ¿Quién está haciendo qué en este preciso momento? ¿Están las acciones coordinadas entre los dominios?
- ¿Cómo afectan estas acciones a mi dominio en particular? (por ejemplo, si el incidente requiere retirar un determinado

servicio para evitar males mayores)
- ¿Qué es lo que va a suceder a continuación?
- ¿Cuándo puedo esperar la vuelta a la normalidad?

Como vemos de nuevo, se trata de tener claras todas las interdependencias desde un primer momento. Como hemos dicho, la complejidad de los sistemas y servicios, la transversalidad del ciberespacio y la creciente dependencia de estos servicios en cada uno de los dominios hacen que un conocimiento absoluto de la situación sea difícil si no imposible. En todo caso, deberemos tender a que este conocimiento sea lo más completo posible so pena de afectar a la adecuada toma de decisiones.

La clave de todo ello es una conciencia situacional global y compartida que permita conocer tanto la situación de los elementos propios, como los del adversario en tiempo real y para ello necesitamos un conocimiento completo de las interdependencias que, sólo podrá alcanzarse cuando la coordinación y la comunicación tanto en vertical como en horizontal sean eficientes, pero sobre todo efectivas.

CONCLUSIÓN

Los silos clásicos en los que se ha movido el mundo cíber, deben desaparecer para entender lo que sucede en el ciberespacio como una parte de un todo mucho mayor. Ya no se trata de entender lo que ocurre en el ámbito técnico, sino también de ser capaces de extrapolar esta información y conseguir que los responsables de los mandos militares entiendan perfectamente las consecuencias de sus decisiones, relacionadas con la parte tecnológica tanto durante el planeamiento como en la ejecución de sus operaciones, y todo ello en tiempo real y de manera continua.

El factor clave que determina la calidad del resultado de la toma de decisiones, es la conciencia situacional y alcanzarla en el ciberespacio es una tarea harto complicada. Los mandos militares requieren de una conciencia situacional global y compartida entre niveles de la organización, entre los diferentes dominios operacionales e incluso entre aliados (tanto en operaciones combinadas como fuera de cualquier crisis). De esta manera se posibilita conocer tanto la situación de los elementos propios (y/o aliados), como los del adversario en tiempo real y para ello necesitamos un conocimiento completo de las interdependencias que sólo podrá alcanzarse cuando la coordinación y la comunicación tanto entre niveles verticales como en horizontalinter-dominios sean eficientes y efectivas.

Aún queda mucho camino que recorrer, hasta que se puedan estandarizar estos procesos y se comprenda claramente la necesidad de una conciencia situacional global y compartida. Por lo tanto, los esfuerzos han de concentrarse ahora en crear un modelo que soporte esas interdependencias y dé respuesta a las necesidades descritas.

REFERENCIAS

Ali, R. (2016). Cyber Situational Awareness for the NATO Alliance. *The threes words magazine,* pp 72-75.

Collaborative Research into Threats. (2019). Recuperado de https://crits.github.io/

Coz, J. R. y Pastor, V. (2013). La conciencia situacional en la ciberdefensa. *Revista SIC Ciberseguridad, Seguridad de la Información y privacidad.* 103, pp 90-92. Recuperado de https://revista-sic.es/archivo/images/pdf/sic103-colab.pdf

Coz, J. R. y Pastor, V. (2013). Retos de la conciencia situacional en la ciberdefensa. *Revista SIC Ciberseguridad, Seguridad de la Información y privacidad.* 104, pp 88-90. Recuperado de https://www.researchgate.net/profile/Vicente_Pastor_Perez/publication/265413376_Retos_de_la_conciencia_situacional_en_la_Ciberdefensa/links/544052740cf2fd72f99dd5c2/Retos-de-la-conciencia-situacional-en-la-Ciberdefensa.pdf

Coz, J. R. y Pastor, V. (2014). El reto de la compartición de información en la ciberdefensa. *Revista SIC Ciberseguridad, Segu-*

ridad de la Información y privacidad. 112, *pp* 94-98. Recuperado de https://www.academia.edu/9191724/El_reto_de_la_compartici%C3%B3n_de_informaci%C3%B3n_en_la_ciberdefensa

Coz, J. R. y Pastor, V. (2015). ISAC como nexo de unión de las arquitecturas en Ciberdefensa. José-Ramón Coz-Fernández y Vicente Pastor. *Revista SIC: Ciberseguridad, Seguridad de la Información y privacidad.* 115, *pp* 100-102. Recuperado de https://revistasic.es/archivo/images/pdf/114-colaboracion.pdf

Coz, J. R. y Pastor, V. (2015). STIX: ¿el estándar para la compartición de la información de la Ciberdefensa?. *Revista SIC: ciberseguridad, seguridad de la información y privacidad.* 113, pp 110-112. Recuperada de https://revistasic.es/archivo/images/pdf/113-colaboracion.pdf

Directiva 2008/114/CE del Consejo. (2008). *Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.* Recuperada de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008L0114

Malware Information Sharing Platform. (2018). Recuperado de https://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).pdf

Mantis. (2019). *Model-based Analysis of Threat Intelligence Sources Framework.* Recuperado de https://django-mantis.readthedocs.io/en/latest/

NATO-Industry Cyber Partnership – NICP. (2019). *Asociación OTAN-Industria para la Ciberdefensa (NATO-IndustryCyberPartnership – NICP 2019).* Fuente NATO Communications and InformationAgency. Recuperada de https://www.ncia.nato.int/Industry/Pages/NATO-Industry-Cyber-Partnership.aspx

The Collective Intelligence Framework. (2019). *Book.* Recuperado de https://github.com/csirtgadgets/massive-octo-spice/wiki/The-CIF-Book

"ENFRENTANDO LAS CIBERAMENAZAS: ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN EL CONO SUR"

Facing cyber threats: National Cybersecurity Strategies in the Southern Cone

Recibido: 09 / 09 / 2019 Aprobado: 30 / 10 / 2019

Doctora
Lucia Dammert
Chile

Doctora en Ciencia Política en la Universidad de Leiden, Holanda. Socióloga. Ha trabajado en instituciones académicas en Estados Unidos, Argentina, y Chile. En la actualidad es Profesor Asociado de la Carrera de Estudios Internacionales de la Facultad de Humanidades de la Universidad de Santiago de Chile. Ha publicado artículos y libros sobre participación comunitaria, seguridad ciudadana, conflictividad social y temas urbanos en revistas nacionales e internacionales. En el plano de la gestión pública ha participado de programas de seguridad ciudadana en diversos países de la Región. Ha realizado asesoría a diversos gobiernos entre los que destacan Chile, Argentina, Perú y México. Se desempeñó además como asesor experto en el Departamento de Seguridad Públlica de la Organización de los Estados Americanos y como Consultor Banco Interamericano del Desarrollo, Banco Mundial, Programa de Naciones Unidas para el Desarrollo, CAF, entre otros organismos regionales y multilaterales. Miembro de la Junta Directiva de UNIDIR (United Nations Institute for Disarmament Research), del Directorio del Centro de Pensamiento Espacio Público, de Asuntos del Sur y de la Fundación Junto al Barrio. Es parte del Consejo Asesor en Temas de Desarme del Secretario General de Naciones Unidas para el periodo 2017-2020 siendo la única representante de América Latina. lucia.dammert@usach.cl

Licenciada
Constanza Núñez
Chile

Licenciada en Estudios Internacionales por la Universidad de Santiago de Chile y Analista en Política y Asuntos Internacionales de la misma casa de Estudios. Actualmente trabaja temas de ciberseguridad. constanza.nunez.c@usach.cl

RESUMEN

En los últimos años, las amenazas cibernéticas han aumentado entre 30% y 40% en América Latina, posicionándose como la región en la que con mayor rapidez se presentaron este tipo de ataques. En este contexto hostil el presente artículo analiza las Estrategias Nacionales de Ciberseguridad desarrolladas por los países del Cono Sur tomando como referencia los lineamientos desarrollados por la OECD para este tipo de situaciones. Los avances son innegables, pero se concentran aún en las tareas procedimentales y discursivas, en general los países analizados se encuentran bastante desprovistos de mecanismos efectivos para enfrentar las ciberamenazas y su potencial desarrollo en el corto plazo.

Palabras clave:
Cono Sur, ciberseguridad, OECD, políticas públicas.

ABSTRACT

In recent years, cyber threats have increased between 30% and 40% in Latin America, positioning itself as the region in which this type of attack occurred most rapidly. In this hostile context, this article analyzes the National Cybersecurity Strategies developed by the Southern Cone countries, taking as a reference the guidelines developed by the OECD for this type of situation. Progress is undeniable, but they are still focused on procedural and discursive tasks, in general the countries analyzed are quite devoid of effective mechanisms to deal with cyber threats and their potential development in the short term.

Keywords:
Southern Cone, cibersecurity, OCDE, public policies.

INTRODUCCIÓN

La diversificación de los usuarios de internet ha provocado que, en los últimos años aumenten con rapidez las interconexiones globales basadas en transmisiones de alta velocidad, estableciendo relaciones cibernéticas casi instantáneas provenientes de distintos puntos del planeta, robusteciendo el mundo virtual más conocido como ciberespacio. América Latina no está fuera de este proceso, de hecho es una de las regiones donde "la población de usuarios de internet ha crecido más rápido en el mundo (OEA & Symantec; 2014: p.11). Este importante acceso a internet trae consigo múltiples factores positivos para el desarrollo de las personas, países e instituciones, tales como: Gobierno electrónico, comercio electrónico, comunicación e información instantánea, banca en línea, diversos servicios públicos y privados ejecutables vía web. Sin embargo, también genera un ambiente idóneo para la producción y desarrollo de delitos cibernéticos, puesto que las características intrínsecas de internet tales como el anonimato y la capacidad de actuar a distancia con costos limitados, permiten vulnerar el normal funcionamiento de los usuarios conectados a la red.

En América Latina y el Caribe, a nivel general, "se produjeron 253 violaciones de datos a gran escala en el 2013, lo que representó un aumento del 62% respecto del año 2012." (OEA & Symantec; 2014, p.11). Esta situación empeora cuando ponemos el foco en la sociedad civil, puesto que "ocho de estas violaciones de datos expusieron 10 millones de identidades o más cada una, lo cual obligó a comerciantes minoristas, empresas financieras y de seguros, y personas físicas a invertir una gran cantidad de tiempo y recursos financieros para responder y recuperarse de esos ataques e implementar mecanismos de protección adicionales." (OEA & Symantec; 2014, p.11). En efecto, la situación expuesta nos muestra el déficit de seguridad que hay en el ciberespacio.

La amenaza es global y requiere de respuestas de igual magnitud. Organizaciones Internacionales tales como: Organización de las Naciones Unidas[1], Organización Tratado Atlántico Norte[2], Unión Europea[3], Organización de Cooperación de Shanghái[4], Organización para la Cooperación y el Desarrollo Económico[5], Organización de Estados Americanos[6], Liga de los Estados Árabes[7] y Unión Africana[8], proponen lineamientos, estrategias y objetivos a sus respectivos países miembros con la finalidad que la seguridad cibernética cumpla estándares internacionales básicos como también elaborar un ambiente regional seguro en materia informática. Especialmente el marco propuesto por la OECD permite enfrentar las ciberamenazas desde distintos niveles de impacto así como desde múltiples perspectivas institucionales por lo que lo consideramos un marco de referencia apropiado para realizar un análisis comparado de iniciativas nacionales.

En consecuencia, en América Latina, diversos gobiernos han comenzado a elaborar o actualizar sus respectivas Estrategias Nacionales de Ciberseguridad (desde ahora, ENCS) con el objetivo de modernizar los resguardos nacionales en asuntos cibernéticos y hacer frente a las amenazas emergentes provistas por las nuevas tecnologías. De hecho, se torna vital asegurar el ciberespacio ya que es "una cuestión nacional estratégica que afecta a todos los niveles de la sociedad" (Leiva, 2015, p.163), mermando no solo el normal funcionamiento gubernamental y privado en el caso que no se tomen las medidas suficientes y a tiempo, sino que también deteriorando las relaciones entre los diversos actores que se desenvuelven en la esfera nacional e internacional. En este mismo sentido, es imprescindible el desarrollo de investigaciones que permitan comprender la nueva configuración de amenazas presentes en los temas de seguridad nacional e internacional. (Organización para la Cooperación y el Desarrollo Económico, 2012).

El presente artículo analiza las ENCS de cinco países del Cono Sur, Argentina, Brasil, Chile, Paraguay y Uruguay, a partir del marco analítico propuesto por la OECD como parámetro de comparación. El objetivo es conocer la preparación de la ciberseguridad de cada Estado mostrando diferencias y similitudes entre sus respectivas estrategias, entendiendo que los riesgos tradicionales, cada vez pierden relevancia, posicionándose otros que tienen una importante dimensión virtual sumado al constante desarrollo, por tanto, es imperativo que los Estados tomen medidas y desarrollen políticas robustas en materia de ciberseguridad (Núñez, 2019).

[1] https://www.un.org/es/
[2] https://www.nato.int/
[3] https://europa.eu/european-union/index_es
[4] http://eng.sectsco.org/
[5] http://www.oecd.org/
[6] http://www.oas.org/es/
[7] http://www.lasportal.org/ar/Pages/default.aspx
[8] https://au.int/

CIBERESPACIO, CIBERAMENAZAS Y CIBERSEGURIDAD

Desde fines del siglo XX, hemos visto cómo las nuevas tecnologías y el acceso a internet han modificando nuestras vidas desde lo más cotidiano hasta las formas más complejas de interacciones en las distintas esferas de la sociedad. De cara a la expansión tecnológica, el autor Van Bendegem (2016) reconoce que este fenómeno emergente trae serios cambios a las estructuras sociales, económicas y políticas, incluyendo una reformulación del orden mundial basado en la Paz de Westfalia.

Desde el ámbito de la Defensa Nacional, de igual manera, se reconoce una quinta dimensión. Ruiz (2010) señala, a veces virtual y a veces real, es un nuevo espacio para el desarrollo de la guerra y por ende una nueva dimensión que se debe asegurar. Esta nueva dimensión conocida también como ciberespacio es un ambiente de "grandes oportunidades, pero también es imposible ocultar que, en él, se tensionan los intereses de los Estados con fines distintos, organizaciones terroristas y redes de crimen organizado [los cuales] se sirven de las facilidades que se ofrece el medio." (Moreno y Gil, 2017, p.65) para realizar ciberamenazas.

A partir de los planteamientos de Ruiz, "podríamos definir las ciberamenazas, como aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su utilización, manipulación, control o sustracción" (2016, p.3). En relación con lo anterior, se pueden identificar al menos nueves actores los que pueden generar ciberamenazas, estos son: Estados, ciberdelincuentes, grupos terroristas, grupos yihadistas, cibervándalos, hacktivistas, actores internos, ciberinvestigadores y organizaciones privadas. (Fernández y Rodríguez, 2017). Cada uno de estos agentes, plantean sus objetivos dependiendo del sector que quieran amenazar/atacar y del nivel de peligrosidad que quieran causar. Teniendo en cuenta la diversidad de las ciberamenazas que se pueden realizar por medio del ciberespacio y lo variado que son sus ejecutores, es que se hace necesario contar con medidas de seguridad para esta nueva dimensión por medio de compromisos por parte de las instituciones para cumplir con los requerimientos básicos de ciberseguridad.

Es por ello que, Hirare propone que "la ciberseguridad constituye una condición para permitir que los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio como dimensión, en la cual las relaciones sociales puedan efectuarse en forma más rápida y económica en comparación con otras formas conocidas de intercambio de información." (2017, p.8).

De ahí la importancia de que las instituciones trabajen y colaboren para desarrollar de manera robusta herramientas políticas y técnicas que beneficien a la ciberseguridad. A nivel internacional encontramos en esta materia que distintos organismos internacionales han trabajado para fortalecer esta área entregando a los Estados líneas de acción y estrategias concretas. Algunos de estos organismos son: la Organización del Tratado del Atlántico Norte[9], la Unión Europea[10], la Unión Internacional de Telecomunicaciones[11], la Organización para la Cooperación y el Desarrollo Económico[12], la Organización de Estados Americanos[13] y Organizaciones de normalización y gestión de internet tales como: Corporation for Assigned Names and Numbers (ICANN), la Internet Engineering Task Force (IETF), la Internet Governance Forum (IGF) y la Inter-

[9] Su trabajo en área cibernética comenzó en el año 1999 en el marco de la Cumbre de Washington D.C., en la que se aprobaron importantes decisiones sobre la capacidad de defensa como en la seguridad para sistemas de comunicación e información de vulnerabilidades. (Gobierno de España, 2014) Desde la fecha se ha ampliado y fortalecido el trabajo a un ritmo acelerado debido al impacto y dinamismo de las tecnologías.
[10] Su célebre trabajo en ciberseguridad y ciberdefensa se enmarca en la Agenda Digital para Europa el cual tiene por objetivo garantizar el crecimiento inteligente de las instituciones y ciudadanos a nivel comunitario. (Gobierno de España, 2014)
[11] Desde el año 1949 es el organismo especializado en el área de las telecomunicaciones de la ONU. "Ha desempeñado un papel importante en las telecomunicaciones mundiales, en la seguridad de la información y en la definición de las normas en los diferentes dominios de las TIC." (Gobierno de España, 2014: 82)
[12] Su trabajo comienza en la década de los 80, desde ahí que este organismo internacional "ha acumulado una amplia experiencia en el debate y discusión de los diversos aspectos relacionados tanto con la seguridad de los sistemas y redes de información como de otras áreas relacionadas, incluyendo la autenticación electrónica, la política de cifrado y la protección de infraestructuras de información crítica." (Gobierno de España, 2014:83) En el año 2002 publica las Directivas de la Seguridad de las TIC, publicación que hace de esta OI uno de los más eficientes en materia de ciberseguridad.
[13] En 2004, la OEA se convirtió en el primer organismo regional en adoptar una estrategia de Seguridad Cibernética a través de la aprobación unánime de "La Estrategia Integral de Seguridad Cibernética Interamericana", que le establece un mandato a la Secretaría General de la OEA en el sentido de ayudar a los Estados miembros en la creación y el fortalecimiento de sus capacidades de seguridad cibernética." (Organización de Estados Americanos,2015:2)

net Society (ISOC)[14], son algunas reconocidas iniciativas mundiales que, hasta la actualidad, fomentan y colaboran a consolidar su capacidad de reacción y respuesta frente a amenazas a los distintos países del globo, respondiendo contundentemente a la necesidad de los Estados y de la misma Sociedad Internacional por instancias supranacionales en esta materia.

PROBLEMAS CIBER EN EL CONO SUR

Realizar un diagnóstico detallado de los delitos o ataques ciber que han ocurrido es aún una tarea pendiente debido a la carencia de registros sólidos así como a los bajos niveles de denuncia de algunos hechos (Núñez, 2019). Sin embargo, se puede afirmar que la tendencia es creciente, que los ataques se destinan a individuos, empresas e instituciones estatales y que los niveles de impunidad de los mismos son aún muy altos. A continuación se presenta un breve repaso de los principales indicadores que sirven para caracterizar la situación.

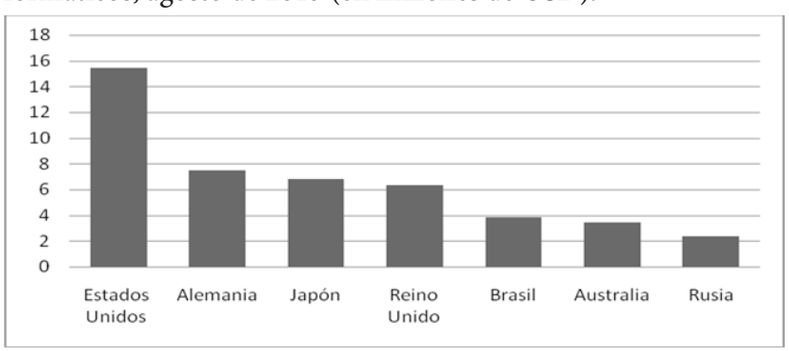
Argentina por años ha sido víctima de distintos tipos de ciberamenazas las cuales han logrado vulnerar las instituciones públicas, privadas y a cientos de ciudadanos. Uno de los más conocidos incidentes fue la modificación del discurso presidencia de Néstor Kirchner en marzo de 2005 publicado en el sitio oficial de la Presidencia de la Nación, el cual fue alterado con frases ofensivas hacia la estructura gubernamental y el sistema político. El mencionado incidente cibernético, es el inicio de una serie de ciberamenazas a los sistemas de administración pública que años más tarde se perpetrarían, viéndose atacadas instalaciones tales como: Ministerio de Economía, Infraestructura y Servicios Públicos de la provincia de Salta, Ministerio de la Producción de la Provincia de Santa Cruz, Ministerio de Relaciones Exteriores y Culto, Secretaria de Ambiente y Apoyo Sustentable de la Nación, entre otras. (Borghello y Temperini, 2013).

Con los años, las ciberamenazas en la Argentina se diversificaron, ya que los ataques no solo estaban destinados al sector gubernamental, sino también a los privados, como el sector empresarial y bancario, los cuales fueron blancos de la vulneración de sus sistemas de protección.

En el año 2017 Argentina, según datos oficiales del Ministerio de Modernización, sufrió más de tres millones incidentes informáticos siendo principalmente las empresas las protagonistas de las denuncias de ciberataques. Estos números y los afectados, muestran claramente un alza de los riesgos de internet y su vinculación a funciones fundamentales para los Estados. El alza es preocupante, debido a que entre 2016 y 2017, en Argentina los hackeos aumentaron en 700% (Dinatale, 2018).

En Brasil, el 2011 fue el año en el que se puso en jaque la seguridad cibernética del país más grande de América Latina debido a uno de los ciberataques más importantes destinado al sector público, en donde se vulneraron las páginas web oficiales de la Presidencia de la República, del Ejército, varios ministerios, y la empresa petrolera Petrobras. Post ciberataque, el servicio de gobierno que se dedica a la recolección de datos y procesamiento informó que "hubo dos millones de accesos ilegales a las páginas, más de 300.000 se produjeron de manera simultánea, en el mayor ataque de la historia de internet de Brasil." (Arias, 2011). Años más tarde, la situación brasileña parece no mejorar. En 2015, Brasil se situaba en quinto lugar a nivel mundial de los países que más pérdidas percibían por delitos informáticos, acompañando a grandes potencias tales como: Estados Unidos y Alemania, incluso superando a Rusia en pérdidas millonarias (ver gráfico 1).

Gráfico1: Volumen de pérdidas generadas por los delitos informáticos, agosto de 2015 (en millones de USD).



Fuente: Elaboración propia en base a Statista, 2019.

[14] Estas organizaciones, en su mayoría privadas y sin ánimo de lucro, han estado promoviendo y desarrollando un espacio permanente abierto a la reflexión. Sus normas y recomendaciones han sido adoptadas por la comunidad de usuarios de Internet, lo que constituye una herramienta importante en la práctica de la administración y el desarrollo técnico."(Gobierno de España, 2014:85)

Uno de los problemas más persistentes que ha tenido Brasil en cuanto ciberamenazas ha sido el ciberespionaje, así lo revelaron las filtraciones de Edward Snowden, el ex trabajador de la Agencia Nacional de Inteligencia de Estados Unidos (NSA, por sus siglas en inglés) el cual denunció que la NSA espiaba las comunicaciones de personas, gobiernos, empresas, organizaciones internacionales y cualquier usuario que estuviera conectado a la red. Brasil fue uno de los mayores afectado de este proceso debido a que este país "hospeda unos de los cables[15] de fibra óptica más grandes e importantes, aquellos por los que se transfieren los correos electrónicos, tuits o fotos de muchos usuarios de internet en el mundo" (Pardo, 2013).

Sin duda, el ciberespionaje estadounidense a las infraestructuras críticas de la información de Brasil dejó en evidencia las graves falencias en ciberseguridad. Si bien el gobierno brasileño ha reaccionado con cambios normativos dirigidos principalmente a atender estos incidentes y así tratar de evitar episodios similares y proteger información estratégica. El tamaño del mercado que suma más de 140 millones de usuarios conectados a la red, equivalentes al 66% de la población; torna esta tarea en un desafío permanente (Moreno, 2018).

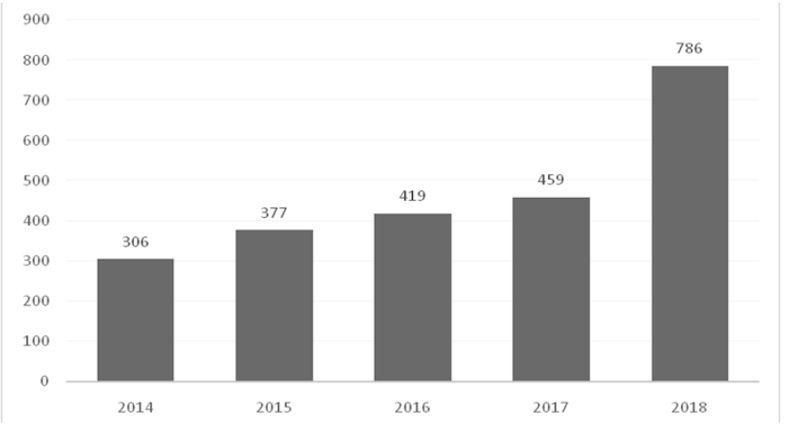
En Chile, desde que el 2000 se incrementó el acceso a internet, ha sido blanco de diversos ciberataques en su mayoría destinados a robar información para cometer fraudes económicos. Si bien estos delitos informáticos en los primeros años eran puntuales, con el paso del tiempo se han convertido en una amenaza más transversal. En el Cyber Monday de 2016, Chile ocupó el quinto lugar en el continente con mayores intentos de ataque repercutiendo en la calidad del servicio (El ciudadano, 2017).

Paraguay, uno de los países más pequeños del mundo, formó parte del listado de los 180 países ciberatacados por el ransomware WannaCry (Frieiro, Pérez y Pascual, 2017) un ataque informático que explota las vulnerabilidades del sistema operativo Windows de Microsoft. El mismo logró encriptar los datos e información crítica de las instituciones gubernamentales, solicitando un pago económico por medio de la criptomoneda Bitcoin para recuperar la información adquirida ilegalmente.

Paraguay, al igual que el resto de los países afectados, maneja sus oficinas públicas con el sistema operativo Windows, por lo que no fue complejo introducir el ransomware de forma transversal (Frieiro, Pérez y Pascual, 2017). El caso paraguayo, si bien no fue tan generalizado como en otros países, igual instaló preocupación e incertidumbre respecto a la capacidad de vulneración de sus sistemas de protección de datos. Uno de los ciberdelitos más reconocidos en este país, es la extorsión sexual hacia menores de edad por medios virtuales. Estos ciberdelitos, que invaden los terrenos más privados de los usuarios de internet, se cometen infectando, a través de un programa informático malicioso, los dispositivos conectados a la red tales como: celulares, Tablet, computadores, notebook, incluso, Smath TV (Segura, 2018).

Uruguay también ha sido víctima de las ciberamenazas. El Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay (CERTUY) cada año publica las estadísticas de los incidentes registrados desde 2014, con la finalidad de observar la tendencia de amenazas cibernética y poder actuar oportunamente (ver gráfico 2).

Gráfico 2: Número de ciberataques, Uruguay, primer semestre 2014-2018.



Fuente: Elaboración propia en base a los datos de CERTUY.

[15] Los cables submarinos se construyen entre ubicaciones que tienen algo "importante para comunicarse". Europa, Asia y América Latina tienen grandes cantidades de datos para enviar y recibir desde América del Norte. Esto incluye a los operadores de la red troncal de Internet que garantizan que los correos electrónicos y las llamadas telefónicas estén conectados, y los proveedores de contenido que necesitan vincular sus centros de datos masivos entre sí. Esto explica por qué hay tantos cables a lo largo de estas rutas principales. (TeleGeography, 2019)

En el año 2015, hubo un incremento del 23,2% en los incidentes respecto al mismo periodo del año anterior, siendo el Phishing/Spam (36%) y la mala configuración de Hardware/Software (20%) los incidentes más detectados a nivel nacional. (Centro Nacional de Respuesta a Incidentes de Seguridad Informática, 2015). Para 2016 la situación era aún más crítica ya que las instituciones públicas y el sector privado, hasta la fecha, no había recibido tantos ciberataques como ese año. (Natalevich, 2017). En ese mismo año se registraron un total de 768 incidentes a la seguridad informática uruguaya, de los cuales 15 tomaron la categoría de "Alta" mientras que otras seis se manifestaron como incidente de "Muy Alta" categoría. (Centro Nacional de Respuesta a Incidentes de Seguridad Informática, 2016).

Se estima que el crecimiento en la cantidad de ciberataques de Uruguay respondió a múltiples factores de los cuales se destacan: un ambiente generalizado de ciberataques en el mundo, y la implementación de nuevos sistemas y herramientas para la detección de riesgos cibernéticos a nivel nacional.

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD

Las ENCS buscan responder a las nuevas necesidades de seguridad en el ciberespacio. Si bien hay diversas definiciones, consideramos que son "un plan de acción nacional sobre la base de una visión nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio" [Luiijf et al., 2013]. Se encuentra a un alto nivel en la pirámide organizacional de una nación, y establece una serie de objetivos nacionales y prioridades que deben alcanzarse en un plazo determinado. Como tal, proporciona un marco estratégico para la implementación de un Sistema de Ciberseguridad Nacional, que se entiende como un conjunto de órganos, organismos y procedimientos que permiten la dirección, control y gestión de la Ciberseguridad. (Leiva, 2015, p.163).

Por su parte, la OECD, en su informe Cybersecurity Policy Making at a Turning Point, nos señala que el objetivo de las ENCS es "aumentar la coordinación gubernamental al nivel de políticas y operaciones así como clarificar los roles y responsabilidades de cada institución" (2012, p.9). Ambas definiciones ponen énfasis en el hecho que las ENCS solo incluyen a los órganos pertenecientes a la estructura estatal, sino también definen el rol que cumplen los actores privados y la sociedad civil en esta materia, para que se gestione una efectiva ciberseguridad, en la que la cooperación, la coordinación y los acuerdos son fundamentales.

Después del 2010 los países latinoamericanos han empezado a desarrollar sus políticas para enfrentar este nuevo fenómeno.

En la tabla 1 se describen las ENCS de los países estudiados así como su año de publicación, en la mayoría de casos son de años muy recientes.

Tabla 1: Estrategia Nacional de Ciberseguridad.

País	Nombre de la Estrategia Nacional de Ciberseguridad	Año de publicación
Argentina	Estrategia Nacional de Ciberseguridad	2015
Brasil	Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal	2015
Chile	Política Nacional de Ciberseguridad	2017
Paraguay	Plan Nacional de Ciberseguridad de Paraguay	2017
Uruguay	Agenda Uruguay Digital 2020	2016

Fuente: Elaboración propia, 2019.

Argentina

Argentina se distingue por ser uno de los primeros países de la región en desarrollar un Equipo de Respuesta ante incidentes de seguridad cibernética (CSIRT Argentina). (BID & OEA, 2016). Su funcionamiento comienza a fines de siglo XX, específicamente en 1994, sin embargo, no era mucho el trabajo que en esos años podía realizar debido a que era incipiente la apertura de internet. Para una gestión más eficiente, en 2011 el CSIRT Argentina pasa a ser parte del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. (BID & OEA, 2016). Dicho programa vinculado al Ministerio de Defensa, aparte de encargarse de mantener un registro centralizado de las ciberamenazas y de las respuestas de las Fuerzas Armadas frente a estos incidentes, también se encarga de la coordinación de los diversos actores y partes interesadas para la elaboración de una contundente ENCS.

Debido al contexto de ciberamenazas, sumado a la vulnerabilidad de la infraestructura crítica nacional, se pone en un proceso la elaboración de una ENCS más integral, incluyendo otros ministerios y subsecretarías en materia de seguridad cibernética en el

año 2015. Desde entonces, Argentina se ha encargado de elaborar un marco jurídico que proporcione facultad a distintos órganos gubernamentales, con la finalidad de ampliar las respuestas ante las amenazas cibernéticas y romper con la única y tradicional respuesta punitiva frente a estos delitos. Uno de los hechos más importantes que mostró el nuevo camino que la ciberseguridad estaba tomando en el país trasandino fue la creación del Ministerio de Modernización, el cual trabaja con cinco ejes: Modernización Administrativa, Gobierno Abierto, Capital Humano, Infraestructura Tecnológica y Ciudadanía Inteligente. (Ministerio de Modernización, 2019). Este ministerio, en definitiva, llega a enriquecer la oferta ministerial y gubernamental en materia de ciberseguridad. Así desde 2017 el Gobierno argentino trabaja con representantes de los Ministerios de Modernización, Defensa y Seguridad, y Ministerio Público Fiscal conformando el Comité de Seguridad con mira a generar una cultura de ciberseguridad.

Brasil

En el año 2015, en el mandado de la ex Presidenta Dilma Rousseff (2011- 2016), se publica la Estrategia Nacional de Seguridad de las Comunicaciones de Información y Seguridad Cibernética de la Administración Pública Federal 2015 – 2018, la que tiene como misión "fortalecer a política e o planejamento de segurança da informação ecomunicações e de segurança cibernética na Administração Pública Federal, visandoassegurar e defender os interesses do Estado e da sociedade para a preservação dasoberania nacional."[16](Departamento de Segurança da Informação e Comunicações. [DSIC], 2015, p.37)

Para cumplir con lo anterior, la Estrategia de Ciberseguridad de Brasil plantea principios norteadores los cuales ayudarán a direccionar las acciones a nivel nacional respecto a la ciberseguridad. Se plantea un órgano central y un sistema nacional (DSIC, 2015) que realice coordinación, seguimiento y evaluación de la implementación futura de la Política Nacional de SIC y SegCiber. Para ello, la estrategia considera indispensable establecer la definición de gobernanza (DSIC, 2015) en los sistemas de seguridad cibernética para aunar a los múltiples actores y de esa forma, contribuir con la formulación de la Política Nacional de Seguridad de la Información y Comunicaciones de Seguridad Cibernética.

De igual modo, la ENCS de Brasil plantea desarrollar la capacidad de posicionamiento y de respuesta de la nación (DSIC, 2015), entendiendo que existen amenazas cibernéticas que constantemente evoluciona. De ahí que, es necesario la articulación y alianzas entre los sectores públicos y privados, y la cooperación nacional e internacional, para el fortalecimiento de los temas cibernéticos.

La estrategia hace hincapié en las delimitaciones de la Soberanía Nacional (DSIC, 2015), garantizando recursos continuos y adecuados para la protección de Brasil y sus infraestructuras críticas. Finalmente, se plantea la importancia de resiliencia (DSIC, 2015), la cual busca la superación de incidentes cibernéticos, contribuyendo con el aumento de la capacidad de las infraestructuras destinadas a la ciberseguridad.

Chile

En el segundo periodo de la presidenta Michelle Bachelet (2014-2018), se planteó la necesidad de contar con una Política Nacional de Ciberseguridad (PNCS) la cual entregara protección a los usuarios privados y públicos contra posibles incidentes cibernéticos que vulneren la protección de la privacidad de los ciudadanos. (Bachelet, 2014). Para responder a tal necesidad, en el 2015 fue creado el Comité Interministerial sobre Ciberseguridad el cual dentro de sus funciones, debía asesorar al Presidente de la República en materia de seguridad cibernética, proponer una política nacional de ciberseguridad identificando amenazas del ciberespacio tanto global, regional como nacional, encargarse de la coordinación de acciones y planes de los distintos actores y partes interesadas, como también analizar la legislación vigente, proponiendo modificaciones constitucionales, legales y reglamentarias necesarias. (Viollier, 2017).

En el año 2017, la PNCS llega para resguardar la seguridad de las personas en el ciberespacio por medio de garantizar un nivel de seguridad el cual permita el normal desarrollo de las actividades. La idea, es proteger la seguridad del país como de sus habitantes, resguardando las redes y los sistemas informáticos del sector público y privado. También busca la colaboración, coordinación entre las instituciones gubernamentales, organizaciones y entidades privadas, como también la cooperación con otros países y orga-

[16] Traducción propia: Fortalecer la política y la planificación de seguridad de la información y comunicaciones y de seguridad cibernética en la Administración Pública Federal, con el objetivo de asegurar y defender los intereses del Estado y de la sociedad para la preservación de la soberanía nacional.

nismos internacionales, para que el análisis y gestión de las ciberamenazas sea más rápida, generando capacidades de prevención, respuesta y recuperación ante incidentes cibernéticos.

Es por lo anterior, que los objetivos de la PNCS se dividen en dos, uno de corto plazo para ser concretado en los años 2017-2018, y otro de largo plazo el cual se extiende hasta 2022. En relación con el primero, identificado como Agenda de Medidas 2017-2018, se elabora a partir de 41 medidas las cuales especifican políticas públicas a implementar y el órgano responsable de llevarlo a cabo. El segundo consta de cinco objetivos: (i) El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos; (ii) El Estado velará por los derechos de las personas en el ciberespacio, (iii) Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnología digitales; (iv) El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en fotos y discusiones internacionales; y (v) El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos." (Comité Interministerial Sobre Ciberseguridad, 2017).

Paraguay

Bajo la responsabilidad de la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs) en conjunto al Ministerio de Relaciones Exteriores y al Centro de Respuesta a Incidentes Cibernéticos de Paraguay (CERT-PY) se aprueba en abril de 2017 por el Decreto 7052 el Plan Nacional de Ciberseguridad de Paraguay, el cual se plantea como un documento estratégico que sirve para coordinar las políticas públicas de ciberseguridad y generar un ambiente cibernético seguro, confiable y resiliente, fomentando la coordinación gubernamental, la cooperación pública-privada, la cooperación internacional como también, la elaboración de un marco legal óptimo que responda a las necesidades de las Tecnologías de la Información y Comunicación.

El Plan, cuenta con seis principios orientadores para la ciberseguridad en Paraguay, los cuales buscan impulsar un cambio cultural a nivel social y gubernamental basado en el uso responsable y seguro del ciberespacio. De igual manera, desde la agenda económica, buscan el progreso y la innovación de la nación, por medio de ambiente favorable para el crecimiento, desarrollo y competitividad para con las tecnologías. (Secretaría Nacional de Tecnologías de la Información y Comunicación [SENATICs], 2017). Para lo anterior, es fundamental la cooperación y coordinación entre el sector público y privado.

Cabe destacar que el Plan tiene una duración de tres años, es decir, cada tres años este será nuevamente evaluado por una comisión interdisciplinaria para ser actualizado y evolucionar al igual que evoluciona el ciberespacio. La idea es que el país paraguayo cuente con una estrategia congruente a las demandas de las personas, las organizaciones nacionales e internaciones como a las del sector público y privado.

Uruguay

La Agenda Uruguay Digital 2020 es el instrumento por el cual el gobierno busca un desarrollo tecnológico bajo el lema 'transformación con equidad'. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, de la Presidencia de la República, es la entidad encargada de impulsar los objetivos y estrategias en base a los actores a quienes se busca beneficiar a través de medidas o políticas públicas. Frente a lo anterior, el Consejo para la Sociedad de Información, es el órgano que orienta los procesos de elaboración y priorización de las metas, así como el monitoreo y evaluación.

La elaboración de dicha agenda en el año 2016 significó el esfuerzo de distintos actores de la sociedad pertenecientes al sector público y privado, la academia, la sociedad civil organizada entendida en tecnología y la comunidad técnica (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay [AGESIC], 2016), para integrar diversas iniciativas que permitan la transformación digital del país. Uno de los principales ejes de la Agenda Uruguay Digital 2020 es la inclusión y el uso sustentable de las tecnologías con el objetivo de ampliar los beneficios de la globalización a la mayor población posible, sobre todo a los sectores sociales que más dificultades tienen, por ejemplo, con la conexión a internet. La idea es generar el fortalecimiento de habilidades específicas para la ciudadanía en general, relacionadas con los dispositivos tecnológicos, la incorporación plena de la tecnología en sectores productivos y empresariales, como profundizar y fortalecer el vínculo ciudadanía-Estado. (AGESIC, 2016)

COMPARACIÓN ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD

Tomando como marco de referencia los indicadores de ciberseguridad de la OECD analizamos las ENCS de los países del Cono Sur. En la tabla 2 se presentan los indicadores de ciberseguridad agrupados según sus fines, ya sean de: Protección, Cooperación y/o Estratégicos. La información relevada en cada caso será analizada en los párrafos posteriores.

Tabla 2: Análisis comparado de Estrategias Nacionales de Ciberseguridad.

	INDICADORES DE CIBERSEGURIDAD OECD / PAISES	ARG	BR	CHL	PAR	URU
Protección	Seguridad del gobierno	X	X	X	X	X
	Infraestructura de información críticas	X	X	X	X	X
	Monitoreo en tiempo real					
	Desarrollo de industrias de seguridad cibernética		X	X	X	
	Consideración de soberanía		X	X		
	Lucha contra el ciberdelito	X		X	X	X
	Respuesta	X	X	X	X	X
Cooperación	Cooperación Internacional	X	X	X	X	X
	Coordinación gubernamental - Multiagencia para un enfoque interinstitucional	X	X	X	X	X
	Cooperación público – privada	X	X	X	X	X
	Diálogo de multipartes interesadas			X	X	X
	Asociaciones con proveedores de servicios de internet (ISP)	X				
Estratégicos	Enfoque de política flexible	X	X		X	X
	Sensibilización	X	X	X	X	X
	Educación, Investigación y Desarrollo	X	X	X	X	X
	Resiliencia		X	X	X	
	Desarrollo de marcos de Identidad digital	X		X		X
	Políticas específicas para la protección de niños en línea	X			X	
	Respuesta de los valores fundamentales			X		

Fuente: elaboración propia, 2019.

Protección:

Se puede apreciar que los cinco países, en sus respectivas ENCS incluyen el indicador seguridad del Gobierno. En efecto, Argentina propone la elaboración de normas destinadas a incrementar los umbrales de seguridad, tanto en los recursos como en los sistemas que están relacionados con tecnologías informáticas del Sector Público Nacional. (Decreto N°13, 2016). Por su parte Brasil, cuenta con una agencia especializada para la seguridad del gobierno, esta es la Agencia Brasileña de Inteligencia, órgano encargado de proporcionar al presidente y a los ministros, información y análisis estratégico, necesarias para la toma de decisiones. (Agencia Brasileña de Inteligencia, s/f). Si bien, este órgano se encarga de cualquier tema que se relacione con la seguridad de gobierno, en los últimos años se ha puesto especial énfasis a las amenazas tecnológicas que pueden sufrir las estructuras gubernamentales a través del Centro de Investigación y Desarrollo para la Seguridad de las Comunicaciones, área de tecnología que desarrolla programas y herramientas para la transmisión segura de informaciones del Gobierno Federal. En cuanto a Chile, bajo el Decreto Supremo N°1 del año 2015 (Ministerio del Interior y Seguridad Pública, 2019), se establecieron normas técnicas sobre sistemas y sitios web de los Órganos de la Administración del Estado, las cuales están vigentes desde 2018 por el Instituto de Normalización (INN) para la Ciberseguridad, conducido por el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT Chile).

Respecto a Paraguay, la Seguridad del Gobierno está coordinada por los agentes representantes o responsables de cada sección gubernamental. En este indicador, Paraguay apela a la correcta función de los altos cargos, teniendo conciencia situacional referente a la ciberseguridad. (SENATICs, 2017). Por último, Uruguay, plantea un trabajo conjunto entre los órganos gubernamentales a través de mesas ante incidentes cibernéticos. Cabe destacar que, para mayor control de los bienes tecnológicos que se utilizan en el sector público, se creó el Convenio Marco, el cual consiste en una modalidad de compras estatales en donde se seleccionan proveedores de bienes, obras y servicios a través de la Tienda Virtual de Agencia de Compras y Contrataciones del Estado. (AGESIC, 2019). La idea principal de este convenio es tener pleno conocimiento de las herramientas del sector gubernamental y un control estandarizado ante eventuales incidentes, además de garantizar menor costo, mayor eficiencia y calidad en el sector gubernamental.

Respecto a la protección de infraestructura de información crítica, de igual manera, los cinco países del Cono Sur incluyen en sus respectivas estrategias este indicador. Cada país cuenta con un equipo de tratamiento de ciberamenazas vinculados a los principales órganos de seguridad de Estado. Argentina cuenta con el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT Argentina) dirigido por el Ministerio de Seguridad de la Nación. También cuenta con la Dirección Nacional de Infraestructura Críticas de Información y Ciberseguridad a cargo del Ministerio de Modernización, estas dos entidades que trabajan en conjun-

to para enfrentar incidentes cibernéticos que pongan en riesgo la información delicada para el normal funcionamiento del país. Además de contar con un CSIRT nacional, Argentina cuenta con el CSIRT de Buenos Aires, el cual se dedica a la asistencia y concientización de los ciudadanos y de los agentes de Gobierno de la capital de este país. En materia de infraestructura de información crítica, el país trasandino es el que ha desarrollado una contundente batería de leyes para responder a las necesidades cibernéticas (Disposición N°1, 2015), no es extraño si consideramos que los incidentes cibernéticos perpetrados en Argentina en los últimos años, han puesto en jaque las estructuras de seguridad de información crítica.

Lo que respecta a Brasil, este cuenta con el Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo[17] (CTIR Gov) conformado por Gendarmería Nacional, Policía Federal, Policía de Seguridad Aeroportuaria y Prefectura Naval. En un trabajo coordinado de las distintas entidades ya nombradas, tiene por objetivo coordinar la realización de acciones destinadas a la gestión de incidentes computacionales, ya sea de monitoreo, tratamiento y respuesta ante incidentes cibernéticos, en órganos gubernamentales. De igual forma, el CTIR Gov debe asesorar al Departamento de Seguridad de la Información del Gabinete de la Seguridad Institucional de la Presidencia de la República para la formulación de normativos y requisitos metodológicos en esta materia, velando por la seguridad de la información nacional. (CTIR Gov, 2019). Chile, por su parte, cuenta con el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT Chile), bajo el alero del Ministerio del Interior y Seguridad Pública. En el caso de Chile, esta es la única entidad en manejar y coordinar los incidentes y vulnerabilidad dentro del Estado, esto, para poder priorizar y responder de forma canalizada las ciberamenazas que afectan a las infraestructuras críticas como también a la infraestructura de información crítica (Ministerio del Interior y Seguridad Pública, 2019). En la misma línea, Paraguay plantea que su Centro de Respuesta a Incidentes Cibernéticos (CERT-PY), sea la institución principal en la coordinación de las notificaciones de incidentes de seguridad que sufren las infraestructuras o redes paraguayas. El CERT-PY depende de la Secretaría Nacional de Tecnologías de la Información y Comunicación, y desde ahí, además del tratamiento de las ciberamenazas a las infraestructuras, promocionan la concienciación sobre los problemas de la seguridad informática. (Ministerio de Tecnologías de la Información y Comunicación, s/f). Por su parte Uruguay, cuenta con el Centro de Respuesta a Incidentes (CSIRT-UY) integrado por la Administración Nacional de Telecomunicaciones de Uruguay (ANTEL), conformando así el CSIRT de ANTEL. La función principal del CSIRT de ANTEL, aparte del tratamiento de las ciberamenazas, es la constante capacitación, coordinación y soporte en materia de seguridad informática tanto de los sistemas de red como del personal y de la comunidad, para así mejorar continuamente los servicios de internet. (CSIRT Antel, s/f). Para apoyar lo ya mencionado, Uruguay también cuanta con el Marco de Ciberseguridad (AGESIC, 2018), el cual suministra a la normativa nacional con normativas técnicas especializada para la protección de ciberamenazas.

Respecto al indicador monitoreo en tiempo real, el cual requiere de la detección inmediata a nivel operativo de las ciberamenazas mediante el establecimiento de Centros de Operaciones de Seguridad Cibernética (CSOC, por sus siglas en inglés), ninguno de los cinco países en estudio contempla en sus respectivas estrategias este indicador.

Por su parte, el desarrollo de industrias de seguridad cibernética está contemplado por tres de los cinco países analizados, Brasil, Chile y Paraguay. En estos tres países podemos ver los esfuerzos y hechos concretos respecto a este indicador. Brasil es el líder de este estudio en desarrollo de industrias de seguridad cibernética, ya que por medio de la Agencia Brasileña de Desarrollo Industrial, Brasil ha buscado el desarrollo constante de personal capacitado para enfrentar el desarrollo tecnológico e innovación, evidenciado en, por ejemplo, las Ciudades Inteligentes y o las energías renovables de Brasil, que requieren estrictamente de fuertes sistemas de seguridad cibernética para dar protección a nivel nacional e internacional. (Agencia para o desenvolvimiento da industria no Brasil, 2019). Paraguay por su lado, en su Plan Nacional de Ciberseguridad menciona que se debe fomentar modificaciones al marco legal para cumplir con la creación y funcionamiento de unidades especializadas de TIC y ciberseguridad, no obstante, no se especifica ningún lineamiento político para alcanzar dichas modificaciones legales. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). En tanto Chile, en su PNCS, este indicador solo se plantea como un esfuerzo que el país debe

[17] Traducción propia: Centro de Tratamiento y Respuesta a Incidentes Cibernéticos de Gobierno.

realizar en el medio y largo plazo. (Comité Interministerial Sobre Ciberseguridad, 2017).

El indicador consideración de Soberanía, tiene un importante enfoque militar y de defensa respecto al reconocimiento de las amenazas cibernéticas, exigiendo políticas que fomenten la seguridad desde esta perspectiva. En las estrategias de Brasil y Chile se especifica la militarización de la ciberseguridad a través de sus respectivas Política Nacional de Ciberdefensa. En el caso de Brasil, su Política Cibernética de Defensa, es establecida por medio de la ordenanza normativa N°3.389 (Lex Magister, 2019), la cual decreta que el Ministerio de Defensa de Brasil debe orientar las actividades de defensa y guerra cibernética a nivel estratégico, operativo y táctico. Para ello las ramas castrenses, Ejército, Fuerza Aérea y Marina, cada una tienen un Centro de Defensa Cibernética preparados para responder a incidentes, especialmente provenientes desde el exterior. En el caso de Chile, bajo la responsabilidad del Ministerio de Defensa Nacional, la Política de Ciberdefensa si bien tiene un enfoque militar, tiende más bien a una perspectiva de gestión de riesgos más que una respuesta relacionada a guerras cibernéticas. (Decreto N°3, 2018). El resto de los países en estudio, no especifican en sus respectivas estrategias la consideración de soberanía.

En cuanto a la lucha contra el ciberdelito, Argentina, Chile, Paraguay y Uruguay señalan en sus estrategias el tratamiento de dichos incidentes. En Argentina, la investigación y el procesamiento de los ciberdelitos y los cibercrímenes son llevadas a cabo por la Policía Federal, a través de la División de Delitos Tecnológicos. (BID & OEA, 2016). Por su parte Chile, para este tipo de delitos cuenta con la Brigadas Investigadoras del Cibercrimen de la Policía de Investigaciones (Policía de Investigaciones de Chile, 2019) y con el OS-9 de Carabineros de Chile. En cuanto a Paraguay, el Ministerio Público, a través de las distintas divisiones especializadas en delitos informáticos de la Policía Nacional enfrenta estos incidentes que se dan a nivel de ciudadanía. Dichas divisiones son: División Especializada Contra Delitos Financieros; División Especializada Contra Delitos Económicos; División Especializada Contra Violación de Derechos Intelectuales; División Especializada Contra Delitos Informáticos, División Especializada Contra el Lavado de Dinero y Financiamientos del Terrorismo; División Seguridad Bancaria; División Especializada Contra Hechos Punibles de la Prueba Documental; División Laboratorio y Estudios Periciales. (Dirección Contra Hechos Punibles Económicos y Financieros Policía Nacional, 2015) Lo que respecta a Uruguay, en su Agenda Uruguay Digital 2020, los delitos cometidos por las redes son tratados por el CERT-UY en conjunto a la Policía Nacional. Se tiene como objetivo adecuar y actualizar el marco normativo referente a la protección de datos personales, cibercrimen, e-residuos y protección e-consumidor, para ampliar el rango de tratamiento y solución ante estos ciberincidentes. Cabe señalar que la Organización Internacional de Policía Criminal (INTERPOL) hace periódicamente capacitaciones a la Policía Nacional de Uruguay para fortalecer las estrategias punitivas en esta materia a nivel nacional e internacional. (AGESIC, 2016).

Ante el indicador respuesta, los cinco países cuentan con sus respectivos Equipos de Respuesta a Incidentes de Seguridad Cibernética ya desarrollados en el indicador de Infraestructura de Información Crítica.

Cooperación:

La cooperación en sus distintas dimensiones sea internacional, intergubernamental y o cooperación público-privada es determinante para que un país cumpla con estándares mínimos de seguridad cibernética, pues la ciberseguridad no será efectiva si solo nutrimos un marco legal entorno a lo nacional, descuidando los quehaceres internacionales en materia cibernética, ya que, como lo hemos visto en capítulos anteriores, las ciberamenazas y todo lo que se relaciona con el ciberespacio, rompe fronteras.

El Convenio de Budapest, elaborado por el Consejo de Europa, el cual entró en vigor en el 2004, fue el primer y principal tratado internacional que se propuso aunar a los estados respecto delitos informáticos. Distintos países europeos como también variados países de otros continentes adhirieron al convenio para aplicar una política penal común en materia de cibercrimen. En efecto, de los cinco países analizados, Chile en el año 2017, Argentina y Paraguay en el año 2018 adhirieron y ratificaron el Convenio de Budapest haciendo con ello vinculante las decisiones pactadas en dicho convenio y la obligación de cumplir las políticas dispuestas para enfrentar los incidentes cibernéticos. (Council of Europe Portal, 2019).

Desde un panorama más regional, se cuenta con la Organización de Estados Americanos (OEA), organización internacional que apoya a los países Americanos, entre ellos Argentina, Brasil, Chile,

Paraguay y Uruguay en materia de ciberseguridad. A través del Comité Interamericano contra el Terrorismo la OEA apoya a los estados miembros en el desarrollo de capacidades técnicas, políticas e investigación (Organización de Estados Americanos, 2019). De igual modo, mejora la coordinación de intercambio de información y la cooperación entre los países americanos brindando asistencia a los CSIRT.

Ante la cooperación internacional, también se puede mencionar que los países en estudio han firmado importantes acuerdos bilaterales en el área de seguridad cibernética. En el caso de Argentina, en el 2017 firmó con España el Memorando de Entendimiento sobre Cooperación en Materia de Ciberseguridad (Ministerio de Modernización de la República de Argentina y Ministerio de Energía, Turismo y Agenda Digital del Reino de España, 2017), con el objetivo de impulsar estrategias comunes para la protección del ciberespacio. De igual modo, en el marco del G20 realizado en Argentina en el 2018, tras un acuerdo de asistencia técnica, Israel fue el país encargado de la protección cibernética de esta cumbre que reúne los principales líderes políticos y económicos del mundo, en la cual, la probabilidad de ciberataques era realmente una preocupación para el Estado argentino. (Dergarabedian, 2018).

En cuanto a Brasil, a través del Acuerdo de Intercambio y Protección Mutua de Información Clasificada, el gran país sudamericano estableció acuerdos bilaterales con España en el 2015 (Decreto N°9.273, 2018) y con Suecia en el 2018 (Decreto N°181, 2018), con la finalidad de proteger sus respectivas infraestructuras de información crítica, como también su soberanía a nivel cibernético, principalmente para enfrentar con mayor herramientas y conocimiento el ciberespionaje de las grandes potencias. Por su parte Chile, durante el 2018 estableció dos acuerdos bilaterales de ciberseguridad, uno con España y otro con Israel (Subsecretaría de Telecomunicaciones, 2018). Ambos acuerdos apuntan al intercambio de buenas prácticas en la aplicación de estrategias nacionales de seguridad cibernética. Específicamente la relación bilateral Chile-Israel, está destinada a robustecer el tratamiento técnico y cofinanciamiento de proyectos pilotos de infraestructura crítica de cara a la revolución tecnología de la quinta generación de tecnologías de telefonía móvil (5G).

Acerca de Paraguay, si bien en su Plan Nacional de Ciberseguridad se señala la importancia de la cooperación internacional, esta se ha mantenido a un nivel de cooperación con organismos supranacionales, principalmente en foros de ciberseguridad de la ONU y la OEA, por lo que no se han desarrollado acuerdos o cooperación bilateral. Ante esta deficiencia, se plantea como uno de los principales objetivos la cooperación multi y bilateral en materia de seguridad cibernética. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Por último, en el caso de Uruguay, en el año 2017 se firmó el Acuerdo entre el Gobierno de la República Oriental del Uruguay y el Gobierno de la Federación de Rusia sobre Cooperación en Materia de Defensa (Ley N°19.607, 2018), en el cual se establecieron cooperación militar, de capacitación teórica y práctica, en temas de defensa y protección de información crítica.

Respecto a la coordinación gubernamental-Multiagencia para un enfoque interinstitucional, los cinco países plantean una coordinación y una cooperación entre los órganos gubernamentales. Argentina en su Estrategia Nacional de Ciberseguridad, cuenta con el Comisión de infraestructuras Tecnológica y Ciberseguridad permitiendo mayor coordinación en el trabajo de prevención y tratamiento de ciberamenazas (Argentina.gob.ar, 2019). En cuanto a Brasil, la función de coordinación la maneja el ya mencionado el CTIR Gov, el cual coordina la red formada por los órganos y las entidades gubernamentales (CTIR Gov, 2019). Por su parte Chile, CSIRT se hace cargo de la coordinación de los órganos del estado en conjunto al Comité Interministerial sobre Ciberseguridad. En este apartado, Chile plantea una Gobernanza para la eficiencia, calidad y buena orientación para la toma de decisiones (Comité Interministerial Sobre Ciberseguridad, 2017). Paraguay, por su lado, el CERT-PY es la principal entidad de coordinación, sin embargo, en el Plan Nacional de Ciberseguridad se platea reforzar la coordinación y cooperación intergubernamental creando procedimientos y líneas de acción específicas para el sector público, con canales de comunicación directo entre los Ministerios y Secretarías del Poder Ejecutivo. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). En el caso de Uruguay, cuenta con la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay (AGESIC), esta agencia es la que coordina todos los asuntos en materia de ciberseguridad, incluida la coordinación entre los órganos gubernamentales del país. (AGESIC, 2016).

La cooperación público – privada es de suma importancia para la ciberseguridad, debido a que los incidentes cibernéticos, en su mayoría van dirigidos a instituciones privadas afectando principalmente al sector financiero. Es por lo anterior, que, en las respectivas ENCS de los cinco países en análisis se presenta este tipo de cooperación. Aunque dicha cooperación es hasta ahora incipiente, existen avances a destacar. Argentina, en su ENCS plantea elaborar, en conjunto al sector privado, políticas que resguarden la seguridad digital haciendo hincapié en las infraestructuras críticas del sector privado que son esenciales para el normal funcionamiento de las ciudades como del país (Resolución N°580, 2011). Brasil, por su parte, para la cooperación público-privada plantea crear un ecosistema digital por medio de la articulación de las empresas y la Institución de Ciencia y Tecnología. El órgano responsable de llevar a cabo esta articulación es el Gabinete de Seguridad Institucional de la Presidencia de la República con asesoramiento del Comité Gestor de la Seguridad de la Información. (Departamento de Segurança da Informação e Comunicações, 2015). En cuanto a Chile, cuenta con cooperación público-privada por medio de la Asociación Chilena de Empresas de Tecnología de Información, de la cual se obtienen conocimientos y asesoramientos en materia de cibernética desde el sector privado hacia el sector gubernamental. (Asociación Chilena de Empresas de Tecnología de Información, 2019).

Respecto a Paraguay, la cooperación público-privada se hace por medio de asistencia técnica y teórica de operadores privados, sobre todo a las infraestructuras de críticas, viéndose reflejado en un constante trabajo en el CERT-PY. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Uruguay por su lado, en su Agenda Uruguay Digital 2020, apunta la innovación del sector privado, trabajando en conjunto al AGESIC, entregando herramientas de tecnologías, capacitaciones y programas de formación al sector privado. (AGESIC, 2016). Cabe destacar que, dentro de estos proyectos, Uruguay contempla potencia la ciberseguridad en las micros, pequeñas y medianas empresas.

Ante el indicador diálogo multipartes interesadas, Chile, Paraguay y Uruguay, en sus respectivas estrategias plantean objetivos que recogen los conocimientos de los diversos actores a los que compromete la ciberseguridad. En Chile, el CSIRT constantemente está solicitando ayuda de expertos en seguridad cibernética, ya sea del sector privado, la academia como la sociedad civil para nutrir y ampliar la capacidad de respuesta ante factores de riesgo cibernéticos. Lo anterior se sustenta en la Alianza Chilena de Ciberseguridad, entidad integrada por las diversas partes interesadas en el desarrollo y promoción de la ciberseguridad. (Alianza Chilena de Ciberseguridad, 2019).

Dicha alianza aúna no solo actores nacionales en la materia, sino también tiene contactos internacionales que permiten mayor cooperación con las autoridades. Por su parte Paraguay, cuenta con la Comisión Nacional de Ciberseguridad, instancia donde se refuerzan las relaciones de coordinación, colaboración y cooperación entre las partes interesadas en la ciberseguridad, incluyendo al Estado, sector privado, la academia y la sociedad civil. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Uruguay por su lado, a través del Centro Nacional de Operación de Ciberseguridad recoge las opiniones y estudios que las diversas partes quieren y pueden aportar en materia de seguridad cibernética e infraestructuras críticas. (AGESIC, 2016). Cabe destacar que los tres países tuvieron la precaución de incluir en la elaboración de sus ENCS las opiniones, sugerencias y críticas de las partes interesadas, por medio de consultas ciudadanas.

El indicador asociaciones con proveedores de servicios de internet, muestra el poco compromiso de cuatro de los cinco países estudiados. Argentina es el único país que establece en su estrategia mecanismo para facilitar el intercambio de información entre el sector gubernamental y los proveedores de internet, sobre todo ante situaciones de fraudes, ciberdelitos o cibercrimen. (Leiva, 2015).

Estrategia:
En todo ámbito, donde es necesaria la toma de decisiones rápida e informada, el constante aprendizaje, retroalimentación y mejoramiento, son esenciales para optimizar recursos y tiempo. Precisamente, es lo anterior lo que busca un enfoque de política flexible en la ciberseguridad. Cuatro de los cinco países estudiados trabajan este enfoque en sus ENCS. Argentina, para fomentar el estudio y la retroalimentación, y que esto repercuta en la buena utilización de los recursos, elabora anualmente un informe de la situación de la ciberseguridad del país. Dicho informe es de carácter público y bajo transparencia para mostrar los costes de esta materia. Brasil por su lado, anualmente mide el nivel de madurez de los principales órganos gubernamentales que trabajan, desarrollan y promo-

cionan la ciberseguridad, estableciendo comparaciones respecto a años anteriores, verificando cuales han sido las metas cumplidas y qué aspectos están por debajo de lo que el país necesita.

En la ENCS de Brasil, se plantea, para mayor control, establecer un mecanismo de mapeo sistemático de los activos que afecten directamente en la continuidad de la misión del Estado y la sociedad que compone la infraestructura crítica de la información. Las entidades encargadas de la medición de madurez como de establecer el mecanismo de mapeo es el Gabinete de Seguridad Institucional de la Presidencia de la República en conjunto al Comité Gestor de la Seguridad de la Información. (Departamento de Segurança da Informação e Comunicações, 2015). En cuanto a Paraguay, en el Plan Nacional de Ciberseguridad se plantea que este mismo será revisado y actualizado cada tres años o cuando sea necesario, ya que se comprende la constante evolución de las amenazas cibernéticas como de las Tecnologías de la Información y la Comunicación. La revisión y actualización dependerá del Coordinador Nacional de Ciberseguridad. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). En el caso de Uruguay, se elabora un constante diagnóstico de la Agenda Digital Uruguay para actualizar las temáticas de la misma agenda e ir ampliando como a su vez precisando la ciberseguridad. (AGESIC, 2016).

Respecto al indicador sensibilización, los cinco países cumplen con estrategias que fortalecen a la población en el uso responsable de las tecnologías e internet. En el caso de Argentina, en su ENCS se promueve la concientización en base a los riesgos que conlleva el uso de medios digitales y tecnologías de la información y comunicación. La concientización del país trasandino está dirigida al sector público, las organizaciones de gobierno, al público en general, como también al sector privado y a las relaciones público-privado. El más reconocido programa argentino que se dedica a la sensibilización y concientización en materia de seguridad informática es el programa "Con vos en la Web". (Argentina.gob.ar, 2019). Dicho programa es dirigido por la Dirección Nacional del Sistema Argentino de Información Jurídica, dependiente del Ministerio de Justicia y Derechos Humanos de la Nación, y tiene por objetivo concientizar a las personas en el uso responsable de las Tecnologías de la Información y Comunicación, dar herramientas para disminuir los riesgos cibernéticos manifestados principalmente en las redes sociales.

El programa "Con vos en la Web" está pensado especialmente para padres, profesores y o adultos significativos de menores. (Argentina.gob.ar, 2019). Brasil por su lado, por medio de los agentes responsables de la Seguridad Cibernética de la Administración Pública Federal, se promueven campañas de concientización para la sociedad, enfocado principalmente en los niños, niñas y jóvenes. (Departamento de Segurança da Informação e Comunicações, 2015). En el caso de Chile, se cuenta con el programa "Ciudadanía Digital" dirigido por el Ministerio de Educación. Dicho programa consiste en un conjunto de medidas que posibilitan y desarrollan el conocimiento, habilidades y actitudes de niños, niñas, jóvenes y adultos, para un desenvolvimiento responsable en el ciberespacio. (Internet Segura y Ciudadanía Digital, 2019).

Este programa se levanta sobre las bases de los derechos digitales, para el respeto de los valores fundamentales de los niños, niñas y jóvenes. Respecto a Paraguay, en su ENCS se plantea la incorporación progresiva de prácticas que promocionen la ciberseguridad por un periodo indeterminado o hasta que se genere una cultura en torno a la seguridad cibernética. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Por su parte Uruguay cuenta con el Plan Ibirapitá el cual está destinado a la inclusión de los jubilados a la era digital por medio de talleres, entrega de dispositivos tecnológicos como tablet, curso para el manejo de los dispositivos y manejo de internet. (Plan Ibirapitá, 2019).

En cuanto al indicador educación, investigación y desarrollo, los países del Cono Sur han puesto todos sus esfuerzos en este tema, cumpliendo cada estado con este indicador. No obstante, los objetivos planteados y medidas implementadas son distantes unas a otras, mostrando cómo algunos países tienen una educación en materia cibernética más robusta en comparación de otros países en análisis. En el caso de Argentina, se plantea un constante asesoramiento a nivel educacional y técnico ante incidentes informáticos en órganos gubernamentales que lo requieran o así lo soliciten.

De igual modo, a un nivel ciudadano, el país trasandino cuenta con el "Internet Sano", programa que enseña de forma didáctica a navegar e interactuar en internet, por medio de videos explicativos que logran evidenciar las situaciones de riesgos como también las formas en las que se debe actuar ante posibles ciberamenazas o ciberdelitos. (Jefatura de Gabinete de Ministros, 2019). Para reforzar la educación, la investigación y el desarrollo, Argentina, a

través del Instituto Nacional de Administración Pública, se dedica a la formación profesional de funcionarios y empleados públicos en sistemas de red y seguridad de la información. (Instituto Nacional de Administración Pública, 2019).

Brasil por su parte, en materia de educación cuenta con convenios universitarios para desarrollar a futuro profesionales en ciberseguridad, tanto en el área técnica como en la formulación de políticas públicas en torno a la seguridad, responsabilidad y tratamiento de ciberincidentes. (Departamento de Segurança da Informação e Comunicações, 2015). En el caso de Chile, cuenta con dos programas educativos para orientar el autocuidado y prevención en el ambiente digital orientado a diferentes rangos etarios. El programa "Enlace" tiene como finalidad entregar conocimientos y herramientas a los adultos responsables de menores para que puedan acompañar y formar a los niños, niñas y jóvenes desde un enfoque responsable y seguro en el ciberespacio. (Enlaces, 2019).

En tanto, el programa "Internet Segura" apuesta por la orientación de escuelas y liceos, desde una mirada pedagógica, para formar ciudadanos conscientes en sus derechos y deberes digitales, es por ello, que este programa está destinado a escolares de educación básica y media de los distintos establecimientos educaciones de Chile, ya sean municipales, particular subvencionado y particulares. (Internet Segura y Ciudadanía Digital, 2019).

En la misma línea educacional, pero desde un nivel de post título, Chile cuenta con la Academia Nacional de Estudios Políticos y Estratégicos del Ministerio de Defensa. Dicha academia imparte diplomados, licenciaturas y magister en el área de defensa, estrategia y ciberseguridad, tanto para personas pertenecientes a las ramas castrenses como para civiles. (Academia Nacional de Estudios Políticos y Estratégicos, 2019). Cabe destacar, que las universidades chilenas también cuentan con espacio para fomentar y fortalecer la ciberseguridad, siendo uno de los más reconocidos es el CLCERT. (Clcerte, 2019).

Por su parte Paraguay, imparte programas y cursos específicos en todos los niveles de enseñanza, desde básica a la superior, para incentivar la ciberseguridad y el buen uso de las Tecnologías de la Información y Comunicación. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017). Por último, Uruguay cuenta con el programa "Jóvenes a Programar", el cual apunta a la capacitación e inserción laboral de jóvenes programadores de las Tecnologías de la Información y Comunicación a empresas privadas. (Plan Ceibal, 2019). Para fortalecer la proactividad en el conocimiento, este país ha elaborado el Sistema Nacional de Repositorio, el que permite compartir y consultar trabajos y artículos científicos de producción nacional en diversos temas y áreas, incluida la seguridad cibernética. (Timbó, 2019).

El indicador resiliencia, entendida como la capacidad de los sistemas de red gubernamentales y privados de estar preparados o recuperarse ante ciberincidentes, es uno de los indicadores claves para ver la efectividad de la ciberseguridad de un país. Brasil, Chile y Paraguay, contemplan en sus respectivas estrategias la resiliencia como fundamental para el normal funcionamiento del país y amortiguar los posibles daños para las estructuras estatales, privadas y ciudadanas. Brasil de cara a lo anterior, mantiene como objetivo en su estrategia establecer mecanismos para el mapeo sistemático de daños de infraestructuras, justamente para tener respuesta de recuperaciones rápidas y efectivas, damnificando lo menos posible las estructuras. (Departamento de Segurança da Informação e Comunicações, 2015).

Chile por su parte, cuenta con la Ley 20.478 sobre la Recuperación y Continuidad en Condiciones Críticas y de Emergencia del Sistema Público de Telecomunicaciones, la cual, si bien indica la recuperación rápida de los sistemas en instancias de catástrofes naturales, en los últimos años se han modificado como agregado artículos para incluir la recuperación de los sistemas a nivel tecnológico. Los artículos 39 A y 39 B de dicha ley se especifican sobre la recuperación de las Infraestructuras Críticas de Telecomunicaciones a través de la coordinación de los órganos encargados de las infraestructuras críticas como también un plan de resguardo de dichas infraestructuras post ciberincidentes a partir de las decisiones de la Subsecretaría de Telecomunicaciones. (Ley Nº20478, 2010).

En el caso de Paraguay, en su Pan Nacional de Ciberseguridad, si bien se menciona que las infraestructuras críticas son resilientes antes las amenazas cibernéticas y que cumplen con garantizar la estabilidad de los servicios esenciales, no se presenta una mayor profundización del tema, no mencionando la entidad a cargo de la resiliencia de los órganos gubernamentales, ni algún tipo de medida, ley o política pública que se refiera al tema. (Secretaría Nacional de Tecnologías de la Información y Comunicación, 2017).

Frente a los indudables avances tecnológicos, los marcos de identidad digital son una necesidad tanto para el Estado como para los ciudadanos para optimizar recursos ante los trámites que se soliciten desde el área gubernamental. El indicador desarrollo de marcos de identidad digital, el cual básicamente trata de la identidad en línea, es recogido por tres de los cinco países en estudio. Argentina, Chile y Uruguay, cada país cuenta con un sistema de identidad digital el cual establece la autenticación en línea, permitiendo el libre acceso a documentos personales y servicios de gobierno de manera remota, en tiempo real y de cualquier dispositivo que cuente con acceso a internet.

En el caso de Argentina, el Sistema de Identidad Digital (SID), la autenticación se hace biométricamente, es decir, el acceso depende del reconocimiento facial de quien solicita ingresar. El SID depende del Ministerio del Interior, Obras Públicas y Vivienda, en conjunto a la Secretaría de Modernización. (Argertina.gob.ar, 2019) Chile por su parte, trabaja por medio de la Identidad Digital Única, perteneciente al programa Gobierno Digital.

La Identidad de Digital Única se hace mediante la "Clave Única", instrumento por el cual se digitaliza la identificación de las personas naturales, permitiendo solo de esta manera, el acceso a los servicios públicos vía web. El Estado chileno paulatinamente ha implementado este instrumento para los servicios de gobierno, fijándose el plazo para el 2020 todos los trámites y servicios gubernamentales se hagan en esta modalidad. Cabe destacar que, aparte de la Identidad Digital Única, Chile también cuenta con otros programas que facilitan los servicios digitales gubernamentales tales como: programa Cero Filas y programa Cero Papel. El Consejo Ejecutivo de Modernización de Estado es el encargado del diseño de los programas nombrados. (Gob digital, 2018).

Uruguay por su lado, este indicador lo desarrolla por medio de ID Uruguay, el cual forma parte del Gobierno Electrónico impulsado en los últimos años. El ID Uruguay es el nuevo sistema de gobierno que permite, a través de una única cuenta, acceder a todos los servicios del Estado. Tener la ID Uruguay no es obligatorio sino, más bien puede obtenerla cualquier persona en el momento que lo desee, y no se exige como requisito para los servicios del Estado. La entidad a cargo de la ID Uruguay es la AGESIC. (AGESIC, 2019).

El creciente acceso a las tecnologías y a internet trae consigo la preocupación de la población más vulnerable del ciberespacio, los niños y niñas, que sin mayor conocimiento a lo que se exponen en la red, son blanco fácil para personas que, desde el otro lado de la pantalla, quieren causar daño. El indicador políticas específicas para la protección de niños en línea, justamente quiere enfrentar las inseguridades que los menores viven en esta dimensión, por ello, es fundamental la formulación de políticas específicas que se encarguen de sucesos tales como ciberacosos, ciberbullying, entre otros. De los cincos países del Cono Sur analizados, solo dos tienen trabajos referentes a este tema. Argentina trabaja por medio de Equipo Niñ@s, el cual brinda asesoramiento y acompañamiento las 24 horas, todos los días del año a niñas, niños y adolescentes víctimas de acoso sexual mediante el uso de internet (Crooming), víctimas de pornografía infantil, víctimas de explotación sexual y víctimas de explotación sexual comercial infiltrada en viajes y turismo. El Equipo Niñ@s desarrolla acciones de sensibilización, prevención y capacitación en todo el país a los actores del área de turismo, educacional, salud, seguridad y funcionarios de los tres poderes del Estado. Es importante resaltar que Equipo Niñ@s cuenta con una línea gratuita y correo para las denuncias en esta materia. (Ministerio de Justicia y Derechos Humanos, 2019).

En cuanto a Paraguay, el Ministerio Público, en conjunto a la Policía Nacional y la cooperación del Centro Nacional para Niños Desaparecidos y Explotados, investigan casos de explotación sexual de niñas y niños contactados por redes sociales como también la exhibición de imágenes y oferta de menores de edad por vía web. Por otro lado, frente a los casos de cyberbullying y ciberacoso, la Policía Nacional cuenta con unidades especializadas para el tratamiento minucioso de estos temas (Ministerio Público, 2019), ya que, al ser cometidos estos delitos informáticos a través de tecnologías e internet, requieren de un abordaje particular, desde la investigación, recolección, manejo de evidencia y prueba digital.

Ante los indudables riesgos de la web, los países tienen la obligación de resguardar la seguridad de las personas en el ciberespacio, incluso de sus propios Estados, pues, en lo inmediato, son los ciudadanos los que no cuentan con las herramientas ni conocimientos idóneos para enfrentar la vulneración de su desarrollo personal en internet. El último indicador de respuesta de valores fundamentales precisamente apunta a que las personas puedan realizar sus actividades personales, sociales y comunitaria vía web

respetándoles la privacidad, la libertad de expresión y el libre flujo de información de cada persona.

Si bien con este indicador se busca que ningún agente quebrante los derechos de quien utiliza la web, está destinado esencialmente a que los Estados no coarten la libertad de sus ciudadanos en la dimensión cibernética. De los cinco países en análisis, solo uno en su ENCS hace énfasis en este tema. Chile en su PNCS(Comité Interministerial Sobre Ciberseguridad, 2017), plantea que los objetivos propuesto como las medidas ya concretadas en ciberseguridad, su diseño y ejecución tienen un enfoque de derechos fundamentales, atendiendo su carácter universal e indivisible y sobre la base que el ciberespacio es un ambiente donde las personas cuentan con los mismos derechos que en el mundo físico. Para que realmente se respeten los valores fundamentales, el Ministerio de Justicia y Derechos Humanos de Chile es el encargado de velar por el cumplimiento, actualización y adecuación técnica de la legislación a los desafíos que trae el desarrollo tecnológico.

El indicador monitoreo en tiempo real es el indicador que ningún país en observación cumple. En base a la definición de este indicador, se entiende que para que este se concrete, se requieren de esfuerzos concentrados en el sector público, principalmente en la administración de las infraestructuras gubernamentales, no obstante, dichos esfuerzos no se refieren precisamente a una coordinación realizada por medio de una reunión o foros en los cuales se lleguen acuerdos entre los distintos representantes de estructuras gubernamentales.

Si bien esas instancias son necesarias, los esfuerzos que solicita el monitoreo en tiempo real apuntan al establecimiento de Centros de Operaciones de Seguridad Cibernética, los cuales logren administrar y coordinar técnicamente las infraestructuras críticas estatales. Por lo tanto, se entiende que, para los cinco países en análisis, es mucho más complicado ejecutar este tipo de Centros de Operaciones de Seguridad Cibernética propuesto por la OECD, puesto que su desarrollo implicaría un uso de recursos monetarios y humano importante. Más aún si consideramos que recién en los últimos años se busca invertir en capital humano apto para cargos que requieren de conocimiento cibernético y de toma de decisiones en momentos de crisis.

De igual forma, llama la atención que el indicador Asociaciones con Proveedores de Servicios de Internet evidencia vacíos. Así, Brasil, Chile, Paraguay y Uruguay, en sus respectivas ENCS, no se han planteado objetivos para generar cooperación con las empresas que prestan servicios a la ciudadanía, a las grandes instituciones privadas y gubernamentales. Los Proveedores de Servicios de Internet son actores fundamentales en el contexto de globalización en donde las nuevas tecnologías conectadas a la red de internet están presentes en las mayorías de trabajos, actividades y quehaceres en general del ser humano. De ahí entonces, que es fundamental generar lazos o, derechamente cooperación, entre estas empresas que brinda la conexión a internet a cientos de usuarios, puesto que son ellos quienes pueden entregar información importante respecto a las amenazas a la web.

En ese sentido, el incumplimiento por la mayoría de los países en análisis demuestra que la cooperación interna, entre las instituciones privadas e instituciones gubernamentales no ha sido prioridad para las estrategias, y que los avances que existen hasta ahora, no consideran una coordinación entre estos sectores la cual apunte a alcanzar una meta de carácter nacional como lo es la protección de los usuarios de internet, por el contrario, la cooperación existente se mantiene a nivel teórica la cual se basa en compartir conocimientos y asesoramientos, pero no en la acción concreta de coordinar a las instituciones.

Respecto al área estratégica, el indicador menos cumplido por los países en análisis es Respuesta de valores fundamentales, ya que solo Chile contempla los valores privacidad, libertad de expresión y el libre flujo de información promovidos por la OECD. Para cumplir con el respeto de los valores fundamentales, se requiere que las políticas elaboradas e implementadas en materia de ciberseguridad tenga un enfoque en donde el respeto al ser humano no se trance, permitiendo el normal desarrollo de este en el mundo cibernético. Esto implica que, el Estado chileno debe garantizar, que a las personas, se nos respete nuestra privacidad, velando por la protección de los datos personales, datos financieros y cualquier documento o imagen que exponga información personal delicada. De igual forma, el Estado debe garantizar la libertad de expresión, entendida esta también como un elemento fundamental de Derechos Humano. Por último, el Estado debe garante del libre flujo de información, para que los diversos sectores y actores de la sociedad tenga la posibilidad de manifestar, bajo respeto, sus pen-

samientos e intereses, como también para permitir el libre acceso a las personas a informase desde múltiples fuentes, considerando que el libre flujo de información es un componente esencial para la democracia.

CONCLUSIÓN

Las ciberamenazas son vulnerabilidades propias del desarrollo tecnológico, de internet y la era de la globalización, estas nuevas amenazas ejecutadas desde y en el ciberespacio se han manifestado en algunos países latinoamericanos, afectando muchas veces el normal funcionamiento de los servicios y otras actividades de quienes utilizan internet. Es por ello, que la ciberseguridad es una necesidad real para la seguridad de los países, tanto para proteger sus infraestructuras críticas del sector gubernamental y privado, como también para proteger y permitir el desenvolvimiento normal y cotidiano de miles de personas conectadas a la red.

Estas amenazas cibernéticas afectan de manera indiscriminada, teniendo un alcance global, por lo que la sociedad internacional, específicamente los organismos internacionales se han pronunciado al respecto para aportar ayuda a los países, tanto en el diseño y lineamientos de sus políticas públicas de ciberseguridad, como en la asistencia técnica. De ahí la importancia del estudio de las políticas, o derechamente, de las ENCS de Argentina, Brasil, Chile, Paraguay y Uruguay teniendo como marco de referencia los indicadores de ciberseguridad, una de las organizaciones más influyentes en el escenario internacional que vela por la promoción de una cultura de seguridad cibernética con un enfoque integral, como es la Organización para la Cooperación y el Desarrollo Económico.

Las ENCS han avanzado en algunos temas propuestos por la OECD (2012), tales como: seguridad del gobierno, infraestructura de información crítica, cooperación internacional, coordinación gubernamental – Multiagencia para un enfoque interinstitucional, cooperación público-privada, sensibilización y educación, investigación y desarrollo. De igual modo, se da cuenta que la mayoría de los países concentran sus esfuerzos en el apartado cooperación, específicamente en el indicador cooperación internacional, ya que desde ahí se han levantado y realizado concretas alianzas que ayudan a mejorar las relaciones bilaterales y multilaterales en materia de seguridad cibernética.

Sin embargo, si bien el estudio de caso comparativo muestra que el resto de los indicadores del apartado cooperación son cumplidos por Argentina, Brasil, Chile, Paraguay y Uruguay al incluir objetivos en sus respectivas ENCS, el análisis posterior nos arroja que dichos indicadores solo son esfuerzos principalmente narrativos, ya que implican acuerdos, asesorías y difusión de conocimientos, siendo que, lo que se espera, es que logre una coordinación real entre las partes cooperantes para sentar las bases de una ciberseguridad efectiva en cada país.

Entre los indicadores de ciberseguridad que quedan pendientes, existe monitoreo en tiempo real, asociaciones con proveedores de servicios de internet y respuesta de los valores fundamentales. El poco compromiso por parte de la mayoría de los países estudiados en estos indicadores, se problematizan más aún cuando consideramos que los indicadores monitoreo en tiempo real y respuesta de valores fundamentales son caracterizados como relevantes y prioritarios.

Se puede concluir, que Chile es el país que cumple con la gran mayoría de los indicadores de ciberseguridad de la OECD, incluso con aquellos de carácter prioritarios definidos por dicha organización. Le sigue Paraguay, que cumple la mayoría de los indicadores, no obstante, solo con dos de los cuatro indicadores relevantes.

Los casos más preocupantes son Argentina, Brasil y Uruguay, ya que no han logrado elaborar sus respectivas ENCS en base a las exigencias nacionales e internacionales que la ciberamenazas traen consigo para la seguridad cibernética. Sin embargo, cabe destacar el caso de Brasil, que, si bien no registra una cantidad de cumplimientos significativos de los indicadores trabajados, al menos en los que marca cumplimiento, en general, son materializados y no se quedan en el nivel narrativo.

Así, el camino a seguir para diseñar e implementar políticas que permitan enfrentar el incremento de las ciberamenazas es aún largo y requiere de serios compromisos políticos así como de acuerdos transversales que incluyan a la empresa privada y la sociedad civil. Tarea que por ahora es esquiva en la región.

REFERENCIAS

Academia Nacional de Estudios Políticos y Estratégicos. (2019). *¿Quiénes somos?* Recuperado de https://www.anepe.cl/portada-quienes-somos/

Agência Brasileira de Inteligência. (s/f). *O que é, O que faz, Como faz.* Recuperado de http://www.abin.gov.br/institucional/a-abin/

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay [AGESIC], (2016). *Agenda Uruguay 2020.* Recuperado de https://www.agesic.gub.uy/innovaportal/file/6122/1/agenda-uruguay-digital---enero-final.pdf

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. [AGESIC], (2019). *Tienda virtual de agencia de compras y contrataciones del Estado.* Recuperado de https://www.comprasestatales.gub.uy/tienda/

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. [AGESIC]. (2018). *Marco de Ciberseguridad.* Recuperado de https://centroderecursos.agesic.gub.uy/web/seguridad/wiki/-/wiki/Main/Marco+de+Ciberseguridad

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (2019). *Firma electrónica.* Recuperado de https://www.agesic.gub.uy/innovaportal/v/6726/38/agesic/que-es.html?idPadre=6723

Agencia para o Desenvolvimento da Industria no Brasil. (2019). *Proyectos.* Recuperado de https://abdi.com.br/inovacao

Alianza Chilena de Ciberseguridad. (2019). *¿Quiénes somos?* Recuperado de https://www.alianzaciberseguridad.cl/#somos

Arias, J. (2011). Brasil sufre un ciberataque a gran escala. *El País.* Recuperado de https://elpais.com/diario/2011/06/25/internacional/1308952808_850215.html

Asociación Chilena de Empresas de Tecnología de Información. [ACTI]. (2019). *¿Quiénes somos?* Recuperado de http://www.acti.cl/quienes_somos/

Banco Interamericano de Desarrollo (BID) & Organización de Estados Americanos (OEA). (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* Recuperado de https://www.casede.org/index.php/biblioteca-casede-2-0/seguridad/ciberseguridad/468-ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe/file

Borghello, C., & Temperini, M. (2013). Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública. En Simposio de Informática y Derecho. *Jornadas Argentinas De Informática, 42.*

Centro Nacional de Respuesta a Incidentes de Seguridad Informática. [CERTUY]. (2015). *Estadísticas de incidentes primer semestre 2015.* Recuperado de https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas/estadisticas-de-incidentes-del-primer-semestre-de-2015

Centro Nacional de Respuesta a Incidentes de Seguridad Informática. [CERTUY]. (2016). *Estadísticas de incidentes de CERTUY en 2016.* Recuperado de https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas/estadistica-de-incidentes-de-certuy-en-2016

Clcerte (2019). *Nosotros.* Recuperado de https://www.clcert.cl/nosotros/

Comité Interministerial Sobre Ciberseguridad [CICS] (2017). *Política Nacional de Ciberseguridad.* Recuperado de: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Con vos en la web (2019). Recuperado de https://www.argentina.gob.ar/justicia/convosenlaweb

Council of Europe Portal. (2019). *Chart of signatures and ratifications of treaty 185.* Recuperado de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=S5PssuRE

CSIRT ANTEL. (s/f). *¿Qué hace el CSIRT de ANTEL?* Recuperado de https://www.csirt-antel.com.uy/que_hace

CTIR Gov. (2019). *Acerca CTIR Gov.* Recuperado de https://www.ctir.gov.br/es/

Decreto N° 181-18. (2018). *Aprova o texto do Acordo entre a República Federativa do Brasil e o Reino da Suécia sobre Troca e Proteção Mútua de Informação Classificada, assinado em Estocolmo, em 3 de abril de 2014.* Camara Dos Deputados. Brasil.

Decreto N°13-16. (2016). *Estructura del Ministerio de Modernización y del Ministerio de Defensa. Información Legislativa. Buenos Aires, Argentina.* Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257556/texact.htm

Decreto N°3-18. (2018). Ministerio de Defensa Nacional aprueba Política de Ciberdefensa. *Diario Oficial de la República de Chile.* Santiago, Chile. Recuperado de https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Decreto N° 9.273-15. (2015). *Promulga o acordo entre a República Fede- rativa do Brasil e o Reino da Espanha relativo à troca e proteção mútua de informações classificadas, firmado em Brasília, em 15 de abril de 2015.* Camara Dos Deputados. Brasil. Recuperado de https://www2.camara.leg.br/legin/fed/decret/2018/decreto-9273-31-janeiro-2018-786134-norma-pe.html

Departamento de Segurança da Informação e Comunicações. [DSIC] (2015). *Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015 – 2018.* Recuperado de http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf/view

Dergarabedian, C. (2018). G20: el Gobierno refuerza la ciberseguridad de la cumbre con ayuda de Israel. En *iprofesional*. Recuperado de https://www.iprofesional.com/tecnologia/281619-buenos-aires-costa-salguero-macri-G20-el-Gobierno-refuerza-la-ciberseguridad-de-la-cumbre-con-ayuda-de-Israel

Díaz, J. R. (2016). Ciberamenazas: ¿el terrorismo del futuro? bie3: *Boletín ieee*, 3, 541-561.

Dinatale, M. (2018). Los hackeos aumentaron un 700% en Argentina y el gobierno aceleró el comando de ciberseguridad. *Infobae.* Recuperado de https://www.infobae.com/politica/2018/02/11/los-hackeos-aumentaron-un-700-en-argentina-y-el-gobierno-acelero-el-comando-de-ciberseguridad/

Dirección Contra Hechos Punibles Económicos y Financieros Policía Nacional. (2015). *Divisiones Especializadas.* Recuperado de http://www.delitoseconomicos.gov.py/index.php/dependencias/sede-central

Disposición N°1. Aprueba la Política Modelo de Seguridad de la Información. Normativa-Ciberseguridad (2015). *Información Legislativa.* Buenos Aires, Argentina. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

El Ciudadano (2017). *Chile sería el quinto país con más ciberataques en todo América.* Recuperado de https://www.elciudadano.com/ciencia-tecnologia/chile-seria-el-quinto-pais-con-mas-ciberataques-en-toda-america/03/22/

Enlaces. (2019). *¿Quiénes somos?* Recuperado de http://www.enlaces.cl/sobre-enlaces/quienes-somos/

Fernández, A. V., & Rodríguez, J. M. C. (2017). Análisis de las ciberamenazas. *Cuadernos de estrategia*, 185, 97-138.

Frieiro, R., Pérez, P. y Pascual, X. (2017). ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía? *Cyber Risk.* pp. 1-32

Gobierno de España. Ministerio de Defensa, Secretaría General Técnica. (2014). *Documentos de Seguridad y Defensa 60. Estrategia de la información y seguridad en el ciberespacio.* Recuperado de https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_60.pdf

Gob digital. (2018). *Instructivo Presidencial de Transformación Digital.* Recuperado de https://digital.gob.cl/instructivo/identidad-digital

Instituto Nacional de Administración Pública. (2019). *Portal de Capacitación.* Recuperado de https://capacitacion.inap.gob.ar/

Internet Segura y Ciudadanía Digital. (2019). *Comunidad educativa.* Recuperado de http://www.internetsegura.cl/comunidad-educativa/

Internet Segura y Ciudadanía Digital. (2019). *Orientaciones de Ciudadanía Digital para la formación ciudadana.* Recuperado de http://www.internetsegura.cl/comunidad-educativa/orientaciones-ciudadania-digital/

Jefatura de Gabinete de Ministros. (2019). *Internet Sano.* Recuperado de http://seguridadinformatica.sgp.gob.ar/paginas.dhtml?pagina=52

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software, 3*(4), 161-176.

Lex Magiste. (2019). *Portaria Normativa N° 3.389, de 21 de dezembro de 2012.* Recuperado de http://www.lex.com.br/legis_24068327_PORTARIA_NORMATIVA_N_3389_DE_21_DE_DEZEMBRO_DE_2012.aspx

Ley N° 19.607-18. (2018) *Apruébese el acuerdo entre el Gobierno de la República Oriental del Uruguay y el Gobierno de la Federación de Rusia sobre la Cooperación en Materia de Defensa, suscrito en la cuidad de Moscú, Federación de Rusia, el 16 de febrero 2017.* Cámara de Representantes, Montevideo, Uruguay. Recuperado de https://medios.presidencia.gub.uy/legal/2018/leyes/04/mrree_1479.pdf

Ley Nº 20.478-10. (2010). *Sobre Recuperación y Continuidad en Condiciones Críticas y de Emergencia del Sistema Público de Telecomunicaciones.* Biblioteca del Congreso Nacional de Chile. Recuperado de https://www.leychile.cl/Navegar?idNorma=1020622&buscar=20478

Ministerio de Justicia y Derechos Humanos. (2019). *Atención a las víctimas.* Recuperado de http://www.jus.gob.ar/atencion-al-ciudadano/atencion-a-las-victimas/equipo-nin@s.aspx

Ministerio de Modernización de la República de Argentina y Ministerio de Energía, Turismo y Agenda Digital del Reino de España. (2017). *Memorando de Entendimiento sobre Cooperación en Materia de Ciberseguridad entre el Ministerio de Modernización de la República Argentina y el Ministerio de Energía, Turismo y Agenda Digital del Reino de España.* Recuperado de http://www.cecra.com.ar/binarydata/file/convenios/bilpai11182.pdf

Ministerio de Modernización. (2019). *¿Qué Hacemos?* Recuperado de https://www.argentina.gob.ar/que-hacemos

Ministerio de Tecnologías de la Información y Comunicación. (s/f). *Institucional.* Recuperado de https://www.cert.gov.py/index.php/certpy

Ministerio del Interior y Seguridad Pública. (2019). *Decretos.* Recuperado de https://www.csirt.gob.cl/decretos/

Ministerio del Interior y Seguridad Pública. (2019). *Funciones.* Recuperado de https://www.csirt.gob.cl/funciones/

Ministerio Público (2019). *Delitos informáticos.* Recuperado de https://www.ministeriopublico.gov.py/delitos-informaticos-i242

Moreno, G. (2018). ¿Cuántos usuarios de internet hay en América Latina? *Statista.* Recuperado de https://es.statista.com/grafico/13903/cuantos-usuarios-de-internet-hay-en-america-latina/

Moreno, J. C., & Gil, M. M. L. (2017). Crisis y ciberespacio: hacia un modelo integral de respuesta en el Sistema de Seguridad Nacional. *Cuadernos de estrategia,* 185, 65-96.

Natalevich, M. (2017) Uruguay sufrió 15 ciberataques de alta severidad durante 2016. *El Observador.* Recuperado de https://www.elobservador.com.uy/nota/uruguay-sufrio-15-ciberataques-de-alta-severidad-durante-2016-2017123500

Núñez, C. (2019). *Estrategias Nacionales de Ciberseguridad en el Cono Sur. Análisis a partir de los indicadores de la Organización para la Cooperación y el Desarrollo Económico.* (Tesis no publicada). Facultad de Humanidades, Universidad de Santiago de Chile, Chile.

OEA & Symantec. (2014). *Tendencias de seguridad cibernética en América Latina y el Caribe*. Recuperado de https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Organisation for Economic Co-operation and Development. (2012). Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the internet economy. *OECD Publishing.*

Organización de Estados Americanos. (2015). Iniciativa de la Seguridad Cibernética de la OEA. *Foro Global sobre Experticia Cibernética (GFCE). 1 – 16.* Recuperado de https://www.sites.oas.org/cyber/Documents/2015%20Iniciativa%20de%20Seguridad%20Cibern%C3%A9tica%20de%20la%20OEA.PD

Organización de Estados Americanos. [OEA]. (2019). *Programa de ciberseguridad.* Recuperado de http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Pardo, D. (2013). Por qué Brasil está en el centro del escándalo de espionaje en EE. UU. *BBC Mundo.* Recuperado de https://www.bbc.com/mundo/noticias/2013/08/130822_tecnologia_brasil_snowden_eeuu_dp

Plan Ceibal. (2019). *Jóvenes a programar.* Recuperado de https://jovenesaprogramar.edu.uy/

Plan Ibirapitá. (2019). *El Plan.* Recuperado de https://ibirapita.org.uy/#el-plan

Policía de Investigaciones de Chile. (2019). *Cibercrimen.* Recuperado de http://www.pdichile.cl/instituci%C3%B3n/unidades/cibercrimen

Resolución N° 580. (2011). Crea el Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad. *Información Legislativa.* Buenos Aires, Argentina. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/314171/norma.htm

Sánchez de Rojas, E. (2010). La ciberseguridad: retos, riesgos y amenazas. *Revista Ejército*, 837, 136-143.

Sancho, C. (2017). Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to dossier. URVIO – *Revista Latinoamericana de Estudios de Seguridad, 20*, 8-15. doi.org/10.17141/urvio.20.2017.2859

Secretaría Nacional de Tecnologías de la Información y Comunicación [SENATICs]. (2017). *Plan Nacional de Ciberseguridad. Retos, roles y compromisos.* Recuperado de http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

Segura, R. (2018). Ciberdelitos íntimos. *Abc COLOR.* Recuperado de http://www.abc.com.py/edicion-impresa/suplementos/abc-revista/ciberdelitos-intimos-1755966.html

SID- Sistema de identidad digital (2019). Recuperado de https://www.argentina.gob.ar/sid-sistema-de-identidad-digital

Statista. (2019). *Volumen de pérdidas generadas por los delitos informáticos en determinados países en agosto de 2015 (en millones de USD).* Recuperado de https://es.statista.com/estadisticas/600983/ciberdelitos-indice-de-perdidas-en-determinados-paises-5/

Subsecretaría de Telecomunicaciones. (2018). *Gobiernos de Chile e Israel firman acuerdo de cooperación en el ámbito de ciberseguridad en las telecomunicaciones.* Recuperado de http://www.pdichile.cl/instituci%C3%B3n/unidades/cibercrimenhttps://www.subtel.gob.cl/gobiernos-de-chile-e-israel-firman-acuerdo-de-cooperacion-en-el-ambito-de-ciberseguridad-en-las-telecomunicaciones/

TeleGeography. (2019). *Submarine Cable FrequentlyAsked-Questions.* Recuperado de https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions?__hstc=196094579.1decb70f607f20f485981d351f-230cd6.1557275976667.1557275976667.1557275976667.1&__hssc=196094579.2.1557275976667&__hsfp=721576298

Timbó. (2019). *Trama interinstitucional multidisciplinaria de bibliografía online.* Recuperado de http://www.timbo.org.uy/

Van Bendegem, J. M. F. (2016). La quinta dimensión digital. bie3: *Boletín ieee, 4,* 834-859.

Viollier, P. (2017). *La participación en la elaboración de la Política Nacional de Ciberseguridad: Hacia un nuevo marco normativo en Chile.* Recuperado de https://www.derechosdigitales.org/wp-content/uploads/ciberseguridad.pdf

"EL INTERNET DE LAS COSAS (IOT) COMO VECTOR DE ATAQUES CIBERNÉTICOS E INCIDENTES DE PRIVACIDAD"

The Internet of Things (IoT) As a Vector for Cyberattacks and Privacy Incidents

Recibido: 12 / 09 / 2019 Aprobado: 31 / 10 / 2019

Ingeniero
Felix Uribe
Estados Unidos

El autor es un profesional de la ciberseguridad y la privacidad en la tecnología de la información (TI) con una larga experiencia en los sectores públicos y privados. En el ámbito Académico, es Profesor Asociado Adjunto en el Programa de Política y Gestión de Ciberseguridad de la University of Maryland, Global Campus (UMGC) donde imparte cursos de ciberseguridad, privacidad y cibercriminalidad. En el ámbito gubernamental, actualmente es un Oficial Federal de Privacidad y Analista de Seguridad de TI en el Departamento del Interior de los Estados Unidos. En el Departamento de Justicia de los Estados Unidos, trabajó como auditor de seguridad de TI en la Oficina de Auditoria del Inspector General. En el Departamento de la Administración de la Seguridad Social de los Estados Unidos (SSA) y bajo el auspicio del Consejo de Administración de la Oficina del presidente de los Estados Unidos llevó a cabo la elaboración de los documentos de base para la creación de una Ciber-Academia en ese Departamento.
felix.uribe@faculty.umuc.edu

RESUMEN

El crecimiento exponencial de dispositivos electrónicos que forman lo que hoy se conoce como el Internet de las Cosas (IoT por sus siglas en inglés) y la implementación y uso de estos tanto en instituciones públicas y privadas, así como la ciudadanía en sus hogares, exige abordar las preocupaciones y retos actuales de ciberseguridad y privacidad que afectan la confiabilidad del actual ecosistema del Internet de las Cosas en el mundo.

Palabras clave:
Internet de las Cosas, IoT, dispositivos inteligentes, ciberataques, privacidad.

ABSTRACT

The exponential growth of electronic devices that form what is now known as the Internet of Things (IoT) and the implementation and use of these in both public and private institutions as well as citizens in general in their homes, requires addressing cybersecurity and privacy concerns and challenges that affect the reliability of the current Internet of Things ecosystem in the world.

Keywords:
Internet of Things, IoT, smart devices, cyberattacks, privacy.

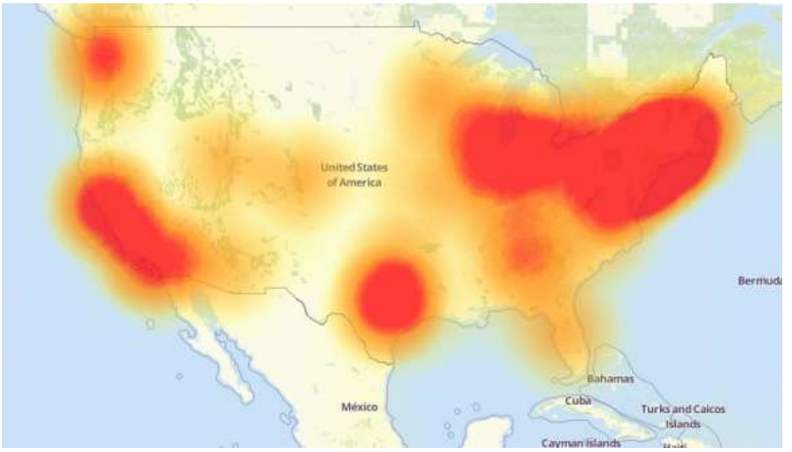
INTRODUCCIÓN

El Internet de las Cosas se usa generalmente para describir aquellos dispositivos electrónicos o electrodomésticos conectados a internet o una red informática. Aunque no existe una definición formal del término, lo describiré personalmente como "la red de dispositivos (cosas) capaces de interactuar con otros dispositivos y/o seres vivos a través de sensores y a través de internet o de una red privada local o global no conectada a internet".

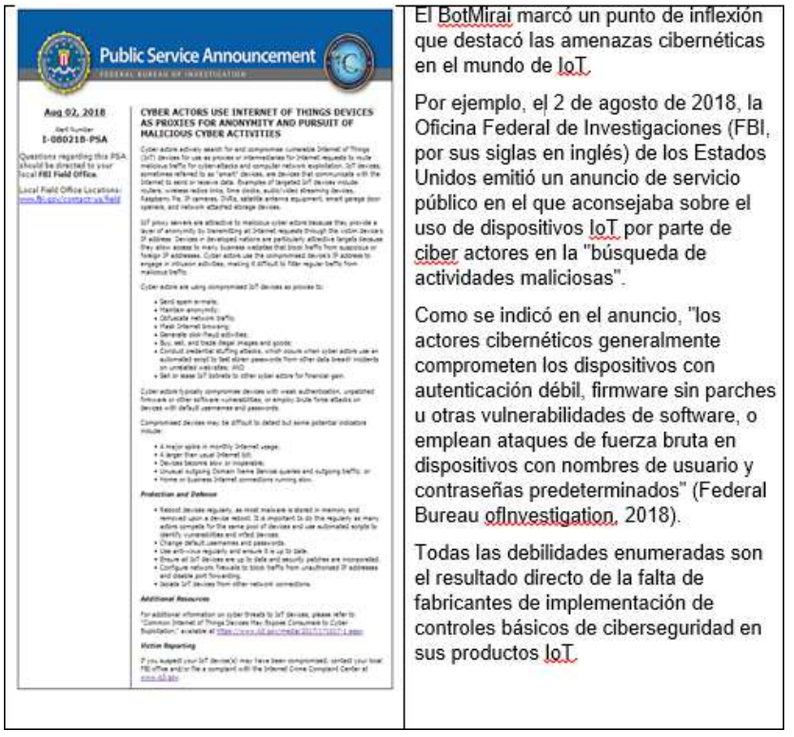
Hay muchas predicciones sobre el crecimiento exponencial de los dispositivos IoT en los próximos años. El rango va de 20 a 30 mil millones de dispositivos conectados a internet para el próximo año (2020) y se espera que siga creciendo en los próximos años. Es obvio que, en un futuro no muy lejano, gran parte del mundo va a estar completamente conectado y lo que llamamos hoy en día "dispositivos IoT" se convertirá en parte de la estructura de este nuevo mundo ciber físico totalmente conectado. Lo que también es obvio es que cuanto más nos conectamos, más nos tenemos que preocupar por los riesgos de ciberseguridad y privacidad.

VECTORES DE CIBERATAQUES

La introducción de miles de millones de nuevos dispositivos inseguros de IoT en la infraestructura actual de internet, abre al mismo tiempo, miles de millones de vectores de ataque a hogares, industrias, organizaciones y cualquier otra infraestructura tocada por esos dispositivos. En 2016, el ahora famoso "MiraiBot", infectó cientos de miles de dispositivos IoT inherentemente inseguros (routers, DVR y cámaras) que se utilizaron para lanzar varios ataques masivos con un récord de denegación de servicio distribuido (DDoS) contra altos objetivos como el sitio web de "Krebs on Security" y el proveedor del sistema de nombres de dominio "Dyn" (adquirido por Oracle en 2016) entre otros. En todos estos ataques, los servicios de internet de la víctima se desactivaron temporalmente (Ragan, 2016). McAfee Labs estimó que 2.5 millones de dispositivos IoT estaban infectados por Mirai a fines de 2016 (Business Wire, 2016).



Este mapa muestra las interrupciones (en rojo) causadas por el BotMiraia la infraestructura Dyn durante el ataque del 2016. Fuente: Downdetector.com


Public Service Announcement

Aug 02, 2018

I-080218-PSA

CYBER ACTORS USE INTERNET OF THINGS DEVICES AS PROXIES FOR ANONYMITY AND PURSUIT OF MALICIOUS CYBER ACTIVITIES

El BotMirai marcó un punto de inflexión que destacó las amenazas cibernéticas en el mundo de IoT.

Por ejemplo, el 2 de agosto de 2018, la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) de los Estados Unidos emitió un anuncio de servicio público en el que aconsejaba sobre el uso de dispositivos IoT por parte de ciber actores en la "búsqueda de actividades maliciosas".

Como se indicó en el anuncio, "los actores cibernéticos generalmente comprometen los dispositivos con autenticación débil, firmware sin parches u otras vulnerabilidades de software, o emplean ataques de fuerza bruta en dispositivos con nombres de usuario y contraseñas predeterminados" (Federal Bureau ofInvestigation, 2018).

Todas las debilidades enumeradas son el resultado directo de la falta de fabricantes de implementación de controles básicos de ciberseguridad en sus productos IoT.

Anuncio del Servicio Público del FBI. Fuente: https://www.ic3.gov/media/2018/180802.aspx

Con el fin de ayudar y brindar orientación y conciencia a los fabricantes de IoT, algunos gobiernos han tomado la iniciativa de desarrollar guías de IoT que tengan como objetivo proporcionar una base de seguridad mínima de características de ciberseguridad que los fabricantes puedan seguir voluntariamente al desarrollar y fabricar dispositivos de IoT. Como ejemplo, en el Reino Unido, el "Código de Prácticas para la Seguridad de IoT del Consumidor" tiene como objetivo "apoyar a todas las partes involucradas en el desarrollo, fabricación y venta minorista de IoT del consumidor con un conjunto de pautas para garantizar que los productos sean seguros por diseño y para facilitar que las personas se mantengan seguras en un mundo digital " (UnitedKingdomDepartmentfor Digital, Culture, Media and Sport, 2018).

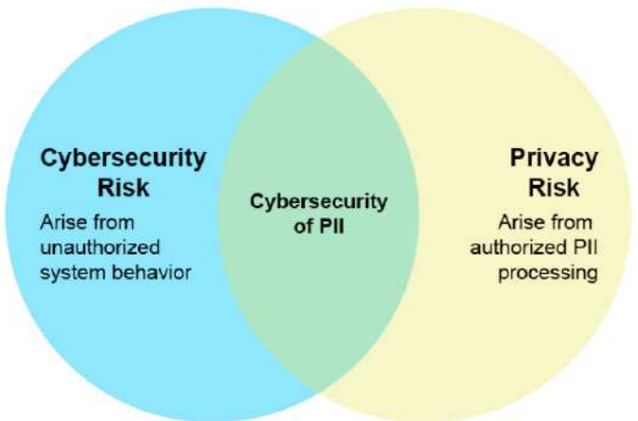
En los Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) publicaron recientemente un borrador titulado "Línea de base de la característica de ciberseguridad básica para dispositivos IoT asegurables: un punto de partida para los fabricantes de dispositivos IoT", aunque todavía está en borrador, este documento está "destinado para ayudar a los fabricantes de dispositivos de internet de las cosas (IoT) a comprender los riesgos de ciberseguridad que enfrentan sus clientes para que los dispositivos de IoT puedan proporcionar características de ciberseguridad que los hagan al menos mínimamente asegurables para las personas y organizaciones que los adquieren y usan" (NIST, julio 2019).

Es obvio que hasta que los fabricantes de IoT se pongan al día con la implementación correcta de los controles de ciberseguridad en la fabricación de dispositivos de IoT, corresponde a las organizaciones y a los consumidores estar informados e implementar buenas prácticas de ciberseguridad al comprar e implementar estos dispositivos. Algunas recomendaciones básicas, como evaluar la configuración de seguridad y las características de los dispositivos IoT, el uso de contraseñas seguras y mantener el software actualizado, entre otras cosas, pueden ayudar a prevenir el uso de estos para perpetrar ataques cibernéticos y delitos cibernéticos.

Incidentes de privacidad

El NIST en su publicación titulada "Consideraciones para gestionar los riesgos de privacidad y ciberseguridad de Internet de las Cosas (IoT)" afirma que "el riesgo de ciberseguridad y el riesgo de privacidad están relacionados, pero son conceptos distintos" (NIST, junio 2019). Por un lado, los riesgos de ciberseguridad se refieren a la protección de la confidencialidad, integridad o disponibilidad de la información y el dispositivo IoT, mientras que los riesgos de privacidad se refieren a la protección de datos personales. (NIST).

Desafortunadamente, en el entorno actual, debido a la rápida fabricación y despliegue de dispositivos IoT sin los controles de ciberseguridad adecuados, por una parte, y por otra, el uso erróneo de estos por parte de organizaciones e individuos, a veces conduce a la divulgación no intencional de datos personales.



Relación entre ciberseguridad y riesgos de privacidad.
Fuente: https://csrc.nist.gov/publications/detail/nistir/8228/final

Datos personales como de geolocalización, datos de comportamiento y biométricos, etc., son recopilados por millones de dispositivos IoT en todo el mundo. Un caso interesante que demostró la recopilación masiva y la divulgación involuntaria de datos personales cuando se utilizan dispositivos IoT, es el caso Strava. Strava es una compañía que desarrolló una aplicación móvil que es utilizada por millones de personas para monitorizar sus actividades físicas (trotar, caminar, andar en bicicleta, etc.).

Además, los usuarios del servicio también pueden enviar al sistema sus actividades registradas en otros dispositivos que también monitorizan la actividad física de estos.

La compañía creó lo que se conoce como Strava Global Heatmap. Este "mapa de calor" se crea utilizando billones de puntos de datos

recopilados de los usuarios del servicio y que se visualizan en un mapa que muestra los millones de actividades físicas registradas por la empresa.

Desafortunadamente, en enero del 2018, se descubrió que el mapa mostraba bases militares secretas en todo el mundo (Hsu, 2018). En el mapa, se mostraba claramente cómo las actividades físicas del personal militar revelaron la ubicación de las bases e identificaron rutas de patrulla que se pueden utilizar para resaltar los perímetros de la base.

Campamento base expedicionario naval de los Estados Unidos Lemonnier en Djibouti. Fuente: mapa de calor de Strava.

En respuesta a las revelaciones de Strava, el Pentágono anunció ese mismo año una nueva política que prohíbe el uso de funciones de geolocalización en áreas operativas donde el Ejército está llevando a cabo ciertas misiones.

El caso Strava mostró cómo la recopilación masiva y el uso de los datos recopilados a través de dispositivos IoT Puede causar resultados negativos si se realizan de manera incorrecta. En este caso, la geolocalización anónima de individuos podría haber puesto vidas en peligro al revelar rutas de patrulla.

Otro riesgo de los dispositivos IoT que crea nuevos desafíos de privacidad tanto para los fabricantes como para el consumidor, es la producción de los llamados "juguetes conectados". Como su nombre lo indica, los juguetes tienen la capacidad de comunicarse con el mundo exterior a través de cámaras, micrófonos y otros sensores diseñados para hacer que la experiencia de juego del niño sea más humana. Desafortunadamente, se ha descubierto que algunos juguetes tienen características de recolección de datos muy invasivas que ponen en riesgo la privacidad y la seguridad de los niños.

En un ejemplo clásico sobre la protección de la privacidad de los niños, en 2017, la Agencia de la Red Federal del gobierno alemán (Bundesnetzagentur) emitió una advertencia oficial para aconsejar al público que destruyera una muñeca llamada Cayla, porque la muñeca podría haber sido utilizada por un actor malicioso para hablar y escuchar a cualquier niño jugando con ella (BBC, 2017).

CONCLUSIÓN

Los casos relacionados con los desafíos de ciberseguridad y privacidad presentados en este documento, son solo un ejemplo mínimo de los muchos otros casos que han ocurrido en el pasado y los que vendrán en el futuro cercano. El crecimiento exponencial de los dispositivos IoT y sus aplicaciones cotidianas requiere la implementación de controles de ciberseguridad y privacidad para abordar las preocupaciones de seguridad y privacidad actuales que afectan la confiabilidad del dominio IoT que existe en la actualidad.

Los fabricantes de dispositivos IoT deben tener en cuenta las guías gubernamentales actuales al diseñar y fabricar dispositivos IoT y sus componentes para garantizar que la seguridad y la privacidad se implementen por diseño y no surjan como una ocurrencia tardía durante el ciclo de vida de desarrollo de dispositivos IoT.

A medida que se construyen e introducen millones y millones de dispositivos IoT en el ecosistema del mundo, quiero finalizar con dos recomendaciones: La primera es la creación de "Unidades de Ciberseguridad y Privacidad IoT" en organizaciones públicas y privadas cuya especialización sea exclusivamente el análisis, estudio y la creación de normas para el uso e implementación de esos dispositivos durante el ciclo de vida del producto para garantizar el cumplimiento de los requisitos mínimos de ciberseguridad y privacidad. La segunda, es la creación de unidades especializadas en instituciones gubernamentales y policiacas encargadas de la investigación y la prosecución del ciberdelito donde los dispositivos IoT fueron utilizados para cometer el ciber delito.

REFERENCIAS

Federal Bureau of Investigation. (2018). *Cyber actors use internet of things devices as proxies for anonymity and pursuit of malicious cyber activities.* Recuperado de https://www.ic3.gov/media/2018/180802.aspx

German parents told to destroy Cayla dolls over hacking fears. (2017). *BBC.* Recuperado de https://www.bbc.com/news/world-europe-39002142

Hsu, J. (2018). The strava heat map and the end of secrets. *Wired.* Recuperado de https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

McAfee labs report highlights critical challenges to threat intelligent sharing (2016). *Business Wire.* Recuperado de https://www.businesswire.com/news/home/20170405006423/en/McAfee-Labs-Report-Highlights-Critical-Challenges-Threat

National Institute of Standards and Technology (NIST). (2019). *Core cybersecurity feature baseline for securable IoT devices: A starting point for IoT device manufacturers.* Recuperado de https://csrc.nist.gov/publications/detail/nistir/8259/draft

National Institute of Standards and Technology (NIST). (2019). *Considerations for Managing Internet of Things (IoT) cybersecurity and privacy risks.* Recuperado de https://csrc.nist.gov/publications/detail/nistir/8228/final

Ragan, S. (2016). *DDoS knocks down DNS, data centers across the U.S. affected.* Recuperado de https://www.csoonline.com/article/3133992/ddos-knocks-down-dns-datacenters-across-the-u-s-affected.html

United Kingdom Department for Digital, Culture, Media and Sport. (2018). *Code of practice for consumer Internet of Things (IoT) security.* Recuperado de https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

Normas para los autores

Lista preliminar para la preparación de envíos

Como parte del proceso de envíos, los autores/as están obligados a comprobar que su envío cumpla todos los elementos que se muestran a continuación.
Se devolverán a los autores/as aquellos envíos que no cumplan estas directrices.
Constatar que el envío no ha sido publicado previamente ni se ha sometido a consideración por ninguna otra revista (o se ha proporcionado una explicación al respecto en los comentarios al editor/a).
El texto reúne las condiciones estilísticas y bibliográficas incluidas en pautas para el autor/a, en acerca de la revista.
En el caso de enviar el texto al Comité de Evaluación por pares ocultos, se siguen las instrucciones incluidas a fin de asegurar una evaluación anónima.

Datos acerca de la revista

Objeto

La Revista SEGURIDAD, CIENCIA & DEFENSA, órgano de divulgación científica del Instituto Superior para la Defensa "General Juan Pablo Duarte y Díez" (INSUDE), siendo una publicación periódica universitaria de la educación superior militar. Publicada por el Departamento de Investigación y Publicaciones Científicas del INSUDE, inscribe su quehacer en la naturaleza y fines de la institución, al desarrollar las estructuras y procesos académicos, necesario para garantizar la educación superior en la carrera militar, para así ser una institución de educación superior militar modelo de excelencia en el desarrollo de las capacidades para la Seguridad y Defensa Nacional; con respeto a la persona humana, a la libertad de investigación y de expresión.

Descripción

Seguridad, Ciencia y Defensa es una publicación anual de divulgación científica del INSUDE (Instituto Superior para la Defensa – General Juan Pablo Duarte y Diez). Está abierta igualmente a colaboraciones nacionales e internacionales. Publica artículos en las áreas académicas del Instituto, a saber: Ciencias Militares, Ciencias Navales y Ciencias Aeronáuticas; además de la Seguridad y Defensa Nacional, Geopolítica y Derechos Humanos y Derecho Internacional Humanitario.

Características de la publicación

SEGURIDAD, CIENCIA & DEFENSA es un medio de publicación de los trabajos de investigación del Instituto Superior para la Defensa "General Juan Pablo Duarte y Diez" (INSUDE), abierta igualmente a colaboraciones nacionales e internacionales. Se da prioridad a aquellos trabajos afines a las Áreas Académicas del INSUDE, a saber: Ciencias Militares, Ciencias Navales y Ciencias Aeronáuticas; además de la Seguridad y Defensa Nacional, Geopolítica y Derechos Humanos y Derecho Internacional Humanitario. SEGURIDAD, CIENCIA & DEFENSA; abarca los temas que se corresponde a los programas de naturaleza estrictamente militar y civil–militar, en lo concernientes a los programas de naturaleza estrictamente militar, es donde los estudiantes o cursantes son militares y son impartidos en el Nivel de grado en las Academias Militares (Ejército República Dominicana, Armada República Dominicana y Fuerza Aérea República Dominicana) y en el Nivel de postgrado en las Especialidades de Comando y Estado Mayor (Conjunto, Terrestre, Naval y Aéreo). En el caso de los programas de naturaleza civil-militar, son aquellos donde participan personal de la clase civil y militar como estudiantes y/o cursantes. Estos programas incluyen: a) la Especialidad en Derechos Humanos y Derecho Internacional Humanitario, b) Geopolítica, c) la Maestría en Defensa y Seguridad Nacional, así como otros cursos de postgrado y de educación continua que tengan la misma naturaleza.

Esta revista científica constituye una de las vías para propiciar la formación permanente de los docentes en el área de la investigación científica, convocándoles a participar con textos científicos, ensayos, entrevistas, testimonios y reseñas bibliográficas. La publicación, además, acoge artículos de autores invitados.

En consideración a los aspectos antes citados, describiremos las normas a seguir por parte de los autores para publicar en la revista y las cuales tienen que ver con información sobre los autores, con el artículo y con los procedimientos:

1. INFORMACIÓN SOBRE EL AUTOR O AUTORES.

   a) Nombre completo
   b) Institución donde se desempeña laboralmente, con la dirección, teléfono (y eventualmente fax) de la misma.
   c) Correo electrónico.
   d) Un breve currículum de un máximo de 20 líneas.
   e) Cada autor debe anexar una foto suya de frente, a color, en fondo blanco, en cualquiera de los siguientes formatos .jpg, con un tamaño no menor de 7.0 píxeles.

2. LOS ARTÍCULOS

   A. La primera página del artículo debe contener:
      I. Título del artículo.
      II. Nombre del autor.
      III. Últimos títulos alcanzados y tipo de afiliación institucional del autor.
      IV. Resumen de un párrafo no superior a 10 líneas o 250 palabras, digitadas del artículo, en español e inglés.
      V. Un máximo de 5 palabras clave sobre el artículo.
      VI. Dirección electrónica del autor.

B. Se estipula que los artículos no deben exceder una longitud de 7 páginas, las reseñas de libros de 5 páginas y las entrevistas de 4 páginas. Sin embargo, queda a disposición del Comité de publicaciones la posibilidad de variar dichos límites.

C. Se dará preferencia a los trabajos de investigación que no hayan sido publicados con anterioridad. Los artículos no deben pasar de unas 25 páginas y serán recibidos en formato de Microsoft Word, en páginas tamaño 8 ½ X 11, a 1½ espacio y en tipografía Arial 12; márgenes: izquierdo 3 cm. derecho 2,5 cm. Superior e inferior 2,5 cm. Todas las páginas deben estar numeradas, así como cada gráfica o tabla. Si un artículo sobrepasa esa cantidad de páginas y el autor puede dividirlo en dos partes de forma natural, también se tomará en consideración para ser publicado en números diferentes de SEGURIDAD, CIENCIA & DEFENSA.

D. Los Artículos deben ser originales y resultados de alguna investigación o estudio. Se aceptan también Notas, Reseñas y Eventos.

E. Todos los trabajos deben estar en español.

F. Identificación del título del trabajo y se aceptan subtítulos aclaratorios.

G. Aunque la estructura del artículo es libre en lo demás, se exige que al final del artículo se manifiesten las conclusiones del mismo y la bibliografía.

H. Las Notas, Reseñas y Eventos no deben pasar de 6 páginas 8 ½ x11 a 1½ espacios y no se exige un formato especial.

I. Las notas y referencias deben aparecer al pie de página. Las referencias deben estar en formato Harvard, a saber, se encierra en un paréntesis: apellido, año, pagina (entre el año y la página se colocan dos puntos).

J. La Bibliografía debe ser en orden alfabético. Si se trata de un libro deberá contener, en este orden y separados por comas: apellido y nombre del autor, año, título del libro en cursivas, editorial, país de edición. Si se trata de un artículo deberá contener, en este orden: apellido y nombre del autor, año, título del artículo entre comillas, título de la revista en cursivas, número, editorial, país, páginas de referencia.

K. Para el uso de citas se requiere el formato APA. A continuación se muestran algunos casos:

I. Cuando la cita directa o textual es corta (menos de 40 palabras), se coloca integrada al texto del informe, entre comillas, siguiendo la redacción del párrafo donde se hace la cita. Por ejemplo:

II. En el proceso de la investigación, "no se debe empezar a escribir hasta que uno no haya completado el estudio." (Acosta Hoyos, 1979, p. 107).

III. Cuando la cita directa o textual es de 40 o más palabras, se cita en un bloque, sin comillas, a espacios sencillos, dejando una sangría dentro del texto del informe. Por ejemplo:

a) Aunque sólo las investigaciones o inventos realizados puedan alcanzar los derechos de autor que concede la ley, ente investigadores siempre se respeta la prioridad que alguien ha tenido para elegir un tema; ya que existen infinidad de problemas para investigar y de nada vale una competencia que no lleve a un mejor perfeccionamiento. (Acosta Hoyos, 1979, pp.16-17).

IV. Al final del documento se incluyen las referencias bibliográficas, si corresponde. Se ordenan alfabéticamente y se escriben según el formato APA. A continuación se muestran algunos ejemplos:

a) Libros y folletos:

I. Apellido, A. A., Apellido, B. B. & Apellido, C. C. (Año de publicación). Título del documento: subtítulo (Edición). Lugar: Editorial.

b) Artículo de publicaciones periódicas:

Autor, A., Autor, B. & Autor, C. (Año de publicación mes / mes). Título del artículo. Título de la publicación periódica, Vol., (núm.), página inicial - final.

c) Revista en formato electrónico:

Autor, A., Autor, B. & Autor, C. (Año de publicación mes / mes). Título del artículo. Título de la publicación periódica, Vol., (núm.), página inicial - final. Extraído día mes, año, de [URL].

3. LOS PROCEDIMIENTOS

A. El envío de los artículos en versión digital dirigidos a la Vice-Rectoría de Investigaciones, Extensión y Educación Continua, será a través de las direcciones electrónicas: revistacientifica@insude.edu.do, jfabriziot@insude.edu.do.

B. El Consejo Editorial someterá los trabajos recibidos a un sistema de arbitraje a través de dos miembros del Comité Científico (revisión por pares ciegos), quienes examinarán cada artículo según criterios de pertinencia, coherencia, aporte, calidad y estilo para decidir sobre la conveniencia de su publicación. En el proceso de evaluación se mantiene el anonimato de los evaluadores puesto que su selección es secreta y se mantiene el anonimato del autor enviando el material ciego, a saber borrando toda información que pueda identificarlo.

C. El proceso de evaluación comienza con la selección de los expertos sobre el tema en cuestión, luego se les envía el artículo con un formato de dictamen corto y preciso pero a la vez flexible.

D. El Comité Editorial remite a los autores de forma anónima las opiniones y recomendaciones sobre el artículo. El resultado de la revisión puede ser que: a) el artículo no debería publicarse, b) el artículo puede publicarse con las modificaciones sugeridas, o c) el artículo puede publicarse en la versión original.

E. Los autores dan permiso para que sus trabajos sean publicados en la versión electrónica de la revista que aparece en la página de la Web del INSUDE.

F. El Comité Editorial de publicaciones se reserva el derecho de no publicar un artículo que no haya sido entregado a tiempo y valorar las posibilidades de publicarlo en un próximo número.

G. Los artículos que no se ajusten a lo establecido serán devueltos hasta tanto cumplan con los requisitos señalados.

H. El envío de una colaboración para su publicación implica, por parte del autor, la autorización al INSUDE para su reproducción, en otras ocasiones, por cualquier medio, en cualquier soporte y en el momento que lo considere conveniente, siempre que el autor sea informado y esté de acuerdo con los fines de la reproducción y se haga expresa la referencia a la autoría del documento.

4. DIRECCIÓN DE LA REVISTA

Revista Científica **SEGURIDAD, CIENCIA & DEFENSA**
Instituto Superior para la Defensa,
"General Juan Pablo Duarte y Diez"
(INSUDE)
Avenida 27 de Febrero, Esquina Avenida Luperón,
Santo Domingo, Distrito Nacional, República Dominicana
Tel: 809-530-5149 Ext.: 3621
Email: revistacientifica@insude.edu.do
Versión electrónica de la revista **SEGURIDAD, CIENCIA & DEFENSA:**
http://revista.insude.mil.do/index.php/rscd

ARBITRAJE

Todos los trabajos originales enviados para publicación son sometidos a arbitraje o evaluación por pares expertos, quienes realizaran una evaluación sobre la calidad y pertinencia técnica y científica del trabajo pro- puesto. El Instituto Superior para la Defensa "General Juan Pablo Duarte y Díez" (INSUDE), a través de la Vicerrectoría de Investigación, Extensión y Educación Continua, entrega a los evaluadores una serie de aspectos para uniformar las revisiones. Los elementos de revisión y el formulario de evaluación en el que se indican los aspectos a considerar en la evaluación les serán entregados a los expertos encargados de valorar los trabajos.

Todos los evaluadores son externos, tanto nacionales como internacionales. Por ello, la Revista Científica "Seguridad, Ciencia & Defensa", tiene una base de datos de potenciales evaluadores. En el proceso de análisis y valoración, se le solicita a los evaluadores que traten el artículo con la misma rigurosidad científica con que se tratan en otras revistas internacionales arbitradas. El nombre de los evaluadores no le es revelado a los autores de los artículos; más sin embargo, los evaluadores tampoco conocen la identidad de los autores del artículo sometido a revisión.

Excelente Evaluación del Año

La Revista Científica "Seguridad, Ciencia & Defensa", otorgará un premio anual denominado: "Excelente Evaluación del Año", reconocimiento otorgado al evaluador que realice la mejor evaluación de los trabajos que les han sido confiados para evaluar.
La elección del mejor evaluador será realizada por el Rector, la Vicerrectora de Investigación, Extensión y Educación Continua y el Editor de la Revista Científica, quienes son las únicas personas que, en forma confidencial, conocen de las opiniones de los evaluadores sobre un determinado artículo. Se considerará las evaluaciones recibidas en el Instituto Superior para la Defensa "General Juan Pablo Duarte y Díez" (INSUDE), durante el año calendario por el cual se otorga el premio.

El ganador o ganadora se hace acreedor a un Certificado de reconocimiento otorgado por Instituto Superior para la Defensa (INSUDE).

COLOFÓN

La presente edición de **Seguridad, Ciencia & Defensa**,
Volumen V, N° 5, año 2019
del Instituto Superior para la Defensa
"General Juan Pablo Duarte y Díez" (INSUDE)
fue impresa en el mes de diciembre de 2019.

La edición consta de 500 ejemplares.
Santo Domingo, República Dominicana.

MINISTERIO DE DEFENSA

INSTITUTO SUPERIOR PARA LA DEFENSA
"GENERAL JUAN PABLO DUARTE Y DÍEZ"
(INSUDE)