EDITORIAL
NAVEGANTE

LA CIBERSEGURIDAD NACIONAL

ANÁLISIS DE LAS ESTRATEGIAS ADOPTADAS INTERNACIONALMENTE Y ELEMENTOS PARA SU FORTALECIMIENTO.

Juan Fernando Ormachea Montes
Rolando Espinoza Barrientos
Sabino Ernesto Villón Bruno
Nino Delgado Viera
Jorge Alberto Montaño Pisfil



LA CIBERSEGURIDAD NACIONAL

ANÁLISIS DE LAS ESTRATEGIAS ADOPTADAS INTERNACIONALMENTE Y ELEMENTOS PARA SU FORTALECIMIENTO.



Juan Fernando Ormachea Montes
Correo: juanferor@gmail.com
ORCID: https://orcid.org/0000-0002-9119-8846
Afiliación: Escuela Militar de Chorrillos (EMCH
Perfil: General de Brigada (R) del Ejército de Perú con agrado académico de DOCTOR en Desarrollo y Seguridad Estratégica. Licenciado en Ingeniería Electrónica y Maestro en Ingeniería Electrónica con mención en Telemática y Maestro en Planeamiento Estratégico y Toma de decisiones.

Rolando Espinoza Barrientos
Correo: rolando0811espinoza@gmail.com
ORCID: https://orcid.org/0000-0002-8565-1675
Afiliación: Universidad Nacional Amazónica de Madre de Dios
Perfil: Magister en Gestión Pública y Economista de profesión, Profesor Auxiliar de la carrera profesional de Administración y Negocios Internacionales, con Experiencia en Gestión y administración de Empresas.

Sabino Ernesto Villón Bruno
Correo: evillon1024@hotmail.com
ORCID: https://orcid.org/0000-0002-6679-6625
Afiliación: Escuela de Posgrado del Centro de Altos Estudios Nacionales
Perfil: Doctor en Administración (Universidad Inca Garcilaso de la Vega), Doctorado en Políticas Públicas, Seguridad Nacional y Desarrollo Sostenible (UAP), Doctorado el Educación (UAP), Doctorado en Educación (UAP), Doctor en Derechos Fundamentales (Universidad Norbert Wiener), Postdoctorado Internacional en Investigación de Ingeniería e Innovación (UNHEVAL), Postdoctorado en Producción Científica (UAP) en Maestro en Administración (Universidad Inca Garcilaso de la Vega).

Nino Delgado Viera
Correo: ninodelgadov@gmail.com
ORCID: https://orcid.org/0000-0003-3777-0765
Afiliación: Escuela de Posgrado del Centro de Altos Estudios Nacionales
Perfil: Doctor en Ciencias de la Educación (UNE) Doctorate in Scientific Research (USA) Doctorado en Políticas Públicas y Gestión del Estado, Postdoctorado Internacional en Investigación de Seguridad y Defensa (CAEN) Maestro en Docencia Universitaria y Gestión Educativa (UAP), Maestro en Desarrollo y Defensa Nacional (CAEN), Maestro E-learning (USMP), Lic. Edu. (UAP). Docente asesor, revisor y metodólogo de tesis de investigación.

Jorge Alberto Montaño Pisfil
Correo: jamontanop@unac.edu.pe
ORCID: https://orcid.org/0000-0002-9220-7134
Afiliación: Universidad Nacional del Callao
Perfil: Ingeniero Electricista, egresado de la Universidad Nacional del Callao. Maestro en Gerencia de Proyectos de Ingeniería y Doctor en Políticas Públicas: Defensa Nacional y Desarrollo Sostenible. Docente Investigador adscrito a la Facultad de Ingeniería Eléctrica y Electrónica de la UNAC. Calificado como Investigador CONCYTEC con código de registro: P0071128. Sus temas de investigación son la Seguridad Nacional y la Ciberseguridad, las energías renovables y el desarrollo energético sostenible.

Todas nuestras publicaciones son sometidas a revisión doble-ciego de pares académicos (*Peer Review Double Blinded*).

Esta publicación cuenta con licencia Creative Commons Reconocimiento - NoComercial - SinObraDerivada 3.0 Unported License.



ISBN 978-628-7623-16-3

© Juan Fernando Ormachea Montes
© Rolando Espinoza Barrientos
© Sabino Ernesto Villon Bruno
© Nino Delgado Viera
© Jorge Alberto Montaño Pisfil

© Editorial Navegante

www.editorialnavegante.com

Este libro es resultado de la investigación Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional, realizada en la “Escuela de Posgrado del Centro de Altos Estudios Nacionales”

Queda prohibida la reproducción bajo cualquier modalidad de toda o una parte de esta obra sin autorización expresa del titular de los derechos.

Diseño de carátula: Rodrigo Medrano Serrano
Diagramación: Rodrigo Medrano Serrano
Edición electrónica: Editorial Navegante

Editado en Colombia
Published in Colombia

LA CIBERSEGURIDAD NACIONAL

ANÁLISIS DE LAS ESTRATEGIAS ADOPTADAS INTERNACIONALMENTE Y ELEMENTOS PARA SU FORTALECIMIENTO.

Juan Fernando Ormachea Montes
Rolando Espinoza Barrientos
Sabino Ernesto Villón Bruno
Nino Delgado Viera
Jorge Alberto Montaño Pisfil

EDITORIAL NAVEGANTE

Índice

Índice Tablas 8
Índice Figuras 8
Introducción 13
Referencias Bibliograficas 135

CAPÍTULO 1. HISTORIA Y NOCIONES BÁSICAS DE LA CIBERSEGURIDAD 11

1.1. Primeros espionajes e intentos de encriptación 12
1.2. Creación del ciberespacio y de la ARPANet 15
1.3.Breve historia de la internet 21
1.4.Nociones sobre seguridad y vulnerabilidades en la web 25
1.5.Amenazas de los sistemas informáticos 27

CAPÍTULO 2. CIBERSEGURIDAD Y AMENAZAS 29

2.1. Inicio de los ciberataques 30
2.2. Ciberseguridad global, asuntos clave y conceptos 36
2.3.Dificultades en la atribución 43
2.4.Nociones de la ciberseguridad en la defensa nacional 45

CAPÍTULO 3. SEGURIDAD NACIONAL 47

3.1. Los ciberataques como actos de guerra y las respuestas geopolíticas 49
3.2.El ciberespacio como entorno militar y la aplicación de leyes internacionales 53

3.3.Elementos para las estrategias en ciberseguridad nacional, desarrollo e implementación 58
3.4.Marco general para las políticas estratégicas nacionales sobre los ciberconflictos 64

CAPÍTULO 4. ESTRATEGIAS INTEGRADAS DE CIBERSEGURIDAD NECESARIAS PARA FORTALECER LA SEGURIDAD NACIONAL DEL PERÚ 67

CAPÍTULO 5. PROPUESTA DE ESTRATEGIA NACIONAL DE CIBERSEGURIDAD EN PERÚBIBLIOGRAFÍA 111

Índice de Tablas

Tabla 1. Estrategias Nacionales de Ciberseguridad 2019 **102**

Índice de Figuras

Figura 1. Elementos para la legitimidad de un ataque preventivo 48 **59**
Figura 2. Estrategia Nacional de Seguridad Ciudadana de EE.UU. **76**
Figura 3. Conflictos activos al año 2019 **77**
Figura 4. Procesos de paz desde una perspectiva de sistemas **81**
Figura 5. Estrategia Nacional de Ciberseguridad de los Países Bajos. **83**
Figura 6. Estrategia Nacional de Ciberseguridad de España **87**
Figura 7. Principios rectores. Estrategia Nacional de Ciberseguridad de España **88**
Figura 8. Política Nacional de Ciberseguridad del Perú. **98**
Figura 9. Ciberamenazas y acciones maliciosas. **101**
Figura 10. Transformación digital **107**
Figura 11. Fases estratégicas de Ciberseguridad Nacional. **119**
Figura 12. Fase I **121**
Figura 13. Fase II **128**
Figura 14. Fase III **134**
Figura 15. Lineamientos para las Estrategias Integradas de ciberseguridad **136**

Presentación

En el mundo actual, el tipo de amenazas a las cuales se debe enfrentar la seguridad nacional han cambiado radicalmente. Si bien el poderío militar aun se mide por medio de la posesión de armamento bélico, esta ya no implica una total seguridad del territorio. La información se ha vuelto un elemento tanto más valioso en el surgimiento del bienestar público como también una herramienta para causar el terror y afectar la seguridad del territorio. Los ejércitos actuales, en un intento por proteger a los ciudadanos bajo su cuidado, debe adecuarse a estos cambios e implementar estrategias de protección frente a las distintas amenazas del ciberespacio.

La noción del ciberespacio puede resultar un tanto ambigua y abstracta, con lo cual se puede dificultar la comprensión de las amenazas que surgen de él. Sin embargo, muchos de los artefactos que se emplean en la vida diaria tienen alguna relación con este entorno. Las compras por internet, el uso de tarjetas de crédito, la información que se coloca y actualiza constantemente en las redes sociales o incluso la información respecto del estado civil, los montos en las cuentas bancarias o los sistemas de navegación y posicionamiento global, todos estos elementos tienen una conexión directa con el ciberespacio y, debido a la enorme importancia que poseen en la vida diaria es que reportan información sumamente valiosa y que, por lo mismo, puede ser explotada por los enemigos del Estado.

Continuamente, y quizás sin que la población civil lo note, se efectúan ciberataques que tienen como objetivo ya sea el robo de información valiosa como también la neutralización de las redes informáticas que se emplean en el territorio. Esta clase de acciones, a su vez, pueden obedecer a diferentes propósitos. Por un lado, la obtención de información valiosa se puede vender en el mercado negro y puede ser utilizada con fines

maliciosos para influenciar el comportamiento de la población atacada. Por otro lado, la neutralización de las redes informáticas puede ocasionar serias dificultades para el desenvolvimiento de la vida diaria, al impedirse la obtención de información, dificultarse las transacciones bancarias o, incluso, interferir en los sistemas de posicionamiento global. Estas dificultades, a su vez, pueden tener consecuencias aún más nefastas, como la neutralización de la capacidad bélica de un ejercito y, con ello, de su capacidad defensiva.

Por este motivo es que, en este trabajo, se busca analizar las estrategias en ciberseguridad empleadas en diferentes países para poder identificar los elementos más pertinentes en el fortalecimiento de la seguridad nacional. De este modo, se analizarán los casos en ciberseguridad de países como EE.UU., España, Países Bajos y, finalmente, Perú, con el propósito de comparar estas diferentes estrategias e identificar elementos clave que se puedan incorporar en la legislación nacional. Sin embargo, para poder realizar dicho análisis, se vuelve necesario un recorrido por los diferentes conceptos que un trabajo de tal magnitud implica. De ese modo, lo que se busca en los primeros capítulos es el repasar nociones clave como el surgimiento del ciberespacio y de las primeras amenazas que lo poblaron, así como el surgimiento y características de las estrategias de defensa que se adoptaron frente a estas nuevas amenazas. Lo que se busca con ello es una comprensión mucho más completa y cabal del análisis en torno a la seguridad en el ciberespacio con el propósito de inculcar en la población civil que, en primer lugar, este tipo de amenazas constituyen una realidad actual con consecuencias palpables y directas en la seguridad del territorio, y que por ello se debe incentivar su análisis para la formulación de posibles soluciones. Solo tomando plena conciencia de la amenaza a la que se enfrenta es que se pueden tomar acciones para su erradicación o, por lo menos, para paliar las consecuencias que estas acciones reportan.

1

CAPÍTULO

HISTORIA Y NOCIONES BÁSICAS **DE LA CIBERSEGURIDAD**

HISTORIA Y NOCIONES BÁSICAS DE LA CIBERSEGURIDAD

Las amenazas que surgen del ciberespacio, a diferencia de aquellas efectuadas por los ejércitos de los diferentes países, se originan en un entorno creado por el hombre, en el cual no se consideró la posibilidad de riesgos al incentivar el intercambio y la transmisión de información. Por ello, se vuelve importante la comprensión, en primer lugar, de que el intercambio y la obtención de datos han formado parte de la seguridad del territorio por medio de acciones militares desde el inicio de la historia escrita. De este modo, en escenarios bélicos, siempre fue importante la obtención de información enemiga que permitiera penetrar en sus defensas con el objetivo de neutralizar su capacidad ofensiva. Cuando surge el ciberespacio, esta situación no se altera, simplemente cambia de escenario, de un físico a uno virtual. Por ello, resulta importante comprender cómo surge y qué características tiene este entorno a fin de comprender mejor la amenaza a la cual la ciberseguridad se enfrenta.

1.1. Primeros espionajes e intentos de encriptación

La importancia de la información en los conflictos humanos ha sido fundamental para verificar la capacidad de las fuerzas enemigas y para idear estrategias de contraataque frente a ellas. A lo largo de la historia de los conflictos humanos, capacidades para recolectar información, como el espionaje, la interceptación de mensajes, la logística en su transporte o la anticipación del accionar enemigo se pueden verificar a lo largo de la historia de la humanidad. Sin embargo, la importancia de la obtención de información enemiga radica, principalmente, en

su capacidad para implementarse en estrategias que vulneren las capacidades contrarias. Este punto es señalado por Springer (2015), al indicar, con respecto a las campañas militares de inteligencia, que "la información solo tenía valor si es que esta podía comunicarse a tiempo, y si la transmisión de la información creaba vulnerabilidades inherentes" (p. 4). De este modo, en las campañas militares de la antigüedad, constantemente se buscaban los medios tanto para recabar información enemiga como para ocultar y descifrar la información obtenida en las campañas. Así, era posible enviar espías, así como también interceptarlos. Se podía obtener información enemiga pero también ocultarla por medio de cifrados y códigos. Este tipo de actividades de inteligencia eran usuales en las tácticas militares de la antigüedad, y se encuentran en numerosos documentos antiguos. Por ejemplo, en el relato de Josué del libro del Éxodo se detallan las campañas militares de este personaje al enviar espías a la ciudad de Jericó para recabar información sobre sus defensas. También es posible encontrar tácticas militares de espionaje en *El Arte de la Guerra*, de Sun Tzu, en tanto que este líder militar aconsejaba a sus comandantes el empleo de espías para recolectar información sobre las intenciones de sus enemigos. También, en el *Arthashastra* de Kautilya Visnú Gupta, se recomendaba el empleo de espías para enviarlos en grupos hacia el territorio enemigo.

Sin embargo, las estrategias de inteligencia de la antigüedad, en vista de las limitaciones que poseían, podía resultar contraproducentes a medida que se necesitaban más recursos para administrar los territorios conquistados. Esto ocurrió en el Impero mongol, el cual poseía capacidades estratégicas altamente sofisticadas que garantizaban el que sus enemigos no pudieran recolectar información acerca de

su ubicación y capacidades, al tiempo que se enfrentaban con gran eficacia a sus oponentes. Las tácticas de los mongoles garantizaron que pudieran conquistar un vasto territorio, el cual se expandía desde las costas del océano Pacífico de Asia hasta el Medio Oriente. Sin embargo, en vista de la enorme extensión del imperio, las comunicaciones de un extremo a otro se dificultaron. Esto es señalado por Springer (2015) al afirmar que

> El gran tamaño de sus territorios era sorprendente, pero también presentaba un problema fundamental, en que la tecnología de comunicaciones no se había desarrollado para permitir el gobierno de tan vasto imperio. Un jinete que buscaba atravesarlo de un extremo a otro podía demorarse meses de cabalgata ardua, haciendo que las estrategias más amplias sean prácticamente inútiles. (p. 5)

Sin embargo, estas dificultades se fueron superando conforme se desarrollaron las tecnologías de la información y la comunicación durante el siglo XIX. Una de las primeras máquinas para computarizar la información se desarrolló en 1822, cuando Charles Babbage diseñó la Máquina de la Diferencia, una especie de gran calculadora que podía compilar grandes cantidades de información matemática en muy poco tiempo. Babbage desarrolló una propuesta teórica para una versión más avanzada de esta máquina: la Máquina Analítica, en 1856. Sin embargo, esta máquina nunca se llegó a completar, pues el gobierno británico de ese entonces no pudo reconocer el potencial de las máquinas de computación y de sus posibles aplicaciones bélicas. Más adelante, durante la Segunda Guerra Mundial, el ejército alemán desarrolló la Máquina Enigma, diseñada para codificar mensajes y proteger las comunicaciones comerciales, diplomáticas y militares. De acuerdo con el portal Cryptomuseum (2020), esta máquina fue tan eficiente en el cifrado de mensajes

que fue empleada por los más altos mandos del ejército Nazi. Sin embargo, un avance tecnológico que resultó decisivo para que el ejército aliado logre ganar la guerra consistió en el desarrollo de la máquina Colossus, una enorme computadora electrónica que se encargó de descifrar los códigos elaborados por el ejército alemán. De este modo, estas primeras máquinas de cifrado empleadas durante la guerra constituyeron los primeros pasos en la obtención de información a larga distancia previos a la invención de la internet, con la cual las estrategias y métodos de obtención de información se radicalizarían hasta constituir, en el peor de los casos, amenazas serias para la estabilidad de la seguridad nacional. La creación de la internet, y con ella, del ciberespacio, también estuvo relacionada con los avances militares.

1.2. Creación del ciberespacio y de la ARPANet

La nación del ciberespacio, aquello en lo cual se ubica lo que conocemos como la internet, puede resultar en un concepto abstracto que no se encuentra del todo en el terreno de lo intangible, pero tampoco enteramente dentro de la materialidad. Aun así, por la familiaridad que puede suscitar debido a la interacción que se tiene con este espacio, es que la definición con respecto a él puede resultar un tanto nebulosa y confusa. De acuerdo con Singer & Friedman (2013), el término "ciberespacio", se originó en una novela de ciencia ficción escrita en 1984 por William Gibson, titulada como *Neuromancer*. La trama de la novela, sin embargo, ya podía dar pistas de los peligros que se podían originar en el ciberespacio, en tanto que se enmarca en un mundo corrupto donde los protagonistas son hackers a sueldo que deben enfrentarse con una poderosa inteligencia artificial., la etimología del término empleado

en esta novela, "ciberespacio", resulta de juntar las palabras "cibernética" y "espacio", y se define como:

> Una alucinación consensuada y experimentada diariamente por billones de operadores legítimos, en cada nación [...] Una representación gráfica de la data extraída de los bancos de cada computadora del sistema humano. Complejidad impensable. Líneas de luz esparcidas en el no-espacio de la mente. Racimos y constelaciones de data. (Gibson, 2001, pp. 69-70)

Por supuesto, esta es la definición que se le da al ciberespacio en la novela de Gibson, cuando este concepto solo formaba parte de la ficción especulativa y no un espacio delimitado dentro de la realidad cotidiana. Sin embargo, otras fuentes señalan un origen más temprano del término. De acuerdo con Lillemose & Kryger (2015), el término "ciberespacio" apreció por primera vez a finales de los años 60, cuando la artista danesa Susanne Ussing, junto con el arquitecto, Carsten Hoff, se constituyen como Atelier Cyberspace, una suerte de nombre artística que los denominaba a ambos y con el cual construyeron una serie de instalaciones tituladas como "espacios sensoriales" basados en los principios de los sistemas abiertos. Sin embargo, en estas instalaciones no se involucraban maquinarias tecnológicas, con lo cual la asociación entre el término y el mundo virtual suele adjudicarse a William Gibson.

Aun así, resulta complicado el ofrecer una definición de este espacio no solo por su naturaleza abstracta, sino porque, además el ciberespacio se encuentra en constante cambio, siempre expandiéndose y diferenciándose de su concepción inicial, como un medio para las comunicaciones y transferencia de datos dentro del ejército estadounidense. De acuerdo con Singer & Friedman (2013), el departamento de defensa de los

EE.UU. puede considerarse como el "padrino" del ciberespacio, pues sus orígenes se remontan a los intentos, durante la Guerra Fría, no solo por establecer comunicaciones más eficientes, sino por disminuir el volumen de las herramientas empleadas. De este modo, de acuerdo con Springer (2015), fue en este periodo de tiempo en que ingenieros estadounidenses desarrollaron una nueva tecnología con la creación de enormes y rudimentarias computadoras capaces de calcular con mayor precisión la trayectoria balística de las armas enemigas. Sin embargo, estas primeras computadoras eran enormes y solo podían ser transportadas en buques de guerra. De este modo, podían ocupar cuartos enteros y producían una enorme cantidad de calor que debía ser redireccionado por medio de tubos de vacío para evitar que las máquinas se sobrecalienten. En forma anecdótica, se considera que los errores de funcionamiento de las máquinas actuales, denominados como "bug" (insecto en inglés), tienen su origen en los insectos que, en ocasiones, se encontraban en estos tubos de vacío de las primeras computadoras y que dificultaban su funcionamiento. Sin embargo, estos errores se verían solucionados en gran parte cuando, en 1958, con la invención de los circuitos integrados por Jack Saint Claire Kilby, las computadoras disminuyeron su volumen y se simplificaron las complicaciones por el sobrecalentamiento. Con estas innovaciones, se daría pie a toda una nueva línea de computadoras que, además de permitir cálculos más precisos y rápidos, originarían nuevas formas de transmisión de datos que, en ese entonces, eran imposibles de imaginar. De acuerdo con Springer (2015), los primeros desarrolladores de las nuevas formas de comunicación que permitieron las computadoras "nunca esperaron que el Sistema fuera usado para el entretenimiento, el comercio, y como soporte para las necesidades en comunicación básicas de billones de usuarios" (p. 14). Sin embargo, el optimism inicial con el cual se desarrolló

esta nueva tecnología no pudo predecir las dificultades en la seguridad que esta supondría. Dado que la meta era conseguir acortar y facilitar las comunicaciones entre un punto y el otro, se diseñaron sistemas de comunicación que privilegiaron la funcionalidad y transferencia de información confiable, sin tener en cuenta las vulnerabilidades que se fueron creado en base a esta concepción.

Según Springer (2015), la estructura inicial del ciberespacio fue desarrollada por un conjunto de académicos financiados por la Agencia de Proyectos de Investigación Avanzada (ARPA), los cuales buscaron prevenir eventualidades estratégicas por parte de la Unión Soviética. Estos desarrollos, sin embargo, motivaron que los investigadores deban trasladarse constantemente, lo cual suponía que se deban implementar innovaciones respecto de las Comunicaciones que se traduzcan en nuevos mecanismos de intercambio de datos. De este modo, las innovaciones con respecto a la conexión de datos se atribuyen a Paul Baran, Donald Davies y Lawrence Roberts, quienes desarrollaron la idea de los "packet switching" (Greene, 2003). Según esto, lo que se buscaba era recolectar flujos de datos en un solo mensaje que pudiera ser direccionado a lo largo de un solo vínculo de información siempre que haya un ancho de banda apropiado para el tipo de información. De este modo, lo que se buscaba era que no solo un conjunto de computadoras se pudiera conectar, sino que cualquier computadora con la capacidad para hacerse se conecte. Así, se elaboró un protocolo que permitía a las computadoras con las direcciones y los paquetes adecuados el que puedan leerse por medio de una "interface de procesador de mensaje" (lo que en la actualidad conocemos como un router). Por todo ello, estas interfaces descomponían la información en paquetes pequeños que pudieran transferirse en vínculos de

forma sencilla, con lo cual se desarrolló la primera red a distancia de computadoras, denominada como ARPANet.

En un inicio, la red ARPANet solo contaba con 4 routers distribuidos en diferentes universidades estadounidenses: Stanford, UCLA, Santa Barbara y la Universidad de Utah. El primer mensaje que se envió por medio de ella se hizo el 29 de octubre de 1969, cuando se transmitió el comando para conectar la computadora de Stanford con la de UCLA. Dicho comando solo consistía en la palabra "login", pero el sistema era tan rudimentario que colapsó tras enviar solo las primeras 2 letras. Sin embargo, poco a poco se fueron implementando mejoras y, en 1973, la ARPANet pudo conectarse vía satélite con la matriz sísmica de Noruega. Sin embargo, no pasó mucho tiempo antes de que esta red se empleara con fines maliciosos pues, solo una década después, es que se desarrollaron los primeros virus informáticos. De acuerdo con Springer (2015), se tiene que:

> El solo uso del sistema de vinculación de las computadoras para fines positivos era un castillo en el aire imposible. Tras una década de los vínculos iniciales de la ARPANet, un gusano rudimentario de computadora había sido desarrollado, aunque este programa malicioso no fue liberado en la red hasta 1988. (p. 18)

Este gusano de computadora fue desarrollado por Robert Morris, un estudiante del Instituto de Tecnología de Massachussets, el cual consistía en un programa que se autorreplicaba y que llegó a afectar a miles de computadoras en forma imprevista. Del mismo modo, ese año también marcó el inicio del uso de virus informáticos con propósitos financieros, pues fue el año en que Donald Burleson liberó una "bomba lógica" para destruir el registro de pagos de su empleador. Con esto, a la par que

se inicia una nueva era en las comunicaciones y que permite la interconexión de diferentes dispositivos, también se inicia un nuevo tipo de ataque en base a las telecomunicaciones para el cual no se desarrollaron sistemas de seguridad. Sin embargo, a pesar de que este espacio virtual puede permitir la transferencia de enormes cantidades de datos, así como puede significar la pérdida de valiosa información, como aquella contenida en las tarjetas de crédito, ¿qué es, en última instancia, el ciberespacio? De acuerdo con Singer & Friedman (2013), el ciberespacio podría definirse como "la esfera de las redes computacionales (y de los usuarios detrás de ellas) en la cual la información es almacenada, compartida y comunicada en línea" (p. 13). Junto con esta definición, se pueden incluir algunos elementos que puedan ayudar a comprender un entorno distinto de la concepción tradicional del espacio. En primer lugar, el ciberespacio es un entorno informativo, el cual se conforma por datos digitalizados que son manipulados ya se para guardarse o transmitirse. Con esto, se puede indicar que el ciberespacio no es solo un entorno físico, con lo cual una definición que contemple categorías tradicionales de espacio no podrá dar cuenta de su naturaleza. Y al mismo tiempo, el ciberespacio no se compone de elementos únicamente virtuales, pues depende de las computadoras, el sistema y la infraestructura física que permite la transmisión de datos. Del mismo modo, el ciberespacio contempla a las personas que interactúan en él y que definen tanto sus características como sus límites. Estos límites, a su vez, no se efectúan del mismo modo que los límites territoriales de los Estados y países, y al mismo tiempo tampoco se desliga de ellos, pues son determinador por personas que sí se insertan en ellos. Sin embargo, con el desarrollo de las interacciones y la necesidad no solo por compartir información, sino también bienes y servicios, es que surge el concepto del e-commerce y la incorporación, dentro del ciberespacio, de la "infraestructura

crítica" de la sociedad, la cual se compone de la agricultura, las redes de distribución de la comida, la banca móvil, los servicios de salud, las operaciones de transporte, entre otros. Por todo ello, de acuerdo con Singer & Friedman (2013), "el ciberespacio está evolucionando [..] en algo más [...] se está convirtiendo en la plataforma dominante de la vida en el siglo XXI" (p. 15-16). Sin embargo, la mayor parte de las interacciones humanas que se realizan en el ciberespacio se realizan por medio de la internet, con lo cual conviene revisar la historia de esta herramienta para poder identificar, luego, el tipo de amenazas que se pueden dar en ella con el objetivo de especificar la importancia de generar respuestas de índole nacional en materia de ciberseguridad.

1.3. Breve historia de la internet

De acuerdo con O´Regan (2016), tras el desarrollo de la red ARPANet por parte del ejército estadounidense, esta red se limitó a aplicaciones académicas o de uso exclusivo del ejército. Durante las primeras décadas tras su aparición, la red no despertó el interés de otros sectores como el de las compañías industriales, pues en ese entonces solo era capaz de enviar mensajes dentro de la red de computadoras que se había formado entre las universidades mencionadas (Ryan, 2010). Esto cambiaría cuando, a finales de la década de los años 80, ARPANet cerrara la red para darle paso a la Fundación Nacional de Ciencia en el desarrollo de su propia red de comunicaciones, la NSFNET. Esta red consistía en múltiples redes regionales conectadas a un servidor principal. Sus vínculos originales consistían en solo 56 Kbps, pero luego se incrementarían a 1544 Mbps. El servidor principal estaba conectado, originalmente, con 13 sitios, pero luego se incrementaron dado que la comunidad académica que empleaba la red se vio cada vez más interesada, al tiempo que el

sector industrial también empezó a involucrarse con la NSFNET, con lo cual empezaron las primeras aplicaciones comerciales de ella. La internet empezó a extenderse a horizontes internacionales cuando empezó a establecer nodos en Canadá y en diferentes países europeos. Algo que se debe tener en cuenta es que, una vez que la red NSFNET empezó a internacionalizarse, la DARPA (la Agencia de Proyectos de Investigación Avanzados de Defensa) empezó a formar, en vista de los primeros ataques con gusanos informáticos, una medida de seguridad inicial frente a este tipo de amenazas (Hafner & Lyon, 1998). Por ello, formó el Equipo de Respuesta a Emergencias Computacionales (CERT) para lidiar con cualquier incidente o emergencia que pueda surgir de la operación de la red.

Más adelante, a inicios de la década de los años 90, se formó una compañía independiente y sin fines de lucro que instalaría una nueva red en reemplazo de la NSFNET. El nombre de esta compañía era Servicios Avanzados en Redes (ANS) y se encargó de instalar la ANSNET, la cual operaba con más de 45 Mbps. Esta fue la primera institución encargada de la regulación de redes comunicacionales por computadora que no estuvo regulada por el gobierno estadounidense. De este modo, la ANSNET se constituyó como una estructura de distribución de redes operada por servidores comerciales y cuyos vínculos se conectaban por medio de una red de múltiples puntos de anclaje, los cuales se denominaron como Puntos de Acceso a la Red (NAPs). A inicios de los años 90, la ANSNET contó con 160 000 puertos conectados a lo que, más adelante, se conocería como la internet (Gillies & Cailliau, 2000). Con respecto al nacimiento de la internet tal y como se conoce en la actualidad, se tiene que esta debe su origen a Berners-Lee (2000), quien inventó la World Wide Web mientras trabajaba en la Organización Europea para

la Investigación Nuclear (CERN). Curiosamente, el nacimiento de la internet debe su origen más a las necesidades de registro de los investigadores de este centro que a las necesidades de comunicación entre sus miembros. De acuerdo con O´Regan (2016), dentro del CERN debían registrarse una enorme cantidad de científicos y académicos de diversas partes del mundo. Sin embargo, un problema frecuente al que debían enfrentarse estos científicos era con respecto al registro de entrada y de salida. El centro tenía numerosos visitantes y científicos que pasaban periodos extensos de tiempo en el CERN, a veces de varios meses, así como también contaba con una cantidad considerable de personal permanente. Este inconveniente se incrementaba con el hecho de que no existía una forma eficiente ni efectiva para compartir la información entre los científicos del CERN. Por este motivo, Berners-Lee desarrolló un programa denominado como "Enquire" para facilitar el intercambio de información y mantener un registro de las entradas y salidas de los científicos. Este sistema, sin embargo, se vio beneficiado con la colaboración de otros científicos con necesidades similares. De este modo, en la década de los años 60, durante los primeros años de la ARPANet, Ted Nelson inventó los hipertextos, los cuales permitían que los vínculos estuvieran presentes dentro de un texto computacional. Por otro lado, y en un periodo de tiempo similar, Douglas Engelbart había desarrollado un dispositivo que, más adelante, sería el precursor del mouse de computadora moderno. Con estas 3 innovaciones, la red "Enquire" de Berners-Lee, el precursor del mouse de Engelbart y la incorporación de los hipervínculos de Nelson se pudo desarrollar lo que, en la actualidad, se conoce como la internet (Abbate, 1999). Para ello, Berners-Lee desarrolló un sistema que le daba a cada página web una dirección estándar conocida como Localizador Universal de Recursos (URL), el cual podía ser accesible por medio de un

Protocolo de Transferencia de Hipertexto (HTTP) y vinculada con otras páginas por medio de los hipervínculos dentro del texto, en la forma de un Lenguaje de Margen de Hipertexto (HTML). Las páginas web eran accesibles por mediante un buscador web, el primero de ellos desarrollado, también, por Berners-Lee. Más adelante surgieron buscadores como Gopher o Mosaic, los cuales fueron reemplazados durante los años 90 por Netscape y este, a su vez, fue reemplazado por Internet Explorer. Así, la internet crea un espacio en el cual los usuarios pueden recopilar información desde cualquier parte del mundo por medio de su acceso a un buscador o de una dirección web. Estas operaciones, a su vez, son reguladas por el World Wide Web Consortium, dirigido por Berners-Lee.

La invención de la internet es uno de los pasos más grandes que ha dado la humanidad con respecto al desarrollo de la computación y el acceso a la información. De acuerdo con O´Regan (2016), el uso de la internet desde su empleo marcadamente académico hasta donde está ahora, transformó una parte integral en la vida de las personas. Este enorme acceso a la información constituye una revolución con respecto al pasado en tanto que se rompieron una serie de barreras, como el hecho de que ninguna organización controla la internet, así como ninguna computadora. Existen millones de computadoras interconectadas, las cuales realizan toda una serie de transacciones comerciales sin ningún tipo de barrera física. Entre estas aplicaciones, se pueden nombrar aquellas dentro de la industria del turismo, el marketing en línea, las compras online, los servicios de reclutamiento, la banca móvil, los servicios de apuestas, subastas, canales de información y redes sociales, entre otros. Con la llegada de la internet se desarrollaron comercios y oportunidades de negocios completamente nuevas

e innovadoras, pero, con ello, también emergieron nuevas vulnerabilidades que, generales, no son comprendidas por la gran mayoría de la población y suelen ser explotadas por un número reducido de personas con fines personales.

1.4. Nociones sobre seguridad y vulnerabilidades en la web

De acuerdo con Springer (2013), las vulnerabilidades que pueden ser explotadas dentro del ciberespacio suelen ser desviaciones con respecto al uso que, originalmente, se le había dado a un dispositivo. Sin embargo, cuando esta desviación se realiza de forma intencional por parte de un adversario, ya se puede hablar de un problema de seguridad. De este modo, la noción de seguridad dentro del ciberespacio tiene que ver con la explotación de vulnerabilidades por parte de una tercera persona que busca beneficiarse de las vulnerabilidades que son explotadas dentro de un sistema, ya sea para obtener información privada, para destruir un determinado sistema o para prevenir el uso que originalmente se le había dado. Dentro del ámbito de la seguridad, por lo general se consideran 3 dimensiones: la confidencialidad, la integridad y la disponibilidad. Con respecto a la confidencialidad, esta se refiere a los esfuerzos por mantener la información de un determinado sistema en forma privada. La privacidad resulta en extremo importante pues, en la era de la información, la data puede llegar a tener un valor sumamente grande, por lo cual debe ser protegida a como dé lugar. Algunas herramientas empleadas para proteger la información pueden ser la encriptación y el acceso restringido. Por otro lado, la integridad se refiere al hecho de que “el sistema y la data en él no han sido inapropiadamente alternados o cambiados sin autorización” (Singer & Friedman, 2013, p. 35). La integridad de un sistema puede ser un indicador del nivel de daño efectuado

cuando se penetra un sistema. Según Bergman & Mazzetti (2019), en esto consistió la estrategia del ataque Stuxnet, en el cual se alteraron los mecanismos de detección de amenazas del sistema de defensa iraní por parte de los gobiernos israelí y estadounidense. Por último, con respecto a la disponibilidad, esta se refiere a la disponibilidad por usar un sistema en forma anticipada. En ese sentido, los problemas de seguridad que se podrían originar tendrían que ver con la interferencia por parte de una tercera persona en alterar la disponibilidad en el uso de un sistema de alguna forma. Un ejemplo de este tipo de escenario podría ser algún ataque a los sistemas GPS de geolocalización, en tanto que se previene a los usuarios de poder usarlo.

La confiabilidad, integridad y disponibilidad son las 3 dimensiones en las que se suelen considerar los ataques en el ciberespacio. Además de estos, Singer & Friedman (2013) menciona una más, relacionado con la resiliencia. Según esta dimensión de la seguridad, la resiliencia es aquello que permite que un sistema pueda soportar los ataques a su seguridad en lugar de someterse al daño recibido. Sin embargo, un medio para poder ejercitar la resiliencia consiste en aceptar la inevitabilidad de los ataques e incluso el incorporar un grado mínimo de vulnerabilidades en las defensas. El objetivo de la dimensión de la resiliencia consiste en la capacidad de un sistema por mantenerse operacional. Por este motivo, “el objetivo debe ser el priorizar los recursos y las operaciones, proteger a los activos clave y a los sistemas de los ataques, y finalmente el reestablecer las operaciones normales” (Singer & Friedman, 2013, p. 36). De este modo, las dimensiones contempladas obligan a considerar el hecho de que, con respecto a la seguridad, ningún sistema informático será infalible.

1.5. Amenazas de los sistemas informáticos

Según Singer & Friedman (2013), la guerra informática consiste en el empleo de medios digitales para atacar la infraestructura de una nación, de forma tal que se ocasiona un daño similar al de un ataque militar. La guerra informática se puede presentar en una variedad de formas. En un sentido general, los ataques informáticos pueden formar parte de acciones de guerra frente a un determinado enemigo. Un ejemplo de ello lo pueden constituir los ataques dirigidos a neutralizar el sistema de defensa de la fuerza aérea del enemigo para poder atacarla más fácilmente (Weinberg, 2007). Sin embargo, los ataques informáticos también pueden contemplar el uso de tácticas como el espionaje o la propaganda. A pesar de ello, el nivel de letalidad que pueden comprender este tipo de ataques ha sido equiparado con aquel de las armas biológicas dentro de un mundo interconectado (Shamah, 2012). A pesar de todas estas amenazas, según Singer & Friedman (2013), parece que no se está haciendo lo suficiente para prevenir y concientizar a la población con respecto al peligro que este nuevo tipo de guerra representa. De este modo, en 2011, el gobierno estadounidense desclasificó videos respecto de una prueba en ciberseguridad de 2007, pero realizaron pruebas públicas con la presencia de reporteros para que estos puedan observar una simulación de vulneración a la ciberseguridad. Por ello, la intención del gobierno era de "mostrar que incluso sus propios expertos no podían prevenir a un equipo de hackers contratados [...] de sobrepasar las defensas de una facilidad crucial" (Singer & Friedman, 2013, p. 37). Estos esfuerzos por demostrar la gravedad de estos ataques también se deben a la falta de importancia que el gobierno estadounidense para otorgarle a este tipo de amenaza, y a la

ciberseguridad en particular. Por este motivo, resulta pertinente el análisis de las estrategias en ciberseguridad, no solo en vista de los daños nefastos que estas pueden ocasionar, sino debido a la poca importancia que se le da al tema en general y, en forma específica, a la falta de adopción de medidas adecuadas contra este tipo de amenazas en nuestro país.

2

CAPÍTULO

CIBERSEGURIDAD
Y AMENAZAS

CIBERSEGURIDAD
Y AMENAZAS

Como se vio anteriormente, la ciberamenaza constituye una realidad con consecuencias palpables y frente a la cual se debe estar preparado. Por ello, existen muchas formas de ciberataques que, si bien en un inicio se limitaban a las redes primigenias que surgieron en un primer momento, en la actualidad pueden afectar gravemente la capacidad defensiva de una nación e, incluso, pueden ponerla en riesgo frente a otros países. Por ello, en esta sección se comienza con el análisis de uno de los primeros ciberataques a nivel militar para poder entender no solo la naturaleza y condiciones en las cuales se efectuó, sino también la importancia que reporta el ser consciente de la amenaza que constituyen los ciberataques y que, en muchas ocasiones, pueden determinar la facilidad en la penetración de las defensas cuando esta importancia se deja de lado. Más aún, la falta de importancia que se le puede dar a las ciberamenazas puede verse incrementada por las propias características de la interacción en el ciberespacio, en las cuales existen enormes dificultades de atribución en tanto que resulta sumamente difícil el identificar a los culpables de un ciberataque, lo cual motiva, a su vez, la adopción de estrategias de defensa distintas de las adoptadas antes de estas amenazas y que obligan a contemplar nuevas formas de acción de defensa.

2.1. Inicio de los ciberataques

De acuerdo con Springer (2015), uno de los primeros ataques en ciberseguridad de los que se tiene noticia lo constituye el ataque a los Laboratorios Rome, de la Fuerza Aérea Estadounidense, en 1994 y efectuados por dos adolescentes. Esta información es detallada en un informe del subcomité

permanente de investigaciones, el cual opera bajo el Senado estadounidense (Federation of American Scientist, 1996). De acuerdo al informe, el 28 de marzo de 1994 (aunque las investigaciones revelarían que las penetraciones al sistema iniciaron el 23 de marzo), los administradores del sistema de cómputo del Centro del Desarrollo Aéreo Rome, en la Base Aérea Griffiss de Nueva York ("Laboratorios Rome"), descubrieron que su red había sido penetrada y comprometida por un "chuponeo" ilegal telefónico bajo un programa computacional denominado como Sniffer, el cual había sido instalado en uno de los sistemas conectados a la red de los Laboratorios Rome. Este ataque resultó extremadamente significativo en vista de que los Laboratorios Rome son el primer centro de mando de la Fuerza Aérea Estadounidense, y dentro de sus proyectos de investigación se incluyen los sistemas de inteligencia artificial, los sistemas de rastreo de radar, y los sistemas de detección y rastreo de objetivos. Tras detectar el programa Sniffer, los administradores del laboratorio inmediatamente notificaron a la Agencia de Defensa de Sistemas Informáticos (DISA) de que varias computadoras de los Laboratorios Rome habían sido penetradas electrónicamente por un intruso desconocido. La DISA posee un Equipo de Respuesta para Emergencias Computarizadas (CERT), el cual reconoció la severidad del incidente y notificó a la Oficina de Investigaciones Especiales de la Fuerza Aérea de EE.UU. (AFOST), quienes, a su vez, notificaron a los expertos en seguridad computacional del Centro de Información para la Guerra de la Fuerza Aérea de EE.UU. La investigación preliminar de los expertos determinó que 2 individuos desconocidos habían penetrado 7 de las computadoras de los Laboratorios Rome y tuvieron acceso a toda la información de los sistemas, descargaron archivos e instalaron otros programas Sniffer en cada una de ellas, los cuales comprometieron a otras 30 computadoras y a un total de 100 cuentas de usuarios al capturar sus identificaciones y contraseñas de acceso. Se leyeron,

copiaron y borraron los correos electrónicos de los usuarios, así como también se leyeron y copiaron programas de simulación desclasificados sobre acciones tácticas. Tras estos ataques, los intrusos emplearon las instalaciones de los laboratorios para lanzar ataques a otros sistemas militares, gubernamentales, comerciales y académicos alrededor del mundo. Tras descubrirse la penetración, el equipo de investigación se comunicó con el comandante de los laboratorios y le dio la opción de asegurar todos los sistemas o dejar libres algunos de ellos para que los agentes pudieran intentar rastrear el camino de los atacantes hasta su origen e identificarlos. Tras elegir esta segunda opción, se determinó que la mayoría de los ataques se originaron de dos servidores comerciales de internet, cyberspace.com, en Seattle, Washington y mindvox.phantom.com en Nueva York. Este último servidor resultó significativo para la investigación, pues algunos artículos de periódicos indicaban que este era administrado por "dos antiguos miembros de la Legion of Doom de la Costa Este".

Tiempo después, se determinó que los alias de los hackers responsables de los ataques eran Datastream y Kuji. Esta información fue reforzada por un informante quien, el 5 de abril de 1994, se comunicó con un hacker bajo el alias de Datastream Cowboy, proveniente del Reino Unido. Este hacker se comunicó con el informante vía e-mail y reveló que se trataba de un adolescente de 16 años al cual le gustaba atacar sitios .MIL (un sufijo ligado a muchas direcciones militares de internet) porque eran particularmente inseguros. El hacker incluso proporcionó al informante el número de teléfono de su casa como parte de un boletín de hackers que él había creado. Tras esto, la Fuerza Aérea de EE.UU. se comunicó con el Scotland Yard del Reino Unido, quienes monitorearon las actividades del hacker por

medio de sus líneas telefónicas. Así, se determinó que cada vez que se penetraban los sistemas de los laboratorios Rome, el hacker ingresaba a ellos por medio de un uso ilegal de las líneas telefónicas. Por todo ello, Scotland Yard solicitó una autorización de allanamiento y el hacker fue arrestado. Con respecto al otro hacker, bajo el alias "Kuji", este fue arrestado el 21 de junio de 1996. Tenía 21 años de edad.

Después de este ataque, el Congreso de los EE.UU. buscó implementar medidas de contención como parte de su presupuesto en el Departamento de Defensa en 1996 pero, de acuerdo con Springer (2015), "hizo muy poco para lograr incluso un nivel rudimentario de seguridad en internet" (p. 19). Desde entonces, los ataques en el ciberespacio se han incrementado y han sido cada vez más sofisticados, y esto se debe en gran parte por el hecho de que, mientras el sector privado refuerza su presencia, "el gobierno hizo casi nada para incrementar la seguridad de la estructura de la red" (Springer, 2015, p. 20). En el año 2000, el Buró Federal de Investigación estadounidense (FBI) empezó a investigar una serie de ataques denominados como "Moonlight Maze". Estos ataques empezaron en 1996 y afectaron a diferentes instituciones gubernamentales, como la NASA o el Pentágono. Según Doman (2018), para finales de 1999, la fuerza de defensa contra estos ataques estaba compuesta por 40 especialistas miembros del ejército, la policía y el gobierno. Tras una exhaustiva investigación, el gobierno ruso fue el principal sospechoso tras los ataques, con lo cual se clasificaron como una Amenaza Avanzada Persistente. Sin embargo, a pesar de la seriedad de los ataques, no se pudo identificar a los culpables, quienes habían penetrado cientos de servidores gubernamentales. Esto se debe a que, como se mencionó, el principal sospechoso resultó ser el gobierno ruso,

no solo porque se rastrearon los ataques hasta un servidor de este país, sino porque "el gobierno ruso impidió cualquier intento de investigación, con lo cual sugirió implícitamente que los culpables podrían estar operando bajo instrucciones del Estado" (Springer, 2015, p. 20).

Por todo ello, se puede indicar que los ataques que han ocasionado las consecuencias más devastadoras con respecto a la economía y el impacto social han sido, por lo general, ataques indiscriminados por medio de ciertos virus y gusanos informáticos. Sin embargo, dentro de la comunidad hacker, este tipo de ataques no tienen el prestigio de la elaboración de programas de software capaces de maniobrar en forma sutil y elegante ataques con un mayor potencial destructivo. Esto se traduce no solo en un número más elevado de computadoras infectadas, sino también en el acceso a la infraestructura informática de la sociedad. Según White (2020), en el año 2000, el virus I-LOVE-YOU, creado por Reonel Ramones y Onel de Guzman en las Filipinas causó un total de 10 billones de dólares en daños por su facilidad en infiltrarse en múltiples servidores. De este modo, las víctimas eran engañadas para abrir un correo titulado LOVE-LETTER-FOR-YOU, el cual contenía un virus que reescribía archivos, robaba contraseñas y automáticamente enviaba copias de sí mismo a todos los contactos de la cuenta en Outlook de la víctima. Más adelante, en 2003, un gusano informático denominado como "SQL Slammer" fue capaz de apagar completamente todo el servicio de internet del planeta por más de 12 horas y, en la actualidad, continúa siendo una amenaza para servidores que no están protegidos con el parche MS02-039. El gusano Slammer es aún uno de los virus más fácilmente detectables del mundo, y su gran capacidad para expandirse proviene, en parte, por el extendido uso de copias pirateadas de programas de Microsoft, los cuales no permiten

instalar los parches de seguridad que se necesitan para detener el avance del virus. Tras el desarrollo del gusano Slammer, se desarrolló el MS Blaster y, en 2004, el virus MyDoom, el cual causó un total de 2 billones de dólares en daños.

Sin embargo, la mayor parte de estos virus y gusanos informáticos son elaborados por hackers individuales, quienes, a inicios de la década de los años 2000, buscaban el reconocimiento de la comunidad al publicar en forma anónima sus ataques, como fue el caso de Database Cowboy. Sin embargo, en la actualidad, los ataques en el ciberespacio ya no solo se efectúan por medio de personas individuales a baja escala, sino que estos son efectuados por equipos organizados y financiados por instituciones gubernamentales para efectuar acciones de ciberespionaje que, en muchos casos, pueden ser consideradas como actos de guerra. El 13 de diciembre de 2020, se descubrieron una serie de ataques informáticos por parte del grupo Cozy Bear, auspiciado por la Agencia de Inteligencia Rusa (SVR), los cuales afectaron al Departamento del Tesoro de EE.UU., y la Administración Nacional de Telecomunicaciones e Información, entre otras instancias gubernamentales (Sanger et al., 2020; Nakashima, 2020). Se ha descubierto, por el momento, que estos ataques tuvieron una duración de entre 6 a 9 meses y se efectuaron por medio de vulnerabilidades en productos de Microsoft y VMWare, los cuales emplearon el software SolarWinds Orion, usado ampliamente en instituciones del gobierno y en la industria de EE.UU. Estos ataques permitieron acceder a los correos del personal de alto nivel, así como el uso de autentificaciones federales por medio de la identificación de las víctimas (Stubbs et al., 2020). Estos ataques, a su vez, afectaron a la población civil, conformada por decenas de miles de usuarios del software SolarWinds. Sin embargo, mientras que algunos políticos del país, como el senador Richard J. Durbin, calificaron

los ataques como un acto de guerra, el aún presidente de los EE.UU., Donald Trump, no les dio mucha importancia e indicó que "todo está bajo control" (Stracqualursi et al., 2020). Esto demuestra que, a pesar de contar con sofisticados sistemas e instituciones encargadas de regular la seguridad nacional en materia de ataques en el ciberespacio, aún no se le otorgan a esta clase de amenazas la importancia debida para salvaguardar la seguridad nacional. Por este motivo, conviene analizar en qué consiste esta clase de amenazas en forma conceptual para, más adelante, comprender la importancia por la implementación de medidas más sofisticadas con respecto a estos ataques.

2.2. Ciberseguridad global, asuntos clave y conceptos

De acuerdo con Kshetri (2016), se ofrecen algunos conceptos clave con respecto a las nociones de ciberseguridad, estrategia en ciberseguridad, el cibercrimen, el ciber poder, entre otros. De este modo, la ciberseguridad involucra las tecnologías, conceptos, políticas, procesos y prácticas empleadas para proteger activos como las computadoras, infraestructura, aplicaciones, etc. En términos más simples, la ciberseguridad consiste en "la habilidad para protegerse a sí mismo y a sus instituciones contra ciberamenazas" (Kshetri, 2016, p. 3). Por este motivo, las estrategias en ciberseguridad se relacionan con los planes y acciones que se contemplan con el propósito de facilitar el logro de ventajas competitivas a nivel nacional. La implementación las estrategias en ciberseguridad se relacionan con el desarrollo de tecnología y entrenamiento de fuerza de trabajo dentro de los lineamientos de las estrategias en ciberseguridad. Estas estrategias buscan implementar medidas en contra del cibercrimen, el cual se define como "una actividad criminal en la cual las computadoras y las redes de computadoras son los medios principales para cometer ofensas" (Kshetri, 2016, p. 3). Algunos ejemplos que se ofrecen

con respecto al cibercrimen son los robos y penetraciones en el ciberespacio, así como también la ciberobcenidad, los ataques a la infraestructura crítica (como aquel realizado en 2003 por el virus SQL Slammer) y las extorciones también realizadas en estos espacios. En los últimos años, un tipo de extorción que se ha incrementado ha sido el relacionado con la "pornografía de la venganza" en la cual una expareja extorsiona a otra con difundir imágenes y contenido sexual de la persona en diferentes medios (como cuentas de Whatsapp o redes sociales) a cambio de beneficios económicos o de otra índole, para la cual, hasta el 2014, no había una sanción penal en los Estados Unidos (Keats & Franks, 2014). En el país, este tipo de extorción en el ciberespacio recién fue contemplada en el código penal el 12 de setiembre de 2018 por medio del Decreto Legislativo Nro. 1410 (El Peruano, 2018). Además de esto, el empleo de este nuevo tipo de extorción por medio de material audiovisual difundido en el ciberespacio puede dar cuenta de la noción de ciberpoder. Según Kshetri (2016), el ciberpoder puede definirse como "la habilidad para usar el ciberespacio para crear ventajas e influenciar eventos en otros ambientes operacionales y a través de los instrumentos del poder" (p. 3). Esta noción por lo general pertenece al ámbito de las relaciones internacionales, en tanto que la capacidad de un Estado por emplear medios informáticos a su favor puede ser determinante en la modificación del mismo espacio para servir a sus propósitos. Un ejemplo de ello se puede encontrar en la regulación estricta del uso de la internet en China, la cual afecta tanto la capacidad de los usuarios para publicar contenido online como para poder verlo y recibirlo. Por lo general, el contenido censurado en este país suele restringirse a las páginas pornográficas, al contenido que promueve el crimen y a ciertos temas que pueden resultar polémicos. Este tipo de censura ha disminuido considerablemente la libertad de expresión de la prensa china, así como también limita la interferencia de gobiernos extranjeros en la política nacional

(Human Rights Watch, 2006). Esta censura con respecto al acceso a la información en China no solo demuestra la enorme capacidad del gobierno por vigilar el contenido al cual tienen acceso sus ciudadanos, sino que también motiva la emergencia de toda una generación de jóvenes quienes, al haber crecido bajo las políticas de censura del gobierno chino, en la actualidad muestran tendencias nacionalistas que se alinean a la ideología del Partido Popular Chino que gobierna el país (Wang, 2020).

Por último, con respecto a la naturaleza de los ataques informáticos, por lo general estos suelen clasificarse en dos grandes grupos: los ataques oportunísticos y los ciberataques dirigidos. Con respecto a los ataques oportunísticos, estos no suelen enfocarse en un solo objetivo, sino que emplean malware que es distribuido en grandes cantidades para que cualquier persona lo pueda descargar o implementar en sitios web a los que cualquier persona puede tener acceso, lo cual suele realizarse por medio de cadenas masivas de correo electrónico. Por otro lado, con respecto a los ciberataques dirigidos, estos suelen combinar múltiples esfuerzos por atacar un solo servidor, con lo cual constituyen un tipo de Amenaza Avanzada Persistente (APT), de forma similar a lo ocurrido en los ataques a instancias gubernamentales estadounidenses descubiertas en diciembre de 2020. De este modo, en esta clase de ataques, los perpetradores “están interesados en atacar una red en particular” (Kshetri, 2016, p. 5), con lo cual, si se obtienen los recursos, estrategia y talento necesarios, resulta “casi imposible el asegurar una red contra un adversario lo suficientemente hábil y tenaz” (Schneider, 2012, p. 1528).

Las diferentes modalidades que pueden adoptar los ciberataques, tanto a nivel individual o amateur como respecto de grupos de especialistas auspiciados a nivel gubernamental pueden dar cuenta del hecho de que, en materia de

ciberseguridad, existe una evidente dificultad por establecer el dominio. La noción de dominio, en el ámbito militar, tiene que ver con la capacidad de control respecto de diferentes dimensiones dentro del campo de batalla. Sin embargo, en el ciberespacio, el dominio no constituye una meta alcanzable debido a que los criterios para establecer el dominio en la guerra convencional no pueden aplicarse del mismo modo ni determinar la efectividad de los ciberataques. Por este motivo es que países con un bajo o, por lo menos, cuestionable poderío militar, como pueden ser el caso de Irán o Corea del Norte, pueden resultar sumamente efectivos con respecto a su capacidad para realizar ciberataques. Esta realidad es lo que motiva a Gartzke (2013) a afirmar que Estados con una tecnología pobremente desarrollada pueden enfrentarse a grandes desafíos y dificultades, pero, en forma contraria a estos estereotipos, los llamados regímenes rebeldes y económicamente atrasados no han sido, de acuerdo con Kshetri (2016), observadores pasivos de los ciberataques y las tácticas militares en el ciberespacio. De hecho, países como los mencionados han desarrollado capacidades avanzadas para la guerra en el ciberespacio, así como una enorme capacidad para infligir daño en sus enemigos. En el caso del ejército iraní, las estrategias militares en el ciberespacio forman parte de la "guerra suave" por parte de Irán, y ha desarrollado sus capacidades hasta tal grado que, según expertos, el país se ha constituido como un poder militar emergente en la ciberguerra (O´Flaherty, 2020; Siboni & Kronenfeld, 2014). Desde el año 2010, la organización denominada como "El Comando de Ciberdefensa" ha operado en Irán bajo la supervisión de la Organización de Defensa Civil Pasiva, la cual en realidad constituye una subdivisión del Comando Conjunto de las Fuerzas Armadas Iraníes (Hossein, 2012). Este impulso hacia el desarrollo de capacidades de defensa y ataque en el ciberespacio se dio, de acuerdo con Kshetri (2016), en base a la amenaza del gusano Stuxnet que dañó la capacidad de procesamiento de uranio.

Esta incapacidad inicial del país frente a las amenazas de la red motivó que, en 2012, el Supremo Líder Ayatollah Ali Khameni creara el Supremo Concilio del Ciberespacio, encargado de vigilar la defensa de la red computacional de la República Islámica y desarrollar nuevas formas de infiltración o ataque de las redes computacionales enemigas.

A partir de entonces, el ejército iraní ha demostrado una gran capacidad para lanzar ciberataques sofisticados hacia sus enemigos. De acuerdo con Finkle (2014), en un periodo de 3 años, un equipo coordinado de hackers del ejército iraní fue capaz de crear diferentes cuentas falsas de Facebook, así como diferentes sitios web de noticias, para espiar a líderes políticos y militares estadounidenses, israelíes y de otros países. Entre sus objetivos, se encontraba un Almirante de la Marina estadounidense, así como abogados y embajadores del mismo país, como también miembros del lobby entre Israel y los EE.UU., personal del Reino Unido, Arabia Saudita, Siria, Irak y Afganistán. Estos hackers al servicio del ejército de Irán pudieron establecer contacto con un total de 2000 miembros del ejército estadounidense por medio de 14 cuentas falsas para establecer conexiones por medio del Facebook como también por la página web falsa NewsOnAir.org. De este modo, para poder crear una apariencia de credibilidad, los hackers establecieron contacto con objetivos de alto valor al entablar conexiones con los amigos, compañeros de clase, colegas y familiares del personal militar. En un primer momento, estos no enviaron contenido malicioso como malware o algún tipo de virus, sino que se valieron de artículos de la página falsa NewsOnAir.org para establecer confianza. Luego de esto, mandaron software malicioso o redireccionaron a sus objetivos hacia portales web en los que se solicitaban las credenciales de registro de los militares.

Por otro lado, con respecto a las capacidades militares de Corea del Norte en el ciberespacio, se tiene que "los ciberataques de Corea del Norte se consideran dentro de las amenazas más significativas para Corea del Sur, como también para las economías occidentales" (Ksherti, 2016, p. 6). En el caso de Corea del Norte, el ente regulador de los ataques en el ciberespacio lo constituye el Buró 121, el cual es la agencia de ciberguerra y forma parte del Buró General de Reconocimiento el ejército norcoreano. De acuerdo con Pike (2018), sin embargo, este Buró también se encarga de realizar operaciones clandestinas no reguladas por las convenciones de guerra, mayormente en Corea del Sur, Japón y los EE.UU. Con respecto a sus ataques en el ciberespacio sobre Corea del Sur, se sabe que este Buró ha desarrollado capacidades de ciberataque sobre el sistema de suministro de poder eléctrico, además de continuas amenazas y deshabilitación de páginas web surcoreanas para promover propaganda de ideología norcoreana.

Sin embargo, un caso conocido respecto de las capacidades de ciberguerra de Corea del Norte lo constituye el ataque del grupo de hackers conocido como "Guardianes de la Paz" sobre la productora Sony Pictures Entertainment en noviembre del 2014, a raíz del estreno de la película The Interview, la cual mostraba una representación caricaturizada del Líder Supremo de Corea del Norte, Kim Jong-Un. Como prueba de la responsabilidad de Corea del Norte sobre los ataques a Sony Pictures, se tiene que un análisis realizado sobre el código fuente empleado para perpetrar los ataques tenía componentes similares a los usados en ataques informáticos efectuados sobre Corea del Sur en el año 2013, así como el uso de código fuente en coreano, los cuales fueron atribuidos, de acuerdo con Robertson et al. (2014) a otro grupo de hackers, denominado como DarkSeoul, un grupo ligado al ejército norcoreano.

Frente a estos dos casos de naciones con serias precariedades económicas y sociales, se tiene que la noción de dominio militar tradicionalmente empleada para calificar el poderío militar de una nación no necesariamente se aplica con respecto a los ciberataques. Razón que lleva a Kshetri (2016) a afirmar que "el avance tecnológico de una nación no necesariamente lleva a una superioridad informática" (p. 7). Más aún, parece ser que es en países con profundas precariedades sociales y, sobre todo, económicas, en que se suelen desarrollar las habilidades informáticas con respecto a los ciberataques para poder incrementar la capacidad bélica de la nación. En el caso de los países desarrollados, en los cuales es posible contar con una gran cantidad de recursos bélicos, no necesariamente se tendrá la misma necesidad por desarrollar la ciberseguridad, lo cual podría explicar, en parte, la razón por la cual sus servidores en internet han sido fácilmente vulnerados por adolescentes. Es por este motivo que, de acuerdo con la evidencia recopilada, se tiene que las grandes democracias industrializadas se encontrarían perdiendo la carrera informática respecto de la capacidad para protegerse de los ciberataques. Por otro lado, parte de las dificultades de los países industrializados, y que suele ser aprovechada por los países con habilidades avanzadas para el ciberataque, tiene que ver con la capacidad para asimilar tanto métodos simétricos como asimétricos para la defensa en el ciberespacio. De acuerdo con Metz (2001), la estrategia más eficaz para la defensa tiene que ver con la implementación de estas dos modalidades. Más aún, este tipo de aproximación a la defensa en el ciberespacio se relaciona con las limitaciones inherentes a las tecnologías para la información y la comunicación. Por este motivo, el poderío militar de naciones industrializadas orientales, como lo son China y Rusia, así como de regímenes económicamente precarios como Irán y Corea del Norte, radica en el hecho de que emplean tanto estas tecnologías para la

información y la comunicación, como también otro tipo de estrategias no convencionales y que no se enmarcan dentro de este tipo de tecnología.

2.3. Dificultades en la atribución

Una característica de los ciberataques es que estos se pueden efectuar por medio de un solo individuo o mediante todo un equipo coordinado, lo cual implica que, en ambos casos, resulta en extremo difícil identificar a los culpables responsables de estos ataques. Incluso es posible que un determinado ciberataque no tenga un culpable en particular, sino que se puede realizar por medio de una inteligencia artificial que se haya desarrollado para adquirir capacidades de ataque sin que estas hayan sido programadas por un humano en específico (Vilarino, 2018). Por este motivo es que, con respecto a los ciberataques, pueden surgir problemas de atribución. Al respecto, se tiene que la atribución se define como "la determinación de la identidad o localización de un atacante o de su intermediario" (Wheeler & Larsen, 2007, p. 1). Sin embargo, debido a que, en sus etapas de desarrollo, la internet fue diseñada para privilegiar la compatibilidad en el uso entre la interfase y el usuario es que no se consideraron cuestiones respecto de un control más estricto de la identidad de los usuarios, lo cual facilitó la aparición de las prácticas contra la ciberseguridad ya descritas. De este modo, en vista del anonimato del atacante y de los problemas respecto de la identificación de la atribución que surgen en este contexto es que resulta en extremo complicado el emplear la amenaza del castigo para limitar a un potencial atacante de emplear estos métodos informáticos. Por otro lado, las acciones de contraataque que podrían desincentivar este tipo de prácticas también requieren de la capacidad de la víctima para reconocer a su atacante, en tanto que, en el ciberespacio, no es

posible emplear métodos tradicionales de identificación de los criminales, como lo pueden ser las muestras de ADN, las huellas dactilares u otro tipo de información con respecto al atacante. Esta situación, por supuesto, resulta en extremo beneficiosa para los hackers, pues los métodos de rastreo de ataques, por lo general, conducen a botnets (un conjunto de máquinas informáticas que realizan acciones de manera autónoma para controlar servidores en forma remota), con lo cual no se puede identificar a la persona encargada de programarlo. Un ejemplo que podría ilustrar la dificultad por identificar a los atacantes lo constituye el caso de la ruptura de data en el banco estadounidense JPMorgan Chase, el cual se estima que llegó a comprometer unos 83 millones de cuentas y unos 7 millones de pymes de EE.UU. (Siegel, 2014), con lo cual constituyó uno de los ciberataques más grandes en la historia del país. Este ciberataque, el cual fue admitido por la entidad bancaria en setiembre de 2014, fue descubierto por el equipo de seguridad de JPMorgan-Chase en julio de ese año, pero no fue sino hasta agosto que la amenaza pudo ser contenida (Goldstein et al., 2014; Chan, 2014). De acuerdo a las investigaciones efectuadas por el propio banco, se pudo determinar que la información de ingreso a las cuentas se los usuarios, como lo son los números de seguridad social o las contraseñas, no fue recuperada por los hackers, pero estos sí tuvieron acceso a nombres, correos electrónicos y direcciones postales, así como a los números telefónicos de las cuentas de los clientes, lo cual despertó la amenaza de potenciales ataques de phishing (un intento fraudulento de obtener información al aparentar ser una entidad confiable por medio de una comunicación electrónica) [Rushe, 2014]. Por otro lado, estos ataques tuvieron como objetivos adicionales otras 9 entidades bancarias además de JPMorgan Chase. Hasta el 9 de octubre de 2014, se pensaba que la firma Fidelity Investments también hacía sido vulnerada por los ataques. Sin embargo, esta no fue atacada, así como tampoco

se llegaron a concretar ataques a compañías como Citigroup, Financial Corporation, HSBC Holdings, Regions, E*Trade, entre otras (Riley, 2014). En noviembre de 2015, empezaron los juicios hacia los hackers responsables y se llegó a enjuiciar a Gery Shalon y a Ziv Orenstein, quienes fueron arrestados en Israel y expatriados a los EE.UU. de acuerdo con la legislación israelita. Sin embargo, esta clase de ataques debieron ser coordinados por todo un equipo de hackers especializados por algún estado enemigo de los EE.UU. y que, en su mayoría, no se pudo llegar a enjuiciar, precisamente por la dificultad en la atribución que acarrea esta clase de acciones. De acuerdo con esto, Kshetri (2016) señala que los ataques a la firma JPMorgan Chase estaban vinculados a sanciones que EE.UU. había efectuado sobre Rusia y que, en venganza, esta había coordinado los ataques. Incluso se pudieron recuperar testimonios por parte de los hackers arrestados, quienes habrían operado desde Rusia y, por lo menos, tuvieron contacto con oficiales del gobierno de dicho país (Goldstein et al., 2014). Sin embargo, las investigaciones efectuadas por parte de la justicia estadounidense no pudieron corroborar estas hipótesis y la mayor parte de los involucrados nunca encararon la justicia.

2.4. Nociones de la ciberseguridad en la defensa nacional

Frente a un escenario en el cual se pueden realizar ataques sin que la amenaza del castigo constituya un incentivo para dejar de efectuarlos, la idea de conformar estrategias de defensa nacional que encaren los ciberataques podría percibirse como fútil o, por lo menos, ineficiente ante esta amenaza. Sin embargo, tal y como se vio en los apartados anteriores, la noción de dominio bélico en el ciberespacio, por lo mismo que no es necesariamente determinada por factores sociales o económicos, puede ofrecer una oportunidad para idear estrategias de defensa en ciberseguridad que pueden

ser aprovechadas por países con un bajo poderío bélico, como puede ser el caso del Perú. Esta falta de determinación del dominio en el ciberespacio, a su vez, podría funcionar como un incentivo en la prevención de ataques a la seguridad nacional pues, a pesar de que existen serias dificultades de atribución en la identificación de los culpables de un ataque informático, se puede motivar la amenaza que puede ejercer una nación si es que llega a ser atacada. Las dificultades en la atribución no se aplican a los territorios en los cuales estos ataques son efectuados, sino a las personas responsables de ellos. El ejemplo de la penetración a los Laboratorios Rome puede ilustrar este tipo de amenaza pues, dentro de los objetivos de los hackers involucrados, se contempló el uso de la propia base militar para efectuar ataques a otros países, entre ellos Corea del Norte. Como se vio anteriormente, el poderío bélico de este país en materia de ciberseguridad fue lo suficientemente amenazante como para motivar la prisa en las investigaciones estadounidenses y prevenir una posible respuesta por parte de Corea del Norte en represalia por un posible ataque. De este modo, se justifica la necesidad por efectuar estrategias de defensa en el ciberespacio que obedezcan tanto a los intereses nacionales por proteger la seguridad nacional como a las motivaciones que una nación pueda tener respecto del establecimiento de un tipo de poderío bélico que no implica la movilización de recursos en gran escala, como lo puede implicar la posesión de armas, tanques, aviones o buques de guerra, sino las capacidades informáticas de una nación que puedan ser capaces de penetrar y neutralizar este tipo de armas.

Juan Ormachea, Rolando Espinoza,
Sabino Ernesto, Nino Delgado, Jorge Alberto Montaño

3

CAPÍTULO

SEGURIDAD NACIONAL

CIBERSEGURIDAD
Y AMENAZAS

Como se pudo apreciar, las ciberamenazas pueden tomar muchas formas y se pueden ver beneficiadas por las propias características del entorno informático. Por ello, frente a este escenario, resulta pertinente el tomar acciones a nivel nacionales para, si bien no erradicar esta amenaza, por lo menor paliar sus consecuencias. Para poder efectuar esto, primero se debe contemplar si, efectivamente, los ciberataques pueden constituir, en vista de las palpables consecuencias que reportan, actos de guerra frente a los cuales el territorio debe defenderse. Esta pregunta resulta pertinente en vista de que, por medio de un ciberataque, es posible neutralizar la capacidad defensiva de un ejército, con lo cual se vuelve necesario si, por medio de la obtención de información externa, se pueden tomar acciones preventivas ante la amenaza de un ataque inminente. De ahí que la pregunta por si esta clase de ataques, al considerarse como actos de guerra, pueden motivar la discusión respecto de si el ciberespacio se puede considerar como un entorno militar, frente a lo cual también resulta pertinente la discusión por la conformación de una nueva rama militar, con la misma categoría del ejército, la marina o la fuerza aérea, que se encargue de operar en este entorno. Este tipo de preguntas no resultan vanas pues, de su reflexión, pueden surgir nuevas y variadas formas de ciberdefensa que puedan fortalecer las estrategias de ciberseguridad nacional, así como la conformación de un marco guía para las estrategias nacionales en torno a los conflictos que surgen de este nuevo espacio.

3.1. Los ciberataques como actos de guerra y las respuestas geopolíticas

Una de las primeras consideraciones que se deben tener en cuenta en la formulación de estrategias de defensa nacional y de respuesta frente a los ciberataques tiene que ver con la determinación de si esta clase de ataques constituyen actos de guerra o no. Esta determinación puede ser especialmente complicada en vista de que, con respecto a los actos de guerra, estos están sujetos a la interpretación de la nación afectada por ello, de forma tal que, según Springer (2015), "no todo ataque es tratado como un acto de guerra, pero la decisión de realizar un ataque esencialmente cede dicha decisión a la víctima" (p. 51). Por otro lado, también se debe tener en cuenta el empleo del término "acto de guerra" en consideración de su acepción tradicional, pues los ciberataques contemplan características que no necesariamente se incluyen dentro de lo que no normalmente se entiende como un acto de guerra. Por lo general, un acto de guerra contempla ataques armados por parte de una nación sobre la propiedad o la población de otro Estado. Además, estos ataques normalmente se efectuaban en forma directa, de forma tal que la nación afectada lo podía reconocer como tal. Dichos ataques tenían como objetivo la conquista del territorio o, en forma más modesta, el empleo de recursos de la nación afectada. En la actualidad, la Carta de las Naciones Unidas de 1945, en el ítem 4 de su artículo 2, expresamente prohíbe "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" (Naciones Unidas, 1945, p. 4). Sin embargo, la misma carta también contempla el empleo de estas acciones solo en los casos en que formen parte de la defensa del territorio. Esta prohibición expresa que es compartida por los Estados miembros de las Naciones Unidas motiva, a su vez, el empleo

de acciones menos convencionales y que se mantengan dentro de la ambigüedad con respecto a su clasificación como actos de guerra. Es por este motivo que Springer (2015) señala que "la ciberguerra del futuro seguramente tendrá características propias de las pequeñas guerras de conflictos irregulares que los enfrentamientos mayores de conflicto abierto" (p. 52). Por este motivo, los ciberataques, al encontrarse en la ambigüedad de ser clasificados como actos de guerra, no poseen las mismas características de los conflictos abiertos tradicionales. En principio, un atacante debe portar armas, usar un uniforme fácilmente identificable, pertenecer a una organización estructurada jerárquicamente en la cual los líderes sean responsables de las acciones de sus subordinados y obedecer a las Leyes del Conflicto Armado (LOAC). Como se podrá apreciar en vista de los ejemplos anteriores, estas características dificultan el hecho de que los ciberataques puedan ser clasificados como acciones bélicas que parten de un conflicto armado y que puedan constituir actos de guerra. En principio, no se están empleando armas, sino computadoras que cualquier civil puede manejar; los atacantes no necesariamente pertenecen a un ejército, a pesar de que podrían estar ligados, de alguna forma, con uno, ni tampoco pertenecen a una organización jerárquicamente estructurada. Por estos motivos, también resulta difícil que sus acciones puedan corresponderse con las Leyes del Conflicto Armado. Estas dificultades en la clasificación de estos ataques también se relacionan con el papel de la población civil con respecto a su participación en los ciberataques. Dentro de las convenciones de los conflictos armados, la población civil se encuentra protegida de los daños directos ocasionados por los actos de guerra, y a cambio de esta protección por parte de las facciones beligerantes es que se espera que la población civil no

se involucre en los ataques ni participe o motive su aplicación. Sin embargo, dado que los ciberataques son efectuados mayormente por la población civil, esto dificulta que puedan ser catalogados como actos de guerra. Una dificultad que se relaciona, a su vez, con la población civil, se corresponde con la propia naturaleza de los ciberataques, dado que, al enviar un virus o un gusano informático, este puede llegar a afectar no solo la red de una instalación militar, sino también a la población civil.

A pesar de estas dificultades, existe un cuerpo considerable de evidencia que señala los propósitos bélicos de los ciberataques, al buscar obtener activos militares por medio de la penetración de sus sistemas. Esto se debe en gran parte al hecho de que los ejércitos más avanzados del mundo se han vuelto en extremo dependientes de los sistemas informáticos, al punto de que los enemigos de un Estado no pueden dejar pasar por alto el valor de las ciberoperaciones como medio para erosionar las capacidades defensivas de un ejército. Por este motivo es que "las ciberoperaciones son, ciertamente, parte de los conflictos tanto del presente como del futuro" (Springer, 2015, p. 53). Esto se corrobora con el hecho de que un ciberataque bien estructurado puede resultar en un daño aún más devastador y útil que aquel efectuado por medio de un ataque físico contra una estructura militar dada. Recuérdese, por ejemplo, el caso del virus informático Stuxnet que dañó seriamente, y por varias décadas, la capacidad de producción nuclear de Irán y que motivó a este país a adoptar políticas de ciberdefensa que lo llevaron a ser considerado como una potencia bélica en este campo. Por este motivo, las capacidades informáticas de una nación pueden constituirse en una herramienta poderosa y ciertamente forman parte de los conflictos del presente siglo, al

punto de que “las naciones simplemente no pueden considerar el involucrarse en conflictos sin implementar medidas para asegurar sus propias redes informáticas” (Springer, 2015, p. 55), más aún considerando que el efecto de los ciberataques puede ser equiparable o incluso peor que aquel efectuado por medio de ataques convencionales. Por todo esto, se debe considerar que la ciberguerra forma parte de las nociones modernas de conflicto.

Tomando esto en consideración, también se deben contemplar las posibles respuestas geopolíticas que se pueden efectuar en un escenario de conflicto en el ciberespacio. Si bien dentro de las redes no se toman en cuenta las fronteras nacionales de los países en conflicto, sí se debe tener en cuenta que los participantes en esta clase de conflictos informáticos forman parte de estas divisiones, por lo cual las consideraciones legales y geopolíticas respecto de la legislación de cada país son un elemento a tomar en cuenta al momento de emprender acciones de respuesta frente a los ciberataques. De acuerdo con Guiora (2017), las consideraciones geopolíticas con respecto a estos ataques tienen que ver con el nivel de proporcionalidad que se debe contemplar como parte de la respuesta a un ciberataque. Al respecto, se tiene que, en principio, la geopolítica es definida como “las relaciones entre las naciones-estados y su compromiso con la amplia comunidad global, con particular énfasis en las relaciones entre geografía y políticas nacionales” (p. 37). Dentro de este escenario, las posibles respuestas frente a las amenazas de los ciberataques pueden tener un enorme impacto sobre la estabilidad tanto regional como global. Por este motivo, resulta en extremo pertinente el identificar cómo es que una nación puede responder, ya sea en forma unilateral, bilateral o multilateral. Como parte de la clasificación de este

tipo de respuestas, una tipología que puede resultar útil tiene que ver con la consideración de si las respuestas a estos ataques se efectúan en forma táctica o en forma estratégica. Si las respuestas se efectúan en forma táctica, se considera que, como parte de su estructuración, se ha privilegiado un tipo de toma de decisiones en la cual se ha colocado un especial énfasis en la inmediatez de la respuesta. Por otro lado, con respecto a las respuestas estratégicas, se considera que se ha tomado en cuenta un tipo de respuesta que considera las consecuencias a largo plazo, en la cual los resultados inmediatos y el impacto de la respuesta no han sido aspectos privilegiados. De este modo, considerando las implicancias geopolíticas de las respuestas a los ciberataques, además del hecho de que la comunidad internacional tiende a juzgar en forma negativa las respuestas militares frente a los ataques, muchas naciones tienden a tomar en cuenta un tipo de respuesta estratégica que busque paliar las consecuencias al largo plazo y que no suponga el empleo de armamento militar.

3.2. El ciberespacio como entorno militar y la aplicación de leyes internacionales

Otro aspecto que se debe tomar en cuenta con respecto al tipo de respuesta que se puede emprender frente a los ataques en el ciberespacio tiene que ver con la consideración respecto de si el ciberespacio constituye un entorno militar, como lo pueden ser las acciones sobre la tierra, el mar o el aire, pues este tipo de consideraciones pueden afectar la aplicación de leyes internacionales con respecto al tipo de respuesta que se puede emprender frente a estos ataques. Este tipo de consideraciones se relacionan con el hecho de que muchas de las operaciones militares se definen, en gran parte, en términos del espacio

en el cual se realizan. Sin embargo, en los últimos años, con el desarrollo de las nuevas tecnologías, surgen interrogantes con respecto a la emergencia de nuevos espacios de conflicto y, con ello, con respecto a la aplicación de las leyes internacionales respecto de este tipo de entornos. De este modo, algunas de estas discusiones tienen que ver con el considerar a las fuerzas militares que pueden emplear armas nucleares como un dominio completamente separado, como lo pueden ser la tierra, el mar o el aire. Este tipo de consideraciones llevan a Springer a considerar que "En el siglo XXI, dos entornos de potencial conflicto, el espacio y el ciberespacio, son fuentes de controversia respecto de la separación de las fuerzas militares como dominios [separados]" (2015, p. 56). Por otro lado, la consideración por el ciberespacio como un entorno militar similar a la tierra o el aire emerge del hecho de que la especialización dentro de uno de estos dominios es el único medio en el cual un líder militar puede efectuar tácticas efectivas en un entorno bélico. Por este motivo, el ciberespacio es considerado como un entorno en el cual el grado de desarrollo tecnológico alcanzado ha motivado su discusión como un entorno militar similar a la tierra o el mar. Sin embargo, a diferencia de estos entornos, los cuales son limitados en vista de sus características físicas, el ciberespacio no solo no posee estas limitaciones, sino que además constituye un entorno enteramente creado por el hombre. Por estos dos motivos es que "los principios bajo los cuales el dominio [del ciberespacio] opera pueden ser, teóricamente, cambiados por medio de variaciones en la arquitectura física o el sistema operativo del software en el ciberespacio" (Springer, 2015, p. 59-60). Por este motivo, en tanto que en el ciberespacio no se efectúan las mismas limitaciones que en los entornos físicos, es que este espacio puede interactuar e influenciar en todos los demás dominios, como el aire o el mar, y puede jugar un papel crucial en el éxito de las operaciones militares. De este modo, las

comunicaciones en el ciberespacio pueden influenciar en los satélites en órbita y determinar el control de activos terrestres y navales en el campo de guerra, así como también pueden influenciar el comportamiento de los activos aéreos, ya sea que estos sean operados por humanos o mediante la inteligencia artificial. Por todo ello, en vista de la enorme relevancia que tiene el ciberespacio para las operaciones militares es que se debe tener en cuenta la aplicación de las leyes internacionales con respecto al tipo de respuesta que se puede efectuar frente a los ciberataques.

De acuerdo con Guiora (2017), una cuestión relevante respecto de la importancia del ciberespacio en las acciones militares tiene que ver con la aplicación de leyes internacionales con respecto a los ciberataques. Esta cuestión resulta relevante en vista de que el modo en el cual una nación o estado efectúa una respuesta frente a esta clase de ataques se puede justificar de acuerdo con la interpretación del Artículo 51 de la Carta de las Naciones Unidas. Según este artículo, se tiene que

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas [...]. 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. (Naciones Unidas, 1945, p. 16)

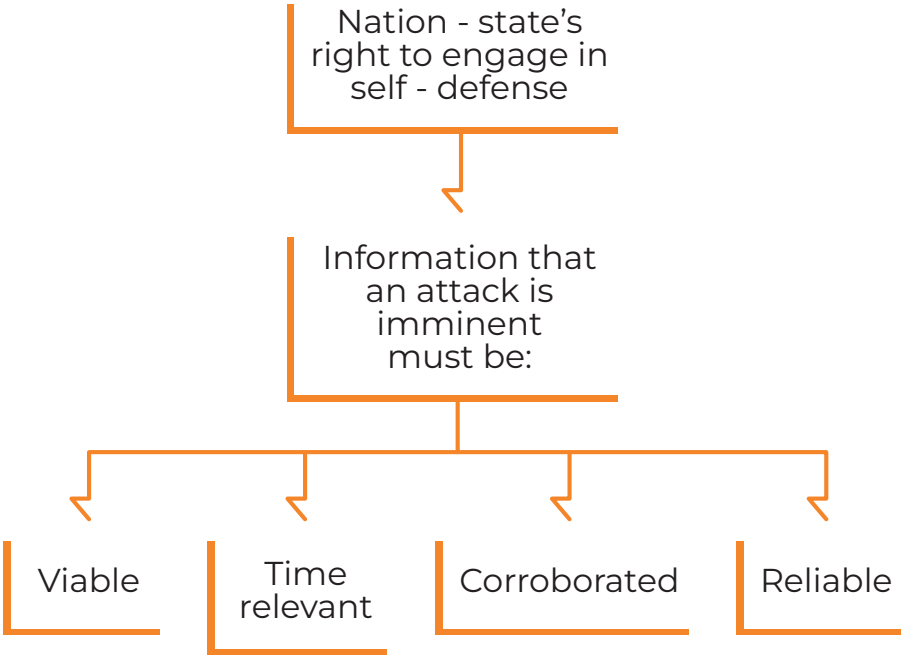
De acuerdo con lo señalado por Guiora (2017), se tiene que el lenguaje empleado en la Carta sugiere que el derecho que posee una nación para efectuar la legítima defensa se limita a responder a los ataques, lo cual refleja una disonancia intelectual y práctica. Sin embargo, al efectuar una lectura e interpretación más abierta del mismo artículo sugiere que el derecho a la autodefensa frente a los ataques resulta legítimo dentro del contexto de la defensa preventiva. De acuerdo con eso, y según lo indicado en el Artículo 51, se puede aceptar una interpretación de dicho artículo en la cual el derecho a la autodefensa frente a los ataques enemigos se puede aplicar, también, cuando se tiene conocimiento de que un agente enemigo va a efectuar un ataque próximamente. De este modo, la inminencia en el contexto de las operaciones contra el terrorismo (informático) se limita a un individuo o grupo de individuos que representan una amenaza directa hacia la seguridad nacional.

Considerando todo esto, en los contextos de los ciberataques, se pueden tomar medidas preventivas en vista de una interpretación amplia del artículo 51 señalado considerando la importancia que posee la infraestructura de las redes informáticas. Esta importancia se ve reforzada con el hecho de que los ciberataques suelen atacar la infraestructura de internet de una nación. En forma contraria a los ataques convencionales, los ciberataques suelen estar dirigidos a la infraestructura de una nación, en lugar de alguna persona en particular o algún edificio. Además de estos objetivos, las consecuencias de los ciberataques suelen ser más psicológicas que físicas, pero no por ello pueden dejar de ser letales. Por estos motivos es que, de acuerdo con lo señalado por Guiora (2017), se debe contemplar una interpretación más amplia del artículo 51 señalado en vista de las devastadoras consecuencias contempladas en los ciberataques para poder considerar las

acciones preventivas de respuesta frente al conocimiento de un ciberataque inminente. Por ello, el derecho de una nación para abordar acciones preventivas de autodefensa se justifica en el hecho de que el artículo 51 puede ser aplicado de acuerdo con los estándares aceptados y principios contemplados en el derecho internacional. De este modo, se puede garantizar la acción de atacar en forma proactiva para prevenir ciberataques inminentes. En la siguiente Figura, se puede apreciar un mapa conceptual en el cual se definen los rasgos que permiten considerar que la información respecto de un ciberataque da cuenta de su inminencia y, con ello, de la legitimidad de acciones preventivas:

Figura 1

Elementos para la legitimidad de un ataque preventivo



Nota. Guiora (2017)

De este modo, tanto en los casos de ciberataques efectuados tanto por agentes militares como por la población civil, el Estado tiene el derecho de efectuar acciones de autodefensa frente a ataques inminentes. Por ello, en los casos en los cuales es posible obtener información fidedigna que indique la inminencia de un ciberataque que busque penetrar la infraestructura computacional de una nación, y con ello causar un enorme daño, dicha nación o individuo se convertiría en un blanco legítimo dentro del contexto contemplado por el artículo 51.

3.3. Elementos para las estrategias en ciberseguridad nacional, desarrollo e implementación

Una vez que se puede determinar tanto la naturaleza bélica de los ciberataques como los motivos para efectuar acciones de contraataque preventivo frente a estas amenazas, resulta conveniente el analizar los elementos a tomar en cuenta como parte de la formulación de una estrategia de ciberseguridad que pueda resultar, en gran parte, efectiva frente a esta clase de ataques. De este modo, un elemento a tener en cuenta es la "escuela de diseño" respecto de la elaboración de estrategias de defense. La estrategia de diseño, de acuerdo con Sarbah & Otu-Nyarko (2014), es un modelo de gestión organizativa que busca lograr un equilibrio entre los elementos externos a una organización (como las amenazas y oportunidades del ambiente externo, así como los factores clave de éxito) y los elementos internos de la institución (como las fortalezas y debilidades o las competencias distintivas). De este modo, se tiene que

> la escuela de diseño propone un modelo de gestión estratégica que busca obtener un encuentro entre las capacidades internas y las posibilidades externas. El modelo coloca especial atención a las estimaciones de las

> situaciones tanto internas como externas, en tanto que las primeras cubren amenazas y oportunidades en el ambiente y las segundas revelan fortalezas y debilidades dentro de una organización (también conocido como análisis SWOT). [Sarbah & Otu-Nyarko, 2014, p. 234]

Este tipo de estrategia, como se puede apreciar, tiene más que ver con los ámbitos corporativos que con los militares. Sin embargo, de acuerdo con Kshetri (2016), se reconoce que los conceptos básicos y la estructura de la escuela de diseño se pueden aplicar a otro tipo de instituciones, como lo pueden ser las agencias gubernamentales, las universidades o las organizaciones sin fines de lucro. Por ello, se tiene que esta escuela puede proporcionar una estructura básica para la implementación de estrategias de defensa en tanto que busca equilibrar las capacidades internas de una organización con los elementos externos que interactúan con ella, como lo pueden ser los ciberataques. De este modo, las estrategias de defensa que se pueden formular mediante este tipo de diseño buscan determinar objetivos al largo plazo, metas a conseguir y la incorporación de políticas, acciones y movilización de recursos vitales para el éxito de las metas.

De este modo, uno de los elementos que forma parte de una estrategia de defensa mediante la escuela de diseño es la identificación de las fortalezas de la organización. En el ámbito de la ciberseguridad, el desarrollo de fortalezas se puede relacionar con el posicionamiento de un país por conformarse como una potencia bélica en materia de seguridad en el ciberespacio. De acuerdo con esto, se puede tomar el ejemplo del Israel, el cual ha logrado posicionarse como uno de los países con mayor cantidad de compañías en ciberseguridad en el mundo. De acuerdo con Press (2017), Israel ha logrado conformar una enorme industria en ciberseguridad que moviliza unos 82 billones de dólares y es capaz de brindar sus servicios no solo a distintas superpotencias, sino

que también puede asistir en el desarrollo de las capacidades de ciberdefensa de países pequeños, como en el caso de Singapur, al crear más de 300 startup en ciberseguridad y exportar más de 6.5. billones de dólares en productos de ciberseguridad. Sin embargo, de acuerdo con Press (2017), el éxito del país en este rubro se debe a 6 factores clave, entre los cuales se encuentra el rol del estado como coordinador y como promotor de empresas, la conformación del ejército como un incubador y acelerador de startups, la inversión del país en capital humano, la adopción de una perspectiva interdisciplinaria y diversificada, y la redefinición de cibercaja (es decir, el pensar más allá de las convenciones en ciberseguridad). Todos estos elementos han podido posicionar al país como una potencia en este rubro, con lo cual incrementan sus fortalezas frente a posibles amenazas.

Sin embargo, el modelo de la escuela de diseño no solo contempla las fortalezas organizativas, sino también la identificación de debilidades para poder superarlas. De acuerdo con Kshetri (2016), se tiene que gran parte de la población mundial no está consciente del peligro que suponen los ciberataques para su estilo de vida y para la permanencia de la estructura social. De acuerdo a una encuesta respecto del nivel de importancia que se les daba a los temas en ciberseguridad (Ponemon Institute, 2014), se obtuvo que el 57 % de los participantes no pensaba que su organización estuviera protegida contra ciberataques, mientras que el 48 % de los participantes respondió que sus jefes inmediatos tenían solo un conocimiento básico en materia de ciberseguridad. Por otro lado, también se pueden considerar como elementos propios de las debilidades respecto a la ciberseguridad el hecho de que el rubro es relativamente reciente o de que supone una enorme dependencia de las tecnologías digitales. Estas dificultades de pueden ver agravadas por el

hecho de que, en muchos casos, los empleados de las diferentes compañías no están capacitados para actuar en escenarios de amenaza por ciberataques. De acuerdo con Kshetri, se tiene que "en muchos casos, los empleados son fácilmente manipulados por cibercriminales debido a factores como su deseo y presión por ser serviciales y atentos, el bajo salario que perciben o una falta de entrenamiento" (p. 12).

Sin embargo, el desarrollo de estrategias en materia de ciberseguridad también puede representar una ventaja para establecer su poderío con respecto a otras naciones, como de hecho fue el caso de Israel y los casos ya mencionados de los programas de ciberseguridad de Corea del Norte e Irán. Junto a estos casos, también se pueden recoger las declaraciones que hicieran dos oficiales chinos, Qiao Liang y Wang Xiangsui, en el libro titulado *Guerra Irrestricta* (1999). En él, los oficiales argumentaban que, en vista de que a fines de la década de los años 90 el ejército chino no contaba con los mismos recursos bélicos que naciones más desarrolladas como los EE.UU. sí poseían, debían enfocarse en el desarrollo de nuevas tecnologías para la información y la ciberguerra, de forma tal que el ejercito chino pueda ser capaz de neutralizar tanto a sus enemigos como la información política, económica y militar dentro de sus estructuras sociales.

Además de los elementos ya señalados, como el desarrollo de fortalezas, la identificación de debilidades o la posibilidad de oportunidades dentro del desarrollo de capacidades para la ciberseguridad, Guiora (2017) identifica, a su vez, 3 elementos clave para el desarrollo de estrategias de defensa frente a este tipo de amenazas, que son la priorización de recursos, los análisis de costo-beneficio y la evaluación de riesgos. Con estos tres

elementos es que se puede empezar a idear una estrategia en ciberseguridad nacional que involucre los aportes de oficiales en seguridad naciones, ejecutivos de negocios, líderes académicos, oficiales de la ley y políticos en la implementación de una política para la ciberseguridad, en tanto que resulta necesario que dicha política se encuentre amparada bajo los límites que establece la ley. De este modo, la creación de una política para la ciberseguridad requiere la identificación de los activos que deben recibir protección y de las características que deberá poseer dicha política. En primer lugar, se debe considerar que el rango de efectividad que tendrá esta política nunca será al 100 % efectiva. Esta falta de efectividad tiene que ver con la naturaleza de los ciberataques ya mencionada, en tanto los crímenes nunca son 100 % prevenibles, los ataques poseen componentes tanto al corto como al largo plazo y además se deben conducir por medio de un balance entre los intereses compartidos, los costos invertidos y las libertades civiles en juego. Con respecto al primer punto, se tiene que la propia naturaleza del accionar terrorista, en este caso expresado mediante ciberataques, previene de la formulación de medidas 100 % efectivas. Esto, como ya se mencionó, tiene que ver con el hecho no solo de que existen dificultades para atribuir responsabilidades, sino que además se debe tomar en cuenta que el propio accionar terrorista no contempla metas al corto o mediano plazo, sino que posee una enorme resiliencia para idear estrategias contempladas a efectuarse al largo plazo. Por este motivo, de acuerdo con Guiora (2017), se tiene que

> si una estrategia contraterrorista solo apunta a amenazas al corto plazo, posiblemente no prestará atención a otras amenazas reales al largo plazo [...] las organizaciones terroristas definen su efectividad a través del prisma de las consideraciones estratégicas al largo plazo. (p. 75)

Esta enorme resiliencia por parte de las organizaciones criminales que se involucran en actividades de ciberataque debe ser tomada en cuenta en vista de que, a su vez, motiva todo un discurso e ideología por parte de estas organizaciones según el cual sus adeptos están dispuestos a efectuar un ciclo sin fin de violencia que les sirve a estas organizaciones para reclutar miembros para su causa. De este modo, uno de los medios principales para formular estrategias de defensa tiene que ver con la identificación de la amenaza más inmediata el contexto que se busca defender. Dado que la identificación de las amenazas puede motivar una clasificación más sencilla de las mismas, estas se pueden colocar dentro de un continuo que busca comprender en qué forma es que una amenaza significativa puede estar compuesta por varias pequeñas amenazas que pueden ser gestionadas en forma más sencilla. De este modo, de acuerdo con Guiora (2017), se pueden clasificar las amenazas dentro de un continuo en razón de si son amenazas inminentes, previsibles, de largo alcance o inciertas. Con respecto a las amenazas inminentes, se tiene que son aquellas para las cuales se debe considerar un plan de acción inmediato (como alguna llamada que indique la presencia de una bomba en algún lugar público, por ejemplo). Mientras que, con respecto a las amenazas previsibles, se tiene que son aquellas que se pueden efectuar en un futuro cercano, pero no inmediato. Un ejemplo de ello podría ser el conocimiento, con semanas de anticipación, de que algún grupo subversivo planea un ataque en determinado lugar. De otro lado, se tiene que las amenazas de largo alcance son aquellas que se podrían llevar a cabo en un tiempo indeterminado. Por ejemplo, se pueden tener reportes de que un grupo subversivo se encuentra realizando entrenamiento sin saber en qué consiste la actividad para la

cual se están preparando. Y, por último, las amenazas inciertas tienen que ver con aquellas que invocan sensaciones generales de miedo en la población, como lo pueden ser las amenazas de ataques terroristas en general, sin que exista una amenaza previa que motive el temor hacia estas.

3.4. Marco general para las políticas estratégicas nacionales sobre los ciberconflictos

De acuerdo con lo señalado por Kshetri (2016), existen 4 dimensiones que se deben tener en cuenta para la formulación de políticas nacionales que le hagan frente a las ciberamenazas. Como se vio anteriormente, algunos elementos que formaban parte de estas políticas tenían que ver tanto con la identificación de fortalezas, debilidades y oportunidades, así como también con el reconocimiento de efectividad de estas políticas y la resiliencia de los grupos subversivos. En este caso, se busca identificar los rasgos estratégicos para la formulación de políticas, los cuales tiene que ver con la capacidad local para el fortalecimiento del ejercicio de la ley y el desarrollo institucional, la creación de redes informales y acuerdos, la creación de oportunidades para el desarrollo de la voz y participación de las economías y el establecimiento de grupos de alto nivel conformado por especialistas en el desarrollo de políticas. Estos cuatro elementos, de acuerdo con Kshetri (2016), son los que podrían garantizar la formulación de políticas contra los ciberataques en la forma más efectiva y eficaz posible.

Con respecto al primer punto, la capacidad local para el fortalecimiento del ejercicio de la ley y el desarrollo institucional, se tiene que una estrategia muy efectiva respecto de la defensa contra los ciberataques tiene que ver con el fortalecimiento de las instituciones locales para enfrentar este tipo de amenazas, como la policía o las instituciones de justicia. Como ejemplo

de ello, se tiene el caso de los ciberataques efectuados en Rumania. De acuerdo con Odobescu (2014), en 2013 se efectuó una iniciativa por parte del FBI estadounidense para capacitar a unos 600 oficiales rumanos en la lucha contra el cibercrimen. Por otro lado, la creación de redes informales como estrategia contra el cibercrimen ha probado tener tanto beneficios como obstáculos. De acuerdo a esta estrategia, lo que se busca es formular redes de asistencia y colaboración entre diferentes instituciones policiales con el objetivo de reforzar capacidades y proporcionar entrenamiento. De este modo, algunos ejemplos de esta clase de colaboración lo pueden constituir, por un lado, el hecho de que, en 2009, el FBI estadounidense anunció que establecería una base permanente en Estonia para contribuir en la lucha contra el cibercrimen en ese país. Además de esto, otra estrategia empleada contra el cibercrimen consistió en el proporcionar oportunidades para el desarrollo de la participación de economías. Según esto, lo que se busca es el establecimiento de beneficios mutuos por medio de la participación conjunta de diferentes entidades. De este modo, se tiene que

> el hacer esfuerzos para entender los problemas de las economías en desarrollo desde su punto de vista y proporcionar oportunidades que garanticen su participación puede ayudar a explorar las ventajas mutuas y a motivar la participación en marcos internacionales formales. (Kshetri, 2016, p. 66)

Por último, con respecto al establecimiento de grupos de alto nivel, lo que se busca por medio de esta estrategia es el empleo de estrategias suaves que, en lugar de obligar a otros países a colaborar en la lucha contra el cibercrimen, se les pueda influenciar para que adopten un compromiso más serio por medio del establecimiento de redes internacionales. Este escenario es ejemplificado por Freedberg (2013) cuando, en medio

de un contexto en el que EE.UU. y China poseen los medios para penetrar la ciberseguridad del otro, se busca establecer un tipo de colaboración más eficaz y que no lleve a un conflicto mucho más serio. De este modo, frente a los constantes ciberataques por parte de China en los que se obtiene sistemáticamente información, lo que se busca es persuadir al gobierno chino de que abandone ese tipo de prácticas (auspiciadas desde el sector militar) en la búsqueda de soluciones más diplomáticas.

Con los elementos analizados previamente, es posible entrar en el análisis de las políticas en ciberseguridad adoptadas por distintos países para identificar los elementos más adecuados y que permitan formular un plan para el fortalecimiento de la ciberseguridad en el país.

4

CAPÍTULO

ESTRATEGIAS INTEGRADAS DE CIBERSEGURIDAD NECESARIAS PARA FORTALECER LA SEGURIDAD NACIONAL DEL PERÚ

ESTRATEGIAS INTEGRADAS DE CIBERSEGURIDAD NECESARIAS PARA FORTALECER LA SEGURIDAD NACIONAL DEL PERÚ

Actualmente es necesario e importante proteger el valor de la información estratégica y crítica del país, así como la información que publican los peruanos en Internet. Si bien Internet ofrece un potencial enorme, también conlleva riesgos potenciales debido a la permeabilidad de la información crítica, privada y confidencial.

Cada sector del gobierno sería responsable del uso de la red. En particular, de la importancia de la prevención del cibercrimen y las posibles amenazas a la seguridad nacional y su impacto en la industria del ciberacoso. En Perú, el acceso de los jóvenes a las tecnologías de la información y la comunicación está relacionado con el nivel educativo del jefe de hogar, por lo que los porcentajes se dividen de la siguiente manera: 99,7% si el jefe de hogar es profesional universitario, 99,2% si el jefe de hogar es del hogar es del hogar. el hogar tiene educación superior no universitaria, el 96.6% de los hogares tiene educación secundaria y el 83.5% de los hogares tiene educación primaria o menos (INEI, 2018). La seguridad de este sector vulnerable y de la población en general está ligada a la existencia de una unidad u organismo responsable de la regulación y planificación integral y multidisciplinaria de estas actividades.

Hasta el 2019, cada sector regulaba las actividades destinadas a proteger las redes y los datos almacenados en sus centros de datos con directivas tanto limitadas como específicas del sector. La publicación de la Ley 30999 el 26 de agosto de 2019 es un cambio de juego para las estrategias integradas

de ciberseguridad. sin embargo, los elementos culturales y la aplicabilidad del estándar son desafíos que requieren atención.

El estudio se centró en el estudio de las estrategias integradas de ciberseguridad del Perú, cuya utilidad es analizar los diversos factores que impiden el disfrute del uso de la tecnología con la plena protección de los derechos de seguridad de la información, lo que ayuda tanto a identificar los elementos, permite incidir en la seguridad cibernética y crear las estrategias necesarias para fortalecer la seguridad nacional y la soberanía nacional, así como fortalecer a los ciudadanos del Perú durante el 2019.

Se demostró la factibilidad del estudio con información suficiente basada en los tres casos de referencia internacional y datos nacionales peruanos que permitieron el desarrollo de este estudio.

Objetivo general

Formular estrategias completas de ciberseguridad indispensables para reforzar la seguridad en el territorio peruano.

- Objetivos específicos

- Evaluar las estrategias completas de ciberseguridad mejor implementadas en tres países seleccionados al 2019.

- Analizar la normativa legal concerniente a la ciberseguridad en el Perú.

- Reconocer las limitantes con respecto al progreso de la ciberseguridad peruana.

- Asentar las diferencias en materia de desarrollo, valoración y renovación de los conocimientos que se tienen en cuanto a ciberseguridad peruana.

- Abordar las diferencias en cuanto a desarrollo, valoración y renovación de los conocimientos que se tienen en cuanto a ciberseguridad peruana.

Enfoque de investigación

El enfoque epistemológico fue cualitativo porque involucra prácticas interpretativas que permiten visibilizar la realidad para ser comprendida y/o influir en el destinatario.

Tipo de investigación

El estudio se basó en un diseño no experimental descriptivo, analítico e intencional. Este tipo de investigación busca la existencia de una singularidad en una población general. De esta forma, dicha investigación tuvo como objetivo crear estrategias de ciberseguridad para fortalecer la seguridad peruana.

Método de investigación

En esta parte de la investigación se usó un método que consiste en el desarrollo del estudio que tiene su base en la hermenéutica, cuyas etapas son las que se mencionan a continuación:

- Etapa exploratoria: primera etapa de la investigación donde se visualizaron las Estrategias Nacionales de Seguridad Cibernética de los Países Bajos, EE.UU., España y Perú.

- Etapa descriptiva: se eventualizó en dos fases:
  - Análisis situacional actual de España, Estados Unidos, Países Bajos y Perú relacionado a las políticas y estrategias de seguridad cibernética.
  - Compilación de las diversas experiencias en el tema de seguridad cibernética.
- Etapa estructural: abarcó la investigación, análisis e interpretación del contenido de documentos nacionales e internacionales y fuentes de datos utilizados en la investigación.

Técnicas de acopio de información

Un observador cualitativo debe posicionarse y mantener una actitud activa en las situaciones sociales, por lo que esta observación va más allá de la mera reflexión sobre el fenómeno.

Instrumentos de acopio de información

- Ficha de registro: Es una herramienta para estructurar los datos a analizar posteriormente, y permite la triangulación teórica, el contraste categórico y la búsqueda de vacíos que no son evidentes a simple vista.
- Forma Analítica: Contiene un número determinado de técnicas de investigación para examinar el contenido de las leyes, doctrinas, tratados, estructuras organizacionales e informes de gestión de seguridad cibernética en Países Bajos, Estados Unidos, España y Perú.

Método de análisis de información

- Análisis documental: se ejecutaron los métodos de la hermenéutica:
  - Registro documental: Leyes de Seguridad Cibernética, Doctrinas, Tratados, Estructuras Organizativas e Informes de Gestión en Países Bajos, USA, España y Perú.
  - Resumir los datos observados en el estudio.
  - Clasificar los documentos por categorías.
- Elaboración de la descripción protocolar: esto incluye la formación de unidades de significado, es decir. investigar el contenido, identificar documentos que contengan sesgos del investigador y/o autores seleccionados, verificar la observación contextual del fenómeno, identificar documentos que contengan sesgos del investigador y/o autores seleccionados, crear una descripción. y la descripción del documento en la sección de notas del formulario de solicitud.
- Lectura total de los documentos detallados: Incluye un estudio en profundidad de las leyes, doctrinas, tratados, estructuras organizacionales e informes de gestión de ciberseguridad en Países Bajos, Estados Unidos, España y Perú.
- Delineación de unidades de significado en torno a una unidad temática: su manifestación específica se categoriza según subcategorías e indicadores establecidos.

- Expresión del tema en cuestión en lenguaje científico: incluye la fase de discusión y comparación entre las realidades de los países en estudio.

Análisis y síntesis de los resultados

Estrategias de seguridad cibernética comparadas con Estados Unidos.

Los pilares sobre los que Estados Unidos basa su Estrategia de ciberseguridad son cuatro:

- **Protección:** Proteja las redes y los datos federales, asegure la infraestructura crítica, luche contra el delito cibernético y mejore la notificación de incidentes.

- **Promoción**: Apoyar una economía digital vibrante y sostenible, fomentar y proteger el ingenio estadounidense y desarrollar una fuerza laboral de seguridad cibernética de alta calidad.

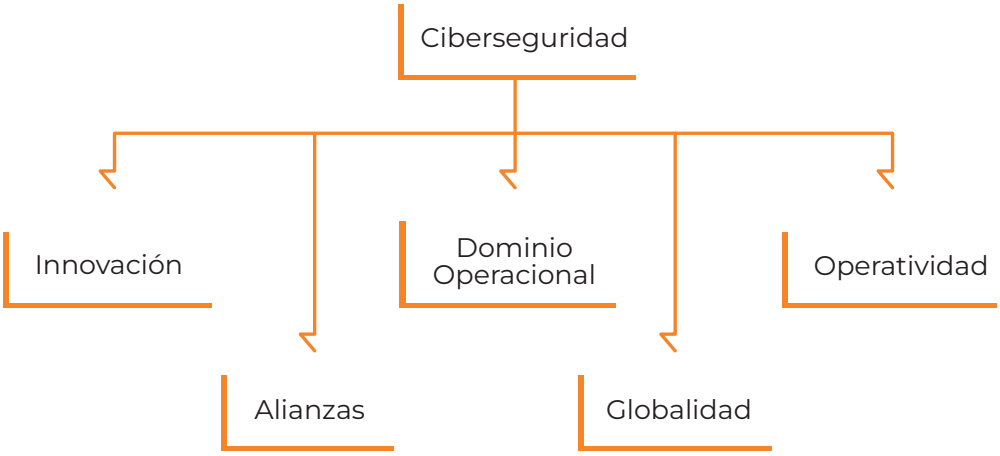
- **Interrupción:** identificar, combatir, interrumpir, socavar y prevenir conductas desestabilizadoras en el ciberespacio que sean contrarias a los intereses nacionales. Mejorar la estabilidad cibernética estableciendo estándares para el comportamiento responsable del gobierno, identificando y enjuiciando el comportamiento inaceptable en el ciberespacio e imponiendo costos a los actores cibernéticos maliciosos.

- **Preservación:** Asegurar la apertura, interoperabilidad, seguridad y confiabilidad a largo plazo de Internet, mientras se apoya el crecimiento de los mercados de infraestructura y nuevas tecnologías y el desarrollo de habilidades cibernéticas a nivel internacional.

Para dar cumplimiento al primer principio de defensa, se elaboró una estrategia nacional de ciberseguridad basada en los cinco ejes que se muestran en la Figura 2.

Figura 2.

Estrategia Nacional de Seguridad Ciudadana de EE.UU.



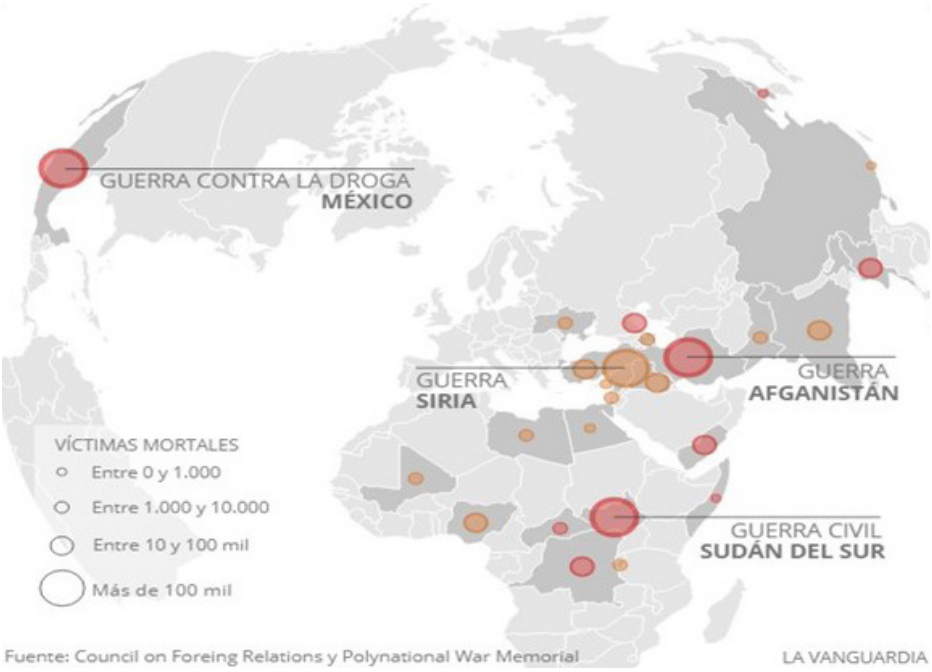
Para garantizar la seguridad cibernética, el Departamento de Defensa de EE. UU. ha desarrollado cinco puntos clave que conducen al desarrollo de cinco estrategias:

1. Dominio de las operaciones: el ciberespacio es el dominio de las operaciones que el Departamento de Defensa utiliza para la planificación, la capacitación y la educación, así como también para proponer tareas encaminadas a aprovechar al máximo el potencial de la red. La irrupción de nuevos dominios: los espectros cibernético, espacial y electromagnético

incrementaron los dominios tradicionales que gobernaron hasta el siglo XX, como los dominios marino, aéreo y terrestre. Desde 1990, la llamada revolución de los asuntos militares RMA ha cambiado la perspectiva de las instituciones militares, provocando cambios como consecuencia del quiebre de las tecnologías de la información y la comunicación (Brose, 2019). El RMA forma un sistema de subsistemas estructurados que permiten la observación de objetivos, la comunicación de comando a comando y la toma de decisiones e instrumentación para el usuario con una herramienta que tiene en cuenta una perspectiva más amplia del campo de batalla, especialmente en el escenario de conflicto activo de hoy (ver figura 3). La disrupción causada por las tecnologías de la información y la comunicación abarca muchos dominios y arenas de confrontación militar y, por lo tanto, se extiende a dominios diversos e interrelacionados: inteligencia, comunicaciones, comando, armamento y otras áreas emergentes en la dinámica actual.

Figura 3.

Disputas activas al año 2019



Nota. Aragó (2019)

Hoy en día se mantiene la concomitancia de varios parámetros en el dominio operacional:

- Riña para obtener información
- Novedosa matriz de conceptos
- Asimilación institucional
- Ataques de precisión
- Empleo de armamento no letal
- Reducción de tiempos en el etapa decisorio
- Hegemonía de los sistemas de Reconaissance, Surveillance and Target Adquisition (RSTA)
- Incongruencias de tiempo en los campos de batalla
- Presentación de tecnologías no armamentista en el ciclo de batalla (Dos Reis y de Brito, 2018).

2. Operatividad: Los conceptos operativos de seguridad y defensa se redujeron, dando lugar a nombres como Network Centric Warfare (NCW) en los Estados Unidos y Network Enabled Capability en Europa. El término Netwar se utiliza en todo el mundo. El concepto de operación de Netwar se refiere a la optimización de procesos en sincronización, diagnóstico, predicción de letalidad y capacidad de supervivencia de la fuerza en operaciones terrestres, aéreas, marítimas, submarinas, espaciales y virtuales. En 2001, como tema de la Revisión Cuatrienal de Defensa (QDR), el concepto de transformación

reorganizó el antiguo concepto de operaciones, dando a las operaciones militares una nueva dimensión en la teleología que refuerza y trasciende la superioridad militar estadounidense. E

En una dinámica global caracterizada por la decadencia de las nuevas tecnologías y el fuerte acortamiento de los tiempos de obsolescencia (US Department of Defense, 2019). Desde 2018, la QDR ha sido reemplazada por la Estrategia de Defensa Nacional (Garamone, 2018). En las últimas dos décadas, la guerra se ha consolidado como un término que se refiere a la renovación de la guerra y el uso de las capacidades militares por parte de las potencias. En la misma línea, el cambio representa una revolución fundamental en los enfoques estratégicos, reemplazando los principios ad hoc asociados con las operaciones de contrainsurgencia para crear una "Estrategia de Tercera Compensación (TOS)". La tercera estrategia de TOS se proyecta como una estrategia basada en la competitividad a largo plazo de las grandes potencias del mundo. TOS tiene como objetivo consolidar y superar el poderío militar estadounidense, adaptar los sistemas de defensa a la dinámica tecnológica y crear una red interactiva en la que se integren a lo largo del tiempo sistemas de inteligencia, mando, control, procesamiento de datos, reconocimiento y vigilancia. Estos objetivos se implementaron en el llamado proyecto Marven, o War Algorithm, que se basa en la aplicación de la inteligencia artificial en la dinámica de los sistemas de defensa y ataque. El algoritmo contribuye a la toma de decisiones en base a escenarios posibles, pero los elementos éticos y morales que influyen en la toma de decisiones exigen que el algoritmo militar siga siendo una herramienta constructora de escenarios, pero no decisiva. En este orden, entre los nuevos conceptos operativos que se establecieron en el diálogo militar:

- Guerra informática: se da por la riña en el dominio del ciberespacio y los flujos informáticos que rondan la red, posicionando tema y agendas (Ropers, 2008).

- Dominio de la información: posee dos dimensiones aludiendo a la dirección de la información y al pronunciamiento de un nombre en la web (Ropers, 2008).

- Campo de batalla vacío: el conflicto ocurre sin la presencia de actores cuando los ejércitos no ocupan el espacio del conflicto (Ropers, 2008).

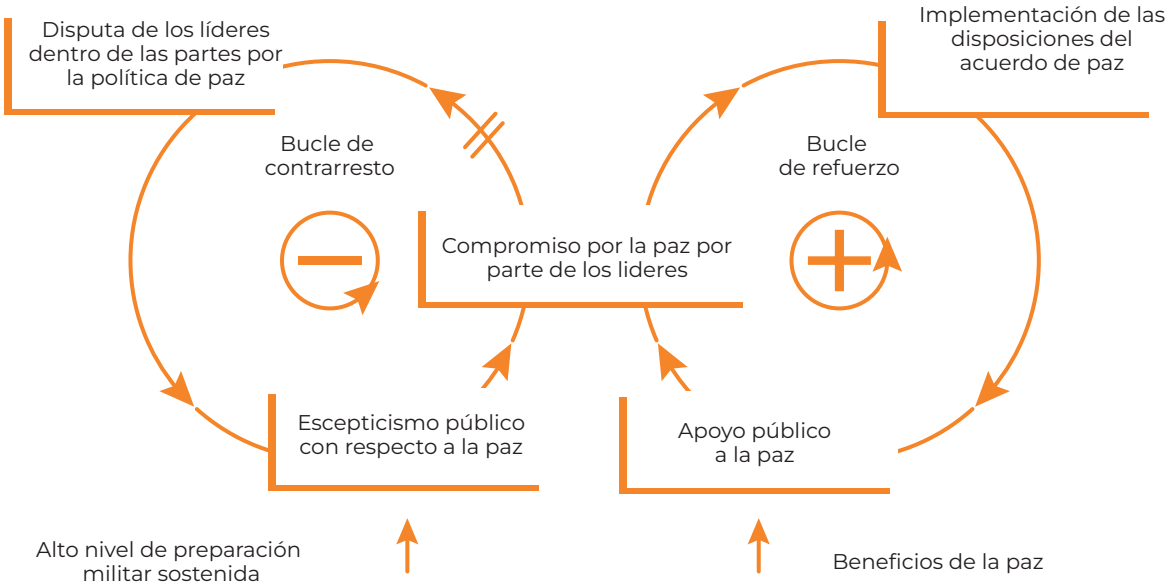
- Campo de batalla digitalizado: se da en el reino de la red esencialmente el reino de Tor y la Deep web (Elizalde, 2016).

- Enfoque sistemático del combate y la paz (ver figura 4): donde vienen a parar todas las variables que potencialmente ocasionan conflictos (Ropers, 2008).

- Operaciones sobre la información: mecanismos que se usan para manipular lo que piensa el público y favorecer las acciones militares en un conflicto (Ropers, 2008).

Figura 4.

Procesos de paz desde una perspectiva de sistemas



3. Globalidad: el Departamento de Defensa busca la participación de varios ministerios, agencias públicas y el sector privado. El sector privado aporta agilidad, motivación y renovación al sector con el objetivo de incorporar personal científico y técnico de alta cualificación para complementar al personal militar.

- Alianzas: predominan las formaciones de alianzas estratégicas asimétricas, incluida la participación de varias agencias estatales y actores privados en la formación de alianzas basadas en la teoría de juegos. Estas alianzas se basan en la defensa de los principios de la libertad, la defensa contra la guerra y el mantenimiento de la paz. Formar alianzas requiere cohesión interna entre varios departamentos y agencias que reaccionan coherentemente en sus acciones contra aliados y adversarios. Las alianzas proporcionan fuerzas y logística complementarias, lo que permite que se dediquen

menos recursos nacionales a misiones preventivas y de consolidación de la paz mundial y objetivos comunes en las relaciones regionales. Actividades concretas propuestas para impulsar este eje:

- Variedad de mercados
- Mejor protección para el diseño de infraestructura crítica: administración, servicios y defensa.
- Pronunciamiento de la consolidación del Estado de Derecho.
- Promoción del desarrollo
- Legítima defensa en cuanto a derechos y privacidad (Leiva, 2015).

4. Ingenio: se encarga de acaparar las mejores mentes en el ámbito científico y de innovación para que se incorporen al Departamento de Defensa.

Tenga en cuenta que la estrategia de los EE. UU. está dirigida esencialmente a fortalecer la superioridad militar de la nación de los EE. UU. en el mundo. Sin embargo, la perspectiva del sistema de ciberseguridad es más amplia, ya que incluye la clarificación de los principios de seguridad y defensa, así como la promoción del desarrollo tecnológico. Estados Unidos ocupa el primer lugar en el ranking de la UIT con un índice de 0,926 (UIT, 2018).

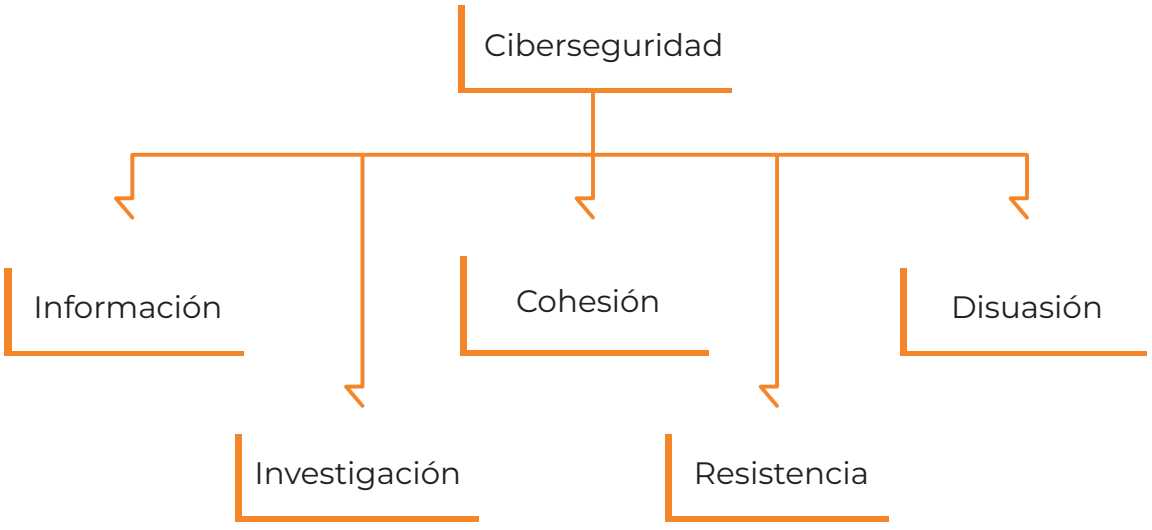
Estrategias de seguridad cibernética de los Países Bajos

La Estrategia Nacional de Seguridad Cibernética de los Países Bajos fue construida bajo 5 pilares que se subdividen en tareas y estrategias (ver figura 5):

1. Información: este eje analiza el capital y la disposición de las organizaciones que realizan investigaciones sobre amenazas de ciberseguridad y ciberdefensa. El Servicio de Seguridad de la Información Militar (MIVD) informa a los ciudadanos y organismos públicos sobre estrategias y herramientas para prevenir el ciberdelito, destacando el imperativo de tomar precauciones ante los ciberataques en curso. La agenda del MIVD incluye la implementación de acciones específicas derivadas de la coordinación con las autoridades públicas y privadas (Ministerie van Defense Netherlands, 2018). El MIVD define la prevención de ataques digitales como un principio.

Figura 5.

Estrategia Nacional de Seguridad Cibernética de los Países Bajos.



Nota. Ministerie van Defense Netherland (2018).

La prevención como principio no solo se deriva de la voluntad de anteponerse a la situación, sino que también necesita de la implementación de análisis y contramedidas que orienten al MIVD ante cualquier eventualidad, y el diseño de contramedidas en colaboración con el Servicio Integrado de Seguridad de la Información (IADL). En este orden, ENCS 2019 propone establecer una plataforma denominada Red Nacional de Detección (NDN). Su tarea es detectar, contener y defenderse de los ataques digitales. NDN es Nacional Cibernético Nacional Cibernético (NCSA), Comando de Defensa Cibernética (DCC), Unidad Conjunta de Señal Cibernética (JSCU) y AIVD, Servicio de Seguridad de la Información Militar (MIVD), Equipo de Defensa de Emergencia Informática de Defensa (DefCERT), Países Bajos Royal Malehauser. NDN construirá una plataforma de cooperación con NCSC, AVID y la policía. El MIVD tiene autonomía para actuar cuando se detecta una amenaza (Ministerie van Defense Netherlands, 2018).

2. Disuasión: esto incluye permitir que los atacantes sopesen el costo de los ataques cibernéticos cuando superan el éxito logrado. El objetivo es garantizar que la ciberseguridad y la ciberdefensa sean específicas del dominio militar mediante la extensión de la Alianza de la OTAN (OTAN) al ciberespacio, como firmó la Alianza de la OTAN (OTAN) en la Cumbre de Varsovia en 2016. 2016). Países Bajos se ha comprometido a contribuir con sus capacidades cibernéticas a las misiones de la OTAN. En este orden, la evaluación de puntos débiles del Ministerio de Defensa es sumamente importante para misiones en el espacio digital que requieren la participación de personal formado en las más altas habilidades en seguridad cibernética (Ministerie van Defense Netherlands, 2018).

3. Resistencia: aborda la adaptación del ejército de Países Bajos a las amenazas cibernéticas y la adaptación de los sistemas de defensa y ataque a los avances en tecnología de la información (TI). Los ataques cibernéticos se pueden contener y disuadir siempre que se logren altos niveles de resiliencia digital, lo que lleva al desarrollo de una cultura de prevención y tiempos de respuesta mejorados. Además, hay niveles de organizaciones de defensa.

- Gobernanza: engloba todo lo relacionado a la dirección, enfoques y marcos que conciernen a la defensa en el mundo digital.

- Seguridad por diseño: se refiere al pilar en el que se implementan sistemas TI.

- Evaluaciones de seguridad: engloba todo lo relacionado a riesgos en menor escala, el seguimiento de estrictos pasos a seguir y reglamentos de seguridad.

- Vigilancia y seguimiento: se enfoca en el seguimiento de las conexiones del Ministerio de Defensa con redes externas (Ministerie van Defense Netherland, 2018).

4. Investigación: en caso de un ciberataque, busca establecer rutas críticas y sensibles a través de copias de seguridad de red paralelas disponibles en la Red Integrada de las Fuerzas Armadas Holandesas (NAFIN). Además, la demanda de personal con las habilidades necesarias para responder a los ciberataques ha llevado al Departamento de Defensa a desarrollar una política de seguridad cibernética que consiste en brindar oportunidades de desarrollo profesional y actualizar toda la información pública. Se planea elaborar estrategias para atraer y retener defensas profesionales. En este orden, el Ministerio de Defensa se unió a la Plataforma Holandesa de Ciberseguridad para la Educación Superior y la Investigación (Dcypher). Esto permitirá coordinar la investigación en las áreas de ciberseguridad, ciberdefensa y criptografía.Asistencia militar: el Ministerio de Defensa asume el compromiso de contribuir al respaldo de las plataformas digitales existentes, así como el diagnóstico de las capacidades y las falencias del propio Ministerio que requieren ser satisfechas.

Países Bajos es un pionero europeo en los campos de la seguridad cibernética y la ciberdefensa, y está impulsando la expansión de la alianza de la OTAN en la red. Países Bajos ocupa el puesto 12 en el ranking de la UIT de 2018 con 0,885 puntos.

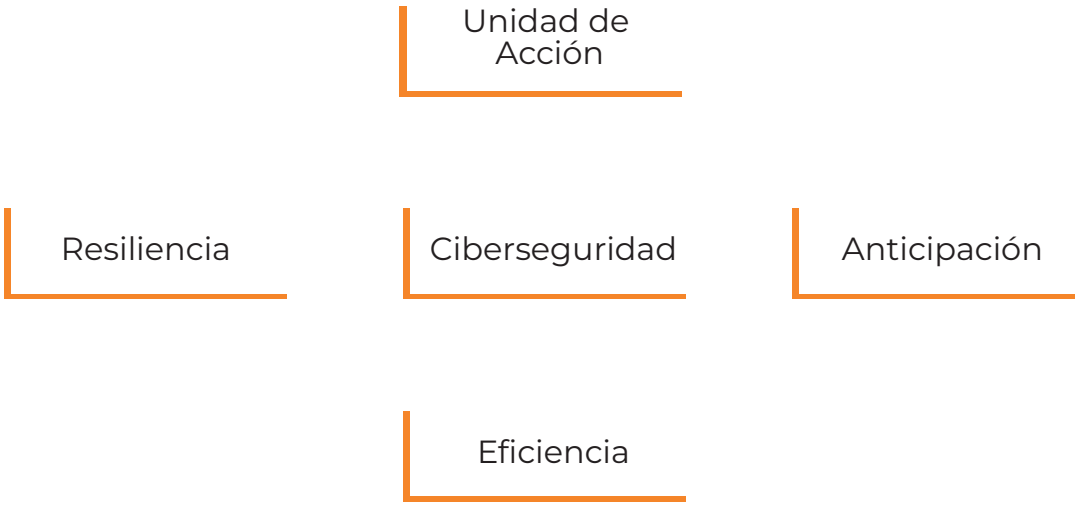
Estrategias de ciberseguridad de España

En España se puso en marcha en 2013 una Estrategia Nacional de Ciberseguridad, basada en el liderazgo y la coordinación entre los sectores público y privado. En 2018 se promulgó mediante Real Decreto la Ley 12/2018 de Seguridad en las Redes y Sistemas de Información. Como resultado, gracias a la experiencia adquirida, se han dado grandes pasos en materia de ciberseguridad. Así se refleja en la Estrategia Nacional de Ciberseguridad 2019, la cual se organiza en torno a los cuatro ejes

o principios rectores que se muestran en el siguiente diagrama.

Figura 6.

Estrategia Nacional de Ciberseguridad de España



Nota. Gobierno de España (2019)

Los principios rectores son un marco de objetivos generales previstos en la Estrategia Nacional de Ciberseguridad "que incluye las garantías del Gobierno de España para el uso seguro e integrado de la red, la protección de los derechos civiles y el fomento del progreso socioeconómico". adentro. España, 2019, p. 34). En este sentido, los cuatro principios están integrados en la Estrategia de Seguridad Nacional.

Figura 7.

Principios rectores. Estrategia Nacional de Ciberseguridad de España



Nota. Gobierno de España (2019)

Los cuatros principios rectores responden a la búsqueda de coherencia y unificación de criterios y acciones de los diversos entes públicos frente a las contingencias que se presenten en el ámbito virtual. En ese orden, estos principios demandan liderazgo que posibilite la convocatoria de los actores nacionales públicos y privados, quienes se comprometan con las tareas de anticipación y prevención de riesgos asociados a los espacios virtuales. La prevención a su vez reclama de eficiencia, lo que se traduce en la actualización permanente de los sistemas tecnológicos y la capacitación de los actores responsables de las plataformas virtuales para contener las amenazas y aprender de ellas.

Los cuatro principios rectores abordan la búsqueda de la consistencia y uniformidad en los estándares y el comportamiento de las distintas administraciones públicas ante las contingencias que se presentan en los entornos virtuales. En ese orden, estos principios requieren de un liderazgo que pueda aunar actores públicos y privados nacionales que se dedican a anticipar y prevenir los riesgos asociados a los espacios virtuales. La prevención requiere eficiencia. Esto se refleja en la constante actualización de los sistemas técnicos y la capacitación de los actores responsables de las plataformas virtuales para contener y aprender de las amenazas.

Los objetivos vertidos de manera específica responden a 4 pilares esbozados:

Garantizar la seguridad y resiliencia de las redes y sistemas de información: "Enfocarse no solo en la prevención, sino también en aprender de experiencias significativas y desarrollar una cultura de buenas prácticas en la gestión de la ciberseguridad" (Gobierno de España, 2019), p. 35). Contiene 12 acciones.

I. Rediseño de las capacidades concernientes a la ciberacción.

II. Implementación de mejoras con respecto a los centros de investigación que estudian las acciones a tomar frente a amenazas.

III. Se promueven las mejores practicas con respecto a la seguridad cibernética.

IV. Coordinación técnica y operativa entre los sectores público y privado y la sociedad en general.

V. Renovación de los protocolos de la seguridad cibernética.

VI. Potenciación de las actividades de ciberdefensa.

VII. Determinación de la evaluación de riesgos llevados a cabo por actores públicos o privados.

VIII. Se promueven actividades del CSIRT-España.

IX. Diseño de plataformas para intercambiar datos con respecto a ciberseguridad.

X. Desarrollo de herramientas para respuesta rápida ante ciberamenazas.

XI. Facilitación del intercambio de información sobre nuevas experiencias en ciberseguridad.

XII. Implementación defensa proactivas contra las amenazas cibernéticas.

Garantizar un uso fiable y seguro del ciberespacio. Esto incluye el seguimiento de actividades ilegales realizadas a través de la red. Entender que el ciberespacio "representa el ciberespacio como medio para que los delincuentes delinquen, como medio para investigar los delitos, y como ámbito en el que los delincuentes encuentran espacio para actividades ilícitas" (España, 2019, p. 36). Contiene 12 acciones.

I. Se promueven actividades de defensa y prevención.

II. Se promueven una mejoramiento de normativas para proteger infraestructuras que están en situación crítica.

III. Promoción del Esquema Nacional de Seguridad y del Sistema Nacional de Infraestructuras Críticas.

IV. Se promueven la inauguración de estructuras en seguridad cibernética en las comunidades autónomas así como también la promoción de los principios y estrategias del Esquema Nacional de Seguridad.

V. Desarrollo del Centro de Operaciones de Ciberseguridad.

VI. Mejoramiento de la infraestructura en telecomunicaciones.

VII. Redefinición de indicadores que posibiliten medir los niveles de seguridad cibernética.

VIII. Fomento de compromisos entre los sectores privado y público para prevenir riesgos.

IX. Diseño de catálogos de servicios y productos para la contratación del sector público en servicios y productos de ciberseguridad.

X. Mejoramiento de los sistemas de seguimiento en materia de seguridad cibernética.

XI. Promoción de la ejecución de simulacros de ensayo de los protocolos de ciberseguridad.

XII. Desarrollo de infraestructura científico-técnicas para su protección.

Proteger los ecosistemas empresariales y sociales de nuestros ciudadanos. Esta es una tarea que involucra a actores públicos y privados que están llamados a hacer un uso responsable de las tecnologías de la información. Además, facilita el intercambio de experiencias con los sectores público y privado para mejorar las estrategias nacionales de ciberseguridad. Incluye ocho actuaciones (Gobierno de España, 2019).

XIII. Redefinir el marco el marco jurídico.

XIV. Promoción de la participación ciudadana.

XV. Incentivar la investigación en el ámbito de la información.

XVI. Inducción de las instituciones y funcionarios públicos para que reporten ante la justicia penal los delitos cometidos en violación de la ciberseguridad.

XVII. Incentivación de la capacitación de las autoridades y policiales orientada a la aplicación de la normativa penal correspondiente en los delitos de criminalidad cibernética.

XVIII. Definir protocolos de ayuda entre investigadores científicos en el área de la seguridad nacional y los operadores de justicia.

XIX. Capacitación de los operadores de justicia, abogados y autoridades judiciales en todos los estratos en materia de cibercriminalidad, tecnologías asociadas y marco legal.

XX. Mejora en la coordinación de las investigaciones en materia de seguridad nacional.

Promover la cultura y la educación en ciberseguridad. Este objetivo persigue un abanico de autonomía tecnológica fomentando y facilitando a los ciudadanos de las competencias necesarias un mejor desempeño en el papel activo de los procesos de ciberseguridad y salvaguardar el patrimonio tecnológico. Incluye nueve medidas (Gobierno de España, 2019).

I. Resguardo de servicios de seguridad cibernética óptimos.

II. Provisión de seguridad cibernética y charlas para la mejora en las Mypymes.

III. Difusión de la perspectiva de seguridad cibernética como protección de la privacidad.

IV. Suministro de plataformas de denuncias eficientes y seguras para los delitos de ciberseguridad.

V. Incentivo a la cooperación tanto privada como pública en materia de seguridad cibernética.

VI. Evaluación de indicadores de riesgo en seguridad cibernética.

VII. Promocionar las mejores prácticas de seguridad cibernética entre las personas en general.

VIII. Implementación de sistemas blindados frente a los delitos de seguridad cibernética.

IX. Promoción de las convocatorias anuales del Foro sobre seguridad cibernética.

Promover la seguridad en la red a nivel internacional. Esto incluye promover un ciberespacio abierto, seguro, confiable y pluralista entre actores internacionales con vínculos bilaterales y multilaterales. Se basa en el respeto de los derechos fundamentales, la Carta de la ONU y el derecho internacional, y está en línea con los Objetivos de Desarrollo Sostenible. Contiene 9 acciones.

I. Incentivo de los programas de I+D+i en seguridad cibernética haciendo énfasis en la atención a las Mypymes.

II. Incentivo a la industria de la seguridad cibernética haciendo énfasis el respaldo a las Mypymes.

III. Desarrollo productos y servicios de seguridad cibernética haciendo énfasis en el estímulo a las Mipymes.

IV. Promoción de la exigencia de certificados de seguridad cibernética en los productos y servicios.

V. Renovación de las habilidades requeridas en los profesionales en seguridad cibernética.

VI. Diagnóstico de las demandas de profesionales en el ámbito de la ciberseguridad.

VII. Mejora de los perfiles profesionales en seguridad cibernética.

VIII. Mejora de las políticas de captación de profesionales especialistas en seguridad cibernética.

IX. Impulso a los programas de I+D+i en seguridad y defensa cibernética.

La Estrategia Nacional de Seguridad Cibernética de España se caracteriza por su mandato de implicar a los agentes públicos y privados en objetivos y actividades comunes encaminados a unificar la cultura de la ciberseguridad. España ocupa el puesto 7 en el ranking ITU 2018. Este es un importante paso adelante en términos de ciberseguridad, ya que ocupó el puesto 9 en 2015 (UIT, 2018).

Estrategias de seguridad cibernética de Perú

El Decreto Supremo N° 012-2017-DE aprobó la política de seguridad y defensa nacional del Perú. Esta política incluye una política de seguridad cibernética que incluye un concepto integrado de defensa nacional como un deber nacional y social. En ese orden, la Política Nacional de Ciberseguridad del Perú incluye la Ley N° 27, el Decreto Supremo N° 012-2017-DE sobre Seguridad y Defensa Nacional, y solo se encuentra la estructura de lo que se resume en la Ley 30999 o Ley de Ciberdefensa. Comprende básicamente el compromiso de la sociedad peruana de fortalecer su defensa nacional y su identidad peruana. En este sentido, las políticas nacionales de seguridad cibernética se actualizan constantemente con la ayuda de los sectores público y privado, fomentando especialmente la participación activa de las comunidades urbanas y rurales.

La difusión de información, la promoción de la ciberseguridad y la formación de funcionarios educadores es uno de los pilares de la política pública peruana. Con esto en

mente, se creó la Secretaría de Gobierno Digital. Esta Secretaría se encuentra sujeta al artículo 7 del Decreto Supremo N° 022-2017-PCM o Reglamento de Organización y Funciones del presidente del Consejo de Ministros. La Oficina de Gobierno Digital es responsable de diseñar y proponer políticas públicas nacionales, regionales y locales con el objetivo de modernizar y actualizar la nación en un proceso continuo que se adapte al proceso acelerado de innovación tecnológica global, cuenta con los permisos requeridos. Son funciones de la Secretaría de Gobierno Digital:

- Rectoría del Sistema Nacional de Informática.
- Definición y proposición de políticas relacionadas al gobierno digital.
- Asimilación de normativas relacionadas a la competencia.
- Revisión de los lineamientos del gobierno digital.
- Ejecución y auditoría de tareas y acciones de promoción y fortalecimiento del Sistema Nacional de Informática.
- Seguimiento y coordinación de la interoperabilidad de los sistemas informáticos.
- Seguimiento y coordinación de los portales Web del Estado, sus dependencias y evaluación sobre el seguimiento de las buenas prácticas.
- Administración del portal Web nacional.
- Acompañamiento de los organismos públicos en el mundo digital.

- Diseño de mejoras.
- Consulta técnica a las instituciones públicas.
- Mejora de propuestas de innovación.
- Seguimiento y diseño de indicadores de digitalización estatal.
- Mejora de la seguridad digital.
- Incentivar la organización público-privada instando a la ciudadanía en materia de innovación y adecuación digital de las instituciones públicas.
- Asesorar a la organización en temas tecnológicos.
- Ofrecer opiniones en el ámbito de su competencia.

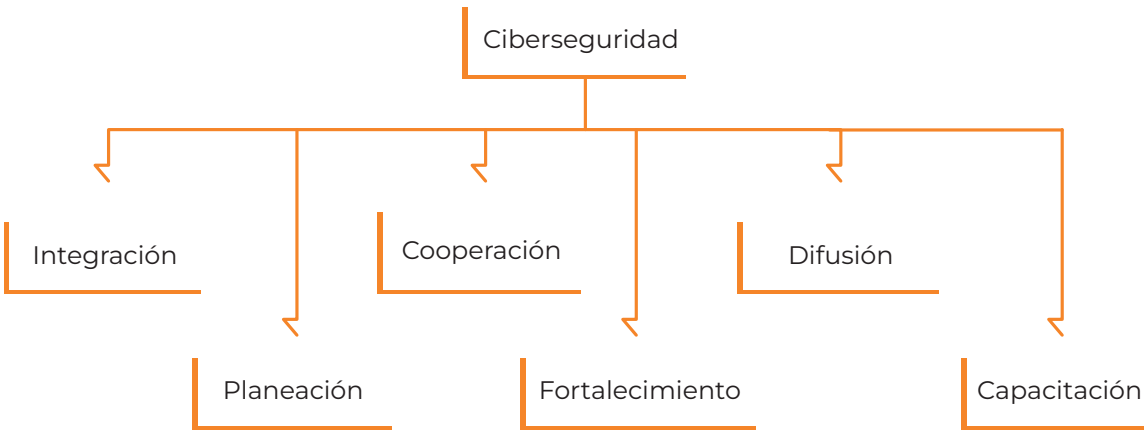
Junto a la Secretaría de Gobierno Digital, se encuentra el Sistema de Coordinación de Emergencias en Redes de Telecomputadoras – PeCERT, de la Presidencia del Consejo de Ministros, establecido en 2007 mediante Acuerdo Ministerial N° 360-2009-PCM. Luego, en 2012, el PeCERT fue asociado por el CERT CC (Equipo de Respuesta a Emergencias Informáticas - Centro de Coordinación) como el CSIRT Nacional de Perú (Equipo de Respuesta de Información de Seguridad Informática) (Presidente del Consejo de Ministros de 2012). La acreditación de PeCERT por parte de la comunidad de seguridad cibernética más importante del mundo marca el ingreso de Perú al sistema mundial de ciberseguridad, dando acceso a recursos de los centros con mayor experiencia en la materia y aumentando el CERT Formado. Sin embargo, la participación en la comunidad CERT no elimina los riesgos asociados con el uso de plataformas

virtuales. En 2016, el Grupo de Trabajo Anti-Phishing (APWG) identificó a Perú como el quinto país más vulnerable a los programas de infección por virus. 95 en el mundo y 12 en el ranking regional (UIT, 2018).

Dentro de esta estructura institucional, Perú promueve una política de ciberseguridad dirigida a proteger la infraestructura cibernética y las bases de datos gubernamentales. El Estado se compromete a proteger los datos nacionales y mantener la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. Las políticas nacionales de ciberseguridad se implementan en este orden (ver Figura 8).

Figura 8.

Política Nacional de Ciberseguridad del Perú.



La política nacional de ciberseguridad peruana se encuentra estructurada en torno a seis ejes:

1. **Fortalecimiento:** esto incluye el desarrollo de capacidades de protección de agencias nacionales para contener y defenderse de las amenazas que emanan de las plataformas virtuales. Este eje incluye el involucramiento de la sociedad

civil en diversas dimensiones como la académica, comunitaria, industrial y comercial, para que puedan participar en el desarrollo de estrategias de ciberseguridad y ciberdefensa. Alcanzar este objetivo se propone sensibilizar al público y profundizar los vínculos con expertos internacionales en la materia.

2. Capacitación: esto incluye capacitar a funcionarios gubernamentales para desarrollar las habilidades necesarias para implementar políticas de seguridad cibernética. Para lograr este objetivo se ha propuesto el uso de la plataforma PeCERT de la OEA, el CERT Internacional y la Comisión Interamericana contra el Terrorismo (CICTE). En una primera fase, será el responsable de reformar el plan de estudios de las escuelas de formación de oficiales y suboficiales, incluyendo asignaturas en las áreas de ciberseguridad y ciberdefensa.

3. Difusión: la implementación del plan de sensibilización de la ciudadanía en ciberseguridad incluye conferencias y foros sobre las mejores prácticas en ciberseguridad y la normativa vigente en la materia.

4. Cooperación: esto incluye fortalecer las leyes de ciberseguridad mediante el apoyo a organismos internacionales, la participación en organismos multilaterales enfocados en ciberseguridad, la firma de los acuerdos existentes en la materia y el cumplimiento de los compromisos inherentes a los Objetivos de Desarrollo Sostenible.

5. Integración: incluye coordinación permanente entre oficinas regionales conectadas al PeCERT y coordinación de procesos de renovación.

6. Planeación: desarrollar un Plan de Acción Nacional de Ciberseguridad, organizado por la Comisión Nacional de Ciberseguridad, que incluya a varias partes interesadas de los sectores público y privado.

Diálogo teórico-empírico

- Ciberseguridad en Perú

Las estrategias y políticas de seguridad cibernética en varios países tienen el objetivo común de mantener la integridad nacional contra las amenazas del mundo virtual (ver Figura 9). Sin embargo, persisten diferencias entre las perspectivas nacionales y los objetivos que se persiguen al implementar las políticas públicas de ciberseguridad. Tenga en cuenta que el mandato hegemónico global y regional de EE. UU. da como resultado una estrategia de seguridad cibernética que aborda la contención de competidores clave y trasciende los ejes de influencia. En el caso de los Países Bajos, sus intereses se equiparan con los de la Unión Europea y la OTAN bajo la teleología de unir estados continentales. Otro caso es España. España, a pesar de ser parte de la Unión Europea, tiene un propósito intrínsecamente endógeno de asegurar la continuidad del estado español y sus comunidades autónomas. Finalmente, el caso peruano presenta una situación en un país en desarrollo con alta penetración tecnológica y evidentes vulnerabilidades de ciberseguridad.

Por supuesto, los casos referidos no permiten comparaciones basadas en indicadores que representen el estado de desarrollo de las estrategias nacionales de ciberseguridad. Los casos mencionados por su naturaleza no permiten comparaciones aplicando indicadores que expresen niveles de desarrollo de las estrategias nacionales de ciberseguridad.

Figura 9.

Ciberamenazas y acciones maliciosas.



Nota. Gobierno de España (2019).

Sin embargo, es posible identificar la presencia de factores que conducen a que las vulnerabilidades requieran de políticas públicas para cerrar las brechas de seguridad cibernética abiertas. Así, aplicamos los indicadores recomendados por Leiva (2015) con el objetivo de identificar indicadores que representen vulnerabilidades en la política nacional de ciberseguridad del Perú.

Tabla 1.

Estrategias Nacionales de Ciberseguridad 2019

	País	Países Bajos	EE.UU.	España	Perú
PROTEGE	Infraestructuras criticas	x	x	x	x
	Economía	x	x	x	
	Seguridad nacional	x	x	x	x
	Bienestar social		x		
ENFOQUE	Concientización		x	x	x
	Conocimiento	x	x	x	
	Educación	x	x	x	
	Capacidades cibernéticas militares	x	x	x	x
SECTOR PUBLICO	Liderazgo/ coordinación	x	x	x	
	Marco jurídico	x	x	x	
SECTOR PRIVADO	Participación en la estrategia	x	x	x	
COOPERACIÓN INTERNACIONAL	Cooperación en su grupo	x	x	x	x
	Cooperación con otros países	x	x	x	x

Nota. Elaboración propia basada en Leiva (2015)

Estados Unidos lidera el camino en satisfacción con los indicadores de ciberseguridad en el Ranking Mundial de la UIT (UIT, 2018). Pionero en Europa en ciberseguridad, los Países Bajos ocupan hasta ahora el puesto 12 en el Índice de la UIT (UIT, 2018), por delante del Reino Unido, Francia, Lituania, Estonia, España, Noruega y Luxemburgo. Los Países Bajos no lograron alcanzar los indicadores de bienestar social y concienciación. Con respecto a los indicadores de bienestar social, los Países Bajos priorizan la seguridad nacional y la seguridad del estado continental de la Unión Europea sobre la protección del bienestar y la conciencia de la comunidad nacional. Es ciberseguridad y no sacrifica una métrica por otra.

La ventaja comparativa de España sobre los Países Bajos se explica por un enfoque de resiliencia. España prioriza concienciar a la ciudadanía sobre la seguridad cibernética y aprender de las desafortunadas experiencias de los CERT en todo el mundo. Esta decisión estratégica situó a España en el 7° puesto del Índice ITU, por delante de solo cuatro países: Estados Unidos, Canadá y Europa.

En el marco anterior, Perú ocupa el puesto 95 en el Índice ITU (ITU, 2018). A nivel regional ocupa el puesto 12, superando a países como Panamá, Ecuador, Venezuela, Guatemala y Nicaragua. Según Leiva (2015), desde 2015, los países de la OEA han fortalecido conjuntamente la ciberseguridad. Quince años después de la adopción de la Estrategia Integral Interamericana de Ciberseguridad, la iniciativa ha identificado un grupo de países con un nivel moderado de capacidad de respuesta cibernética, mientras que un grupo de países con una capacidad de respuesta cibernética mínima continúan mostrando asimetrías regionales

graves. , como la presencia de Varía entre media y alta. Perú es uno de los países con capacidad de respuesta moderada a baja.

El caso peruano es único en el sentido de que cuenta con una amplia legislación de ciberseguridad que abarca múltiples instrumentos legales. En 2019 se promulgó la Ley de Ciberdefensa estando pendiente de promulgación la Ley de Ciberseguridad. Ambas leyes contienen aportes innovadores para mejorar el índice de ciberseguridad, pero solo se encuentra vigente la Ley de Ciberdefensa. En el momento de la evaluación de la UIT, se están discutiendo dos instrumentos legales y se necesita más tiempo para demostrar el impacto de la adopción de leyes de ciberdefensa en las métricas de ciberseguridad.

Es importante distinguir entre los dos instrumentos. La Ley de Ciberdefensa tiene por objeto regular las operaciones militares en el ámbito de la ciberdefensa, mientras que la Ley de Ciberseguridad se ocupa de las medidas cautelares frente a las ciberamenazas. Tanto las medidas vigentes como las previstas tienen la tarea de cumplir con los indicadores de la UIT, protegiendo así al país ya la sociedad peruana de las ciberamenazas y reduciendo el rezago tecnológico que genera la aceleración de la dinámica en el desarrollo de la productividad digital. Sin embargo, las leyes por sí solas son insuficientes para proteger la estructura económica y el bienestar social, y la velocidad del desarrollo de las TIC tiende a hacer obsoletas las regulaciones antes de que entren en vigor las leyes más recientes. Esto no conducirá a retrasos regulatorios inevitables, sino solo a una alineación permanente de los asuntos regulatorios en línea con las mejores prácticas de ciberseguridad y ciberdefensa. Para

los latinoamericanos esta dinámica representa un gran desafío, ya que el peso de la burocracia hispana es un gigante a vencer.

De esta manera, el país y la sociedad peruana continúan realizando acciones de sensibilización y desarrollo de capacidades cibernéticas militares como indicadores clave en el diseño de la política nacional de ciberseguridad. El liderazgo está en gran medida en manos del Estado, pero la ciberseguridad es una obligación social que requiere claridad entre los sectores público y privado, algo que el Perú aún debe reconocer. ámbitos, construyendo una plataforma que acerque a los internautas públicos y militares, públicos y privados, académicos, investigadores, industriales, comerciantes, y en general a la sociedad peruana en su conjunto.

Perú muestra un comportamiento diferente en indicadores de cooperación regional, bilateral y multilateral. Contamos con un contrato de asesoría militar con Estados Unidos, lo que nos permite fortalecer nuestras ciberdefensas y sistemas de ciberseguridad en base a nuestra experiencia en Estados Unidos. Adicionalmente, dentro de la plataforma de la OEA existen acuerdos regionales que facilitan la cooperación con socios regionales.

Según los mencionados indicadores, el Estado peruano confronta el reto de satisfacer los indicadores ITU, lo que se resume en:

I. Elaboración de plataformas sumamente seguras que protejan los sistemas del Estado y de las personas.

II. Capacitación de fuerza de trabajo altamente especializada.

III. Mejora de los CERT regionales.

IV. Convocatoria eficiente a la ciudadanía para que se incorpore al desarrollo de planes y protocolos de seguridad cibernética.

V. Coordinación regulada y firma de convenios internacionales de seguridad civernética innovadores.

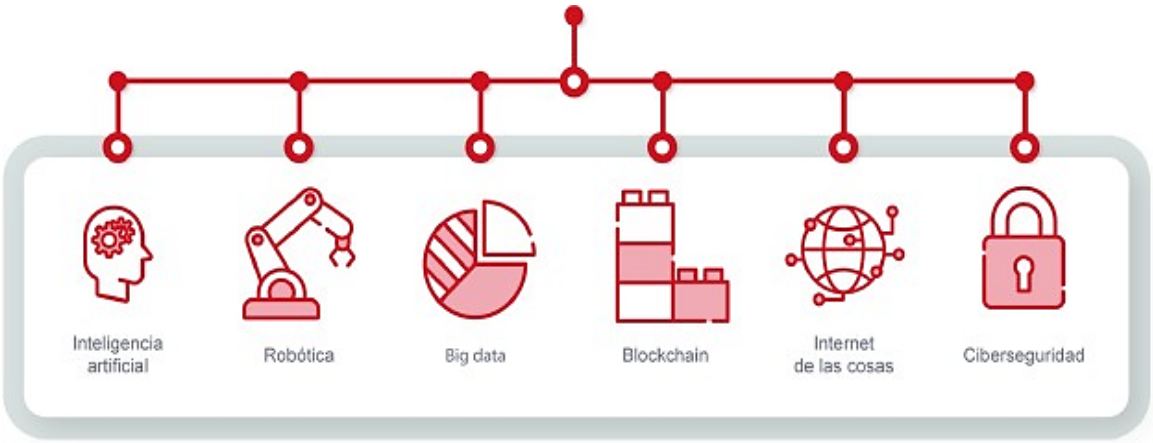
VI. Reafirmación y reimpulso del PeCERT.

VII. Democratización de la participación ciudadana en materia de seguridad cibernética.

Todo esto con el afán de mejora y alcanzar la transformación digital del Estado peruano bajo la premisa del blindaje cibernético (ver figura 10).

Figura 10.

Transformación digital



Nota. Gobierno de España (2019).

Conclusiones

La ciberseguridad constituye un aspecto fundamental para la consecución de los objetivos socioeconómicos de las economías modernas; asimismo, las estrategias están formuladas para ser implementadas conforme al sistema de categorización específico que ha decidido cada país para aplicarla de tal modo que estas puedan presentarse a la población mediante una norma, un reglamento, políticas o programas generales nacionales existentes en relación con la ciberseguridad. Es importante también mencionar que una de las estrategias de ciberseguridad está configurada por el resultado del esfuerzo multidisciplinario de colaboración en provecho de los conocimientos, experiencia y pericia de las organizaciones públicas y privadas a favor de las políticas nacionales y reconocimiento de la necesidad de reforzar por convenios participativos de cooperación de la comunidad

internacional en materia de constante capacitación para dar respuesta oportuna en relación con los índices de respuestas ante ciberataques de cualquier índole. Cabe mencionar que, en 15 años desde la adopción de la Estrategia Interamericana Integral de Ciberseguridad, esta iniciativa continúa evidenciando profundas asimetrías regionales donde existen grupos de países con capacidad mínima de respuesta ante ciberataques, otros se encuentran en niveles intermedios con capacidades de respuestas que fluctúan entre medias y altas. Perú se ubica entre los países con capacidad de respuesta de media a baja.

Asimismo, se observó que la Constitución Política del Perú en su artículo 44°, concatenado con el artículo 163°, establece que son deberes primordiales del Estado brindar la seguridad tanto en relación con la protección de la población, garantizar derechos humanos, y entre otros, la defensa de la seguridad y la soberanía de la nación, dejando expuesto que el acceso a contenidos y materiales gráficos del internet puede ser perjudicial por no ser apto tanto para menores de edad (por el contenido sexual, violencia y de drogas al que se expone) como para la sociedad que está expuesta al "hackeo" de información personal, entre otros. Por otro lado, en el 2011 se aprobó un Plan Estratégico de Desarrollo Nacional, denominado Plan Bicentenario, el cual se proyectó hasta el 2021, en función de mejorar tanto el aspecto del ciberespacio como el comercial inclinándose hacia este último. Por lo que, aun cuando se plantean proyectos y planes estratégicos de acciones estratégicas cuyo despliegue se proyecta en tres fases, en las cuales se pretende visionar cómo abordar las áreas vulnerables deducidas en la tabla mencionada anteriormente, se enfocó en dar respuesta a las amenazas y riesgos que pudieran presentarse a la seguridad

nacional, bajo tres lineamientos, según la época claves, ya que tendían a la modernización y reforma de las Fuerzas Armadas, el fortalecimiento de las acciones sociales y la lucha contra el narcotráfico, actividades exclusivas del Ejercito del Perú, por lo que dista de la fusión de la actividad civil, mientras que el Estado y la sociedad peruana transiten por el largo camino de plano táctico del desarrollo y análisis de riesgo, y los enfoques de la concientización en el desarrollo de las capacidades cibernéticas, tanto de la sociedad civil y militar como indicadores prevalentes en el diseño de las políticas nacionales de ciberseguridad, demanden un verdadero compromiso social que involucre la articulación entre el sector público y el sector privado, lo que en Perú aún no se concreta, razón por la cual no se aprecian avances.

En cuanto a las limitaciones resaltantes en el desarrollo de la ciberseguridad en Perú, se señala que las debilidades estructurales y las fluctuaciones de la gobernabilidad en la vía virtual requieren la construcción de plataformas donde concurran los ámbitos público y privado para la configuración de estrategias nacionales de ciberseguridad que respondan a las demandas de internautas civiles y militares, públicos y privados, académicos, investigadores, industriales, comerciantes y en general de la sociedad peruana en su conjunto. En ese orden, el diseño de la Estrategia Nacional de Ciberseguridad del Perú constituye una necesidad que demanda ser satisfecha, desde la palestra de la planificación para la prevención y no como respuesta a los ciberataques, lo cual amerita intencionalmente un cambio en la postura de la política nacional que sustenta erradamente la idea que las estrategias se irán definiendo en relación con los logros alcanzados.

En cuanto a las brechas en materia de desarrollo, se concluye que son un efecto más interesante que la mega tendencia del uso del ciberespacio y las facilidades que presenta se obtiene en un gran impacto para la reducción de las brechas de acceso a la información en el acceso de bienes y servicios que auguran nuevas oportunidades de negocios y de desarrollo, pero a su vez configura la apertura de una gran brecha a los ladrones de información que acechan el ciberespacio, esto afecta a los sectores de bajos ingresos de los países en vías de desarrollo. Asimismo, hay que indicar que la principal brecha que se presenta es una gran carencia de tecnologías adecuadas y/o novedosas que permitan el funcionamiento y mantenimiento del orden interno, orden público y seguridad ciudadana. Y debido a la carente tecnología de punta, la inestable y crítica infraestructura de protección y gestión del riesgo de desastres, por contener programas ya obsoletos e ineficaces evita una articulación en tiempo real, bien por la ausencia de un ente rector que verifique, promueva y canalice estas acciones a través de tecnologías de la información y comunicación que contribuyan a garantizar la seguridad nacional.

Finalmente, mencionar los diversos elementos técnicos que utilizan los hackers para lograr estos puntos de entrada y salida de ciberataques con el fin de llenar los vacíos y optimizar el desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú. Las infracciones se combaten con la adecuación y renovación de tecnología avanzada para enfrentar las amenazas desde una perspectiva preventiva, y no eliminar los males ya causados. La segunda es la falta de integración de intereses personales y unificarlos por el bienestar del país en general.

Recomendaciones

Fortalecer la seguridad nacional a través de una estrategia de ciberseguridad estructurada como resultado de la colaboración interdisciplinaria para beneficiarse del conocimiento, la experiencia y la especialización del público, luego de una investigación profunda sobre ciberseguridad realizada, se propone aplicar las propuestas desarrolladas en la investigación y organismos privados. Asimismo, se debe reconocer la necesidad de potenciar la formación continua a través de acuerdos de cooperación participativa de la comunidad internacional para posibilitar una respuesta oportuna en cuanto a índices de respuesta ante ciberataques de todo tipo.

Estudiar y mejorar los sistemas de intercambio de información, investigación y respuesta con los estados y organismos del sector privado que han contribuido a los avances en la predicción de ataques y crisis cibernéticos.

A nivel nacional e internacional se requiere evaluar y mejorar la capacidad de los gobiernos para identificar, arrestar y alinear los sistemas legales nacionales con los marcos normativos internacionales para enjuiciar a los perpetradores de delitos cibernéticos.

Se recomienda desarrollar constantemente los recursos normativos, humanos y técnicos para crear espacios para la integración de alianzas estratégicas que puedan ajustarse con precisión en el momento en que se detecten las limitaciones. Ampliar la cobertura de detección de ciberataques para permitir la detección y el bloqueo en tiempo real, y desarrollar técnicas de respuesta que tienen como base la IA.

Se recomienda que se introduzcan técnicas innovadoras de administración de instalaciones, interfaz avanzada y servicio de dominio, o acceso remoto apropiado para remediar las violaciones desde una perspectiva proactiva en lugar de como respuesta a un ataque. Acceso VPN para gestionar de forma centralizada los cortafuegos de los sistemas de detección de amenazas para respaldar y prevenir los delitos cibernéticos y crear una red de ciberseguridad que incluya a todas las autoridades, empresas y organismos gubernamentales pertinentes.

Juan Ormachea, Rolando Espinoza,
Sabino Ernesto, Nino Delgado, Jorge Alberto Montaño

5

CAPÍTULO

PROPUESTA DE ESTRATEGIA **NACIONAL DE CIBERSEGURIDAD** EN PERÚ

PROPUESTA DE ESTRATEGIA NACIONAL DE CIBERSEGURIDAD EN PERÚ

La seguridad siempre ha sido una gran preocupación para los Estados y las organizaciones. Fue crucial incluso en los días de las tarjetas perforadas y la presentación manual de datos en formato impreso. Un solo archivo perdido en esos días podía costar mucho a la industria y también con mayor afectación a la seguridad nacional. Hoy, sin embargo, las apuestas son aún mayores porque la información circula por el ciberespacio donde existen demasiados riesgos y ahora amenazas.

Con la creciente frecuencia de los ataques cibernéticos, el costo también ha aumentado. Informes recientes revelan que el costo de una sola violación cibernética es de alrededor de 84,000 a 148,000 dólares para una pequeña empresa. Esto ni siquiera incluye el costo de remediación y recuperación; si el ataque es al Estado, a una infraestructura crítica u organización estatal, agregue la pérdida de confianza de los inversionistas y el daño será irreparable. En la banca y la empresa privada, con un golpe tan grande, no es de extrañar que el 60 % de estas empresas cierren en los seis meses posteriores a un ciberataque. Una sola violación puede resultar fatal para un negocio y también para la seguridad nacional, por lo tanto, la mejor estrategia es la prevención.

La ciberseguridad no es solo una palabra de moda. No es un truco de marketing para vender servicios y soluciones. Con un número creciente de amenazas cibernéticas que también se están volviendo más sofisticadas cada día, la seguridad cibernética o ciberseguridad es la necesidad imperiosa de hoy. Cualquier país podría estar a solo una brecha de un ciberataque que comprometa seriamente la economía, el bienestar de su

población y hasta la seguridad en todas sus dimensiones, hay mucho más en juego que dinero, por lo tanto, se debe contar con políticas adecuadas y con estrategias integradas para lograr la anhelada seguridad digital, y al referirse a que deben ser integradas es consecuencia de que si estas amenazas afectan a la seguridad, se entiende ahora que esta seguridad es multidimensional, por lo tanto, las estrategias y acciones coordinadas que se proponen en esta investigación deben de ser de competencia política, económica, social, medioambiental y militar inclusive, aun sabiendo que las FF.AA. son responsables de la ciberdefensa.

La presente propuesta, cónsona con el tema desarrollado, es conducente directamente con la ciberseguridad, cuya actividad se concentra a nivel estratégico en maximizar la participación y atención por parte de este nivel, abordar la planificación para la protección, persecución, detección y sanción de los agentes delictuales en el ciberespacio, y la disminución del nivel de riesgo que permita preservar la confidencialidad, integridad y disponibilidad ante las amenazas, peligros y daños al que está expuesta la información de los ciudadanos en el ciberespacio.

En cualquier área en la que se pretenda resguardar la seguridad y derechos de los ciudadanos, la improvisación es el primer detonante de debilidad y riesgo, por ello, en la ciberseguridad la carente capacidad de enfrentar riesgos cibernéticos (SEDENA, 2014), la carencia de tecnologías de última generación y la ausencia de un ente rector que plasme estas acciones a través de tecnologías de la información y comunicación que contribuyan a garantizar la seguridad nacional, tal y como se enuncia en la Política de Seguridad y Defensa Nacional sustentada en lo expuesto en el Decreto Supremo N° 012-2017-DE, son algunos de los aspectos que impulsan la necesidad de implementar un plan estratégico concentrado en complementar

y reducir las brechas en materia de tecnología y ciberseguridad para optimizar el desarrollo, evaluación y actualización de la Estrategia Integrada de Ciberseguridad en Perú.

La ciberseguridad comprende una cultura multidisciplinaria de conciencia participativa y preventiva de la materia. Ofrecer un grado mínimo de seguridad amerita vigorosamente la participación conjunta de expertos, tecnologías y estrategias integrales de ciberseguridad para obtener un control en las redes que detecte las "alertas tempranas" con base en una estructura de supervisión y monitoreo, para la detección temprana con generación de alertas ante cualquier actividad anómala. Por ello, es menester la existencia de un mecanismo o procedimiento para determinar con precisión qué infraestructuras, plataformas, dispositivos, redes y sistemas deben ser monitoreados permanentemente y de qué forma se desarrollarán y revisarán los correspondientes informes de resultados de la evaluación de monitoreo, apegados a las líneas de acción en las estrategias de ciberseguridad que involucre el desenvolvimiento del nivel estratégico, regional o local.

El Estado como ente que, mediante la verificación, ejecución de supervisión y diseño de las acciones de mejora, mantiene activo el estado de seguridad, comprende en la presente propuesta comprometerse específicamente en trazar este primer nivel que se ciñe a un plan estratégico de lineamientos, selección de los recursos, modo de acción y ámbito de participación. No obstante, en cuanto a los otros dos niveles restantes se hace ocasionalmente referencia que el desarrollo de estos se fomentará en el devenir del desarrollo de las mismas estrategias.

El plano local o táctico, o nivel usuario, comprende el desarrollo y análisis del riesgo, el diseño de estrategias de acción y sus zonas de aplicabilidad preferencial o piloto, el diseño de ingeniería de seguridad, el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), y el gobierno de seguridad e implementación del SGSI, de los cuales por integración multidisciplinaria se genere la probabilidad de controles de sistema de capas, bien con protección de los DNS o sistemas de tecnologías biométricas, lo que permite pasar al nivel operacional, que consiste en el funcionamiento y plena ejecución de la maniobra de cómo se plantea el empleo y funcionamiento de las herramientas de gobierno de seguridad mediante la monitorización, supervisión y detección de eventos dentro del sistema de intercepción de datos de diferentes capas de seguridad, que genera un impacto como buena estrategia encadenada a la escala de documentación del evento registrado, apropiado en una visión realista que se active, así como también clasificar o categorizar las alarmas permite efectuar un monitoreo y detección.

El panorama de riesgos a abordar es de amplio espectro por el carácter global del ciberespacio, el riesgo y amenazas provienen originariamente tanto del exterior como del interior del territorio peruano, por causa de actividades delictuales, afectando los derechos de las personas y socavando la confidencialidad, integridad y disponibilidad de los activos de información en el ciberespacio, y otras labores como el espionaje y vigilancia llevadas a cabo con diversos fines.

El principal objetivo de los ciberdelincuentes es acceder a la valiosa información confidencial, tanto de carácter personal como de las instituciones del Estado, como lo son los secretos militares que pueden ser usados para construir armamento,

rastrear movimientos de tropas o exponer a agentes de contrainteligencia, siendo una lista interminable de propósitos malévolos, por ello, se hace necesaria cada vez más profundizar y actualizar las estrategias para abordar la gran diversidad de ciberataques que perturban o pretenden destruir las infraestructuras gubernamentales físicas e incluso la posible producción de una ciberguerra.

El objetivo de la propuesta de estrategias integradas nacionales de ciberseguridad en el Estado peruano plantea cimentar un sistema participativo y cooperacional en el que se alienta la participación conjunta de todas las personas, organizaciones e instituciones públicas, privadas y militares a participar en actividades para desarrollar eficazmente un programa de ciberseguridad dentro de la nación que involucre la cooperación con la comunidad internacional, ya que esto exige una atención y acción más proactivas.

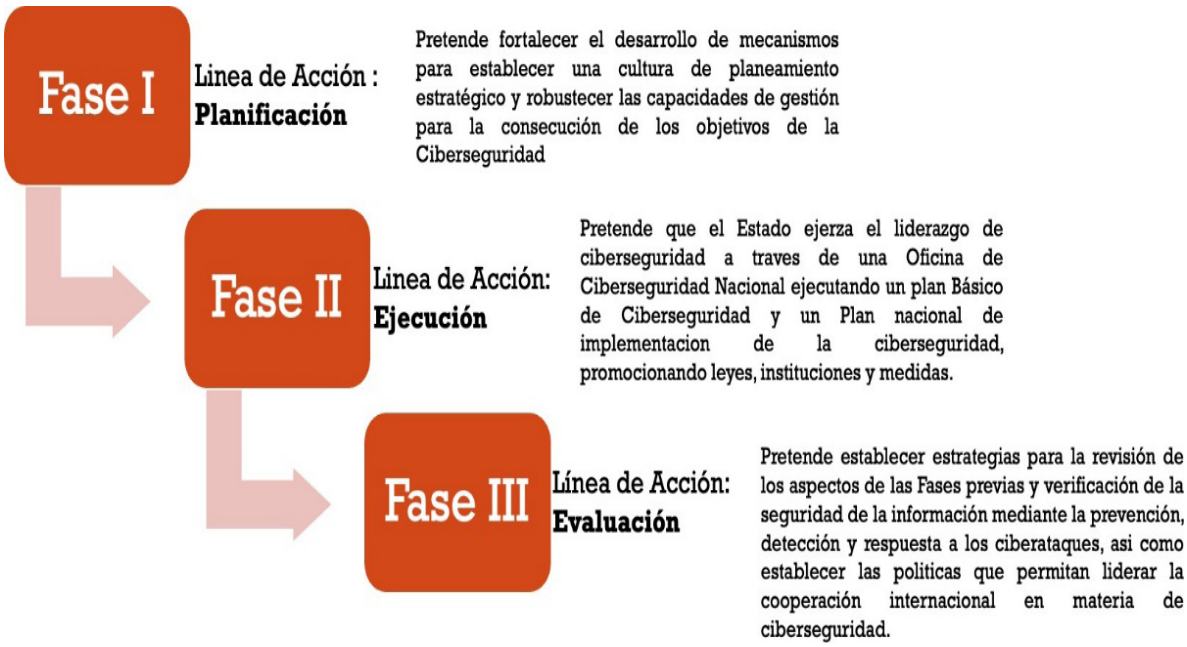
El ámbito de aplicación advierte que tiene alcance nacional y está específicamente referido a toda persona natural o jurídica y comunidad integrante del territorio nacional e incluso las instituciones u organismos del Sistema de Seguridad y Defensa Nacional sin que esto sea discriminatorio para las comunidades autóctonas.

Las acciones estratégicas se despliegan en tres fases (ver figura 11), en las cuales se pretende visionar cómo abordar las áreas vulnerables deducidas en la tabla mencionada en el capítulo anterior, donde se deduce la necesidad de una estructuración hacia una visión donde se procure disminuir la brecha en la capacidad de respuesta, reforzando las capacidades cibernéticas nacionales que involucran tanto la separación de las redes internas del Estado y de la internet pública como la

creación de una organización única encargada de liderar y gestionar la ciberseguridad a nivel nacional y de un sistema de alta tecnología para detectar y responder a los ataques cibernéticos en tiempo real.

Figura 11.

Fases estratégicas de Ciberseguridad Nacional.



Línea de Acción o Fase I

Las líneas de acción se presentan y se ponen a disposición, no solo con la finalidad de contribuir a la postura institucional, sino que también pretenden fortalecer el desarrollo de mecanismos para establecer una cultura de planeamiento estratégico y robustecer las capacidades de gestión en la institución con visión en la consecución de los objetivos de la seguridad nacional.

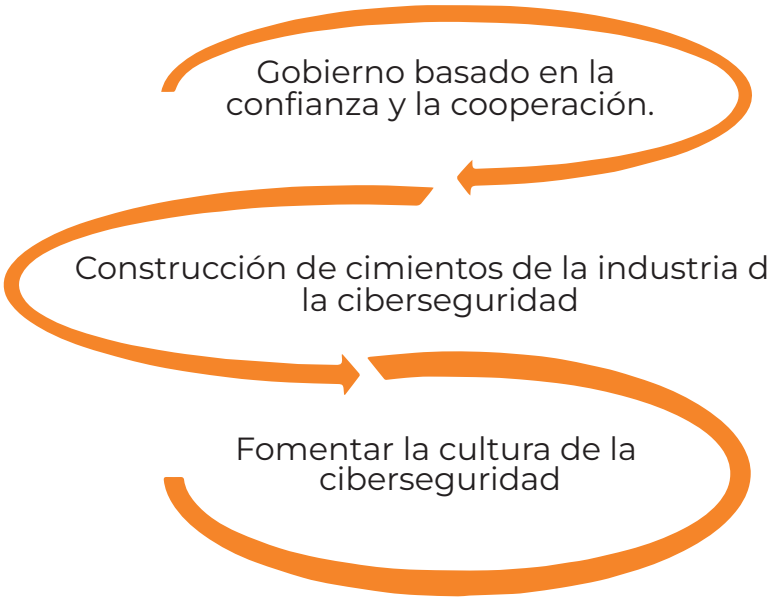
Generalmente, los efectos de los ciberataques se conocen cuando este ya se ha ejecutado, es decir, cuando el mal siempre está oculto y sale a la luz; es porque algo en su configuración falló y

hay muchos eslabones en la cadena de las "mafias organizadas". La estrategia de planificación involucra una apertura mental que proporcione una técnica con la capacidad de observar a profundidad, con alcance y trascendencia al punto máximo de poder ubicar la actividad del dominio asociado a la amenaza que sirve como conducto para redireccionar con sistemas sofisticados a los servidores y proxys que ocasionan el ciberdelito; sin embargo, equipos desactualizados y componentes obsoletos permiten que las amenazas se materialicen mediante la falsa sensación de seguridad que ofrecen ciertos cifrados de datos que se almacenan y quedan desprotegidos, esto y mucho más evoca la necesidad del diseño en el ámbito estratégico de "defensa informática" de vías técnicas para minimizar los riesgos del Sistema de Gestión de Seguridad de Información, por lo que involucra las medidas siguientes:

- El establecimiento de un gobierno basado en la confianza y la cooperación.
- La construcción de cimientos de la industria de la ciberseguridad.
- Fomentar la cultura de la ciberseguridad.

Figura 12.

Fase I



Establecer un gobierno basado en la confianza y la cooperación, conlleva:

Facilitar la cooperación e interacción público-privada-militar

- Crear un sistema de gobernanza en virtud del cual todas las entidades, incluido el Gobierno, compartan funciones y responsabilidades para cooperar en materia de ciberseguridad.

- Apoyar a las personas y a las empresas para que comparta la visión nacional de la ciberseguridad y mejoren sus capacidades para cumplir sus funciones.

- Crear una red de cooperación de expertos nacionales e internacionales para llevar a cabo investigaciones en profundidad sobre estrategias, políticas y otras cuestiones pertinentes en materia de ciberseguridad.

- Hacer esfuerzos para reducir los puntos ciegos de la ciberseguridad en el sector privado, mejorando la respuesta a los ataques cibernéticos, fortaleciendo la cooperación entre los organismos pertinentes y ampliando los recursos para apoyar a las instituciones.

- Ampliar las organizaciones y expertos dedicados y facilitar la colaboración con el sector privado para establecer un sistema de autogestión de la seguridad en el sector público.

- Mejorar la defensa de la ciberseguridad nacional para responder activamente a las amenazas de las redes de información y comunicaciones en las entidades públicas del Estado.

- Crear la Secretaria de Ciberseguridad Nacional, y a través de ella supervisar la cooperación público-privada-militar, para lo cual se desarrollarán e implementarán políticas de ciberseguridad a nivel nacional.

- Construir y facilitar una información a nivel nacional con sistema de reparto

- Construir un sistema nacional de intercambio de información entre los sectores público, privado y de defensa para facilitar el intercambio de información sobre las amenazas cibernéticas.

- Desarrollar medidas para compartir al máximo la información sobre las ciberamenazas en los sectores público, privado y militar, y mejorar el funcionamiento de estos sistemas.

- Elaborar medidas legales para garantizar la confidencialidad y evitar usos no previstos, como la violación de la privacidad cuando se comparte información.

- Promover activamente el intercambio de información con organizaciones especializadas en el extranjero y compartir la información pertinente con las organizaciones nacionales para responder a las amenazas cibernéticas transnacionales.

Reforzar el fundamento jurídico de la ciberseguridad.

- Mejorar las leyes y las instituciones con el fin de responder sistemáticamente a las amenazas de la ciberseguridad, maximizando las capacidades de ciberseguridad en los sectores público, privado y militar, y concentrar las capacidades nacionales.

- Elaborar medidas legales que permitan obligatoriamente compartir, analizar y utilizar sistemáticamente la información sobre las ciberamenazas entre los sectores público, privado y militar.

- Fortalecer la base jurídica para responder al cambiante entorno de ciberseguridad, como la aparición de nuevas vulnerabilidades debidas a la utilización de la tecnología de inteligencia artificial.

- Construir las bases para el crecimiento del Sistema de Ciberseguridad Nacional conlleva crear un ecosistema innovador para la ciberseguridad en aras de garantizar la competitividad de la tecnología, los recursos humanos y las industrias que son fundamentales para la ciberseguridad nacional.

Ampliar la inversión en ciberseguridad.

- Promover la reforma reglamentaria y el apoyo para permitir que el sistema de ciberseguridad desempeñe un papel clave en la mejora del nivel de ciberseguridad del país.

- Incrementar progresivamente el presupuesto del gobierno orientado a la ciberseguridad y concebir medidas de financiación que puedan utilizarse en situaciones de emergencia, por ejemplo, para responder a ataques cibernéticos masivos.

- Promover el sistema de "notificación pública de la seguridad de la información" para fomentar la inversión en el sector privado y ampliar el apoyo fiscal a las inversiones en sistemas de seguridad e I+D.

Fortalecer la competitividad de la seguridad, mano de obra y tecnología

- Potenciar la experiencia y competitividad del personal de ciberseguridad del sector público con la capacitación permanente.

- Fortalecer los programas personalizados de desarrollo de personal para proporcionar a las empresas, el gobierno,

FF.AA. y la sociedad una fuerza laboral cibernética equipada con diversas capacidades.

- Dictar medidas para mejorar los conocimientos especializados en materia de ciberseguridad y contratar a personal con talento.

- Incrementar significativamente el presupuesto de I+D en ciberseguridad para reducir las brechas tecnológicas con los países desarrollados y adquirir tecnologías innovadoras de fuentes básicas para liderar el mercado mundial.

Fomentar un entorno de crecimiento para las entidades de ciberseguridad.

- Fomentar un entorno de cooperación entre la industria, sistema educativo e instituciones de investigación.

- Promover el apoyo gubernamental y la mejora continua de los planes para fomentar la creación de nuevas organizaciones de ciberseguridad.

- Fortalecer la competitividad global de la ciberseguridad nacional mediante el fomento de asociaciones estratégicas con entidades internacionales para intercambio de experiencias y conocimientos técnicos.

Establecer un principio de competencia ética en las actividades de ciberseguridad.

- Incrementar la capacidad tecnológica de los sistemas de ciberseguridad del Estado con adquisiciones basadas en la calidad de los equipos y no en el precio.

- Proponer procedimientos y normas para el establecimiento de los servicios particulares de ciberseguridad y de sus contrataciones de parte de entidades del Estado.

- Fomentar una cultura de ciberseguridad conlleva que la población reconozca la importancia de la ciberseguridad y esforzarse por aplicar normas básicas de seguridad, mientras que el gobierno debe respetar los derechos fundamentales de los ciudadanos al aplicar las políticas y facilitar la participación ciudadana.

Incrementar la conciencia de ciberseguridad y reforzar prácticas de ciberseguridad.

- Definir principios y normas de ciberseguridad para que la población pueda ser consciente de la importancia de la ciberseguridad y ponerlas en práctica en su vida diaria.

- Desarrollar y ejecutar programas educativos de cibernética y seguridad adaptados en sectores específicos de la sociedad, tales como estudiantes, funcionarios gubernamentales, personal militar y empleados del Estado.

- Fortalecer el concepto de la importancia de la seguridad de las informaciones en todas las entidades públicas y privadas, así como en las FF.AA.

Asegurar que los derechos fundamentales no sean afectados por la ciberseguridad.

- Asegurar que Perú cuente con un ciberespacio libre y abierto, respetando los derechos y la privacidad del pueblo.

- Establecer procedimientos para promover la participación de los sectores público y privado, así como de las FF.AA. en el proceso nacional de elaboración de las políticas de ciberseguridad.

- Mantener informado a los diferentes sectores, público y privado, sobre los riesgos e incidentes de ciberseguridad que afectan la seguridad nacional.

Línea de Acción o Fase II

Comprende replantear de manera constante una nueva vía o curso de acción para aumentar la infraestructura de seguridad nacional. El Gobierno deberá ejercer el liderazgo y cumplir con sus responsabilidades para alcanzar la visión y los objetivos de la estrategia nacional de ciberseguridad en cooperación con sus ciudadanos y empresas, así como con la comunidad internacional.

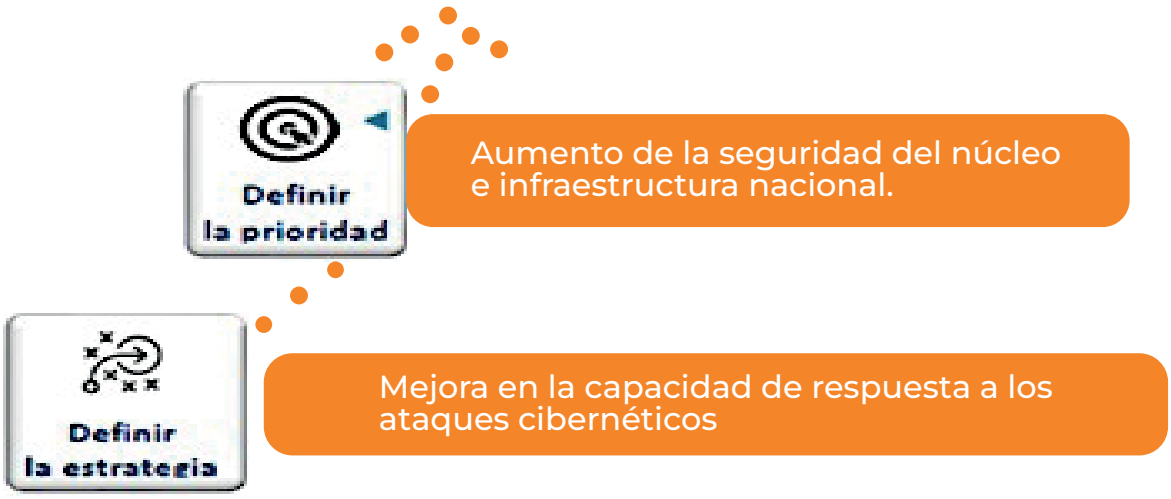
Establecer y llevar a cabo el plan básico nacional de ciberseguridad y el plan nacional de implementación de la ciberseguridad (nivel táctico y operacional) para dar forma e implementar esta estrategia con proporcionalidad, racionalidad y eficacia, en la cual cada ministerio y organismo debe perseguir los objetivos establecidos en dicha estrategia, cumplir con los principios básicos y llevar a cabo las tareas estratégicas de promoción de las leyes, instituciones y políticas relacionadas con la ciberseguridad, acorde a las siguientes medidas:

- El incremento de la seguridad en la infraestructura nacional.

- La mejora en la capacidad de respuesta a los ataques cibernéticos.

Figura 13.

Fase II



D. Incrementar la seguridad de la infraestructura central nacional amerita tanto reforzar la seguridad como la resistencia de la infraestructura básica nacional frente a los ataques cibernéticos para garantizar la prestación continua de servicios esenciales, para ello es menester:

Asegurar la seguridad de la información nacional y redes de comunicación

- Implementar medidas de seguridad por etapas para garantizar que las redes nacionales de información y comunicaciones estén protegidas contra las ciberamenazas en toda entidad del Estado, garantizar la operación y la eliminación de la amenaza.

- Desarrollar sistemas para ejecutar fiscalizaciones y mejoras permanentemente a fin de detectar y prevenir

cualquier amenaza de vulnerabilidad de seguridad en la red nacional de información y comunicaciones, así como en las redes y equipos conexos.

- Adoptar medidas de control estrictas para asegurar el funcionamiento de las redes nacionales de información y comunicaciones, incluyendo los sistemas de rendimiento avanzados y las instalaciones ampliadas de respaldo, a fin de garantizar la prestación de servicios frente a los diversos ataques cibernéticos.

- Mejorar los sistemas de seguridad de información, tanto criptográfica como confidencial, para que la información confidencial en general esté protegida contra filtraciones o daños en los datos.

- Incrementar la capacidad tecnológica y potencial humano del PCERT que permita sea el centro nacional líder e integrador en la gestión de los incidentes informáticos del sector público, privado y de las FF.AA.

Mejorar el entorno de ciberseguridad en las infraestructuras críticas.

- Mejorar los planes para permitir que el Gobierno designe y proteja rápidamente las instalaciones en infraestructuras críticas cuya interrupción en caso de ataque perturbe considerablemente la vida cotidiana de la población.

- Apoyar a las instituciones que gestionan infraestructuras críticas, para crear departamentos dedicados a la ciberseguridad y asignar un presupuesto suficiente para ello como prioridad del Estado.

- Suscribir directrices para que las instituciones asuman prioritariamente la seguridad de la infraestructura crítica para el establecimiento y creación de planes pertinentes e inspección.

- Fomentar un entorno que permita realizar evaluaciones voluntarias e inopinadas de seguridad a las redes o equipos de red e información de las infraestructuras que son críticas del sector privado.

- Diseñar e implementar procedimientos de evaluación de las vulnerabilidades de la seguridad específicas en cada sector y aplicar medidas correctivas para garantizar la continuidad de los servicios en caso de que se produzca un incidente de seguridad.

Diseñar e implementar un sistema de ciberseguridad nacional de alta tecnología.

- Ejecutar planes técnicos o multisectoriales para responder eficientemente a las nuevas amenazas contra la seguridad nacional provocadas por la convergencia tecnológica y el advenimiento de nuevas tecnologías en el ciberespacio.

- Implementar la “seguridad desde el diseño” del software y servicios de las TIC que pueden afectar directamente a la integridad de las personas, lo que permitirá garantizar su seguridad.

- Desarrollar e implementar redes informáticas de alta seguridad en las infraestructuras críticas que aseguren la eficiente operación y funcionamiento como parte de la seguridad nacional.

- Diseñar e implementar a nivel nacional un sistema de autenticación digital único que permita la utilización de los servicios de las infraestructuras críticas en seguridad.

- E. Mejorar las capacidades de respuesta a ataques cibernéticos, implica ampliar la capacidad para vislumbrar eficazmente los ataques cibernéticos por adelantado y conseguir lo antes posible la resiliencia.

Asegurar la prevención de los ciberataques.

- Contar con capacidades para responder activamente (defensa pasiva) a todos los ataques cibernéticos que infrinjan la seguridad y los intereses nacionales concentrando las capacidades nacionales.

- Fortalecer la capacidad preventiva mediante la creación de un sistema de monitoreo nacional que recopile, gestione y elimine eficazmente las vulnerabilidades del ciberespacio.

- Adquirir capacidades técnicas y tecnológicas para analizar y determinar las causas de los ciberataques e identificar la fuente.

Reforzar las medidas defensivas contra los ataques cibernéticos masivos.

- Evaluar y mejorar el sistema de intercambio de información, investigación, análisis forense y respuesta de los organismos pertinentes en relación con un ataque o crisis cibernética.

- Incrementar la capacidad de detección de ciberamenazas para permitir la alerta y el bloqueo en tiempo real, y desarrollar tecnologías de respuesta basadas en la IA.

- Mejorar las capacidades de respuesta frente a las crisis cibernéticas en todo el país mediante ejercicios conjuntos público-privados- militares, incluidos ejercicios nacionales de gestión de crisis.

- Propiciar y facilitar la cooperación público-privada-militar, incluyendo los deberes de emitir alertas de crisis cibernéticas, compartir información sobre amenazas y realizar exámenes e investigaciones conjuntas.

- Normar y establecer la clasificación cuantitativa y la categorización de las alertas de una cibercrisis, que permitan a los individuos, las empresas y el gobierno una respuesta a la crisis de acuerdo a protocolos establecidos con prontitud y eficiencia.

Coordinar permanentemente con las FF.AA. (Comando Operacional de Ciberdefensa del CCFFAA) sobre las respuestas activas para ataques cibernéticos.

- Revisar y alinear todos los medios de respuesta con las normas internacionales en caso de amenaza importante para la ciberseguridad y ciberdefensa y planificar medidas específicas de manera conjunta con las FF.AA.

- Desarrollar varias estrategias y tácticas, a través de los Comandos de Ciberdefensa de las FF.AA. y adquirir tecnologías básicas para salvaguardar la seguridad nacional y los intereses en la guerra cibernética.

- Capacitar a especialistas militares en guerra cibernética y apoyar la conformación de unidades de respuesta para llevar a cabo actividades de ciberdefensa de manera eficiente y coordinada con la ciberseguridad.

Mejorar las capacidades de respuesta contra la ciberdelincuencia.

- Fortalecer la gestión de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la PNP, responsable de investigar los delitos cibernéticos y establecer una red de seguridad cibernética, con la participación de todos los organismos, empresas, organizaciones e individuos pertinentes.

- Mejorar la capacidad del Gobierno para identificar, localizar, detener y enjuiciar a los autores de delitos cibernéticos mediante el potenciamiento de los conocimientos técnicos especializados de los responsables de investigar esos delitos, así como asegurar la cooperación con los organismos pertinentes en el país y en el extranjero.

Línea de Acción o Fase III

Corresponde a la revisión de todos los aspectos comprendidos en las fases previas, proceso que pretende alcanzar la revisión de protección de la información mediante la prevención, detección y respuesta a los ataques, para así evaluar las políticas que permitan liderar la cooperación internacional en materia de ciberseguridad.

La Oficina de Ciberseguridad Nacional, señalada en la fase II, deberá supervisar periódicamente la aplicación de esta estrategia y las mejoras de ciberseguridad de las personas,

empresas y entidades gubernamentales. Además, deberá examinar tanto la idoneidad del marco de ciberseguridad necesario para aplicar la estrategia como la eficacia de las estrategias de ejecución e implementación de la ciberseguridad a la luz de los cambios en el entorno de seguridad, subsanará las deficiencias, tomando siempre en consideración a lo reflejado por deficiencias en la estrategia, perseverando la inserción de mejoras cuando sea necesario, conforme a la siguiente medida:

Figura 14.

Fase III



F. Enriquecer los sistemas de cooperación bilateral y multilateral. Es decir, la cooperación internacional tanto pública como privada necesaria en virtud de la propia naturaleza de las amenazas, para el monitoreo y evaluación de las políticas públicas de ciberseguridad, impulsando la innovación y el desarrollo económico en materia de ciberseguridad a través de la promoción del debate multilateral y bilateral basada en relaciones fluidas en el ámbito de la ciberseguridad y orientada hacia la construcción de capacidades, lo que permite, además,

fomentar un criterio unificado de normas internacionales que promuevan la confianza y seguridad en el ciberespacio.

Explorar medios que permitan la cooperación práctica (bilateral y multilateral) para así establecer sistemas de asistencia mutua mediante la celebración de consultas sobre políticas cibernéticas, el fortalecimiento de la asociación con organizaciones internacionales y la adhesión a acuerdos internacionales.

Promover la cooperación en sectores como la defensa nacional, la inteligencia y el sistema judicial, así como el intercambio con el sector privado para responder a las amenazas a la ciberseguridad, incluidos los actos de guerra, terrorismo y delincuencia.

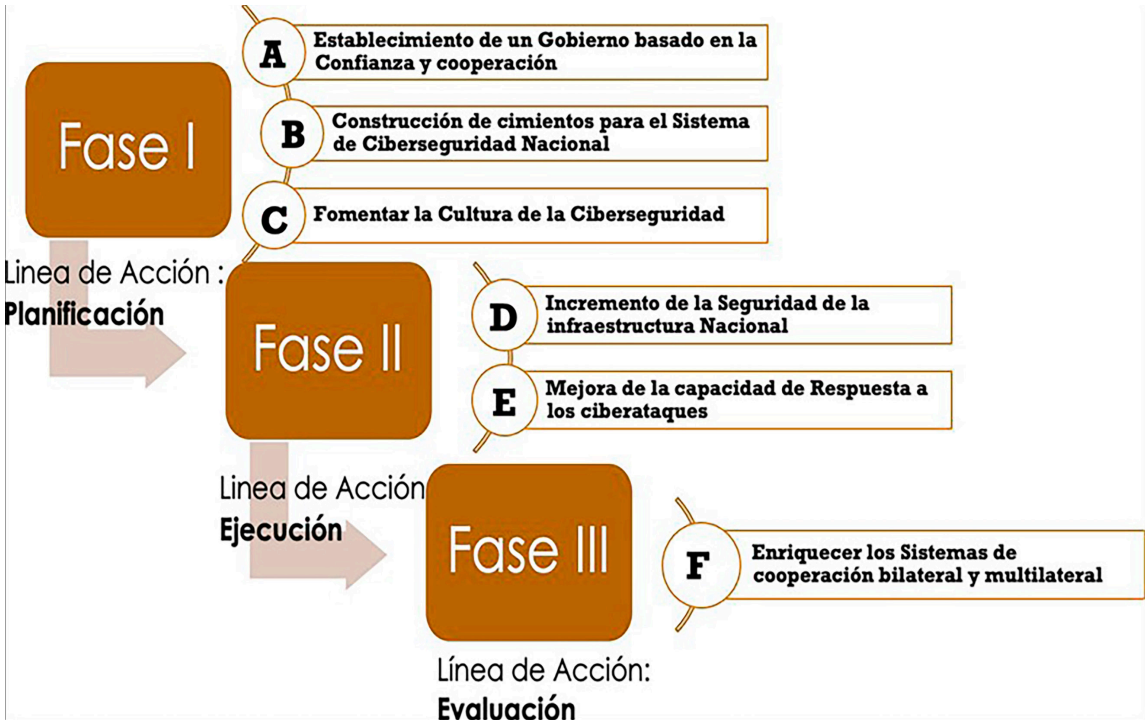
Proporcionar mecanismos que permitan a los entes u organismos pertinentes proponer orientaciones de política gubernamental para compartir la información recopilada durante todo el proceso de cooperación internacional.

El desarrollar una fuerza de trabajo de ciberseguridad superior, con alianzas con países como Japón, Corea, etc., y profesionistas a nivel mundial comprometidos en la constante capacitación, creada con el fin de mitigar los riesgos de la seguridad digital, incide directamente como una gran contribución al crecimiento de la economía digital nacional, y esta a su vez permite impulsar una mayor prosperidad social y económica del país, ya que al desarrollar plenamente un vasto grupo de talentos nacionales, al mismo tiempo atraerá a los mejores y más brillantes entre los extranjeros que comparten los valores peruanos, todo ello permite contar con una mano de obra altamente cualificada en materia de ciberseguridad, lo que es una ventaja estratégica para la seguridad nacional.

Cumpliendo así el propósito de garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos, y seguridad nacional promovida en la Estrategia de Seguridad Nacional del Perú.

Figura 15.

Lineamientos para las Estrategias Integradas de ciberseguridad



Referencias Bibliográficas

Abbate, Janet (1999). *Inventing the Internet*. MIT Press

Aragó, L. (2019). *El mapa de las guerras que siguen activas este 2019*. https://www.lavanguardia.com/internacional/20190120/454204868905/mapa-guerras-2019.html

Bergman, R. & Mazzetti, M. (2019, September, 4th). The Secret History of the Push to Strike Iran. The New York Times Magazine. https://www.nytimes.com/2019/09/04/magazine/iran-strike-israel-america.html

Berners-Lee T (2000) *Weaving the web*. Collins Book

Brose, C. (2019). The New Revolution in Military Affairs War's Sci-Fi Future. *Foreing Affaire, 98*(3). https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs

Chan, C. (2014, October 2nd). Hackers´ attack on JPMorgan Chase affects millions. *The New York Times*. https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0

Cryptomuseum. (2020). *History of the Enigma*. https://www.cryptomuseum.com/crypto/enigma/hist.htm

Doman, C. (2016, July 7th). The First Cyber Espionage Attacks: How Operation Moonlight Maze made history. *Medium*. https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7

Dos Reis, A. E. & De Brito, R. (2018). No Boots on the Ground': Reflections on the US Drone Campaign through Virtuous War and STS Theories. *Contexto Internacional, 40*(1), 53-71. http://www.scielo.br/pdf/cint/v40n1/0102-8529-cint-2018400100053.pdf

El Peruano. (2018, 12 de setiembre). *Decreto Legislativo 1410*. https://busquedas.elperuano.pe/download/url/decreto-legislativo-que-incorpora-el-delito-de-acoso-acoso-decreto-legislativo-n-1410-1690482-3

El Peruano. (2019). *Ley 30999 o Ley de Ciberdefensa*. https://busquedas.elperuano.pe/download/url/ley-de-ciberdefensa-ley-n-30999-1801519-5#:~:text=La%20presente%20ley%20tiene%20por,de%20competencia%2C%20conforme%20a%20ley.

Federation of American Scientist (1996, June 5th). *Security in Cyberspace. Appendix B. The case study: Rome Laboratory, Griffiss Air Force Base, NY Intrusion*. https://fas.org/irp/congress/1996_hr/s960605b.htm

Finkle, J. (2014). Iranian Hackers Use Fake Facebook Accounts To Spy On US Officials. Reuters. https://www.businessinsider.com/r-iranian-hackers-use-fake-facebook-accounts-to-spy-on-us-others-2014-29

Freedberg, S. J. (2013). Back off: How to curb Chinese cyber-theft. http://breakingdefense.com/2013/07/24/theyre-already-afraid-us-can-scare-china-gently-into-stopping-cyber-theft/

Garamone, J. (2018). *US Dept. of Defense (2018). DoD Official: National Defense Strategy Will Enhance Deterrence*. https://www.defense.gov/Explore/News/Article/Article/1419045/dod-official-national-defense-strategy-will-enhance-deterrence/

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, 38(2), pp. 41–73

Gibson, W. (2001). *Neuromante*. Ediciones Minotauro

Gillies, J. & Cailliau, R. (2000). *How the Web was Born: The Story of the World Wide Web*. Oxford University Press

Gobierno de España. (2019). *Estrategia Nacional de Ciberseguridad*. https://www.dsn.gob.es/es/documento/estrategia- nacional-ciberseguridad-2019

Goldstein, M., Perlroth, N. & Sanger, D. (2014, October 3rd). Hackers´ attack cracked 10 financial firms in major assault. *The New York Times*. https://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/

Greene, T., et al. (2003). *A Brief History of NSF and the Internet*. National Science Foundation

Guiora, A. (2017). *Cybersecurity. Geopolitics, Law and Policy*. Routledge

Hafner, K. & Lyon, M. (1998). *Where Wizards Stay Up Late: The Origins Of The Internet*. Touchstone

Hossein, B. (2012, December 13th). Structure of Iran's Cyber Warfare. Institut Francais d´Analyse Stratégique. http://www.strato-analyse.org/fr/spip.php?article223#outil_sommaire_3

Human Rights Watch (2006). *How Censorship Works in China: A Brief Overview*. Retrieved from https://www.hrw.org/reports/2006/china0806/3.htm

Instituto Nacional de Estadística e Informática –INEI–. (2018). *Estadísticas de las Tecnologías de Información y Comunicación en los Hogares*. https://www.inei.gob.pe/media/MenuRecursivo/boletines/01-informe-tecnico- n02_tecnologias-de-informacion-ene-feb-mar2018.pdf

ITU. (2018). *Global Cybersecurity Index. Committed to connecting the world*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01- 2018-PDF-E.pdf

Keats, D. & Franks, M.A. (2014). Criminalizing revenge porn. *Wake Forest Law Review*, 49, pp. 345-391

Kshetri, N. (2016). *The Quest to Cyber Superiority. Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*. Springer

Leiva, E. (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. DOI: https://doi.org/10.18294/relais.2015.161-176

Liang, Q. & Xiangsui, W. (1999). *Unrestricted Warfare*. People's Liberation Army Literature and Arts Publishing House

Lillemose, J. & Kryger, M. (2015, August 24th). The (Re) invention of Cyberspace. *Kunstkritikk*. https://kunstkritikk.com/the-reinvention-of-cyberspace/

Metz, S. (2001). Strategic asymmetry. *Military Review*, pp. 23–31

Ministerie van Defensie Neatherland. (2018). *Defensie Cyber Strategie 2018 Investeren in digitale slagkracht voor Nederland*. https://www.defensie.nl/binaries/defensie/documenten/publicaties/2018/11/12/defensie-cyber-strategie-2018/web_Brochure+Defensie+Cyber+Strategie.pdf

Naciones Unidas (1945). *Carta de las Naciones Unidas y estatuto de la Corte Internacional de Justicia*. Naciones Unidas

Nakashima, E. (2020, December 13th). Russian government spies are behind a broad hacking campaign that has breached U.S. agencies and a top cyber firm. *The Washington Post*. https://bit.ly/2M1s0oL

NATO. (2016). *NATO Summit Warsaw 2016*. https://www.nato.int/cps/en/natohq/events_132023.htm

O´Flaherty, K. (2020, January 6th). The Iran Cyber Warfare Threat: Everything You Need To Know. *Forbes*. https://www.forbes.com/sites/kateoflahertyuk/2020/01/06/the-iran-cyber-warfare-threat-everything-you-need-to-know/?sh=5181ac5d15aa

O´Regan, G. (2016). *Introduction to the History of Computing. A Computing History Primer*. Springer

Odobescu, V. (2014). *U.S. data thefts turn spotlight on Romania*. http://www.usatoday.com/story/news/world/2014/01/13/credit-card-hacking-romania/4456491/

Pike, J. (2018). North Korean Intelligence Agencies. *Federation of American Scientist*. https://fas.org/irp/world/dprk/

Ponemon Institute. (2014). *Exposing the cybersecurity cracks: A global perspective*: Part I: Deficient, disconnected & in the dark, Sponsored by Websense, Inc

Presidencia del Consejo de Ministros. (2012). *PeCERT ingresa a la comunidad internacional de CERT y es reconocido como CSIRT nacional para el capítulo Perú*. https://www.gobiernodigital.gob.pe/noticias/segdi_noticias_detalle.asp?pk_id_noticia=367

Press, G. (2017, July 18th). 6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry. *Forbes*. https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/?sh=76dd8a1420aa

Robertson, J., Lawrence, D., & Strohm, C. (2014). Sony's breach stretched from Thai hotel to Hollywood. http://www.bloomberg.com/news/2014-12-07/sony-s-darkseoul-breach-stretchedfrom-thai-hotel-to-hollywood.html

Roperts, N. (2008). *Transformación sistémica de conflictos: reflexiones acerca del conflicto y del proceso de paz en Sri Lanka. Berghof Research Center for Constructive Conflict Management*. https://www.berghof-foundation.org/fileadmin/redaktion/Publications/Handbook/Dialogue_Chapters/spanish_ropers_dialogue6_lead.pdf

Rushe, D. (2014, October 2nd). JP Morgan Chase reveals massive data breach affecting 76m households. *The Guardian*. https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach

Ryan, J. (2010). *A history of the Internet and the digital future*. Reaktion Books

Sanger, D., Perlroth. N. & Schmitt, E. (2020, December 14th). Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit. *The New York Times*. https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

Sarbah, A. & Otu-Nyarko, D. (2014). An overview of the design school of strategic management (strategy formulation as a process of conception). *Open Journal of Business and Management*, 2, pp. 231-249

Schneier, B. (2012). Securing medical research: A cybersecurity point of view. *Science*, 336 (6088), pp. 1527–1529

SEDENA. (2014). *Estudio prospectivo de la seguridad y defensa nacional al 2030. Lima*. https://es.calameo.com/read/00566600762a706c3e84f

Shamah, D. (2012, June 6th). Latest viruses could mean 'end of world as we know it,' says man who discovered Flame. *The Times of Israel*. https://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/

Siboni, G. & Kronenfeld, S. (2014, April 3rd). Developments in Iranian Cyber Warfare, 2013-2014. *Institute for National Security Studies*. https://www.inss.org.il/publication/developments-in-iranian-cyber-warfare-2013-2014/

Siegel, T. (2014, October 3rd). Ways to Protect Yourself After the JPMorgan Hacking. *The New York Times*. https://www.nytimes.com/2014/10/04/your-money/jpmorgan-chase-hack-ways-to-protect-yourself.html

Singer, P.W. & Friedman, A. (2013). *Cybersecurity and Cyberwar. What everyone needs to know*. Oxford University Press

Springer, P. (2015). *Cyber Warfare. A Reference Handbook*. ABC-CLIO

Stracqualursi, V. et al. (2020). Trump downplays massive cyber hack on government after Pompeo links attack to Russia. *CNN Politics*. Retrieved from https://edition.cnn.com/2020/12/19/politics/pompeo-us-government-hack-russia/index.html

Stubbs, J., Satter, R. & Menn, J. (2020, December 14th). U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack. *Reuters*. https://www.reuters.com/article/global-cyber-idUSKBN28O1Z3

US Department of Defense. (2019). *National Defense Strategy*. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Vilarino, D. (2018). When Bots Teach Themselves to Cheat. *Wired*. Retrieved from: https://www.wired.com/story/when-bots-teach-themselves-to-cheat/

Wang, Y. (2020, September 1st). In China, the 'Great Firewall' Is Changing a Generation. *Politico*. https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385

Weinberg, S. (2007, April 10th). How Israel Spoofed Syria's Air Defense System. *Wired*. https://www.wired.com/2007/10/how-israel-spoo/

Wheeler, D & Larsen, G. (2007). Techniques for Cyber Attack Attribution. Institute for Defense Analysis. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf

White, G. (2020, April 21st). Revealed: The man behind the first major computer virus pandemic. *Computer Weekly*. https://www.computerweekly.com/news/252481937/Revealed-The-man-behind-the-first-major-computer-virus-pandemic



EDITORIAL
NAVEGANTE