Diseño de la Aplicación Ciberseguridad y Ciberdefensa Como Estrategia Informativa Para Evitar Ataques Cibernéticos

Mayor (EJC) José Vicente Aranda Gómez

Especialización en Seguridad y Defensa Nacionales, Escuela Superior de Guerra “General Rafael Reyes Prieto”

PhD (C) Miguel Antonio González Martínez

7 octubre 2024

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) José Vicente Aranda Gómez
Identificación	**:**	91456604
Programa académico	**:**	Especialización en Seguridad y Defensa Nacionales
Tutor metodológico	**:**	PhD (C) Miguel Antonio González Martínez
Tutor temático	**:**	PhD (C) Miguel Antonio González Martínez
Fecha de entrega	**:**	07 de Octubre del 2024
Extensión	**:**	**5.548 palabras**

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este artículo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Resumen

Actualmente la información y la tecnología se encuentran sincronizadas, la población general tiene acceso a gran cantidad de información en tan solo unos segundos sin la limitación de la distancia física entre un país y otro; este flujo de información ha permitido una sociedad cada vez más globalizada que utiliza el ciberespacio para relacionarse, adquirir bienes, servicios, tener acceso a educación, entre otros; por tal motivo es crucial considerar los riesgos que enfrentan las personas al interactuar a través de dispositivos personales de comunicación en el ciberespacio. Esta revisión bibliográfica busca: examinar el estado actual de las estrategias de defensa empleadas en el uso cotidiano del ciberespacio, analizar las amenazas escondidas, determinar la eficacia de los programas y políticas que los países elaboran para hacerles frente.

Palabras clave: Ciberguerra, ciberseguridad, ciberdefensa, ciberespacio, ciberataques, estrategia, Estado.

Abstract: Currently, information and technology are synchronized; the general population has access to a large amount of information in just a few seconds without the limitation of physical distance between one country and another; This flow of information has allowed an increasingly globalized society that uses cyberspace to interact, acquire goods, services, have access to education, among others; For this reason, it is crucial to consider the risks that people face when interacting through personal communication devices in cyberspace. This bibliographic review seeks to: examine the current state of defense strategies used in the daily use of cyberspace, analyze hidden threats, determine the effectiveness of the programs and policies that countries develop to confront them.

Keywords: Cyberwar, cybersecurity, cyberdefense, cyberspace, cyberattacks, strategy, State.

Introducción

Comprender la ciberseguridad como un ámbito de la defensa de los Estados es crucial en el siglo XXI, el presente trabajo tiene como objetivo resaltar la importancia que tiene justamente la ciberseguridad y la ciberdefensa en un área clave de cualquier Estado: su infraestructura crítica enfocada en el sector financiero.

"Las tecnologías informáticas transforman nuestra manera de pensar y actuar en cualquier aspecto de nuestras vidas, introduciendo importantes cambios estructurales, al permitirnos modelar objetos de todo tipo en forma de información, permitiendo de este modo su manipulación por medios electrónicos" (Unión Internacional de Telecomunicaciones, ITU. 2007). Es por esta razón que el mundo es cada vez más dependiente de la tecnología, más puntualmente a la internet, lo cual, hace a los Estados más vulnerables a un ciberataque, que puede poner en jaque estructuras críticas de un Estado, ya sea en su parte militar y no menos importante, infraestructura que puede afectar directamente a la población civil sin necesidad de disparar una sola bala. (pag.3).

En este orden de ideas, se eligió como la aplicación de la ciberseguridad y ciberdefensa como estrategia informativa caso, para conocer la debida importancia que tiene la ciberdefensa de su infraestructura crítica, buscando explicar cómo es que surge una necesidad de cada uno de los Estados, frente a las nuevas posibles amenazas que vienen no solo de otros Estados con altas capacidades para realizar ciberataques sino también de parte de nuevos actores organizados en el sistema internacional que hoy por hoy son considerados como un tema clave en la agenda de seguridad de la mayoría de gobiernos a nivel mundial. Estos nuevos actores, son especialmente relevantes por sus capacidades de daño a larga distancia sin la posibilidad de un contraataque; a estos grupos a pesar de que se les ha intentado vincular con Estados (en casos

como por ejemplo grupos de Hackers vinculados con China, Rusia y Corea del Norte (Reuters, 2020; Semana (2020), son en su mayoría grupos independientes de hackers o piratas informáticos que actúan por su cuenta y que funcionan en el marco de la criminalidad e incluso algunos cuentan con un trasfondo político.

Ahora bien, a esto se le suma la idea de que en una era moderna la dependencia en redes de comunicaciones y dispositivos electrónicos interconectados y propensos a ser ciber atacados es tal, que un simple fallo o descuido en sus estructuras de defensa puede resultar en un acontecimiento catastrófico para una nación.

Metodología

El presente escrito, se fundamenta en un estudio cualitativo frente a la importancia que ha tenido para los Estados el construir capacidades de ciberseguridad y ciberdefensa, donde a partir del análisis de diversos autores, especialmente aquellos enfocados en fuentes secundarias como artículos y textos relacionados con el impacto de la ciberseguridad y ciberdefensa como estrategia informativa, así como un par de análisis de expertos frente a cómo debería ser la relación entre privados y el Estado; con esto se buscó construir un contexto general de ciberseguridad y ciberdefensa, ya que permite a través de él llegar a describir, de manera detallada, profunda y analítica la estructura, conformación y competencias.

Definición del tema de investigación

Según Sánchez, disponer de estructuras organizativas nacionales, regionales e internacionales, para fortalecer su ciberseguridad y luchar contra la ciberdelincuencia, En la década de los sesenta se concibe el fenómeno donde se le da importancia a la tecnología y a la información, se da el desarrollo de las telecomunicaciones. Desarrollo de diferentes herramientas tecnológicas que facilitarían las comunicaciones a nivel mundial, generando ventajas comparativas en aspectos económicos, políticos, sociales, etc.

Hallazgos

La supervivencia del Estado nación, entendida como la razón de Estado. Actualizándolo al siglo XXI, las variables a tener en cuenta para lograr esta supervivencia se actualizan a las nuevas tecnologías y especialmente a los nuevos teatros de operaciones donde resalta de manera clara el ciberespacio, comprendido de la manera como lo explica Maughan (2010) quien dice que: “cyberspace is the complex, dynamic, globally interconnected digital and information

infrastructure that underpins every facet of society and provides critical support for our personal communication, economy, civil infrastructure, public safety, and national security".

El primer punto para tener en cuenta es que como menciona Mearsheimer (2001), "the claim that security competition and war between the great powers have been purged from the international system is wrong. Indeed, there is much evidence that the promise of everlasting peace among the great powers was stillborn." (pág.25).

Lo planteado por Mearsheimer apunta que existe una competencia de seguridad y guerra entre los Estados, más específicamente entre los grandes poderes, una competencia que se traslapa al ciberespacio, y que impulsa a los Estados en una constante competencia de superioridad armamentística, que, para el caso, se reduce a capacidades de ataque y defensa orientadas a la infraestructura del Estado, que para el siglo XXI, se ve identificado como parte de sus redes informáticas y de comunicación.

Kating-Borland (2012) de la mano con lo que explica Mearsheimer dice que: A cyber-attack can occur at any time and may not always be associated with political or economic activities or any actual military operations. Additionally, because identity can be concealed so easily online, it is unlikely that the source of an attack will be readily apparent. (pág. 4).

En este orden de idea el ciberespacio se ha convertido en una prioridad de los Estados para proteger sus intereses y su integridad, Kating-Boland (2012) en su texto "Cyberwar: A Real and Growing Threat" incluso retoma una frase clave que menciona Ene Ergma, Speaker del parlamento estonio la cual reza que "Like nuclear radiation, cyberwar doesn't make you bleed, but it can destroy everything". (pág.6)

Esto presenta una idea de cuan real puede ser considerada esta situación, y como esta misma preocupación ha llevado a un escalamiento armamentístico y de defensa en cuestiones de ciberseguridad.

De esta forma, el ciberespacio puede ser considerado como un nuevo campo de guerra donde los Estados han venido construyendo nuevas capacidades de poder, sin embargo, a diferencia de otras situaciones de escalamiento similares, como por ejemplo la Guerra Fría, el desarrollo de capacidades en ciberseguridad y ciberdefensa no requieren de recursos físicos tan especializados como el caso del escalamiento nuclear a mediados del siglo XX; por supuesto requieren de recursos humanos y de un presupuesto considerable, cosa que es clara cuando se analizan las capacidades de "ciberguerra" que tienen grandes potencias como China o Rusia comparadas con las capacidades del resto de naciones.

Ahora bien, hay un segundo punto expuesto por Mearsheimer que funcionaría en cierto sentido para explicar cómo funciona la ciberdefensa actualmente, este es su concepción de la política internacional, para ello, este dice que:

> […] international politics has always been a ruthless and dangerous business, and it is likely to remain that way. Although the intensity of their competition waxes and wanes, great powers fear each other and always compete with each other for power. The overriding goal of each state is to maximize its share of world power, which means gaining power at the expense of other states." (Mearsheimer, 2001).

Lo que indica Mearsheimer, es que existe una competitividad que, aunque en cuestiones críticas aumenta y disminuye, sin embargo, fuera de estas situaciones sigue existiendo un "miedo" de unos frente a otros Estados y sus capacidades, que se traduce en una competencia de

poder donde cada Estado busca maximizar sus capacidades para protegerse de amenazas latentes y en cierta forma como un medio de participación en el poder mundial, proyectando influencia y especialmente capacidad de poder duro a otros Estados.

De la mano con Mearsheimer, Huth, Gelpi y Bennett (1993) presentan una serie de elementos claves que permiten comprender como el realismo estructural se enfoca en los atributos propios del sistema internacional y desde este este se puede explicar también el escalado de capacidades en ciberdefensa. Los autores mencionan que particularmente el realismo estructural hace énfasis en "resolver y relativizar las capacidades militares de los Estados adversarios", dando a entender que la construcción de capacidades se basa fuertemente en los atributos propios con los que cuenta el sistema internacional.

Los autores en su texto si bien presentan un análisis acerca de cómo el realismo estructural, de la, función para analizar el escalamiento de los conflictos entre Estados, ofrecen una serie de características importantes para comprender la visión y la estructural del sistema y permiten conectar estas ideas con el tema del escalamiento de capacidades militares y seguridad nacional.

Esta situación vista desde el enfoque de ciberseguridad y ciberdefensa se reflejaría primero en la premisa de la existencia de una asimetría en cuestión de capacidades frente a las grandes potencias respecto al resto del mundo, y esto se hace presente en la política disuasiva de las grandes potencias que entre ellas han dejado claro que la ciberguerra es una posibilidad y que están preparados para defenderse y para atacar, esta situación en particular es lo que impulsa a que todos los Estados contemplen la importancia de implementar capacidades propias en el área y a pesar de que no sean comparables con las de los Estados más grandes, entra en juego la descripción de la estructura del sistema, donde las alianzas y los patrones comportamentales

definirán qué tan amenazado se siente un Estado de otro, o incluso qué tan amenazado se siente un Estado de un actor internacional con ciertas capacidades ofensivas.

El mismo sistema, sin embargo, ha buscado proponer varias maneras de concebir al ciberespacio de manera equilibrada en cuanto a condiciones de capacidades para justamente evitar un escalamiento, pero ninguna se ha logrado imponer, ya que la importancia que han cobrado las estructuras de redes de comunicación e información al interior de los Estados yace en el núcleo de su defensa nacional, que es, a su vez, parte de lo que se consideraría su propia "razón de Estado. Por ello, el ciberespacio se sigue considerando un espacio anárquico sin unas regulaciones internacionales claras o establecidas frente a cómo proceder o a los límites o alcances que tiene cada Estado a la hora de construir infraestructura de defensa o contraataque cibernética, a esto se le suma el argumento de que existen nuevas amenazas no convencionales que no son necesariamente Estados, pero que representan un peligro latente a su infraestructura crítica.

Continuando con la idea, Mearsheimer argumenta que bien las grandes potencias siempre están buscando poder para convertirse en hegemonías o incluso para retar la existente, y para ello plantea 5 "bedrock assumptions" que permitirían explicar por qué llegan a ser "agresivos en la búsqueda del poder".

De estas 5 "assumptions" de Mearsheimer, se puede interpretar la construcción de, primero, una anarquía en el ciberespacio, donde nadie por encima de nadie puede decidir sobre normatividades o acciones agresivas de otros Estados en la misma idea que según Kello (2017) es más allá de condenarlos si es demostrada la culpabilidad, cuestión que se vuelve complicada debido al tipo de conflicto que la ciberguerra representa, la alternativa que queda es fortalecer sus propias capacidades. (pág.214)

Segundo, debido a que ningún Estado puede dar por sentada la actuación de otro o el uso de la fuerza de su parte, cada uno se ha preparado individualmente para enfrentar lo peor y precisamente para proteger sus propios intereses, traducido a ciberseguridad, esto se ve reflejado, de nuevo, en el crecimiento del interés tanto de las grandes potencias como de los demás Estados en sus políticas de ciberseguridad y ciberdefensa, mientras que los países más pequeños y menos desarrollados se ven replegados a adoptar las medidas que pueden en función en que consideran esto como una amenaza.

Discusión

Ciber-disuasión: Capacidades que previenen de ser atacado.

Por otra parte, Reardon & Choucri (2012) en Craig y Valeriano (2018) complementan esta perspectiva y la vinculan también con la teoría realista, e incluyen de nuevo el concepto de disuasión o "deterrence", pues mencionan que las teorías realistas de disuasión, gestión de crisis y conflictos pueden utilizarse para comprender si el ciberespacio se está estabilizando o desestabilizando, si las tecnologías cibernéticas serán una nueva fuente de conflicto o de paz, y si los estados participarán en carreras de armas cibernéticas.

En este orden de ideas, el análisis desde la perspectiva de la estrategia cobra aún más sentido para explicar las nuevas situaciones de ciber guerra. Craig y Valeriano (2018) cuentan además que, con la proliferación de la información de las tecnologías de la información y la comunicación, la ciberseguridad se ha convertido en un "tema de primer nivel" para policymakers, así como un tema relevante y de gran interés para académicos de las relaciones internacionales. Se hace evidente como el realismo ofrece herramientas para comprender el ciberespacio, inicialmente como un espacio anárquico, pero también como otro escenario de actuación de los Estados, el cual no tiene un mismo control como lo sería las intervenciones

militares o incluso económicas. Con todo ello, el realismo entonces ofrecería herramientas para considerar que la protección de la infraestructura crítica, cualquiera que fuese, de cualquier estado, va más allá de un sistema de gobernanza y es comprendida como una carrera individual por protegerse de otros Estados u actores con capacidades de incluso impedir el normal funcionamiento de otro Estado.

Resultados

Ahora bien, ahondando más profundamente en como la ciberseguridad y la ciberdefensa es un asunto propio de cada Estado. Gehem, Usanov, Frinking y Rademaker (2015) explican que las Estrategias Nacionales de Seguridad Cibernética (NCSS, por sus siglas en inglés) son un fenómeno nuevo, pues las primeras estrategias comenzaron a aparecer solo en los primeros años del siglo XXI. Estados Unidos fue uno de los primeros países en publicar una estrategia de este tipo en 2003. Demostrando claramente que la seguridad cibernética ya se ha convertido en una prioridad nacional.

Lo mencionado por estos entonces, deja claro que la ciberseguridad se ha convertido en una prioridad de seguridad nacional, sin embargo, según datos que retoman Gehem et al¸ de la European Network and Information Security Agency (ENISA), a 2015 solo se tenía conocimiento de 33 países que tenían aprobada una Estrategia Nacional de Ciber Seguridad o NCSS por sus siglas en inglés, así como solamente se conocía de 8 que tenían su NCSS en preparación.

Por otra parte, Bauer y Dutton (2015) explican que las razones para la existencia de estas medidas de protección yacen en la necesidad de combatir amenazas de todo tipo, pues argumentan que la amplia gama de problemas relacionados con asuntos de seguridad en el mundo en línea es grande y creciente, y se está volviendo cada vez más grave, aunque si destacan que se han realizado muchos esfuerzos a lo largo de los años para mejorar la ciberseguridad. (pág.2)

Los autores argumentan que esto se debe en parte a la creciente centralidad de Internet en el desarrollo económico y social, lo que la convierte en un objetivo más valioso, pero también se debe a la dinámica cambiante del problema, como el número creciente de usuarios que no solo

son vulnerables a amenazas de ciberseguridad, pero también cada vez más culpables incluso si no participan directamente en actividades malévolas en línea. (Bauer y Dutton, 2015)

El planteamiento de estos autores, apuntan a que justamente la "centralidad creciente" del internet en distintos ámbitos sociales, políticos, económicos y como relataba anteriormente militares, han llevado a que surja la necesidad de implementar medidas nuevas de protección frente a la creciente cantidad de atacantes y de diversas amenazas que se presentan. Ahora bien, Maughan (2010) presenta una aproximación frente a esta situación y a como los Estados deberían tomar el asunto de la seguridad, pues menciona que:

The U.S. and the world at large are currently at a significant decision point. We must continue to defend our existing systems and networks. At the same time, we must attempt to be ahead of our adversaries, and ensure future generations of technology will position us to better protect critical infrastructures and respond to attacks from adversaries.

En contraposición, el estudio "Does cybersecurity risk stifle corporate innovation activities" de Wang, Ho, y Shan (2024) ofrece una visión esencial acerca de cómo los peligros de ciberseguridad pueden impactar de manera adversa en la habilidad de las empresas para innovar. Este análisis meticulosamente realizado proporciona pruebas de que los riesgos cibernéticos funcionan como un obstáculo considerable para la innovación, particularmente en empresas con limitaciones financieras y las de sectores de alta tecnología y alto riesgo. Este descubrimiento es crucial para entender la dualidad de la ciberseguridad como un campo que requiere innovación pero que a su vez puede restringir dicha capacidad en el contexto empresarial.

Esta cita es contundente al afirmar que primero, se debe continuar construyendo defensas para las estructuras ya existentes a la vez que se asegura que en los próximos desarrollos estarán por encima de los rivales y que a su vez van a permitir proteger de mejor manera los diferentes

puntos críticos del Estado. Esto va por la misma línea con lo que se mencionaba anteriormente, donde primero se debe entender que el desarrollo de capacidades en ciberdefensa va de la mano de la agenda de cada Estado, que, a su vez, dependerá de si consideran o no que hay un nivel de riesgo suficiente para invertir en este tipo de capacidades, que representan un gasto importante en infraestructura y mano de obra capacitada.

Ahora bien, con todo esto es posible entrever que la agenda de la ciberseguridad en el Estado está presente debido a la alta sistematización, la alta dependencia del funcionamiento de puntos críticos del Estado y de la sociedad con las redes computarizadas, además de que como menciona Dutton: "the rapid adoption of mobile phones and devices, as well as the networking of an increasing number of objects in IoT, has further increased the number of attack points and expanded the footprint of cybercrime […]" (Orji 2012; Shalhoub & Al Qasimi, 2010 en Dutton 2012 pag. 3).

Lineamientos y Protocolos

El ciberespacio es un vasto, complejo y rápidamente cambiante de batalla. La clave para que prevalece en un entorno ciberespacio hostil puede estar en la capacidad de generar una imagen completa de ese ambiente como anteriormente se expuso. Hay tres clases de sistemas para la gestión de una postura defensiva, que se pueden clasificar por cuando operan en relación con un ataque: después, durante y antes.

Sistemas forenses ayudan a las organizaciones investigan los ataques después de que han ocurrido a entender tanto su impacto y sus causas profundas. El núcleo de estas soluciones es los registros históricos que registran la actividad en cada aspecto de la infraestructura, de software para dispositivos de red. Estos registros pueden ser analizados de forma manual para determinar la secuencia de los acontecimientos que han llevado a una intrusión o interrupción. Sin embargo,

el volumen y la complejidad de estos datos son enormes. Por lo tanto, las organizaciones ahora implementar sistemas de gestión de registros que recogen, almacenan y analizan los datos auto-ticamente (Shelly, Marchany, & Tront, 2010).

Estos sistemas se correlacionan información de múltiples sistemas para identificar patrones, y armar una línea de tiempo del incidente. Con esta información, las fuerzas armadas pueden remediar los problemas que permitieron la violación, e identificar, evaluar y tratar los daños causados basados en una consciencia situacional en un ámbito cibernético.

Es la conciencia situacional la principal ayuda a los esfuerzos para detectar y responder a un ataque en curso. Estos sistemas se basan en sensores y sistemas de detección de intrusos desplegados en toda la infraestructura para identificar comportamientos sospechosos, desviación de la normalidad, y elevar las alarmas. Una alarma se puede analizar de forma manual, pero una intrusión puede plantear demasiadas tales alarmas mientras se mueven a través de la infraestructura. Y el ordenamiento de un verdadero ataque del ruido de fondo normal de falsas alarmas es una tarea extremadamente compleja.

Para hacer frente a esto, los sistemas de información de seguridad y gestión de eventos se pueden implementar para recogen acontecimientos, analizarlos de forma a toda la infraestructura, e identificar dónde un evento denominado (exploit) que está ocurriendo en ese momento en el tiempo (Hathaway, 2009). Con información así obtenida, los equipos de respuesta a incidentes pueden tomar medidas para evitar la intrusión progresar más allá.

El último y más importante clase de sistemas de conciencia situacional está diseñado para funcionar antes de que comience un ataque, se centra en detener los atacantes antes de que obtengan entrada. Para ello, las defensas que bloquean el software malicioso y el acceso no autorizado son cruciales. Además, las normas de configuración de línea de base deben ser

establecidas y supervisadas para evitar la desviación y el incumplimiento que puede crear vulnerabilidades en el sistema. Esto requiere que los sistemas que identifican vulnerabilidades, errores de configuración, y otros riesgos en la infraestructura.

Al igual que los sistemas forenses y basadas en eventos, estos sistemas están equipados con componentes que evalúan los dispositivos individuales, tales como escáneres. (Sommer & Brown, 2011)

La vulnerabilidad y herramientas similares identificar un gran número de problemas de dispositivos posibles, la mayoría de las cuales están mitigados eficazmente por las arquitecturas de defensa en profundidad de seguridad. Soluciones de gestión de la postura de seguridad se pueden implementar que analizan las configuraciones y las vulnerabilidades de los diferentes dispositivos y hosts en toda la infraestructura, se correlacionan entre sí, e identificar los problemas de seguridad de todo el sistema que existen en la infraestructura. Con esta información, los responsables de la seguridad.

El hecho es que el anonimato, el alcance global, la naturaleza dispersa, y la interconexión de las redes de información continúan reduciendo la probabilidad de detección y descubrimiento del origen de un ataque, con lo que la atribución de un problema permanente. Los atacantes pueden utilizar cada vez más los medios de engaño, la mayoría de ellos ofrecen una negación plausible. Piratas informáticos inteligentes pueden ataques de ruta a través de países con los que el gobierno de la víctima mantiene relaciones diplomáticas pobres o sin la cooperación policial.

Pero incluso las investigaciones exitosas a menudo conducen solamente a otro equipo hackeado. Por lo tanto, los estados y los gobiernos todavía se enfrentan a la perspectiva de perder un conflicto cibernético sin conocer la identidad de su adversario.

Vacíos en la literatura

La exploración bibliográfica ha revelado varios vacíos en la literatura existente sobre la aplicación ciberseguridad y ciberdefensa como estrategia informativa para evitar ataques cibernéticos. Si bien ha habido un aumento en las publicaciones sobre estos temas en la última década, especialmente en el contexto de la ciberseguridad, todavía hay áreas que no han sido exploradas convenientemente, por tal razón la investigación sobre la integración de la seguridad tanto informática como del mismo Estado, es una total estrategia a pesar de que esta tecnología podría transformar, y seguir innovando y marcando siempre un antes y un después.

Conclusiones

Con lo investigado se encontró que primero, hay una creciente preocupación nacional como internacional respecto a los temas de ciberseguridad y ciberdefensa, que abarcan tanto los Estados en primera medida, pero también los privados y como innovación los más afectados son los sectores públicos debido al bajo nivel de seguridad que se maneja en diferentes entidades, esto se presenta como resultado de que hay actores con capacidades de atacar las redes y los sistemas con el riesgo de afectar de forma grave el funcionamiento incluso de una nación, así que esto posiciona al tema de ciberseguridad y ciberdefensa en las primeras posiciones de la agenda.

Se encontró también que a pesar de que el tema es una preocupación generalizada, no todos los Estados cuentan con las mismas capacidades tanto económicas como tecnológicas para invertir en el área de la ciberseguridad y la ciberdefensa, lo que ha llevado a que algunos Estados estén mejor preparado respecto a otros frente a estos ataques y amenazas, de la misma forma en que algunas naciones tienen una mayor inminencia a ser atacados debido a la importancia global que tienen, claro ejemplo son los Estados Unidos y aplicado al caso su sistema financiero.

Ahora para el caso colombiano, queda por decir que, efectivamente si existe una preocupación y se ha ejecutado una estrategia de ciberseguridad y ciberdefensa al interior del país pues en la medida en que se hizo evidente la tecnificación y la inclusión digital de la población, el Estado ha respondido preparándose frente a las amenazas del siglo XXI y específicamente en el marco de su sistema financiero de la mano con las empresas privadas se ha construido una estrategia de respuesta a las amenazas ya existentes y se consiguió formar un esquema de respuesta que se prepara para responder a las amenazas a gran escala que puedan afectar al país.

Es importante resaltar que específicamente en la construcción de capacidades para proteger el país y sus infraestructuras críticas el sector privado ha jugado un papel sumamente importante, pues son las capacidades individuales las que mitigan gran parte de los ataques que reciben, y a la vez alertan cualquier ataque o intentos.

Referencias

Aguilar, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO. Revista Latinoamericana de Estudios de Seguridad, (25). 24-40.

Benitez Manaut, R. (2019). El pensamiento militar de Clausewitz. *Revista Mexicana De Ciencias Políticas Y Sociales*, *32*(126).https://doi.org/10.22201/fcpys.2448492xe.1986.126.71848

Choucri, N.; Madrick, S., y Ferwerda, J. (2013). Institutional Foundations for Cyber Security: Current Responses and New Challenges. MIT. Massachusetts, EUA, 27.

Cybersecurity Ventures (2016). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Recuperado el 12 de enero de 2020 de: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Deibert, R. & Rohozinski, R. (2010). Beyond Denial: Introducing Next Generation Information Access Controls, en Deibert, R.; Palfrey, J.; Rohozinski, R. & Zittrain, J. (eds.) Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. MIT Press: Cambridge,3-13.

Edmunds, T. (2014). Complexity, strategy and the national interest. International Affairs, 525-539

Firdous, M. (2020). Cyber Warfare and Global Power Politics. CISS Insight Journal, 71-93.

GCI (2018). Global Cybersecurity Index. International Telecommunication Union. Recuperado el 12 de agosto de 2024 de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Gray, C. & Sloan, G. (1999). Geopolitics, Geography and Strategy. Routledge Taylor & Francis Group, Oxfordshire: United Kingdom, 298

Hackmageddon (2020). Cyber Attacks Statistics. Recuperado el 12 de agosto de 2024: https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

Hughes, R. (2010). A treaty for cyberspace. International Affairs,523-541.

Kapersky (2020). Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina. Recuperado el 12 de agosto 2024: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

Kello, L. (2017). The virtual weapon and international order. Reino Unido: Yale University Press, 320.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. International Security, 7-40.

Klimburg, A. (2012.). National Cyber Security Framework Manual. Tallinn; Estonia: NATO CCD COE Publication.

Kuehl, D.T. (2009). From Cyberspace to Cyberpower: Defining the Problem", en Kramer, F.; Starr, S.; Wentz, L. Cyberpower and National Security. Washington D.C.: National Defense University Press. 25-42.

Martín, P. (2015). Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos. Instituto Español de Estudios Estratégicos. Obtenido de: file:///C:/Users/USER/Downloads/Dialnet-InseguridadCiberneticaEnAmericaLatina-7686843.pdf

Moreno; J.; Albornoz, M., y Maqueo, M. (2020). Ciberseguridad en América Latina. Revista de Administración Pública INAP. Ciberseguridad Nacional.23-46.

NCSI (2019). National Cyber Security Index. E-Governance Academy, Recuperado el 12 de agosto de 2024 de: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

Newmeyer, P. (2015). Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal,9-19.

Nye, J. (2014). The regime complex for managing global cyber activities. Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 32

Nye, J. (2010). Cyber power. Harvard University, Cambridge MA Belfer Center for Science and International Affairs.

OEA & BID (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. 204 pag. Recuperado el 12 agosto de 2024 de: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

OEA (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. pág.186, Recuperado el 12 de agosto de 2024 de: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

OEA & BID (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? 193. Recuperado el 12 agosto de 2024 de:

https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

OEA/Symantec (2014). Tendencias de Seguridad Cibernética en América Latina y el Caribe. 100 págs. Recuperado el 12 de agosto de 2024 de: https://www.sites.oas.org/cyber/Es/Paginas/default.aspxPalfrey, J. (2010). Four Phases of Internet Regulation. Social Research, 981-996.

Samaan, J. (2010). Cyber command: The rift in US military cyber-strategy. The RUSI Journal,16-21.

Sheldon, J. (2012). "Deciphering Cyberpower: Strategic Purpose in Peace and War." Strategic Studies Quarterly, vol. 5, 95–112.

Sicherheitstacho (SF). Overview of Current Cyber Attacks. Deutsche Telekom. Recuperado el 12 de enero de 2021 de: https://www.sicherheitstacho.eu/start/main

Singer, P. y Friedman, A. (2014). Cyber Security and Cyber War. Oxford, Reino Unido: Oxford University Press, 321

Stanković, N. (2019). The conceptual analysis of identities and interests in the thought of Alexander Wendt. Politeia, 37-154.

Starr, S.H. (2009). Toward a preliminary theory of cyberpower, en Kramer, F.; Starr, S. & Wentz, L. Cyberpower and National Security. Washington D.C.: National Defense University Press, 43-88.

Take, I. (2012). Regulating the Internet infrastructure: A comparative appraisal of the legitimacy of ICANN, ITU, and the WSIS. Regulation & Governance, 499-523.

Van Creveld, M. (2002). The transformation of war revisited. Small Wars and Insurgencies, 3-15.

Van Creveld, M. (1991). The transformation of war: the most radical reinterpretation of armed conflict since Clausewitz. Washington D.C.: Free Press, 254

Wendt, A. (1994). Collective identity formation and the international state. American Political Science Review, 384-396.

Zittrain, J. & Palfrey, J. (2007). Access denied: the practice and policy of global Internet filtering. United Kingdom: Oxford Internet Institute, 80