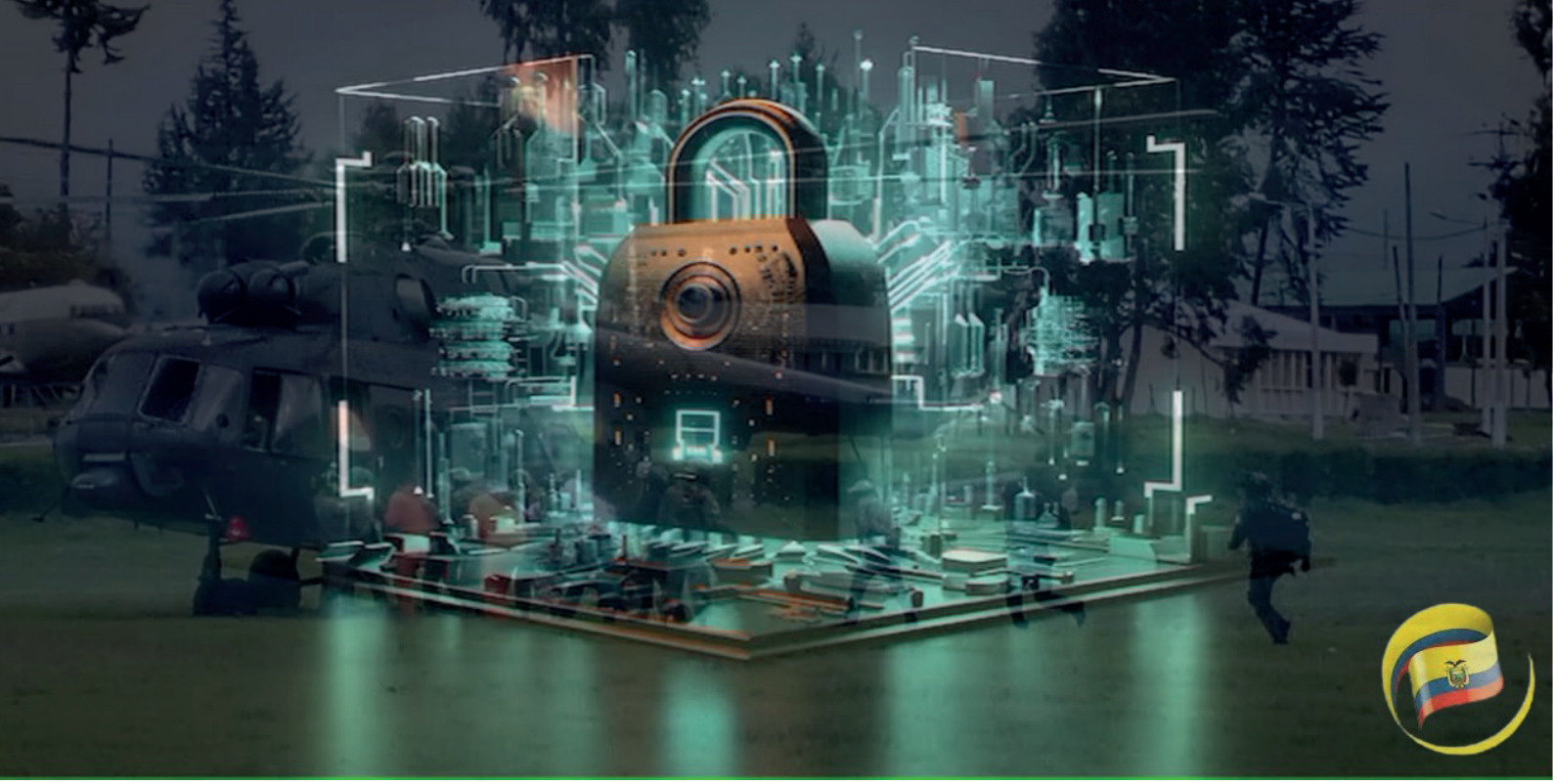


EL CIBERTERRORISMO Y LA SEGURIDAD NACIONAL

Tcrn. de E.M. Manolo Paredes Calderón [1]
Tcrn. de E.M. Ángelo Semanate [2]

Resumen

El artículo profundiza en tres aspectos claves sobre el ciberterrorismo: su origen, su evolución y las políticas y estrategias que actualmente dispone el Estado ecuatoriano para enfrentarlas. Para el efecto, analiza el modelo de madurez de ciberdefensa, propuesto por la Universidad de Oxford y reconocido mundialmente. Además, deja en evidencia que el terrorismo es un acto causado por organizaciones violentas y que sus formas de actuación se han situado fuertemente en el ciberespacio, generando movimientos económicos muy importantes, hechos que motivan a que cada día mucha gente acepte y se vincule a este accionar. Por otro lado, se presenta un breve resumen sobre la evolución del terrorismo y ciberterrorismo, luego de analizar las condiciones actuales, se demuestra la necesidad de trascender profundamente en las definiciones tradicionales, puesto que, el terrorismo de la actualidad no cumple con todas las características del terrorismo convencional, pero se acentúa en unas dos de ellas, tal vez las más tangibles e intolerables, como son el sembrar el temor y frenar el desarrollo de una sociedad, dado que a través de esta, se atenta contra la seguridad y existencia del Estado, y se alcanza el respeto social basado en el terror.

Palabras clave: ciberterrorismo, ciberseguridad, ciberdefensa, madurez de ciberseguridad.

Abstract

The article delves into three key aspects of cyberterrorism, its origin, its evolution and the policies and strategies that the Ecuadorian State currently has to confront them. For this purpose, it analyzes the globally recognized cyber defense maturity model. Furthermore, it makes it clear that terrorism is an act caused by violent organizations and that their forms of action have been strongly situated in cyberspace, generating very important economic movements, facts that motivate many people to accept and become linked to this activity every day. actuate. On the other hand, a brief summary of the evolution of terrorism and cyberterrorism is presented, and after analyzing the current conditions, the need to deeply transcend traditional definitions is demonstrated, since current terrorism does not comply with all the characteristics of conventional terrorism, but it is accentuated in two of them, perhaps the most tangible and intolerable, such as sowing fear and stopping the development of a society.

Keywords: cyberterrorism, cybersecurity, cyberdefense, cybersecutiry-maturity.

[1] Academia de Guerra del Ejército - Máster en Ciencias de Ingeniería Electrónica - dmparedes@espe.edu.ec
[2] Academia de Guerra del Ejército - Máster en Estrategia Militar Terrestre - angelosemanate@yahoo.es

DOI: https://doi.org/10.24133/AGE.VOL17.N01.2024.11
Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 17. Núm. 1, abril 2024. pp. 144 - 158

Introducción

Cuando se pretende hablar de terrorismo, es fundamental iniciar estratificando de forma adecuada los diferentes tipos de terrorismo que son comúnmente concebidos en el mundo y que los autores plantean como objeto de la investigación, puesto que, este es el punto de inflexión para abordar de forma cabal a este fenómeno. Más aún, si se desea abordar al terrorismo desde un enfoque social, político o de seguridad y defensa. Durante el presente artículo, se proveerá información puntual sobre los tipos de terrorismo, sus características, capacidades y motivaciones.

Una vez que se adopta la definición de terrorismo planteada por la Asamblea General de la ONU: "Actos delictivos concebidos o planeados para provocar un estado de terror en la población en general en un grupo de personas o en determinadas personas que son injustificables en todas las circunstancias, cualesquiera que sean las consideraciones políticas, filosóficas, ideológicas, raciales, étnicas, religiosas o de cualquier otra índole que se hagan valer para justificarlos" (Council of Europe, 2023), es preciso enmarcar que las acciones que realizan estos grupos sociales organizados son diversas, y que durante el presente artículo, se abordará de forma específica a una de ellas, como es el ciberterrorismo. Se analizará al ciberterrorismo en el Ecuador y las capacidades que tiene el Estado para evitar la proliferación de estas acciones ilegales.

En el contexto del ciberterrorismo que se ha evidenciado en el Ecuador, se analizará también en el estudio de la infraestructura crítica del estado, bajo la consideración de que, en las últimas décadas, la vertiginosa evolución de las tecnologías de información y comunicación han dado paso al surgimiento de una serie de actividades ilegales, las cuales emplean las plataformas digitales y tecnologías disponibles para fortalecer o incrementar sus accionares ilícitos, lo cual ha ido tornando cada vez más inútil a la capacidad del Estado, pues estos accionares se traslapan en medio de la legalidad.

Por tanto, el objetivo principal de la investigación es determinar la sinergia de la estrategia de ciberseguridad del Estado y la guía de la ciberdefensa para minimizar el impacto del ciberterrorismo, así como también, proporcionar información útil para esclarecer la zona gris en la que se encuentra la nación, al intentar definir de forma puntual, la infraestructura crítica que debe proteger el Estado, de tal forma que se puedan establecer roles y responsabilidades para una defensa efectiva de este componente fundamental para la vida y desarrollo del país.

Dos son las hipótesis que han orientado esta investigación: la primera sostiene que el ciberterrorismo explota las limitadas capacidades de los países más débiles para incrementar sus actividades ilícitas en ellos. De esta forma, los vuelve aún más vulnerables, de tal forma que no existirán gobiernos capaces de enfrentar y erradicar el terrorismo. Por tanto, al ser el ciberespacio uno de los dominios de acción del terrorismo, el Estado debe actuar de forma proactiva en la defensa y seguridad de este. Para lo cual, es pertinente determinar el nivel de madurez cibernética del Estado, y esto es posible hacerlo a partir del estudio de la estrategia de ciberseguridad y la guía de ciberdefensa y la operacionalización efectiva de las mismas.

La segunda hipótesis de la investigación refiere que el ciberterrorismo es una forma de terrorismo y que incrementará potencialmente su accionar en el ciberespacio, puesto que, este dominio le garantiza una comunicación rápida y subrepticia, a través de la cual, continuará perpetrando sus actos ilícitos e incrementando su legitimidad en la ciudadanía, sin la necesidad de un mayor desgaste logístico ni la necesidad de enfrentar físicamente al poder de control estatal.

Por otro lado, una vez que se han determinado las capacidades actuales y futuras del terrorismo, así como también, la madurez cibernética que ha alcanzado el Ecuador; la investigación realiza una propuesta que se enfoca en el adecuado levantamiento de la infraestructura crítica del país, debido a la importancia que esta significa para la vida y desarrollo de la nación.

Para el efecto, la investigación se desarrolló desde un enfoque cualitativo y deductivo, el cual determina y mide capacidades de ciberdefensa del Ecuador, a partir de un modelo internacional ampliamente aceptado, para posteriormente analizar la proliferación del ciberterrorismo y proponer posibles soluciones para enfrentar esta amenaza.

Por tanto, se pone a consideración de los lectores, un artículo que presenta información relevante para el presente y futuro del país, la cual es ampliamente explicada a partir de la Sección I, en la que se aborda la evolución del terrorismo y ciberterrorismo en el mundo. Seguidamente, la Sección II hace referencia a los modelos de determinación de la madurez de ciberseguridad de una nación. En la Sección III se presenta una propuesta de levantamiento de infraestructura crítica del Estado; y finalmente, se exponen las conclusiones y recomendaciones determinadas luego de la investigación.

1. LA EVOLUCIÓN DEL TERRORISMO Y CIBERTERRORISMO

1.1. El terrorismo

Sin duda, en las últimas décadas, la población mundial refiere al terrorismo como una actividad criminal que está en auge, y cuya máxima expresión de poder se perpetró en el ataque a las Torres Gemelas ocurrido el 11 de septiembre del 2001. Sin embargo, como lo refiere (Laqueur, 2003), el terrorismo es un fenómeno que data de más de dos siglos, puesto que, tanto el terrorismo como la guerra de guerrillas, son

consideradas como guerras asimétricas que han estado presentes desde la época contemporánea, donde resaltan historias como la de Cachemira, Argelia, SriLanka, Colombia, Los Balcanes, entre otras.

El terrorismo es un término que ha generado una serie de definiciones, condición que ha llevado a que incluso en la actualidad, no ha sido posible amalgamar las ideas en un único concepto; sin embargo, conforme lo señala (Bueza, F., 2022), sea cual fueren las formas o tipos de terrorismo, cada país lo coloca en su código penal sobre la base de su realidad, incluso, las formas de terrorismo también pueden variar significativamente, lo que obliga a que periódicamente se evalúen estos conceptos. Para establecer un corolario sobre lo que tradicionalmente ha sido un sinónimo o un reflejo del terrorismo, seguidamente se presentan algunos rasgos característicos señalados por (Bueza, F., 2022):

1. Utilizan la violencia como su forma típica de actuación, discuten el legítimo monopolio de la violencia. Es una forma de violencia clandestina, no controlan un territorio específico.
2. Es una forma de violencia clandestina.
3. Persiguen un objetivo preferentemente político; sin embargo, también pueden tener objetivos religiosos, nacionalistas, de extrema derecha o izquierda.
4. Buscan generar miedo por parte de sus enemigos y admiración de sus seguidores.
5. Requieren un alto nivel de propaganda.

Al analizar la evolución del terrorismo, y acorde al objeto de la presente investigación, es importante citar la filosofía de clasificación del terrorismo referida por Rodríguez (2012) y expuesta en la Tabla 1, la cual muestra una perspectiva comúnmente aceptada sobre el accionar terrorista en el mundo, y que ha sido validada y adoptada por todos los organismos internacionales. Además, para Rapoport (2004) el terrorismo nace en el primer siglo de la historia humana; sin embargo, los historiadores refieren cuatro olas de surgimiento y resurgimiento del terrorismo, las cuales se detallan a continuación, (a pesar de que la ola de violencia marcada por el crimen organizado en las últimas décadas, también podría ser categorizada en una oleada de una nueva forma de terrorismo):

- Rusia zarsista en 1880.
- Anticolonialismo en 1917.
- Izquierda nacionalista, 1968.
- Integrismos religiosos, 1980.

A partir de la clasificación de los tipos de terrorismos publicada por Rodríguez (2012), los escenarios actuales dan cabida a un nuevo tipo de terrorismo, como es el ciberterrorismo, puesto que a diferencia de la clasificación anterior el ciberterrorismo no conoce de fronteras, y emplea una dimensión especial, como lo es el ciberespacio, para perpetrar sus actos. Por tanto, esta forma de terrorismo no requiere la presencia física de un grupo de personas, o tampoco el empleo de armas de fuego; sin embargo, su impacto y consecuencia puede ser de igual o mayor magnitud al que podría alcanzar un acto terrorista convencional.

Tabla 1

Tipos de terrorismo acorde a la ubicación geográfica

Variable de análisis	Tipos de terrorismo	
	Local o regional	**Global e internacional**
Evolución histórica	Muy común en la época de la guerra fría	Muy común en la actualidad
Límites geográficos	El espacio geográfico	No se limitan a un espacio geográfico específico
Enemigo	Existe un enemigo claramente definido, circunscrito en un espacio geográfico	El enemigo es el mundo pro occidente, indiferente de su ubicación geográfica.
Objetivos	Definidos con elevada precisión y ajustados a su espacio geográfico	Objetivos no son rigurosamente selectivos
Tipo de armas	Armas de fuego convencionales con capacidades comunes	Diversas, no observan límites para su uso

Nota. Elaborado por los autores, sobre la base de lo expresado por Rodríguez (2012) y Laqueur (2003).

Entonces, esto implica que la responsabilidad y compromiso de un Estado legalmente constituido es cada vez mayor, puesto que debe garantizar el ambiente de paz y desarrollo que demandan sus ciudadanos, siendo fundamental actuar de forma oportuna y contundente ante las amenazas que emergen y evolucionan de forma dinámica.

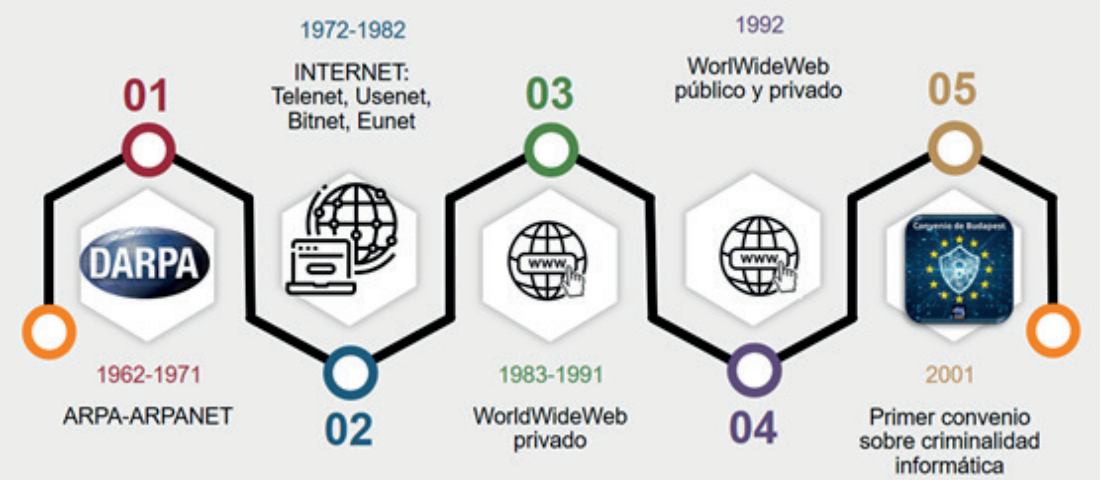
1.2. El ciberterrorismo

Para hablar del ciberterrorismo, es substancial establecer ciertas precisiones que permitirán delimitar y comprender su concepto, definición, filosofía, alcance y fines que persigue este tipo de accionar delictivo. Para el efecto, es fundamental un análisis explicativo e inductivo para conocer la evolución del internet y de las tecnologías de la información y comunicación, y comprender cómo este ha permitido el aparecimiento del ciberespacio y el ciberterrorismo.

A partir de estas definiciones, se podrá esclarecer la capacidad del ciberterrorismo y comprender por qué este accionar se convierte en una amenaza para la seguridad de cualquier Estado, al igual que comprender la importancia de la existencia de políticas y estrategias estatales que deben ser evaluadas e innovadas permanentemente, puesto que la evolución del internet, de las tecnologías de información y comunicación y de otros ámbitos tecnológicos, no se detiene en ningún instante y mantiene una dinámica altamente peligrosa para la convivencia pacífica y desarrollo de las naciones.

En este contexto, resulta relevante conocer la vertiginosa evolución del Internet. Según la Internet Society (2023), los primeros escritos sobre Internet fueron presentados en 1962 por el catedrático del Instituto Tecnológico de Massachusetts, J. Licklider, quien denominó a la capacidad de interconexión de computadores como una "red galáctica". En 1966 aparece el proyecto ARPANET, como parte del portafolio de proyectos de la agencia de investigación avanzada del Departamento de Seguridad de los Estados Unidos de América Investigación Avanzada (DARPA); y es la primera vez que se definen los conceptos de redes informáticas. En 1972 nace un proyecto que daba continuidad a ARPANET, el cual se lo denominó "internetting". En 1985, el Internet brindaba mucha facilidad para el desarrollo de investigaciones y comunicaciones entre ciertas comunidades privadas, quienes usaban las redes BITNET y USENET. En 1991 se funda la Internet Society y se inicia la comercialización del Internet. Finalmente, en 2006, la Organización Internacional de las Telecomunicaciones (ITU), declara al 17 de mayo como el día de las telecomunicaciones y sociedad de la información (ITU, 2023), y a esa fecha se luchaba por combatir los crímenes informáticos que aparecieron desde el 2001. Esta cronología es expuesta en la Figura 1.

Figura 1
Evolución del internet y las TICs



Nota. Elaborado por los autores. Nótese que, a pesar de que los esfuerzos por controlar los delitos en Internet se iniciaron en los años 90, no fue hasta la firma del Convenio de Budapest, en el 2001, que se inicia un tratamiento internacional de la ciberdelincuencia.

Así mismo, se trae al análisis la definición referida por el Consejo de Seguridad Europeo, que cataloga al ciberterrorismo como el uso de las TICs por parte de las organizaciones terroristas, cuyos fines son la intimidación, extorsión y coacción a la sociedad, todo esto motivado pro fines religiosos o políticos. Esta definición planteada por García y Sigmman (2017) también despierta ciertas alertas referentes a la seguridad del Estado, debido a que el ciberterrorismo se

desarrolla en espacios cuyo monitoreo y control estatal se convierte en algo altamente complejo. De igual forma, Bany Collin, a finales del siglo XX señaló que el ciberterrorismo es la convergencia del ciberespacio con el terrorismo (Masana, 2002).

En el ámbito del Internet y del ciberespacio, esta evolución de actos ilícitos que han escalado hasta la denominación de crímenes cibernéticos y ciberterrorismo ha evidenciado que las ventajas que ofrecen las tecnologías de la información y comunicación son cada vez más útiles para estos fines. En la actualidad afloran nuevas formas de terrorismo, vinculadas al crimen organizado y al narcotráfico; y que al igual que otros actos ilegales que se realizan en la world wide web[1] generan un impacto negativo en la sociedad, pues es algo muy rentable para quienes se involucran, conforme lo muestra la Tabla 2.

Tabla 2

Análisis de las actividades ilegales en el Internet

	Actividades	Transacciones
Caso silkroad (Prego, 2023)	- Venta de armas, droga y veneno - Sicariato - Servicios de piratería	Para el 2013: 1 millón de dólares y un decomiso de bitcoins por 3,6 millones de dólares
Darkweb (Cueto, 2023)	- Venta de droga - Servicios de fraude - Información bancaria	2022: 1.500 millones de dólares
Darkweb: productos y servicios más demandados (Wahnon, 2023)	- Lavado de dinero y criptomonedas - Servicios de fraude - Información bancaria - Venta de virus	2023: 8.000 millones de dólares
Darkweb: La tercera economía más grande del mundo (Villanueva, 2023)	- Servicios de ataques informáticos - Servicios de fraude - Información bancaria - Seguimiento de cuentas de redes sociales	2023: 8 billones de dólares

Nota. Es muy importante precisar que el ciberterrorismo es una forma de actuar del terrorismo, y que para el efecto emplean el ciberespacio, en el cual, el internet más oculto (deepweb, darknet y darwkweb)[2] brindan las facilidades propicias para que, a través de la venta de armas y droga, el terrorismo siga incrementando sus tentáculos y sus capacidades de acción.

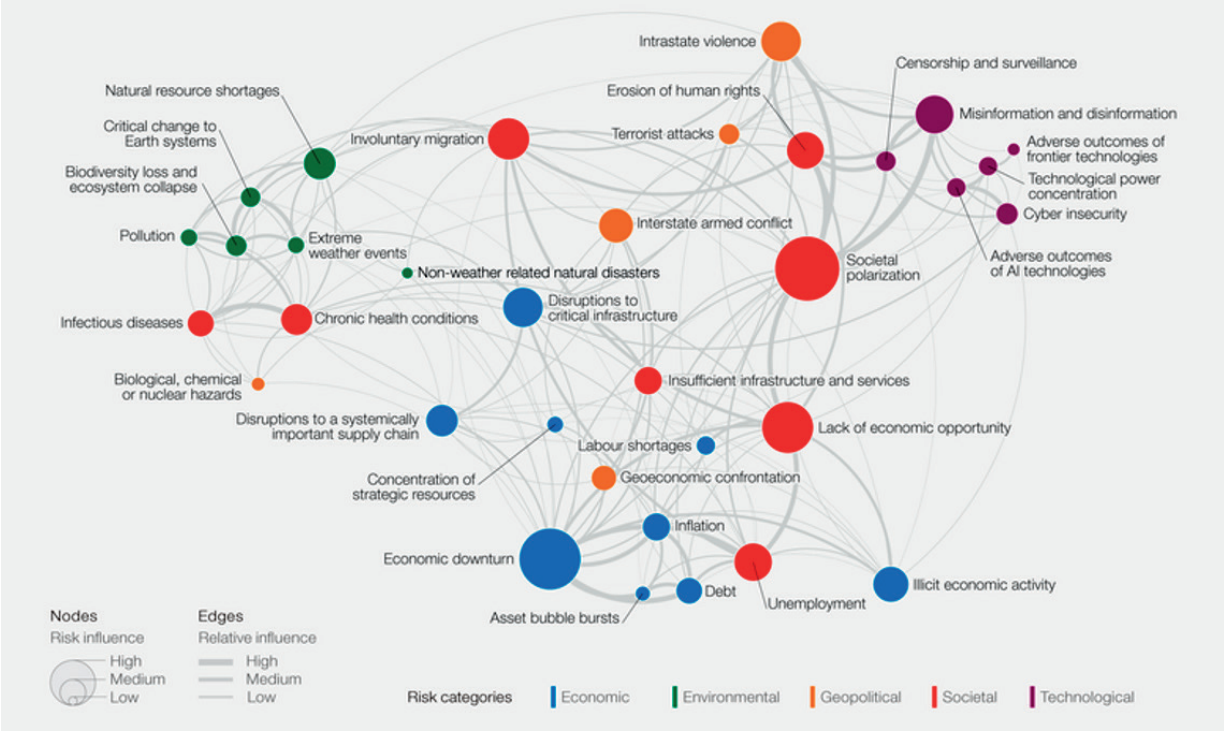
Continuando el análisis de esta vinculación del terrorismo al crimen organizado y al narcotráfico, resulta atractivo conocer lo mencionado por García y Sigmman (2017) al referir lo mencionado por el Observatorio de la Unión Europea de Drogas y Toxicomanías, destacando que en el 2016 se comercializaban 2 mil millones de euros mensuales, producto de la venta de drogas ilegales, especialmente en el ámbito del micro tráfico. Por tanto, este flujo económico fortalece al terrorismo y al ciberterrorismo. Nótese que, debido a las facilidades que ofrece el espacio cibernético, estas acciones que atemorizan, aterrorizan y causan daños físicos y económicos en la población, tendrá un crecimiento exponencial, incontrolado y altamente temerario; debido a que cuentan con la plataforma tecnológica disponible y gratuita, cuentan con dinero físico-electrónico e incrementan con gran facilidad el número de personas adeptas al cometimiento de estos ilícitos.

[1] La World Wide Web —comúnmente conocida como WWW, W3, o la Web— es un sistema interconectado de páginas web públicas accesibles a través de Internet. La Web no es lo mismo que el Internet: la Web es una de las muchas aplicaciones construidas sobre Internet (MDN web docs, 2023).

[2] https://www.xataka.com/servicios/deep-web-dark-web-darknet-diferencias

Esta evolución ha sido cuidadosamente analizada por el Foro de Davos, cuyos informes sobre riesgos globales de los últimos cinco años dejan en evidencia la importancia y relevancia que viene tomando el ciberterrorismo en el escenario actual. Es así como luego de la pandemia, los ciberataques y el ciberterrorismo ha tomado mayor importancia en estos reportes. En el reporte 2024, conforme lo ilustra la Figura 2, si bien es cierto que no se menciona taxativamente al ciberterrorismo, existe una fuerte relación entre los ataques terroristas, el crimen organizado en el espacio cibernético, las armas de destrucción masiva, la erosión-cohesión social, la desinformación, la pérdida de información y el colapso de un Estado.

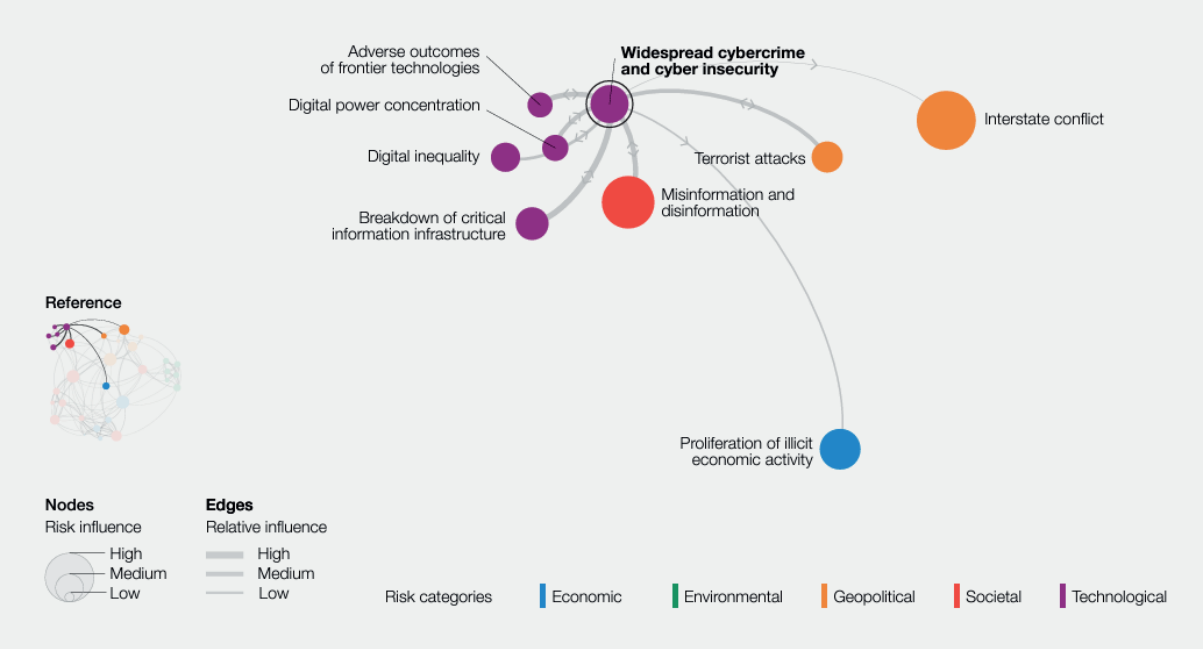
Figura 2
Riesgos globales 2024



Nota. Tomado de (WorldEconomicForum, 2023).

Seguidamente, la Figura 3 expone de forma específica las interconexiones que alimentan los riesgos cibernéticos y que generan un espacio de control debilitado de los Estados, a través del cual se realizan crímenes cibernéticos que pueden llegar a escalar hasta acciones de ciberterrorismo. Nótese que las tecnologías de vanguardia no sólo generan bienestar y progreso, sino también, cuando estas son mal utilizadas, pueden causar daños a la población. Así mismo, los monopolios digitales, la falta de equidad en el acceso a la digitalización segura y las vulnerabilidades existentes en la infraestructura crítica son ventanas abiertas para el cibercrimen y la inseguridad cibernética. Por tanto, es responsabilidad del Estado, establecer las políticas y normativas internas, que permitan alcanzar los más altos niveles de seguridad para su infraestructura crítica; y de esta forma, ser más resilientes a las acciones ciberterroristas.

Figura 3
Interconexiones que provocan los riesgos cibernéticos



Nota. Tomado de (WorldEconomicForum, 2023).

Si bien es cierto, comúnmente se piensa en que el terrorismo son acciones ejecutadas por un grupo terrorista en contra de uno o varios objetivos previamente definidos; el ciberterrorismo tiene varias particularidades que se originan en una generalidad, que es el Internet. Por tanto, si algún Estado, institución o persona, no se siente blanco de ciberterrorismo, deben estar muy conscientes que, al ser usuarios de Internet, automáticamente incrementan la probabilidad de tornarse en un auditorio objetivo para la ejecución de ataques cibernéticos que causen daños de gran magnitud a la población. Es por esto que el Ecuador, a pesar de no tener una historia muy nutrida en el ámbito de ciberterrorismo, el hecho de usar el Internet y de conocer que el entorno digital es cada vez más neurálgico en la vida cotidiana, lo convierte en un posible blanco; y por tanto, debe ser preventivo y proactivo en este ámbito.

La historia mundial en el ámbito del ciberterrorismo relata hechos como: el hacktivismo, el primer bloqueo virtual a gran escala, el contraataque del pentágono, los ciberataques en Kosovo, el avión espía o el evento Young intelligent hackers against terror (YIHAT). Los cuales reflejan la capacidad y el daño que se puede causar en la población a través de la consecución de actos de ciberterrorismo. Es así como las FARC de Colombia, los ETA de España, los Hacktivistas proetarra o el grupo IRA, también han mostrado que rasgos terroristas pueden ser llevados a cabo a través del espacio cibernético (Masana, 2002).

2. LA CIBERSEGURIDAD, UNA FORMA DE ENFRENTAR AL CIBERTERRORISMO

2.1. La Ciberseguridad en la actualidad

Para la ITU, la ciberseguridad es la suma de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos seguros y tecnologías que se emplean para proteger activos de la organización y los usuarios del ciberespacio, de tal forma que se garantice la seguridad de los activos de la información a través de la disponibilidad, integridad y confidencialidad (Recomendación ITU-T X.1205, 2008). Y para evaluar los niveles de ciberseguridad, analizan los siguientes parámetros: marco legal, marco técnico, organización, creación de capacidad y cooperación.

El Ranking global de ciberseguridad publicado por la ITU, es un índice que analiza el nivel de compromiso de los diferentes Estados con la ciberseguridad mundial, y ratifica la necesidad de orientar esfuerzos conjuntos, cooperativos y colaborativos, puesto que poco o nada ayudan los esfuerzos individuales. Para el año 2024, según el Ministerio de Telecomunicaciones del Ecuador, se tiene como meta alcanzar una puntuación de 51,3%, es decir, duplicar la puntuación actual (MINTEL, 2023), la cual, según el último informe disponible (ITU, 2021), refleja el siguiente ranking respecto de la ciberseguridad:

- A nivel mundial, los países más seguros, según este ranking difundido por la ITU, son:

1. Estados Unidos, alcanzando el 100% como país mejor puntuado
2. Reino Unido
3. Arabia Saudita
4. Estonia
5. Korea del Sur
6. Singapur
7. España
8. Rusia
9. Emiratos Árabes
10. Malasia

- En América Latina, los países han alcanzado los puntajes detallados, lo cual se ubica en el siguiente orden: desde el país con mayor índice de ciberseguridad hasta el país con menor índice de ciberseguridad. En este sentido, el Ecuador se ubica como el país con menor índice de ciberseguridad de la región, y en la parte baja del tercer cuartil a nivel mundial:

1. Brasil (96.6%)
2. México (81.68%)
3. Uruguay (75,15%)
4. República Dominicana (75.05%)
5. Chile (68,83%)
6. Costa Rica (67.45%)
7. Colombia (63,72%)
8. Cuba (58,76%)
9. Paraguay (57,09%)
10. Perú (55,67%)
11. Argentina (50,12%)
12. Venezuela (27,06%)
13. Ecuador (26,3%)

Otro dato importante a nivel mundial es el detalle de prioridades que los Estados e industria han definido en el ámbito de la ciberseguridad, en el cual se observa que la nube (cloud), para el 2023, pasó a ser la prioridad número 1, a diferencia de la posición 3 que alcanzó en el 2021. Seguido del análisis de datos, la automatización industrial, la inteligencia artificial y la tecnología 5G (Deloitte, 2023).

2.2. El modelo de madurez de capacidades de ciberdefensa (CMM) para las naciones

El Centro de Capacidades de Ciberseguridad Global, como parte de sus objetivos y sobre la base de la experiencia académica y científica alcanzada, emite un modelo construido con elevada rigurosidad científica, denominado el Modelo de Madurez de Capacidades de Ciberseguridad para Naciones (CMM, por sus siglas en inglés), mismo que tiene como objetivo fundamental el fortalecimiento de la capacidad de ciberseguridad de los diferentes países, pero que inicialmente, en el 2014, se tomó como base la experimentación realizada en 11 países (GCSCC, 2016). Para fines de esta investigación, el modelo de madurez será considerado como la base de análisis, medición y referencia para conocer la realidad del Ecuador en este ámbito, por lo que, la Figura 4 expone las dimensiones sobre las cuales se fundamenta el modelo.

Figura 4

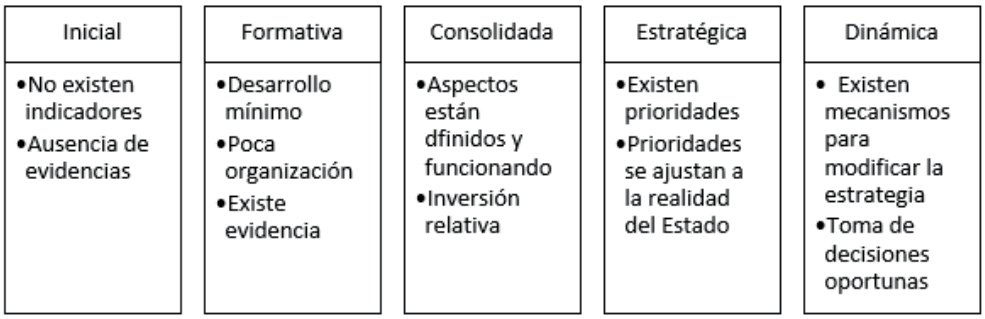
Dimensiones de análisis y medición del modelo de madurez

Nota. Tomado de (Global Cyber Security Capacity Centre, 2016).

Profundizando en el análisis del modelo, cada una de las dimensiones se fundamenta en factores de análisis, los cuales se alimentan de la medición realizada a 5 momentos (inicial, formativa, consolidada, estratégica y dinámica) y en cada uno de estos momentos se determinan los respectivos indicadores. Esta estructura se expone en la Figura 5 y permite disminuir el grado de subjetividad en el momento de evaluar el desarrollo de estas importantes capacidades.

Figura 5

Filosofía para la definición de indicadores en los diferentes aspectos que forman parte de las dimensiones del CMM



Nota. Tomado de (GCSCC, 2016).

Contextualizando en términos generales las dimensiones del modelo CMM, se pueden destacar los factores y aspectos que alimentan la medición de cada una de sus dimensiones, y a través de qué indicadores son evaluadas las mismas. Cada una de las dimensiones dispone de una rúbrica para la evaluación, conforme lo especifica GCSCC (2016) (Global Cyber Security Capacity Centre, 2016), la cual es aplicada a la estructura que se detalla en la Tabla 2 de la siguiente sección, en la cual se establecen ciertas mediciones para la realidad ecuatoriana.

3. LA CONCEPCIÓN DE CIBERSEGURIDAD Y CIBERDEFENSA DEL ECUADOR

La seguridad de un Estado se centra en fortalecer las estrategias y formas necesarias para responder por el estricto respeto de los derechos humanos, como es el caso del respeto al derecho a vivir sin violencia y criminalidad; es así como la seguridad se ha convertido en un concepto multifacético que abarca aspectos militares, económicos, sociales y tecnológicos. En la era actual, es por demás acertada la concepción de seguridad como la capacidad de adaptarse a amenazas cambiantes y mantener la estabilidad interna de la sociedad. En este sentido, los Estados deben adoptar enfoques holísticos que articulen esfuerzos orientados al establecimiento de un marco legal que fortalezca las acciones de las instituciones del Estado.

El artículo 2 de la Ley de Seguridad Pública y del Estado (LSPE), en el ámbito de la ley establece: *"La implementación de políticas, planes, estrategias y acciones oportunas para garantizar la soberanía e integridad territorial, la seguridad de las personas, comunidades, pueblos, nacionalidades y colectivos, e instituciones la convivencia ciudadana de una manera integral, multidimensional, permanente, la complementariedad entre lo público y lo privado, la iniciativa y aporte ciudadanos, y se establecerán estrategias de prevención para tiempos de crisis o grave conmoción social..."*.

De igual manera, el objetivo primero del Plan Específico de Defensa Nacional 2019-2030 señala: "(…) El Estado participará activamente en el control efectivo del territorio nacional (espacios terrestres, marítimos, aéreos y el ciberespacio) impulsando el desarrollo de políticas y estrategias para la ciberseguridad, ciberdefensa y defensa aeroespacial, permitiendo que estas se encuentren en las mejores condiciones para afrontar las amenazas y riesgos que atenten a la paz y seguridad".

Bajo este contexto, la concepción de la seguridad del Estado ecuatoriano tiene un enfoque multidominio, encaminado a desarrollar actividades dirigidas a proteger el ciberespacio, lo que conlleva a incrementar medidas de seguridad de las instituciones gubernamentales y sectores estratégicos relacionados especialmente a centros tecnológicos ante el acaecimiento de nuevas amenazas y el control del ciberespacio. El Ecuador tiene la obligación de establecer políticas públicas para contrarrestar las ciberamenazas, ciberataques, salvaguardar la infraestructura crítica digital, los servicios esenciales del Estado, la infraestructura crítica digital (ICD) de defensa y determinar los instrumentos estratégicos de la ciberseguridad y ciberdefensa.

3.1. La Política y la Estrategia Nacional de ciberseguridad del Ecuador

Ante las expectativas de conseguir la supremacía del ciberespacio, diversos actores se han convertido en luchadores permanentes por conseguir el control y dominio del ciberespacio, lo que ha creado un nuevo escenario de confrontación digital, donde los delincuentes informáticos batallan por la hegemonía tecnológica, generando grandes ataques cibernéticos en pos del robo y/o destrucción de la información. Ante esta situación, los Estados en todo el mundo han orientado sus esfuerzos para implementar estrategias de ciberseguridad, buscando mantener un adecuado sistema de seguridad informática.

Por lo expuesto, se puede afirmar que el Ecuador asume el desafío de desarrollar planes tecnológicos orientados al fortalecimiento de las capacidades de seguridad del ciberespacio. En este sentido, con Registro Oficial, Suplemento 557 de 17 de abril de 2002, se expide la Ley de comercio electrónico, firmas electrónicas y mensajes de datos, con el objetivo de *"Regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas".*

Los nuevos escenarios exigen a los Estados desarrollar políticas, reglamentos y maniobras claras para alcanzar horizontes óptimos de vigilancia del ciberespacio. Bajo este contexto, el Ecuador en el 2013 expide el primer esquema gubernamental de seguridad de la información (EGSI) basado en la norma ISO 27001:2013, por la Secretaría Nacional de la Administración Pública (SNAP) que buscaba "Brindar seguridad en el uso de internet a los usuarios, y tenía como objetivo implementar controles para garantizar la confidencialidad, integridad y disponibilidad de la información que se gestionan en las instituciones de Estado".

Con resolución ST-2014-0247 del 18 de julio de 2014, se aprobó la creación del Centro de Respuesta a Incidentes informáticos EcuCERT[1] de la Agencia de Regulación de las Telecomunicaciones (ARCOTEL), cuya finalidad es "Brindar a la comunidad el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, capacitación y soporte técnico" (ARCOTEL, 2017). El EcuCERT para mantener las relaciones con organismos internacionales, en el 2017 renovó su membrecía con el Foro de Respuestas a Incidentes y Equipos de Seguridad (FIRST) para facilitar interacciones de confianza entre los equipos de respuesta a incidentes y seguridad. En el contexto nacional existen varios CERT o CSIRT en ámbitos académicos, sector privado y sector financiero; así como también, un CERT militar. A pesar de lo existente, se requiere una estructura que permita accionar o reaccionar ante incidentes cibernéticos de una forma centralizada y sistematizada (Santos, 2022a).

En el Plan Estratégico Institucional de la Defensa 2017-2021, considerando los nuevos escenarios, se avizora que en la región hay pocas posibilidades de conflictos armados estatales, pero hay una ola creciente de nuevas amenazas en el campo de la seguridad y soberanía: Ante "la inseguridad ciudadana, el crimen transnacional organizado, corrupción, ataque cibernético, el narcotráfico; es necesario tener unas Fuerzas Armadas con la capacidad de poder desarrollar una defensa efectiva del territorio frente a estas nuevas amenazas" (MIDENA, 2017). Por lo que, para minimizar la afectación de los nuevos riesgos y amenazas es necesario sentar bases sólidas y adaptativas, capaces de combatirlas.

Otro documento importante en la concepción de la ciberseguridad y ciberdefensa que se debe hacer referencia es el Acuerdo Ministerial No. 15-2019, del 18 de julio del 2019 y publicado en el Registro Oficial 69 del 28 de octubre de 2019, en el Artículo 4, en el campo de la eficiencia y seguridad de la información, tiene como objetivo "Proteger la seguridad de los activos críticos de información y gestionar los riesgos del ciberespacio, de una forma integral y desde una visión nacional; estableciendo las líneas de acción, en coordinación y cooperación con los sectores público, privado, academia y sociedad civil (MINTEL, 2019).

En el 2020, el crecimiento de las amenazas y la necesidad de asegurar la información impulsa al MINTEL a emitir la versión 2.0 o conocida como segunda versión del EGSI, que con Acuerdo Ministerial No. 025-2019, donde refiere de manera continua: a "Planificar, hacer, verificar, actualizar y que busca preservar la confidencialidad, integridad y disponibilidad de la información" (MINTEL, 2020).

Ante la carencia de regulación en materia de ciberseguridad, el MINTEL como órgano rector de las Telecomunicaciones a través del Acuerdo Ministerial 006-2121 del 17 de mayo del 2021, emite la Política Nacional de Ciberseguridad (PNC), con el objetivo de "construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio" (MINTEL, 2021). Política que nos permite acercarnos a un Ecuador ciberseguro, que garantice el Estado de Derecho, proteja los servicios e infraestructuras críticas del Estado y dé seguridad a la población en el ciberespacio, para este cometido se trazó su línea de acción asentada en 7 pilares:

1. Gobernanza de ciberseguridad
2. Sistemas de información y gestión de incidentes
3. Protección de servicios e infraestructuras críticas digitales

[3] Opera bajo la Agencia para la Regulación y Control de las Telecomunicaciones (ARCOTEL) está regida por la Ley Orgánica de Telecomunicaciones, es el punto de contacto nacional e internacional para la coordinación de la respuesta de gestión de incidentes cibernéticos.

4. Soberanía y defensa
5. Seguridad pública y ciudadana
6. Diplomacia en el ciberespacio y cooperación internacional
7. Cultura y educación de ciberseguridad

Es necesario mostrar a la Política Nacional de ciberseguridad (PNC) como un instrumento estratégico para enfrentar las amenazas cibernéticas en el campo de la seguridad y defensa, evidenciando el rol del Estado ecuatoriano frente a la incidencia de las nuevas amenazas y el control del ciberespacio, considerando que el uso de las Tecnologías de la Información y de la Comunicación es el eje donde circunscriben las sociedades del conocimiento y la evolución permanente del desarrollo tecnológico y por ende el crecimiento exponencial del hábito delictivo.

Una vez detallada la concepción general de ciberseguridad en el Ecuador, es necesario tomar en cuenta que luego de casi dos años de la publicación de la PNC, aún tiene algunos vacíos que deben reconsiderarse, por ejemplo, el componente privado que ejerce ciberseguridad en el país está aislado o tiene poca participación. Así mismo, ciertos sectores demandan la necesidad de abordar contenidos perceptivos como "la identificación y dotación de los recursos financieros necesarios para la implementación de la PNC y su estrategia o plan de acción, y a cuáles instituciones públicas se debe escalar, entre otros temas, las deficiencias presupuestarias (MINTEL, 2022a).

Pensando en fortalecer la ciberseguridad en el Ecuador, el MINTEL emite la Estrategia Nacional de Ciberseguridad el 16 de junio del 2022, con un asesoramiento técnico internacional como el Proyecto de Resiliencia Cibernética para el Desarrollo de la Unión Europea (Cyber4Dev) y el programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos (CICTE/OEA). Además, participaron actores de sector privado, académico, expertos en ciberseguridad y representantes del Comité Nacional de Ciberseguridad[4], lo que permitirá mejorar la resiliencia cibernética de la sociedad ecuatoriana, con el objeto de establecer la dirección y un marco para alcanzar objetivos específicos y claros para los próximos tres años (MINTEL, 2022b).

La estrategia expuesta será aplicada en el período 2022 al 2025, sobre la base de seis ejes de acción que comprenden temas coyunturales como: gobernanza y coordinación nacional, resiliencia cibernética, prevención y combate a la ciberdelincuencia, ciberdefensa, habilidades y capacidades de ciberseguridad, y cooperación internacional. En todo caso, la perspectiva de ciberseguridad en el Ecuador debe articular el accionar de entidades del sector público y privado, la sociedad civil, la academia, las entidades del Estado y la cooperación regional, considerando que la evolución de la amenaza es dinámica y vertiginosa.

3.2. La estrategia de ciberdefensa y la Guía Político – Estratégica de Ciberdefensa

Una de las misiones de Fuerzas Armadas en la Agenda Política de la Defensa 2014-2017 es "Garantizar la defensa de la soberanía e integridad territorial, considerando las operaciones de protección de espacio cibernético, además, participar en la seguridad integral y operaciones de protección a las áreas de infraestructura estratégica". Bajo esta perspectiva, el Ministerio de Defensa Nacional, con Acuerdo Ministerial Nro. 281, de fecha 24 de septiembre del 2014, dispone la creación del Sistema de Ciberdefensa como mecanismo que articula las instancias permanentes y de conformación que aborden el tema desde el nivel político-estratégico, estratégico-militar y operacional, a fin de coordinar e implementar políticas y estrategia de Ciberdefensa.

La ejecución del Acuerdo Ministerial 281 que en sus considerandos indica: " es necesario que en el nivel del Comando Conjunto de Fuerzas Armadas se cree una instancia que implemente las directrices del nivel político, así como la capacidad de ciberdefensa". En este sentido, se acuerda la creación del Comando de Ciberdefensa de Fuerzas Armadas (COCIBER) (MIDENA, 2021a).

En el Plan Estratégico Institucional de la Defensa 2017-2021, uno de los objetivos estratégicos es la capacitación de los sistemas de ciberdefensa, proporcionándoles la capacidad para detectar vulnerabilidades, proteger su infraestructura crítica y contrarrestar efectivamente los ciberataques.

Así mismo, en el Plan Específico de Defensa Nacional 2019-2030, en su Objetivo 1 establece:

> Concomitante con lo anteriormente mencionado, el MIDENA, mediante Acuerdo Ministerial No. 199, publicado en la Orden General Ministerial Nro. 071, de fecha 11 de mayo de 2021, expidió la Política de Ciberdefensa para el sector defensa, que en sus disposiciones generales dispone, expedir la Estrategia de Ciberdefensa y Guía Político-Estratégica de Ciberdefensa, para contribuir a la protección de la infraestructura crítica digital y servicios esenciales del Estado e infraestructura crítica del sector Defensa (MIDENA, 2021b).

En junio 2021, el MIDENA, mediante acuerdo ministerial 199, expide la Estrategia de Ciberdefensa, dentro de su alcance tiene como propósito:

> Desarrollar la Guía Político – Estratégica de Ciberdefensa 2021, que dentro de su contenido hace referencia al ciberespacio como escenario de confrontación, detalla los activos a defender y su propósito. Bajo este contexto, la aplicación de la ciberdefensa se establece la rectoría al MIDENA y en el nivel de planificación y ejecución de las operaciones militares en el ciberespacio al CC.FF. AA. y las Fuerzas (MIDENA, 2021c).

[4] Comité Nacional de Ciberseguridad: Está conformado por los "Ministerios de Telecomunicaciones y de la Sociedad de la Información, Defensa Nacional, Gobierno, Interior, Relaciones Exteriores y Movilidad Humana, Centro de Inteligencia Estratégica y Secretaría General de la Administración Pública de la Presidencia.

El Estado ecuatoriano, a través del COCIBER debe contrarrestar las ciberamenazas, ciberataques, salvaguardar la ICD, servicios esenciales del Estado, infraestructura crítica digital de defensa, así como la protección de derechos en el ciberespacio (Santos, 2022b); y para el efecto, es fundamental fortalecer las coordinaciones interinstitucionales e interagenciales.

3.3. La infraestructura crítica digital del Ecuador

Según la estrategia de seguridad, el MIDENA es el subsidiario de la protección de las infraestructuras críticas digitales y servicios esenciales, específicamente en el pilar 4 "Ciberdefensa", afirma que su objetivo es "Incrementar y fortalecer las capacidades de Ciberdefensa del Estado ecuatoriano de tal forma que se pueda conseguir la actitud estratégica defensiva dispuesta por la Política de la Defensa Nacional, para la protección de la ICD y servicios esenciales en el ciberespacio". Sin embargo, en el Ecuador todavía no se han levantado los activos de la ICD a nivel nacional.

Actualmente, el MIDENA a través del COCIBER inició el proceso de identificación de las infraestructuras críticas en Ecuador, aparentemente están realizando esta actividad únicamente con entidades gubernamentales, lo que no está dando buenos resultados. Por lo que, es prioritario y urgente realizar la convocatoria al entorno de la seguridad; el mismo que está conformado por el sector público: entidades del gobierno, ministerios y secretarias; sector privado: empresas y corporaciones; y el sector civil: sociedad, academia y grupos epistémicos[5].

La protección a la ICD a nivel nacional se torna un poco compleja, considerando que no se ha levantado ni categorizado la ICD por sectores, pudiendo categorizar al sector financiero, hidrocarburifero, eléctrico, de salud, educativo, entre otros. Es urgente, que el Estado a través del comité de ciberseguridad y reforzados por el sector privado conjuguen los esfuerzos y aporten de manera activa al COCIBER en los procesos de levantamiento, categorización y posteriormente en la protección de la infraestructura crítica.

Actualmente, no todos los países cuentan con una normativa que esté ligada estrechamente a la protección de la ICD del Estado y peor aún, planes específicos para minimizar el impacto de los posibles riesgos y amenazas que afecten directamente a los servicios esenciales. Bajo este contexto, proponemos que es prioritario formular una ley que defina, primeramente, al ente rector a nivel de secretaría, responsable de proyectar el enfoque integral de la protección de la Infraestructura Crítica (PIC), que plantee una descripción clara de las principales acciones colectivas impulsadas regionalmente y hemisféricamente, es decir, articular la ciberdiplomacia, concentración en ciberdefensa y la búsqueda de normas vinculantes, en pos de garantizar la protección de la infraestructura crítica del Estado. En ese contexto, además de una adecuada definición de la ICD del Ecuador, es fundamtental también, fortalecer su nivel de ciberseguridad, puesto que, las condiciones actuales son muy desfavorables para alcanzar niveles mínimos de protección ante el ciberterrorismo, conforme se analiza en la tabla 3.

Tabla 3

Evaluación sobre del CMM para el Ecuador

Dimensión	Factores y Aspectos	Indicadores Ecuador
Políticas y estrategias de ciberseguridad, se estructura a través de:	○ Estrategia nacional de ciberseguridad ▪ Elaboración, organización, contenido ○ Respuesta a incidentes ▪ Identificación de incidentes, organización, coordinación, modo de operación ○ Protección de infraestructura crítica ▪ Identificación, organización, gestión de riesgos y respuesta ○ Gestión de crisis ▪ Planificación, evaluación ejercicios y simulaciones sobre de la gestión de crisis ○ Consideración de ciberdefensa ▪ Estrategia, organización, coordinación ○ Redundancia en comunicaciones ▪ Redundancia digital y de comunicaciones	○ Consolidada ○ Consolidada ○ Inicial-Formativa ○ Inicial ○ Inicial-Formativa ○ Inicial
Dimensión 2: Cibercultura y sociedad, se estructura a través de:	○ Mentalidad en ciberseguridad ▪ Gobierno, sector privado, usuarios ○ Confianza y seguridad en internet ▪ Confianza y seguridad de los usuarios en internet, de los servicios de gobierno y de comercio en línea ○ Conocimiento del usuario sobre protección de información personal en línea ▪ Conciencia del usuario público y privado sobre protección en línea	○ Formativa-Consolidada ○ Inicial-Formativa ○ Formativa-Consolidada

[5] Grupos epistémicos: Se define como una red de profesionales con reconocida experiencia y competencia en un campo particular.

	○ Mecanismos de denuncia ▪ Facilidades para colocar denuncias ○ Medios de comunicación y redes sociales ▪ Ciberseguridad en la prensa convencional, rol de la prensa en la educación de ciberseguridad.	○ Inicial-Formativa ○ Inicial
Dimensión 3: Educación, capacitación y habilidades en ciberseguridad, se estructura a través de:	○ Campaña de sensibilización ▪ Programas de sensibilización y sensibilización ejecutiva ○ Marco educativo ▪ Programas educativos para educadores y educandos. ○ Marco para capacitación profesional ▪ Programas y asimilación de profesionales	○ Inicial ○ Inicial-Formativa ○ Formativa
Dimensión 4: Marcos regulatorio y legal, se estructura a través de:	○ Marco legal ▪ Marco legislativo sobre seguridad de TICs ▪ Derechos humanos en línea, libertad de expresión y privacidad ▪ Protección de datos ▪ Protección en línea para menores de edad ▪ Protección al consumidor ▪ Propiedad intelectual ▪ Legislación para la ciberdelincuencia ○ Justicia penal ▪ Fuerzas del orden ▪ Fiscalía ▪ Tribunales ○ Marcos de cooperación formal e informal contra la ciberdelincuencia ▪ Cooperación formal ▪ Cooperación informal	○ Formativa ○ Formativa ○ Consolidada
Dimensión 5: Normas, organizaciones y tecnologías	○ Cumplimiento de normas ▪ Normas de seguridad de las TICs ▪ Normas de adquisición ▪ Normas de desarrollo de software ○ Resiliencia en la infraestructura de internet ▪ Servicios e infraestructuras resilientes y confiables ○ Calidad del software ▪ Calidad y funcionalidad en la implementación de software ○ Controles técnicos de seguridad ▪ Controles técnicos para usuarios público y privados ○ Controles criptográficos ▪ Técnicas de criptografía empleadas ○ Mercado de ciberseguridad ▪ Tecnologías de ciberseguridad ▪ Seguro cibernético ○ Revelación responsable ▪ Recepción y diseminación de información vulnerable	○ Formativa ○ Formativa ○ Inicial ○ Inicial ○ Inicial ○ Inicial ○ Inicial

Nota. Elaborado por los autores, sobre la base del CMM.

CONCLUSIONES Y RECOMENDACIONES

Una de las hipótesis planteadas en la investigación es adecuadamente verificada, dado que se puede confirmar que existe un crecimiento indiscriminado del terrorismo y ciberterrorismo en América Latina, escenario en el que el Ecuador aparece con una incipiente capacidad de gestión y acción para el fortalecimiento de la ciberseguridad y ciberdefensa, lo que lo ubica en el último lugar en el ranking de ciberseguridad de la ITU. A su vez, esto genera la imperiosa necesidad de revolucionar las políticas y estrategias en este ámbito, para lo cual, se debe promulgar y generar un mayor compromiso de la sociedad, del gobierno y de las distintas instituciones, para de esta forma, generar verdaderas políticas públicas que incrementen la gobernabilidad y posibiliten la suma de esfuerzos públicos y privados.

El Estado deberá incorporar el monitoreo y análisis de la capacidad de ciberdefensa al seno del COSEPE, toda vez que, cada vez son más frecuentes los ciberataques

a todo nivel, es por ello por lo que, este ámbito debe dejar de ser observado desde una perspectiva puramente administrativa y pasar a formar parte de los análisis permanentes y sigilosos de las amenazas que afectan a la seguridad nacional. Precisamente, en instantes en que el terrorismo se siente amenazado por el poder coercitivo del Estado, son el espectro electromagnético y el espacio cibernético, los lugares más propicios para que mantengan sus coordinaciones, reorganizaciones, entre otras.

En cuanto a los indicadores de madurez de la capacidad de ciberdefensa, el Ecuador refleja una condición crítica, siendo que la mayoría de índices (catorce) alcanza un nivel inicial, siete índices están en nivel formativo y apenas tres índices tienen una capacidad consolidada, siendo estos específicamente los referentes a la existencia de la normativa nacional, es decir, la normativa existe, por lo menos en un nivel aceptable; y se evidencia que el problema radica en el ámbito de la gestión para alcanzar los recursos para el cumplimiento de la misma. Es importante mencionar que, durante la presente investigación, se ha realizado una evaluación sobre la base de la información disponible en el internet.

El mundo entero está dando un giro importante para enfrentar al ciberterrorismo y los ciberataques, conforme se planteó en otra de las hipótesis de la investigación, se ha convertido en una forma de terrorismo, es así que, en la actualidad es considerado como el quinto riesgo más alto para la humanidad, y que por tanto, en el caso específico ecuatoriano, se deben gestionar los cambios necesarios para su fortalecimiento, cambios como: definición precisa de la infraestructura crítica del Estado, incremento de la capacidad de ciberdefensa e incremento de una participación conjunta de sociedad y estado para alcanzar una sinergia que permita tener la resiliencia mínima requerida para evitar que estos ataques causen efectos críticos o catastróficas en la vida de nuestro país, promover el desarrollo tecnológico endógeno, tanto de software como de hardware y disminuir la dependencia tecnológica en un índice razonable.

Referencias

ARCOTEL. (Julio de 2017). *Resolución ARCOTEL* - 2017. Resolución ARCOTEL. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.arcotel.gob.ec/wp-content/uploads/downloads/2017/08/Resolucion-0734-ARCOTEL-2017.pdf

Bueza, F. (feb de 2022). *Qué es el terrorismo.* Fundación Fernando Bueza: https://www.youtube.com/watch?v=U_pzWY3QOPE

Council of Europe. (2023). *Manual de educación en los derechos humanos con jóvenes.* Guerra y Terrorismo: https://www.coe.int/es/web/compass/war-and-terrorism#What%20is%20terrorism, recuperado el 30 de noviembre de 2023

Cueto, H. (09 de feb de 2023). *YahooFinance.* Ganancias totales de mercados en la dark web se redujeron más de 1,000 mdd en 2022, revela Chainalysis: https://es-us.finanzas.yahoo.com/noticias/ganancias-totales-mercados-dark-web-010014820.html, recuperado el 13 de diciembre de 2023

Deloitte. (2023). Global Future of Cyber Survey 2023. https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html, recuperado el 16 de diciembre de 2023

García-Sigmman, L. (2017). Narcotráfico en la Darkweb: los criptomercados, DOI: http://dx.doi.org/10.17141/urvio.21.2017.2824. URVIO, 191-206.

Global Cyber Security Capacity Centre. (2016). *Modelo de Madurez de Capacidades de Ciberseguridad para Naciones* (CMM). Universidad de Oxford.

Internet Society. (2023). *Historia del internet.* https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/, recuperado el 09 de diciembre de 2023

ITU. (2021). Unión Internacional de Telecomunicaciones. Índice global de ciberseguridad: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E, recuperado el 15 de diciembre de 2023

ITU. (2023). Unión internacional de las telecomunicaciones. https://www.itu.int/es/wtisd/Pages/about.aspx, recuperado el 09 de diciembre de 2023

Laqueur, W. (2003). *La guerra sin fin. El terrorismo del siglo XXI*. Planeta Colombiana S.A., ISBN 958-42-0815-2.

Masana, S. (jul de 2002). El ciberterrorismo: ¿una amenaza real para la paz mundial? Trabajo de tesis previa la obtención del título de Magíster en Relaciones Internacionales por la Facultad Latinoamericana de Ciencias Sociales. Ecuador: FLACSO, disponible en: https://docplayer.es/7003720-El-ciberterrorismo-una-amenaza-real-para-la-paz-mundial.html.

MIDENA. (2017). *Plan Estratégico Institucional de la Defensa* 2017-2021. 33-34. https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/02/PEI-2017-2021.pdf

MIDENA. (2021d). Aplicación de la ciberdefensa en el Ecuador. *Guía político-estratégico de ciberdefensa*, 85.

MINTEL. (julio de 2019). 2019. Acuerdo Ministerial No. 15-2019, 4-5. chrome-extenhttps://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/10/Acuerdo-No.-015-2019-Politica-Ecuador-Digital.pdf

MINTEL. (enero de 2020). Acuerdo ministerial No. 025-2019. chrome-extension:/https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf

MINTEL. (2021). Política Nacional de Ciberseguridad. En M. d. información, Política Nacional de Ciberseguridad. Acuerdo ministerial 006-2121.

MINTEL. (2022b). *Diagnóstico de las capacidades de ciberseguridad en el Ecuador 2022*. 30-31.

MINTEL. (06 de jun de 2023). Observatorio Ecuador TIC. https://observatorioecuadordigital.mintel.gob.ec/wp-

content/uploads/2023/07/RESULTADOS_MINTEL_JUNIO-2023.pdf, recuperado el 15 de diciembre de 2023

Prego, C. (01 de ene de 2023). Qué fue de Silk Road y su creador, Ross W. Ulbricht: el caso que marcó el tráfico de drogas en Internet. *Xataka*: https://www.xataka.com/historia-tecnologica/que-fue-silk-road-su-creador-ross-w-ulbricht-caso-que-marco-trafico-drogas-internet, recuperado el 12 de diciembre de 2023

Rapoport, D. (21 de jun de 2004). Las cuatro oleadas del terrorismo moderno. *Dialnet:* https://dialnet.unirioja.es/descarga/articulo/5774612.pdf, recuperado el 12 de diciembre del 2023

Recomendación ITU-T X.1205. (18 de abr de 2008). Unión Internacional de Telecomunicaciones. *Recomendaciones de Telecomunicaciones*: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-S&type=items, recuperado el 13 de diciembre de 2023

Rodriguez, T. (2012). El terrorismo y nuevas formas de terrorismo. Universidad Autónoma del Estado. Espacios Públicos, vol. 15 (33), disponible en: http://www.redalyc.org/articulo.oa?id=67622579005, 72-95.

Santos, M. (2022a). Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la informació y el conocimiento. file:///C:/Users/Familia/Desktop/T3975-MRI-Santos-Marco.pdf

Santos, María. (2022b). Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la informació y el conocimiento. 85. file:///C:/Users/Familia/Desktop/T3975-MRI-Santos-Marco.pdf

Villanueva, D. (11 de jul de 2023). *La Jornada*. Mueve la 'dark web' la tercera economía más grande del mundo: https://www.jornada.com.mx/notas/2023/07/16/economia/mueve-la-dark-web-la-tercera-economia-mas-grande-del-mundo/?from=homeonline&block=ultimasnoticias

Wahnon, P. (05 de jul de 2023). *Forbes.* Dark web: cuáles son los productos y servicios más demandados por los cibercriminales que llegarán a US$ 8 billones en 2023: https://www.forbesargentina.com/innovacion/stephane-bancel-ceo-moderna-anuncia-tendran-una-vacuna-cancer-acciones-disparan-n45095, recuperado el 13 de diciembre de 2023

WorldEconomicForum. (ene de 2023). WorldEconomicForum. Global Risk Report 2023. 18 va. edición: https://www.weforum.org/publications/global-risks-report-2023/, recuperado el 15 de diciembre de 2023