FACULTAD DE CIENCIAS HUMANAS

HACKTIVISMO DE ANONYMOUS EN EL ECUADOR: ANÁLISIS REALISTA DE LAS ESTRATEGIAS Y CONSECUENCIAS DE LOS ACTORES NO ESTATALES TRANSNACIONALES EN EL MODELO ECUATORIANO DE CIBERSEGURIDAD (2011-2020)

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE LICENCIADA EN RELACIONES INTERNACIONALES

VALERIA ESTEFANÍA CARVAJAL ARTIEDA

DIRECTORA: Mtr. GILDA GUERRERO SALGADO

MAYO, 2022

QUITO-ECUADOR

DEDICATORIA

Para las mujeres de mi vida,

Mary y Lupita.

Por su forma de amarme, cuidarme y enseñarme con su ejemplo que las mujeres valientes no tenemos límites ni obstáculos tan grandes que nos hagan dudar de nuestra capacidad en el mundo.

AGRADECIMIENTOS

A la Facultad de Ciencias Humanas de la Pontificia Universidad Católica del Ecuador y a mis maestros por su calidad humana, por brindarme una formación integral para mi desarrollo académico, profesional y personal.

A la Magister Gilda Guerrero, por su don de gente, por su paciencia y colaboración durante todo el proceso de investigación, pero, sobre todo, por ser mi guía y ejemplo en todos estos años universitarios.

A mis padres, por su sacrificio y por haberme forjado como la persona que soy hoy en día.

A mi familia, por ser mi fortaleza y pilar fundamental en esta etapa de mi vida.

A mis amigos, por ser mis cómplices y permitirme compartir juntos este increíble viaje.

A él, por ser mi compañero de aventuras y brindarme su amor y apoyo incondicional.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

I. RESUMEN

En los últimos años el ciberespacio se ha consolidado como un nuevo dominio para el desarrollo de las relaciones internacionales. Por lo tanto, su desarrollo actual coincide con la llegada de las tecnologías de la información, interacción entre los individuos con las redes cibernéticas y el nuevo fenómeno del Internet que ha logrado configurar una nueva dimensión aplicable para las guerras modernas, afectando la vida de los miembros en el sistema internacional. En este contexto, el hacktivismo nace como una nueva forma de activismo mediante herramientas virtuales que logra la aparición de nuevos actores no estatales que representan intereses públicos contribuyendo la extensión del poder. De hecho, Anonymous se ha posicionado como un actor no estatal transnacional relevante en el ciberespacio por sus operaciones en contra de los Estados. En ese sentido, la presente investigación propone el análisis del modelo de ciberseguridad del Estado ecuatoriano desde una visión realista tras una exploración analítica-conceptual de las estrategias y normativa vigente por los hackeos efectuados por estos actores no estatales, ya que el estudio de estos espacios se vuelve una tarea específica para la formulación de políticas estratégicas de defensa de las naciones.

Palabras clave: Anonymous, hacktivismo, políticas estratégicas, ciberespacio, estudios estratégicos, actores no estatales.

II. ABSTRACT

In recent years cyberspace has been consolidated as a new domain for the development of international relations. Therefore, its current development coincides with the advent of information technologies, interaction between individuals with cybernetic networks and the new phenomenon of the Internet that has managed to configure a new dimension applicable to modern wars, affecting the lives of members in the international system. In this context, hacktivism is born as a new form of activism through virtual tools that achieves the emergence of new non-state actors representing public interests contributing to the extension of power. In fact, Anonymous has positioned itself as a relevant transnational non-state actor in cyberspace for its operations against states. In this sense, this research proposes the analysis of the Ecuadorian State's cybersecurity model from a realistic vision after an analytical-conceptual exploration of the strategies and regulations in force by the hacks carried out by these non-state actors, since the study of these spaces becomes a specific task for the formulation of strategic policies for the defense of nations.

Keywords: Anonymous, hacktivism, strategic policies, cyberspace, strategic studies, non-state actors.

III. INTRODUCCIÓN

El desarrollo de las Tecnologías de la Información y Comunicación ha transformado la vida humana, incluyendo sus estructuras sociales y políticas, que a su vez ha generado un escenario que acompaña este proceso con la facilidad de intercambiar información y crear interacciones con la ciudadanía y las funciones del Estado. Así bien, el concepto de seguridad ha estado evolucionando durante los años y ha sido parte fundamental de las diferentes concepciones tradicionales que se incorporan en el Ecuador desde la Constitución del 2008 para una nueva conducción estratégica del Estado por los nuevos dominios que se incorporan. Por lo tanto, entra en debate los términos de ciberseguridad, ciberdefensa y ciberespacio para la comprensión de su estructura y configuración, ya que la creciente importancia del ciberespacio para las sociedades actuales y su uso mayoritario como un nuevo escenario de conflictos virtuales ha tomado interés para la seguridad nacional de los gobiernos y de las fuerzas armadas con la presencia de nuevos actores no estatales -como los hacktivistas- que pueden vulnerar la seguridad nacional.

El Ecuador desde el 2011 ha enfrentado diversos ataques hacktivistas por el grupo no estatal transnacional Anonymous debido a la coyuntura política que ha atravesado; sin embargo, el Estado y los gobiernos no han enfocado sus esfuerzos en plantear y ejecutar verdaderas políticas públicas que impliquen no solo el cuidado de la información de la ciudadanía, sino también prevenir las potenciales amenazas que pueden representar las acciones de estos actores para la infraestructura crítica del Estado, puesto que el estudio de la ciberseguridad para el sistema internacional permite establecer nuevas temáticas de seguridad. La pregunta que se plantea sobre la problemática se dirige a responder ¿Cuáles fueron las estrategias y consecuencias efectuadas por el Estado ecuatoriano durante el 2011 al 2020?, tomando en consideración que la hipótesis central es que los hackeos y hacktivismo efectuado

por Anonymous durante este periodo, tendría origen en una falta de políticas y estrategias de ciberseguridad en el Estado y gobierno del país.

El objetivo principal de la investigación propone analizar las estrategias y consecuencias del hackeo y hacktivismo de Anonymous como actor no estatal transnacional en el Estado ecuatoriano durante el periodo 2011 al 2020; examinando los ataques hacktivistas de este actor no estatal transnacional a nivel internacional y nacional; explicando su incidencia de estos actores nocivos para la lógica estatal desde una perspectiva teórica y casuística; analizando el alcance y aplicación de las políticas públicas del Estado ecuatoriano en materia de ciberseguridad alrededor de este periodo de estudio.

El enfoque teórico se basa directamente desde la perspectiva realista de los estudios estratégicos de seguridad para su comprensión a partir de la lógica de la seguridad nacional y el posicionamiento estatocéntrico de para las agendas políticas de los Estados. En primera instancia, se considera a la teoría del realismo estructural o neorrealismo de Kenneth Waltz (2000) debido a que determina que el sistema internacional está configurado en un principio de ordenación que puede ser anárquico o jerárquico en el que las unidades de análisis o Estados se encuentran bajo los elementos de distribución de capacidades y principios ordenadores. En segunda instancia, el realismo ofensivo de Mearsheimer (2001) por su percepción de anarquía para el sistema internacional por la no presencia de una autoridad central que pueda proteger a las potencias de las posibles amenazas, y que conlleva a una supervivencia como objetivo principal de cualquier Estado.

En ese sentido, el primer capítulo de esta investigación se presenta como una sección destinada al análisis y conceptualización del grupo o colectivo no estatal transnacional Anonymous, para la mejor comprensión de su funcionamiento, estructura e ideología con los ciberataques tanto a nivel internacional como nacional y su evolución e importancia dentro de las agendas políticas del sistema internacional. El segundo capítulo se aproxima con las

discusiones teóricas neorrealistas sobre la ciberseguridad, ciberdefensa y el nuevo escenario del ciberespacio involucrado directamente con el colectivo, puesto que es cuando en materia de seguridad el Estado ecuatoriano tiene un desafío coyuntural importante para impulsar políticas estratégicas de defensa sobre este nuevo dominio internacional que se vuelve vulnerable por las posibles amenazas y ataques que representan un peligro de desestabilización al Estado. Correspondiente al capítulo tres, se busca determinar el análisis de las políticas públicas en materia de ciberseguridad con la normativa jurídica vigente desde la concepción de seguridad integral de la Constitución del 2008 y su entendimiento del desarrollo jurídico para comprender si estos avances han logrado ejecutar dentro del Estado ecuatoriano una agenda estratégica de seguridad que involucre los temas referentes al ciberespacio y las posibles amenazas que enfrenta con los nuevos actores presentes, desde la metodología planteada por David Easton (1965) en su enfoque del sistema político.

La investigación aporta un nuevo enfoque en los estudios de seguridad frente a la comprensión de prácticas de ciberseguridad estatal, análisis frente a su importancia, posibles amenazas y nuevas vulnerabilidades que pueden existir en el actual sistema. También, el enfoque realista de las relaciones internacionales, especialmente con el cuidado de la defensa y seguridad, permite determinar las limitaciones que pueden presentar las instituciones encargadas del cuidado y protección del Estado, para plantear la posibilidad de nuevas estrategias con esta concepción de seguridad desde la misma línea teórica. Finalmente se espera contribuir con una aproximación sobre el contexto del ciberespacio correspondiente como un lugar anárquico que debe integrarse completamente a las relaciones internacionales ya que los Estados no son los únicos en crear amenazas en este nuevo dominio y que a la vez impulse a formar investigaciones que contribuyan a la realidad internacional como nacional desde los enfoques multidisciplinarios.

CAPITULO I

HACKTIVISMO COMO MOVIMIENTO POLÍTICO-SOCIAL

Este primer capítulo de la investigación se desarrolla con la finalidad de presentar los ataques hacktivistas del actor no estatal transnacional Anonymous a nivel internacional y nacional para responder las demandas que se han producido con las nuevas amenazas que representan los hackeos en el sistema internacional. Así pues, estos temas evidencian la vulnerabilidad de seguridad por la presencia de los nuevos actores que han estado presentes modificando el sistema internacional, sobre todo la concepción de las manifestaciones y protestas sociales.

Por otra parte, con la constante actualización de la era digital se toma en cuenta la inquietud de los Estados por las estrategias y formas en la que los ciberataques atentan contra la infraestructura de ciberseguridad de las instituciones gubernamentales tomando en consideración los antecedentes de los primeros colectivos que han comenzado con el hacktivismo a través de la historia. En este ámbito, los principales ataques dentro del sistema internacional se generan por aspectos políticos en contra de regulaciones o decisiones estatales que están en contra de la libertad de expresión, provocando el malestar de los individuos que luchan por los derechos fundamentales a través de medios digitales por las múltiples posibilidades que el ciberespacio conlleva con la interacción de redes.

1.1. Conceptualización del hacktivismo

Los primeros acercamientos al hacktivismo se producen en la década de los 60 con los nuevos movimientos sociales y grupos de expertos en temas de seguridad y desarrollo informático. Sin embargo, es en 1984 que "La Secta de la Vaca Muerta" [1]crea un proyecto llamado "Hacktivismo" con el objetivo de luchar contra la censura del Internet e incluso brindar apoyo técnico a internautas que se encontraban bajo el mando de gobiernos opresivos (Torres, 2015). Por lo tanto, el hacktivismo nace como una de las nuevas formas de protesta con la

[1] Grupo de hackers estadounidenses que se crea en 1984 haciendo referencia con su nombre al matadero texano donde se ejecutaban sus reuniones (Torres, 2015)

concepción que se produce por la actualización de las TIC's (Tecnologías de la Información); incluso por la era de digitalización y la evolución de la web, el hacktivismo puede considerarse como un fenómeno rizomático[2] abierto que logra extender sus raíces por todos los lugares (Alcalá & Rodrigues, 2012) ya que el Internet rechaza los controles verticales por lo que no existe una estructura central o jerarquizada que regule la información que se encuentra en todos los niveles pero en el mismo plano cibernético (Ragnedda, 2011). Es importante comprender que la comunicación en redes ha permitido que las interpretaciones sobre el activismo cambien incorporando elementos adaptables a la sociedad que las necesita. Sin embargo, para entender lo que es el hacktivismo es necesario definir las palabras que lo conforman.

Por un lado, el término se despliega de "hacker" haciendo alusión a los individuos que mantienen habilidades con los sistemas informáticos; y "activismo" como una actividad social de personas que forman movimientos para manifestaciones o protestas (Burgos, 2014). De esta forma, el hacktivismo - la combinación entre la cultura hacker[3] y activismo - se manifiesta como un acercamiento de interacciones con herramientas tecno-políticas que son accesibles para la sociedad (Barandiaran, 2003).

Desde otra perspectiva, para Vicente (2004) el hacktivismo busca involucrarse con los movimientos sociales que existen con el objetivo de incorporar nuevas tácticas y una nueva infraestructura virtual de protesta alternativa para lograr difusión de las manifestaciones en espacios virtuales y locales. Al mismo tiempo, autores como Alonso y Arzoz (2005) se alejan de la perspectiva heroica del hacker o hacktivista rechazando los estereotipos de crear solo virus destructivos con fines políticos o sociales para entender que el término implica la activa

[2] Determinado por Deleuze y Guattari (2000) creando referencia a: "Una serie de redes constitutivas que logran conectar cualquier punto en cualquier red como las bases de las dinámicas estructurales definidas dentro de los conceptos nuevos de identidad superando las concepciones de la subjetividad y el espacio" (Barandiaran, 2003)
[3] Subcultura formada por individuos que tratan de superar los límites de los sistemas de software. Aparece dentro de la academia en los 60 por el Tech Model Railroad Club (TMRC) del Instituto Tecnológico de Massachusetts (MIT) y el laboratorio de Inteligencia Artificial del MIT (Raymond, 2000)

participación de organizaciones e instituciones en ámbitos físicos y digitales. Por añadidura, esta labor debería enfocarse en la invención de diseños nuevos en la red, mantener comunidades virtuales, crear software y hardware libres que permitan desarrollar una verdadera cibercultura (Alonso & Arzoz, 2005, pág. 122).

El activismo online -como también se conciben a las protestas originadas en la red o internet- ocasiona ciberataques que afectan de forma directa a varios sitios web. Aun así, la Oficina de las Naciones Unidas contra la Droga y el Delito (2020) explica que este tipo de protestas genera una controversia sobre el proceso de tipificación de acciones que pueden considerarse como delito y cuáles no, ya que, en muchas ocasiones la inmediatez de la información lo único que produce es notoriedad de estas acciones y el hacktivismo contempla características que lo diferencia que se abordará más adelante.

En primer lugar, estos ataques cibernéticos son acciones que cuentan con una gran apertura mediática y social; también las técnicas que se emplean permiten dominar las TIC´s y evadir la normativa establecida (Torres, 2015). Es así como entre los ilícitos comúnmente ejecutados por los hacktivistas en contra de entidades públicas y privadas se encuentran los ataques de denegación de servicio (DoS[4]), ataques distribuidos de denegación de servicio (DDoS[5]), deformación de sitios web (defacement), distribución de programas maliciosos, redireccionamientos de sitios web, divulgación y robo de datos e información, sabotaje e incluso parodias de sitios web (UNIR, 2021).

1.1.1 Grupos relacionados con el movimiento hacktivista

Los grupos activistas o hackers han conformado nuevos tipos de participación social, económica y política a través de las plataformas digitales creando, planificando e incluso introduciendo nuevos términos que permitan su representación en el ciberespacio. Por

[4] Provoca que los recursos o servicios sean inaccesibles a los usuarios mediante la saturación de los puertos con múltiples flujos de información para que exista una sobrecarga en el servidor (Lazár, 2018).
[5] Saturación de la red generando un gran flujo de información desde varios puntos de conexión (Lazár, 2018).

ejemplo, el grupo *Critical-Art- Ensemble* [6]establece el Tactical Media [7]como una forma de desobediencia civil electrónica dentro de la resistencia digital, buscando apertura tanto en las manifestaciones físicas como en el ciberespacio (Vicente, 2004).

Sin embargo, varios de los hacktivistas se enfocan directamente en la defensa de causas ideológicas, luchas contra la discriminación o la defensa del internet como un espacio libre y democrático (Alcalá & Rodrigues, 2012). Así bien, entre los grupos más relevantes podemos mencionar a *Cult of de Dead Cow*, *Chaos computer club*, *Anonymous*, *LulzSec* y *Syrian Electronic Army*. Cada uno de ellos lucha por una causa que no se encuentran al margen de las leyes y que pueden considerarse como éticas o justas, pero no necesariamente corresponden como actividades legales (Enriquez, 2021).

Los ciberataques engloban una complejidad en sí mismos, debido a que la mayoría son ataques intangibles que no cuentan con una regulación en el área, puesto que no existe una sola definición reconocida por la comunidad internacional que contenga en sí mismo las concepciones que abarca la terminología en cada país (Lazár, 2018). De forma similar, el ciberespacio aborda esta complicación terminológica por su manera de almacenar información mediante el uso de la tecnología como un dominio global mediante redes interconectadas (Gamón, 2017).

No obstante, la Convención del cibercrimen de Budapest[8] del 2001 es el instrumento internacional de mayor relevancia en esta materia; y desde su enfoque tradicional clasifica a los delitos informáticos en cuatro: delitos como fin, como medios, de contenido; y relacionados con infracciones a la propiedad intelectual (Enriquez, 2021), aunque no tipifica al hacktivismo como un delito informático, toma en consideración en la actualidad al

[6] Critical-Art-Ensemble (2001). Digital Resistanse Autonomedia. http://critical-art.net/
[7] Forma de intervencionismo digital, donde por digital se entiende el espacio definido por la copia, la recombinación y la representación. TM cuestiona el régimen semiótico, creando eventos participativos, criticando a través de un proceso experimenta (Vicente, 2004).
[8] Primer tratado internacional frente a los delitos informáticos y delitos de internet.

terrorismo cibernético y a cualquier otro delito cometido por medio de un sistema informático según el artículo 14 del Convenio. Sin embargo, la Asociación Ecuatoriana de Ciberseguridad (AECI) ha estado buscando que el Ecuador sea ratificante de este Convenio con el objetivo de contar con herramientas en común para procesar cada una de las actividades delictivas mediante cooperación internacional en materia de delincuencia cibernética y ayuda jurídica para unificar las jurisdicciones nacionales e internacionales (iT Tecnología, 2021).

Ahora bien, la existencia de varios grupos hacktivistas en el sistema internacional han generado un debate sobre si sus acciones se encuentran estipuladas en el marco de la ley o se pueden determinar cómo ciberataques o amenazas a las instituciones y organizaciones; y tal como indica Lazár (2018) “el anonimato es la ventaja más grande de los ataques cibernéticos porque pueden parecer que fueron originados en las redes y computadoras de un Estado, pero no significa que se encuentre involucrado” (pág. 159).

No obstante, en un mundo en evidente actualización, los actores no se limitan solo a los Estados, sino se incorporan entre civiles o militares, incluso gubernamentales y no gubernamentales con el uso únicamente de herramientas tecnológicas como el grupo hacktivista Anonymous, que ha tenido una participación importante dentro del sistema internacional, del cual ampliaremos su concepción de lucha contra la libertad de expresión y búsqueda de justicia (Coleman, 2014).

Con el análisis anterior, y de acuerdo con la secuencia de los hechos estipulados entre el hacktivismo y la era de digitalización, surge un actor principal dentro del escenario internacional que ha provocado el planteamiento de la nueva concepción de seguridad dentro de las relaciones internacionales. De esta manera, se desarrollará en las próximas líneas el fenómeno transnacional no estatal Anonymous para concretar con los análisis enfocados en el surgimiento de las amenazas que representan para la ciberseguridad y ciberdefensa tanto a nivel doméstico como internacional.

1.2. Estudio de Anonymous como actor no estatal transnacional

Las acciones propiciadas por Anonymous- en especial por sus connotaciones políticas- abren lugar para nuevos espacios públicos de protestas digitales, en el que lo virtual se relaciona directamente con lo real, con el fin de ejercer presión desde las agendas públicas y la propia institucionalidad (Rivera, 2018). La mediatización de este grupo hacktivista ha provocado que los conflictos domésticos e internacionales tomen al ciberespacio, y en palabras de Mikhaylova (2014) como nuevo objeto de estudio por el "exponencial avance de las TIC´s con su particular relación con la ciberseguridad" (Rivera, 2018).

El significado de la máscara de Guy Fawkes[9] con el que se identifica el grupo, al igual que la representación cinematográfica de V for Vendetta[10] relacionan a estos hacktivistas con causas como la indignación de movilizaciones alrededor del mundo por estallidos sociales y protestas por causas políticas. Por ende, este colectivo llega a contar con una incidencia más amplia en los espacios digitales para luego llegar a los espacios públicos, dado que su "nacimiento" fue incluso en un foro en la web.

La académica y antropóloga Gabriela Coleman (2014), señala que este colectivo tuvo origen en un foro denominado 4chan[11] en el 2003 y que permite compartir diferentes temas desde el anonimato principalmente. Esta interacción del foro entre los internautas se produce mediante un tipo de humor poco convencional derivado incluso de la humillación, o como los Anons[12] lo identifican, el Lulz[13]. No obstante, Anonymous no se posiciona en el sistema hasta el 2008 en búsqueda de objetivos activistas, y es aquí cuando este nombre se interpreta como uno solo sin la necesidad de jerarquías, ni la fragmentación de grupos o élites políticas, de manera que su único objetivo es revelar información confidencial o secreta de actores

[9] Personaje revolucionario de Inglaterra que intentó volar el parlamento inglés en 1605 (Rivera, 2018)
[10] Adaptación de la novela gráfica V for Vendetta (V de Venganza)
[11] Foro con marcadores poco identificables que permiten juzgar los posts por su contenido.
[12] Forma de identificación de los individuos que forman parte del colectivo de Anonymous.
[13] Similar al LOL, que significa reírse a carcajadas o a costa de otras personas.

como organizaciones privadas, gobiernos, entre otros, que han dañado a la sociedad. Incluso se puede describir que el colectivo no cuenta con una ideología definida y acorde a la investigación de Coleman (2014) sus principios se basan únicamente en el anonimato y la igualdad de todos, porque incorpora varias relaciones y actitudes morales para no caer en la tiranía de esta falta de estructura y evitar la lucha por el poder para intereses individuales, aunque por periodos limitados de tiempo algunos Anons son más activos e influyentes que otros (pág. 289).

El primer acercamiento que tuvo Anonymous con el hacktivismo fue en el 2008 por un video publicado por la Iglesia de la Cienciología en el que aparece el actor Tom Cruise -como mayor exponente- invitando a unirse a esta religión de élite que estaba siendo acusada por múltiples estafas por dinero a cambio de un verdadero progreso espiritual. Sin embargo, debido a la impresión del video, la Iglesia de la Cienciología lo elimino de sus plataformas, provocando el *efecto streisand* [14] (Coleman, 2014). En este acercamiento al activismo online se lo denominó "Proyecto Chanology" ya que el colectivo comenzó a efectuar ciberataques a los servidores de la Cienciología como llamadas telefónicas en broma e incluso saturaron sus faxes. El objetivo principal era paralizar por completo las operaciones de la Iglesia de la Cienciología e incluso incitaron a las manifestaciones no violentas en la vía pública como medio legal de protestas por la desinformación y represión de la disidencia que proporcionaba la cienciología (Clarin, 2020).

Por consiguiente, en el 2010, inició la "Operación Vengar a Assange" en el que un grupo de Anons enfocaron sus esfuerzos para hackear varios sistemas informáticos de entidades bancarias y financieras como VISA, PayPal y MasterCard por atentar en contra de la participación de Julian Assange con el caso de WikiLeaks (EFE, 2010). Así mismo, en el 2011 el colectivo comenzaba a hackear los sitios web del gobierno de Túnez como el

[14] Fenómeno de Internet mediante el cual el intento de censurar una información consigue el efecto contrario: más personas quieren conocerla para entender el motivo de la censura (Coleman, 2014)

Ministerio de Cultura y de varios partidos políticos españoles llamando a sus ciberataques "Operación Túnez". Los objetivos principales de esta operación contemplaron la ayuda a las protestas por la libertad de la gente para luchar contra la opresión del gobierno corrupto (El Mundo, 2011).

Por otro lado, entre los ataques cibernéticos a nivel internacional más actuales destaca el accionar del colectivo durante los primeros meses del 2022. Anonymous hostigó a Rusia declarando una guerra cibernética por los acontecimientos suscitados en Ucrania desde su invasión. Así entre sus acciones están el hackeo de las transmisiones de los canales de televisión rusos para que se puedan compartir las imágenes de guerra que viven los ciudadanos en Ucrania y el robo de información confidencial de instituciones estatales rusas solo con ataques DDoS (Tidy, 2022). Incluso, el grupo hacktivista aseguraba que había cumplido sus objetivos, ya que generaba conflicto en las instituciones gubernamentales -como el Banco Central de Rusia- por sus amenazas directas de revelar información confidencial y otros documentos secretos. Así mismo, abiertamente le declararon la guerra a Rusia y se posicionaron por primera vez como aliados del pueblo ucraniano desde el inicio del estallido de este conflicto armado (La Vanguardia, 2022), aunque es importante comprender que Anonymous no es el único colectivo que mantiene estos principios ni ideales hacktivistas, más bien es el que más fuerza ha generado -y más famoso- durante la última década.

1.2.1. Ataques de Anonymous en el Ecuador

La presencia del grupo hacktivista en el Ecuador se determina dentro de dos períodos presidenciales: Rafael Correa Delgado (2007-2017) y Lenin Moreno (2017-2021) con ideales de apoyo a los débiles contra los poderosos. De esta forma, el presente caso de estudio analiza los ataques efectuados desde el 2011 hasta el 2020.

Los primeros ataques del grupo de hackers informáticos Anonymous en el Ecuador comienzan en el 2011 con la "Operación Condor Libre" como rechazo a la sentencia contra el

diario El Universo por la censura de la libertad de expresión durante el periodo de Rafael Correa. El 1 de agosto compartieron un video expresando su rechazo, sin embargo, el colectivo escogió el 10 de agosto como la fecha en la que se efectúan la mayoría de los ciberataques (El Comercio, 2014). El Gobierno de Ecuador -con los ataques- emitió un comunicado desde el Ministerio de Telecomunicaciones en el que advertían que cualquier otro ataque se castigará de acuerdo con la ley; y la respuesta de Anonymous fue publicar datos de la Policía Nacional con números de cédula y fechas de nacimientos (La República, 2011).

Por otro lado, en el 2012, el colectivo hackeo algunas páginas de organismos públicos como las de los Municipios de Rocafuerte, Chone, San Vicente como muestra del rechazo a la privacidad de los internautas por el interés que mantenían los proveedores de servicio de Internet por conocer las direcciones IP. Así mismo, páginas como la Presidencia, Asamblea Nacional, Ministerio de Telecomunicaciones tuvieron una suspensión temporal. No obstante, Anonymous inició este mismo año con la Operación Surkisha -la mayor intervención que han tenido- atacando 45 páginas gubernamentales como pronunciamiento en contra de la Ley de Comunicación, explotación del Yasuní y la sublevación policial del 30-S (El Universo, 2012).

De la misma forma, desde el 2013 hasta el 2017 las redes sociales de Anonymous Ecuador [15]pusieron en evidencia la campaña que mantenían contra los partidos políticos como el PSP de Lucio Gutiérrez, Revolución Ciudadana e incluso la página de la Universidad Católica de Guayaquil usando los hashtags #EcuadorHackingTeam y #OpFalsaRevolución. Así como las cuentas de CEDATOS, Consejo Nacional Electoral, la página de la Presidencia, Vicepresidencia y la Alcaldía de la capital por las diversas manifestaciones que se realizaban por las campañas electoras y la reelección del presidente Rafael Correa (El Telégrafo, 2011).

[15] Página Oficial de Anonymous Ecuador: https://twitter.com/anonecuador_?s=11

Además, para el 2019 en el periodo de Lenin Moreno, se efectúo el retiro del asilo político de Julian Assange que generó aproximadamente 17 millones de ataques cibernéticos hacia la infraestructura informática nacional como el Ministerio del Interior, el Banco Central, la Embajada de Ecuador en Londres y la página de la Presidencia (El Universo, 2019). Durante este proceso el colectivo publicó en sus redes videos en el que mencionaban: "Somos Anonymous y no olvidamos. Estamos hackeando el Gobierno ecuatoriano varios activistas del mundo entero", lo que corresponde como las frases más concurrentes del colectivo al iniciar con sus ataques cibernéticos (La Información, 2019).

En ese mismo año, durante el paro nacional existieron hackeos e intentos de bloqueos de las cuentas oficiales del movimiento indígena como las de Comunicación Confenaie, Conaie Comunicación, las cuentas personales de algunos actores políticos como la de Jaime Vargas y como describe Tapia (2019) "generaban información falsa, maliciosa y tergiversada". De la misma manera, existió un linchamiento mediático por la persecución que existía por parte del Gobierno a comunicadores y opositores políticos (Tapia & Castro, 2019).

Así bien, durante el 2020 los casos de corrupción del gobierno ecuatoriano a raíz de la pandemia por COVID-19 provocó que Anonymous publicará en redes sociales [16]información sobre el seguimiento y espionaje que manejaba las paginas gubernamentales en contra de opositores y actores políticos más cercanos al gobierno en páginas web como anonymousecuador.wixsite y telegra.ph/Moreno-Espinoaje, aunque no se asegura que sean las páginas oficiales de Anonymous en el Ecuador, de manera que carecen de una jerarquía y liderazgo, por sus ideales de trabajar de forma conjunta sin la necesidad de tener un líder que ejecute todas las acciones.

[16] La mayoría de las publicaciones ya no están disponibles. https://twitter.com/anonecop/status/366408875836051456?s=24

TABLA 1
ATAQUES DE ANOYMOUS EN EL ECUADOR-PERIODO PRESIDENCIAL DE RAFAEL CORREA

Año	Institución/Actor Afectada	Operación	Mecanismos y Argumentación
2011	-Presidencia del Ecuador. -Ministerio de Telecomunicaciones. -Policía Nacional. -Redes Sociales de Rafael Correa (Twitter) -Ministerio del Turismo. -CNT.	Operación Condor Libre #OpCondorLibre	Ataques DoS y DDoS. Inició su accionar el 10 de agosto por el día de la Independencia en el país. Rechazo de la sentencia emitida contra el diario El Universo por la censura de libertad de expresión. Con la página de la Policía Nacional publicaron los números de cédula y fechas de nacimientos de los funcionarios.
2012	-Municipios (Rocafuerte, Chone, San Vicente, Manta) -Ministerio de Telecomunicaciones. -Presidencia del Ecuador. -Asamblea Nacional.	Sin nombre específico	Ataques DDoS con suspensión temporal de las páginas. Rechazo por el interés de conocer las direcciones IP por los proveedores de servicios de Internet como una violación a la privacidad de los Internautas.
2012	Presidencia del Ecuador. Ministerio del Ambiente. Vicepresidencia del Ecuador. Ministerio del Telecomunicaciones, entre otras.	Operación Surkisha #OpInternetSurkisha	Ataques DDos mediante software #RefRef. Es la mayor intervención del colectivo con un total de 45 páginas gubernamentales suspendidas y colapsadas como rechazo a la Ley de Comunicación, explotación del Yasuní y sublevación policial del 30-S.
2013 2014 2015 2016 2017	-Presidencia del Ecuador. -Ministerio Coordinador de Conocimiento y Talento Humano. -Ministerio de Justicia; de Turismo; del Interior; de Cultura; de Deporte, Electricidad y Energía; de Agricultura; de Defensa; de Salud; del Ambiente; de Transporte y Obras Públicas; de Desarrollo Urbano y Vivienda. -Secretaria Nacional de Comunicación; de la Administración; de Gestión de la Política; y del Migrante. -Departamento de Informática.	#EcuadorHackingTeam	Ataques DDos y Dos. Campaña en contra de los partidos y actores políticos “corruptos” (Lucio Gutiérrez, Revolución Ciudadana, CREO)
		#OpFalsaRevolución	En contra de las reelecciones del partido de Rafael Correa y su mandato presidencial.

Fuente: El Universo (2012); El Telégrafo (2011); El Comercio (2014)
Elaborado por: Valeria Carvajal Artieda

TABLA 2
ATAQUES DE ANOYMOUS EN EL ECUADOR-PERIODO PRESIDENCIAL DE LENIN MORENO

Año	**Institución/Actor Afectada**	**Operación**	**Mecanismos y Argumentación**
2018	Ninguna institución visible afectada		
2019	-Ministerio del Interior -Banco Central -Embajada del Ecuador en Londres -Presidencia del Ecuador -Vicepresidencia del Ecuador	Liberen a Julian Assange	Ataques con DDoS y DoS desde todos Anonymous. Rechazo por el retiro del asilo político que mantenía Assange por el caso de WikiLeaks. Existieron al menos 17 millones de ataques cibernéticos de todo tipo hacia la infraestructura informática nacional.
2019	-Comunicación CONFENAIE -CONAEI Comunicación -Cuentas personales de dirigentes políticos (Jaime Vargas, Leonidas Iza) -Ministerio del Interior -Fuerzas Armadas -Policía Nacional	Paro Nacional	Sabotaje desde sistemas de inteligencia del gobierno hacia comunicadores y opositores políticos. Ataques DDoS y DoS por Anonymous Iberoamérica y Ecuador. Publicar información falsa, maliciosa y tergiversada con la suspensión de cuentas de políticos activos durante octubre.
2020	Redes Sociales de Lenin Moreno, actores y opositores políticos más cercanos al gobierno.	Espionaje de Lenin Moreno a: Patricio Mery Bell (periodista chileno) Julio Bueno y Patricio Celi (casos de corrupción) Guillermo Lasso y Jaime Nebot Gustavo Larrea Rafael Correa Fuerzas Armadas Inteligencia	Exposición en las redes de Anonymous Ecuador (anonymousecuador. wixsite, telegra.ph/Moreno-Espinoaje, @AnonEcuador, @AnonEcOp) casos de espionaje que mantenía el gobierno de Moreno con actores políticos y medios de comunicación.

Fuente: El Universo (2019); @AnonEc (Cuenta de Twitter), Tapia y Castro (2019)
Elaborado por: Valeria Carvajal Artieda

1.2.2. Estrategias y consecuencias de los ciberataques de Anonymous

La mayoría de los ataques efectuados se generan a través de DoS o DDoS que provocan que exista una saturación en los servidores de las instituciones y luego colapsen hasta que puedan corregir estos inconvenientes por medio de los protocolos establecidos en cada departamento (El Telégrafo, 2011). Sin embargo, la principal acción de Anonymous es hackear los sistemas para enviar mensajes en contra del gobierno con humor. De la misma manera, la creación de páginas en redes sociales y el uso de la cuenta de Twitter ayuda que los hackers difundan la información a través de publicaciones por la mediatización que pueden llegar a tener dentro del mundo digital. No obstante, la falta de regulación en materia cibernética permite incluso que los propios ataques se atribuyan a grupos que no necesariamente son colectivos hacktivistas, sino más bien las propias entidades estatales con fines únicamente políticos (Ecuavisa, 2017), ya que la legislación en materia de ciberseguridad y ciberdefensa en el Ecuador no se ha desarrollado de forma completa para este tipo de accionar, sino más bien ha tenido un enfoque de protección de datos informáticos a nivel de entidades públicas y privadas que lograremos identificar en los siguientes capítulos de la investigación.

1.2.3. Consecuencias de los ataques cibernéticos de Anonymous

Los activistas informáticos pueden realizar sus ciberataques con mayor precisión por lo que las medidas de seguridad disminuyen. Además, este tema involucra la discusión que existe sobre la privacidad de los datos e información y el accionar de los Estados tomando en consideración la seguridad (Lazár, 2018). En este marco, resulta importante mencionar que la soberanía que mantienen los Estados sobre su población, territorio y jurisdicción es diferente a la que existe en el ciberespacio, puesto que las regulaciones que se han efectuado por el sistema internacional involucran la creación de instituciones y normas para que no se encuentren solo en un Estado, sino que abarquen convenios e instrumentos relacionados con la accesibilidad de la información y delitos informáticos (Salinas, 2018).

De la misma forma, Mario Pazmiño -ex jefe de inteligencia militar y analista en geopolítica, seguridad y defensa- concibe que el Ecuador cuenta con instituciones que se encargan de los sistemas de ciberseguridad y ciberdefensa como las Fuerzas Armadas (Comando de Ciberdefensa); Policía Nacional (Comando de ciberseguridad), no obstante, el trabajo que realizan es de forma individual lo que provoca que las acciones no estén articuladas entre sí permitiendo la vulneración del sistema digital nacional (El Universo, 2019).

Este capítulo ha logrado en primer lugar, abarcar las actualizaciones que mantiene el activismo dentro de una era digitalizada por medio del uso de redes sociales como herramientas importantes para la participación de protestas o manifestaciones sociales. Por otro lado, logró posicionar al internet como un mecanismo digital importante para los hacktivistas, sobre todo para Anonymous como el colectivo informático más relevante dentro del sistema internacional. Además, ha establecido las nuevas amenazas y estrategias utilizadas por este colectivo con el objetivo de crear una aproximación directa de los hackeos a nivel internacional y doméstico demostrando su modus operandi como un elemento relevante para la estructura jurídica, política e institucional que mantiene el Ecuador.

Por lo tanto, con la evidencia de los hackeos a nivel internacional y doméstico, en el territorio ecuatoriano se mantiene la percepción sobre la falta de regulación en materia de ciberseguridad en las instituciones del Estado puesto que la presencia de este grupo no estatal transnacional refleja la posible vulnerabilidad de la infraestructura crítica del Estado, lo que conlleva a un análisis exhaustivo de las políticas públicas correspondientes a esta materia desde la perspectiva realista de las relaciones internacionales que se abordará en los capítulos siguientes.

CAPITULO II

ACTORES NO ESTATALES TRANSNACIONALES: PERSPECTIVA REALISTA DE LA SEGURIDAD INTERNACIONAL

El término de seguridad ha evolucionado durante los años siendo una parte fundamental de los debates que giran en torno a sus concepciones tradicionales y de la defensa. Sin embargo, el desarrollo de las tecnologías de la información y comunicación han transformado las estructuras sociales y políticas incluso abriendo la posibilidad de nuevas miradas teóricas y epistemológicas (Vargas, 2017).

Para comenzar y siguiendo la lógica del capítulo anterior es importante destacar el objeto referente de la seguridad desde las concepciones teóricas tanto del realismo como el neorrealismo en el que "la seguridad se relaciona principalmente sobre la integridad territorial del Estado" (Orozco, 2006). Sin embargo, las diversas interpretaciones teóricas del realismo nos permiten entender cómo es que los autores como Waltz (2000) y Mearsheimer (2001) comprenden a los actores no estatales transnacionales en la configuración del sistema y de la política internacional para el entendimiento de este caso de estudio.

2.1. Entendiendo el realismo en los estudios estratégicos de seguridad

Los estudios estratégicos fundamentan su enfoque mayoritario sobre la teoría realista de las Relaciones Internacionales, de esta forma, investigan el comportamiento estratégico de los actores políticos, pero tomando como prioridad a los Estados, lo que determina el paradigma estatocéntrico y realista en el que se ha configurado el sistema internacional (Jordán, 2015). En primer lugar, este paradigma realista se fundamenta a través de cómo se interpreta la realidad y desarrolla cuestiones claves para la teoría como: "causas de la guerra y las diferentes condiciones que se producen para alcanzar la paz, seguridad y estabilidad del sistema; la naturaleza del poder; unidades de análisis y actores; percepciones del mundo; y las características del sistema internacional" (Muñoz, 2013). Aun así, resulta insuficiente para

poder analizar los fenómenos que se presentan en el sistema internacional actualmente, de manera que la posibilidad de formular respuestas propicias a los problemas actuales se ve limitado, incluso se observa en la "incapacidad de los Estados por mantener un control efectivo de las fuerzas sociales con una creciente autonomía por los actores subnacionales, transnacionales, no gubernamentales" (Muñoz, 2013). Por lo tanto, para comprender la política internacional es importante profundizar sobre el estudio de las teorías realistas y asimilar de forma correcta los conceptos fundamentales que permiten diferenciar entre las corrientes y los puntos clave de convergencia.

2.1.1. Realismo Estructural (neorrealismo) de Waltz

Desde el punto de vista del realismo estructural o neorrealismo de Waltz (2000) se plantea tres niveles de análisis: individual, estatal y la del sistema internacional; sin embargo, direcciona su teoría a la estructura del sistema internacional, aun así no niega la influencia de los factores individuales y estatales (ideología, régimen político, racionalidad o irracionalidad de los actores) pero prefiere enfocarse en los supuestos que se dan en la estructura internacional ya que considera que tiene más influencia el comportamiento exterior de los Estados que su nivel doméstico. Por otro lado, Waltz (2000) entiende al sistema internacional como una estructura que se encuentra compuesta por unidades que convergen entre sí con una serie de principios como: el principio de ordenación (anárquico o jerárquico), carácter de las unidades (similares o diferenciadas) y la distribución de las capacidades (Jordán, 2015).

Por ende, su mayor aporte se desarrolla desde esta perspectiva anárquica del sistema internacional por la falta de una autoridad política a escala internacional que provoca a su vez que el interés nacional y el principio de autoayuda de los Estados desarrollen un comportamiento similar (Salinas, 2018). De esta forma, Waltz (2000) le asigna al Estado un rol principal ya que determina que "los Estados pueden usar la fuerza en cualquier momento y que los demás deben estar preparados o vivir a las expectativas de los otros." (pág. 11). De

manera que el neorrealismo -más allá de la interacción de los Estados- analiza cómo se posicionan frente a otros y logran determinar su poder relativo (Jordán, 2015).

2.1.2. Realismo ofensivo desde la mirada teórica de Mearsheimer

Ahora bien, los realistas ofensivos como Mearsheimer (2001) en la misma línea, explican que el sistema internacional es anárquico y al igual que Waltz (2000), afirman que no existe una autoridad central que pueda proteger a las potencias de las posibles amenazas; y que por lo tanto la supervivencia es el objetivo básico y principal de cualquier Estado. Aun así, las potencias persiguen otros intereses como el bienestar de sus ciudadanos, velar por la defensa de las amenazas siempre y cuando estas acciones impliquen la menor cantidad de costos y la mayor parte de beneficios en el marco de la seguridad nacional (Toft, 2005).

La perspectiva de Mearsheimer (2001) se centra directamente en las grandes potencias debido a la potencial influencia que mantienen sobre el sistema internacional, porque son estos Estados con suficiente poder militar aquellos dispuestos a enfrentarse en una guerra con la potencia más poderosa, para vencerla o debilitarla dentro del sistema, por lo que el incremento de poder que propicia una potencia crea temor o incertidumbre en el resto y la manera de garantizar su seguridad consiste en maximizar su poder relativo (Mearsheimer, 2001). Incluso las principales causas de la conflictividad internacional se derivan de la estructura del sistema internacional, pero es más probable desde un escenario multipolar, ya que beneficia a los desequilibrios del poder, los niveles potenciales de conflictos entre las grandes y pequeñas potencias; y también se dificulta predecir el comportamiento de los Estados y el cálculo de su poder (Jordán, 2015).

Sin embargo, el autor sigue centrando el rol del Estado como institución y principal actor de la política internacional y no prevé otros factores y actores distintos -como es el caso de los hacktivistas o las guerras mixtas- que en la actualidad se encuentran configurando el sistema internacional con los fenómenos actuales, limitando de forma estricta a los conflictos

vinculados solo con las guerras militares y territoriales que, si bien nos ayudan a comprender los límites del poder, le restan importancia a las nuevas herramientas que pueden remontar las guerras en un futuro como la constante actualización de las tecnologías de la información.

2.2. Aproximaciones conceptuales del ciberespacio, ciberseguridad y ciberdefensa

La creciente relevancia que se ha incorporado en el ciberespacio para las sociedades actuales y su escenario en disputa se ha convertido en una inquietud de seguridad nacional para los gobiernos, Estados y las Fuerzas Armadas a nivel mundial, ya que sus características poco detalladas determinadas por su naturaleza asimétrica e incluso como medio eficiente para la promulgación de delitos cibernéticos, espionaje, hackeos, etc. ha provocado que se convierta en un dominio atractivo para actores estatales, no estatales y demás en conflictos virtuales (Sigholm, 2013). De esta forma, es importante detallar como menciona Vargas (2017) que: "el concepto de seguridad se vincula con la concepción de confianza que se genera al estar libre de amenazas, daños o riesgos", y que, por lo tanto, debe brindar respuestas con sus condiciones para defenderse desde la estructura social y política del Estado-nación (pág. 30).

Por otro lado, la interacción que existe entre las personas con las computadoras, softwares, internet, redes sociales, redes de telecomunicación y la estrecha interdependencia entre estos sectores, impulsaron la creación del nuevo escenario virtual que "modifica constantemente las perspectivas de defensa y seguridad por la vulnerabilidad que representa para las estructuras civiles y militares" (Sigholm, 2013). Así bien, William Gibson (1984) es el primero en describir, en su obra Neuromancer[17] el término "ciberespacio" en el que menciona que integraba condiciones cibernéticas y del espacio con la finalidad de crear un nuevo campo de interacción (Choucri, 2012). De esta forma, comienzan las numerosas definiciones, concepciones y posibles elementos que determinan al ciberespacio.

[17]Novela de ciencia ficción que relata un mundo completamente desconocido en el ámbito virtual y que está controlado por entidades que no son los Estados necesariamente.

Por ejemplo, Richard Clarke y Robert K. Knake (2010) describen al ciberespacio como “las redes de computadoras mundiales que se conectan y logran controlar la información” (pág. 10). Aunque esta definición se limita únicamente a lo cibernético dejando de lado los nuevos paradigmas de las tecnologías como procesadores, softwares, etc. En cambio, Joseph Nye (2011) detalla al ciberespacio explicando que cuenta con una “infraestructura física que se relaciona con las leyes económicas, políticas de soberanía y competencia por recursos incluso para justificar su control y regulación” (pág. 19). A diferencia de otros escenarios, el ciberespacio maneja una ventaja de anonimato en sus actores, por lo que sus atacantes pueden realizar acciones dentro del dominio con un porcentaje mínimo de riesgo, lo que provoca que los Estados no tengan tanto interés en apoyar una definición que se vincule de forma jurídica para asumir la responsabilidad de los ataques cibernéticos ejecutados (Sigholm, 2013).

En ese sentido, la seguridad y supervivencia del Estado corresponden como los elementos supremos en el realismo clásico, lo que permite identificar que el interés nacional se vincula directamente con esta supervivencia y para cumplir estos objetivos, los Estados buscan maximizar su poder tal como lo menciona Mearsheimer (2001). Por lo tanto, esta perspectiva neorrealista permite abarcar la terminología del ciberespacio como un área estratégica similar a un espacio territorial, debido a la importancia que mantienen los intereses estatales, creación de conflictos, proyección de amenazas y vulnerabilidades que se encuentran asociados directamente con el manejo de la seguridad nacional del Estado. Incluso con el uso de la tecnología, se ven afectados por la dinámica tan cambiante en la que se encuentra el proceso estratégico de guerra (Quintero, 2014).

Ahora, para los autores de esta corriente teórica, el internet es un factor importante que amenaza la soberanía estatal y que se vincula de forma directa con estos colectivos por ser su canal principal al momento de ejecutar sus acciones cibernéticas, debido a que representa un

fuerte riesgo de desestabilización a la capacidad que mantiene el Estado soberano de controlar e intervenir cada uno de los acontecimientos políticos que se desarrollan dentro de sus fronteras (Pabón, 2019). Esto refleja el debilitamiento del poder soberano por los inconvenientes jurisdiccionales de los regímenes propios de cada país y las constantes disputas extraterritoriales; y tal como lo describe Rabinad (2008) la no existencia de fronteras geográficas permite la convergencia de diversos actores provocando conflictos al intentar establecer modelos bajo los cuales actúen y la búsqueda sobre quien debe recaer el control soberano, como el accionar de Anonymous a nivel internacional y doméstico.

Por ello, los problemas actuales dentro del campo de las relaciones internacionales deben avanzar en la búsqueda y análisis de soluciones para los nuevos fenómenos emergentes como el ciberespacio, ciberguerras, guerras mixtas, ciberterrorismo, entre otros; para entender, inclusive como los grupos no estatales e individuos se encuentran configurando la política internacional dentro de este espacio virtual (Vargas, 2017), ya que tanto las políticas públicas de cada país como las normativas a nivel internacional deben buscar trabajar de forma conjunta para tipificar mejor los delitos informáticos, como ha logrado ejecutar el Convenio de Budapest (2001) con los delitos de pornografía infantil, robo de información en la red o acceso ilícito y ataques a la seguridad del sistema (Sorbo, 2020) pero solo con los Estados que han ratificado este instrumento internacional.

Por otro lado, la presencia de organizaciones como la Organización Internacional de Policía Criminal (INTERPOL) o la Organización de las Naciones Unidas (ONU), entre otras, ayudan a incrementar el análisis de este tipo de crímenes permitiendo establecer los cambios que han tenido en la ciberdelincuencia, de manera que sus investigaciones ponen en manifiesto que existe un cambio sustancial en cada uno de sus ataques a nivel virtual, ya que antes se podían enfocar solo en empresas pequeñas y con distinciones en particular, pero en la

actualidad buscan objetivos más grandes como multinacionales, infraestructuras esenciales y administraciones estatales (Stock, 2020).

Entonces, se podría afirmar que el cuidado de las amenazas, riesgos y daños debería enfocarse tanto para un mundo virtual como para el real y de forma transversal, ya que la seguridad del ciberespacio no compone únicamente una necesidad individual, sino que se involucra directamente con la soberanía nacional y seguridad que determina la gobernanza nacional (Choucri, 2012). Incluso para autores como Erikson y Giacomello (2006) el Estado continúa con su rol principal en proveer seguridad a nivel del espacio físico como del ciberespacio. Por lo tanto, el Estado junto a las instituciones debe buscar la manera de enfrentar el reto que implica la seguridad y defensa del ciberespacio, incluso proteger y garantizar el acceso, uso y contenidos a la sociedad civil tomando en consideración las posibles repercusiones a nivel local, nacional y global. Además, el tratamiento de la información ha comenzado con nuevos hitos en el balance en el poder mundial entre los actores individuales, organizaciones públicas, privadas y Estados que han generado competencia por su control y aprovechamiento (Vargas, 2017, pág. 34), debido a que el sistema internacional al igual que el ciberespacio reflejan su característica anárquica por la falta de concordancia en la normativa internacional (Muñoz & Frasson, 2011).

Tomando en cuenta la información anterior y la vulnerabilidad que representa el ciberespacio para las personas y los Estados se acuña el término “ciberseguridad” que corresponde con el conjunto de políticas y acciones que se dirigen con el fin de “proteger activos de una organización y a la comunidad en general dentro del ciberespacio” (UIT, 2014). Asimismo, Vargas (2017) caracteriza al término con dos designaciones diferentes: desde un ámbito más estratégico y desde un lado operativo. La primera identifica la condición que presenta el ciberespacio como un lugar libre de amenazas, daños y peligros, mientras que

la segunda busca preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio (pág. 34).

Ahora bien, la ciberdefensa también se establece como término, pero orienta a las acciones de un Estado con el objetivo de proteger y controlar las amenazas o riesgos que implica la naturalidad cibernética. También autores como Cano (2010), la definen como "una connotación sistémica y sistemática que desarrollan los gobiernos para comprender las responsabilidades del Estado en el contexto ciudadano de fronteras nacionales electrónicas o digitales" (pág. 115). Considerando las definiciones anteriores, el ciberespacio por lo tanto promueve que los Estados revisen las estrategias y las agendas de seguridad en el contexto de defensa de la gobernabilidad (Cano, 2010). De la misma manera, necesita que se pueda analizar en un contexto nacional para establecer si es que este escenario virtual necesita de la militarización o puede resolver únicamente con políticas públicas que respalden la soberanía de cada Estado desde la perspectiva realista en la que se configuran las fuerzas del orden de los Estados.

2.3. Convergencia de los actores y los ciberataques en el nuevo escenario

Al analizar el papel que desempeña la ciberdefensa en el ámbito de la seguridad nacional, es importante categorizar a los actores que provocan que los Estados estén buscando estrategias y alternativas de protección, ya que al convertirse en un nuevo campo de batalla el ciberespacio abarca con nuevas acciones que se derivan del conflicto y recaen sobre este nuevo escenario. Es así como, en este caso de estudio se pretende responder si el Estado ecuatoriano en materia de ciberseguridad cuenta con políticas y estrategias de ciberseguridad que permitan responder, gestionar y prevenir estas amenazas efectuadas por actores no estatales como Anonymous dentro de este espacio virtual.

En primer lugar, es importante entender que los actores no estatales dentro de las teorías realistas son presentados como casos anómalos porque simplifican su realidad al

enfatizar ciertos factores dentro de la lógica estatocéntrica mientras ignoran los otros. Incluso son los factores estructurales como la anarquía y la distribución del poder los que toman más relevancia para explicar la política internacional, sin embargo, la teoría no toma en consideración estas cuestiones individuales o internas (Mearsheimer, 2001).

Para ello es importante, conocer cuál es la participación de los actores no estatales en los ataques cibernéticos. Por ejemplo, estos actores pueden realizar ataques de forma encubierta, utilizando los métodos de ataque adecuados que no impliquen muchos gastos, deciden cual es la duración y que efectos quieren provocar. Además, en el caso de que sean identificados -por la falta de legislación internacional que pueda señalar a las guerras cibernéticas o ciberataques- protege las políticas de los actores y crea un ambiente de ambigüedad legal (Sigholm, 2013).

Por ende, es muy importante que se cuente con programas que estén interesados en la ciberseguridad y ciberdefensa, puesto que en el momento menos pensado tanto los Estados como los grupos o individuos interesados en debilitar el poder estatal podrían vulnerar todo el sistema del país y causar perdidas de información, dinero, vulnerabilidad de las infraestructuras cibernéticas, incluso generar caos en la sociedad civil. Así, los Estados, organizaciones regionales, órganos de seguridad y defensa de las entidades estatales han comenzado a realizar cambios en sus estrategias para intentar contrarrestar las amenazas que tiene el ciberespacio y disminuir el impacto en todos los niveles (Vargas, 2017).

Acosta (2009) nos detalla algunos ejemplos de los actores que han incrementado políticas en cuestiones de ciberseguridad o ciberdefensa. Por ejemplo, Alemania en el 2011 crea el *Centro Nacional de Ciberdefensa y el Plan Nacional para la protección de Infraestructuras de Información* como una estrategia de seguridad cibernética; España por su lado, en el 2011 creó un *Centro y Plan Nacional de Protección de Infraestructuras Críticas* y en el 2013 un *Mando Conjunto de Ciberdefensa*. También países latinoamericanos han

efectuado políticas de esta índole, como Colombia que en el 2005 creo un *Grupo de Inteligencia para el análisis del ciberespacio* y en el 2011 la *Estrategia Integral para Ciberseguridad y Ciberdefensa* (Acosta, 2009).

También organizaciones han enfocado sus esfuerzos en generar modelos o estrategias para afrontar las amenazas que conlleva el ciberespacio para la ciberdefensa y ciberseguridad de los Estados como la Unión Internacional de Telecomunicaciones[18] que desarrolló un estándar como la *Guía de ciberseguridad para los países en desarrollo* (ITU, 2007) o el *National Cybersecurity Strategy Guide* (ITU, 2011) que baso su análisis en las capacidades, amenazas, riesgos de los sectores públicos y privados de los Estados para la construcción de una estrategia de ciberseguridad nacional (Vargas, 2017).

Aunque, estas propuestas no garantizan que los países se adapten a los modelos, por las diferencias que cuentan cada uno de los Estados en sus capacidades, infraestructura, gestión política y presupuestos lo que provoca que no se adapten de forma adecuada a los modelos señalados y sus acciones prevalezcan solo como referencias no aplicables en su totalidad. Al respecto, en Ecuador, se evidencia la imperativa necesidad de implementar alguna acción o capacidad estratégica que permita establecer un modelo propio y nacional de gobernanza para la ciberseguridad y defensa del ciberespacio por el incremento del uso de las TIC´s para la transformación en el desarrollo económico, producción y el bienestar de la población.

En ese sentido, Vargas (2017) destaca que dentro del Ecuador se genera un debate en relación con a la ciberseguridad y ciberdefensa desde estos conceptos fundamentales: Estado, seguridad, desarrollo y defensa. Por lo tanto, es imprescindible que se "incluya en la estrategia nacional de seguridad al ciberespacio y que se vincule con los distintos niveles de

[18] Organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras (Vargas, 2017)

toma de decisión e influya con las normativas y estándares nacionales e internacionales aplicables con los sectores e instituciones estratégicas del Estado" (pág. 38); a pesar de contar con una normativa legal en la materia y las instancias pertinentes para la reproducción de la norma no se ha determinado cuáles son los criterios técnicos y metodológicos del rol de los actores y su influencia en el uso de la tecnología, puesto que si "el Ecuador no trabaja en ciberseguridad de manera sistemática con políticas definidas y sin un plan de acción para las entidades del país, las decisiones en materia de ciberseguridad incurren únicamente en los administradores de sitios web" (Delgado, 2014).

Por lo tanto, desde la perspectiva neorrealista, los Estados deben orientar las políticas de defensa y seguridad de una forma pragmática por la presencia de estas nuevas amenazas y actores a nivel internacional identificados como anomalías, ya que la posición de un actor en el sistema se basa en el éxito que ha tenido para acumular poder determinado por sus capacidades materiales (Waltz, 2000). En ese sentido, la creación de un objetivo estratégico provoca que el Estado regule y controle al internet, y que de la misma manera busque construir nuevas doctrinas que tomen estos elementos para salvaguardar la integridad de la soberanía estatal, los intereses en la seguridad nacional y de su política exterior (Thompson, 2012). Así mismo, el ciberespacio resulta tan importante como los demás espacios de interacción que manejan las unidades del sistema internacional, pero sus características se diferencian del resto de espacios, ya que sale de esta concepción tradicional que tienen los Estados westfalianos de gobierno, territorio y población.

Del mismo modo, un aspecto primordial de esta teoría es que tipifica al poder en el ciberespacio como "ciberpoder" para identificar las acciones con el uso de recursos informáticos en este espacio virtual; aunque el ciberpoder no reemplaza al espacio geográfico ni anula la soberanía del Estado-nación, caracteriza su funcionamiento como un nuevo régimen que cuenta con componentes materiales y físicos que deben alinearse con el poder

estatal (Aguilar, 2021). Por ende, el dominio de las herramientas informáticas -que son esenciales para la comunicación y transmisión de la información- han logrado que Anonymous se expanda a través del ciberespacio a través de dos de sus capacidades básicas.

La primera, entendida desde el *hard power* con los ataques mediante denegación de servicio (DDoS) y web hacking a instituciones privadas y públicas como se ha desarrollado previamente, de manera que el colectivo logra causar daños materiales a las infraestructuras y así redireccionar las acciones posteriores en defensa de los actores. En segundo lugar, desde la concepción del *soft power*, Anonymous logró colocar en las agendas domésticas de los Estados el interés por los temas relacionados al ciberespacio y sus posibles amenazas, lo que provoca que a nivel interno existan debates por la reglamentación de estos nuevos escenarios (Thompson, 2012).

En ese sentido para un funcionario de las Fuerzas Armadas (2022) la ciberseguridad debe ser comprendida desde esta linera teórica realista, ya que la información en el ciberespacio surge como el "botín de guerra" que se emplea a favor de los aliados de quien la disponga o en contra de sus antagonistas como lo que sucedió con la información revelada por WikiLeaks en 2019, incluso la concepción del ciberespacio como parte de la nueva dimensión del campo de batalla permite la ejecución de la ciberguerra o de las guerras hibridas como lo que sucede con el conflicto entre Rusia y Ucrania, ya que el acceso a la tecnología es fundamental para una posible victoria, por la capacidad de recopilación de información, transmisión de la misma en tiempo real a través de medios seguros de inteligencia que sirven para la toma de decisiones en los centros de mando y control en todos los niveles: táctico, operacional y estratégico.

Este capítulo ha logrado describir las concepciones teóricas del realismo para el entendimiento de los estudios estratégicos de la seguridad que se relacionan con los nuevos escenarios en el que la seguridad se ve vulnerada por las amenazas externas a los Estados

actuales y cómo se interpreta dentro de la misma teoría a los actores no estatales puesto que no son tomados en consideración en el ejercicio de poder y supervivencia del paradigma estatocéntrico en el sistema internacional, también nos permite identificar sus limitaciones teóricas con estos nuevos actores en comparación al accionar de las entidades estatales pero a su vez, formula la posibilidad de exponer nuevos acercamientos para el entendimiento del ciberespacio, ciberdefensa y ciberseguridad.

Por otro lado, se ha analizado la importancia de la incorporación de estos fundamentos teóricos relacionados al ciberespacio y al actor no estatal transnacional Anonymous como elementos esenciales que nos va a permitir determinar en el próximo capítulo si las políticas públicas, estrategias, materia institucional y jurídica ha demostrado un avance y ha permitido contrarrestar o disminuir los ciberataques que han afectado la estructura de las instituciones estatales dentro del Ecuador durante el periodo de estudio del 2011 al 2020 con estas perspectivas neorrealistas por el supuesto interés de los Estados en articular este tipo de amenazas con sus propias políticas de defensa.

CAPITULO III

POLÍTICAS PUBLICAS Y AGENDAS DE POLÍTICA EXTERIOR EN EL MODELO ECUATORIANO DE CIBERSEGURIDAD

La adopción de tecnologías ha provocado conflictos en los mecanismos y herramientas de ciberseguridad en el Ecuador, aunque los ataques cibernéticos hacia el Estado se han efectuado en diferentes direcciones evidenciando la vulnerabilidad que mantienen las instituciones en esta materia como el sistema financiero, sistemas electorales, medios de comunicación, redes sociales de personajes públicos y el hacktivismo atribuido a Anonymous.

Por esta razón, el gobierno del Estado ecuatoriano ha buscado minimizar los problemas de esta materia y entre sus primeras iniciativas esta la creación del *Centro de Operaciones Estratégico Tecnológico* que tenía la finalidad de realizar monitoreos de los ataques informáticos hacia los equipos de seguridad de las instituciones públicas. También destacan la implementación de esquemas encargados de la protección y seguridad de la información perteneciente a las entidades públicas (Vargas, 2017), sin embargo, la relación que mantienen estas políticas inicialmente se refleja en la protección de datos y no en la protección del Estado ecuatoriano ante las posibles amenazas y riesgos que se pueden generar en el ciberespacio como lo revisamos con el caso del grupo hacktivista Anonymous, por lo tanto, la finalidad del capítulo será identificar como las políticas públicas han demostrado su efectividad o fracaso desde el 2011 al 2020.

3.1. Políticas de ciberseguridad en el Estado Ecuatoriano

La utilización de las tecnologías de la información y comunicación (TIC´s) y su relación directa con todas las actividades del Estado y demás actores de la sociedad provocó que exista una interdependencia entre el ciberespacio y estas herramientas tecnológicas, demandando un enfoque de seguridad integral [19]para las amenazas existentes o ataques cibernéticos

[19] Amplia a tres aspectos fundamentales: Estatocéntrico (Estado), antropocéntrico (ser humano) y biocéntrico (naturaleza) (Plan Nacional de Seguridad Integral, 2014, p.25)

comprendiendo que este nuevo panorama no tiene límite alguno puesto que está inmerso en la seguridad del Estado, del individuo y con ello afectando la infraestructura crítica del Estado (Leyva, 2021). De esta forma, Delgado (2014) explica que "el Estado ecuatoriano se ha estado adaptando a estas nuevas amenazas que se encuentran en el ciberespacio", incluso que el Ministerio de Defensa Nacional busca acciones que se relacionen con el desarrollo tanto de las capacidades operativas como políticas específicas por el bienestar y cuidado de la seguridad estatal y de la sociedad.

Por lo tanto, las políticas públicas del Estado deberían tener un enfoque orientado en el uso seguro de los sistemas de información mediante "el fortalecimiento de las capacidades de detección, prevención, análisis, defensa, investigación, recuperación y respuesta a los ciberataques" (Leyva, 2021), pero todo en función de una Estrategia Nacional de Seguridad Cibernética, ya que esto le permite identificar los procesos del cuidado de la información para que el Estado logre controlar y construir doctrinas que tome en consideración al Internet y ciberespacio, como elementos cruciales para amparar la integridad soberana, intereses, seguridad nacional y política exterior de los Estados (Aguilar, 2021). Ahora, es importante comprender que todos los Estados son susceptibles a los ataques cibernéticos, aunque esto se debe a una falta de regulación institucional (El Universo, 2019), que permita proteger la infraestructura critica del Estado o que a su vez exista un organismo que asuma de forma nacional el control de la seguridad cibernética siempre y cuando se trabaje de manera articulada con las demás entidades institucionales.

Así bien, es importante mencionar como se define a una política pública para continuar con el análisis del caso. En primer lugar, Roth (2009) define a una política pública como el "conjunto conformado por objetivos colectivos, medios y acciones considerados necesarios o deseables que son tratados por una institución u organización gubernamental con la finalidad de orientar el comportamiento de los actores para modificar una situación

percibida como insatisfactoria o problemática" (pág. 27). Por lo que, desde este punto de vista, las políticas públicas se entienden como el proceso que inicia el gobierno por la existencia de una problemática que altera la convivencia de todos los actores o miembros dentro de la sociedad.

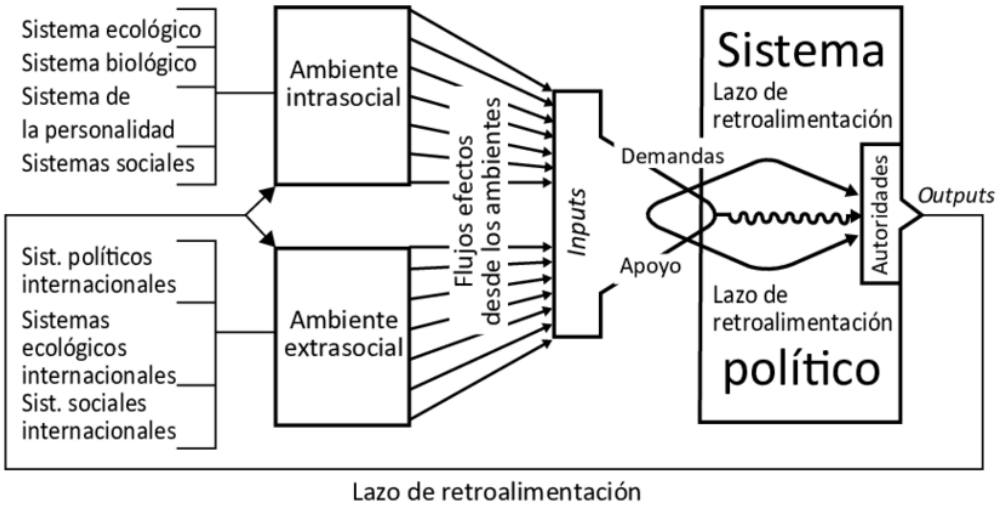
Por otro lado, Guerrero (2007) describe que "las políticas públicas ponen en manifiesto a la naturaleza y composición interna del sistema jerárquico de autoridades y el ejercicio de poder entre competencias y responsabilidades del poder institucionalizado", es decir, se comprende como la interacción entre el Estado y sociedad a través de los gobiernos como vías políticas (Leyva, 2021). Así es como, el tema institucional se presenta como prioritario para la implementación de la seguridad integral, por los cambios constantes que existen de las amenazas y los nuevos escenarios de seguridad y defensa, con lo que David Easton (1965) propone una serie de categorías de relevancia empírica para explicar la vida política como un sistema de conducta.

Easton (1965) considera que la vida política corresponde a un sistema de conducta que se logra incorporar a diferentes ambientes cuyas influencias logran modificar o alterar el mismo sistema político provocando una reacción frente a las mismas, lo que de cierta forma se logra entender como un sistema abierto por los tipos de intercambios que este sistema mantiene con el ambiente. Es así como, cada uno de los miembros del sistema pueden brindar una forma de respuesta ante estos intercambios y las determinantes a cualquiera de los procesos dinámicos. Ahora para poder identificar la evolución de las políticas públicas en materia de ciberseguridad -para este caso de investigación- Easton (1965) considera primordial comprender el ambiente del sistema político en intrasocietal y extrasocietal.

El ambiente intrasocietal se refiere a todos aquellos sistemas que pertenecen a la misma sociedad que el sistema político, comprendiendo así series de conductas, actitudes e ideas e incluso las fuentes de influencia que crean y dan forma de las circunstancias políticas,

como los sistemas sociales, de personalidad, etc. Por otro lado, el extrasocietal, conforma todos los sistemas que se encuentran fuera de la sociedad (sistemas políticos, sociales, ecológicos internacionales), estos parten como componentes funcionales de una sociedad internacional como suprasistema que se encuentra dentro de la sociedad individual (Easton, 1965).

IMAGEN 1
SISTEMA POLÍTICO DE DAVID EASTON



Fuente: David Easton (1965) A. Systems Analysis of Political Life

De esta forma, las nuevas connotaciones sistemáticas que deberían desarrollar los Estados para comprender sus nuevas responsabilidades en estos escenarios virtuales se enfocarían directamente con el cuidado de las fronteras nacionales, digitales o electrónicas, por la vulnerabilidad que representa para la infraestructura crítica de la nación (Cano,2013). Así, el análisis de Easton (1965) reflejaría la demanda efectuada desde estos ambientes en especial del sistema internacional, ya que el contexto de la evolución digital perpetua el proceso de inseguridad a nivel operacional y tecnológico. Por lo tanto, el Estado -como una caja negra y unidad de los sistemas políticos internacionales- debe buscar la forma de producir respuestas para continuar con el mejoramiento de su desarrollo interno, en este caso, con la formulación de estrategias de seguridad o políticas públicas vinculadas directamente

con las agendas de seguridad estatal, pero de forma articulada con cada uno de los miembros presentes en el sistema político.

Ahora bien, si nos referimos al ciberespacio, este corresponde como un territorio que debe ajustarse al dominio y control de las normativas jurídicas de cada uno de los gobiernos correspondientes para los Estados, por el nivel de amenaza que representan los ataques cibernéticos en el mundo virtual, lo que para un miembro de las Fuerzas Armadas (2022) toma gran importancia en el Estado ecuatoriano porque está considerado como parte de la seguridad nacional desde la *Política Nacional de Defensa* vigente desde el 2018, así como política de Estado mediante el *Acuerdo Ministerial Número 006-2021*. De esta forma, el objetivo principal es buscar una sincronía con el proceso de gobernanza de las tecnologías de la información, y del Internet (Choucri, 2013), e incluso con los procesos internos acordes al cuidado de la información y la infraestructura crítica del Estado en esta materia. Por otro lado, es importante entender como el Estado ecuatoriano a lo largo de los años ha respondido ante estos ambientes (societal y extrasocietal) y si estas demandas (inputs) de los miembros del sistema político lograron poner en evidencia los lazos de retroalimentación con las autoridades y poder constituir outputs dentro del sistema político. Así bien, el análisis de las políticas implementadas en materia de ciberseguridad es crucial para el entendimiento de este sistema político descrito por Easton (1965).

3.1.1. Descripción de las políticas públicas implementadas

La arquitectura de las políticas de defensa y seguridad se ha transformado de forma constante y con ello sus instituciones, el marco legal y las políticas, sin embargo, el Estado ecuatoriano carece en sí de la implementación de una Política y Estrategia Nacional de Ciberseguridad como tal. Dentro del marco legal de ciberdefensa del Ecuador, Salinas (2018) determina que los documentos normativos se establecen bajo dos objetivos principales. En primer lugar, se encuentra la designación de responsabilidades y funciones de las Fuerzas

Armadas y del Ministerio de Defensa Nacional con la creación del sistema de Ciberdefensa como el *Comando de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas*, y desde los cuerpos legales de la *Constitución de la República, Ley de Seguridad Pública y del Estado*; y la *Ley Orgánica de Defensa Nacional* (Salinas, 2018), normativa que se ha mantenido vigente con la mayoría de ataques efectuados por el colectivo y actor no estatal transnacional Anonymous en el periodo de estudio de esta investigación correspondiente al 2011-2020.

Por otro lado el enfoque desde la información como un activo que se protege en el contexto neto de la cibernética entendido desde la norma con *el Código Orgánico Integral Penal (COIP), Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y la Ley Orgánica de Telecomunicaciones (LOT),* que buscan principalmente mejorar las condiciones jurídicas en las que se encuentra la concepción de ciberdefensa del país (Salinas, 2018).

Con estos documentos correspondientes al marco legal en seguridad cibernética en el Ecuador, se pone en manifiesto que el proceso de creación de leyes y organismos ha sido paulatino, por el cual la gobernanza de internet logra la intervención de varios actores y sectores, sin embargo, los resultados se encuentran en las políticas, resoluciones, acuerdos, leyes, e instrumentos que por lo general son emitidos directamente por los Estados, aunque los resultados del marco jurídico en materia de ciberseguridad deben evaluarse según la capacidad de respuesta que han brindado las entidades estatales para los ataques cibernéticos que ha sufrido el Estado, gobierno y sociedad ecuatoriana, puesto que eso permite identificar si esta normativa y las consecuentes políticas públicas o proyectos de ley en el Legislativo han logrado contrarrestar y prevenir las amenazas existentes en los sistemas cibernéticos con el cuidado de la información de datos o con las nuevas amenazas en el ciberespacio.

TABLA 3

NORMATIVA INSTITUCIONAL DE SEGURIDAD DE DATOS E INFRAESTRUCTURA ESTATAL

ENFOQUES	**MARCO LEGAL**	**CARACTERÍSTICAS**	**ARTÍCULOS ESPECIFICOS**
Responsabilidades y funciones de las Fuerzas Armadas y del Ministerio de Defensa Nacional	Comando de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas Creada el 12/Septiembre/2014 bajo el Acuerdo Ministerial No. 281	Misión: Defender, explotar el dominio cibernético y responder ante incidentes o amenazas que atenten la infraestructura crítica digital de FF. AA y del Estado mediante operaciones de ciberdefensa.	----------
	Constitución de la República 2008	Establece y determina el rol de las Fuerzas Armadas que contribuye a la defensa de la soberanía estatal	Art. 158: "Las Fuerzas Armadas y la Policía Nacional son instituciones de protección de los derechos, libertades y garantías de los ciudadanos. Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial"
	Ley de Seguridad Pública y del Estado Registro Oficial: 28/Septiembre/2009 Última modificación: 09/Junio/2014	Esta Ley permite reconocer la importancia de la soberanía de la tecnología y los riesgos que derivan de las operaciones cibernéticas	Art. 2: "Se protegerá (…) en el ámbito de la seguridad del Estado la protección y control de los riesgos tecnológicos y científicos, la tecnología e industria militar (…)". Art. 43: "El ministro de Defensa Nacional (…) dispondrá a las

			Fuerzas Armadas, como medida de prevención, la protección de las instalaciones e infraestructura necesaria para garantizar el normal funcionamiento”
	Ley Orgánica de Defensa Nacional Registro Oficial 4-19/Enero/2007 Última modificación 28/Septiembre/2009	Determina las misiones de los órganos de la defensa nacional, establece su organización y fija sus atribuciones, así como la relación de mando y subordinación de sus componentes	Art. 3: “Las funciones constitucionales, en los aspectos político-administrativos, las implementará el Ministerio de Defensa Nacional; y, los aspectos militar-estratégicos, el Comando Conjunto”
Información como activo protegido en la cibernética	Código Orgánico Integral Penal Registro Oficial: 10/Febrero/2014	Normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso. Además, se aproxima a las amenazas de los ataques cibernéticos	Sección Tercera: Delitos contra la seguridad de los activos de los sistemas de información y comunicación. Art. 229: Revelación ilegal de base de datos Art. 230: Interceptación ilegal de datos Art. 231: Transferencia electrónica de activo patrimonial Art. 232: Ataque a la integridad de sistemas informáticos

			Art. 233: Delitos contra la información pública reservada legalmente Art.234: Acceso no consentido a un sistema informático, telemático o de telecomunicaciones
	Ley Orgánica de Transparencia y Acceso a la Información Pública Registro Oficial 18/Mayo/2004	Garantizar el derecho de la ciudadanía al acceso de la información, considerado como un modelo de participación democrática y se dirige a los funcionarios y organismos del Estado. Archivos públicos accesibles con excepción de información que se encuentre clasificada como reservada o confidencial por temas de seguridad nacional	Art. 2: d.) Garantizar la protección de la información personal en el sector público/privado. e.) La democratización de la sociedad ecuatoriana y la plena vigencia del estado de derecho, a través de un genuino y legítimo acceso a la información pública; y, f.) Facilitar la efectiva participación ciudadana en la toma de decisiones de interés general y su fiscalización.
	Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Registro Oficial 17/Abril/2002	Establece que los mensajes de datos tienen un valor jurídico similar a los documentos escritos (art. 2). Importancia establecer herramientas jurídicas que reconozcan que el acceso y el uso de los servicios electrónicos se deben realizar en un entorno seguro	Art.1: “Esta ley regula los mensajes de datos, la firma electrónica, los servicios de contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información como el

			comercio electrónico y la protección a los usuarios de estos sistemas".
	Ley Orgánica de Telecomunicaciones Registro Oficial 18/Febrero/2015	Dispone del derecho de administrar, regular y controlar los sectores estratégicos de telecomunicaciones para emitir políticas públicas, planes y normas técnicas nacionales de cumplimiento en todos los niveles del gobierno.	Art. 1: "1 Desarrollar el régimen general de telecomunicaciones y el espectro radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajo los principios y derechos constitucionalmente establecidos"

Fuente: (Constitución del Ecuador, 2008) (COIP, 2014) (Ley de Seguridad Pública y del Estado, 2009) (Ley Orgánica de la Defensa Nacional, 2007) (Ley de Comercio Electrónicos, Firmas y Mensajes de Datos, 2002) (Ley Orgánica de Telecomunicaciones , 2015) (Salinas,2018).

Elaborado por: Valeria Carvajal Artieda

3.1.2. Iniciativas de ciberseguridad en los gobiernos ecuatorianos

Durante el periodo presidencial de Rafael Correa, el *Plan Nacional de Seguridad Integral 2011-2013* fue uno de los proyectos destacados por el nuevo enfoque de seguridad, en él se ejecuta la inclusión de ocho agendas [20]orientadas a los Ministerios y Secretarias del sector de seguridad, entre las cuales destaca la Agenda Estratégica de Política Exterior y la de Defensa para este análisis de caso. Este enfoque se centra en el bienestar del ser humano, como centro de las políticas de seguridad, estrategias y acciones, aun así, se encuentra en la obligación de definir los nuevos retos que afronta la sociedad en materia de justicia, seguridad nacional,

[20] Agenda Estratégica de Política Exterior, Agenda de Seguridad Ciudadana y Gobernabilidad, Agenda de Política de Defensa; Agenda de Justicia, Derechos Humanos y Cultos, Agenda Política de Gestión de Riesgos, Agenda Nacional de Inteligencia, Agenda de Plan Ecuador y Seguridad Vial

inteligencia, prevención y respuesta, etc. Esta visión multidimensional de la seguridad incluye tanto a las amenazas tradicionales como a las nuevas amenazas, sus propias preocupaciones y otros desafíos de la seguridad (Ministerio de Coordinación de Seguridad, 2011), por lo tanto, determina las secciones que inician las estrategias y amenazas en el ámbito tecnológico y científico, aunque no analiza de manera profunda los temas relacionados con la defensa, seguridad y gobernanza tanto del internet como del ciberespacio (Salinas, 2018).

Por otro lado, el *Plan Nacional de Seguridad 2014-2017*, dentro del mismo periodo presidencial manifiesta los primeros acercamientos con los debates sobre ciberseguridad, ciberataques, ciberdefensa y las nuevas aproximaciones conceptuales a las guerras cibernéticas. Es así como menciona que la defensa -como un componente de la seguridad- tiene que ver con la acción de protegerse o resguardarse ante una agresión, ya sea desde el ámbito externo o interno; pero para defender al Estado, a sus instituciones y sus ciudadanos, las Fuerzas Armadas se preparan para prevenir un conflicto, o para reaccionar si existe un ataque o agresión (Plan Nacional de Seguridad, 2014); y a diferencia del Plan de Seguridad Integral, se enlaza la ampliación y operatividad del concepto seguridad integral con las instituciones que conforman el Consejo Sectorial de Seguridad [21].

Ahora, desde el periodo presidencial de Lenin Moreno, con el *Plan Nacional de Gobierno Electrónico*, se buscaba crear iniciativas que permitan el fortalecimiento de las TIC's en el Ecuador desde el *Plan Nacional 2018-2021*, de manera que las principales decisiones se enfocaban en la gestión del Esquema Gubernamental de Seguridad de la Información (EGSI) junto al Centro de Respuesta ante incidentes informáticos (EcuCERT) con la incorporación de la tipificación de delitos informáticos en el Código Orgánico Integral Penal. En ese sentido, este plan buscaba concientizar sobre la importancia de la

[21] Organismo de la Función Ejecutiva que contiene instituciones relacionadas con la seguridad y, aprueba políticas sectoriales e intersectoriales (Plan Nacional de Seguridad, 2014)

ciberseguridad en las instituciones gubernamentales para que puedan ser incorporados como objetivos planteados a nivel nacional (Heredia, 2021).

3.2. Una nueva agenda de políticas públicas

Por otro lado, es importante entender que los hackeos en el sistema crítico de la información del Estado se han visto afectados notoriamente por la falta de regulación cibernética a nivel doméstico e internacional, aunque en los periodos del 2011 al 2020 el marco legal descrito no ha logrado controlar estas amenazas que considera el Estado como importante. Aun así, es en el 2021 cuando se comienzan a ejecutar las políticas públicas en esa materia.

Para un funcionario de las Fuerzas Armadas (2022), es fundamental que el Ecuador presente una política clara en este tipo de campo, ya que podría generar las reformas necesarias a las leyes para tipificar de mejor manera este tipo de infracciones, facilitar la obtención de recursos, obtener apoyo internacional y capacitar al personal técnico que tengan estas responsabilidades en los ámbitos públicos y privados, siempre cuando el desarrollo de las leyes en esta materia sean debidamente priorizados.

De esta forma, el proyecto de *Ley Orgánica de Seguridad Cibernética*[22], presentada por el asambleísta José Serrano, corresponde como el primer proyecto que se intenta por la importancia que se le atribuye a la creación de un organismo institucional doméstico que logre controlar, analizar y responder a las amenazas que se encuentran en el ciberespacio, pero trabajando de forma articulada con las demás instituciones del Estado ecuatoriano. De manera que, la creación de un nuevo órgano que se vincule con las demás instituciones del país requiere la modificación del presupuesto del Estado lo que incurre en un Gasto Público que solo podría solicitar el presidente de la República (Serrano, 2021). En ese sentido el funcionario de las Fuerzas Armadas (2022) considera importante que tomando en cuenta los ejemplos de los otros países, la ciberseguridad -como un tema de seguridad del Estado- debe

[22] Presentado el 10 de mayo del 2021 y actualmente se encuentra en trámite de revisión en el Consejo de Administración Legislativa.

contar con una respuesta interagencial ante estas vulnerabilidades y amenazas, es decir, un Centro que fusione las capacidades que al respecto están desarrollando el Centro de Inteligencia Estratégico, Ministerio de Telecomunicaciones y Sociedad de la Información, Fuerzas Armadas con su Comando de Ciberdefensa, Fiscalía General del Estado y Policía Nacional con sus unidades especializadas e incluso el apoyo de la academia.

Ahora, el Estado ecuatoriano según las perspectivas de Easton (1965) no ha podido comprender el ambiente societal y extra societal (sistema internacional) organizaciones internacionales, contexto, ambiente (desarrollo de la tecnología) ya que existe a nivel de Estado una caja negra (input) que permita establecer las demandas para la creación de políticas públicas (output) y ahí radica el problema, porque no existe un verdadero lazo de retroalimentación, y tal como lo describe el Funcionario de las Fuerzas Armadas (2022) aún existen bases de datos con información sensible de los usuarios y entidades estatales que presentan casos de robos o de ventas ilegales, como los ataques a los servidores y redes de entidades como el Banco del Pichincha que presentó problemas en sus plataformas digitales y aplicaciones móviles durante el 2021 y 2022, u otras instituciones como la Agencia Nacional de Tránsito (ANT), Municipio de Quito, etc.

En ese sentido, las acciones ejecutadas por el grupo no estatal trasnacional Anonymous a nivel internacional se ven reflejados a medida que encuentran la forma y mantienen la capacidad de controlar los sistemas operativos de sus objetivos específicos como las instituciones estatales, aun cuando esto no signifique que puedan tener control total para cambiar las reglas establecidas, aunque los Estados consideren poner en consideración estos temas en específico, la visibilidad del colectivo se ve presente en relación con sus ataques cibernéticos a lo largo del ciberespacio (Thompson, 2012). Sin embargo, al encontrarse estas amenazas en el ciberespacio los Estados tienen la obligación de ejecutar acciones inmediatas por la velocidad con la que se generan las operaciones dentro de este entorno (Mogollón,

2021). Así bien, el Ecuador cuenta con algunas herramientas para contrarrestar estos ataques cibernéticos -que no significan que sean exitosas- a nivel privado se enfocó principalmente en la banca y algunos servicios industriales, y a nivel estatal aún mantienen falencias que comienzan desde la concepción de las acciones virtuales en su enfoque dentro del marco jurídico y la falta de personal técnico y medios que les ayude a fortalecer los departamentos de delitos informáticos o la Unidad de Delitos Cibernéticos de instituciones como la Fiscalía General del Estado, Policía Nacional, entre otros, aunque estos primeros acercamientos son pasos importantes para contrarrestar los ataques cibernéticos, aun no permiten una cobertura total de la infraestructura crítica del país que tampoco ha logrado una total automatización y digitalización (Fuerzas Armadas, 2022).

No obstante, a pesar de que el Ecuador ha gestionado en sus enfoques de seguridad y defensa políticas públicas que abarquen estas nuevas concepciones desde la seguridad integral, aun no mantiene un marco normativo específico de ciberdefensa que pueda articular el accionar de las instituciones estatales frente a estas amenazas digitales y la relación que manejan con otros organismos para que sus funciones no colapsen (Mogollón, 2021), ya que en la actualidad los Estados modernos visualizan la generalidad del problema o del fenómeno para adoptar las medidas que están a su alcance para proteger su información sensible, sin enfocarse directamente en el colectivo, grupo o individuo (Fuerzas Armadas, 2022), aunque esto pueda significar una falencia que presentan al concebir las estrategias de cuidado y protección de la información por este enfoque general, de tal manera que dejan de lado las características de los actores, motivaciones o incluso sus potenciales ataques a futuro.

Por otra parte, la Asociación Ecuatoriana de Ciberseguridad (AECI), con su estudio planteado durante los primeros seis meses del 2020 identificó que el Ecuador mantenía riesgos relacionados con la falta de regulación, dedicación y gestión directa del manejo de ciberseguridad en las empresas o instituciones tanto públicas y privadas, como también reflejó

que los ataques más frecuentes que recibían las instituciones corresponden con pishing[23] y software espía [24] (Heredia, 2021). Aunque el Estado ecuatoriano comenzó a sancionar los delitos informáticos desde el año 2009, no se ha realizado una actualización del marco jurídico provocando que algunos delitos queden impunes por la falta de regulación.

Desde otra perspectiva el *Acuerdo Ministerial 006-2021* en el que el Ministerio de Telecomunicaciones aprueba la *Política Pública de Ciberseguridad* establece directrices que buscan afianzar este nuevo dominio del ciberespacio y así contribuir al desarrollo económico, social y humano del país. En ese sentido el experto -en derecho informático- Santiago Acurio (2021) menciona que la ciberseguridad debería ser comprendida como la capacidad del Estado, empresas, industrias, academia y ciudadanos para protegerse a sí mismos (bienes, información, demás servicios) de las amenazas y riesgos que se encuentran en el ciberespacio, puesto que los gobiernos del país solo han enfocado al Estado como el único actor con la posibilidad de protección, e incluso como coordinador para los demás actores a nivel doméstico. Por lo tanto, Acurio (2021) afirma que esta protección debería ser a nivel de país y no solo con un enfoque estatista de la ciberseguridad.

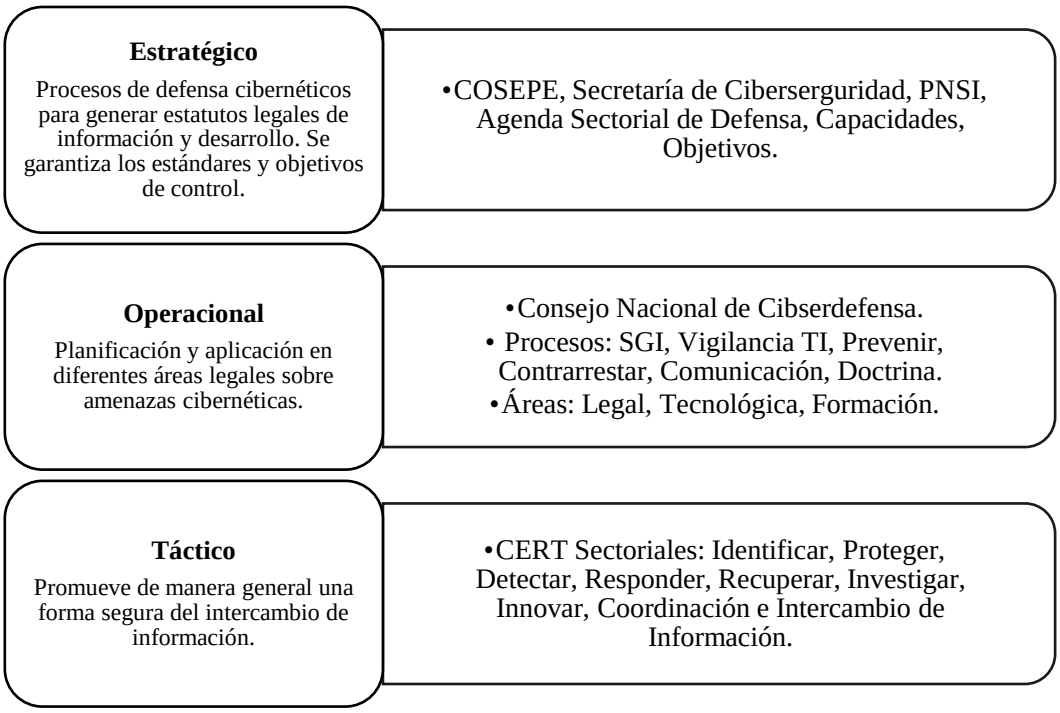
3.2.1. Ataques de Anonymous y la normativa vigente

El Ecuador carece de la formulación de políticas y estrategias nacionales en el ámbito de la ciberseguridad que deberían fortalecerse o mejorarse, aunque las organizaciones e instituciones deberían plantearse estas responsabilidades bajo tres niveles para permitir la jerarquización y direccionamiento de la ciberdefensa y ciberseguridad en el Ecuador (Vargas, 2017), puesto que el debate que gira en torno a la ciberseguridad y ciberdefensa en el país debe enfocarse desde sus conceptos fundamentales correspondiente al Estado, su seguridad, y el desarrollo y defensa, para que las estrategias y políticas influyan en cada uno de los niveles

[23] Estafa que busca obtener información a través de internet de los datos privados de los usuarios para acceder a sus cuentas bancarias.
[24] Programas que se encuentran en las computadoras para recopilar información y enviar a terceros, sin que los usuarios tengan constancia

de decisión y se encuentren involucrados con los demás sectores estratégicos. Así, estos niveles son: político estratégico (se elabora las políticas y objetivos de ciberseguridad como de ciberdefensa), operacional (planificación total), y el táctico (respuesta a los ciberataques o incidentes).

FIGURA 1
JERARQUIZACIÓN ESTRATÉGICA DE LA CIBERSEGURIDAD Y CIBERDEFENSA



Fuentes: Pirámide Organizacional de Ciberdefensa (Vargas, 2017)

Los análisis y resolución de estos conflictos permiten abordar y establecer cada uno de los objetivos correspondientes de seguridad derivados de las necesidades nacionales, a partir de los tres niveles establecidos por Vargas (2017) para que exista un balance entre el flujo de la información y la seguridad de los sectores públicos, privados y de la sociedad ecuatoriana, ya que la formulación de una Secretaria de Ciberdefensa permitiría coordinar las actividades en este ámbito con cada sector a nivel doméstico e incluso con otros países y entidades regionales internacionales.

Por ende, los ataques de Anonymous deberían estar vinculados en las iniciativas propuestas de estrategias de implementación de ataques cibernéticos y utilizar estándares de

ciberseguridad y ciberdefensa para minimizar los riesgos y tener prevención de estos, ya que desde los ataques efectuados en el 2011 se han intentado regular bajo un marco normativo tradicional tomando en consideración únicamente a la Constitución de la República del 2008, Ley de Seguridad Pública y del Estado, Ley Orgánica de Defensa Nacional, Código Orgánico Integral Penal, Ley Orgánica de Transparencia y Acceso a la Información Pública; y Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, lo que evidencia hasta el 2020 no se han creado normativas que permitan la regulación de estos ciberataques, a excepción de la creación de la Ley Orgánica de Telecomunicaciones en 2012 y el Comando de Ciberdefensa en 2014, que de igual manera no han logrado contrarrestar todos los delitos informáticos o cuidar la infraestructura del Estado.

Aunque, a nivel internacional algunos países han alcanzado un avance mucho más rápido en cuanto a sus capacidades en contra de las amenazas cibernéticas, los demás países -como el Ecuador- se han visto en la necesidad de adoptar o replicar, como parte de su funcionamiento interno de políticas públicas, las acciones que han sido efectivas de los modelos de los otros Estados (Mogollón, 2021) aunque el Ecuador no exponga en sus documento oficiales o en la ejecución de las políticas si tiene como base un modelo de alguna organización en específico o de otro Estado, de tal manera que un proceso de cooperación internacional e intercambio de información con un país u organización con experiencia en ciberdefensa y ciberseguridad, permitiría la creación de una política clara en este tipo de campo para generar las reformas necesarias a las leyes y tipificar de mejor forma las infracciones relacionadas, ya que el acceso no autorizado a los sistemas tecnológicos y de información por parte de individuos, organizaciones -como Anonymous- e incluso Estados rivales suponen una afectación directa a su propia supervivencia dentro del campo de la defensa nacional (Fuerzas Armadas, 2022).

TABLA 4
RELACIÓN DE LOS ATAQUES CON LA LEGISLACIÓN

NORMATIVA/ ORGANISMO	OBJETIVO	ATAQUES DE ANONYMOUS	FALENCIAS EN LA NORMATIVA
2011-2012 Ley Orgánica de Telecomunicaciones Publicado en el Registro Oficial No.439.	Desarrollar el régimen general de telecomunicaciones y del espectro radioeléctrico, como sectores estratégicos del Estado en beneficio de los ciudadanos. Además, de fortalecer la estructura institucional y los procesos de regulación y control.	#OpInternetSurkisha (2012) #EcuadorHackingTeam (2013-2015) #OpFalsaRevolución (2016-2017)	-Se trata a todos los riesgos estipulados en la normativa jurídica de la misma manera y no hay prioridad a aquellos que afectan más a los sistemas estratégicos estatales. -La norma busca la protección de los datos, pero no se ha evidenciado el fortalecimiento de la estructura institucional.
12 de septiembre de 2014 Acuerdo Ministerial 281 Comando de Ciberdefensa del Comando Conjunto de las FF.AA.	Proteger y defender la infraestructura crítica e información estratégica del Estado	#OpFalsaRevolución (2015) Liberen a Julian Assange (2019) Paro Nacional, Sabotaje de sistemas de inteligencia Espionaje a Lenin Moreno (2019)	-Falta de continuidad de los procesos para la protección de datos e infraestructura del Estado. -No hay seguimiento de las acciones en iniciativas como el Comando de Ciberdefensa.

Fuente: (Pautasio, 2014), (Vargas, 2017), (Ley Orgánica de Telecomunicaciones , 2015) (Mogollón, 2021)
Elaborado por: Valeria Carvajal Artieda

Ahora, la creación de una estrategia nacional de seguridad implica un direccionamiento en conjunto con el marco legal principal del país que es la Constitución de la República del 2008, puesto que como estipula el artículo 16 de esta norma, el acceso de las tecnologías de la información es para los ecuatorianos un derecho humano. Por lo tanto, los nuevos proyectos que se puedan plantear desde el poder legislativo deberían buscar que se efectúe una verdadera política pública de ciberseguridad, como lo que sucede actualmente con

el *Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos*; y el *Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia* que se encuentran -desde el 2021- en la Comisión de Soberanía, Integración y Seguridad Integral para su revisión y posterior debate.

El presente capítulo se centró en analizar los ataques cibernéticos efectuados con el grupo no estatal transnacional Anonymous y evaluar el desarrollo jurídico de la normativa vigente que se relaciona con la materia de ciberseguridad en el Estado. Así mismo, se detalló la metodología planteada por David Easton (1965)al explicar el sistema político como un sistema de conductas que permite la identificación de la falta de entendimiento de los ambientes hacia la caja negra del Estado para brindar respuestas a las demandas adquiridas por cada miembro del sistema por las amenazas que representa para el Ecuador los grupos no estatales como Anonymous y su participación e influencia en el nuevo dominio virtual.

De la misma manera, se efectúo un análisis relacionado a los proyectos de ley más importantes que contienen la protección de datos por la propagación de la información desde el desarrollo de las tecnologías de la información y cuales han sido los ataques del grupo no estatal transnacional Anonymous desde la implementación de normativas e instituciones encargadas del cuidado y la protección del Estado como de la información de la sociedad ecuatoriana. Finalmente se establece un breve acercamiento de los proyectos de ley que se encuentran en la Asamblea Nacional que cuentan con ámbitos de ciberseguridad, ciberdefensa y ciberinteligencia.

IV. CONCLUSIONES

El análisis de la presente investigación plantea que la hipótesis, el hackeo y hacktivismo realizado por el grupo no estatal transnacional Anonymous en el Ecuador durante el periodo del 2011 al 2020, tuvo como consecuencia develar la falta de políticas y estrategias de ciberseguridad en el Estado y gobierno del país, se cumple de forma parcial; debido a que el Ecuador si bien es cierto no cuenta con un modelo de ciberseguridad establecido que permita el cuidado y protección de la información sensible tanto del Estado como de sus ciudadanos e infraestructura crítica, mantiene algunas iniciativas que permiten una respuesta a nivel jurídica y tecnológica para los ataques cibernéticos, aunque existen muchas debilidades y vacíos en el establecimiento de la norma que impiden un accionar completo alrededor de las nuevas amenazas tecnológicas, ya que Anonymous no es el único actor que vulnera la ciberseguridad del Estado. De esta manera, se presenta las conclusiones obtenidas de la presente investigación que detallan lo siguiente.

La aproximación de los términos de ciberespacio, ciberdefensa y ciberseguridad cuentan con una problemática interna por su variable no física al ser analizados. Por lo tanto, desde la visión realista de las relaciones internacionales, estos términos se asocian con sus postulados políticos y militares, ya que este nuevo campo de batalla toma en cuenta que su botín o principal objeto de guerra es la información que puede vulnerarse. Por otro lado, el término ciberdefensa maneja una visión exhaustiva del poder. Aunque, las amenazas presentes en ambos casos no se efectúen únicamente desde los Estados, el realismo los enfoca como una forma de manejar un espacio soberano mediante el uso del poder, similar al espacio territorial.

El ciberespacio brinda una dimensión importante para el análisis de la distribución del poder aun cuando a nivel doméstico e internacional no se aborda a cabalidad, ya que, con la incorporación de nuevos actores en el sistema internacional, los Estados deberían enfocarse en

la formulación de políticas que tomen en consideración herramientas cibernéticas, amenazas virtuales, actores no estatales, organizaciones internacionales, instituciones privadas y públicas para un accionar interagencial. De la misma forma, los ciberataques cobran importancia a nivel internacional por la coyuntura en la que aparecen. Anonymous ha enfocado sus acciones en contra de entidades gubernamentales, organizaciones internacionales o locales, desarticulando por momentos su funcionamiento mientras propagaban información para expandirse en el ciberespacio y fuera de él.

Ecuador ha enfocado su esfuerzo en implementar políticas de protección de datos, pero requiere un modelo de gobernanza que se enfoque en la ciberseguridad y ciberdefensa de forma integral para brindar soluciones globales a largo plazo, ya que si bien es cierto cuenta con un marco jurídico, aún existen limitaciones por la naturaleza cambiante que representan estos nuevos actores y amenazas, que incluso dejan de lado nuevos delitos informáticos para posibles sanciones y tipificaciones. Así bien, la teoría neorrealista permite articular las estrategias de defensa de los Estados con los procesamientos en los nuevos dominios, por su relación al ciberespacio como un nuevo modelo de territorio físico que debe garantizar la soberanía del Estado.

Es importante reconocer que el Estado ecuatoriano debe definir qué corresponde como infraestructura crítica, con ello la problemática de seguridad vinculada al ciberespacio con los ciberataques no se concentraría únicamente en un análisis técnico, sino más bien incluye la reflexión de que dichos ataques no solo tienen repercusión a nivel virtual, sino implican analizar las consecuencias generadas en el mundo real y en la sociedad ecuatoriana, puesto que este fenómeno como Anonymous se encuentra en todos los países del mundo, lo que abre la posibilidad de buscar un fortalecimiento a nivel tecnológico a partir de las experiencias de países del exterior que puedan contribuir con el formulación de estrategias y políticas en el país.

La perspectiva neorrealista pone en evidencia el problema que manejan las instituciones encargadas de la protección del Estado, ya que la rigidez con la que maneja el concepto de poder en esta línea teórica supone una debilidad constante a la hora de explicar estas nuevas amenazas y nuevos actores que se encuentran constantemente en el ciberespacio, ya que el Estado sigue siendo la unidad principal de análisis y no permite abarcar de forma detallada a las demás partes que están en disputa por el control del internet, debido a que en el ciberespacio la agencia de estas unidades se vuelve relativa porque el ciberpoder puede proceder de diferentes fuentes y ya es una cualidad exclusiva del Estado.

Finalmente, Anonymous al ser un colectivo que no cuenta con una jerarquía establecida como los grupos activistas tradicionales, representa una amenaza real para los Estados y cualquier entidad o actor político que decida restringir los derechos de libertad de expresión, incluso manipular la información para su conveniencia, aunque no se hay tipificado como una amenaza directa, se entiende que toda persona u organización que intente acceder ilegalmente a datos sensibles o restringidos del Estado ecuatoriano para poner en peligro la estabilidad política, social y económica del país, reúne los requisitos de una amenaza.

V. RECOMENDACIONES

1. El Ecuador por las limitaciones y falta de regulación, debería enfocar sus esfuerzos en la búsqueda de un apoyo internacional con naciones que han manejado políticas de ciberseguridad y ciberdefensa, que le puedan servir como referencia para materializarlo a nivel interno, con el fin de desarrollar un proceso conjunto en contra de las amenazas cibernéticas, tomando en consideración las características anárquicas y transfronterizas del ciberespacio.
2. El Estado ecuatoriano debería plantearse una entidad u organismo que busque articular las acciones de cada una de las instituciones encargadas del cuidado del Estado, para una convergencia coherente en materia de ciberseguridad y cualquier otro ámbito que se pueda ejecutar, pero como una propuesta inmersa en el Plan Nacional del Gobierno para que las instituciones como Fiscalía General del Estado, Ministerio de Defensa, Ministerio del Interior, Fuerzas Armadas, Policía Nacional, Presidencia de la República, se articulen y fusiones sus esfuerzos en el cuidado de estas amenazas virtuales.
3. Fortalecer las investigaciones desde la academia e instituciones involucradas con el cuidado de la protección de datos y amenazas virtuales, para que de esta forma se canalice las operaciones e iniciativas de los poderes del Estado, sector público y privado, organizaciones no gubernamentales, organizaciones gubernamentales y sociedad civil que permitan identificar aspectos esenciales de la ciberseguridad y ciberdefensa para prevenir ataques por actores no estatales o cualquier otra entidad o actor que vulnere la información sensible del Estado.
4. El Estado ecuatoriano debería analizar la posibilidad de ratificar el Convenio sobre ciberdelitos cibernéticos o Convenio de Budapest, al ser el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en internet

a través de la cooperación conjunta entre las leyes de los Estados para mejorar le investigación y poder tipificar las sanciones a nivel interno de una forma más técnica para abarcar la mayor cantidad de delitos informáticos y que puedan articularse con las instituciones y marco jurídico del país.

5. Evaluar los Proyectos de Ley que se encuentran en la Comisión de Soberanía, Integración y Seguridad Integral desde el 2021, para fortalecer la constante actualización de las tecnologías de la información y prevenir futuros ataques cibernéticos al sistema financiero, instituciones estatales, datos de la sociedad civil y proteger la información del Estado.
6. Es importante considerar la formulación de metodologías que impliquen el desarrollo de informes, datos estadísticos e información en tiempo real sobre las amenazas y ciberataques a las entidades del Estado que prevean y ayuden con las investigaciones y creación de políticas públicas, para que no solo se tome en consideración los ataques que surgen en el ciberespacio, sino se busque incluso fortalecer las oportunidades que brinda este nuevo dominio.
7. En referencia a la academia, es importante que se puedan profundizar sobre los temas relacionados a la gobernanza del internet y su relación con el ciberespacio, de manera que al ser un entorno en constante cambio puede presentar nuevos elementos que requiere un análisis continuo para fortalecer los estudios y acciones previas.
8. En relación con el aspecto teórico utilizado, se recomienda ahondar en el área de especialización de cada institución puesto que, desde las Fuerzas Armadas, se mantiene esta concepción realista de la seguridad estatal aun cuando el ciberespacio no es un dominio físico, corresponde como un espacio que implica la posibilidad de su utilización para perseguir intereses particulares de los Estados, actores privados o públicos o individuos a través de internet.

BIBLIOGRAFÍA

Acosta, P. (2009). *Seguridad nacional y ciberdefensa*. http://www.catedraisdefe.etsit.upm.es/2010/07/CUADER-NO-Nº-6.pdf.

Acurio, S. (24 de agosto de 2021). *Política Pública de Ciberseguridad*. iT ahora: https://itahora.com/2021/08/24/politica-publica-de-ciberseguridad/

Aguilar, J. M. (2021). *Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior*. Estudios Internacionales (198), 169-197.

Alcalá, M. I., & Rodrigues, N. (2012). *Hacktivismo: la nueva cara de la participación. Comunicación: estudios venezolanos de comunicación* (159-160), 38-45. https://dialnet.unirioja.es/servlet/articulo?codigo=6025635

Alonso, A., & Arzoz, I. (2005). *La quinta columna digital: Antitratado comunal de hiperpolítica*. Gedisa.

Barandiaran, X. (2003). *Activismo digital y telemático. Poder y contrapoder en el ciberespacio*. 1, 26. https://sindominio.net/xabier/textos/adt/adt.pdf

Burgos, E. K. (2014). *El hacktivismo: Entre la participación política y las tácticas de subversión digital.* (U. d. Hemisferios, Ed.) Razón y Palabra (88), 27. http://www.redalyc.org/articulo.oa?id=199532731006

Cano, J. (2013). *Ciberseguridad empresarial: De las prácticas de aseguramiento a las capacidades de defensa*. Asociacón de Especialistas en delitos financieros: https://es.scribd.com/document/443738898/PG6-Ciberseguridad-Jeimy-Cano

Cano, J. J. (2010). *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global*. http://52.0.140.184/typo43/fileadmin/Revista_119/Editorial.pdf

Choucri, N. (2012). *Cyber Politics in International Relations*. Cambridge: MIT Press.

Clarín. (4 de junio de 2020*). Anonymous: que fue el "Proyecto Chanology" y por qué rechazan a Tom Cruise y la Cienciología*. Clarín Internacional.:

https://www.clarin.com/internacional/anonymous-proyecto-chanology-rechazan-tom-cruise-cienciologia_0_HrAooUB4Z.html

Clarke, R. A. & Knake, R. K. (2010). *Cyber War: The Next Threat*. Nueva York: Ecco

COIP. (2014). *Código Orgánico Integral Penal*. https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Coleman, G. (2014). *Hackers, activistas, espías y bromistas: Las mil caras de Anonymous*.

Constitución del Ecuador. (2008). *Constitución de la República del Ecuador*. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Counsil of Europe. (2001). *Convenio sobre la ciberdelincuencia.* Budapest. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Critical-Art-Ensemble (2001). *Digital Resistanse Autonomedia*. http://critical-art.net/

Deleuze, G., & Guattari, F. (2000). *Mil mesetas: capitalismo y esquizofrenia* (Cuarta ed.). (M. d. francés, Trad.) Pre-textos. http://www.medicinayarte.com/img/deleuze_mil_mesetas_capitalismo_esquizofrenia_deleuze_guattari.pdf

Delgado, A. (2014). *Gobernanza de Internet en Ecuador: Infraestructura y acceso*. http://repositorio.educacionsuperior.gob.ec//handle/28000/1579

Easton, D. (1965) A. *Systems Analysis of Political Life*

Ecuavisa. (18 de enero de 2017). *Anonymous Ecuador niega hackeo de cuentas de asambleísta y comunicador*. Ecuavisa: https://www.ecuavisa.com/noticias/ecuador/anonymous-ecuador-niega-hackeo-cuentas-asambleista-comunicador-BHEC231356

EFE. (8 de diciembre de 2010). *Un grupo de Hackers ataca a entidades relacionadas con el acoso a WikiLeaks*. El País:

https://cincodias.elpais.com/cincodias/2010/12/08/tecnologia/1292050006_850215.html

El Comercio. (28 de marzo de 2014). *Ataques de Anonymous se iniciaron en 2011*. El Comercio: https://www.elcomercio.com/actualidad/politica/ataques-de-anonymous-se-iniciaron.html

El Mundo. (5 de enero de 2011). *Anonymous ataca varios sitios del Gobierno de Túnez*. El Mundo: https://www.elmundo.es/elmundo/2011/01/05/navegante/1294225836.html

El Telégrafo. (10 de agosto de 2011). *Ataques hacker a redes de Ecuador*. El Telégrafo: https://www.eltelegrafo.com.ec/noticias/tecnologia/1/mas-paginas-web-oficiales-hackeadas

El Universo. (10 de agosto de 2012). *Anonymous Ecuador se atribuye intervención a 45 sitios web gubernamentales*. El Universo: https://www.eluniverso.com/2012/08/10/1/1355/anonymous-ecuador-atribuye-intervencion-algunos-sitios-web-gubernamentales.html/

El Universo. (12 de abril de 2019). *Millones de ataques cibernéticos a Ecuador se reportan tras detención de Julian Assange, según exjefe de Inteligencia Militar*. El Universo: https://www.eluniverso.com/noticias/2019/04/12/nota/7281890/exjefe-inteligencia-militar-recomienda-gobierno-fusion-sus-sistemas/

Enriquez, L. (15 de junio de 2021). *La ciberdelincuencia organizada I: diferencia entre hacktivistas y mercenarios*. Observatorio de Ciberderechos y Tecnología: https://www.uasb.edu.ec/ciberderechos/2021/06/15/la-ciberdelincuencia-organizada-i-diferencia-entre-hacktivistas-y-mercenarios/

Eriksson, J., & Giacomello, G. (2006). *The Information Revolution, Security, and International Relations: (IR)relevant Theory?*. International Political Science Review, 27(3), 221–244. https://doi.org/10.1177/0192512106064462

Fuerzas Armadas. (27 de mayo de 2022). Hacktivismo de Anonymous en el Ecuador: Políticas públicas, ciberseguridad, ciberespacio y ciberdefensa. (V. Carvajal, Entrevistador).

Gamón, V. P. (2017). *Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad*. Revista Latinoamericana de Estudios de Seguridad (20), 80-93. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2563

Gibson, W. (1984). *Neuromancer*. Ace.

Guerrero, L. (2007). *Los Derechos Humanos como Política Publica* (Primera ed.). Universidad Nacional, Facultad de derecho, Ciencias Políticas y Sociales.

Heredia, J. S. (2021). *Ciberseguridad en Ecuador y Latinoamerca. Killkana Técnica.* Revista de Investigación Científica, 5(1). doi:10.26871/killkanatecnica.

iT Tecnología. (6 de julio de 2021). *La AECI impulsa la participación de Ecuador en el Convenio de Budapest*. iT Tecnología: https://itahora.com/2021/07/06/la-aeci-impulsa-la-participacion-de-ecuador-en-el-convenio-de-budapest/

ITU. (2007). *Guía de ciberseguridad para los países en desarrollo*. http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

ITU. (2011). *National Cybersecurity Strategy Guide*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNational-CybersecurityStrategyGuide.pdf

Jordán, J. (2013). *Enfoques teóricos de los Estudios Estratégicos.* Manual de Estudios Estratégicos y Seguridad Internacional. https://www.researchgate.net/publication/273127222_Enfoques_teoricos_de_los_Estudios_Estrategicos/citation/download

La Información. (14 de abril de 2019). *Ecuador acusa a Anonymous de ataques informáticos tras el arresto de Assange*. La Información:

https://www.lainformacion.com/mundo/ecuador-anonymous-ataques-assange/6497516/

La República. (8 de agosto de 2011). *Anonymous responde a Ecuador y hackea al Municipio de Guayaquil.* La República: https://www.larepublica.ec/blog/2011/08/08/anonymous-responde-a-ecuador-y-hackea-la-web-del-municipio-de-guayaquil/

Lazár, E. (2018). *Los ciberataques: Una noción sin tipificación, pero con un futuro*. Anuario da Facultade de Dereito da Universidade da Coruña, 22, 157-175. doi: https://doi.org/10.17979/afdudc.2018.22.0.5180

Ley de Comercio Electrónicos, Firmas y Mensajes de Datos. (2002). *Ley de Comercio Electrónicos, Firmas y Mensajes de Datos.* https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Ley de Seguridad Pública y del Estado. (2009). *Ley de Seguridad Pública y del Estado*. http://www.oas.org/juridico/pdfs/mesicic5_ecu_panel5_sercop_1.3._ley_seg_pública.pdf

Ley Orgánica de la Defensa Nacional. (2007). *Ley Orgánica de la Defensa Nacional*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2015/04/ene15_LEY-ORGANICA-DE-LA-DEFENSA-NACIONAL.pdf

Ley Orgánica de Telecomunicaciones. (2015). *Ley Orgánica de Telecomunicaciones*. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Orgánica-de-Telecomunicaciones.pdf

Leyva, A. (2021). *Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano*. Polo del Conocimiento, 6(3), 1229-1250. doi:10.23857/pc.v6i3.2431

Mearsheimer, J.J. (2001). *The tragedy of great power politics*. W.W. Norton & Company

Mikhaylova, G. (2014*). The "Anonymous" movement: Hackitivism as an emerging form of political participation*. Maters Thesis, Texas State University.

Ministerio de Coordinación de Seguridad. (2011). *Plan Nacional de Seguridad Integral*.

Mogollón, S. (2021). *La adaptación asimétrica de las doctrinas de Defensa en torno al ciberespacio: los casos de Chile y Ecuador (2014-2018).* Tesis de maestría, Facultad Latinoamericana de Ciencias Sociales, FLACSO Ecuador, Estudios Internacionales y Comunicación.

Muñoz, O., & Frasson, F. (2011). *El realismo en el siglo XX y XXI*. Revista Analectas política, 1(1), 81-106}.

Muñoz, P. (2013). *La influencia de los actores no estatales en el sistema internacional.* Revista afese, 100-112. http://www.revistaafese.org/ojsAfese/index.php/afese/article/view/330

Nye, J. S. (2011). *Nuclear lessons for cyber security? Strategic Studies Quarterly*, 5(4), 18-38.

Orozco, G. (2006). *El concepto de la seguridad en la Teoría de las Relaciones Internacionales*. Revista CIDOB d'Afers Internacionals , 161-180.

Pabón, A. (2019). *El individuo como instrumento en la narratca de ciberseguridad internacional contemporánea*. Tesis de grado, Pontificia Universidad Javeriana

Plan Nacional de Seguridad. (2014). *Plan Nacional de Seguridad 2014-2017*. Ministerio Coordinador de Seguridad.

Rabinad, G. (2008). *La soberanía del Ciberespacio.* Lecciones y ensayos, 85, 85-107.

Ragnedda, M. (2011). *Internet y control social: Entre rizoma y gran hermano*. Perspectivas de la comunicación, 4(1), 45-52.

Raymond, E. S. (2000). *Breve historia de la cultura hacker. La gran explosión de la web*, 16. http://culturainformatica.es/descargas/articulos/Breve%20historia%20de%20la%20cultura%20hacker.pdf

Rivera, D. (2018). *Internet y su potencial político: hacktivismo en Anonymous Chile (2011-2016)*. Faro, 1(27), 86-116. http://www.revistafaro.cl

Roth, A. N. (2009). *Políticas Públicas: Formulación, implementación y evaluación* (Séptima ed.). Aurora.

Salinas, C. (2018). *Ciberdefensa en el Estado Ecuatoriano: Período 2013-2016.* Tesis de Grado, Pontificia Universidad Católica del Ecuador.

Serrano, J. (2021). *Proyecto de Ley Orgánica de Seguridad Cibernética*.

Sigholm, J. (2013). *Non-State Actors in Cyberspace Operations*. Journal of Military Studies. 4. 1-37. 10.1515/jms-2016-0184.

Sorbo, H. D. (5 de agosto de 2020). *Tenencia de Pornografía Infantil. Regulación a partir de la incorporación de la Nación Argentina al Convenio de Budapest*. El Dial: https://www.eldial.com/nuevo/nuevo_diseno/v2/doctrina1.asp?id=13247&base=50&indice=doctrina&vengode=suple

Stock, J. (4 de agosto de 2020). Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. Obtenido de INTERPOL: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Tapia, A., & Castro, A. (11 de diciembre de 2019). *Ataques, vulneraciones y cerco mediático al movimiento indígena durante el paro nacional en Ecuador*. RedKapari: https://redkapari.org/2019/12/11/ataques-vulneraciones-y-cerco-mediatico-al-movimiento-indigena-durante-el-paro-nacional-en-ecuador/

Thompson, J. C. (2012). *La distribución de poder en el ciberespacio: Anonymous y las capacidades de ciberpoder 2010-2012.* Fundación Universidad Argentina de la Empresa.

Tidy, J. (17 de marzo de 2022). *Rusia y Ucrania: Anonymous "Intensificaremos los ataques contra el Kremlin"*. BBC News Mundo: https://www.bbc.com/mundo/noticias-internacional-60781082.

Toft, P. (2005). *John J. Mearsheimer: an offensive realist between geopolitics and power*. Journal of International Relations and Development (8), 381–408. Doi: 10.1057/palgrave.jird.1800065

Torres, M. R. (22 de junio de 2015). *Una brevísima historia del "Hacktivismo"*. Grupo de Estudios en Seguridad Internacional: https://www.seguridadinternacional.es/?q=es/content/una-brev%C3%ADsima-historia-del-hacktivismo-0

UIT. (2022). *Actualidades de la UIT*. http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

UNIR. (13 de diciembre de 2021*). ¿Qué es el hacktivismo y qué delitos implica?*. Revista UNIR: https://www.unir.net/derecho/revista/hacktivismo/

UNODC. (2020). *Ciberdelincuencia. Serie de módulos universitarios*. Guía didáctica, 2-43.

Vicente, L. (2004). *¿Movimientos sociales en la Red? Los hacktivistas*. El Cotidiano, 20(126), 1-8. https://www.redalyc.org/articulo.oa?id=32512615.

Waltz, K. (2000). *Structural Realism after the Cold War*. The MIT Press. https://www.jstor.org/stable/2626772.

ANEXOS

ANEXO 1: ENTREVISTA A UN FUNCIONARIO DE LAS FUERZAS ARMADAS (Anónimo)

1. **¿Qué tan importante es la ciberseguridad y ciberdefensa en el país?**

En el actual contexto de un mundo hiperconectado con una casi total dependencia de sistemas y redes de información que permiten almacenar una incontable base de datos, tanto en servidores físicos como en sistemas virtuales ("nubes"), así como controlar los procesos automatizados que hoy dirigen la vida diaria (concepto de internet de las cosas), demandan un gran esfuerzo desde lo individual, empresas privadas y más aún los Estados para precautelar su integridad, ya que el acceso no autorizado a estos sistemas tecnológicos y de información por parte de personas, organizaciones e incluso Estados rivales, podría suponer la grave afectación a su estabilidad, estado de derecho, seguridad económica, seguridad energética y desde luego su propia supervivencia (campo de la defensa nacional). La información desde siempre ha sido la principal arma y herramienta para mantener la paz o ganar la guerra por lo cual su protección ha sido desde tiempos bíblicos hasta nuestros días y en el escenario anteriormente descrito, la ciberdefensa y ciberseguridad son las nuevas defensas que se emplean en una nueva dimensión de lo que los analistas militares a nivel mundial han definido como el nuevo espectro o dimensión del campo de batalla: El Ciberespacio. En la actualidad los conflictos bélicos como el de Ucrania vienen precedidos de acciones que se enmarcan en conceptos de ruptura en la planificación militar denominado "Guerras Híbridas", las cuales tienen un amplio componente de acciones a nivel del ciberespacio con los cuales buscan debilitar la infraestructura comunicacional, provocar caos en los sistemas y redes de información, ataques electrónicos a los sistemas que controlan las transacciones bancarias, a los sistemas de transporte, sistemas energéticos y hacia los sistemas de información militar que permite la dirección y el control de la defensa nacional. Podríamos remontarnos como un antecedente a esto el ataque informático que sufrió Estonia ocurrido en 2007, país que hacia esa fecha ya había alcanzado un muy alto grado de automatización de sus sistemas de comunicaciones y digitalizado casi todos los campos de la administración pública, acercándose a la Unión Europea, situación que provocó la reacción del Gobierno de Rusia a quien se le acusó de un masivo ataque mediante "ordenadores zombis" que

finalmente hicieron colapsar las redes informáticas de bancos y entidades gubernamentales de Estonia. Este hecho marcó la pauta de lo que hoy es la denominada “ciberguerra”. Actualmente Estonia es considerado como “el país más digital” del mundo y uno de los mayores generadores de conocimiento en el campo informático tras estos sucesos.

2. **¿Porque se requiere una política nacional de ciberseguridad y ciberdefensa en el país?**

Es fundamental porque el Ecuador, a pesar de ser un país marginal en cuanto a la automatización de sus sistemas de información, no es menos cierto que se han dado grandes pasos en ello y tanto en el área privada como estatal existen amplias bases de datos con información sensible de usuarios y entidades estatales, presentándose casos de robo y ventas ilegales de las mismas, tal es el caso de la denuncia que se hiciera en Miami sobre la vulneración de esta información contenida en servidores del Registro Civil, BIESS entre otros. También han existido ataque a los servidores y redes de entidades como el Banco del Pichincha que durante el año 2021 e inicios del 2022 presentó problemas en sus plataformas digitales y aplicaciones móviles, la ANT, el Municipio de Quito 2022, entre otros. Una política clara en este tipo de campo podría generar las necesarias reformas a las leyes para tipificar de mejor forma este tipo de infracciones, facilitar la obtención de recursos, obtener apoyo internacional y capacitar al personal técnico que en los ámbitos público y privado tengan estas responsabilidades.

3. **¿El país cuenta con las herramientas, personal y la infraestructura adecuada para contrarrestar los ataques cibernéticos?**

A nivel privado existen algunos desarrollos principalmente en la banca y cierto tipo de servicios industriales, mientras que a nivel estatal se debe enfatizar que las falencias inician desde la misma concepción de este tipo de acciones a nivel de la Ley; igualmente la Fiscalía donde se persiguen los denominados “delitos informáticos” quienes no poseen el suficiente personal técnico y medios, la Policía Nacional que a través de la Policía Judicial estableció la Unidad de Delitos Cibernéticos que igualmente mantiene las carencias antes descritas pero que se ha fortalecido gracias a la cooperación internacional; y, las Fuerzas Armadas quienes han dado algunos pasos importantes con la creación del Comando de Ciberdefensa. Lo descritos son pasos importantes para contrarrestar las acciones de los

piratas informáticos, pero no permiten una mayor cobertura de la infraestructura crítica del país que tampoco ha llegado a una total automatización y digitalización.

4. **¿Qué sucedió con los proyectos de Ley que están en debate en la Asamblea Nacional?**

Igual que muchos otros proyectos no han sido debidamente priorizados tal es el caso del Proyecto de Ley orgánica de seguridad cibernética presentado el 1º de mayo de 2021. No poseo una mayor información en este aspecto.

5. **¿Qué instituciones deberían ser las encargadas de la protección de la infraestructura del Estado en ciberseguridad y ciberdefensa?**

En este aspecto considerando los ejemplos de otros países, este es un tema de Seguridad del Estado y como tal es el Estado en su conjunto el responsable de ello, para el efecto la respuesta debe ser interagencial con un Centro que fusiones las capacidades que al respecto están desarrollando el Centro de Inteligencia Estratégico, Ministerio de Telecomunicaciones y Sociedad de la Información, FF.AA con su Comando de Ciberdefensa, Fiscalía y Policía Nacional con sus unidades especializadas e inclusive la academia.

6. **¿Considera que las estrategias en materia de ciberseguridad corresponden a la perspectiva realista de las relaciones internacionales?**

El realismo clásico como fue detallado por Maquiavelo, Hobbes a mi criterio no ha sido superado, aun cuando el idealismo o las teorías críticas de la seguridad hayan ganado apogeo en el discurso internacional, la desconfianza es una constante y los Estados y sus gobernantes se siguen rigiendo por sus intereses generalmente coyunturales, pasando las alianzas y rivalidades de bando conforme estos intereses se hacen más fuertes y chocan entre sí; ejemplo de ello es la firma del AUKUS que dejó por fuera a Francia para favorecer al Reino Unido de un multimillonario contrato para la fabricación de submarinos para Australia, bajo el direccionamiento de los Estados Unidos, cuyos intereses se materializan en el sur del Mar de China. Pasa lo mismo en con la ciberseguridad, donde la información es el "botín de guerra" que puede ser empleado a favor de los aliados de quien la disponga o contra sus antagonistas, este es el caso de la información revelada por WikiLeaks.

7. **¿Para el Estado ecuatoriano el ciberespacio debe ser parte de la seguridad nacional?**

Definitivamente sí y de hecho está considerado en la Política Nacional de Defensa aún vigentes desde el 2018, así como Política de Estado publicada mediante Acuerdo Ministerial Número 006-2021.

8. **¿La constante actualización de las TICs y el poder por su manejo representa una nueva condición de conflicto internacional?**

Ya está ocurriendo, tal como inicié en la pregunta número 1, es parte fundamental de la nueva dimensión del "campo de batalla", el ciberespacio donde se libra la "ciberguerra" como un componente de la denominada "guerra híbrida", eso es lo que actualmente vemos por ejemplo en el conflicto entre Rusia y Ucrania; igualmente inmediatamente anterior vimos la guerra entre Armenia y Azerbaiyán por el control de la región del Nagorno Karabaj del 2020, donde quien tuvo mayor acceso a la tecnología (Azerbaiyán) fue finalmente el vencedor, siendo fundamental para la su victoria la puesta en escena de nuevos elementos como las municiones merodeadoras, drones "Byraktar" de origen turco, pero sobre todo la capacidad de colección de información y la transmisión en tiempo real y por medios seguros de inteligencia útil para la toma de decisiones en los centros de mando y control en todos los niveles: táctico, operacional y estratégico.

9. **¿El Estado ecuatoriano ha regulado los ataques cibernéticos que ha sufrido su infraestructura y entidades estatales?**

Están catalogados a nivel del COIP específicamente en la Sección Tercera: "Delitos contra la seguridad de los activos de los sistemas de información y comunicación", un ejemplo de ello es el proceso judicial contra el ciudadano sueco Ola Bini por "presunto acceso no autorizado a sistemas informáticos y telemáticos" Art. 234.

10. **¿Cuáles son las principales amenazas que enfrenta el Estado ecuatoriano en el ciberespacio?**

En la Política de Ciberseguridad 2021 se detalla este tipo de amenazas y determina con la nomenclatura técnica los mismos, pero en forma general los ataques generalmente van orientados al robo de información, secuestro de base de datos y denegación de servicios, empleando para el efecto direcciones falsas empelando VPN y programas maliciosos (malaware), atacando servidores, redes y equipos

incluidos los teléfonos inteligentes y tablets. Laboratorios como Kaspersky en el año 2020 ubicó al Ecuador en el puesto 89 de entre los países que mayores ataques informáticos ha recibido a nivel global.

11. **¿El ciberespacio es un nuevo campo de batalla para el Estado ecuatoriano?**

Como lo he detallado en las preguntas anteriores definitivamente sí.

12. **¿El grupo no estatal transnacional Anonymous es considerado una amenaza para el Estado ecuatoriano?**

No poseo información al respecto, pero toda persona u organización que intente acceder ilegalmente a datos sensibles sobre el Estado ecuatoriano y que utilice esta información para poner en peligro la estabilidad política, social y económica; buscar la ruptura del estado de derecho y la paz del país; reúne los requisitos de una amenaza: capacidad, motivación e intención.

13. **¿Consideran a Anonymous como un elemento de análisis desde la política de defensa del Estado, o deben ser un tema gestionado a nivel de políticas públicas por sus antecedentes de hackeo a nivel internacional?**

Los Estados modernos no se enfocan en un grupo, colectivo o persona en específico, visualizan la generalidad del problema, del fenómeno y adoptan las medidas que están a su alcance para proteger su información sensible. Hay muchas más personas u organizaciones que actúan en y desde la Deep Web cuyos intereses son muy variados desde lo delictivo hasta lo político.

14. **¿El Estado ecuatoriano está preparado para enfrentar estas nuevas amenazas a nivel jurídico como tecnológico?**

La velocidad con la que mutan las amenazas tecnológicas generalmente es más rápida que la capacidad de los Estados para adaptarse política y legalmente a las nuevas amenazas, pero en el Ecuador como hemos visto se han dado ya algunos pasos que van permitiendo mejorar la respuesta tecnológica y judicial.