Facultad Latinoamericana de Ciencias Sociales, FLACSO Ecuador
Departamento de Estudios Internacionales y Comunicación
Convocatoria 2018-2020

Tesis para obtener el título de maestría de investigación en Relaciones Internacionales con mención en Seguridad y Derechos Humanos

La adaptación asimétrica de las doctrinas de Defensa en torno al ciberespacio: los casos de Chile y Ecuador (2014 -2018)

Francis Stephania Mogollón Flores

Asesor: Lester Cabrera
Lectores: Diego Arancibia Morales y Luis Umbría

Quito, marzo de 2021

Tabla de contenido

Resumen

El presente trabajo tiene como objetivo comprender el porqué de la asimetría existente entre los procesos de adaptación doctrinaria de Defensa en torno al ciberespacio de Chile y Ecuador, países con principios dogmáticos similares. Para poder lograr este objetivo se construyó un marco teórico desde varios enfoques con la finalidad de mantener una visión holística del problema en cuestión. A partir de las tres teorías utilizadas se pudo entender los diferentes aspectos que inciden en el comportamiento y la toma de decisiones en Chile y Ecuador. En esta etapa de la investigación confluyeron preceptos teóricos de tinte clásico y reflectivistas dado que, en el plano global, dentro del ciberespacio, se puede aplicar ambos. Esto responde al hecho de que los países mantienen necesidades básicas que los motivan a tomar decisiones frente a posibles riesgos. No obstante, escenarios como el cibernético los obligan a adaptarse en torno a amenazas no convencionales de las cuales las teorías más clásicas no logran dar cuenta. A su vez, se realizó el análisis de la estrategia de Ciberdefensa que ha estructurado cada República, tomando en cuenta los parámetros que dan cuenta de una transformación doctrinaria frente a las ciberamenazas; problemática relevante para el Estado. Una vez estudiado cada plan, se efectuó la comparación entre ambos casos de estudio lo cual fue de utilidad para poder observar en que aspectos del proceso de ajuste han tenido similitudes y en qué áreas se ha manifestado una brecha amplia. De tal manera que se pudo dilucidar cual es el factor determinante dentro del fenómeno que se ha estudiado. Se llego a la conclusión de que la Política de Ciberdefensa es la variable que ha determinado la asimetría entre ambos países.

Agradecimientos

A Dios por haber puesto en mi camino una oportunidad tan valiosa para poder crecer personal y profesionalmente.

A FLACSO Ecuador y al su cuerpo docente del Departamento de Estudios Internacionales y Comunicación, por otorgarme el conocimiento propicio para aprovechar al máximo mi potencial como investigadora.

Al Doctor Lester Cabrera, por su inmejorable labor como tutor del presente trabajo y sus oportunos consejos a lo largo de este proceso educativo.

Al Doctor Luis Umbría y al Doctor Diego Arancibia por el tiempo prestado para le revisión de la presente investigación y sus valiosas observaciones.

Al personal administrativo de esta honorable institución, especialmente a Gladys Molina y Vanessa Bonilla, por resolver de manera eficiente cualquier requerimiento de los estudiantes y por prestarnos una mano amiga ante cualquier problema.

A mis padres por su amor incondicional, mismo que me ha dado la motivación para culminar con éxito esta nueva etapa de mi vida.

A mi hermano quien me ha apoyado en todo momento y se ha hecho presente con la palabra justa y el consejo indicado.

A mi sobrino, que con sus gestos de cariño me ha impulsado a ser mejor cada día.

A mi esposo por el amor, el apoyo, la comprensión y la confianza, gracias por estar siempre presente.

A Pablito y Jael con quienes hemos sobrepasado todos los retos que se nos presentaron en el transcurso de nuestro perfeccionamiento académico, y que más que compañeros han sido grandes amigos.

Introducción General

1. Planteamiento del problema

Debido al acelerado desarrollo de las tecnologías de la información en la actualidad, dentro del ciberespacio circula y se interconecta información sensible en términos políticos y militares. Tales datos han sido utilizados por Estados y agrupaciones ilícitas para realizar ataques cibernéticos contra instalaciones críticas de otros países. Estas nuevas amenazas han generado respuestas ofensivas que a su vez han configurado vulnerabilidades a nivel global. De modo que, los desafíos que presenta el ciberespacio deben ser factores a ser tomados en cuenta dentro de la doctrina de Defensa.

Al hablar de ciberespacio se hace alusión a diversas conceptualizaciones, mimas que se han desarrollado en contextos específicos. Generalmente este entorno ha sido visto como el medio transmisor de datos constituido por un entramado de infraestructuras tecnológicas de la información como internet, controladores remotos, procesadores, redes de telecomunicaciones y sistemas informáticos. Asimismo, se lo puede concebir como el espacio virtual donde se procesa, almacena y se difunden datos informáticos (CEEAG 2018). De acuerdo a Daniel Kuehl, dichos conceptos son útiles para poder entender de forma general al espacio cibernético, sin embargo, carecen de información crítica, es decir que no contemplan las características que hacen único a este entorno o dominio. Tomando en cuenta dicha particularidad, dentro de la presente investigación se visualizará al ciberespacio como:

> Un dominio global dentro del entorno de la información cuyo carácter distintivo y único se enmarca en el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando tecnologías de la información y la comunicación (Kuehl 2009, 27).

Esta dimensión virtual otorga anonimato a los perpetradores de un ciberataque lo cual problematiza la terea de identificación de los agresores cibernéticos, pues se puede saber desde que lugar se realizó un ataque, pero no exactamente el autor, o autores, del mismo. El atacante puede ser intencionado o inintencionado, el primer tipo de ciberagresor es fácilmente catalogable pero un ejemplo del segundo sería un usuario que por descuido abrió algún documento que contengan un malware (Norwood y Catwell 2009). A ello se le adiciona la incongruencia que existe entre los recursos que se necesitan para poder generar una amenaza

y las capacidades que deben ser empleadas para neutralizarla. Para configurar una amenaza de este tipo no se necesita de una infraestructura amplia o de gran cantidad de personal, sin embargo, el receptor del ataque si debe contar con personal capacitado y una infraestructura considerable para que este no genere mayores afectaciones.

Las amenazas cibernéticas han sido consideradas nuevas amenazas debido a que no suponen un riesgo que se estructure desde un Estado hacia otro únicamente. Estas pueden ser articuladas por otros actores internacionales, ya sea grupos ilícitos o individuos, y suelen tener repercusiones de carácter social y transnacional. Dichos actores emplean distintas innovaciones tecnológicas las cuales pueden ser utilizadas en contra de la supervivencia del Estado, así como también del funcionamiento de sus infraestructuras estratégicas (Cabrera 2012). Ello ha significado una difuminación de la frontera entre aquello que se puede concebir como una problemática eminentemente doméstica y asuntos netamente internacionales. De manera que se genera una imprecisa definición de lo que le concierne a la Defensa Nacional y aquello que le ataña a la seguridad interna de Estado.

Uno de los principales retos que presenta el ciberespacio es la ausencia de fronteras, el cual sugiere que los principios doctrinarios para defender al Estado deben ser repensados, pues al no haber un territorio claramente delimitado que proteger, acciones y estrategias tradicionales no tienen cabida. Esto responde a que desde 1648, con la paz de Westfalia, las doctrinas de Defensa se han visto vinculadas a la protección de la integridad territorial, dado que el sistema internacional moderno se basa principalmente en la soberanía. No obstante, en el ciberespacio no existe una zona sobre la cual el Estado pueda mantener control efectivo, de modo que, sus amenazas trascienden a las autoridades territoriales (Halpin, y otros 2006).

Las especificidades que presenta este entorno han supuesto una adaptación de la doctrina de Defensa del Estado, pero para poder comprender esto, es preciso primeramente establecer a que hace referencia el concepto de doctrina. De manera general, una doctrina es definida como un grupo de principios que establecen un sistema de creencias. A nivel estatal puede considerarse como una declaración de políticas gubernamentales fundamentales y a nivel militar, es un conjunto de estrategias. En el fondo, una dotrina comprende los principios mediante los cuales se va a regir un colectivo. Sirve como base común de conocimiento para actuar de la mejor manera en un determinado contexto ya que se estructura en función de un cumulo de experiencias vinculadas a la toma de decisiones estratégicas dentro de un dominio.

Esta suele presentar características específicas de los actores que las emplean y de sus procesos históricos, de modo que puede tomar diversas formas ya sean ligadas a los hechos o a la interpretación de los actores (Colarik y Janczewski 2012).

Históricamente la doctrina de Defensa ha sido fuertemente vinculada a la doctrina militar, al punto de considerarse que ambas son lo mismo. Empero, aunque ambas tienen el objetivo común de proteger la integridad del Estado, se constituyen en campos diferentes. Los principios que rigen a la Defensa establecen una estructura política que comprende la protección del Estado, esto supone la creación de una serie de políticas públicas. Los dogmas militares rigen el accionar de las Fuerzas Armadas para dar apoyo a los objetivos nacionales (Colarik y Janczewski 2012).

Si bien la doctrina de Defensa varía de acuerdo a los desafíos que se le presentan a cada país, en América del Sur las amenazas exógenas tradicionales, articuladas por otro Estado, siguen siendo una prioridad dentro de la agenda de Defensa (Bartolomé 2009). En la actualidad las llamadas "nuevas amenazas" se han vuelto relevantes para la región en vista de que constituyen un riesgo no solo hacia el Estado sino también hacia sus ciudadanos. Dicha región forma parte del cuarto mayor mercado del mundo y más de la mitad de su población ocupa internet (ITU 2018). En virtud de ello, los países que lo conforman han implementado nuevas tecnologías para gestionar los sistemas Estatales sin tomar las debidas medidas de seguridad para que los mismos no sean intervenidos.

Todo esto ha posicionado a Latinoamérica como una objetivo atractivo para los ciberdelitos y ha dado la pauta para que se articule un número considerable de redes cibernéticas irregulares con características transnacionales, mismas que no han podido ser controladas debido a la ineficacia de los sistemas de protección utilizados por estos países (Kshetri 2013). A pesar de este panorama, no todos los países han tratado esta problemática dentro de sus doctrinas de Defensa y aquellos que lo han hecho no lo han tomado como un tópico central, pues sus principios siguen fuertemente ligados a la protección de la soberanía estatal. Razón por la cual el ámbito de la Defensa sigue siendo altamente militarizado en la región (Bartolomé 2009). Afirmación que da cuenta de una territorialización latente, lo cual es problemático en un entorno como el ciberespacio donde no se ha logrado establecer internacionalmente zonas de dominio. De allí que la mayoría de las investigaciones que han surgido desde países sudamericanos en este campo, se hayan enfocado en la protección de los medios kinéticos del Estado. Con

respecto al ciberespacio, se han realizado estudios generales sobre Ciberseguridad más que trabajos específicos orientados a la Ciberdefensa. A nivel político ha sucedido lo propio, se han establecido procesos que han dado prioridad a la Defensa en función de las fronteras tradicionales claramente delimitadas, motivo por el cual se considera que Latinoamérica se encuentra poco preparada para hacerle frente a las ciberamenazas (OEA y BID 2016).

La razón por la cual se han tomado como casos de estudio a Chile y Ecuador, es porque ambos países, a nivel América Latina, se han destacado por posicionarse entre los países que más han implementado las TICs en el sector público. De conformidad con el Informe mundial sobre tecnología de la información del 2016, presentado por el Foro Económico Mundial, tanto el país del Cono Sur como el país andino se han establecido entre los países latinoamericanos más preparados en la red. Esto quiere decir que estas Repúblicas tienen como prioridad aprovechas las TICs en beneficio del desarrollo socioeconómico (World Economic Forum 2016). No obstante, al momento de comparar la Ciberseguridad y la Ciberdefensa en estos Estados, se visualiza una fuerte asimetría con Chile liderando los rankings y Ecuador ubicándose en las últimas posiciones. De acuerdo con el Índice Nacional de Seguridad Cibernética (NCSI por sus siglas en ingles), Chile lidera el ranking en América del Sur y muestra una superioridad frente a Ecuador en aspectos políticos, técnicos y de desarrollo profesional (National Cyber Security Index 2018).

Asimismo, ambos países cuentan con principios dogmáticos similares, y han contemplado a los desafíos cibernéticos dentro de sus doctrinas de Defensa. En ellas se concibe a las ciberamenazas como un factor que puede comprometer áreas o sectores estratégicos del Estado. Lo cual debería suponer un proceso de transformación, en torno al ciberespacio, semejante en estos países. Sin embargo, en la práctica se ha presentado una adaptación disímil, lo que ha generado la siguiente interrogante: ¿Cueles son la o las variables intervinientes que han determinado la asimetría en la adaptación doctrinaria entre Chile y Ecuador?

Tanto en Chile como en Ecuador, se ha suscitado el mismo fenómeno, sus doctrinas han tenido como principal objetivo la protección de la soberanía del Estado en términos territoriales, de tal manera que se encuentran fuertemente vinculada a las Fuerzas Armadas, y a la doctrina militar. En ambos países la unidad militar es la institución designada para poder desempeñar acciones estratégicas con el fin de proteger la integridad territorial, la soberanía,

los intereses nacionales, los bienes nacionales y a la población (Colarik y Janczewski 2012). Esto se convierte en un dilema al momento de generar estrategias dentro del ciberespacio en vista de que en esta dimensión la desterritorialización y la anarquía no permite que concepciones relacionadas con la protección soberana, puedan ser efectivas.

No obstante, los Gobiernos de dichos países han tomado acciones desde el 2014 en términos de Defensa contra las ciberamenazas. El Gobierno chileno, propuso en aquel año la política de Ciberseguridad, misma que fue puesta en vigencia en el año 2017, con el fin de materializar políticas de Ciberdefensa y así poder desarrollar sus capacidades en el ciberespacio. El Ecuador, por su parte, creó el Comando de Ciberdefensa como parte de sus Fuerzas Armadas, y publicó la Agenda de Defensa, que contempla el desarrollo de capacidades para la protección cibernética.

La relevancia que tiene esta investigación radica en que analiza un fenómeno global que ha tenido incidencia en todos los países indistintamente de su nivel de desarrollo, capacidades materiales o status, a nivel internacional. A su vez, es un fenómeno que se ha configurado en torno al desarrollo tecnológico, el cual ha sido acelerado, de modo que debe ser tratado oportunamente por todo aquel país que no quiera sufrir desfases en cuanto a su Defensa. Ello supone, que ni el Estado chileno ni el ecuatoriano, pueden dejar este factor por fuera de su doctrina.

Dicho fenómeno se convierte en una prioridad toda vez que complejiza todas las dimensiones en las que se despliega la doctrina de Defensa. Si bien el ciberespacio está desprovisto de cualquier característica territorial, esto no quiere decir que sus amenazas no puedan tener una connotación física. Es decir que, existen amenazas las cuales se pueden estructurar en la dimensión cibernética pero que son ejecutadas físicamente. Ello se debe a que este espacio tiene la capacidad de dinamizar o agilizar la intercomunicación entre personas o grupos de cualquier índole incluido aquellos de perfil ofensivo.

De allí que en el presente trabajo se busque determinar cuál es o son los elementos que refuerzan la adaptación asimétrica de las doctrinas de Defensa de Chile y Ecuador en función del ciberespacio durante el período 2014 – 2018. Para alcanzar dicho objetivo, se procederá a:

- Describir y comprender la arquitectura de ciberdefensa de Chile.

- Evidenciar las capacidades cibernéticas con las que cuenta el Ecuador.
- Ponderar y analizar los factores que han determinado la adaptación desigual entre la doctrina de Defensa de Chile y Ecuador.

Es pertinente resaltar que en el presente trabajo se habla de una adaptación en lugar de cambio de doctrina debido a que las dinámicas que se desencadenan dentro del ciberespacio no son completamente nuevas. El escenario digital es otro espacio del sistema internacional donde chocan los intereses de los distintos actores y la defensa se sigue basando en la protección de aquello que es vital para el Estado (Kasaab 2014). Los conflictos entre países dentro de este contexto se pueden generar sin importar si son tiempos de guerra o de paz, basta con que alguno de los interés de una de las unidades del sistema interfiera con el de otra para que lleguen las discrepancias.

La hipótesis de trabajo que rige a la presente investigación es que el ciberespacio ha afectado de manera asimétrica a la doctrina de Defensa del Estado chileno y del ecuatoriano, países que cuentan con principios dogmáticos similares, con Chile presentando mayores capacidades en términos de Ciberdefensa para hacerle frente a las amenazas informáticas. La variable dependiente de esta conjetura es, la doctrina de Defensa de Chile y la doctrina de Defensa de Ecuador, mientras que la variable independiente es el ciberespacio.

Uno de los principales aportes que genera este análisis es de carácter metodológico ya que es la primera tesis en FLACSO Ecuador en utilizar process tracing como método, mismo que permite analizar ampliamente aquellos sucesos que han intervenido dentro de un fenómeno. Tiene como objetivo abrir la "caja negra" de las relaciones causales, es decir que va más allá de la sola asociación de varios fenómenos. Ello contribuye a la prueba y el refinamiento de diversas teorías, así como también, permite la utilización de diversos enfoques teóricos, lo cual es coherente con la diversidad del campo disciplinario de las Relaciones Internacionales (Aviles 2018).

Otro de los aportes de la presente investigación se basa en que genera una pauta para analizar en América del Sur la incidencia del ciberespacio en las doctrinas de Defensa, campo que muchas veces suele ser asimilado o dado por hecho dentro de las investigaciones que se hacen en base a la Seguridad Nacional. En la práctica, la protección de la soberanía del Estado cuenta con características propias que requieren de un análisis específico. El ciberespacio

como se expuso anteriormente presenta riesgos a la supervivencia del Estado los cuales requieren una investigación a fondo para poder generar estrategias de Defensa efectivas. Esto supone que la contribución del trabajo en cuestión no se enmarca únicamente en la academia, sino que los conocimientos generados en este, igualmente puede ser de utilizad para la toma de decisiones en torno a la Ciberdefensa. Si se dimensiona los efectos que puede tener el ciberespacio para la supervivencia del Estado, se toma en cuenta la dependencia que tiene el mismo de las tecnologías de la información, y se analiza por qué su impacto puede ser diferente en un país u otro, se podría manejar la adaptación doctrinaria de Defensa con un carácter preventivo más que reactivo. Ello disminuye los costos de operación ya que minimiza la vulnerabilidad del país frente a los ciberataques.

2. Metodología y técnicas de recopilación de información

La metodología que se utilizará en el presente trabajo será de carácter cualitativo la cual, de acuerdo a Lamont, se emplea para comprender de mejor manera la forma en la que se ve el mundo, ya que toma en cuenta los significados o subjetividades que subsisten en los fenómenos a investigar (Lamont 2015). La pertinencia de este tipo de metodología radica en que lo que se pretende dentro de esta investigación es explicar cuáles han sido las variables intervinientes que han reforzado la adaptación asimétrica entre las doctrinas de Defensa de Chile y Ecuador en torno al ciberespacio. Admite la visualización de acepciones que subsisten en las experiencias vividas por cada país en relación a este espacio virtual mediante las cuales han establecido sus principios dogmáticos.

La investigación cualitativa se diferencia de la investigación cuantitativa debido a su forma de validar a la teoría y de analizar los fenómenos. La segunda considera que el investigador puede estar separado del objeto de estudio, que las teorías deben tener capacidad predictiva y que los fenómenos pueden ser replicables en un ambiente artificial (Lamont 2015), mientras que la primera considera que el investigador no puede separarse del objeto de estudio de forma que debe ir a realizar observaciones en el lugar donde se está configurando el fenómeno (Creswell 2014). Esta especificidad de la metodología cualitativa permite comprender fenómenos sociales que se desarrollan en nuevos contextos tales como el ciberespacio (Flick 2007).

La observación del problema, tomando como casos a dos países, es importante para conseguir comprender las particularidades del mismo en distintos contextos y desde distintas

realidades. Ayuda a cotejar los documentos escritos, concebidos como instrumentos que forjan procesos con respecto a las vivencias de cada actor. En virtud de ello, se puede elevar la investigación y generar conocimiento que no solo tenga fines científicos, sino que también tenga relevancia práctica y pueda emplearse para dar soluciones apropiadas (Flick 2007). Otra característica de este tipo de investigación que contribuye a analizar el fenómeno que compete a esta tesis es su visión holística. Esto admite la utilización de diferentes perspectivas teóricas en función de dar razón de aquellas subjetividades que forman parte del objeto de estudio y que a su vez lo vuelven más sofisticado (Creswell 2014). De modo que permite la examinación de una gama más amplia de significados y consideraciones. Dado que la dimensión en el que se desarrolla la problemática presenta nuevos actores, desafíos, afectaciones y dinámicas, no se la puede analizar desde una sola perspectiva teórica, hacerlo significaría inconsistencias dentro del trabajo ya que no contaría con las herramientas analíticas suficientes. Se requiere la utilización de varias corrientes teóricas para poder dar cuenta de este fenómeno.

Específicamente se realizará una comparación entre dos países utilizando Process Tracing como método, el cual posee un amplio espectro de posibles comparaciones. Admite el cotejamiento de variables, casos o ambas. Este tipo de exploración permite dar cuenta de un fenómeno particular que resulta desconcertante a simple vista (Beach y Brun 2013). Da profundidad a la investigación puesto que permite observar aquellos eventos que subyacen en el fenómeno mismos que han ocasionado un efecto determinado. En resumen, lo que se busca con esta estrategia es rastrear una secuencia de sucesos que produjeron el resultado que se quiere explicar (Lamont 2015).

Este método permite visibilizar una causalidad asimétrica, congruente con la adaptación doctrinaria desigual que se asume existe entre la Defensa de Chile y Ecuador. En este sentido, los elementos contextuales adquieren gran importancia ya que son aquellos que nos permitirán respaldar dicha relación causal (Aviles 2018). Se ha seleccionado países como casos de análisis puesto que posibilita las comparaciones múltiples dentro de un mismo marco analítico. También porque este contexto es el más apropiado o lógico si lo que se quiere confrontar son aspectos de carácter estatal.

Para ello se compararán “Causal Process Observations” (CPOs), datos clave que proporcionan información sobre el contexto y el proceso, lo cual es útil para poder establecer una inferencia

causal (Beck 2010). Los CPOs se establecerán mediante el análisis documental de textos que den cuenta sobre aspectos políticos, legislativos, institucionales y económicos, de ambos países, en materia de Ciberdefensa. Una vez realizado esto, se procederá a analizar cuáles de los CPOs son necesarios y cuales suficientes para que se dé la relación asimétrica en la adaptación doctrinaria del Estado chileno y el ecuatoriano.

Con el fin de discriminar la relevancia de cada uno de los "Causal Process Observations", se hará uso de tablas de verdad. Estrategia que será de utilidad en cuanto a poder mapear las configuraciones causales (Aviles 2018). Las tablas de verdad serán construidas en base a fuzzy sets, de tal manera que se pueda aislar aquellos factores que son necesarios y aquellos que son suficientes. Los fuzzy sets contribuyen con la constitución de grupos de elementos que guardan cierta correspondencia, de tal manera que se llegue a establecer conexiones lógicas entre las condiciones causales y el resultado que se está estudiando (Mendel y Korjani 2012).

Ejemplo de tabla de verdad:

- Tiene = 1
- Carece = 0
- Variable interviniente necesaria = 1 1
- Variable interviniente suficiente = 1 0

CPOs	Chile	Ecuador
Institucionalidad	1	1
Capacidades técnicas	1	0

Resultados:

- Institucionalidad = Variable interviniente necesaria
- Capacidades técnicas = Variable interviniente suficiente

Entre los CPOs suficientes se deberá ponderar cual es el que refuerza la adaptación asimétrica que se articula entre la doctrina de Defensa de Chile y Ecuador. Esta ponderación se realizará a través de los hallazgo que se establezcan en los, documentos oficiales ya que en ellos se

reflejan los factores que han tenido mayor relevancia para los tomadores de decisiones en cada país y que en definitiva caracteriza el fenómeno a analizar.

Para la obtención de datos se cuenta con fuentes primarias y fuentes secundarias. Las fuentes primarias son aquellas en las que el autor ha obtenido los datos directamente y que no ha pasado por un proceso de edición. Las fuentes secundarias se basan en el análisis de las fuentes primarias las cuales han sido editadas. En la presente tesis se hará uso de ambas fuentes para poder llevar a acabo el análisis documental mediante el cual se procesará la información y se extraerán aquellos datos que sean de utilidad para la investigación. La forma de análisis documental que se implementará en este trabajo es el análisis de contenido mediante el cual se tomarán ciertas palabras clave que hagan alusión a la temática que se está tratando para poder establecer patrones de comunicación o de disparidad (Lamont 2015). Como fuentes primarias se analizará:

- El Plan de Defensa Nacional de Chile
- La Política de Ciberseguridad de Chile
- Las leyes en materia de ciberdefensa de Chile
- El Libro de Defensa de Chile
- La Agenda de Defensa Nacional del Ecuador 2014-2017
- El Plan de Seguridad Integral del Ecuador 2014-2017
- Las leyes en materia de ciberdefensa de Ecuador
- El Libro de Defensa de Ecuador

Se hará uso de estas fuentes primarias dado que en los planes de Defensa y Seguridad se encuentra reflejada de manera explícita la doctrina de cada país. En las leyes y políticas ocurre lo mismo, con la diferencia de que estos documentos proporcionan información acerca de otros campos que abarca la Defensa habilitando el análisis de qué tópicos han sido tratados como prioridad del Estado y contrastarlos con los apartados dirigidos a la Ciberdefensa. Los libros de Defensa serán de utilidad para poder evidenciar la doctrina militar que se sujeta directamente a la doctrina de Defensa.

Como fuentes secundarias se examinarán libros y artículos redactados por académicos expertos en temas de Defensa los cuales son convenientes ya que brindan diferentes

perspectivas analíticas que facilitan el abordaje de las fuentes primarias. Cuando se hace uso de este tipo de instrumentos se debe verificar la perspectiva desde la cual está escribiendo el autor de lo contrario se podría utilizar textos que rivalicen con el marco teórico que preside la tesis. También se tomarán en cuenta artículos de revistas militares mismos que aportan datos igualmente útiles para el presente trabajo pues provienen de autores que han formado parte de Fuerzas Armadas, así como de académicos.

A su vez se procederá, de ser posible, a realizar entrevistas semiestructuradas a oficiales de alto rango de las Fuerzas Armadas y a expertos en materia de Defensa tanto de Chile como de Ecuador. La pertinencia de este tipo de entrevistas reside en que el tiempo del que disponen estos profesionales puede variar y estas proveen cierta flexibilidad al investigador. Ello debido a que en esta estrategia el entrevistador posee una serie de preguntas que le ayudarán a organizar la entrevista, sin embargo, el orden en el que se planteen las mismas podría variar. Las preguntas funcionan a modo de marco referencial dejando al investigador un margen de libertad para poder hacer más preguntas de considerarlo necesario (Bryman 2012).

Las entrevistas tienen un amplio espectro de aplicación y no contienen limitaciones espacio temporales (Díaz, y otros 2013). Estas se van a realizar para establecer hallazgos que no podemos determinar únicamente mediante el análisis documental. Además, serán de utilidad para identificar si existe congruencia entre los textos y la percepción de los actores ya que posibilita la visualización de aspectos subjetivos que no son abiertamente observables.

Capítulo 1

Aproximación teórica: la adaptación doctrinaria de la Defensa, en torno al espacio cibernético, de Chile y Ecuador

En el presente capítulo se pretende alcanzar una articulación teórica que permita explicar la vinculación que existe entre el ciberespacio, los factores intervinientes y la asimetría que subsiste en la adaptación doctrinaria de Defensa de Chile y Ecuador. Las perspectivas teóricas que se utilizarán para poder responder a la hipótesis de la presente tesis son: el realismo estructural o neorrealismo, el constructivismo y la Escuela de Copenhague. Estas tres teorías de principio podrían parecer incompatibles, ya que la primera maneja un determinismo estructural mientras que las dos últimas se decantan más por la mutua constitución entre el agente y la estructura. No obstante, para el presente problema de investigación que supone un carácter global, es necesario utilizar algunos de sus preceptos ya que cada uno de ellos nos ayudará a explicar ciertos aspectos del fenómeno.

La primera postura teórica permite dar cuenta del accionar de Chile y Ecuador en un entorno anárquico como el espacio cibernético. A su vez, ayuda a comprender en parte como es que, aunque ambos países sudamericanos hayan adaptado sus doctrinas de Defensa en torno al ciberespacio para así precautelar su supervivencia, su proceso difiere. Desde esta perspectiva se puede analizar cómo es que el poder de un país, basado en sus capacidades, puede influir en las acciones que toma en función de su Defensa. De igual manera, se puede dilucidar de qué manera la estructura incide en el desarrollo de habilidades. Sin embargo, su debilidad se fundamenta en el estatocentrismo y la importancia que le otorga a la estructura.

El constructivismo es la teoría que ayuda a dilucidar con mayor claridad la desigualdad existente entre los casos de estudio, ya que toma en cuenta un factor crucial para el proceso de adaptación doctrinaria de Defensa que son los significados intersubjetivos. Las significaciones intersubjetivas de la realidad que comparte un Estado con otro, pueden influenciar a los actores a que actúen de una manera determinada y diferente de otros. El posicionamiento que tiene un actor dentro del sistema internacional es otro elemento que afecta a este proceso, ya que la mutua constitución que existe entre los agentes y la estructura, hace que la toma de decisiones sea específica.

Si bien el constructivismo provee ciertas herramientas para analizar el fenómeno en cuestión, toma al Estado como el actor principal de las relaciones internacionales, de modo que a la hora de hablar de amenazas se enfoca mayormente en aquellas que son tradicionales. Sin embargo, dentro del espacio cibernético se articulan amenazas no convencionales que son estructuradas por diversos actores, y por ello es pertinente tomar a la Escuela de Copenhague para analizar los nuevos desafíos que representa el ciberespacio a la doctrina de Defensa del Estado chileno y del ecuatoriano. A ello se le suma la segurización de esta nueva dimensión que se ha desarrollado en el plano global, misma que ha influido en el accionar tanto de Chile como de Ecuador, y que dicha escuela además analiza.

Estas tres teorías se vinculan en primer lugar en base a la percepción del Estado, todas ellas ven a este como la unidad más relevante del sistema internacional. También se encuentran enmarcadas dentro del debate agente-estructura. A su vez, ven al poder y a las capacidades como un factor primordial que da cuenta del comportamiento de las unidades y que puede diferir entre unos y otros.

1. El accionar de los Estados ante un entorno anárquico: realismo estructural

El neorrealismo, a diferencia del realismo clásico, se enfoca en la estructura ya que esta condiciona el comportamiento de los actores. Kenneth Waltz busca explicar el entorno en el que los Estados deben desenvolverse, y afirma que todos los países actúan en función de su supervivencia y que cualquier otro objetivo que pueda tener este actor estará vinculado a este propósito. El sistema internacional lleva a que los Estados compitan entre sí para aumentar su poder y así tener la capacidad de sobrevivir ya que, al no existir un Gobierno global, los Estados se encuentran en un sistema de autoayuda (Collins 2013).

Un sistema, para el autor antes mencionado, está compuesto por una estructura y unidades interactuantes. La estructura es aquel componente que hace posible pensar al sistema como un todo (Keohane 1986). Son los principios ordenadores ajenos a la voluntad de los actores, pero que condiciona su accionar. Esta determina la forma en que las unidades se interrelacionan y se diferencian funcionalmente entre sí. El relacionamiento que se da entre las partes no se da al azar, sino que se desarrolla de acuerdo a como se posicionan las mismas con respecto a otras (Buzan, Jones y Little 1993). El ciberespacio es evidenciado como esa estructura que condiciona la conducta de sus actores. Inclusive se podría ver al entorno cibernético, desde esta teoría, como una extensión del sistema internacional (Kassab 2014), en

el cual los Estados sudamericanos en cuestión se desarrollan e interrelacionan con otros actores estatales, aunque no son los únicos.

No obstante, la restricción que representa la estructura no genera en los actores conductas similares o idénticas. Las unidades yuxtapuestas y combinadas se relacionan de maneras diferentes dentro de su entorno, de acuerdo al nivel de poder que tengan. La diferenciación en sus actuaciones y a la vez en su relacionamiento puede producir resultados diferentes en cuanto a la manera sobre como un Estado maneja su política doméstica (Waltz 1979). La forma mediante la cual la estructura influencia al comportamiento de las unidades es mediante la socialización y la competencia, mismas que funcionan en base a la racionalidad de los contendientes más exitosos (Vargas 2009). De allí que Chile haya tomado como referente para su proceso de adaptación doctrinaria a la Organización del Tratado del Atlántico Norte (OTAN), mientras que Ecuador no ha expuesto de manera explícita que esté siguiendo el modelo de alguna organización en específico o de algún otro país.

La socialización y la racionalidad, de conformidad con Waltz, se basa en la imitación de prácticas efectivas para alcanzar el poder necesario que le permita proteger su integridad. El racionalismo es esa conexión que existe entre las condiciones que establece la estructura y el comportamiento que tiene el Estado, ya que estos pueden adquirir estrategias correctas. Los Estados deben actuar de manera tal que el sistema no los deseche, en vista de que este se encarga de filtrar a aquellas unidades errantes. La estructura es la responsable de proporcionar estabilidad, por lo que les impone a los países mantener su política doméstica bajo ciertos estándares de racionalidad. Si se apartan completamente de este modelo, lo más probable es que no sean capaces de asegurar su existencia (Vargas 2009).

Las características que tiene el ciberespacio demandan de los Estados acciones inmediatas debido a la velocidad con que se pueden efectuar un sin número de operaciones dentro de este entorno. Motivo por el cual, la mayoría de países han emprendido distintas estrategias en contra de las amenazas cibernéticas. Algunos países han tomado la delantera en cuanto al desarrollo de sus capacidades mientras que otros están iniciando este proceso. Aquellos que se encuentran rezagados se han visto obligados a adoptar o replicar como parte de sus políticas domesticas las acciones que han sido efectivas para otros Estados, a pesar de que hasta ahora no existe un país que haya podido alcanzar una seguridad integral que lo mantenga libre de

amenazas. Lo cual pone en evidencia que existen países que se presentan más vulnerables que otros ante diversos ataques (Enríquez 2012).

El Gobierno chileno ha manifestado que el ciberespacio se ha constituido como un contexto global en un periodo de tiempo relativamente corto. Sus riesgos y desafíos han llevado a los Estados a adoptar ciertas medidas que aseguren su existencia al interior de esta estructura. De modo que, Chile ha emprendido una adaptación de los principios rectores de su Defensa de tal manera que pueda proteger aquellos sistemas fundamentales para el correcto funcionamiento del Estado (Ministerio de Defensa Nacional de Chile 2017). Los desafíos cibernéticos también han generado afectaciones sobre la noción de Defensa del Estado ecuatoriano, mismo que ha tomado conciencia de la importancia que ha adquirido la protección de las infraestructuras críticas con respecto al desarrollo del país (Ministerio de Defensa Nacional del Ecuador 2018).

Para el neorrealismo, el sistema internacional es una estructura anárquica, ya que no cuenta con una autoridad que pueda ejercer control por sobre las unidades y garantice la seguridad o la relativa armonía entre las mismas. Dado que los Estados, independientemente de su tamaño o fuerza, tienen como principal objetivo su subsistencia, ante esta condición que se les presenta, se ven abocados a competir por ella. Esto significa que cada unidad va a tener que buscar la manera de protegerse a sí misma y va a hacer todo lo posible por alcanzar sus propios intereses (Collins 2013). Dentro del espacio cibernético, no existe un marco normativo estricto que regule el accionar de las partes, mucho menos una entidad que los proteja. En este entorno existe una evidente falta de gobernanza (Kasaab 2014) que ha resultado en la búsqueda de medidas individuales por parte de cada país para poder resguardarse y evitar ser eliminados por la estructura.

La naturaleza anárquica del plano global deja a los Estados en una condición de autoayuda, lo cual supone que cada uno de los actores va a perseguir políticas competitivas unilaterales para protegerse a sí mismos mediante la persecución de sus propios intereses. En tal contexto, el conflicto es una posibilidad, pero esta es una realidad difícil de combatir, pues la idea de que algún Estado pueda utilizar la fuerza para debilitar o destruir a otro hace que los países no puedan abandonar sus políticas de autoayuda. De hacerlo, corren el riesgo de disminuir sus capacidades para defenderse y estar vulnerables ante cualquier ataque (Waltz 1979).

A nivel internacional, existe una organización que ha aceptado el reto de crear un marco normativo global que regule el accionar principalmente de los Estados en este espacio, que es la Unión Internacional de Telecomunicaciones (UIT). Empero, estas leyes no son vinculantes hasta que un Estado las implemente en su Constitución. Esto quiere decir que no tiene la capacidad de garantizar la seguridad de ninguno de sus miembros, ya que su adopción está sujeta a la voluntad de los países. Hecho que ha contribuido con la idea de que el camino a seguir para hacerle frente a las ciberamenazas es llevar a cabo estrategias individuales.
En el 2002, la Asamblea General de Naciones Unidas estableció, en una de sus resoluciones que la seguridad virtual debía tener un enfoque principalmente estatocéntrico. Los Estados miembros son considerados como los responsables de promover la Ciberseguridad internacional y gestionar de manera adecuada su propia seguridad (Radu 2014). De modo que, a pesar de ser un planteamiento a nivel de organización, la protección de cada país se maneja a discreción de los mismos.

En tal virtud, y a pesar de haber manifestado que los riesgos cibernéticos deberían ser abordados a través de la cooperación internacional, Chile ha mantenido como parte de su estrategia una adaptación doctrinaria propia. Decisión que se ha manifestado en la estructuración de su Política de Ciberdefensa, con la cual se pretende desarrollar ciertas capacidades que le permitan autoprotegerse (Ministerio de Defensa Nacional de Chile 2017). En el caso ecuatoriano se ha evidenciado que el país también apoya las iniciativas internacionales para poder enfrentar esta problemática, sin embargo, ha optado por estructurar un plan que le permita defenderse. Esto se ha demostrado a partir, no de una política específica, como en el caso chileno, sino de acciones como la creación de infraestructuras de Defensa e iniciativas que promuevan una cultura de protección (Ministerio de Defensa Nacional del Ecuador 2018).

El sistema de autoayuda es unos de los mayores riesgos que existe dentro de un mundo de Estados libres, ya que puede desencadenar una guerra, misma que afectaría a la economía de los países involucrados. No obstante, la sola posibilidad de conflicto hace que los actores del sistema internacional tengan una fuerte inclinación hacia el incremento de sus habilidades para poder proteger sus sistemas indispensables. Para poder lograr esto último, los Estados pueden realizar esfuerzos internos, así como externos que les permita fortalecerse e incluso debilitar a su oponente. Aquellos países que comprenda esto, podrán llevar a cabo estrategias inteligentes y efectivas, mientras que los demás se quedaran en el camino (Keohane 1986).

En el ciberespacio se vive una situación de agresión constante en el que cualquiera de sus unidades puede recibir un ataque independientemente de su naturaleza. Inclusive las grandes potencias se han visto afectadas por un bombardeo constate de agresiones, y aunque sus efectos no han sido tan cruentos como las guerras clásicas, sus efectos sobre la estabilidad del Estado son reales. Contar con la tecnología necesaria puede ayudar a disuadir y hasta desarticular una amenaza, pero si no se cuenta con una política adecuada, no se puede hablar de Defensa (Greathouse 2014). En este sentido, Chile ha adquirido una ventaja importante frente a Ecuador, toda vez que ya cuenta con una política de Ciberdefensa, base sobre la cual se edifica todo el accionar del Estado en función de las ciberamenazas (Ministerio de Defensa Nacional de Chile 2017). Es decir que el Estado chileno cuenta con los cimientos sobre los cuales puede erguir una estrategia más organizada, y por ende una adaptación doctrinaria más concreta.

A nivel doméstico, la estructura política se fundamenta en un ordenamiento jerárquico, mediante el cual las instituciones se relacionan en una dinámica de super y subordinación. Los actores políticos se diferencian entre sí por su grado de autoridad el cual se verá representado en el tipo de funciones que cumple y los alcances del poder que puede ejercer legítimamente. Dicha especificación de funciones y roles se hace presente en todos los Estados y se vuelve más profunda a medida que un Estado es más desarrollado (Waltz 1979).

En la política doméstica de Chile se puede evidenciar este ordenamiento jerárquico, en esta se han establecido los roles y responsabilidades que tienen las diferentes instituciones estatales, que a su vez son complementarias y funcionales para el país. Las instituciones de Defensa están llamadas a la protección externa del país de tal modo que se pueda cumplir con los objetivos nacionales sin la incidencia de otros actores. En este sentido, su sistema de Defensa se ve liderado por autoridades políticas y de Fuerzas Armadas. Esta estructura se mantiene en el contexto cibernético, ya que su política de Ciberdefensa es un marco normativo subsidiario de la política de Defensa, de modo que se mantienen sus principios básicos (Ministerio de Defensa Nacional de Chile 2017).

Ecuador, a nivel doméstico también cuenta con una estructura jerárquica que ha especificado las funciones de sus distintas instituciones. En materia de Defensa, se visualiza al ministro en cuestión como la autoridad política, y al comandante de las Fuerzas Armadas como la

autoridad militar. No obstante, a pesar de que este país cuenta con una política de Seguridad y Defensa, no tiene un marco normativo específico de Ciberdefensa que rija el accionar de los organismos estatales frente a las amenazas digitales, y su relacionamiento con otras instituciones, con la finalidad de que sus funciones no se solapen. Medida que se debe tomar si se quiere realiza una adaptación propicia ante nuevos desafíos, necesidad que se ve plasmada dentro de su Libro blanco (Ministerio de Defensa Nacional del Ecuador 2018).

A nivel internacional, las alianzas se hacen presentes para poder generar estrategias conjuntas que maximicen las posibilidades de protección. Empero, las unidades se muestran reacias a adoptar cualquier política que pueda ir en desmedro de sus capacidades. Esto se debe a que ni siquiera los tratados pueden ser garantía de nada, pues si una de las partes decide engañar a la otra, esta puede quedar sumamente vulnerable ante un ataque. Si bien lo que se debería buscar es solo la protección de aquello que ya se tiene, existen Estados que buscan maximizar sus recursos avanzando más allá de sus fronteras lo cual aumenta la percepción de inseguridad en otros (Collins 2013). Es decir que la mayoría de los países actúa en función de las ganancias relativas, más que de las ganancias absolutas, sobre todo si sus intereses se ven en riesgo.

A lo largo del Libro de Defensa y de la política de Ciberdefensa, el Estado chileno ha manifestado su interés por generar acuerdos con otros países para fortalecer sus capacidades y así poder alcanzar sus intereses nacionales. Ello implica el desarrollo de aptitudes para poder generar contraataques en legítima defensa de ser necesario (Ministerio del Interior y Seguridad Pública 2018). Lo cual se diferencia de las declaraciones ecuatorianas en las cuales no se manifiesta de manera tan evidente una posible ofensiva cibernética y se establece una planificación de carácter defensivo (Ministerio de Defensa del Ecuador 2018). Ecuador persigue, de acuerdo a documentos oficiales, establecer tratados con otros países para aumentar sus posibilidades en función de la neutralización de un ciberataque y no tanto de un contraataque. Desigualdad que se ve reflejada en los cambios doctrinarios que han generado, ya que las habilidades que persigue cada país, para su personal, se diferencian.

Dado que el ciberespacio es otra arena de la política mundial donde se pone en juego la supervivencia del Estado, todos estos actores están dispuestos a hacer lo necesario para defenderse de la amenaza que representan los demás actores. La falta de gobernanza de este entorno deja abierta la posibilidad de que cualquier unidad del sistema pueda destruir la seguridad y la autonomía de un país (Kasaab 2014). De allí que se haga presente en este

contexto la necesidad por parte de los Estados, de generar políticas que puedan minimizar la incertidumbre en torno a su Seguridad y Defensa.

Chile ha avanzado en la incorporación de tecnologías de la información para el manejo de sistemas tanto privados como públicos. Hoy en día, en este país, sectores como el del transporte, la salud y la alimentación dependen de sistemas digitales que funcionan a través del ciberespacio (Ministerio del Interior y Seguridad Pública 2018). Ecuador igualmente ha devenido en la implementación de nuevas tecnologías para digitalizar el sector público (Ministerio de Telecomunicaciones y de la Sociedad de la Información 2016). Esto significa que las infraestructuras vitales de Chile y Ecuador dependen de las complejas dinámicas cibernéticas. Ello incorpora a ambos países en la anarquía de este entorno, la situación de autoayuda y una inevitable competencia para sobrevivir.

Waltz afirma que, dentro de dicha competencia, en una primera instancia todos los Estados son iguales, ya que todos cuentan con el derecho a su soberanía, son independientes y cuentan con la capacidad de tomar decisiones frente a su entorno o para sus propios intereses. Sin embargo, estos se van diferenciando no en base a sus cualidades básicas, sino en términos de poder; unos son más o menos poderosos que otros (Dunne, Kurki y Smith 2010). El poder es el que brinda al Estado las capacidades inmediatas que lo habilitan para luchar y defenderse. Es así que, la doctrina de Defensa se ve supeditada a las variaciones de poder (Waltz 1979). El que un país tenga más o menos poder tiene que ver con la distribución de capacidades.

El principio de distribución se basa en que la estructura hace que las capacidades fluctúen entre las diferentes unidades. Estas capacidades pueden ser económicas, militares, poblacionales, territoriales y políticas. Estos factores son atributos de los Estados, pero su asignación no lo es. La forma en que estas estén repartidas, depende estrictamente de factores estructurales y en base a ello estará definido el relacionamiento de los actores, así como su posicionamiento en el plano internacional. El poder se encontrará medido en función de estas disposiciones (Buzan, Jones y Little 1993).

En este sentido, Chile ha perseguido activamente alianzas estratégicas que le permitan mejorar su posicionamiento a nivel internacional y a su vez incrementar su poder. Los tratados binacionales que ha firmado el país del Cono Sur, constituyen uno de los pilares fundamentales de su estrategia de Ciberdefensa (Estado Mayor Conjunto 2019). A este

respecto, Ecuador también ha incurrido en el establecimiento de acuerdos internacionales con distintos Estados para incrementas sus capacidades, empero la cantidad de acuerdos firmados con los que cuenta Chile, difieren de aquellos que ha podido cerrar Ecuador (Ministerio de Defensa de Ecuador 2018). De igual manera existen países que han firmado un acuerdo de Ciberdefensa con el Estado chileno, que no han firmado con el Estado ecuatoriano.

La forma en que se relacionan las unidades de un sistema tiene que ver tanto con su diferenciación funcional como por el alcance de sus capacidades. En un sistema donde no existe un Gobierno central, las partes se ven diferenciadas por tener más o menos aptitudes para poder desempeñar funciones similares. Un cambio en la distribución de capacidades puede generar un cambio estructural y a su vez transformar las expectativas que se tiene acerca del comportamiento que tendrán los Estados y los resultados que pueden tener sus interacciones (Waltz 1979).

Dentro del ciberespacio, el poder igualmente se manifiesta y es perseguido por sus actores. En este escenario de las relaciones internacionales la información forma parte fundamental ya que lo que se pretende alcanzar es su control (Kiggins 2014). Quien logre blindar aquellos datos que comprometan sistemas sensibles del Estado y conjuntamente logre controlar la información de sus adversarios, corre con una gran ventaja. Siendo así, la asignación de capacidades debería ser relativamente uniforme entre todos los Estados ya que todas las unidades cuentan con las mismas características para ser consideradas como tales. Si se lleva esto a la práctica, dicha premisa no se materializa, ya que las competencias de un país pueden ser muy diferentes con respecto a otros (Buzan, Jones y Little 1993). Por ende, dentro del sistema internacional se puede ver a países que son considerados potencias mundiales y aquellos que son vistos como subdesarrollados.

Al observar los índices de Ciberseguridad que presentó la Unión Internacional de Telecomunicaciones en el 2017, se puede confirmar que, en el plano cibernético, las capacidades difieren entre un país y otro. De acuerdo a los indicadores que utiliza este organismo internacional para realizar su análisis, existen países que cuentan con mayores competencias de Defensa en comparación a los demás (ITU 2017). Si bien la mayoría de tomadores de decisiones de los países han establecido doctrinas relacionadas con la Ciberdefensa, todavía existe una amplia brecha en cuanto a conciencia, comprensión, conocimiento y capacidades para poder desplegar programas adecuados que garanticen el uso

seguro de las tecnologías de la información que contribuyan con el desarrollo estatal. Los países que cuentan con economías en desarrollo encuentran limitaciones con respecto a expertos en Ciberdefensa, educación y aplicación de las leyes.

De allí que, aunque todos los Estados son similares en cuanto a las funciones que deben desempañar, pues el sistema internacional crea los mismos incentivos para todos y los fines a los que aspiran son similares, se diferencian en términos de sus capacidades (Waltz 1979). Es decir que, a pesar de que todos los Estados buscan maximizar sus capacidades materiales para poder asegurar su supervivencia y lograr que el enemigo no obtenga ventajas militares, no todos tienen el mismo poder ni alcanzan sus objetivos de la misma manera (Buzan, Jones y Little 1993).

Países como Chile y Ecuador han comprendido que los ataques cibernéticos, al comprometer la supervivencia del Estado, han dejado de ser una temática que se circunscriba únicamente al ámbito técnico, ha pasado a formar parte del contexto político. Razón por la cual ambos han buscado maximizar sus capacidades en el ciberespacio a través de una adaptación doctrinaria. Chile ha adoptado políticas de Ciberdefensa con el objetivo de desarrollar competencias, de tal modo que el Estado pueda hacerles frente a los desafíos que se le presenten, y de esta forma defender su soberanía. Soberanía que de acuerdo a su Ministerio de Defensa será procurada a través de la protección de las infraestructuras sensibles de la información. Para ello busca desarrollar una estructura robusta y resiliente de la información como parte de su Defensa Nacional que permita la protección de las personas, su información, su identidad y velar por el bienestar económico y social (Ministerio del Interior y Seguridad Pública 2018). De esta manera, se puede generar un avance doctrinario que, de paso a la implementación y aplicación idónea de las habilidades digitales, así como a la capacitación apropiada del personal pertinente.

El Ecuador ha incluido a la ciberdefensa dentro de su plan integral de Seguridad Nacional y ha creado organismos cuya finalidad es la protección de la información, resguardo del ciberespacio, prevención, disuasión y respuesta frente a eventuales ataques (Vargas, Recalde y Reyes 2017). El objetivo que persigue el Gobierno con este tipo de iniciativas es maximizar sus posibilidades de mantener, mejorar y desarrollar nuevas destrezas, las cuales lo posibiliten para gestionar de manera oportuna las amenazas. Además, ha planteado una futura implementación de la catedra de Ciberdefensa como parte de la formación académico militar,

para incentivar la investigación en esta área, propiciando el avance en cuanto a conocimientos útiles a nivel estratégico, operativo y táctico (Ministerio de Defensa del Ecuador 2018).

Estas estrategias denotan un cambio o adaptación de los paradigmas de Defensa Nacional, ya que ambos países han considerado al ciberespacio como una dimensión dentro de la cual se deben resguardar. De este modo, se puede evidenciar que si bien estos Estados persiguen un mismo objetivo, que es la conservación en base a una adaptación doctrinaria, la pertinencia con la que se lleve a cabo este ajuste dependerá de cómo se encuentren posicionados en el plano internacional y de la distribución de capacidades, mismas que se traduce en poder. El poder cibernético depende de los recursos que caracterizan al entorno en el que se desenvuelve y se basa, de acuerdo a Joseph Nye, en la capacidad de utilizar los recursos de la información que se encuentran interconectados para obtener el resultado deseado (Nye 2010).

Esto se traduce en el hecho de que los avances que ha tenido Chile le hayan dotado con mayores potencialidades que Ecuador dentro del ciberespacio (Valenzuela 2018). El Estado chileno ha aprovechado al máximo su alta conectividad para poder transformarse en un centro de innovación empresarial, lo cual ha hecho apremiante generar herramientas de Defensa. Asimismo, ha generado alianzas que han sido de utilidad para afianzar aquellos objetivos propuestos en materia de Ciberdefensa. De acuerdo al Banco Interamericano de Desarrollo, Chile es uno de los pocos países en América Latina que se ha convertido en un referente de buenas prácticas en temas de Defensa (OEA y BID 2016).

El neorrealismo explica parcialmente el problema ya que la rigidez con la que se maneja en esta perspectiva, el concepto de poder, supone una debilidad a la hora de explicar nuevas amenazas y nuevos actores, dos fenómenos que se han manifestado ampliamente dentro del ciberespacio. Para poder adaptarse a un entorno cambiante y confuso es precisa la flexibilidad de los conceptos y la adaptabilidad de las premisas (Kassab 2014). El poder en el ciberespacio ha dejado de ser una cualidad exclusiva del Estado, ya no es un poder meramente político y se traslada a otros actores del sistema internacional. La asimetría en cuanto a las capacidades que posea un actor u otro se diluye ya que el control de la información no es algo exclusivo de los Estados sin importar si son un hegemón o no. Los datos sensibles del Estado se pueden encontrar en manos de individuos que podrían utilizarlos para sus propios fines.

El determinismo estructural es otras de las debilidades que presenta esta teoría, tomando en cuenta que, si bien la estructura puede moldear el accionar de las unidades, las particularidades con las que cuenta cada una de ellas, puede afectar a la configuración internacional. Es decir que la estructura deja de ser esa esfera inmutable que restringe a sus unidades y las moldea. Si se considera la agencia de las partes, se puede comprender como cada actor puede tener una relación de constitución mutua con la estructura que es particular y se diferencia de la relación que puedan tener los otros actores. En el ciberespacio la agencia de las unidades se potencia debido a que la asimetría en términos de poder se vuelve relativa ya que el poder informático puede provenir de diferentes fuentes.

En cuanto a los actores, dentro del plano digital, aunque el Estado sigue siendo la unidad principal, coexisten otras partes que también se disputan el control del internet. Los principales contendientes que buscan regular el uso del internet, a más de los países, son organizaciones internacionales, el sector privados, académicos y organizaciones no gubernamentales (Kasaab 2014). Motivo por el cual una teoría que analiza a los países como los únicos actores del sistema internacional no posee las herramientas suficientes que permiten dar razón de un fenómeno como el que ataña a la presente investigación. Las capacidades dejan de ser tradicionales y objetivas, estas se vuelven cada vez más relativas.

2. Diversas estructuras e identidades estatales: constructivismo

El constructivismo también toma en cuenta a la estructura, pero no la ve como un conjunto de principios único e inamovible. La institucionalización está basada en el acoplamiento de distintos intereses e identidades, de modo que, el sistema de autotutela es una forma específica de institución en la cual se han articulado identidades e intereses particulares, pero no es la única que se puede dar en una situación de anarquía. Para los constructivistas puede haber otro tipo de disposiciones en el sistema internacional como por ejemplo la de la seguridad colectiva, una realidad donde los Estados se perciben no como amenazas sino como parte fundamental para alcanzar su propia seguridad. La seguridad es vista como la responsabilidad de todos dentro de este tipo de estructura (Salomón 2002). Es por esta razón que Chile y Ecuador, dentro de sus respectivas doctrinas de Defensa, han apostado por la participación en iniciativas internacionales que promueven la interacción pacífica entre los Estados, las buenas prácticas y el establecimiento de un marco normativo global.

La interacción entre los Estados puede dar como resultado estructuras más o menos conflictivas. Las principales unidades en las que se organiza el sistema internacional moderno no son egoístas o amigables por naturaleza, sino que lo que representan va de la mano con sus circunstancias culturales, sociales, políticas y materiales. Estas no son estáticas, sino que van evolucionando a medida que van interactuando con su entorno (Dunne, Kurki y Smith 2010). Por lo tanto, las identidades e intereses de los actores no preexisten a sus interrelaciones, sino que se desarrollan en base a las relaciones que generan con otros (Salomón 2002).

> No hay una "lógica" de la anarquía aparte de las prácticas que crean y que representan una estructura de identidades e intereses concreta en lugar de representar otra; la estructura no tiene ni existencia ni fuerza causal separada del proceso. La autoayuda y la política de poder son instituciones, no características esenciales de la anarquía. La anarquía es lo que los estados hacen de ella (Wendt 2005, 5).

Enmarcado en este principio, el Estado chileno considera que para poder contrarrestar los desafíos que supone el ciberespacio se debe incurrir en la cooperación internacional con otros países y organismos de tal forma que se pueda acceder a un entorno digital seguro. De modo que este país se ha mostrado predispuesto para la participación en el establecimiento de medidas de transparencia, mismas que promueven la confianza entre actores, ya sean bilaterales o multilaterales (Ministerio del Interior y Seguridad Pública 2018). El Estado ecuatoriano coincide con dicha perspectiva y ha declarado su interés por fomentar la convivencia pacífica, en el plano global, enmarcada en el respeto (Ministerio de Defensa de Ecuador 2018).

La anarquía, que le es inherente al espacio cibernético, ha adquirido una connotación conflictiva debido a que es una estructura que representa un conjunto de identidades e intereses relativamente estáticos. Las significaciones colectivas que han creado los Estados en torno a este ambiente virtual son las que lo han constituido como una estructura sin gobernanza ni gobernabilidad, la cual igualmente configura el accionar de estos agentes. Las estructuras no son objetos reificados, inmutables y eternos, por el contrario, mutan mediante la praxis de los Estados (Guzzini y Leander 2006). Si los países tuvieran percepciones o ideas distintas de este entorno, su carácter anárquico dejaría de ser sinónimo de conflicto. Tanto para Chile como para Ecuador el ciberespacio representa un entorno conflictivo, el cual ha

presentado desafíos importantes para la política doméstica y el derecho internacional debido a las malas prácticas de sus actores.

Las estructuras suelen ser mantenidas en el tiempo debido al costo que implica el cambio y a que genera patrones de conducta. Se podría decir que las diferentes estructuras se ven como algo inalterable ya que estas pueden reducir la incertidumbre con respecto al accionar de los Estados. Pero en la práctica, los agentes cuentan con la capacidad de incidir en la estructura tanto como la estructura en ellos. En este punto se denota la mutua constitución entre agente y estructura (Wendt 2005). A pesar de que para ambos países sudamericanos el espacio cibernético es sinónimo de conflicto, las representaciones que cada uno ha generado en torno al mismo podrían ser diferenciadas debido a las experiencias que hayan tenido al interior del mismo.

Las significaciones colectivas que comparten los Estados, a su vez se desprenden de sus interacciones en el sistema internacional. Estas también forman parte de la constitución de distintas estructuras, en las cual los países se manifiestan de maneras diversas ya sea para contribuir o para solucionar un problema (Salomón 2002). Ello quiere decir que si los países, mediante su relacionamiento han adquirido intereses e identidades egoístas, se van a concebir en una situación de autoayuda y se generará una estructura en la cual el conflicto es latente. Si los Estados se relacionan con otros actores, los cuales se muestran menos conflictivos, entonces la concepción de una estructura donde la cooperación pueda ser alcanzada, se hace más real. Esto también podría ser posible si los Estados se preocuparan por alcanzar el bien común o intereses comunes.

A pesar de que el entorno digital ha llevado a los países a tomar acciones individuales, estos son conscientes de que un fenómeno global como este necesita de estrategias colectivas que ayuden a contener sus desafíos. En base a dichas estrategias se busca llegar a un compromiso por parte de todas las unidades para tratar de afectar a la estructura y generar alternativas ante el conflicto. El Estado chileno, dentro de su política de Ciberdefensa, considera que una de las mejores formas de hacerle frente a los desafíos transfronterizos que supone el ciberespacio es establecer relaciones de cooperación con otro Estados, con organismos internacionales y participar activamente en iniciativas globales que promuevan un espacio seguro (Ministerio del Interior y Seguridad Pública 2018).

El Gobierno chileno se ha mostrado presto a acatar los tratados internacionales e interpretarlos de tal manera que puedan concordar con la política exterior del país. También, expone que su Defensa Nacional proporcionará ayuda para la creación de mecanismos que permitan alcanzar una seguridad colectiva y a su vez con la posterior implementación. De modo que, Chile busca promover y adoptar códigos de conducta que promulguen la paz y la seguridad internacional dentro del ciberespacio (Ministerio del Interior y Seguridad Pública 2018), accionar que denota la agencia del Estado chileno para afectar a la naturaleza de esta estructura y generar nuevos significados en torno a la anarquía.

Ecuador se visualiza como un Estado que actúa y actuará, en el contexto internacional, de conformidad con los principios de soberanía y cooperación. En concordancia con ello, fomenta la convivencia pacífica y la solución de conflicto mediante vías diplomáticas, por lo que apoya y contribuye, al igual que Chile, con la creación de medidas de confianza mutua. Todo esto sin dejar de lado el hecho de que hará uso de la fuerza si los intereses nacionales se ven comprometidos. Promueve iniciativas globales para mantener un entorno regional y un sistema internacional estable y seguro en todos sus ámbitos, incluyendo la arena digital (Ministerio de Defensa Nacional del Ecuador 2018).

El Ministerio de Defensa Nacional del Ecuador (MIDENA) plantea que se coordinaran acciones conjuntas e intercambio de información con otros países conforme a los tratados e instrumentos internacionales que se encuentren acordes o que no se vayan en contra de la constitución ni de las leyes del país. Se muestra presto a colaborar con toda estrategia que tenga como principal objetivo la consecución de un bien común, es decir proyectos en los cuales todos los países obtengan beneficios (Ministerio de Defensa del Ecuador 2018). Se deja de pensar únicamente en los beneficios relativos sino también en los absolutos, evitando ver al conflicto y la desconfianza como la única alternativa dentro de una estructura sin un Gobierno central.

El constructivismo hace énfasis en el ámbito ideacional para dar cuenta de que los Estados en realidad no son iguales, difieren en cuanto su proceso de construcción identitaria y a los intereses que persiguen, por lo cual para analizar su comportamiento es importante tomar en cuenta los significados intersubjetivos que comparte entre sí, al interior del plano global (Guzzini y Leander 2006). Esto significa que las ideas pueden influir más en el accionar de los países que su poder valorado mediante capacidades materiales. A manera de ejemplo se

puede citar que el comportamiento de un país con respecto a otro diferirá de acuerdo a los valores que comparta o no con ese otro.

> La identidad es fundamental para la investigación del constructivismo por una razón básica: la identidad nos dice quiénes son los actores, cuáles son sus preferencias e intereses y cómo la preferencia podría informar sus acciones. Simplemente, el interés no puede persistir sin una identidad particular y las identidades, el interés y el comportamiento de los agentes políticos se construyen mediante interpretaciones y suposiciones de significados colectivos sobre el mundo (Adler 1997, 324).

No se puede asumir que en esta arena del sistema internacional los actores tengan una concepción de sí mismos y de su entorno anterior a la interacción, ya que un país no puede identificarse a sí mismo sin tener conciencia de que existe un otro. El Estado no puede tener intereses e identidad por fuera de la praxis internacional (Salomón 2002). Por ello analizar las interacciones que han tenido Chile y Ecuador entre sí y con otros países en el ciberespacio es necesario, si lo que se quiere es analizar una asimetría dentro de un mismo proceso. Ello debido a que "el significado en torno al cual se organiza la acción surge de la interacción" (Wendt 2005, 12).

Los agentes se relacionan con las unidades que se le presentan en la realidad según el significado que compartan con ellas. Los Estados reaccionan de una manera con aquellos agentes que son sus amigos y de diferente manera con aquellos que son sus enemigos, pues representan una amenaza. Las ideas que comparten ciertos Estados son aquellas que de una u otra forma inciden en su accionar y dan sentido a sus intereses. Estas ideas pueden ser valores como la democracia o el comunismo; si yo comparto con otro actor los mismos valores, lo más probable es que no me represente una amenaza y que respete mi soberanía, es decir que lo puedo ver como un amigo. A aquellos países que no comparten mí misma corriente de pensamiento los veo como adversarios ya que, su accionar es incierto o impredecible para mí (Wendt 2005).

Esto se puede ver asociado con los círculos sociales de George Simmel. Para este autor, el proceso identitario del ser humano se desarrolla en torno a los círculos sociales a los que pertenece. Cada círculo social se constituye en base a intereses que son compartidos por sus integrantes. Si se ve cuáles son los intereses que una persona comparte en cada circulo, nos va

a dar una formula única, que representa su identidad (Souto 2015). En el plano global se podría hablar de círculos internacionales, los cuales son representados por los diferentes organismos. Dentro de estas organizaciones, sus miembros comparten valores específicos que son los que los han llevado a asociarse. Los Estados no suelen pertenecer a una sola organización, sino que son miembros de varias instituciones con las cuales se sienten identificados. Si se analiza las diferentes instituciones a las que pertenece un país y cuáles son las significaciones intersubjetivas que comparte, se puede tener como resultado la identidad de esa unidad y se develará aquellas características que la diferencian de las demás.

La política exterior de Chile, así como la de Ecuador, han pasado por diferentes etapas y sesgos ideológicos, los cuales han ido de la mano de distintos periodos de gobierno. Esto ha generado que la imagen de estos países haya cambiado a nivel internacional, al igual que su relacionamiento con las unidades del sistema y sus significados intersubjetivos. A modo de breve reseña, se puede observar que, durante la presidencia de Salvador Allende, a pesar de tener una ideología de corte socialista, existía la conciencia de que un país joven como Chile necesitaba generar relaciones con la mayor cantidad posible de países, sin importar si tenían una afinidad de pensamiento o no. En esta época Chile buscaba abrirse y posicionarse en el contexto internacional. Con Augusto Pinochet se inició una deliberada guerra contra el socialismo soviético y se demostró una fuerte desconfianza en cuanto a organizaciones de origen multilateral. Chile se aleja políticamente de Naciones Unidas y de la Organización de Estados Americanos (OEA) y rompe con su tradición de presentar una imagen prestigiosa ante el mundo (Perry 2009).

Con el retorno a la democracia en Chile, cuando Patricio Aylwin fue electo como presidente, se pone de manifiesto la necesidad de restaurar los lazos que se rompieron durante la dictadura (Perry 2009). Los presidentes que lo sucedieron han mantenido la imagen del país abierta a la cooperación internacional en todos los ámbitos, lo cual incluye al ámbito de la Ciberdefensa. En este último aspecto, el Estado chileno se ha posicionado como un país que participa activamente en propuestas lanzadas principalmente por Naciones Unidas, la Organización de Estados Americanos y el Consejo de Defensa Suramericano de la Unión de Naciones Sudamericanas (Ministerio de Interior y Seguridad Pública 2018). Propuestas mediante las cuales se puede llevar a cabo un intercambio de información con países que tienen una mayor trayectoria enfrentándose a los desafíos cibernéticos.

Dentro de la Defensa ecuatoriana, indistintamente del periodo de gobierno, desde el siglo XX se ha visto a la cooperación multilateral y bilateral como un eje fundamental para alcanzar los objetivos nacionales. Ecuador se declara convencido de que el multilateralismo es la forma más adecuada de resolver problemas de carácter global (García 2008) como lo son las ciberamenazas. Es por ello que propuso la creación de la Escuela Sudamericana de Defensa como parte de la Unión de Naciones Suramericanas (UNASUR), donde se buscaba promover la capacitación académica de personal civil y militar. El objetivo principal de esta iniciativa era afianzar una identidad regional a través de pensamientos propios y potencializar las capacidades de cada uno de los Estados miembro (Ministerio de Defensa Nacional del Ecuador 2013).

Los teóricos constructivistas dan un papel relevante a las organizaciones internacionales dentro de sus estudios, ya que influyen en los procesos de reconfiguración de intereses de los Estados (Salomón 2005). Ello ya que todos los que pertenecen al mismo círculos son afines, mientras que aquellos que no la haces, si bien no son mis enemigos en estricto rigor, son diferentes. Los significados intersubjetivos que comparten los Estados son aquellos que rigen en gran medida su comportamiento y que estructuran sus objetivos. A partir de ellos, se podría saber si un país es amigo o enemigo, si respetará los acuerdos internacionales y la soberanía de los demás o qué tipo de utilización le dará a su poder. Los Estados miembros de un organismo, como participantes en procesos globales, comparten significaciones acerca de una problemática ante la cual deben actuar. A partir de ello buscan anticiparse de mejor o peor manera a los desafíos que se les presentan y establecen sus estrategias. (Wendt 2005).

Como ejemplo se puede ver el papel que ha tenido la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) en la reestructuración de políticas en varios Estados miembros, a partir de procesos de reconfiguración de intereses estatales. La Organización del Tratado del Atlántico Norte (OTAN) es otro ejemplo, ya que ha incidido en la construcción de las percepciones mutuas entre sus miembros y sus intereses acerca de su Seguridad. Esto es lo que ha hecho la organización citada con la Unión Europea. Ha creado estándares en cuanto a lo que se espera que haga un país para alcanzar una Seguridad optima (Salomón 2005). No obstante, muchas veces las organizaciones no solo inciden en sus propios miembros, sino que sus principios suelen ser vistos como modelo a seguir por otros países que no lo son pero que a lo mejor quieren llegar a serlo.

Chile desde el año 2000, a través del Ministerio de Defensa ha firmado varios acuerdos en los cuales se dispone el cumplimiento de las normativas y estándares de la OTAN. Esto supone mantener una compatibilidad tecnológica, doctrinaria y procedimental con dicho organismo (Hess 2015). La búsqueda que ha emprendido este país para cumplir con los parámetros que son necesarios para alcanzar el modelo de Defensa de los Estados miembro de la Organización del Tratado del Atlántico Norte, lo han abocado a generar un ajuste en su sistema. Es decir, que ha tenido que destinar recursos para poder incrementar sus capacidades y poder alcanzar ese modelo de desarrollo.

En el Libro de Defensa de Chile del 2017, ya se constituye un cambio paradigmático en cuanto a la Defensa Nacional, preparado por el Ministerio y el Estado Mayor Conjunto de las Fuerzas Armadas. Mediante este proceso el Estado busca acercarse a los estándares más altos a nivel internacional. Para ello se utiliza como referencia los parámetros que maneja la OTAN y su metodología conjunta de planificación operacional. En relación al ciberespacio, se utilizan los conceptos de soberanía y jurisdicción desarrollados en el manual de Tallin 2.0 sobre normas del derecho internacional aplicables a operaciones realizadas en el espacio cibernético (Ministerio de Defensa Nacional de Chile 2017). El Ejército chileno ha participado en la Fuerza Militar Multidimensional de Estabilización (SFOR), bajo la instrucción de la OTAN (Ejército de Chile 2019).

Ecuador como miembro de la Organización de Estados Americanos históricamente a buscado tener una intervención activa dentro de esta organización y su participación en las cumbres lo han demostrado. A diferencia de Chile, también miembro de la OEA, pero que toma a la OTAN como referente dentro de su política de Defensa, el Estado ecuatoriano, dentro de su Libro Blanco, vincula su estrategia de Defensa Nacional directamente con la política regional y hemisférica establecida por la OEA y la Junta Interamericana de Defensa. Toma como modelo a los parámetros que se especifican en los instrumentos de seguridad propuestos por la entidad en cuestión, los cuales promueven la confianza entre Estados, la conservación de la estabilidad y la consecución de la paz hemisférica (Ministerio de Defensa Nacional del Ecuador 2018).

Los agentes adquieren identidad en base a sus expectativas e interpretaciones, la cual es relativamente estable y coherente con el papel que desempeñan en el plano global. Todo Estado desempeña un rol diferente dentro de la construcción de los significados colectivos.

Esto supone que al igual que las personas, los países presentan diversas identidades dependiendo del papel que estén cumpliendo dentro de un entorno específico. Estos actúan de diferente manera a nivel doméstico y a nivel global, ya que su posicionamiento no es el mismo. En otras palabras, los países pueden tener varias identidades en función del papel que desempeñan en la estructura, ya sea como soberano, como potencia mundial, como país periférico o como líder regional. De igual manera el compromiso y la importancia que adquiere cada identidad, varía en cada país (Wendt 2005).

El Estado chileno y el ecuatoriano han tenido posicionamientos distintos a nivel regional y global, lo cual ha incidido en las representaciones que han creado en virtud de las amenazas. Existe una relación causal entre las interacciones y las estructuras, entre lo que es un Estado a nivel individual y su comportamiento a nivel internacional. Dicho de otra manera, existe una vinculación directa entre lo que "son" y lo que hacen (Wendt 2005).

Chile defiende el modelo económico neoliberal, es decir una economía abierta al mercado mundial y gran parte de su crecimiento económico se ha debido a los tratados de libre comercio que ha firmado con diversos países. La firma de estos tratados con las economías más fuertes a nivel mundial puede generar grandes oportunidades y beneficios para una economía como la de este país sudamericano y darle poder en la región. Empero también supone grandes desafíos y obligaciones que implican la aplicación de políticas de Defensa adecuadas que contemplen los avances tecnológicos (Schmidt 2006).

Ecuador de acuerdo al Instituto Económico Suizo es un país poco global, ubicándolo en el penúltimo lugar a nivel América Latina dentro del índice de globalización. Su puesto se debe a las restricciones económicas que tiene el país, las barreras arancelarias que impone a otro países y la falta de tratados de libre comercio (Merlo 2017). No obstante, Ecuador se ha visto inmerso en un proceso de transformación de su modelo económico hacia una economía más abierta, lo cual lo ha insertado en el mercado mundial, tal vez no en la medida que lo ha hecho Chile, pero si lo suficiente como para tomar a las ciberamenazas como una problemática latente que compromete su economía. Para el 2016, el Gobierno ecuatoriano firmó un Tratado de Libre Comercio con la Unión Europea, generándose así otro frente que defender en el plano cibernético (Vicepresidencia de la República del Ecuador 2016).

Dado que las identidades son la base de los intereses, estos también difieren entre unos Estados y otros. El rol que cada país desempeñe en el plano internacional definirá sus intereses sin importar el grado de relevancia que este tenga (Wendt 2005). En el caso de Chile y Ecuador, se puede observar que ninguno de los dos países en cuestión ha tenido un papel preponderante dentro del fenómeno cibernético, no obstante, han generado propensiones alrededor de este, ya que los ha afectado de una u otra manera. Esto significa que la combinación de factores materiales e ideológicos pueden arrojar resultados diversos (Dunne, Kurki y Smith 2010).

De este modo, la adaptación doctrinaria de Defensa de Chile y Ecuador se ve vinculada a las percepciones que tiene cada una de las amenazas, sus significaciones intersubjetivas mediante las cuales se asocian a una u otra organización internacional y su posicionamiento dentro de las mismas. Factores que combinados tienen un efecto diferenciado en el proceso. A ello se le debe sumar el relacionamiento distinto que tiene cada uno con diversos agentes internacionales y las distintas organizaciones a las que pertenecen. Esto genera identidades específicas en cada uno de ellos, las cuales afectarán a la normativa doméstica.

En este sentido, la mayoría de países de América del Sur, cuando se habla de tecnología, consideran que lo más adecuado es generar alianzas con potencias mundiales, ya que de esta forma obtendrían ciertos beneficios que les dan ventaja sobre los demás. Es así que el Estado chileno durante el 2018 inició la preparación de su postulación como país no-OTAN (Aránguiz 2018). Si se llega a ese status, se obtiene una variedad de ventajas militares y proyección de trabajo conjunto con las Fuerzas Armadas Estadounidenses.

Esta teoría, como se veía al inicio del presente apartado, marca una innovación dentro del debate agente estructura. Se considera un punto medio ya que no ve a la estructura como el determinante de todo aquello que ocurre a nivel internacional, ni tampoco se aferra al hecho de que el agente es el que determina a la estructura íntegramente. La influencia que tienen ambos, de acuerdo al constructivismo, permite ver la diferenciación de los procesos que constituyen la identidad de un Estado y deja de lado la perspectiva de que todas las unidades tienden a ser homogéneas o pretenden serlo. Si lo llegan a ser no es porque existan disposiciones ajenas a ellas que las restringen; si lo hacen es debido a que comparten significados o valores que las han llevado a asociarse, y aun así no llegan a ser idénticas.

Los obstáculos que se le presentan a esta teoría, y que no le permiten ser la más adecuada para explicar el problema que compete al presente trabajo, radican en las ciberamenazas y sus autores. Si bien proporciona herramientas para poder comprender las identidades e intereses de cada Estado, en torno a la Defensa, estos factores surgen en función de otros países. A pesar de tener una base sociológica, analiza al Estado como el agente en el sistema internacional y a aquellas amenazas que son configuradas por otros agentes de iguales características. Se habla de una sociedad internacional, pero esta está constituida por Estados que cuentan con identidades propias. En otras palabras, se le da al Estado dentro del ámbito internacional, las mismas características que se le da al individuo actuante dentro de la sociedad.

No obstante, en el ciberespacio los Estados no solo se relacionan entre sí, comparten esta dimensión con actores, que inclusive carecen de institucionalización formal, pero que también son capaces de incidir en la estructura. De manera que el relacionamiento con estos agentes puede ser un factor fundamental para poder comprender la diferenciación en cuanto a la adaptación doctrinaria de Chile y Ecuador. La tipificación que hagan de los perpetradores de ciberataques y la conciencia que genere cada país de los diferentes riesgos que corren, hará que les den mayor prioridad a algunos aspectos de la Defensa que a otros.

3. Segurización de amenazas no convencionales: Escuela de Copenhague

La Escuela de Copenhague al igual que el realismo estructural y el constructivismo, ve al Estado como el actor principal del sistema internacional. Para autores como Barry Buzan, mientras el mundo esté dividido por fronteras que establecen los límites de un país, el Estado seguirá siendo la forma más alta del orden político y por ende el objeto de referencia predominante para los estudios de seguridad (Dunne, Kurki y Smith 2013). Sin embargo, lo que la diferencia de otras teorías, en términos de Seguridad y Defensa, es la crítica que hacen al subdesarrollo teórico de estos conceptos y su fuerte vinculación con lo político-militar. Para esta corriente de pensamiento dichos términos deben trascender el campo al cual han sido circunscritos históricamente. Los fenómenos de seguridad contemporáneos como el ciberespacio vinculan a la sociedad, el Estado y el sistema internacional, de modo que requieren un análisis holístico en el cual se tome en cuenta otras dimensiones a más de la militar (Buzan 1983). Ello supone una adaptación en el concepto de Defensa y su doctrina, la redefinición de su objeto referente y la consideración de distintas fuentes de amenazas.

El espacio cibernético cuenta con la particularidad de no poseer características físicas, lo cual supone una transformación en cuanto a la interacción de los actores internacionales en esta dimensión. Ello implica un cambio en la forma en la que las sociedades pudieran entrar en guerra y en el accionar de Fuerzas Armadas (Eissa et al. 2014). Motivo por el cual es pertinente replantear los principios dogmáticos de la Defensa de modo que esta no sea concebida solamente como la protección a la integridad territorial y a su vez contemple tanto riesgos militares como no militares que se pueden presentar en este espacio anárquico (Buzan y Hansen 2009). A fin de poder comprender las diferencias que existen en este proceso de ampliación se debe considerar la concepción de Defensa que maneja Chile y Ecuador.

Desde la perspectiva chilena, la protección territorial y de sus ciudadanos sigue siendo el interés prioritario para la Defensa; pero manifiesta que esta debe estar en constante actualización de manera que pueda acoplarse a nuevas realidades nacionales y globales. Por lo que ha dejado de ser una competencia netamente militar y ajena a otras instituciones estatales (Ministerio de Defensa Nacional de Chile 2017). El planteamiento ecuatoriano maneja una terminología más tradicional a pesar de exponer que la Defensa debe ser flexible. Esta debe ajustarse a los cambios geopolíticos nacionales e internacionales con el objetivo de asegurar la soberanía del Estado, la paz y la seguridad de su población (Ministerio de Defensa Nacional del Ecuador).

Frente a un fenómeno como el ciberespacio, los Estados no pueden centrar su Defensa en proteger al Estado como única unidad política, ni tomar como objeto de referencia únicamente a las infraestructuras críticas. En los años 90 se comenzó a hablar de manera técnica sobre las ciberamenazas, es decir a nivel de sistemas, pero posteriormente esto cambió debido a que los efectos de dichas operaciones podían tener consecuencias sociales devastadoras (Hansen y Nissenbaum 2009). Los individuos pueden verse afectados a través del Estado como el resultado de la constitución de amenazas cibernéticas globales (Buzan 1983). Si se atacan a los sistemas fundamentales de un país y se incurre en el mal funcionamiento de los servicios públicos esto afecta directamente a los ciudadanos. Si se hace una extracción de fondos, el costo de esto por lo general recae en la población. Por ello este tipo de eventos no son considerados como crímenes que competen exclusivamente a la seguridad pública, sino ataques a la red que afectan a la sociedad y por lo tanto comprometen la integridad estatal (Hansen y Nissenbaum 2009). De allí que la seguridad de los ciudadanos deba ser tomada en cuenta dentro de las políticas públicas de Ciberdefensa.

Esta relación que existe entre el sistema internacional, el Estado y la sociedad no solo se manifiesta desde lo macro hacia lo micro; las personas pueden hacer uso de sus capacidades cibernéticas para constituirse como una amenaza para el país y dependiendo de su número y alcance, pueden poner en riesgo la existencia del mismo. Por lo tanto, no es posible centrarse en uno solo de los niveles para comprender las problemáticas que comprometen al ciberespacio. Las conexiones ascendentes y descendentes entre las categorías interactúan para sostenerse entre sí. Así como la Defensa no puede ser alcanzada únicamente por los individuos, esta tampoco puede reunir toda la responsabilidad y el poder en los niveles superiores. Cuando esto ocurre, se generan amenazas para las unidades más pequeñas a las cuales se supone se debía proteger (Buzan 1983). Es por esta razón que, en el mundo contemporáneo, debido a que existen otro tipo de desafíos, cuando se habla de doctrina de Seguridad y por ende de Defensa, ya no se puede hacer referencia únicamente a las afectaciones que puede tener el Estado visto desde una perspectiva racionalista. Se debe contemplar los riesgos que pueden forjar estas amenazas no convencionales sobre sociedades y Estados (Battaleme 2013).

Las Fuerzas Armadas chilenas tienen como misión, a más de la protección de la integridad del Estado, la protección de los ciudadanos en el ciberespacio y en virtud de ello deben trabajar para proporcionar un entorno cibernético seguro. A su vez, persigue el desarrollo de una cultura de Seguridad a partir de la sensibilización de sus habitantes (Barrios 2018). Chile establece que su política de Ciberdefensa debe contribuir a la consecución de los tres pilares sobre los cuales se edifica su política de Ciberseguridad. El primer pilar se enfoca en la formación de una infraestructura que le permita resistir y recuperarse de posibles ataques. El segundo pilar se basa en la protección de los derechos de las personas. En el tercer pilar se plantea el desarrollo de una cultura de seguridad cibernética basada en la educación, la responsabilidad en cuanto al manejo de tecnologías de la información y las buenas prácticas (Barrios 2018).

El Ecuador, en el plan de seguridad integral, se proyecta hacia el desarrollo de acciones que permitan defender a las redes, las infraestructuras críticas y la información digital. Esto no se puede realizar únicamente desde las Fuerzas Armadas, se precisa el fortalecimiento de mecanismos interinstitucionales (Gobierno Nacional de la República del Ecuador 2014-2017). Como parte del Libro Blanco de Defensa del Ecuador, se contempla la capacitación del

personal militar en el exterior, tanto en instituciones militares como civiles, y se visualiza como una problemática el hecho de que la sociedad civil no se interese en los temas de Defensa (Ministerio de Defensa Nacional del Ecuador 2018) y que las universidades tanto privadas como públicas no oferten este tipo de cursos. Si bien este país contempla tanto la protección del Estado como la de su pueblo, y persigue el establecimiento de una cultura de Defensa, al no contar con una política de Ciberdefensa (Ministerio de Defensa Nacional del Ecuador 2018), no habla de la sensibilización específica de los ciudadanos en cuanto a las amenazas cibernéticas. La cultura de Defensa que manifiesta el Gobierno ecuatoriano es de carácter más general y aún no ha sido llevada al campo específico cibernético. Lo cual da cuenta de la diferenciación que puede existir entre los países para establecer las conexiones entre el Estado, su sociedad y el sistema internacional.

Para poder alcanzar este objetivo, el concepto de Defensa debe contemplar aspectos que vayan más allá de lo político-militar (Buzan, Waever y de Wilde 1998) y para ello es importante tomar en cuenta que la sociedad civil tiene algo que decir al respecto.
En este sentido, Chile y el Ecuador consideran que las Fuerzas Armadas es la institución llamada a actuar en caso de un ataque externo, pero que el conocimiento que comprende la Defensa deja de ser exclusivo de su personal y se abre hacia el ámbito civil. La exclusividad militar a la hora de generar estrategias también se difumina y se visualiza como una alternativa al trabajo interinstitucional y al análisis multinivel de los desafíos. En el caso chileno se puede visibilizar la importancia que adquiere la academia y sus investigaciones, en el ámbito de la Defensa cibernética, para tener una nueva óptica y cambiar los paradigmas tradicionales (Barrios 2018). En la política pública ecuatoriana aún no se ha hecho una especificación acerca de los aportes que puede tener la esfera académica en temas específicos de Ciberdefensa.

Todo lo antes mencionado supone una ampliación de la agenda de Defensa para lo cual, es importante ver como la protección de la integridad estatal puede ampliar su espectro si se la moviliza a otras dimensiones. Aquí entra otro de los conceptos característicos de la Escuela de Copenhague, que es la segurización. Ole Waever la define de la siguiente manera:

> Seguridad es el movimiento que lleva a la política más allá de las reglas establecidas del juego y enmarca el tema como un tipo especial de política o como política en sí. La segurización

> puede verse como una versión más extrema de la politización (Buzan, Waever y de Wilde 1998, 23).

Este proceso advierte que cualquier amenaza que atente contra la supervivencia del Estado será agregada a la agenda de Defensa y formará parte de la política pública (Buzan, Waever y de Wilde 1998). Ello pone a tales amenazas por encima de cualquier otra, por lo que se las debe tratar oportunamente (Dunne, Kurki y Smith 2013). Una vez realizado este proceso, el Estado comienza a destinar recursos al tema que ha sido segurizado. El peso de la amenaza se verá reflejado en el grado de segurización que conlleve o la cantidad de recursos que se le asigne. No obstante, se debe tomar en cuenta que maximizar un proceso como este debe ser llevado a cabo con cautela, ya que puede llegar al punto en que los distintos ámbitos que se incorporan a la agenda se superpongan y ya no se pueda distinguir entre los alcances de cada uno. Así mismo se puede difuminar el límite entre el control y la irrupción. Debido a que en el ciberespacio se maneja información de toda índole y que es importante para todos los sectores fundamentales del Estado, no extralimitarse en la segurización es un reto. Al momento de considerar que es lo que debería estar dentro de su agenda, todo podría caber en ella (Kasaab 2014).

La adaptación doctrinaria de Defensa en torno al ciberespacio es la respuesta a la segurización de todas las amenazas a la supervivencia que se le presenta a los Estados en este entorno. Chile y Ecuador han puesto en evidencia que están llevando a cabo este proceso mediante las acciones que han tomado. Dentro de sus agendas de seguridad, ya se ve al ciberespacio como un ambiente a ser resguardado. Chile exterioriza dentro de su política de Ciberdefensa, que los riesgos y amenazas que representa el ciberespacio requieren de la generación de nuevas capacidades las cuales permitan proteger la disponibilidad, la integridad y la confidencialidad de la información, con el fin de precautelar los intereses de las personas que se encuentren en el país, así como también de los ciudadanos que se encuentren en el exterior (Ministerio de Defensa Nacional de Chile 2017).

Ecuador, a través de su Libro Blanco, plantea que la mundialización de las tecnologías de la información y la comunicación supone el desarrollo de políticas y estrategias en torno a la Ciberdefensa, con el fin de potenciar las capacidades de protección de las Fuerzas Armadas, en nuevos escenarios. A su vez destaca que su sector de Defensa impulsa la acción interinstitucional en el marco de la seguridad cibernética y que posee una capacidad

considerable para defender las infraestructuras críticas digitales militares (Ministerio de Defensa Nacional del Ecuador 2018).

Para que un espacio sea segurizado existen elementos segurizadores los cuales pueden ser factores internos y externos que justifiquen la inclusión de una amenaza en la agenda de Defensa. Los factores internos serían el objeto referente que en este caso es el ciberespacio, la audiencia que es la población chilena y ecuatoriana, y el actor segurizador que son ambos Gobiernos. Como factores externos se ve el contexto que incluye a todos los conflictos cibernéticos y la diversidad de ciberagresores, las relaciones de poder que se establecen en el sistema internacional, las prácticas agresivas que mantienen algunos actores y los múltiples instrumentos cibernéticos que se utilizan para configurar un ataque (Santander 2019).

Para que se justifique todo lo que implica una adaptación doctrinaria de Defensa en torno a ciberespacio a través de elementos segurizadores, es necesario un hilo conductor que es el discurso. Ello se debe a que la audiencia no existe por sí misma, sino que esta articulada dentro de la retórica, misma que tiene la capacidad de constituir a los objetos de referencia de la Defensa y coloca a otros sectores, a más del militar, en la problemática. La capacidad discursiva de los agentes segurizadores moviliza los incidentes cibernéticos particulares que han tenido ciertos individuos hacia el plano colectivo, de modo que en este lenguaje los individuos no aparecen como identidades aisladas sino como un conjunto. Esto con la finalidad de volver a los escenarios de segurización más plausibles, de tal manera que la sensación de miedo ante una amenaza alcance a cada sujeto receptor. También les permite sostener el rol privilegiado para poder hablar de algo que es desconocido para los demás (Hansen y Nissenbaum 2009). En otros términos, las amenazas tienen una naturaleza retórica y discursiva. Puede que el desarrollo de la amenaza se deba a un proceso específico o subjetivo, pero el discurso lo objetivisa ya que persigue convencer a las masas de tal manera que todos lleguen a tener una concepción común al respecto de algo en concreto (Battaleme 2013).

El Estado chileno, con Michelle Bachelet en el gobierno, mantuvo el discurso de que Chile, al igual que otros países de América Latina, ha incorporado rápidamente nuevas tecnologías a su sistema público. La ola de innovación tecnológica que se ha generado a nivel global también ha constituido vulnerabilidades; en numerosas ocasiones se ha visualizado que los sistemas digitales no son infalibles. Empresas y Estados han sufrido ataques, con los cuales se ha visto

comprometida su integridad. Motivo por el cual, era preponderante para este país sudamericano, la adopción de una política de Ciberdefensa (Ministerio del Interior y Seguridad Pública 2018). Discurso que exhorta la segurización de las amenazas cibernéticas ya que las establece como una temática que debe ser gestionada por el Ministerio de Defensa y las Fuerzas Armadas, apoyados por otros sectores.

El Gobierno chileno también ha expuesto en su agenda de Defensa la necesidad de proteger los sistemas informáticos, no solo del Estado sino de todos los sectores del país, pero haciendo énfasis en aquellos que representan a las infraestructuras críticas. Para ello se deben adoptar soluciones institucionales y tecnológicas que tomen en cuenta el alto nivel de interdependencia que se manifiesta entre las diferentes instituciones estatales y privadas. Se debe crear iniciativas que implementen adecuadamente las capacidades de los diferentes organismos nacionales. Con el fin de alcanzar esta meta, se asignará recursos para lograr la concientización y así lograr el desarrollo de acciones coordinadas (Ministerio de Defensa Nacional de Chile 2017).

Este país considera que la Ciberdefensa no solo debe ser responsabilidad de las Fuerzas Armadas, sino que se debe trabajar conjuntamente con las empresas privadas que representan una gran parte de la economía chilena, puesto que su afectación supondría la desestabilización del país. Además, estima que la ampliación de la agenda no solo debe darse a nivel nacional o a discreción de cada Estado, lo más adecuado es que la complejidad del ciberespacio también sea tomada en cuenta por los organismos internacionales, de tal manera que se pueda generar normativas internacionales que regulen el accionar de los agentes en al plano global (Ministerio de Defensa Nacional de Chile 2017). Esto supone una segurización que afectaría a la agenda de Seguridad Internacional.

El Gobierno ecuatoriano, para justificar la segurización cibernética, señala que en el plano global se han generado cambios importantes en las condiciones en las que se debe desarrollar la Seguridad y Defensa de los Estados. Esto se debe a la interacción de los bloques hegemónicos en el Sistema Internacional que se disputan el dominio de entornos como el ciberespacio y el control de sus recursos. Los conflictos en la actualidad han dejado de ser convencionales ya que trascienden las fronteras, vulnerando la supervivencia del Estado. Este contexto requiere de acciones conjuntas entre los países para poder hacerle frente a las

ciberamenazas. De modo que se hace necesario tomar acciones que potencien las capacidades ya existentes (Ministerio de Defensa Nacional del Ecuador 2018).

A su vez, también ha manifestado que la Defensa Nacional permite el control sobre las afectaciones que puedan llegar a tener diversos riesgos y amenazas, en la supervivencia del país, por lo cual la Ciberdefensa es fundamental para la consecución de una seguridad integral. También ha expuesto que las Fuerzas Armadas cuenta con las capacidades idóneas para poder hacerle frente a las amenazas que se le presenten en el marco de la seguridad. Cuenta con un talento humano capacitado sobre la base de una doctrina actualizada (Ministerio de Defensa Nacional del Ecuador 2018).

A través del discurso de ambos países se puede visibilizar diferencias en torno al proceso de segurización del ciberespacio. Esto responde al hecho de que la posición de las autoridades políticas frente a las ciberamenazas, misma que es susceptible al cambio histórico, puede diferir. A partir de los posicionamientos de los Gobiernos, y sus percepciones en relación al ciberespacio, se legitima una mayor o menor segurización de los desafíos cibernéticos (Hansen y Nissenbaum 2009).

4. Conclusiones

El realismo estructural, contribuye a la comprensión del problema que ataña a la presente tesis en cuanto a cómo la estructura anárquica puede incidir en el comportamiento de las unidades. Muestra el porqué de las similitudes que mantiene Chile y Ecuador en sus principios dogmáticos de Defensa. Esto se debe a que, de acuerdo al neorrealismo, la necesidad básica de todo Estado es procurar su supervivencia y en función de ella se desarrollan sus estrategias defensivas. En un entorno anárquico como el ciberespacio, el Estado chileno y el Estado ecuatoriano han desarrollado herramientas propias para poder maximizar su poder y resguardar su integridad. De esta manera pueden desarrollar sus capacidades y obtener atributos superiores a los de los demás países, con la particularidad de que este proceso, de conformidad con el realismo estructural, no depende de las unidades, sino que se encuentra determinado por la estructura.

Es en este último punto donde se comienza a visibilizar las diferencias que existen dentro de las estrategias que han construido las Repúblicas en cuestión. En la dimensión cibernética se puede observar países que poseen más o menos capacidades para poder hacerle frente a las

amenazas que se les presentan. Este es uno de los factores que diferencia los procesos defensivos de los Estados. El poder que ha adquirido Chile dentro del ciberespacio se diferencia del poder que tiene el Ecuador ya que ha sabido adoptar varias estrategias específicas en el ámbito de la Ciberdefensa. No obstante, el poder en el espacio cibernético no es algo que se encuentre estrictamente determinado por la estructura. En este ambiente se ha podido observar actores que cuentan con capacidades muy inferiores a las de un Estado pero que pueden configurar amenazas que pongan en riesgo su soberanía.

De este fenómeno puede dar cuenta el constructivismo, enfoque teórico en el cual la agencialidad de los países adquiere un papel importante. El Estado deja de ser un actor para convertirse en una unidad que puede afectar a la estructura, pero que a su vez también se ve influenciado por la misma. Esta dinámica constitutiva se manifiesta de diferente manera en cada país, la capacidad que tenga un país para afectar la estructura y la influencia que tenga la estructura con el agente se diferencia. Razón por la cual la situación de conflicto deja de ser el único escenario que restringe el comportamiento del Estado. Es posible la existencia de una diversidad de estructuras, así como diversas pueden ser las identidades de los Estados. Empero, en un escenario donde no existe un Gobierno que rija el comportamiento de los países, Estados como Chile y Ecuador seguirán buscando maximizar su poder el cual no se encuentra establecido irremediablemente por la estructura, sino que también depende de las experiencias y los significados intersubjetivos que manejen estas unidades.

La naturaleza diversa y compleja que tiene el ciberespacio representa algunos obstáculos para las teorías antes mencionadas que no les permite ser las más aptas para tratar el problema en cuestión. Para comprender este tipo de desafíos que se les presentas a las concepciones doctrinarias de Chile y Ecuador en torno al ciberespacio, se considera que la aproximación teórica más apropiada es la Escuela de Copenhague. Este enfoque se posiciona entre las teorías tradicionales estatocéntricas y las teorías críticas. Acepta que la toma de decisiones en torno a la Defensa está fuertemente influenciada tanto por las dinámicas que se dan a nivel individual como por las estructuras globales (Buzan y Hansen 2009). Los diferentes niveles de análisis que abarca la convierten en una teoría flexible que puede ser adaptada a otros escenarios. Toma en cuenta el discurso como un elemento fundamental de la segurización que a su vez se diferencia de país en país y de Gobierno en Gobierno.

Capítulo 2

La estrategia cibernética de Chile

El objetivo del actual apartado es presentar la estrategia de Ciberdefensa de Chile y cómo en base a ella se evidencia el proceso de adaptación doctrinario que ha tenido lugar en este país. Para lo cual se detallará el escenario cibernético chileno a través de estudios realizados por organismos internacionales y compañías especializadas. En ellos se reflejan los índices de ciberataques que ha tenido esta República en diferentes años y su posicionamiento a nivel mundial. A su vez, se hará mención de los principales ataques que se han ejecutado en contra de instituciones chilenas y sistemas públicos a manera de evidencia sobre lo que se menciona en los documentos previamente citados.

Habiendo contextualizado la situación de Chile, se detallará la política de Ciberseguridad dentro de la cual ya se contempla la creación de un instrumento político de Ciberdefensa. Igualmente se determina la actualización del Libro de la Defensa donde se incluye al ciberespacio como campo de acción de las Fuerzas Armadas. Si bien en las políticas de Seguridad cibernética no se habla ampliamente del papel que tendrá la Defensa en este ámbito, sí se bosqueja el rol que tendrá el Ministerio de Defensa en el plano digital, el cual a más de suponer funciones propias también conlleva un trabajo conjunto con otras instituciones públicas. El Gobierno chileno, a través de esta iniciativa posiciona al trabajo interinstitucional como la vía para poder alcanzar una estructura fuerte y resiliente. No obstante, la Defensa requiere de principios específicos que determinen sus alcances.

En tal virtud, se detallará la política de Ciberdefensa chilena, con la finalidad de comprobar si existe un cambio en los fundamentos bajo los cuales se va a manejar la Defensa dentro del ciberespacio. Esta herramienta política se encuentra constituida por tres pilares principales, el primero es el empleo de medios en el que se expone en qué casos el Estado hará uso de sus capacidades cibernéticas. El segundo se basa en la cooperación internacional, es decir que contempla las estrategias que se llevarán a cabo por parte del Estado para posicionarse a nivel internacional y para aumentar sus competencias. El tercer pilar, que va de la mano con lo anterior, se basa en el interés por desarrollar capacidades mediante diferentes mecanismos.

A raíz de estos instrumentos estatales, se comienzan a generar iniciativas concretas y aumenta la oferta académica en cuanto a la especialización en Ciberdefensa. Otro indicador relevante

al momento de analizar un proceso de transformación dogmático, pues supone capacitación, investigación e incremento del conocimiento en esta área. Igualmente se puede dilucidar, aunque de a poco, el interés de personas civiles en temáticas de Defensa y en fenómenos complejos que requieren de una visión holística.

En un cuarto momento se observará los tratados internacionales que ha firmado el Gobierno chileno en materia de Ciberdefensa, mismos que se han convertido en un factor estratégico en cuanto al desarrollo de capacidades. Estos suponen intercambios de información, tecnológicos y de experiencias. Posibilitan el intercambio académico para que el personal especializado se pueda instruir en el exterior. En ocasiones los acuerdos conllevan al accionar conjunto entre los países signatarios si se llevara a cabo un ataque contra uno de ellos.

Finalmente se analizarán las fortalezas y debilidades que presenta la estrategia chilena. Se estudiará de qué manera las políticas y las iniciativas concretas que, ha establecido este Gobierno, han sido beneficiosas y consecuentes con los intereses nacionales. Igualmente se examinará cuáles son los vacíos que dan paso a cierta confusión, que pueden reducir la efectividad de las operaciones que se pongan en marcha para proteger los sistemas estratégicos del Estado y que entorpecen el ajuste dogmático de la Defensa en el país.

1. Contextualización del escenario cibernético en Chile

Chile ha tenido una masiva aceptación de tecnologías de la información para gestionar los distintos servicios que ofrece el Estado a sus ciudadanos. Algunos ministerios chilenos permiten que sus usuarios puedan realizar distintos tramites de forma virtual de modo que se reduzcan los costos de transacción y el tiempo de los mismos. Aquellas instituciones públicas que no han implementado este tipo de innovaciones, se ven en la necesidad de hacerlo ya que de lo contrario su imagen se ve deteriorada. No obstante, en territorio chileno, no todas las infraestructuras críticas se encuentran administradas por el Estado, existen algunas redes de la información que son de vital importancia para el país y que son manejadas por el sector privado (Jarpa 2016).

De conformidad con la Encuesta del Gobierno Electrónico de Naciones Unidas del año 2014, el Estado chileno es el que presenta mayor evolución digital en la región y mayores avances en términos de gobierno electrónico. De modo que, en su condición de sociedad abierta e interconectada, tiene un mayor riesgo a ser atacada cibernéticamente. Países como Chile, que

se encuentran en vías de desarrollo se constituyen como un blanco de agresiones digitales y el impacto que estas podrían tener, es importante. Esto supone una serie de desafíos para el país del Cono Sur, ya que un sostenido crecimiento económico acompañado de la incorporación de tecnologías de la información y el creciente uso de internet, forman un ambiente propicio para que proliferen las ciberamenazas (Amigo 2015).

En este sentido, los sistemas con mayor susceptibilidad a ser afectados por una irrupción o denegación de servicios en Chile son:

- El sistema de emergencias chileno que comprende los diferentes números telefónicos a los cuales se puede comunicar la ciudadanía en caso de requerir auxilio inmediato.
- El sistema de transporte aéreo y terrestre que controla de manera automática el tráfico, la emisión de boletos y el número de pasajeros.
- El sistema de salud el cual supone, entre otros aspectos, datos sensibles como la base de datos de pacientes críticos, requerimientos de donaciones, medicamentos y presupuestos.
- El sistema de las Isapres asociación gremial de instituciones de salud previsional que tiene una labor importante en función de las atenciones médicas que reciben los usuarios.
- El sistema de las AFP y la información sensible con respecto a los fondos previsionales de pensionado.
- El sistema bancario y sus bases de datos en relación a los créditos, cobranzas y movimientos de los clientes.
- El sistema del Banco Central de Chile y otras instituciones financieras (Jarpa 2016, 99).

Tal afirmación se ve respaldada en los datos que arrojó Kaspersky acerca de los países más afectados por ataques cibernéticos durante el año 2018. En el informe Chile aparece en el top 10 de los países más atacados a nivel mundial con un 20,9% de usuarios afectados (Kaspersky 2019). La mayor cantidad de agresiones contra los intereses nacionales en este país han sido destinadas al robo de información confidencial, al espionaje de correos electrónicos militares y hacktivismo en apoyo a los movimientos civiles (Amigo 2015). También se han llevado a cabo secuestros de los servidores digitales de distintos Ministerios chilenos para posteriormente pedir recompensa por su recuperación. Esto ocurrió con un servidor informático del Ministerio de Agricultura cuando fue atacado a través del secuestro de datos. Los hackers pidieron un pago a cambio de liberar los servidores y permitir el acceso a su información (Rodríguez 2019).

En relación a la usurpación de datos, en uno de los ataques generados contra organismos públicos, se extrajo la información privada de 6000 personas para posteriormente publicarla. Las instituciones afectadas fueron el Ministerio de Educación, el Servicio Electoral de Chile y la Dirección de Movilización Nacional. Las entidades de Defensa Nacional también han sido atacadas; en el año 2014 se dio a conocer el accionar de unos hackers peruanos que se infiltraron en los sistemas informáticos de la Fuerza Aérea chilena y filtraron una gran cantidad de correos institucionales. Entre los datos que fueron hurtados y posteriormente revelados se encontraba documentación acerca de compra de armamento, el desarrollo del sistema de armas y la adquisición de radares. Con respecto al hacktivismo, se ha articulado en este territorio un grupo denominado "Anonymous Chile" los cuales han efectuado ataques contra sitios web pertenecientes a instituciones públicas y privadas, causando la denegación de acceso a distintos servicios y la publicación de contenido en contra de algunas decisiones gubernamentales (Amigo 2015).

En el 2018, de acuerdo a la empresa Novared, las agresiones cibernéticas en Chile aumentaron en un 74% con respecto al 2017 (Estrategia 2019). En este año, se dio uno de los ataques más emblemáticos perpetrado por actores internacionales al Banco de Chile. En esta ocasión el hackeo al sistema de esta implicó el robo del equivalente a 10 millones de dólares mediante tres transacciones. Cada transferencia llegó a una cuenta diferente en Hong Kong. Este hecho alarmó al Gobierno quien pidió se tome las medidas pertinentes por parte de las instituciones financieras para que este tipo de sucesos no vuelvan a ocurrir. De allí nació el compromiso de trabajar interinstitucionalmente para alcanzar una seguridad óptima, tomando en cuenta las brechas que pueden existir entre el sistema seguritario nacional en materia cibernética y los sistemas de seguridad que han forjado aquellos países que se han establecido como referentes a nivel internacional (Fundación Jaime Guzmán 2018)

En el mismo año, el Banco Consorcio fue víctima de un hackeo en el cual perdió 2 millones de dólares. Los piratas cibernéticos violaron los sistemas de seguridad informática de la institución mediante la utilización de una falsa actualización de Word, misma que fue ejecutada por uno de los empleados al recibir una notificación en su bandeja de correo. Por medio de un virus lograron acceder a la información de cuentas bancarias desde las cuales se extrajo dinero (Flores 2018).

El mes de julio del 2018, la Superintendencia de Bancos registró un ataque masivo a distintas entidades financieras del país y también extranjeras. La información de alrededor de 14.000 tarjetas de crédito pertenecientes a clientes de distintos emisores fue filtrada. Las instituciones afectadas tuvieron que desactivar las tarjetas de sus clientes para poder controlar la problemática que se les había presentado. La Superintendecia les dio pautas a los bancos nacionales para minimizar la afectación del ataque y mantener la seguridad de los beneficiarios implicados en el incidente (El Dínamo 2018).

A partir de los ejemplos citados se puede dar cuenta el carácter global de las ciberamenazas y de los alcances que pueden llegar a tener. En base a dichos suceso, el Estado chileno ha contemplado el hecho de que los ciberagresores podrían ser tanto nacionales como internacionales. Los riesgos que más se han destacado para este país han sido a nivel interno como por ejemplo fugas involuntarias de información confidencial debido a una mala utilización de las herramientas digitales por parte de los usuarios, interrupción accidental del funcionamiento de los sistemas informáticos, incidentes inintencionados que han comprometido la integridad, trazabilidad y disponibilidad de datos sensibles. Los desastres naturales también han tenido efectos colaterales para la Ciberseguridad del país, ya que se han visto afectadas instalaciones en las cuales se encontraban los equipos donde se almacenaba información esencial (Gobierno de Chile 2017).

Las actividades de espionaje por parte de actores estatales es otro de los desafíos que se le presenta Chile en el ciberespacio, ya que la sustracción de datos mediante esta práctica suele ser utilizada con fines políticos o estratégicos. En este tipo de amenaza, los agresores se valen de las vulnerabilidades que pueda tener el software utilizado a nivel público para penetrar en el objetivo deseado. El espionaje se ha llevado a cabo hacia el Gobierno, así como también hacia empresas privadas y de Defensa, lo cual compromete gravemente los intereses nacionales. A su vez se ven afectados los derechos fundamentales de los ciudadanos al verse violentada la confidencialidad de su información personal. En América Latina el acceso y robo de datos se ha incrementado y entre los países más atacados se encuentra Chile (Gobierno de Chile 2017).

La evidencia mostrada en el presente apartado permite visualizar que la red de conectividad del Estado chileno es receptora de un sin número de actividades irregulares y sospechosas. Igualmente, hace plausible que la interrupción del adecuado funcionamiento de servicios y las

alteraciones de los sitios web gubernamentales se han incrementado considerablemente. En el 2015 los administradores de esta red pudieron constatar que existieron intentos de acceso forzoso, escaneos de la plataforma, alteración de contraseñas, transferencia no autorizada de archivos, infiltración de virus digitales y acceso a información clasificada (Gobierno de Chile 2017).

Dichos incidentes cibernéticos, a primera vista se podrían considerar como situaciones que se vinculan mayormente con la Ciberseguridad, sin embargo, estos le competen a la Defensa puesto que en todos ellos se ven comprometidas infraestructuras críticas y por ende la soberanía del Estado. Para Chile, un ataque cibernético hacia un sector importante del Estado adquiere la misma connotación que un ataque armado. Por esta razón, es importante alcanzar capacidades que les permitan proteger toda aquella información estratégica del Estado, que se encuentra en formato digital, de tal manera que no pueda ser cooptada por un enemigo (Centro de Estudios e Investigaciones Militares Ejército de Chile 2018). Con este objetivo en mente, el Gobierno chileno ordenó la realización de una política de Ciberseguridad, y a través de la misma la creación de la política de Ciberdefensa.

2. Establecimiento de la política de Ciberseguridad y ejecución de la política de Ciberdefensa

La realidad que se le presenta a Chile en el ciberespacio lo ha conducido a iniciar una adaptación en su doctrina de Defensa con el objetivo de desarrollar capacidades dentro de este dominio que, si bien no es completamente nuevo, se ha podido evidenciar que la velocidad de sus avances hace que cualquier acción para controlarlo tenga carácter reactivo más que preventivo. Tomando en cuenta el desfase temporal que existe entre los avances tecnológicos y las estrategias de Defensa, desde el año 2014, el Estado comienza a tomar acciones concretas que marcan un proceso de transformación de cara a las particularidades del entorno digital. El Estado chileno ha considerado imprescindible contar con estrategias de gestión y minimización de riesgos que tengan en consideración a las ciberamenazas en contra de las infraestructuras críticas de la información y al contexto global actual en relación a la protección cibernética de los Estados.

Como parte de la estrategia de Ciberdefensa, en el 2014 se emitió una orden ministerial para que se inicie con el diseño de dos instrumentos que ayudarían a la consecución de los objetivos nacionales en este ámbito. El primer instrumento es la política de Ciberdefensa,

herramienta que se materializaría en el Libro de la Defensa del 2017. En el año 2015 se generó una orden mediante la cual se detalla el diseño que deberá tener dicha herramienta, y la necesidad de que cuente con un documento específico además de la mención general que se le hace en el libro referido. A través del segundo instrumento, se dictaminó que el Comando Conjunto de las Fuerzas Armadas debía iniciar la planificación del proyecto que ayudaría a suplir las necesidades de la institución en términos de infraestructura, equipamiento, personal y capacitación del mismo (Ministerio de Defensa de Chile 2020).

Consecuentemente con el objetivo de hacerle frente a los desafíos cibernéticos, en el 2015 se creó el Comité Interministerial de Ciberseguridad, órgano asesor de la Presidencia de la República para la estructuración de una estrategia de seguridad digital. Los miembros permanentes de este órgano pertenecen a los sectores que son considerados esenciales para el Estado los cuales son:

> Un representante de la Subsecretaría del Interior, un representante de la Subsecretaría de Defensa, un representante de la Subsecretaría de Relacione Exteriores, un representante de la Subsecretaría de Justicia, un representante de la Subsecretaría General de la Presidencia, un representante de la Subsecretaría de Telecomunicaciones, un representante de la Subsecretaría de Economía y Empresas de menos tamaño, un representante de la Subsecretaría de Hacienda, un representante de la Subsecretaría de Energía y un representante de la Subsecretaría de la Dirección Nacional de la Agencia Nacional de Inteligencia (Decreto 533, 2015, art. 3°).

En un primer momento el objetivo principal del Comité fue proponer una política nacional de Ciberseguridad, misma que contiene las medidas y los planes de acción específicos. Actualmente sus funciones se basan en el seguimiento de los avances que se han llevado a cabo en cuanto a la implementación y el cumplimiento de las políticas. También asume el asesoramiento para la coordinación de acciones, proyectos y programas en materia de seguridad cibernética, entre los actores públicos y privados. De igual manera, tiene la capacidad para analizar alternativas y proponer opciones para la estructura cibernética del Estado, y plantear al Primer Mandatario cambios en la normativa constitucional, legal o reglamentaria vigente, si las modificaciones son necesarias para el cumplimiento de los objetivos en materia de Ciberseguridad (Ministerio del Interior y Seguridad Pública y Ministerio de Defensa Nacional 2015). A fin de mantener un ciberespacio abierto, libre y seguro, dentro de esta iniciativa se contempla la actualización permanente de los

requerimientos que tenga cada mecanismo en función de las características que tiene el ciberespacio (Ministerio de Defensa de Chile 2020).

El Ministerio de Defensa se ve representado por el Subsecretario de Defensa quien se encuentra a cargo de la Secretaría Ejecutiva del Comité. Lo que le corresponde a esta institución pública es proponer y evaluar políticas que tengan que ver con la protección de la integridad del Estado en el ciberespacio, así como también hacer el análisis estratégico de aquellas amenazas o riesgos que pueden generar afectaciones para la integridad del país o para su seguridad exterior. Tiene como potestad, proponer al presidente políticas que velen por la seguridad de los sistemas informáticos utilizados por entidades estratégicas como por ejemplo el sistema de salud, energía o transporte. Para ello, la Subsecretaría de Defensa contaría con los medios técnicos y los equipos necesarios, entre los cuales se encuentran las unidades de respuesta de incidentes informáticos y los grupos multidisciplinarios, de tal manera que se realice un trabajo de carácter integral que tome en cuenta los requerimientos de diversos sectores (Ministerio del Interior y Seguridad Pública y Ministerio de Defensa Nacional 2015).

Desde el 2016, de conformidad con las órdenes ministeriales antes mencionadas, el Estado Mayor Conjunto inició el proceso de desarrollo del proyecto de Ciberdefensa. Alcanzó la etapa final de diseño para continuar con la fase de facticidad. Para este ciclo se elaboró un informe en el cual se llevó a cabo un diagnóstico sobre el estado en el que se encontraba el Sistema de Seguridad Cibernética en relación a la Defensa Nacional y las amenazas o riesgos que tiene que enfrentar el Estado en la red. En cuanto a la protección de documentación se obtuvo un avance importante ya que se realizó la implementación de un nuevo sistema criptográfico interinstitucional el cual sustituyó a un sistema obsoleto. Esta innovación cuenta con las características necesarias para poder gestionar información confidencial de forma segura en formato digital (Ministerio de Defensa Nacional y Gobierno de Chile 2017). Ello fue una de las primeras acciones que pautaron el fortalecimiento de la institucionalidad conjunta.

Hasta mayo del 2016 el Ministerio de Defensa indicó como parte de los progresos en términos de Ciberdefensa, que se había incrementado la participación del país en procesos internacionales tanto bilaterales como multilaterales. Disposición que tuvo como finalidad alcanzar un rol más activo en debates sobre los conflictos cibernéticos y ampliar sus

capacidades de cooperación en esta área. Asimismo, dio inicio al proceso de diseño de planes de protección cibernética que fueron de utilidad para poder estructurar políticas de Defensa en el ciberespacio. Posteriormente se entregó el primer borrador de la política de Ciberdefensa, la cual orienta el proceso de adaptación y el desarrollo de capacidades del Ministerio de Defensa y de las Fuerzas Armadas en cuanto a protección de información y redes digitales se refiere (Fonseca y Ansorena 2017).

En el 2017 se firma y se aprueba la política de Ciberseguridad, convirtiéndose en el primer instrumento estatal destinado a la constitución de una estrategia nacional en el espacio cibernético. Al interior de este documento se trata a la Ciberdefensa como un ámbito de competencia exclusiva del Ministerio de Defensa y de las Fuerzas Armadas. Se dispone que dicha institución tiene la responsabilidad de proteger la soberanía del Estado, sus atribuciones constitucionales y legales al interior del ciberespacio, a través del resguardo de las redes y de la información clasificada. A la Subsecretaría de Defensa se le adjudica el rol de Formulación de políticas cuya misión es realizar el análisis pertinente para proponer políticas e iniciativas que ayuden a desarrollar las capacidades del Estado y mantenerlas actualizadas. Por su parte, el Estado Mayor Conjunto y las Fuerzas Armadas adquieren un rol preventivo y reactivo. El primero es el organismo de trabajo y asesoría permanente del Ministro de Defensa con respecto a la preparación y el empleo conjunto de las instituciones militares, mientras que Fuerzas armadas cuentan con la misión de realizar planes institucionales y operativos, proteger sus propias infraestructuras de la información y colaborar con las tareas de Ciberseguridad que involucren la protección nacional y el sistema nacional de inteligencia (Gobierno de Chile 2017).

En el mismo año, se presentó el nuevo Libro de la Defensa de Chile, en el que se busca renovar los objetivos que persigue el Estado en esta área y se incluye al ciberespacio en su radio de acción. En este documento se establece la concepción de ciberespacio bajo la cual se generará una estrategia específica. Se considera que el ciberespacio es “el conjunto de infraestructuras físicas y lógicas y de las interacciones que ahí se producen” (Ministerio de Defensa Nacional de Chile 2017, 82). La masividad que caracteriza al espacio cibernético genera dependencia y vulnerabilidad la cual en el plano de la Defensa podría llegar a ser crítica y significar un alto riesgo para la seguridad exterior y la soberanía del Estado. De la misma manera, los conflictos internacionales que se desencadenan en el plano digital en conjunto con la dificultad para detectar el origen de los ataques y atribuir responsabilidad, le

genera obstáculos a la comunidad internacional (Ministerio de Defensa Nacional de Chile 2017).

En base a esta percepción, como parte del texto en cuestión, se establece la necesidad de generar una estrategia propia que permita garantizar el correcto funcionamiento de los servicios estratégicos para el país, incluido el sistema de Defensa. Para lo cual, se debe proteger las redes de interacciones que ocurren dentro del entorno cibernético y aquellas infraestructuras que las posibilitan. Esto significa que la agenda tradicional tiene una transformación ya que en ella se suman riesgos no convencionales tales como los ciberataques o cualquier tipo de comportamiento irregular que se manifieste en esta dimensión. Es así que, en esta nueva percepción de la Defensa se comprende que las estrategias que se aplican para proteger la integridad territorial del país son difíciles de aplicar en el ciberespacio. La identificación del área de influencia que pueda tener un país en este entorno, así como el origen de un ataque es complejo, lo cual no es así cuando se habla en términos físicos (Ministerio de Defensa de Chile 2017).

A pesar de que Chile es consciente de lo difícil que es para la comunidad internacional establecer normas internacionales que regulen el accionar de los Estados en el ciberespacio, y de que ha generado una estrategia propia de Ciberdefensa, considera que este es un ambiente creado artificialmente que debe ser regulado a nivel global de alguna forma. Por esta razón el Estado chileno, conjuntamente con otros países, promueve la creación de nuevas políticas internacionales, estándares de buena conducta y mecanismos de transparencia que incentiven la confianza entre los Estados y se eviten conflictos. Esto implica la adopción de políticas domésticas que promulguen principalmente el espíritu que persiguen dichos objetivos internacionales (Ministerio de Defensa de Chile 2017).

En el Libro de la Defensa de Chile, ya se especifican los parámetros bajo los cuales se estructuraría la Política de Ciberdefensa que se publicaría un año después. Con respecto a esta temática en particular se expone que la política de Ciberdefensa se encontrará subordinada a la política de Defensa por lo que mantienen los mismos objetivos y principios rectores. La constitución de este instrumento estatal se rige por la protección de la población, de la integridad del país y de los intereses nacionales, y el respeto al Derecho Internacional Público, la igualdad soberana de los Estados y la abstención del uso de la fuerza con la salvedad de que se lo haga en legítima defensa (Ministerio de Defensa de Chile 2017).

La política de Ciberdefensa, fue aprobada en el 2018 y contiene una serie de disposiciones mediante las cuales se pretende alcanzar un compendio de capacidades. Ello no solo supone la adquisición de equipos, sino que implica principalmente el desarrollo de una doctrina sobre el uso de competencias digitales, a través de la capacitación y el entrenamiento del personal que trabajará en esta área, el intercambio de información con centros de respuesta a incidentes informáticos nacionales e internacionales, tanto públicos como privados, y el desarrollo de software que permita proteger a las infraestructuras críticas y su información clasificada. Orienta a la institución militar hacia una industria de la Defensa Nacional que provea bienes y servicios en cuanto a tecnologías de la información. Promueve una industria que les permita alcanzar cierta independencia y soberanía digital (Ministerio de Defensa de Chile 2017).

En este instrumento estatal se establecen las medidas que deben adoptar tanto las instituciones del sector público, así como también las del sector privado, de manera que el país pueda llegar a tener un ciberespacio seguro, libre y resiliente. Se plantea como objetivo primordial la protección de las personas y sus derechos generando las condiciones adecuadas para que puedan desarrollar sus actividades de manera segura, pacífica y equitativa en el ciberespacio; asimismo establece los parámetros bajo los cuales pueden realizar dichas acciones. También se disponen otros objetivos los cuales se espera alcanzar progresivamente hasta el 2022. Para ello es necesario que las instituciones de Defensa realicen actividades de planificación a corto, mediano y largo plazo, de modo que se pueda hacerle frente a los desafíos que se le presentan en el presente inmediato al país y aquellas que se puedan presentar a futuro (Ministerio del Interior y Seguridad Pública 2018).

La política de Ciberdefensa se basa en tres pilares fundamentales que son: el primero es el empleo de los medios de Ciberdefensa, en el cual el Estado chileno manifiesta que un ataque cibernético puede causar el mismo efecto que un ataque armado. Por este motivo, el país actuará ante un ciberataque masivo que afecte a su soberanía, sus infraestructuras críticas, sus ciudadanos o sus intereses, de la misma manera que lo haría ante un ataque armado. Esto significa que el país se acogerá al artículo 51 de la Carta de Naciones Unidas y hará uso de los medios que considera convenientes, ya sea físicos o digitales, en legítima defensa. Igualmente, dicho Estado expone que protegerá sus infraestructuras críticas ejerciendo su soberanía sobre las redes y recursos digitales que en ellas sean utilizados. Las instituciones de la Defensa son las llamadas a materializar este objetivo mediante la identificación de los

ataques y la tipificación de los atacantes para así poder adjudicar de manera acertada la responsabilidad a otro Estado o actor no estatal. De esta manera se puede generar una respuesta adecuada (Ministerio del Interior y Seguridad Pública 2018).

El segundo es la cooperación internacional, conjuntamente con la promoción de la transparencia y la confianza entre los Estados. En esta sección se sostiene que debido a que el ciberespacio tiene características transfronterizas, la mejor opción para poder enfrentar sus desafíos es generando relaciones de cooperación en Ciberdefensa, ya sean bilaterales o multilaterales. Para ello es importante participar activamente en foros internacionales cuya finalidad sea generar un ambiente seguro en el ciberespacio, integrar los proyectos de elaboración e implementación de medidas de confianza, códigos de conducta y normativa internacional. Chile se compromete a cumplir con la implementación de todas estas herramientas ya que se muestra a favor de fomentar la paz y la seguridad internacional, principalmente a nivel regional (Ministerio del Interior y Seguridad Pública 2018).

El tercer pilar es el desarrollo de capacidades donde se expone que el Estado mantendrá y desarrollará capacidades para poder proteger la estructura informática institucional de Defensa, principalmente sus sistemas de armas, sistemas y redes de comunicaciones y sus sistemas y redes de mando y control. El objetivo de esto es poder contar con una estructura de Ciberdefensa robusta que les de la capacidad para poder mantener la integridad, confidencialidad y disponibilidad de los servicios. Igualmente se estipula que el Estado generará habilidades para defenderse y perseguirá sus intereses nacionales, para lo cual se debe adquirir equipamiento adecuado, la contratación de personal capacitado, y programas especializados de formación para el personal de Defensa (Ministerio del Interior y Seguridad Pública 2018).

En función de esto, el Ministerio de Defensa Nacional debe:

a. Identificar y definir el rol del recurso humano en la Ciberdefensa;
b. Implementar los modelos formativos que sean necesarios para cumplir con ese rol;
c. Definir y crear las especialidades, subespecialidades o especialidades secundarias en el área de la Ciberdefensa para oficiales y suboficiales, manteniendo una continuidad de trabajo en dicha área de desempeño, reestudiando los requisitos de ascenso y otras obligaciones o interferencias que pudieran afectar su continuidad como especialistas. Se

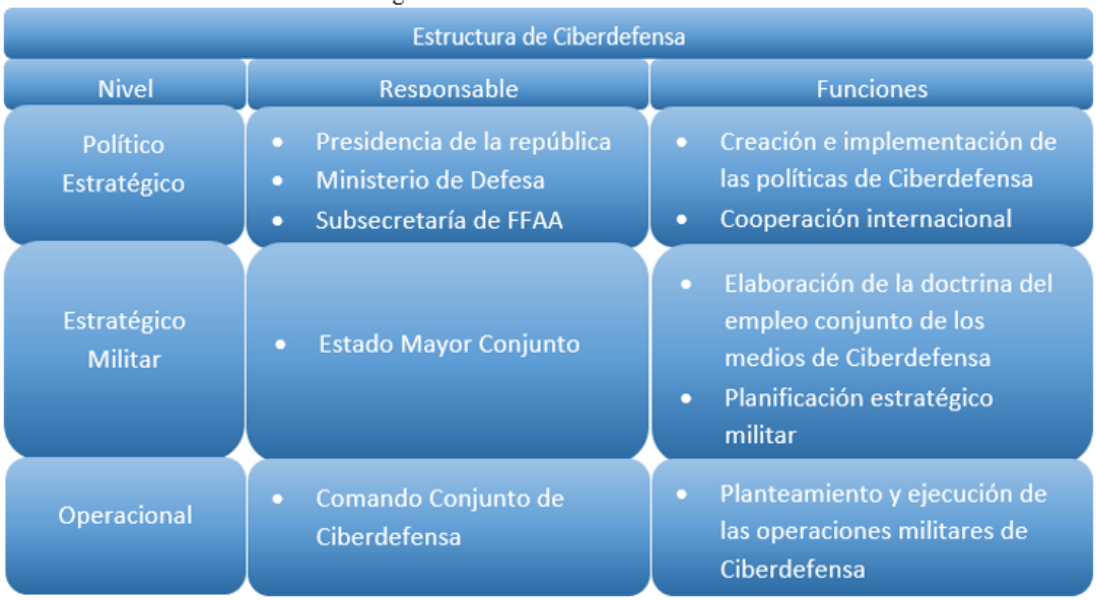
deberá considerar y promover la igual participación de mujeres y hombres en el área de la Ciberdefensa;

d. Identificar e implementar modelos de reclutamiento y reserva de personal calificado;
e. Incrementar la interacción con el sector privado y académico, para contar con sus capacidades en la materia; y
f. Promover la innovación y la investigación aplicada en materia de Ciberseguridad, desde una perspectiva conjunta (Ministerio del Interior y Seguridad Pública 2018, 5).

Una vez aprobada la política de Ciberdefensa se plantean las siguientes medidas como apremiantes para poder cumplir con los objetivos fundamentales que persigue este proyecto estatal:

a. Se creará un Comando Conjunto de Ciberdefensa, bajo el mando del jefe del Estado Mayor Conjunto, responsable del planeamiento y ejecución de las operaciones militares conjuntas de ciberdefensa del país; b. Se creará un Equipo de Respuestas a Incidentes Informáticos (CSIRT) de la Defensa Nacional que, junto con brindar seguridad a las redes y sistemas del Ministerio de Defensa Nacional, actuará como ente coordinador técnico con los CSIRT de las instituciones de la Defensa Nacional, el que será dirigido por el Estado Mayor Conjunto. En el mediano plazo se implementará un CSIRT sectorial que coordine los CSIRT institucionales;
b. Cada rama de las Fuerzas Armadas contará con un CSIRT, y se evaluará la necesidad de crear nuevos equipos en los organismos relacionados o dependientes del Ministerio de Defensa Nacional;
c. Se creará una Oficina de Ciberdefensa y Seguridad de la Información en el Gabinete del Ministro de Defensa Nacional, que tendrá por función esencial prestar asesoría en materia de Ciberseguridad y Ciberdefensa;
d. Se fortalecerán las capacidades de Ciberseguridad del Ministerio de la Defensa Nacional y sus instituciones dependientes o relacionadas; y
e. Se creará una capacidad de reserva nacional para la Ciberdefensa del país (Ministerio del Interior y Seguridad Pública 2018, 5).

Figura 2.1. Sistema de Ciberdefensa



Fuente: Elaboración en base a los datos recopilados en Ministerio del Interior y Seguridad Pública. 2018. "Ministerio de Defensa Nacional aprueba Política de Ciberdefensa." *Diario Oficial de la República de Chile*, 9 de marzo. https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Todas estas acciones tomadas por el Estado chileno permiten inferir el inicio de una transformación en su doctrina de Defensa dado que ya establecen principios y funciones específicas, tanto ministeriales como a nivel de Fuerzas Armadas dentro del ciberespacio. No obstante, Chile ha estructurado un documento donde se detalla la doctrina conjunta de Ciberdefensa. En este se establecen concepciones y procedimientos generales que utilizarán las instituciones de Defensa en relación al espacio cibernético (Ministerio de Defensa Nacional 2018).

Las Fuerzas Armadas de Chile, perciben a la dimensión cibernética como un ambiente artificial e intangible que surge a partir del desarrollo de tecnologías de red, las cuales se han vuelto necesarias para el Estado. Las acciones que se llevan a cabo en este entorno, si bien son digitales, tienen efectos tangibles en la vida de las personas, en la estabilidad del Estado y en el Sistema Internacional. En consecuencia, en el plano digital las operaciones militares tradicionales deben ser repensadas (Ministerio de Defensa Nacional 2018).

En este sentido se observa la complejidad que caracteriza a las amenazas que se desarrollan en esta dimensión. Este tipo de actividades irregulares pueden tener connotaciones criminales o de inteligencia. Lo segundo entendido como actividades de espionaje, sabotaje u estrategias psicológicas relacionadas con algún tipo de activismo político ilícito. En teoría se las podría

diferenciar, pero existen casos en los que las actividades delictuales se asocian con actividades de espionaje (Ministerio de Defensa Nacional 2018).

A pesar de ello se hace una diferenciación entre las competencias de la Ciberdefensa, el combate del cibercrimen que comprende actividades legales, policiales e internacionales y la protección de infraestructuras críticas donde se condensan todos los esfuerzos públicos y privados. De este modo se determina que las instituciones de Defensa se encargaran principalmente de proteger sus sistemas informáticos, enfrentar a cualquier ciberamenaza que atente contra los mismos y realizar operaciones que contribuyan con la consecución de objetivos militares. A su vez actuar en función de la Defensa de sistemas vitales del Estado y en legítima defensa dentro del ciberespacio (Ministerio de Defensa Nacional 2018).

En otras palabras, la Ciberdefensa tiene como objetivo proteger sus sistemas y las infraestructuras críticas de cualquier acción maliciosa que involucre contraposición de voluntades, institucionalidad y enfrentamientos con fines militares. Para lo cual, se han desarrollado operaciones defensivas y ofensivas. En el ámbito defensivo se contempla la gestión de riesgos, medidas preventivas y medidas reactivas. En relación a las acciones ofensivas, estas se basan en la inteligencia y serán desplegadas en caso de conflicto. Su intensidad dependerá del grado de peligro que represente la amenaza (Ministerio de Defensa Nacional 2018).

3. Desarrollo de conocimiento en materia de Ciberdefensa en Chile

A raíz de los mencionados marcos normativos surgió en Chile la oferta de cursos especializados en Ciberdefensa y se inició la capacitación del personal militar. Uno de los cursos más relevantes impartidos a los funcionarios públicos estuvo a cargo de la Secretaría General de la Presidencia. El mismo se centró en la explicación del marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en ingles), publicado en Estados Unidos en el año 2014 para el fortalecimiento de la Ciberseguridad de las redes federales y de las infraestructuras críticas (Amazon Web Services 2019), el cual se implementaría en el país del Cono Sur. La OTAN fue una de las pioneras en desarrollar manuales orientados hacia la Defensa Nacional para la protección óptima de las Infraestructuras críticas (Silva 2018).

Asimismo, se presentaron los objetivos principales del marco de trabajo de Ciberseguridad. Dicho manual del NIST fue constituido con el objetivo de identificar estándares óptimos y buenas prácticas de seguridad, de modo que se pueda establecer guías aplicables para todos los sectores públicos y privados que manejen infraestructuras críticas y de esta manera puedan reducir y gestionar las ciberamenazas. Del mismo modo busca instaurar un lenguaje común que sea funcional para la gestión de riesgos cibernéticos, con la finalidad de fomentar la comunicación entre los actores internos y externos a las instituciones. Busca proporcionar un enfoque neutral flexible y replicable en función de un desempeño efectivo que pueda adaptarse a las necesidades o requerimientos de una institución o empresa sin importar su naturaleza. Ello posibilita al personal responsable de los sistemas esenciales a identificar, gestionar e inventariar los riesgos informáticos que se presenten (Silva 2018).

En este sentido, también busca establecer criterios que permitan verificar la implementación optima de los parámetros de Ciberseguridad. Instaurar controles comunes para la protección de la privacidad de los ciudadanos, las libertades de los civiles y la propiedad intelectual en el momento en que se realice una operación de Seguridad y Defensa en el ciberespacio. Evidenciar áreas que necesitan ser trabajadas para poder mejorarlas en base a colaboraciones futuras con sectores específicos y organizaciones orientadas al desarrollo de esquemas de Defensa cibernética. Esto implica la investigación de iniciativas que ya se hayan desarrollado previamente y que sean prácticas para cubrir los requerimientos de las instituciones (Silva 2018).

A pesar de que es un documento discrecional, es decir que permite a los usuarios implementar o no las prácticas y directrices, en algunos casos las organizaciones gubernamentales pueden requerir el cumplimiento obligatorio de la guía dentro de sus deferencias contractuales (Silva 2018). Para la Defensa de Chile, la adopción de este marco de trabajo es fundamental y propicia, tomando en cuenta que, aunque puede ser utilizado en diversos sectores, su desarrollo en un principio fue pensado específicamente para las infraestructuras críticas de Estados Unidos. Si bien este instrumento fue creado para las necesidades estadounidenses, no significa que sea inmutable o inamovible, este puede ser adaptado a las condiciones de otros países sin importar su tamaño o susceptibilidad a las ciberamenazas (Amazon Web Services 2019). El principio de la integración de criterios y buenas prácticas a nivel internacional hacen que su implementación no se circunscriba a la potencia norteamericana. Inclusive podría ser

utilizado para poder alcanzar un nuevo nivel de cooperación en materia de Ciberdefensa entre países (Silva 2018).

Para poder aplicar las directrices del NIST en el área de Defensa, se han establecido cinco funciones principales: Identificar, proteger, detectar, responder y recuperar. La primera permite identificar cuáles son los sistemas, activos o datos de la institución que deben ser protegidos, así como también las capacidades con las que cuentan sus redes, los recursos que poseen para resguardar las infraestructuras críticas del Estado y las estrategias que han sido establecidas anteriormente (Amazon Web Services 2019). La gestión de activos se logra a través del mantenimiento de inventarios sobre los dispositivos físicos, los sistemas, las plataformas y las aplicaciones utilizadas por la organización, el mapeo de las comunicaciones y la priorización de los recursos de acuerdo a la importancia y el valor que tengan los datos que contienen las entidades de Defensa (Silva 2018).

De igual manera, como parte de esta función, se evidencia la importancia que tiene la institución y su información para el Estado, se instituyen los objetivos, la misión y las actividades en materia de Ciberdefensa y se determinan los roles que tendrá el personal encargado de la protección de los sistemas. En cuanto al Gobierno, se visibiliza si existe una política pública que contribuya a la asignación de funciones, la consecución de objetivos, la constitución de una estrategia. Como parte de la evaluación de riesgos, se analizan las amenazas y vulnerabilidades que se le presenta al Estado, tanto internas como externas. Una vez realizado esto se llega a la estrategia de gestión de riesgo en la cual las partes involucradas, se reúnen para establecer la estrategia (Silva 2018).

La segunda función, viabiliza el desarrollo y la implementación de medidas de protección y contraataque, de ser necesario, para poder contener un incidente cibernético potencialmente dañino para el Estado o minimizar su impacto. Como parte de este ejercicio se realiza el control de acceso a los bienes y servicios de la organización, mediante el requerimiento de identificaciones y credenciales para ingresar a páginas que contengan datos confidenciales. En este sentido, se debe controlar el acceso remoto que se puede tener a las máquinas institucionales. Es importante mantener los servidores resguardados ya que contienen toda la información importante. Ello incluye la adquisición de tecnología de protección y su mantenimiento. Si bien, estas acciones son cruciales, pierden efectividad si los recursos humanos no reciben una capacitación y concientización continua. Gran cantidad de ataques

cibernéticos han sido llevados a cabo debido a una falla humana, a la utilización de medios informáticos sin las precauciones necesarias (Amazon Web Services 2019).

La tercera función comprende la detección de anomalías en la red, eventos y el control de los procesos de identificación. Si una anomalía se detecta a tiempo se puede prever la potencial afectación que esta puede tener y así actuar oportunamente, teniendo a favor el tiempo e incurriendo en un menor gasto de recursos. El control continuo de las medidas adoptadas contribuye a la verificación de la efectividad de los mismos o a su adaptación de ser necesaria, en función de la rápida transformación que caracteriza al ciberespacio y que vuelven obsoletas a un sin número de herramientas informáticas. El aporte fundamental de este ejercicio es robustecer el conocimiento, en cuanto a protección cibernética, con el que cuenta el área de Defensa de Chile, el cual le permita actuar de manera efectiva ante los desafíos que se le presenten, inclusive si estos son relativamente nuevos (Sila 2018).

La cuarta función radica en la planificación de las respuestas que puede dar el país ante un ciberataque. Dicha planificación se realiza para poder mantener y garantizar respuestas eficientes que contrarresten un ataque. Las actividades de contraataque no son ejecutadas por una sola sección de la institución, sino que se requiere de la comunicación entre los diferentes departamentos para poder interceptar la amenaza y erradicarla. De igual manera, se genera dicha planificación para poder ayudar a las actividades de recuperación. La contribución de esta sección se fundamenta en la incorporación de lecciones aprendidas ante ataques previos, las cuales conceden un avance en la estrategia de ciberdefensa y en futuras operaciones (Silva 2018).

La quinta y última función es la de recuperación, en la cual se analizan los procesos y procedimientos para rescatar o restaurar aquellos datos que han sido usurpados o dañados por medio de un ciberataque. Esto incluye la reparación de los equipos que han sido afectados y hayan dejado de funcionar correctamente. Dicha actividad también es coordinada con otras instituciones, proveedores de sistemas informáticos y otros CSIRT (Silva 2018).
A demás de este taller, el cual ha sido importante para la consecución de los objetivos estatales, existen otros cursos y seminarios en los cuales ha participado el personal de Defensa chileno, dando cumplimiento al objetivo de capacitación para Oficiales, Suboficiales y Empleados Civiles, fundado por el Estado Mayor Conjunto:

a) Taller “I.S.R.” para GG.MM., A-2 y C-2 de Comandos Conjuntos – DIRINTA.
b) Curso “Gestión en Defensa en un contexto amplio de Seguridad” – ANEPE.
c) Curso “Ciencias Geoespaciales y Geomática – S.A.F. – Fuerza Aérea de Chile.
d) Taller práctico para reforzar técnicas de análisis – A.N.I.
e) Seminario Internacional de Ciberseguridad – SOFOFA.
f) Seminario de Ciberseguridad – CONGRESO.
g) Seminario Cyber IAI/ELTA – EMCO.
h) Taller CYBER SMEE – DIRINTA.
i) Jornada de Cyber – ROADSHOW.
j) Workshop Ciberoperaciones – Santiago.
k) Seminario de Seguridad de Instalaciones y Apoyo de Contrainteligencia – Tucson – EE.UU.
l) Taller de planeación de la Ciberseguridad, Ciberdefensa y jornada de trabajo en Operaciones militares en el ciberespacio – Madrid - España
m) Curso de “Analista Desarrollador de Aplicaciones de Software” – CORFO.
n) Diplomado en Alta Dirección (D.A.D.) – Academia de Guerra Naval.
o) Curso de Planificación Estratégica año 2018 – ANEPE – EMCO.
p) Curso Técnico Nivel Superior de Ciberdefensa – Academia Politécnica Militar. (Termino curso 28.DIC.2018)
q) Taller de Inteligencia y Contrainteligencia – CCN (Estado Mayor Conjunto de Chile 2019, 12).

La Academia de Guerra de Chile igualmente, ha generado eventos académicos en materia de Ciberdefensa. En mayo del 2019, realizó una conferencia sobre Defensa cibernética en la cual se realizó un análisis de la problemática del ciberespacio en términos defensivos a nivel nacional y mundial, destacando las concepciones que han establecido Estados Unidos y Rusia sobre el tema, tales como ciberataques o armas cibernéticas, y describiendo experiencias que han tenido que enfrentar algunos Estados. Se hizo énfasis en los desafíos que se le manifiestan al Estado chileno, para así poder vincular a la dimensión cibernética con su Defensa (ACAGUE 2019).

La Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) del Ministerio de Defensa de Chile, de igual manera, ha ofrecido cursos de posgrado en torno a la Ciberseguridad y Ciberdefensa. El objetivo de este tipo de cursos ha sido comprender a la dimensión en la que se desarrolla este tipo de seguridad, sus características, normativas y

protocolos en función de los riesgos cibernéticos que surgen en el contexto actual. De modo que, a partir de este conocimiento se pueda seleccionar una estrategia adecuada como parte de la toma de decisiones en relación a la protección de la información (ANEPE 2020). Estos programas han contado con la asistencia de personal de Fuerzas Armadas, Policía y personas civiles que poseían el interés en las áreas de Seguridad y Defensa.

En el ámbito privado la oferta de cursos o programas de nivel superior en materia de Ciberdefensa no cuenta con un gran espectro, sin embargo, existe. Una de las instituciones privadas que ofrece este tipo de conocimientos es la Universidad de Chile, que oferta un programa de Diploma de Postítulo en Ciberseguridad y Ciberdefensa. Esta iniciativa se caracteriza por una mirada integral al fenómeno de la ciberseguridad a partir de la especificación, caracterización y análisis de las principales peculiaridades de las ciberamenazas que pueden comprometer o afectar a la seguridad de las personas, las capacidades del país y la supervivencia del Estado. Es un curso orientado a profesionales de ciencias sociales, derecho, políticas públicas, ingenierías y sistemas, además de oficiales pertenecientes a las Fuerzas Armadas. Como parte de su malla curricular, se imparte una materia titulada Ciberdefensa, en la cual se tratan los enfoques y paradigmas de la Defensa cibernética en dos sesiones, y a la Ciberdefensa y ciberinteligencia en otras dos sesiones (Universidad de Chile 2020).

En la misma institución, la Facultad de Derecho ofrece el programa de posgrado de Ciberseguridad, en el cual se analizan los principales aspectos técnicos y jurídicos de la Ciberseguridad a partir del estudio de políticas públicas, estrategias y normas que regulan el escenario cibernético frente a los riesgos que se generan debido a su masificación. En este sentido, el curso aborda a la Ciberdefensa desde su política, la respuesta estatal ante un ciberataque y la disuasión (Universidad de Chile 2020).

4. Acuerdos Internacionales firmados por Chile en materia de Defensa cibernética

En cuanto a Acuerdos Internacionales, Chile ha firmado algunos de carácter bilateral en torno a la Ciberdefensa. El país se ha suscrito a convenios de Defensa cibernética y cooperación en desastres con: “EE. UU, Reino Unido, Canadá. México, Argentina, Brasil, Perú, Uruguay, Colombia, Paraguay y Ecuador” (Estado Mayor Conjunto 2019, 4). Mismos que, involucran cooperación académica, científica, seguritaria, intercambio tecnológico e innovación, claros potenciadores de sus capacidades (Estado Mayor Conjunto 2019).

En el 2017 Chile y Ecuador firmaron varios acuerdos de cooperación, entre los cuales se contemplaban aspectos de Ciberdefensa y Ciberseguridad (Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador 2017). El 26 de abril del 2018, Chile y Argentina firmaron un acuerdo de Ciberseguridad y Ciberdefensa con miras hacia el establecimiento de un grupo de trabajo binacional que les permita materializar el trabajo conjunto (CSIRT 2019). El 9 de agosto del mismo año, Chile y Brasil firmaron un acuerdo sobre Ciberdefensa y el protocolo de catalogación de la OTAN, el cual supone la capacitación conjunta de sus Fuerzas Armadas en este aspecto, la realización de investigaciones comunes y la coordinación de acciones en caso de que una de las partes sea atacada. El Ministro de Defensa ha destacado la importancia que significa para el país recoger la experiencia y la tecnología brasileña (Ministerio de Defensa Nacional de Chile 2018).

El 17 de agosto del 2018, el Estado chileno firmó un acuerdo de cooperación en Ciberdefensa con Estados Unidos. La declaración conjunta se materializaría a través de intercambios tecnológicos, ejercicios conjuntos y capacitación (Ministerio de Defensa Nacional de Chile 2018). En el 2019 se llevó a cabo el primer ejercicio conjunto (Secretaría de Defensa de Chile 2019). En marzo de este año, el Gobierno chileno firmó con Colombia un acuerdo bilateral de Ciberdefensa en virtud del trabajo conjunto en organismos y foros internacionales e igualmente promoviendo medidas de confianza y seguridad a nivel cibernético (Ciberseguridad 2019).

La Dirección de Inteligencia de Defensa (DID), como parte de sus actividades, participó en una reunión bilateral de Estados Mayores de Chile y Perú, en la cual el alto mando chileno expuso la situación actual de la Ciberdefensa de su país y los objetivos dispuestos en su Política de Ciberdefensa. Además, formaron parte de la Célula de Inteligencia y Ciberdefensa en la Fuerza Multinacional en el ejercicio "PANAMAX 2018" (Estado Mayor Conjunto 2019). El evento fue organizado por Estados Unidos, conto con la asistencia de 20 países y tuvo como objetivo el promover la interoperabilidad y desarrollar capacidades para realizar ciberoperaciones y ejecutar tareas como integrantes de una Fuerza multinacional en el marco del respeto a la soberanía de los países miembros (Sandoval 2018).

La institución en cuestión también participó en "la aprobación y publicación de la "Doctrina Conjunta de Ciberdefensa" para conocimiento de todas las instituciones de las Fuerzas Armadas" (Estado Mayor Conjunto 2019, 14). Dicha doctrina forma parte de la Doctrina de

Defensa Conjunta del 2018, documento en el cual se especifica la representación que tiene el ciberespacio para el Estado chileno y su integridad. En este documento se indica la forma en la que debe gestionarse el accionar conjunto entre las Instituciones de Defensa frente a una ciberamenaza (CEEAG 2018).

5. Fortalezas y debilidades existentes en la estrategia de Ciberdefensa de Chile

Una de las principales fortalezas que tiene la estrategia chilena es su Política de Ciberdefensa dado que esta funciona como un esquema para poder establecer que es lo que se debe hacer para defender los sistemas esenciales o estratégicos del país, bajo que términos y en cuanto tiempo. En este documento, en la sección introductoria y en el apartado de diagnóstico se especifica la situación del país en relación al entorno cibernético. Se hace evidente la dependencia que tiene el sector público y el privado hacia las tecnologías de la información y los desafíos y riesgos que esto conlleva. A su vez, se manifiesta la forma en que se concibe al ciberespacio de tal manera que tanto las instituciones de Defensa como sus funcionarios tengan una comprensión común de lo que representa este entorno para el Estado. Esto logra una mayor sensibilización hacia el tema y ayuda a enfatizar la necesidad de contar con una estrategia adecuada.

Posteriormente en la tercera sección se establece el status de subordinación que va a tener esta política con respecto a la Política de Defensa Nacional. Esto significa que ambas políticas deben estar estructuradas bajo los mismos principios y con los mismos objetivos. Deben proteger a los ciudadanos mediante la defensa de las infraestructuras críticas del Estado, evitar que desde Chile se generen acciones irregulares y mantener el respeto al Derecho Internacional Público y cualquier instrumento que promueva un ambiente seguro y pacífico. Habiendo señalado esto con claridad, se evita que los instrumentos de Defensa, proyectos e iniciativas se vayan en contra de estas máximas y se vuelvan contraproducentes para los intereses nacionales y que estos se vuelvan inviables.

En un cuarto momento, en el texto se presentan las políticas de Ciberdefensa en base a tres divisiones. En el primer fragmento se esclarece en qué momento se hará uso de las capacidades cibernéticas. Si el Estado recibe un ataque que pone en riesgo su supervivencia, hará uso de sus competencias en legítima defensa. En base a ello se delega a las instituciones de Defensa la función de identificar a los autores de cualquier ciberataque. Esto funciona como un mecanismo de disuasión para otros Estados y actores, ya que, en otras palabras, si

alguien agrede a Chile, este utilizará todo su poder no solo para detener el ataque, sino también para responder y contraatacar.

En el segundo fragmento el Estado admite que, aunque propenda una estrategia propia, un fenómeno global como el ciberespacio necesita ser enfrentado mediante la cooperación. De allí que Chile busque participar activamente en iniciativas que persigan contrarrestar las ciberamenazas y promover patrones de conducta aceptables para poder mantener un entorno seguro. La cooperación que busca este país, de acuerdo al escrito en cuestión, no es únicamente para alcanzar que todos los Estados mantengan buenas prácticas en el ciberespacio sino también para realizar intercambios de información. A partir de esta declaración, Chile da una imagen de sí mismo al mundo y busca desarrollar y mejorar sus capacidades a través de tratados o convenios.

En el tercer fragmento, se especifica que el Estado mantendrá y desarrollará capacidades para autodefenderse. Ello implica infraestructura, personal debidamente capacitado, programas de formación, entre otros. Para poder lograrlo se describen las medidas que debe adoptar el Ministerio de Defensa y las Fuerzas Armadas. Ello no quiere decir que el proyecto se circunscribirá al ámbito militar, en este punto se genera una vinculación con la academia. Tomando en cuenta que el ciberespacio presenta varios actores y diversos riesgos, es acertado incluir a la academia para poder darle otra perspectiva a la concepción de Defensa. Esto además de ser el plan de acción que debe seguir el Ministerio citado para constituir una estructura de Ciberdefensa óptima, se puede interpretar como otro mecanismo de disuasión ya que como se evidenció, el país afirma que ya cuenta con las habilidades necesarias para defenderse y que desarrollará más capacidades para poder blindarse aún más.

La institucionalización de la ciberdefensa también es considerada como parte de este fragmento, un paso fundamental si se quiere construir una estructura fuerte. Se menciona la creación de un Comando Conjunto de Ciberdefensa, encargado de las operaciones militares de Defensa cibernética del país, un Equipo de Respuesta a Incidentes Informáticos que ayuda al Ministerio de Defensa en su labor de proteger a las infraestructuras críticas, la disposición de un CSIRT en cada rama de las Fuerzas Armadas y la creación de un Oficina de ciberdefensa en el gabinete del Ministerio de Defensa. Con la creación de estas instituciones se puede lograr la continuidad a este proyecto de Estado y adquiere una mayor credibilidad.

Esto se ve reforzado mediante la implementación del marco de trabajo de Ciberseguridad del NIST, en el cual se esclarece la forma en la que se debe estructurar e implementar una estrategia de Ciberdefensa. Proporciona los pasos que se deben realizar para poder actuar de forma integral en el ciberespacio y describe las funciones que debe cumplir el Ministerio de Defensa a través de sus distintas instituciones. Esto supone el fortalecimiento de la institucionalidad en base a la importancia que tiene cada uno de sus roles. La practicidad y la flexibilidad de este instrumento es otra ventaja ya que se puede adaptar a las necesidades de Chile en el ciberespacio y a los requerimientos establecidos en la Política de Ciberdefensa.

Si bien el trabajo a nivel doméstico y la implementación de nuevos sistemas son vitales, estos se deben ver apoyados en un trabajo a nivel internacional, tomando en cuenta las características del fenómeno que se está abordando y la transformación doctrinaria que se quiere alcanzar. En este sentido Chile ha trabajado de forma constante y ha logrado firmar una cantidad considerable de acuerdos bilaterales con distintos países. La retroalimentación que puede obtener el Ministerio de Defensa chileno a través de los tratados de Ciberdefensa, de países con un mayor tiempo de experiencia en la constitución de una estrategia viable, es valiosa para poder generar una táctica propia.

Dichos convenios posibilitan la adquisición de nuevos conocimientos en términos de Defensa cibernética a partir de los intercambios académicos, tecnológicos y de información. La capacitación del personal es fundamental y en base a los intercambios, los profesionales que asisten a cursos en el exterior tienen la capacidad de generar un aporte institucional en base a la información adquirida, misma que puede ser impartida a otros funcionarios públicos de las instituciones de Defensa y ser utilizada en distintas planificaciones.

Una de las principales debilidades estratégicas que se hace visible tanto en la Política de Ciberseguridad como en la Política de Ciberdefensa chilena es la opacidad con la que se han definido las funciones específicas de la Defensa en el plano digital. Es decir que no se han establecido los alcances y limitaciones que tienen las Fuerzas Armadas en el ciberespacio. La única función que se podría ver como específica de la institución es la protección de sus propias infraestructuras críticas, por lo demás, debe colaborar en cualquier actividad que contribuya con el desarrollo de la Ciberseguridad. No existe una diferenciación entre lo que es competencia de la Seguridad Pública y lo que ataña a la Seguridad Nacional. Hecho que

puede conllevar a que cualquier riesgo cibernético sea considerado como una amenaza a la integridad del Estado o que ninguno lo sea.

La solución a este problema parecería obvia, bastaría con establecer como competencia de la Fuerza Pública a aquellos incidentes que afecten a la seguridad de las personas e instituir como responsabilidad de las Fuerzas Armadas a los incidentes que comprometan a la Seguridad Nacional, como por ejemplo ataques a infraestructuras críticas. Sin embargo, como se vio en su momento, las amenazas cibernéticas pueden afectar de manera simultánea a ambas seguridades, por lo que no es tan sencillo tipificarlas. Un ataque cibernético a un Banco chileno puede ser considerado un delito ya que afecta a los usuarios de la entidad financiera, pero también tiene afectaciones en la Seguridad del Estado ya que estas empresas forman parte del sistema financiero, considerado una infraestructura crítica. Por ello cabe resaltar que esta no es una falencia exclusivamente de Chile, la mayoría de países tienen que lidiar con esta problemática. Empero, a pesar de que la labor es compleja, es necesaria ya que hace que el accionar de las instituciones sea más eficiente, cosa que no ocurre si las actividades se solapan y cada institución maneja el mismo incidente a discreción.

En virtud de ello es importante realizar investigaciones acerca de las amenazas que se pueden presentar en el ciberespacio y la situación del país ante las mismas. No obstante, para desarrollar documentos académicos que enriquezcan el conocimiento de la Ciberdefensa hace falta un trabajo conjunto entre Fuerzas Armadas y la academia. Esta arista necesita ser desarrollada en Chile, pues, aunque distintas instituciones de Defensa ofertan cursos de posgrado y talleres, los asistentes son mayormente militares o miembros de la Fuerza Pública, lo cual demuestra una falta de interés por parte de las personas civiles en estos temas. Patrón comprensible, tomando en cuenta que durante años se ha visto a la Defensa Nacional como un área exclusivamente militar, inclusive sus programas académicos eran únicamente pensados para los miembros de las Fuerzas Armadas. De modo que, se necesita desarrollar una cultura que permita comprender a los académicos civiles que su aporte es significativo para la protección de las infraestructuras críticas del Estado, y que se puede lograr un trabajo conjunto con los tomadores de decisiones.

Como consecuencia del desinterés o la desinformación del sector civil en torno a temáticas de Ciberdefensa, a nivel privado, las Universidades no presentan una gran oferta de programas académicos en estos temas. Es así que, en la presente investigación únicamente se encontró

una universidad que brinda cursos de posgrado en esta área. Contexto que incide en una falta de trabajo académico que permita comprender con claridad la situación en la que se encuentra el Estado chileno frente al ciberespacio. Por lo general los artículos de Defensa cibernéticos se suelen encontrar en revistas militares o en bases de datos pertenecientes a instituciones de Defensa y suelen estar escritos por personas vinculadas a dichas entidades. Aunque existen académicos civiles que escriben sobre la protección de la información en Chile, es más común observar autores que tengan algún cargo militar u observar trabajos de esta índole que sean el requisito para la graduación de cursos de acenso. El personal de Fuerzas Armadas tiene una formación bastante rígida al momento de tratar temas de soberanía, se piensa hasta cierto punto de manera más tradicional, pero ante las ciberamenazas hace falta un pensamiento más flexible, cualidad que pueden aportar profesionales que provengan de otras áreas.

6. Conclusiones

En Chile se puede constatar que ya existe un proceso de adaptación de la Defensa en torno al ciberespacio teniendo como base su política. A través de ella, se pone en evidencia la percepción que tiene este país del ciberespacio y de los desafíos que representa para el mismo. Se pone al descubierto cómo dichos retos obligan a este Estado a apropiarse de conocimientos que le permitan asegurar su supervivencia en un ambiente con características diferentes las territoriales. La política de Ciberdefensa marca la pauta para que se tomen otras iniciativas que favorezcan a la transformación que se debe llevar a cabo para poder proteger su integridad y continuar con el desarrollo del país.

Esta política tiene debilidades importantes como se observó previamente, no obstante, es un instrumento que tiene el potencial para ser mejorado y del cual ya han surgido acciones concretas que benefician a los intereses del Estado. Entre ellas está el incremento de la oferta académica en materia de Ciberdefensa que, si bien no es muy amplia, es un paso importante para lograr la transformación dogmática deseada. El incremento del conocimiento en este campo va a ayudar a la mejor comprensión de los desafíos a los cuales se enfrenta Chile dentro del ciberespacio. Inclusive, con el desarrollo de nuevos conocimientos, se podría retroalimentar a la política y minimizar sus falencias.

A pesar de que la oferta académica en Chile, en materia de Ciberdefensa, aún necesita ser desarrollada, el Ministerio de Defensa ya ha plasmado una Doctrina específica en este tema. Pese a que esta también tiene debilidades, pues arrastra los mismos principios que tiene la

política de Ciberseguridad y la política de Ciberdefensa, en ella ya se hace evidente la intencionalidad de un cambio en el pensamiento tradicional que ha caracterizado a las instituciones de Defensa por mucho tiempo. La comprensión de lo complejo que puede llegar a ser el manejo de ciertos incidentes en el ciberespacio y de lo impropias que pueden ser las estrategias clásicas en un ambiente intangible se hace presente a lo largo del texto. En definitiva, esto supone un avance significativo para Chile y posiblemente le otorgará ventajas por sobre otros países.

Capítulo 3

La estrategia cibernética de Ecuador

El presente capítulo tiene la finalidad de analizar la estrategia ecuatoriana de Ciberdefensa y averiguar si existe un proceso de adaptación doctrinaria en función del ciberespacio. Para ello primeramente se estudiará la realidad que se le presenta al Ecuador en el plano digital. Se detallarán, a través de diversos estudios, cuáles son los sectores más atacados y las amenazas que más agobian al Ecuador, así como también los incidentes que han surgido en este sentido. A través de estudios realizados por empresas especializadas en seguridad informática se expondrá la posición que mantiene el Estado ecuatoriano a nivel mundial y regional en cuanto a los países más ciberatacados.

Una vez expuesta las condiciones en las que se encuentra el Ecuador en la dimensión digital se procederá a explorar cuales son las políticas que ha instituido el Estado en materia de Defensa cibernética. En este punto se pretende dilucidar la existencia de principios que dictaminen qué es lo que deben hacer las instituciones de Fuerzas Armadas en caso de un ataque. Igualmente se detallarán las iniciativas que se han tomado en torno a las ciberamenazas y el desarrollo de infraestructuras. Mediante esta información se podrá percibir la concepción que tiene el país acerca de los riesgos que representa el entorno cibernético y si se ha iniciado un cambio doctrinario para contrarrestarlos.

A continuación, se profundizará sobre el desarrollo académico en materia de Ciberdefensa. Se indagará en términos de oferta académica en instituciones de tercer y cuarto nivel, privadas y públicas. Igualmente, se tomará en cuenta la capacitación recibida por el personal de Defensa, es decir, los cursos de especialización que se les haya impartido. Estas variables dan cuenta del compromiso que mantiene el país en promover el desarrollo de conocimiento para poder enfrentar una situación en concreto. Las iniciativas para fomentar la investigación en áreas de interés para el Estado son fundamentales si lo que se quiere es generar una adaptación frente a un fenómeno complejo y cambiante.

Si el país no cuenta con las capacidades para poder generar conocimientos rápidamente sobre sistemas informáticos, puede buscar apoyo en países que tengan más experiencia en el área o que hayan trabajado por más tiempo. De allí que, en un cuarto apartado se examinen las relaciones internacionales de Ecuador en cuanto a Ciberdefensa. Si bien las experiencias de

cada país son particulares y no se vuelven a repetir, existen fundamentos en los planes de acción que son comunes en la mayoría de países, sobre los cuales se puede edificar una estrategia propia. Ecuador podría sacar provecho del conocimiento de otros países y de sus experiencias para poder generar un plan que le permita enfrentar a las ciberamenazas de mejor manera.

Finalmente se presentarán las fortalezas y debilidades que muestra la estrategia ecuatoriana. En este punto se analizarán cuáles son los pilares más sólidos que ha desarrollado el Ministerio de Defensa para incrementar sus capacidades. Igualmente se determinarán cuáles son las falencias de su planificación y cómo estas pueden tener consecuencias contraproducentes al momento de enfrentar una amenaza hacia sus sistemas fundamentales.

1. Contextualización del escenario cibernético en Ecuador

En el Ecuador el uso y la implementación de Tecnologías de la Información y la Comunicación (TICs) han experimentado un aumento considerable desde el año 2014 hasta el año 2018. Esto se hace evidente en el hecho de que la mayoría de sus instituciones públicas y privadas han adoptado sistemas informáticos que permiten a los ciudadanos realizar distintas diligencias en línea o de forma virtual. De conformidad con el reporte mundial sobre tecnologías de la información del 2016, realizado por el Foro Económico Mundial, el Ecuador se encuentra en el puesto 82 de 139 países en cuanto a innovación en economía digital y aprovechamiento de las TICs (Baller, Dutta y Lanvin 2016).

Si bien la automatización de las empresas ecuatorianas supone el desarrollo del país, también devienen en problemas de carácter cibernético. En el país, los ciberataques han tenido como objetivo principal a las entidades financieras y a los sistemas estatales. De acuerdo al Ministerio Coordinador de la Seguridad, en el año 2014 se observó un incremento del 37% en relación a robos virtuales a la banca (Vargas, Recalde y Reyes 2017). Cifra que es alarmante tomando en cuenta que en el año 2013 fueron sustraídos 13,3 millones de dólares del banco central mediante un ataque cibernético. En el 2015 el banco del Austro sufrió un fraude digital en el cual se extrajeron alrededor de 12 millones de dólares (Bouveret 2018). Este acto irregular fue atribuido al grupo Lazarus el cual transfirió el dinero a una cuenta en Estados Unidos (Mogollón 2017).

En cuanto a los sistemas públicos, estos han sido atacados por distintas agrupaciones, entre ellas Anonymous (Vargas, Recalde y Reyes 2017). En rechazo a la falta de libertad de expresión, dicha agrupación ha filtrado información sobre personal policial y trabajadores pertenecientes a otras instituciones públicas. Se considera que las entidades militares, policiales, diplomáticas y gubernamentales ecuatorianas han sufrido ciberespionaje. Se ha registrado ataques que han dejado sin servicio a las páginas web gubernamentales por varias horas. El sistema electoral también ha sido víctima de miles de ataques con la finalidad de sabotear las elecciones presidenciales. En el año 2016, la fragilidad del sistema informático de las instituciones públicas ecuatorianas se hizo evidente cuando la Secretaría Nacional de Educación Superior, Ciencias y Tecnología recibió un ataque en el cual se registraron títulos ilegalmente. En este incidente se reveló que los beneficiarios pagaban entre 1000 y 10.000 dólares por título a los atacantes (Salinas 2018).

En un estudio realizado en el año 2018 por la empresa Deloitte acerca de la tendencia de riesgos y seguridad informática en Ecuador, en el cual un 39% de las instituciones participantes eran públicas, se visualizó que 4 de cada 10 entidades han recibido agresiones que atentan contra su seguridad a lo largo del año 2017 y 2018. Uno de los principales problemas que manifiesta el personal encargado de la Ciberseguridad para poder neutralizar estos incidentes es la falta de recursos y de presupuesto suficiente (Deloitte 2018). Sin embargo, la implementación de los sistemas informáticos y la automatización de procesos es algo que se ha llevado a cabo gradualmente y que a medida que aparezcan nuevos avances tecnológicos, se seguirán actualizando.

Kaspersky, compañía dedicada a ofrecer productos de seguridad informática, registró que en América Latina se inscriben 45 ataques cibernéticos por segundo, y dentro de esta valoración Ecuador es el quinto país con más ataques cibernéticos en América del Sur (Kaspersky 2019). La misma empresa público el hallazgo de una campaña de ciberespionaje denominada “Machete”, en la región. Los autores de estas agresiones buscaban datos clasificados de Seguridad Nacional, como radares, proyectos, registros y operaciones militares. Ecuador fue víctima en esta campaña y se detectaron 282 víctimas de espionaje (Salinas 2018).

Los ciberataques en el país sudamericano no solamente se han incrementado, sino que se han vuelto más sofisticados, tal es así que el sistema de contratación pública fue víctima en el año 2015 de un ataque con la finalidad de favorecer en la concesión de proyectos a determinadas

empresas (Bravo 2015). Como resultado, alrededor de 2500 procesos se vieron perjudicados, hecho de gran relevancia tomando en cuenta que a través de las herramientas digitales que maneja la institución en cuestión, se realizan transacciones que oscilan los 10 millones de dólares, equivalente al 10% del PIB más o menos. En el mismo año empresas privadas en Cuenca, Quito y Guayaquil fueron presa de un ciberataque masivo orientado a manipular el sistema de facturación electrónica, mismo que fue requerido por el Servicio de Rentas Internas para mejorar la gestión de estos datos (Salinas 2018).

El incremento de dichos incidentes también ha tomado ventajas de los vacíos sistémicos del Gobierno ecuatoriano en términos cibernéticos. Este ha acusado a una transnacional de haber adquirido de manera irregular información confidencial del presidente y ciertos funcionarios de Estado. A su vez se ha manifestado que el país ha recibido ataques de un país vecino para robar información sensible presidencial y militar (PanAm Post 2014), así como también agresiones desde un país de primer mundo con la misma finalidad (Salinas 2018).

Las Fuerzas Armadas, quienes están llamadas a proteger la integridad del país en distintas dimensiones, incluido el ciberespacio, asimismo ha automatizado la mayoría de sus procesos. De modo que, hace uso de las TICS para realizar las operaciones requeridas por el Estado y aquellas que son propias de la institución, toda vez que se ha contemplado a estas tecnologías como una fuerza multiplicadora y de optimización de recursos. En este sentido, la dependencia tecnológica de esta institución agudiza las vulnerabilidades que se le presentan en el ciberespacio (Ministerio de Defensa Nacional de Ecuador 2018). La falta de conocimiento en torno a los sistemas utilizados hace que las soluciones de seguridad no se ajusten a las necesidades que presenta el país. Actores extranjeros, con un entendimiento superior acerca del funcionamiento de los sistemas informáticos, tienen la capacidad de irrumpir, transgredir, interrumpir y obtener datos sensibles (Quintero 2014).

De acuerdo con expertos en el tema de ciberdefensa, los sistemas militares que son más susceptibles a recibir ataques son la infraestructura informática del Comando Conjunto de las Fuerzas Armadas (COMACO), los servidores que contienen información clasificada, el sistema del comando de inteligencia militar, de radares, armas y navegación, y el sistema del Instituto de Seguridad Social de las Fuerzas Armadas (ISSFA). A nivel estatal, las principales infraestructuras críticas que serían blanco de irrupciones digitales son las centrales eléctricas, las instituciones financieras y los sistemas de información y comunicación.

2. Establecimiento de planes, agendas y políticas en relación a la Ciberdefensa

Como consecuencia de los acontecimientos previamente citados y el panorama cibernético en el cual se desarrolla Ecuador, este ha articulado un plan para poder posicionarse de mejor manera ante los riesgos que representan las ciberamenazas. El Estado, para poder minimizar sus vulnerabilidades, ha tomado acciones políticas que suponen el inicio de una estrategia que deberá ser desarrollada y actualizada continuamente. En materia de Ciberdefensa, a partir del año 2014, se han generado iniciativas específicas que persiguen la resiliencia de su sistema para poder proteger de forma efectiva sus infraestructuras críticas, así como también las del Estado.

Una de las primeras decisiones relevantes que tomó el Gobierno ecuatoriano en torno a la Defensa cibernética se manifestó en el Plan Nacional de Seguridad Integral (PNSI) 2014-2017. En este plan se establecen principios para diversos sectores del Estado, de modo que se pueda generar una estructura integra que precautele la seguridad del país, y se hace un acercamiento a la dimensión cibernética. Cabe mencionar que dicho instrumento se encuentra ligado al buen vivir de manera que está destinado a proteger el libre ejercicio de los derechos humanos y de la naturaleza en diversas dimensiones. Es decir que se ven a estos como objetos de Seguridad y Defensa cuyas amenazas, en este caso, son los riesgos cibernéticos (Gobierno de la República del Ecuador 2014-2017).

En el documento en cuestión se observa a la revolución tecnológica y digital como un hecho que supone una serie de desafíos políticos, económicos, sociales y seguritarios. Se hace latente la fragilidad del Estado en un entorno abstracto. El ciberespionaje, la revelación de información confidencial y las irrupciones cibernéticas son reales y no son ajenas al contexto ecuatoriano. Estas ponen en entredicho a conceptos como la privacidad y la protección de información sensible para los intereses nacionales. El ambiente virtual ha posibilitado el surgimiento de nuevos actores en el ámbito internacional que posiblemente poseen un poder material considerablemente inferior con respecto al que puede poseer un país, pero que puede articular un ataque que comprometa la supervivencia del mismo (Gobierno de la República del Ecuador 2014-2017).

Para el Gobierno ecuatoriano, las estrategias globales de Defensa, la vigilancia global que es clandestina e irregular y sobre todo el espionaje, caracterizan al escenario global en la dimensión digital. Por ello, en el PNSI, Ecuador plantea que es necesario mantener el

compromiso con el desarrollo de la Ciberdefensa[1]. Para garantizar la perdurabilidad del Estado se debe contar con capacidades soberanas que permitan alcanzar los intereses nacionales. En consecuencia, es pertinente desarrollar investigaciones en ciencia y tecnología que doten a las instituciones de Defensa con las herramientas necesarias para poder resguardar los sistemas sensibles del país (Gobierno de la República del Ecuador 2014-2017).

Entre las estrategias de seguridad que se plantean en este documento, se han planteado algunas que son específicas de la Defensa cibernética. En este ámbito se establece que se debe generar y fortalecer las capacidades de las Fuerzas Armadas con la finalidad de proteger la infraestructura informática, las redes estratégicas y la información clasificada. A su vez se busca robustecer los mecanismos interinstitucionales para poder contrarrestar las amenazas que atentan contra la integridad del Estado (Gobierno de la República del Ecuador 2014-2017).

En la agenda política de Defensa, comprendida en el PNSI, el Ministerio de Defensa ecuatoriano plasma la percepción que tiene sobre las Tecnologías de la comunicación y la información como un eje transversal y potencializador de amenazas no-convencionales. Para la institución, las herramientas informáticas han dado paso a la materialización de la guerra cibernética y por ende a un cambio en la forma de concebir la seguridad. En el contexto internacional, los sistemas informáticos se han convertido en elementos fundamentales dentro de la Defensa de los países, así como también en instrumentos ofensivos (Gobierno de la República del Ecuador 2014-2017).

Previo a esta concepción, las funciones de la Defensa en Ecuador se limitaban al control, el cuidado y la protección del espacio territorial ecuatoriano en el plano terrestre, marítimo y aéreo. No obstante, en la presente agenda se toma al ciberespacio como otra dimensión en la cual el país debe ser defendido y que ha adquirido importancia debido a su particularidad y sus alcances. Es vital poder resguardar los derechos y libertades de los ciudadanos y cumplir con la misión fundamental de Fuerzas Armadas que es garantizar la soberanía e integridad territorial. Realidad que requiere de un cambio en la estructuración de la Defensa ya que en la actualidad la territorialidad del Estado se interrelaciona con el escenario virtual donde es

[1] Para Ecuador la Ciberdefensa se concibe como "la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte a la soberanía nacional" (Ministerio Coordinador de Seguridad 2014-2017, 118)

complejo hablar de una soberanía o un dominio claramente delimitado (Ministerio de Defensa del Ecuador 2014-2017).

Para poder solventar la disyuntiva que existe entre las percepciones tradicionales de lo que es soberanía y este concepto en el plano digital, el mismo ha sido ampliado para abarcar las decisiones independientes que toma el Estado al interior de sus fronteras físicas y el amparo de los derechos y libertades de los ciudadanos en otros ambientes donde igualmente se desarrolla su vida. En este sentido la soberanía del país en el contexto cibernético se traduce en el resguardo de sus sistemas estratégicos de los cuales depende el desarrollo estatal, la protección de los recursos informáticos y la preservación del conocimiento en torno a la Defensa cibernética (Ministerio de Defensa del Ecuador 2014-2017).

Con la finalidad de poder materializar y ejercer soberanía de la manera antes estipulada, el Ministerio de Defensa ecuatoriano expone como parte fundamental de su planificación la creación de políticas específicas en relación al espacio cibernético. Así misma procura realizar operaciones de protección de la integridad del país sudamericano en la red. Dichas operaciones estarían dirigidas hacia las infraestructuras críticas del país que contengan información clasificada (Ministerio de Defensa del Ecuador 2014-2017).

La definición que maneja el Ministerio de Defensa en cuanto a Ciberdefensa es la siguiente:

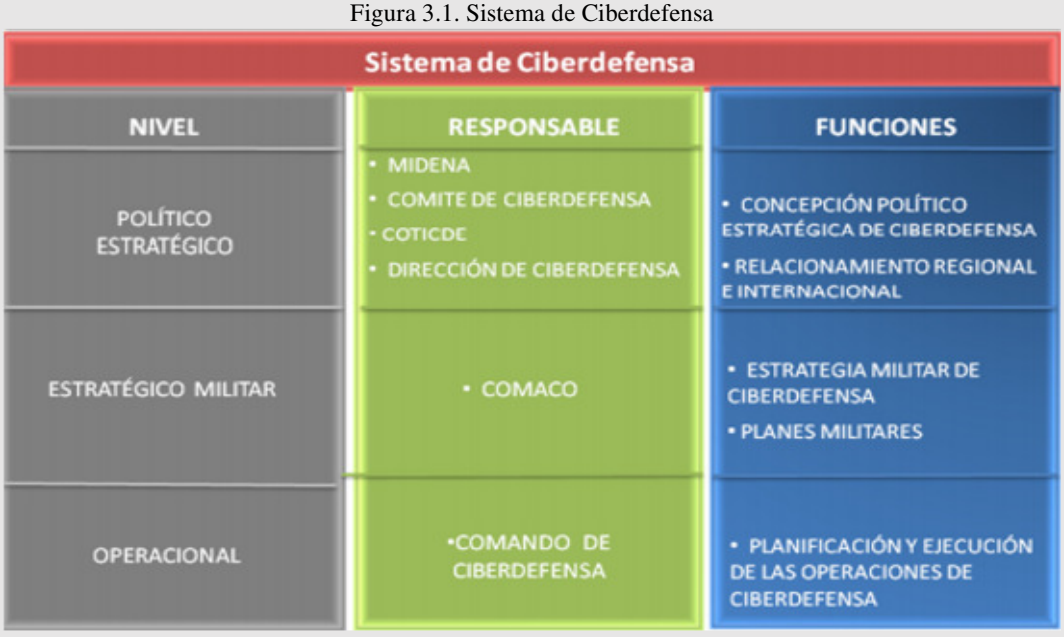
> La Ciberdefensa constituye una iniciativa diseñada para ampliar los sistemas de defensa de los estados y protegerlos de los nuevos riesgos emergentes en la sociedad de la información. Entre estos riesgos se encuentran la "guerra cibernética", entendida como la utilización de las debilidades de las redes informáticas que van desde el espionaje y la infiltración de los sistemas informáticos hasta la destrucción física de los recursos del oponente; y el "espionaje cibernético", cuyo objetivo es obtener información confidencial circulante en ese medio. la ciberdefensa es fundamental en este momento, en el que se han visto las enormes consecuencias que este tipo de ataques pueden generar a la seguridad del estado (Ministerio de Defensa del Ecuador 2014-2017, 94).

A pesar de la importancia que ha adquirido el ciberespacio para la supervivencia del Estado, de acuerdo a lo expuesto por el Ministerio de Defensa hasta el momento, las políticas que se han presentado en este aspecto son subsidiarias de otros ámbitos de la Defensa. Se han

planteado estamentos bastante generales como: el desarrollo de capacidades de Ciberdefensa para garantizar la soberanía del Estado en función del Buen Vivir, la participación de las fuerzas militares en la Seguridad integral y la protección de información estratégica del país. El fortalecimiento de los mecanismos interinstitucionales es otra de las políticas que se han establecido como parte de la agenda de Defensa. Aquí se aclara que esta responsabilidad o labor no ataña única y exclusivamente a las Fuerzas Armadas, aunque es la institución principal en aras de velar por la integridad del Estado. Dado que ello es un bien público el compromiso debe provenir de todas y todos los ciudadanos (Ministerio de Defensa del Ecuador 2014-2017).

Hasta este punto, dentro de los objetivos que persigue el Ecuador en materia de Ciberdefensa, plasmados en el PNSI y en la Agenda de Defensa, no se visualizan acciones concretas que vayan a realizar para procurar las infraestructuras críticas del Estado. Pese a ello, en el año 2014 mediante el Acuerdo Ministerial 281, se crea el Sistema de Ciberdefensa como la herramienta que, articula el accionar de las instituciones llamadas a conformar dicha estructura y delega sus funciones. Es decir que su finalidad es coordinar e implementar políticas de Defensa cibernética (Ministerio de Defensa del Ecuador 2014).

Figura 3.1. Sistema de Ciberdefensa



Fuente: Ministerio de Defensa 2014

Esta iniciativa consta de 3 pilares fundamentales que son: el político estratégico, el estratégico militar y el operacional. Cada uno de ellos contiene instituciones responsables específicas que cuentan con funciones particulares. En el pilar político estratégico se encuentra el MIDENA, el Comité de Ciberdefensa, el Comité de Tecnologías de la Información y Comunicación de la Defensa (COTICDE) y la dirección de Ciberdefensa. Sus funciones se basan en la concepción político estratégica de la Defensa cibernética y la gestión de acuerdos internacionales en este aspecto. En el segundo pilar se encuentra el Comando Conjunto (COMACO), entidad encargada de generar estrategias militares. El tercer pilar es responsabilidad del Comando de Ciberdefensa (COCIBER), el cual debe llevar a cabo la organización y realización de las operaciones cibernéticas (Ministerio de Defensa del Ecuador 2014).

En esta estructura existen cuatro entidades a las cuales se les ha otorgado mayores responsabilidades o que se les ha asignado objetivos claramente delimitados. La primera es el Comité de Ciberdefensa cuya misión es establecer el trabajo de los organismos internos de manera que se materialice el desarrollo de capacidades y la Defensa ante amenazas digitales que puedan afectar sustancialmente al Estado. Diseñar el pensamiento político-estratégico, el cual debe guardar coherencia con la Agenda de Defensa Nacional, y promocionar el mismo a nivel nacional. Debe crear políticas públicas de acuerdo a sus competencias conjuntamente con las instancias correspondientes. El monitoreo del cumplimiento de las políticas y el buen funcionamiento de los sistemas de Ciberdefensa también consta dentro de sus funciones. Asimismo, tiene la responsabilidad, junto al MIDENA, de promover y generar iniciativas de formación y capacitación (Ministerio de Defensa del Ecuador 2014).

Este comité se constituye de la siguiente forma:

- Ministra/o de Defensa o su delegado/a, quien lo presidirá
- Subsecretario/a de Gabinete Ministerial o su delegado/a
- Subsecretario/a de Apoyo al Desarrollo o su delegado/a
- Subsecretario de Defensa o su delegado/a
- Coordinador/a General Jurídico o su delegado/a
- Director/a de Ciberdefensa, actuará como secretario/a
- Jefe del Comando Conjunto, o su delegado/a
- Comandante del Comando de Ciberdefensa

- Podrá contar con la participación de los/las funcionarios u otros especialistas cuando se lo requiera (Ministerio de Defensa Nacional del Ecuador 2014, 5).

La segunda es el Comité de Tecnologías de la Información y Comunicación de la Defensa que se desempeña como una instancia de asesoría. Su finalidad es orientar al Comité de Ciberdefensa en aspectos técnicos y mantener un control en cuanto a la pertinencia de los sistemas que se estén utilizando. Sus competencias no se limitan a el asesoramiento del Comité sino también al de la Presidencia de la República para poder delinear el esquema gubernamental de Seguridad informática (Ministerio de Defensa Nacional del Ecuador 2014).

La tercera es la Dirección de Ciberdefensa, subordinada al Ministerio de Defensa y que cuenta con las siguientes funciones:

- Apoyar con el diseño e implementar la concepción político-estratégica de ciberdefensa que se someterá a la aprobación de la máxima autoridad del Ministerio de Defensa.
- Coordinar con el Comando de Ciberdefensa Conjunto las estrategias necesarias para la ejecución del Plan de Ciberdefensa.
- Articular el adecuado funcionamiento de los sistemas de información, comunicación e inteligencia relativos a la Ciberdefensa, y evaluarlo periódicamente.
- Proponer disposiciones y directrices para el desarrollo e implementación de la capacidad de Ciberdefensa, a ser concertadas en el Comité de Ciberdefensa.
- Promover la política de Ciberdefensa a nivel nacional y regional.
- Las demás competencias serán asignadas por la máxima autoridad del Ministerio de Defensa (Ministerio de Defensa Nacional del Ecuador 2014, 5).

La cuarta dignidad, y la que ha sido mayormente visibilizada, es el Comando de Ciberdefensa. Este está conformado por personal técnico civil y operativo militar, ingenieros electrónicos, ingenieros en sistemas y masters en seguridad informática. Mismos que han recibido capacitación en Ethical Hacking, informática forense, y Linux (Mogollón 2017). Su función es gestionar las capacidades digitales para poder actuar de forma defensiva y de esta manera lograr resguardar las infraestructuras críticas y estratégicas del Estado, así como también generar respuestas ante incidentes con fines malintencionados (Ministerio de Defensa del Ecuador 2014). De conformidad con el Jefe de Estado Mayor del Comando de Ciberseguridad, se espera que para el año 2021 la entidad en cuestión alcance las capacidades necesarias para poder cumplir con sus propósitos de manera óptima (Mogollón 2017). El

Estado realizó una inversión de ocho millones de dólares para dar inicio al proyecto (El telégrafo 2014).

Las competencias de este Comando son:

- Proteger la infraestructura crítica del Estado en el corto, mediano y largo plazo.
- Desarrollar la capacidad de Ciberdefensa en: exploración, prevención, defensa y respuesta.
- Generar una estructura del Comando de acuerdo al modelo de gestión por procesos de la Defensa.
- Elaborar el Plan de Ciberdefensa con calificación correspondiente, para conocimiento y análisis del Comité de Ciberdefensa y aprobación de la máxima autoridad del Ministerio de Defensa.
- Coordinar con la Dirección de Ciberdefensa los temas de su competencia (Ministerio de Defensa del Ecuador 2014, 6).

Las iniciativas que estableció el Ecuador durante el año 2014 marcaron un punto de partida de una estrategia que suponía un mayor desarrollo y una actualización continua. No obstante, fue hasta el 2018, con el Libro Blanco de Fuerzas Armadas, que se retoma el tema de la Ciberdefensa. En este texto se vuelve a manifestar los riesgos que ha traído consigo la mundialización de las TICs, los cuales exigen políticas específicas y una planificación adecuada. Nuevamente se observa las particularidades del ciberespacio y las ventajas que ofrece a actores y organizaciones que pretenden atacar los sistemas vitales del país (Ministerio de Defensa del Ecuador 2018).

Acorde a lo que se expone en el documento, las Fuerzas Armadas ven al ciberespacio como el quinto dominio donde se debe precautelar la soberanía del Estado. Los riesgos que presenta la dimensión digital se mencionan en un primer momento de manera muy general como: ataques cibernéticos, manipulación de datos y robo de información. Posteriormente se describen las amenazas de forma más detalladas (Ministerio de Defensa del Ecuador 2018).
Los peligros que se le presenta al Ecuador en el espacio cibernético son:

> Los ciberataques y vulneración de la infraestructura crítica del estado, que se basan en la explotación de las debilidades de las redes informáticas, ejecutadas a través de mecanismos tecnológicos de ciberterrorismo, ciberdelito, cibercrimen, ciberespionaje, e infiltración de los

> sistemas informáticos, convirtiéndose en un potente instrumento de agresión contra la infraestructura del estado, lo cual podría comprometer la seguridad nacional (Ministerio de Defensa Nacional del Ecuador 2018, 53).

En este escrito se manifiesta una realidad que no es exclusiva del Ecuador, sino que se ha presentado en la mayoría de países. Como se vio en su momento los diversos actores y las características que presenta el ciberespacio limitan el accionar de una sola institución, es decir que no admite el acaparamiento de todo el conocimiento, por lo que necesita de un análisis más integral desde distintas aristas. Empero, el interés de la población civil por apropiarse de los temas de Defensa y generar investigaciones es mínimo. Ello se debe a que por muchos años las únicas personas que podían tratar estos temas y acceder a la información eran militares. En este sentido, con la actualización del Libro Blanco, se busca romper con este paradigma y generar una cultura de Defensa (Ministerio de Defensa del Ecuador 2018).

El perfeccionamiento de las capacidades cibernéticas de las Fuerzas Armadas aporta directamente al desarrollo del país. De conformidad con el Ministerio de Defensa, las aptitudes que poseen en términos informáticos son importantes y le permitirían salvaguardar los sistemas de los sectores estratégicos del país en caso de una agresión. Sin embargo, es necesaria la actualización constante de mecanismos y estrategias. Para ello se considera que la generación de conocimientos y el uso propicio de los mismos, es fundamental. Esto es lo que permitirá solventar las necesidades que presenta el país en la dimensión cibernética. Generar sistemas propios mitigaría la dependencia hacia software extranjero (Ministerio de Defensa del Ecuador 2018).

3. Desarrollo de conocimiento en materia de Ciberdefensa en Ecuador

Si lo que se quiere es avanzar en cuanto a generación de conocimiento, la oferta académica debe incrementarse. Empero en el Ecuador la educación en Ciberdefensa es limitada especialmente para la sociedad civil. Según Frankie Catota, Granger Morgan y Douglas Sicker, el nivel de educación en Seguridad cibernética es elemental, con lo cual se puede comprender que la situación sobre la instrucción académica en términos de Ciberdefensa es aún más restringida, dado que es un área mucho más específica. A nivel pregrado la oferta académica es prácticamente inexistente, y existen escazas iniciativas de posgrado. En el estudio realizado por los autores antes mencionados, entre todas las instituciones que fueron analizadas, solamente se encontró un curso de posgrado en Defensa cibernética. Esto se debe

a la prioridad que le dan las universidades a otro tipo de contenido (Catota, Morgan y Sicker 2018).

En el ámbito militar la capacitación del personal cuyas funciones se enmarcan en el ámbito digital si ha sido llevada a cabo. En el año 2014 se planteó la inclusión de Ciberdefensa en la malla curricular de las instituciones de formación militar, proyecto que hasta el 2018 no se ha concretado. No obstante, en la rendición de cuentas del MIDENA, presentada el mismo años, la institución expuso que ya se había iniciado el proceso de capacitación para que se puedan ejecutar estrategias y operaciones cibernéticas (Ministerio de Defensa del Ecuador 2014). También han tenido participación en seminarios como el "Seminario Regional de Ciberdefensa". Cabe mencionar que este tipo de preparación no es algo que se puede alcanzar en unos días, requieren de una constante actualización. La situación académica en las instituciones de Defensa no es mucho más alentadora que la de la sociedad civil. Este es un inconveniente que parte de la falta de comunicación entre la academia y el sector público. Ello limita la toma de decisiones en base a los hallazgos de estudios académicos e impide la comprensión de la demanda que presentan los fenómenos cibernéticos (Catota, Morgan y Sicker 2018).

4. Acuerdos internacionales de Ecuador en términos de Ciberdefensa

El Estado ecuatoriano ha manifestado en su agenda de Defensa que las relaciones internacionales se encuentran supeditadas a los intereses de su pueblo. En relación a ello, apoya la independencia de los Estados y la igualdad jurídica. Promueve la convivencia pacífica entre países y condena la imposición de un país por sobre otro, manteniendo cierta injerencia sobre aquellas decisiones que deberían ser soberanas y propias. Apoya la iniciativa del desarme universal, y se encuentra presto a respetar los derechos humanos y el Derecho Internacional (Ministerio de Defensa del Ecuador 2018).

Para Ecuador la cooperación en la región es fundamental para poder solucionar problemáticas globales como los riesgos cibernéticos. Participar activamente para poder alcanzar la integración de América del Sur es una prioridad para el Gobierno ecuatoriano (Ministerio de Defensa del Ecuador 2018). Si se alcanza esta meta se podría generar una respuesta de mayor eficacia frente a las ciberamenazas (Ministerio de Defensa del Ecuador 2014-2017). En una de las cumbres de la UNASUR, se le asignó al Consejo de Defensa suramericano la creación de una propuesta de Ciberdefensa a nivel regional. Con este proyecto se pretende materializar

una especie de cinturón que permita resguardar la información que manejan los jefes de Estado y la soberanía de los países miembro (El telégrafo 2014). Al apoyar este tipo de iniciativas, Ecuador demuestra que su objetivo es mantener buenas relaciones y acuerdos en materia de Defensa con los países Sudamericanos, especialmente con Colombia y Perú, países fronterizos (Ministerio de Defensa del Ecuador 2018). En este sentido, Ecuador ha participado activamente en las iniciativas de Defensa que ha desarrollado la UNASUR. Mediante el Centro de Estudios Estratégicos de Defensa de la Escuela Suramericana de Defensa se intentó establecer una concepción compartida en términos de Protección regional y generar proyectos de Ciberdefensa (Ministerio de Defensa del Ecuador 2014-2017).

Este país sudamericano también mantiene relaciones con Estados Unidos en cuanto a Defensa. Estas se gestionan a través de una oficina de cooperación la cual posibilita el intercambio de información, la adquisición de tecnología y la capacitación de miembros de Fuerzas Armadas en el país norteamericano (Ministerio de Defensa Nacional del Ecuador 2018). Aunque el objetivo de esta colaboración se basa principalmente en la lucha contra el narcotráfico y amenazas relacionadas, este es un canal que permitiría la cooperación de ambos países en otras áreas y así potencializar las capacidades ecuatorianas de Ciberdefensa. Asimismo, la Unión Europea (UE) se ha convertido en un organismo estratégico para Ecuador en lo que respecta a Defensa. A raíz de la firma de acuerdos comerciales entre ambas partes las relaciones internacionales ecuatorianas se han diversificado. Esto ha posibilitado la adquisición de equipamiento militar, la formación especializada del personal en territorio europeo y el intercambio tecnológico (Ministerio de Defensa del Ecuador 2018).

Dentro de los documentos estatales que rigen a la Defensa ecuatoriana no se hace una alusión específica a la cooperación en Ciberdefensa, no obstante, el Ecuador si ha firmado acuerdos en este sentido. En el año 2017, el Estado chileno firmó un acuerdo bilateral de Defensa con el Estado ecuatoriano. Este supone la cooperación de ambas partes en materia de Ciberdefensa, lo cual incluye la comunicación entre comandos conjuntos, intercambios académicos, intercambio de experiencias y conducción de políticas para el empleo óptimo de las capacidades digitales de Fuerzas Armadas (Infodefensa 2017).

Ecuador también ha buscado estrechar lazos con Brasil para poder alcanzar una cooperación en términos de Defensa cibernética. El país ha mostrado gran interés en adquirir conocimientos del país carioca en cuanto al desarrollo de centros de Defensa contra

ciberataques. El conocimiento que posee el gigante sudamericano sería una herramienta importante para poder fortalecer la estrategia ecuatoriana (Infodefensa 2015).

5. Fortalezas y debilidades de la estrategia de Ciberdefensa ecuatoriana

La principal fortaleza que presenta la estrategia ecuatoriana es el Sistema de Ciberdefensa. Dicho instrumento mejora la capacidad de organización y gestión del ámbito de la Defensa cibernética. Permite delegar funciones especializadas a las instituciones correspondientes, evitando que se superponga el accionar de unos y otros. Se reduce las maniobras a discreción de las entidades y se alcanza una gestión mucho más efectiva. Cada entidad cuenta con objetivos específicos pero complementarios al momento de construir una estrategia de Ciberdefensa resiliente.

En el sistema en cuestión se establece claramente los responsables de crear las políticas públicas en relación a la Ciberdefensa, quienes desarrollarán la estrategia netamente militar y quienes se desenvolverán en al ámbito operativo. Si este tipo de organización es aprovechado tiene el potencial para poder agilizar el cumplimiento de los objetivos nacionales en materia de Defensa cibernética.

El primer problema que se visualiza en la estrategia ecuatoriana es la falta de continuidad en los procesos. En el 2014 se genera el Sistema de Ciberdefensa a partir del acuerdo 281, en el cual se planifica la creación de una política de Defensa cibernética y la constitución del Comando de Ciberdefensa. En el mismo año se establece la Agenda de Defensa que contiene ciertas políticas referentes a la protección del Estado en el ciberespacio. En los tres años siguientes no se evidencia un seguimiento a estas iniciativas, lo cual se sustenta en la rendición de cuentas del MIDENA. Únicamente en el informe del 2014 se mencionan los avances que ha tenido la institución en cuanto a Ciberdefensa, en los documentos posteriores no se hace alusión sobre este tema. Es para el año 2018 que se vuelven a generar acciones concretas con la actualización del Libro Blanco, pero aun así no se llega a materializar una política centrada en los riesgos cibernéticos.

Ello constituye la principal debilidad de la estrategia ecuatoriana que es la falta de una política específica en materia de Ciberdefensa. Sobre la base de una política pública de Defensa cibernética se pueden establecer los intereses del Estado y de su sociedad frente a un fenómeno específico. La creación de las mismas determina la importancia que le da un país a

problemas como las ciberamenazas. Empero, a pesar del análisis que ha realizado el Estado ecuatoriano sobre los riesgos que representa la dimensión cibernética, este no ha formulado un instrumento estatal que rija el accionar de las instituciones de Defensa en el plano digital. La necesidad de proteger al Estado frente a posibles ataques cibernéticos requiere de una transformación doctrinaria que demuestre la voluntad política de querer solucionar este problema. Si no se cuenta con principios concretos y objetivos claramente definidos se agudizan las vulnerabilidades y mitigarlas se vuelve un trabajo complejo. De igual manera se reduce la capacidad de coordinación interinstitucional.

Como consecuencia surgen otras debilidades, entre ellas la falta de institucionalización que conlleva al desconocimiento del alcance que tiene cada entidad pública. Al no existir una política especifica en lo que ataña a la Defensa cibernética, se genera una ambigüedad en cuanto al rango de acción que tiene Fuerzas Armadas. En consecuencia, las competencias de cada dignidad quedan a criterio propio. El Ministerio de Defensa ha armado su propia estrategia tomando como parte de su responsabilidad a todos los ataques que se realicen contra infraestructuras críticas. Sin embargo, como se mencionó en el caso chileno, los ataques cibernéticos a infraestructuras críticas pueden ser abordados desde diferentes áreas, de modo que un mismo ataque puede considerarse un tema netamente de Defensa o de Seguridad pública. Por lo tanto, es importante contar con un instrumento político que organice el accionar de cada institución, así como también las operaciones conjuntas.

La falta de concepciones compartidas acerca de infraestructuras críticas y amenazas que afectan al Ecuador es otra de las falencias que se hacen presentes en la estrategia ecuatoriana. El registro que se mantiene en lo referente a sistemas estratégicos es muy general, se estipulan todas las infraestructuras críticas del Estado, pero no se observa un análisis minucioso acerca de cuáles han sido los sistemas más atacados en el país. En relación a las ciberamenazas se evidencia el mismo inconveniente, se trata a todos los riesgos que se configuran en el ciberespacio de igual manera, sin darles prioridad a aquellos que afectan mayormente a los sistemas estratégicos nacionales. No todos los países son atacados por todas las ciberamenazas existentes, cada Estado cuenta con experiencias que le obligan a generar estrategias que se adapten a sus propias necesidades. El mantener una visión tan generalizada de la situación del país frente a las amenazas cibernéticas, limita las capacidades operativas y por ende cualquier respuesta, ya sea defensiva u ofensiva, será parcial.

Para poder llegar a este nivel de análisis se necesita de una academia fortalecida en este tipo de fenómenos globales. Desafortunadamente, el desarrollo de este aspecto en el Ecuador es mínimo. La oferta académica es escaza y los cursos que se ofertan en las instituciones académicas del país son de carácter técnico. A su vez, el sector de Defensa se mantiene cerrado a la sociedad civil. A pesar de que en la agenda de Defensa se estipule que se quiere romper con el pensamiento erróneo de que los asuntos de Defensa les competen solo a los militares, es algo que persiste en el inconsciente colectivo. La participación de académicos en la toma de decisiones en dicho ámbito es casi inexistente. De allí que las investigaciones sobre el tema de Ciberdefensa sean escazas, así como también el interés en desarrollarlas.

Existen países donde se ha promovido de mejor manera la investigación académica en esta era y que cuentan con capacidades y conocimientos importantes acerca del espacio cibernético, de los cuales Ecuador podría beneficiarse. Sin embargo, el Estado ecuatoriano cuenta con una minúscula cantidad de acuerdos internacionales de Defensa cibernética. Si bien el país ha participado activamente en iniciativas regionales, este no ha trabajado mayormente en establecer alianzas bilaterales. Ello supone una desventaja al momento de desarrollar capacidades, dado que al pertenecer a un organismo hasta cierto punto dependes de las aptitudes de los demás o de la fortaleza que alcancen en conjunto. En el instante en que la organización se desestabiliza, la seguridad de todos los países miembro, especialmente de los más débiles, también se desestabiliza.

6. Conclusiones

El Ecuador ha sido testigo de incidentes cibernéticos de gran alcance, los cuales le han llevado a constatar de primera mano lo peligrosos que pueden llegar a ser para la supervivencia del país. Este ha recibido ataques a empresas privadas y a instituciones públicas con consecuencias considerables. Las irrupciones al sistema financiero han representado pérdidas valoradas en millones de dólares. Las páginas web y los sistemas públicos también han sido interceptados, impidiendo su correcto funcionamiento. Han sido víctimas de espionaje cibernético y se ha filtrado información clasificada. Hechos que han llevado al Estado a percibir al ciberespacio como un dominio a ser considerado dentro de su Defensa. El considerar al ciberespacio como una dimensión más donde el Estado debe ejercer soberanía supone la creación de todo un aparato político que posibilite el cumplimiento de dicho objetivo y que determine una adaptación de la doctrina de Fuerzas Armadas. No obstante, el Estado ecuatoriano no cuenta con estas herramientas, simplemente se han generado ciertas

políticas que contribuyen con otros ámbitos de la Defensa. Lo cual, es alarmante considerando que se ha posicionado como uno de los países más ciberatacados en la región. La falta de una política pública ha formado un círculo vicioso entre la falta de seguimiento a las iniciativas que ya han sido emprendidas y la consecución de un instrumento político bien constituido. A partir del sistema de Defensa se plantea la creación de la política en cuestión, pero no se ha llegado a alcanzar esa meta debido a que el Ministerio ha manejado discrecionalmente el desarrollo de este instrumento que es de interés nacional. Por lo que, se podría decir que en realidad la estrategia ecuatoriana no es una estrategia estatal sino institucional, dando como resultado una estructura con vacíos considerables.

De allí que no se puedan cumplir con otros objetivos fundamentales al momento de conseguir una adaptación doctrinaria, como lo es el establecimiento de alianzas estratégicas y el desarrollo académico. Por esta razón no se puede asegurar que en el Ecuador se haya iniciado algún proceso en concreto para acoplar los principios rectores de la Defensa a las características cibernéticas. El plan de Ciberdefensa ecuatoriano se circunscribe a algunas iniciativas aisladas que no cuentan con una coordinación entre sí. Se podría llegar a pensar que estas son respuestas a ciertas coyunturas más que a una problemática constante.

Capítulo 4
Contrastación de estrategias

En el presente acápite se busca contrastar las estrategias de Ciberdefensa de Chile y Ecuador para comprender la asimetría que existe en la adaptación doctrinaria de Defensa en torno al espacio cibernético. Para poder lograrlo se hará el análisis de las variables que intervienen en este fenómeno. En primer lugar, se analizarán las políticas públicas que ha establecido cada país. Se observará si cuentan con una política específica para el área de Ciberdefensa o si carecen de ella. A través de ellas se puede visualizar si han existido cambios en los principios rectores de las Instituciones de Defensa en relación a la dimensión cibernéticas. En un segundo momento se estudiará las capacidades materiales de Defensa cibernética que tiene cada país, a partir de su infraestructura informática. En este punto se comparará la inversión que ha hecho cada país en software y hardware apropiado. La asignación de recursos en este ámbito da cuenta de la importancia que da el Estado a la lucha contra las ciberamenazas. Supone la ampliación de la agenda de Defensa hacia el ciberespacio debido a al alcance que tienen las amenazas cibernéticas.

Posteriormente se examinará el desarrollo académico que ha tenido cada Estado en el ámbito de la Ciberdefensa. Para ello se observará la oferta educativa que existe en esta área y las investigaciones que han surgido. Se comparará los programas académicos que existen en cada país ya sea en instituciones civiles o militares. Esto pondrá en evidencia el nivel de conocimiento que poseen estos países en relación al ciberespacio, sus características y los desafíos que representa.

Consecutivamente se presentará el indicador enfocado en los acuerdos internacionales. Aquí se cotejará la estrategia que ha mantenido a nivel internacional tanto Chile como Ecuador. Así mismo se verificará cuáles han sido sus prioridades en este sentido y bajo que parámetros han generado dichos acuerdos. En este punto se expondrá si estos países han trabajado ampliamente en establecer relaciones internacionales en el área en cuestión y se examinarán las diferencias existentes entre cada plan de acción.

Finalmente se presentará una tabla de verdad basada en CPOs, que son las variables antes mencionadas. Esto con el objetivo de examinar cuales son variables intervinientes necesarias y cuáles de ellas son suficientes. Los indicadores suficientes son los que determinan la

asimetría presente en los procesos de adaptación doctrinaria de Defensa entre ambos países. De esta manera se podrá analizar la relación causal que existe entre la variable suficiente y el fenómeno considerado en este estudio.

1. Políticas públicas de Ciberdefensa

Las políticas públicas son concebidas como decisiones y planificaciones instituidas por autoridades legítimas para poder solucionar fenómenos complejos que aquejan al país. De conformidad con la Secretaría Nacional de Planificación y desarrollo (SEMPLADES), son directrices generales que transparentan el deseo y la prioridad que le da el Gobierno a la modificación de un escenario adverso. En teoría, los principios rectores de un país deberían funcionar como una herramienta que ayude al Estado a garantizar los Derechos de los ciudadanos. En otras palabras, deben obedecer a las necesidades sociales de corto plazo buscando generar efectos a mediano y largo plazo (SEMPLADES 2011). En resumen, la política pública es "un curso de acción de la gestión pública que institucionaliza la intervención pública en respuesta a un problema social identificado como prioritario, y que se convierte de esta manera en materia de política de Estado" (SEMPLADES 2011, 10).

Dicho instrumento potencia la capacidad de gestión del Estado y surge como el resultado de una transformación frente a una necesidad, que en este caso es la protección de la integridad nacional en el espacio cibernético. Esto ocurre cuando el Estado busca encausar las capacidades gubernamentales, voluntades y conocimientos, para solventar alguna dificultad que no solamente es de interés estatal sino también social. Dichas políticas tienen la finalidad de alcanzar metas que preserven valores sociales e intereses estatales, y se las considera como una respuesta a amenazas que no han sido contempladas en la agenda vigente. Para poder obtener los resultados deseados estas deben contar con una planificación minuciosa y deberse a un objeto referente que se deba proteger (Molina 2016). En el ciberespacio los elementos referentes son las infraestructuras críticas.

El rol planificador del Estado es fundamental para que se puedan establecer los distintos niveles estructurales y las metas que se deberán alcanzar en cada uno de ellos, pero que a su vez deben estar articuladas entre sí. Como se describió anteriormente, estas metas tienen la finalidad de solucionar problemas a largo plazo (SEMPLADES 2011). Esto supone un proceso de transformación en relación a amenazas relativamente nuevas que poseen características diferentes a las tradicionales. La dimensión cibernética demanda un cambio en

las nociones y los conceptos básicos de la Defensa, una adaptación en la doctrina de Defensa. Lo cual significa que la responsabilidad de proteger la integridad territorial del Estado y procurar la soberanía del país, debe ser repensada y adaptada al campo digital. El fenómeno cibernético es constante y evolutivo, por lo que las iniciativas que se generen en torno al mismo deben ser pensadas a futuro y contar con cierta flexibilidad que les permita adecuarse a los desafíos que se vayan presentando. Es decir que, la política de Ciberdefensa debe constituirse como un proceso de adecuación constante debido a la gran cantidad de variables que contempla, pero sin perder de vista su objetivo primordial (Molina 2016).

Para que se pueda afirmar la existencia de una política pública de Ciberdefensa, deben existir los siguientes elementos en el proceso:

- Conjunto de medidas concretas
- Decisiones a la hora de asignar los recursos
- Marco general de acción
- Existencia de un público a quien afecta las decisiones y las acciones
- Normas y valores por los que se trabaja
- Debe responder a una idea de desarrollo: objetivos, estrategias y planes (Molina 2016, 69-70).

En el caso chileno, se puede observar el papel preponderante que ha tenido el Gobierno dentro de la planificación y estructuración de la política de Ciberdefensa, así como también en la asignación de recursos para el proyecto. Para el Gobierno chileno, es fundamental contar con un instrumento nacional de minimización de riesgos cuyos objetivos se centren en contrarrestar a las amenaza cibernéticas que puedan afectar a los sistemas sensibles del país. Es necesario establecer una herramienta estatal que describa las metas que deben conseguir gradualmente las instituciones de Defensa, y que coordine su accionar. Ello implica un seguimiento y una continuidad de los procesos.

La política en cuestión cuenta con los elementos que estipula Molina. Esta ha sido concebida como un conjunto de medidas concretas que versan específicamente sobre los desafíos que se les presenta en la red. Es un esquema que especifica las medidas que debe tomar el sector de la Defensa para que se pueda constituir un ambiente digital seguro y resiliente. Les da las pautas para poder resguardar aquellos datos que son de vital importancia para el país y que

benefician a su desarrollo. Coordina la Defensa de la soberanía del país a través de medios digitales (Ministerio de Defensa de Chile 2018).

Dicho esquema es un marco general de acción en base al cual se rige el trabajo interinstitucional. Contempla objetivos estratégicos a corto, mediano y largo plazo destinados a mitigar los riesgos que corre el país en el espacio cibernético. Es el instrumento que determina cuáles son los pasos a seguir en caso de un ataque cibernético y que regula el ejercicio de las competencias militares. A su vez orienta la doctrina de Fuerzas Armadas en lo referente a desarrollo de capacidades y a la generación de bienes y servicios informáticos que les permita mantener cierto nivel de independencia tecnológica (Ministerio de Defensa de Chile 2018).

La política de Ciberdefensa chilena tiene como objeto referente a las infraestructuras críticas y los intereses nacionales, que de ser afectados se pondría en riesgo la supervivencia del país y el estilo de vida de su sociedad. De modo que, responde a una idea de desarrollo mediante el establecimiento de estrategias que posibiliten la protección de sus sistemas fundamentales. No basta con establecer parámetros, sino que estos se deben hacer efectivos, y eso ya se ha podido evidenciar en el balance de gestión integral elaborado por el Ministerio de Defensa Nacional de Chile. En él, se transparenta el trabajo que se ha comenzado a hacer con respecto al desarrollo de capacidades principalmente. Inclusive ya se ha creado la doctrina de Ciberdefensa que compromete a todas las instituciones de Fuerzas Armadas.

En el caso ecuatoriano no existe una política pública concreta sobre Ciberdefensa, lo que se ha instituido en el país son políticas en torno al ciberespacio pero que se encuentran supeditadas a otras áreas de la Seguridad y Defensa. En el PNSI y la Agenda de Defensa únicamente se hace mención del desarrollo de capacidades, pero no se ha creado algún documento en el que se detalle el plan de acción que se debe seguir para lograrlo. En sí, lo que ha hecho el Estado ecuatoriano ha sido mencionar de manera esporádica al espacio cibernético y sus amenazas en sus planes y agendas.

Si bien el Ecuador cuenta con un Sistema de Ciberdefensa en el cual ya se contempla la creación de políticas públicas, este objetivo no ha sido precisado. A pesar de que se han asignado recursos a esta iniciativa, el Estado ecuatoriano no ha llevado un seguimiento sobre el cumplimiento de los proyectos que se establecieron en el sistema citado. Ha sido complejo

poder encontrar evidencias de un trabajo ininterrumpido en esta área por parte del Ministerio de Defensa o de Fuerzas Armadas, lo cual demuestra que la protección de la integridad estatal en Ecuador mantiene otro tipo de amenazas como su prioridad. De igual manera, no se ha podido evidenciar por parte del Gobierno algún pronunciamiento oficial acerca de la creación de instrumentos normativos que rijan la Ciberdefensa. Las iniciativas en esta área se han manejado a nivel ministerial e institucional.

2. Infraestructura informática

Para poder alcanzar una estructura fuerte y resiliente de Ciberdefensa es necesario contar con infraestructura informática adecuada. Esta se define como un conglomerado de software y hardware a través de los cuales se gestionan los servicios que ofrece una institución para solventar ciertas necesidades (Comunicaciones 2020). En este aspecto, tanto Chile como Ecuador han tomado medidas y han asignados recursos. De ello depende en gran medida la generación de capacidades de cada país ya que amplía el rango de acción de las instituciones de Defensa frente a las amenazas cibernéticas.

En Chile se creó el Comando Conjunto de Ciberdefensa, mismo que se responsabiliza de la planificación y ejecución de operaciones militares conjuntas. Dignidad que tiene un carácter operativo y que se ha constituido como el primer instrumento público que materializa el accionar del país contra posibles ataques (Aránguiz 2018). Es el encargado de realizar aquello que se estipula en la política pública de Ciberdefensa. Es el hilo conductor que mantiene la concordancia entre los principios rectores de la Defensa cibernética y los planes de acción. A partir de este organismo, Chile pretende generar TICs propias que doten de independencia y soberanía a sus sistemas estratégicos.

A su vez, el Gobierno chileno ha invertido en la creación de Centros de Respuesta a Incidentes Informáticos (CSIRT). Chile tiene un CSIRT nacional que recopila y sistematiza los datos provenientes de otros Centros. Articula el funcionamiento de los CSIRT sectoriales y coordina las respuestas técnicas de ellos mismos. Para podes reforzar la seguridad nacional, se creó un Centro de Respuesta específico de la Defensa (Gobierno de Chile 2017-2022). Su finalidad es coordinar a nivel técnico las decisiones de los CSIRT institucionales. Es decir que cada institución de Fuerzas Armadas tendrá su propio CSIRT encargado de evaluar riesgos, amenazas y vulnerabilidades del sistema de Defensa (Ministerio del Interior y Seguridad Pública 2018).

El país del Cono Sur ha demostrado la intención de establecer una infraestructura robusta de Ciberdefensa. En tal virtud, el Gobierno ha considerado la asignación de recursos para la adquisición de herramientas de monitoreo, prevención y respuesta de incidentes. De modo que, el Estado se ha esforzado por equipar de la mejor manera a sus instituciones para que estas puedan cumplir con las funciones asignadas sin mayores complicaciones. Una buena infraestructura agilita la consecución de las metas planteadas. Esta, al ser amplia, mejora el rendimiento de las instituciones o les ofrece esa posibilidad. Les permite aprovechar al máximo los recursos informáticos actuales e incrementa la velocidad de respuesta. En definitiva, Chile es consciente de la relevancia que adquiere una infraestructura informática fuerte al momento de proteger a las infraestructuras críticas del Estado (Ministerio de Defensa de Chile 2020).

Ecuador por su parte, también ha creado un Comando de Ciberdefensa, proyecto que fue capitalizado con 8 millones de dólares. Su misión es efectuar permanentemente operaciones de Defensa que posibiliten la protección de las infraestructuras críticas y la degradación de las TICs del adversario. Igualmente debe definir cuáles son los objetos referentes que deben ser resguardado y cuales las amenazas más relevantes. El análisis periódico contribuye a la generación de capacidades. De igual manera, debe gestionar los recursos materiales y humanos, de modo que el personal se mantenga debidamente capacitado (Ministerio de Defensa Nacional del Ecuador 2018).

El país andino cuenta con un Centro de Respuesta a Incidentes Informáticos, como órgano de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). Este coopera con otros equipos CSIRT tanto nacionales como internacionales. El Ministerio de Defensa tiene un CSIRT (CSIRT.EC 2020). Estos son los dos únicos centros que ha creado el Estado ecuatoriano, en materia de Ciberdefensa, para poder gestionar cualquier ataque que se genere en el país. Realidad que deja en entredicho el entendimiento que tiene el Estado ecuatoriano acerca de las afectaciones que pueden causar las ciberamenazas. Para que se pueda materializar una estrategia de Defensa cibernética, se debe contar con la infraestructura adecuada. Si no se posee este elemento, las operaciones institucionales se ven limitadas y la consecución de los objetivos nacionales se entorpece.

Si bien en el Ecuador se ha asignado recursos para la protección de información estratégica, esto no ha sido suficiente para establecer una infraestructura fuerte. Además, es importante

mencionar que el gasto público en el área de Ciberdefensa es continuo debido a la rápida evolución de las TICs; no basta con hacer una única inversión en un momento determinado. Si se quiere hacerle frente a las ciberamenazas la innovación de los recursos informáticos es fundamental. Sistemas y computadores obsoletos son sinónimo de vulnerabilidad e inseguridad. Al no estar actualizados no tiene las herramientas para poder neutralizar un ataque cibernético. Lamentablemente, en el caso ecuatoriano no se ha podido evidenciar mayores iniciativas para mejorar su infraestructura informática.

3. Desarrollo de conocimiento en materia de Ciberdefensa

Como se manifestó en acápites previos, el espacio cibernético se ha configurado como un fenómeno repleto de particularidades. Características que lo hacen diferente de los demás dominios del Estado. Su virtualidad ha hecho que los conceptos tradicionales de Defensa sean repensados. La soberanía deja de ser algo evidente que está determinado por fronteras rígidas y sólidas. Las delimitaciones entre el "territorio" de un Estado y otro son prácticamente ilusorias, por lo que la protección de la integridad del país se vuelve ambigua. Las especificidades del plano digital, también han generado actores no tradicionales en la relaciones internacionales y les ha dado poder. Les ha conferido habilidades que les permite articular ataques hacia países, mismos que poseen más capacidades materiales.

Esto ha llevado a los países a considerar que las ciberamenazas no son un problema que puede ser abordado de manera unilateral y con mecanismos tradicionales. Es necesario la institución de estrategias multidisciplinares u holísticas que contemplen diversos enfoques. De allí la importancia que adquiere la vinculación de la academia con los temas de Defensa. Desde este sector surgen investigaciones que contemplan diferentes perspectivas teóricas. Premisas que buscan explicar fenómenos complejos; problemáticas como el ciberespacio que presenta grandes desafíos a las teorías más clásicas.

Para poder alcanzar esta vinculación, que es una labor formidable para la gran mayoría de países, es necesario promover la creación de iniciativas académicas en torno a la Defensa Cibernética. Se debe romper con la exclusividad que han mantenido las Fuerzas Armadas en estas áreas e incentivar la incursión de la sociedad civil en estos temas. El conocimiento es básico para poder generar un cambio en la doctrina y este se adquiere a través de investigaciones. Si los académicos no se interesan en generar conocimientos de Ciberdefensa, el conocimiento en esta especialidad va a ser escaso. De igual manera, la capacitación del

personal militar en instituciones académicas abiertas a estudiantes civiles es importante. En este caso Fuerzas Armadas comienza a adquirir un pensamiento más crítico y a ponderar a la Defensa por fuera de la tradición castrense.

Cuando el Gobierno chileno llegó a concretar la política de Ciberdefensa, la oferta académica de especializaciones en esta área se incrementó. Igualmente, se puso en marcha la capacitación de los funcionarios públicos. Se organizaron iniciativas para impartir cursos de protección de infraestructuras críticas para poder establecer criterios compartidos que faciliten la implementación de las políticas. El personal militar ha culminado cursos de especialización y han asistido a seminarios y talleres internacionales abiertos al público en general.
Las instituciones académicas de las Fuerzas Armadas chilenas también han generado iniciativas académicas en torno a la Ciberdefensa. Ha propiciado conferencias donde se han efectuado análisis en torno a la problemática de Defensa en la red. Eventos donde se ha dimensionado los riesgos cibernéticos a nivel nacional y mundial, y se han explorado las estrategias de países hegemónicos. Por otro lado, la Academia Nacional de Estudios Políticos y Estratégicos de Chile (ANEPE) ha ofertado cursos de posgrado en materia de Defensa cibernética. Estos cursos fueron abiertos, por lo que académicos civiles que estaban interesados en el tema tuvieron la posibilidad de cursarlos.

En cuanto a las instituciones educativas privadas y públicas la oferta académica existe, pero es limitada. Por lo general se suelen crear mallas curriculares en torno a la Ciberseguridad más que en Ciberdefensa debido a una mayor demanda. A pesar de esto, algunas universidades privadas de Chile ofrecen cursos de postgrado específicos en esta línea. En otras universidades se han estructurado cursos de Ciberseguridad que contemplan la asignatura de Ciberdefensa.

En el caso ecuatoriano el desarrollo académico no tiene un panorama muy alentador ya que existe, pero es sumamente escaso. Se ha planteado la inclusión de la especialización en Ciberdefensa como parte de la formación del personal militar, pero esto no se ha materializado. La manera en la que estos funcionarios públicos han adquirido conocimientos ha sido a través de cursos de capacitación. En las instituciones educativas civiles la situación no varía, es complejo encontrar cursos de pregrado y postgrado especializados en este ámbito. Razón por la cual supone una ardua labor el obtener documentos que contengan estudios académicos sobre Ciberdefensa en el Ecuador y si se logra encontrarlos, por lo general suelen

ser técnicos. La mayoría de documentos pertenecen a autores militares y son muy pocos los académicos civiles que tratan estos asuntos. Es decir que, la vinculación entre la academia y las Fuerzas Armadas es precaria en el caso ecuatoriano, pero fundamental si se quiere generar un cambio en los principios de la Defensa. El desarrollo de conocimiento debería ser tomado como un factor primordial en el Ecuador para mejorar su estrategia de Ciberdefensa y así poder emprender un proceso de adaptación concreto.

4. Estrategia internacional

Los acuerdos internacionales pueden potenciar todos los indicadores previos en beneficio de la estrategia de Ciberdefensa. Mantener relaciones de cooperación con otros países es favorable debido a que se pueden obtener beneficios que por sí mismo el Estado no ha podido desarrollar. A través de ellos, se puede aprender de las experiencias que ha tenido el otro con respecto a las ciberamenazas y así reforzar ciertos aspectos que pueden haber sido desatendidos. También se fomenta las buenas relaciones con distintos países de modo que se minimiza el riesgo de ataque entre ambos. Se trata de establecer principios de cooperación que no se vayan en contra de los intereses nacionales de cada país.

Generalmente los acuerdos bilaterales contemplan el intercambio de información, de tecnología e inclusive intercambio académico. Esto incrementa las capacidades de los países para poder proteger sus sistemas estratégicos. Chile y Ecuador, debido a que son países consumidores de tecnología, se podrían favorecer grandemente de los acuerdos que firmen con otros países, si saben negociar correctamente. Existen países que tienen una amplia trayectoria en el tratamiento de ciberamenazas, y aunque la situación de los Estados no sea la misma, han establecido parámetros que pueden ser de utilidad para otras realidades.
El intercambio tecnológico es un factor claramente favorable para la infraestructura informática nacional. Poseer equipos de vanguardia que puedan gestionar rápidamente los requerimientos de los usuarios es una gran ventaja. Asimismo, poseer el conocimiento acerca del funcionamiento de este tipo de tecnología extranjera también es un plus. El intercambio académico impulsa el desarrollo investigativo he incentiva la creación de programas académicos especializados en Ciberdefensa. También, se mejora la capacitación del personal y se incrementa el trabajo calificado.

Para Chile, las relaciones internacionales son un pilar esencial para poder conseguir el tipo de estructura que persigue. Para el Gobierno chileno, el alcanzar un ciberespacio libre y seguro

no es una responsabilidad individual, es colectiva, pues se necesita del compromiso y las buenas prácticas de todos los actores internacionales para poder estar libres de amenazas. En este sentido, el país del Cono Sur ha procurado apoyar a los proyectos que promuevan una convivencia pacífica entre Estados y el establecimiento de marcos normativos internacionales que regulen el comportamiento de los países.

Pese a esta visión un tanto liberal, Chile no ha dejado de priorizar su supervivencia, razón por la cual también se ha mostrado ampliamente interesado en firmar acuerdos bilaterales de cooperación. Mismos que pueden ser considerados alianzas estratégicas, las cuales le pueden habilitar al Estado chileno para desarrollar mayores capacidades y posicionarse como un referente a nivel regional. El número considerable de acuerdos que tiene firmados con otros países amplía sus posibilidades para blindarse frente a ciberataques y poder generar respuestas. El Estado chileno ha sido enfático al mostrar su postura frente a cualquier agresión cibernética que reciba. Considera que las amenazas cibernéticas pueden generar afectaciones graves como la de armamento de guerra, de modo que cualquier irrupción en sus sistemas estratégicos será gestionada en este sentido. Esto significa que Chile no solamente quiere ser capaz de neutralizar una amenaza sino también de generar una respuesta que lesione o dañe los sistemas del agresor.

Chile ha firmado mayormente acuerdos con países sudamericanos en términos de intercambio de información, capacitación conjunta e innovación. En el Cono Sur mantiene relaciones de cooperación en Ciberdefensa con todos los países ubicados en esta zona. Con Argentina los acuerdos se han basado en la creación de un grupo binacional. Dicha entidad tiene la finalidad de articular estrategias conjuntas para poder darle tratamiento a esta problemática. Asimismo, han firmado tratados en este ámbito con Brasil, país que históricamente ha ambicionado el status de país hegemónico, no solo a nivel regional sino también mundial. Con el gigante sudamericano, a más del intercambio de información, capacitación profesional y la realización de investigaciones científicas, se ha consensuado una coordinación entre ambos países en el caso de sufrir un ataque. De igual manera el Ministerio de Defensa de Chile mantiene convenios con Paraguay y Uruguay.

En la Zona Andina, el Gobierno chileno ha establecido relaciones de cooperación con Colombia, Ecuador y Perú. Con los tres países ha promovido la creación de mecanismos de transparencia en el plano digital. También, se ha acordado el trabajo conjunto y el apoyo

dentro de organizaciones internacionales. Igualmente, en dichos acuerdos se ha contemplado el intercambio de información, el intercambio académico, el entrenamiento militar y la creación de protocolos de Ciberdefensa.

Dentro de América del Norte ha establecido convenios con Canadá, Estados Unidos y México. De estos tres, el acuerdo que ya ha generado resultados concretos es el de Estados Unidos, país hegemónico que tiene una larga trayectoria en la Defensa contra las ciberamenazas. Los parámetros de cooperación entre estos Estados se basan en intercambios tecnológicos, ejercicios conjuntos y capacitación de sus profesionales. Dado que el Gobierno estadounidense destina gran cantidad de recursos a su Defensa, incluyendo la Ciberdefensa, las alianzas que se puedan generar con el mismo pueden ser muy beneficiosas. Sin entrar en la discusión de las ganancias relativas, poder acceder al conocimiento que ha desarrollado Estados Unidos a nivel cibernético, es una ventaja importante.

En la forma como Chile ha configurado sus relaciones internacionales en torno al ciberespacio se transparenta el deseo de cubrir la mayor cantidad de flancos. Tiene cubierto la mayoría de América del Sur y toda América del Norte, inclusive cuenta con un acuerdo con un país europeo, concretamente Inglaterra. Para el Gobierno chileno, el cerrar acuerdos bilaterales y multilaterales es una política de Estado. Es decir que, sin importar que exista un cambio de Gobierno, se debe continuar con este objetivo.

La estrategia ecuatoriana por otro lado hace énfasis en la integración regional para poder unificar esfuerzos y así enfrentar a los desafíos cibernéticos. En este sentido, el Estado ecuatoriano ha participado activamente en las iniciativas de la UNASUR y ha sido uno de los miembros más entusiasta al momento de proponer proyectos comunes en relación a la Defensa cibernética. Para Ecuador lo que se requiere para mantenerse fuerte al recibir un ciberataque es alcanzar un blindaje como región; por separado las respuestas son limitadas y los esfuerzos insuficientes. Por ello, el país ha priorizado su participación en acuerdos multilaterales.

No obstante, Ecuador también ha firmado tratados con países por fuera de América del Sur y organizaciones distintas a la UNASUR. El Ministerio de Defensa ha cerrado acuerdos de Defensa con Estados Unidos que, si bien no han sido específicos en el área cibernética, pueden dar paso a que se coopere en este ámbito. Igualmente, el país ha firmado un acuerdo

de Ciberdefensa con Chile que incluyen, intercambio académico, coordinación entre Comandos Conjuntos e intercambio de experiencias. Asimismo, ha puesto los ojos sobre la estrategia de Ciberdefensa brasileña; el concretar un acuerdo de cooperación con el país carioca es una meta importante para incrementar las capacidades ecuatorianas. En lo que respecta a organizaciones internacionales, la firma del TLC con la Unión Europea, ha sido beneficiosa para la Defensa ecuatoriana ya que posibilita el acceso a tecnología informática.

5. Procesamiento de hallazgos a partir del análisis documental

CPOs	Chile	Ecuador
Política de Ciberdefensa	1	0
Infraestructura informática	1	1
Desarrollo de conocimiento en materia de Ciberdefensa	1	1
Estrategia Internacional	1	1

A través de la presente tabla se puede observar cuales han sido variables suficientes y cuales necesarias dentro de la asimetría, que se ha podido evidenciar a lo largo de la investigación, entre los procesos de adaptación doctrinaria de Chile y Ecuador. La codificación que se ha utilizado se basa en 1 y 0 donde uno significa que se cuenta con la variable y cero significa que carece de la misma. Para que uno de los parámetros sea considerado necesario debe tener 1 en ambos casos, para que sea considerado suficiente debe tener 1 0.

En base a la explicación previa, se puede observar que la infraestructura informática es una variable interviniente necesaria pero no suficiente. Tanto Chile como Ecuador han desarrollado una infraestructura en torno a la Ciberdefensa. Ambos países han asignado fondos a la configuración de instalaciones que cuentan con equipamiento especializado. Los dos han instituido Comandos de Ciberdefensa que suponen la creación de departamentos adecuadamente equipados para poder gestionar todas las operaciones de Fuerzas Armadas en el ciberespacio. Sus Ministerios de Defensa han invertido parte de su presupuesto a la adquisición de software y hardware que le permita al personal poner en práctica los conocimientos adquiridos y neutralizar cualquier ciberataque o en su defecto tratar de que cause el menor daño posible. En resumen, Chile y Ecuador han adquirido computadores y sistemas informáticos para proteger los intereses nacionales en la plataforma cibernética.

Los acuerdos internacionales también se constituyen como una variable interviniente necesaria. Para el Estado chileno y para el Estado ecuatoriano el establecer tratados con otros países en materia de Ciberdefensa, es importante, aunque mantengan enfoques diferentes. En el caso chileno, los acuerdos bilaterales son los que tiene cierto protagonismo en su estrategia. Chile es un país que mantiene una participación constante en las iniciativas multilaterales pero su prioridad son los acuerdos que pueda establecer con otros países individualmente. De allí que cuente con tantos acuerdos de este tipo, los cuales le otorgan ventajas sobre otros países a nivel regional y mundial. Ecuador, a diferencia de Chile que prioriza la generación de alianzas estratégicas bilaterales, apuesta por los acuerdos multilaterales. Ha sido un país que promueve activamente las iniciativas regionales de Ciberdefensa. De lo que se ha podido encontrar por medios oficiales, el Ministerio de Defensa ha cerrado solamente con Chile un acuerdo específico en cooperación de Defensa en la red. Por lo demás, todos sus esfuerzos han sido enfocados en el apoyo a organismos como la UNASUR. Durante el periodo que se estipula en la presente investigación, el Gobierno ecuatoriano enfocó su energía y recursos en iniciativas regionales.

De igual manera, el desarrollo académico se manifiesta como una variable interviniente necesaria ya que en los dos países existen programas académicos especializados en Ciberdefensa, así como también investigaciones en el tema. Cabe mencionar que este indicador no da cuenta del nivel de desarrollo académico de cada país, es decir que no supone un amplio desarrollo académico en el país del Cono Sur y un bajo desarrollo en el país andino. La realidad es que en Chile se han generado iniciativas de capacitación para tener trabajo calificado y se han ofertado algunos cursos de postgrado en Ciberdefensa, pero no se ha podido evidenciar mucho más allá de eso. La situación ecuatoriana es aún más deficiente pero no dista mucho de la realidad chilena. Lo que se quiere expresar es que en este parámetro no se ha visto una diferencia amplia o muy marcada. De allí que el acceso a documentos académicos que analicen la estrategia de Ciberdefensa de cada país fue un reto. Son muy pocos los académicos que han tomado este desafío y han desarrollado investigaciones sobre el tema. Esto da cuenta de la reactividad con la que funcionan las estrategias cibernéticas en ambos países. Al no desarrollarse estudios sobre Ciberdefensa se genera un retraso en el conocimiento con respecto a las ciberamenazas que van a una velocidad distinta. Pese a ser una temática que ha ganado protagonismo falta incentivar el interés de la sociedad civil en esta área, así como también promover la incursión del personal militar en ambientes académicos.

En el CPO referente a la Política de Ciberdefensa sí se visibilizó una amplia diferencia que lo convierte es una variable interviniente suficiente, pues Chile ha desarrollado una política de Ciberdefensa mientras que Ecuador no lo ha hecho. El Gobierno chileno partió de la creación un instrumento político en su estrategia de Defensa cibernética. Herramienta que da inicio a su proceso de adaptación doctrinaria y que permite que este sea llevado a cabo de manera más organizada y efectiva. Esto guarda una coherencia con la importancia que ha adquirido el ciberespacio para Chile y el comprometimiento de su Gobierno en cubrir las necesidades que se han generado en torno al mismo. A partir de esta política nacen todos los objetivos de la Ciberdefensa y se comienzan a desarrollar los demás indicadores citados en la tabla de verdad, los cuales también dan cuenta de la adaptación dogmática que ha comenzado en el país.

En contraposición se encuentra el Ecuador, donde ya se han tomado acciones frente a las ciberamenazas sin haber estructurado una política en concreto; sin contar con un plan de acción que dirija toda la estrategia de Ciberdefensa. En el caso ecuatoriano no se evidencia un pronunciamiento claro por parte del Gobierno con respecto a esta problemática. Las iniciativas que se han llevado a cabo han surgido desde el Ministerio de Defensa directamente. Por este motivo, la estrategia del Estado ecuatoriano es un tanto difusa y se basa en procesos aislados que guardan una relación mínima. Es así que, por un lado, se encuentra el Sistema de Ciberdefensa que juega una suerte de esquema rector y establece funciones y objetivos, y por otro lado los proyectos que han sido realizados. En dicho sistema se plantea la necesidad de construir una política de Defensa cibernética, pero en su lugar se han creado un par de políticas en la agenda Defensa y cuatro años después se procede a actualizar el libro de Defensa, antes que concretar el objetivo que se planteó en primer lugar; dando como resultado que en Ecuador la adaptación doctrinaria en torno al ciberespacio sea apenas un plan.

6. Conclusiones

En conclusión, en cada parámetro que se ha presentado en este acápite, se han podido observar ciertas diferencias entre un caso y otro, unas más amplias que otras. Chile y Ecuador a pesar de tener concepciones similares con respecto al ciberespacio, han emprendido sus estrategias de formas diferentes. Esto demuestra que, aunque ambos países compartan ciertos principios dogmáticos, sus procesos de adaptación no han sido idénticos, generándose una asimetría entre ambos. Los países tienden a dar prioridad a ciertos aspectos más que a otros y en base a ello se va tejiendo la planificación estatal.

En el primer parámetro, el Gobierno chileno ha mostrado su interés en generar un cambio para poder suplir las necesidades de contrarrestar a las amenazas cibernéticas, mientras que en el caso ecuatoriano no ha existido un pronunciamiento por parte del Gobierno, de modo que no cuenta con una política específica. Del segundo parámetro se puede concluir que ambos países han adquirido equipamiento para poder dotar de las herramientas necesarias a su personal y así puedan desempeñar su labor de manera satisfactoria. En este punto no se ha precisado quien cuenta con más o menos capacidades materiales en este ámbito. En la tercera variable la diferenciación entre la situación de cada Estado no ha sido concluyente. El desarrollo académico de ambos países se encuentra en un nivel muy básico. Si bien en el Ecuador la oferta académica es prácticamente nula y las investigaciones escazas, Chile no está muy alejado de esta realidad. En Chile se pudo encontrar un par de cursos de especialización en Defensa cibernética y las investigaciones académicas sobre el tema son limitadas. En ambos casos se puede encontrar más estudios centrados en Ciberseguridad. Del cuarto parámetro se llega a la conclusión de que, pese a que ambos países hayan trabajado en sus relaciones internacionales para mejorar sus capacidades, Chile ha puesto un mayor énfasis en los acuerdos bilaterales, mientras que Ecuador ha apostado por los acuerdos multilaterales.

De todas estas variables existe una que es suficiente, aquella que se refiere a la política pública. La disparidad en este aspecto es clara y concisa. Chile cuenta con una política de Ciberdefensa y el Ecuador no, de modo que es el factor determinante del fenómeno que comprende el presente trabajo. Chile no solo que ha estructurado una política de Ciberdefensa, sino que a partir de ella ya ha creado la doctrina de Ciberdefensa que contempla los principios rectores que presiden el accionar de Fuerzas Armadas en la red. En Ecuador no se ha llegado a visualizar tantos avances en su proceso de adaptación debido a la falta de un instrumento político que priorice esta necesidad. La creación de un marco político en torno a un problema le da prioridad a su tratamiento, por lo que se generan iniciativas concretas que contribuyan a darle solución. Al no contar con esta herramienta, apenas y se puede hablar de que Ecuador haya emprendido una adaptación en su sistema de Defensa.

Conclusiones y recomendaciones generales

Generar un ajuste dogmático de la Defensa en torno a un fenómeno complejo como es el ciberespacio representa retos categóricos para todos los Estados, incluyendo Chile y Ecuador. Las características particulares de este entorno generan amenazas que requieren de un tratamiento distinto al que se ha manejado históricamente con las amenazas convencionales. El repensar los principios doctrinarios que han regido la protección de la soberanía de un país en función de una dimensión donde los alcances y las limitaciones de los actores internacionales no son claros ni concisos, es un reto. La integridad territorial se vuelve abstracta y el objeto referente de la Defensa se amplía exponencialmente.

Al existir un aumento en el rango de acción de Fuerzas Armadas, este puede llegar chocar con las competencias de otras instituciones de Seguridad. De modo que, el rol de la Seguridad Pública y el de la Defensa no son fácilmente identificables. El alcance de las amenazas no convencionales permite que estas generen afectaciones tanto a la integridad del país como a su sociedad, razón por la cual es difícil poder determinar qué amenazas cibernéticas corresponde al ámbito puramente militar y cuáles a la esfera policial. La gran mayoría de los ciberataques que afectan a las infraestructuras críticas de un Estado generan afectaciones a los ciudadanos. Asimismo, el costo de la reparación de los daños suele recaer en los usuarios de estos sistemas.

No obstante, generar una aproximación hacia los desafíos cibernéticos es fundamental para procurar la supervivencia del Estado, toda vez que sus infraestructuras críticas dependen en gran medida de esta dimensión. Países como Chile y Ecuador han optado por adoptar software que mejoren los sistemas públicos, que reduzcan el costo de operación y que les permita a los beneficiarios realizar ciertos trámites de manera rápida y efectiva. Los servicios en línea se han incrementado exponencialmente y la estabilidad del Estado se encuentra ligada al correcto funcionamiento de los mismos. Cualquier ataque a estas estructuras informáticas desafían a la conservación del país.

En este sentido, la segurización se vuelve relevante, pues es lo que se busca alcanzar al momento de generar ciertos cambios en la Defensa Nacional e incluir amenazas no convencionales dentro de sus competencias. Esto significa la ampliación de la agenda, pero para poder alcanzarlo es necesario convencer a la sociedad de que estas amenazas son potencialmente destructivas y por ende requieren de la asignación de recursos estatales. El

factor discursivo es fundamental al momento de instituir una transformación en un área de vital importancia para el Estado. Persuadir a las masas no solamente facilita la transición, sino que también contribuye a la sensibilización de la población frente a los riesgos digitales. Una vez comprendida la gravedad de la amenaza, lo que lleva a cabo como parte del proceso de segurización, es generar herramientas políticas en las que se determine las concepciones básicas que caracterizan al fenómeno y que es lo que se debe hacer para mitigarlo. Dichos instrumentos materializan al discurso y muestran el compromiso que tiene el Gobierno para poder solucionar este problema. Es decir que, para poder generar una transformación real alrededor de una temática en específico, es necesario establecer políticas públicas que den cuenta de las intenciones gubernamentales y que dirijan toda la estrategia estatal. De allí que se considere que la segurización es una versión más extrema de la politización.

El problema que comprende a al presente trabajo versa sobre la asimetría existente en este proceso entre el Estado chileno y el Estado ecuatoriano. Al hacer la comparación entre ambos países se pudo evidenciar que Chile tiene mayores capacidades que Ecuador en términos de Ciberdefensa lo cual se encuentra íntimamente ligado a una adaptación doctrinaria mucho más desarrollada. En el caso chileno se observó una estrategia más madura que ya ha arrojado resultados positivos para poder alcanzar los objetivos nacionales. Como parte de dichos logros ostenta la "Doctrina Conjunta de Ciberdefensa" en la cual se delinean los principios de aplicación de operaciones de Ciberdefensa.

A través del procesamiento de datos se concluyó que el factor determinante para que exista tal desigualdad entre estos países es la política de Ciberdefensa. Chile ha desarrollado una política de Defensa cibernética, misma que fue requerida y considerada por el Gobierno como una prioridad para alcanzar los intereses nacionales. A través de distintos decretos, la presidencia expuso la importancia que ha adquirido el ciberespacio para el adecuado funcionamiento del Estado y por ende como la protección del país en esta dimensión se ha vuelto una necesidad. De modo que, la generación de instrumentos políticos específicos en relación a esta dimensión se planteó como algo indispensable para poder alcanzar los objetivos nacionales. Mediante esta iniciativa, el Gobierno chileno ha mostrado su compromiso con el proceso de adaptación doctrinaria en torno al ciberespacio para así solventar las necesidades del país en este entorno.

La política pública de Ciberdefensa de Chile ha jugado una suerte de columna vertebral dentro de su estrategia. A través de ella se han establecido los objetivos que persigue el país en el ciberespacio, las instituciones encargadas de su defensa, las funciones que deberá cumplir cada una de ellas y los pilares que se tendrán que desarrollar para crear una estructura fuerte y resiliente. Eso ha ayudado a que la estrategia chilena sea organizada y a que los proyectos llevados a cabo por las instituciones de Defensa sean coordinados y consecuentes con los intereses estatales. De igual manera, determina el curso de acción que seguirá la Defensa para poder contrarrestar a los ataques cibernéticos y articula el trabajo conjunto de Fuerzas Armadas. Dicho plan de acción con tribuye con el desarrollo del país y puede llegar a mejorar la calidad de vida de la población chilena ya que procuran un espacio cibernético libre y seguro.

El Estado chileno, a través de la política de Defensa cibernética, ha posicionado a la protección del país en el ciberespacio como un campo que debe seguir desarrollándose independientemente de la ideología política que caracterice a los Gobiernos venideros. Es decir que la actualización y el perfeccionamiento de los principios doctrinarios de Ciberdefensa se han convertido en una política de Estado. Ello pone en evidencia que los objetivos que se ha planteado Chile tienen la finalidad de suplir una necesidad a largo plazo; y esto es lo que requiere un fenómeno que se encuentra en constante transformación. En otras palabras, la planificación que se ha llevado a cabo en Chile se basa en un análisis no únicamente de los incidentes que ya han ocurrido en el país sino en el análisis de posibles ataques que le podrían afectar.

No obstante, la estrategia chilena no es perfecta, tiene debilidades como se vio en su momento. Al tener una política de Ciberseguridad que involucra a varias entidades del Estado corre el riesgo de que las funciones de la Defensa se superpongan con las funciones de otros sectores públicos. De igual manera existen áreas como la academia, fundamentales para su proceso de adaptación doctrinaria, que necesitan ser trabajadas a profundidad para que se pueda generar un mayor conocimiento sobre el ciberespacio y sus propiedades. Empero, a pesar de estos vacíos la estrategia del Estado chileno ha cuenta con bases consistentes y con el potencial para poder alcanzar un sistema de Ciberdefensa fuerte.

El Ecuador en contraposición, no cuenta con una política de Ciberdefensa, pese a ser uno de los países en Latinoamérica que más ha implementado servicios públicos en línea. Al no

contar con un instrumento político específico que dirija su estrategia cibernética, solamente ha podido generar iniciativas aisladas como parte de su planificación. Los avances que ha tenido el país en términos de Defensa cibernética no han generado los resultados esperados y en consecuencia no han generado una adaptación real. Ni siquiera se puede hablar de una verdadera ampliación de la agenda en vista de que todo lo que se ha hecho es introducir el termino de Ciberdefensa o ciberespacio, de manera esporádica, en otros instrumentos públicos de cara a la Defensa. No se ha dimensionado las afectaciones que pueden tener las ciberamenazas y como pueden poner en riesgo la supervivencia del Estado.

El Gobierno de este país, a diferencia del Gobierno chileno, no se ha pronunciado en cuento a la dependencia que presenta el país con respecto al ciberespacio y a la magnitud que puede llegar a tener un ataque cibernético, no solo para el Estado sino también para la sociedad. La entidad que ha tomado el liderazgo en este aspecto ha sido el Ministerio de Defensa; institución que ha generado proyectos a discreción, mismos que carecen de organización y coordinación entre sí. Esto incurre en una falta de liderazgo político, motivo por el cual no ha habido una apropiada socialización de la concepción estatal del ciberespacio y de los objetivos que persigue en este entorno. Esto significa que la población ecuatoriana no ha asimilado la gravedad de los ciberataques y los costos que estos representan para el país. De tal forma que no se ha llegado a comprender la importancia de generar toda una planificación en relación a estos desafíos no convencionales. Es así que hasta la actualidad tal planificación política no se ha llevado a cabo.

En Ecuador la falta de una política de Defensa cibernética incide en la carencia de continuidad en su proceso de adaptación doctrinaria, inclusive se podría llegar a asegurar que tal ajuste ni siquiera ha iniciado. Las acciones que ha tomado este país desde el 2014 han sido manejadas sin un orden claro. Esto deja en evidencia que el Ecuador ha actuado, no en función de los riesgos cibernéticos que se le presentan sino en base a coyunturas para poder resolver una problemática del momento. Razón por la cual, a pesar de que se puso como horizonte al 2022 para que sus instituciones cuenten con las capacidades para generar respuestas a los ciberataques es evidente que va a ser sumamente complejo que esto se vuelva una realidad. La adaptación doctrinaria no es algo que se pueda alcanzar en el corto plazo, se necesita de un trabajo constante y de largo aliento. En el caso de contar con bases sólidas este se irá desarrollando dentro de los tiempos esperados, pero si no es así no se puede poner ningún tipo

de plazo. Este podría extenderse indefinidamente sin generarse ningún tipo de avance en concreto y propicia la subutilización tanto de recursos humanos como de recursos materiales.

Los proyectos que ha generado el MIDENA hasta el momento no representan un ajuste propiamente dicho, en función de los riesgos cibernéticos. Han sido proyectos que únicamente demuestran la ligereza con la que se ha analizado esta problemática global de vital importancia para la subsistencia del país. Ecuador debe comprender que una política pública no es un fin sino un medio. Son las bases por donde se va a erguir toda una estrategia con miras a solucionar un fenómeno de interés nacional. Por lo que no es adecuado generar proyectos en Ciberdefensa sin establecer una política. De allí que en el caso chileno ya se haya podido observar resultados concretos, derivados de sus proyectos, mientras que en el caso ecuatoriano esto no ha sido posible.

Lo más recomendable para el Estado Ecuatoriano es la constitución de un instrumento político que se traduzca en bases sólidas para su estrategia. Una estructura en la cual se establezcan políticas públicas que posicionen a la ciberdefensa como un interés nacional que debe ser procurado por cualquier gobierno, sin importar su sesgo ideológico. Esto supone la institucionalidad de la Ciberdefensa ecuatoriana. A su vez supone un ordenamiento y una articulación entre las acciones de las instituciones de Defensa. Es decir que se reduce la discrecionalidad de dichas entidades. Lo cual se traduce en soluciones a corto, mediano y largo plazo, para una problemática de carácter global.

Asimismo, los proyectos que ya han sido desarrollados por parte del MIDENA, deben ser modificados en función del instrumentó político antes citado. Esto garantizaría la continuidad de las iniciativas tomadas en este ámbito. Con ello también se lograría profundizar en el análisis de las herramientas con las que ya cuenta el Estado ecuatoriano y poder solventar todas sus falencias. Estas dejarían de responder simplemente a coyunturas y ofrecerían recursos para resolver problemas inmediatos y futuros.

Finalmente es preciso mencionar que es fundamental para Chile y Ecuador, así como también para los demás países latinoamericanos, estrechar lazos entre la academia y los tomadores de decisiones, toda vez que se podría desarrollar una visión holística sobre este fenómeno. Las características que presentan las ciberamenazas requieren de una visión mucho más amplia de la Defensa, en la cual, a más de tomarse en cuenta a las estrategias tradicionales, se planteen

opciones no convencionales que se adapten a este tipo de riesgos. En este aspecto, los investigadores civiles pueden generar valiosos aportes.

Listado de Abreviaciones

ANEPE	Academia Nacional de Estudios Políticos y Estratégicos
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones
COCIBER	Comando de Ciberdefensa
COMACO	Comando Conjunto de las Fuerzas Armadas
COTICDE	Comité de Tecnologías de la Información y Comunicación de la Defensa
CPO	Causal Process Observations
CSIRT	Centros de Respuesta a Incidentes Informáticos
DID	Dirección de Inteligencia de Defensa
ISSFA	Instituto de Seguridad Social de las Fuerzas Armadas
MIDENA	Ministerio de Defensa Nacional
NCSI	National Cyber Security Index
NIST	Instituto Nacional de Estándares y Tecnología
OEA	Organización de Estados Americanos
OTAN	Organización del Tratado del Atlántico Norte
PNSI	Plan Nacional de Seguridad Integral
SEMPLADES	Secretaría Nacional de Planificación y desarrollo
TICs	Tecnologías de la Información y la Comunicación
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
UNASUR	Unión de Naciones Suramericanas
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

Lista de referencias

ACAGUE. 2019. “ACAGUE realizó conferencia sobre Ciberdefensa”, https://www.acague.cl/acague/acague-realizo-conferencia-sobre-ciberdefensa/

Adler, Emanuel. 1997. “Seizing the Middle Ground: Constructivism in World Politics” *Revista europea de Relaciones Internacionales*. 3: 319- 363

Amazon Web Services. 2019. “Marco de seguridad cibernética NIST (CSF, por sus siglas en inglés)”, https://d1.awsstatic.com/whitepapers/es_ES/compliance/NIST_Cybersecurity_Framework_CSF.pdf

Amigo Tossi, Alejandro. 2015. “Consideraciones sobre la ciberamenaza a la Seguridad Nacional”. *Revista Política y Estrategia* 125: 83-96.

Antoine, Bouvereyt. 2018. “Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment”, https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924

Aviles, Edgar. 2018. "Contribuciones contemporáneas de metodologías cualitativas para el análisis de políticas públicas: Process Tracing y Qualitative Comparative Analysis." *Revista de Sociologia e Política* 26 (67): 21-37.

Baller Silja, Soumitra Dutta y Bruno Lanvin. 2016. *The Global Information Technology Report*. Ginebra: Johnson Cornell University.

Banco Interamericano de Desarrollo. 2016. “Cybersecurity: Are We Ready in Latin America and the Caribbean?”. https://publications.iadb.org/handle/11319/7449?locale-attribute=es&.

Barrios, Verónica. 2018. “Política Nacional de Ciberseguridad: 2017-2022”, https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf

Bartolomé, Mariano. “Las Fuerzas Armadas sudamericanas y las perspectivas de cooperación en la lucha contra el terrorismo y el crimen organizado”. *Revista Estudios Internacionales* 164 (2009): 7-30.

Battaleme, Juan. 2013. “Los estudios de seguridad internacional: de los enfoques racionalistas a los críticos”. En *Relaciones Internacionales: teorías y debates*, editado por Elsa Llenderrozas, 133 - 165. Buenos Aires: Editorial Universitaria de Buenos Aires.

Beach, Derek, y Rasmus Brun. 2013. *Process- Tracing Methods.* Michigan: The University of Michigan Press.

Beck, Nathaniel. 2010. "Causal Process ''Observation'': Oxymoron or Fine Old Wine". *Revista Political Analysis* 18: 499-505.

Biblioteca del Congreso Nacional de Chile. 2015. "Decreto 533", https://www.leychile.cl/Navegar?idNorma=1079608&idParte=

Bravo, Diego. 2015. "Ecuador se muestra vulnerable a ciberataques". *El Comercio*, 26 de julio. https://www.elcomercio.com/actualidad/ecuador-muestra-vulnerable-ciberataques.html

Buzan Barry, Charles Jones y Richard Little. 1993. *The Logic of Anarchy: Neorealism to Structural Realism*. Nueva York: Columbia University Press.

Buzan, Barry, Charles Jones y Richard Little. 1993. *The Logic of Anarchy: Neorealism to Structural Realism*. Nueva York: Columbia University Press.

Buzan, Barry, Ole Waever, y Jaap de Wilde. 1998. *Security. A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, Inc.

Buzan, Barry, y Lene Hansen. 2009. *The Evolution of Internacional Security Scudies*. Cambridge: Cambridge University Press.

Buzan, Barry. 1983. *People, State and Fear. The National Security Problem in International Relations*. Brighton: Whealsheaf Books.

Cabrera, Lester. 2017. "Reflexiones en torno a los conceptos de nuevas amenazas, amenazas emergentes y amenazas no tradicionales". *Revista Escenarios Actuales* 01: 17- 26.

Catota Frankie, Granger Morgan y Douglas C Sicker. 2019. "Cybersecurity education in a developing nation: the Ecuadorian environment". *Revista Journal of Cybersecurity* 5: 1-19.

CEEAG, Centro de Estudios Estratégicos. 2018. *La ciberguerra: sus impactos y desafíos*. Chile: Andros Impresores.

CEEAG. 2018. "Planificación militar, ciberdefensa e inteligencia", http://www.ceeag.cl/wp-content/uploads/2019/03/CUADERNO-DE-DIFUSION-42.pdf

Ciberseguridad. 2019. "Gobiernos de Chile y Colombia Firman Acuerdo Bilateral de Ciberseguridad", https://www.ciberseguridad.gob.cl/noticias/gobiernos-de-chile-y-colombia-firman-acuerdo-bilateral-de-ciberseguridad/

Colarik, Andrew y Lech Janczewski. 2012. "Establishing Cyber Warfare Doctrine". Revista *Journal of Strategic Security* 5: 31-48.

Collins, Alan. 2013. *Contemporary Security Studies*. Oxford: OXFORD University Press.

Comunicaciones. 2020. “Cómo aumentar el rendimiento de tu infraestructura informática”, http://rcg-comunicaciones.com/rendimiento-infraestructura-informatica/#:~:text=Llamamos%20infraestructura%20inform%C3%A1tica%20al%20conjunto,cooperaci%C3%B3n%20con%20proveedores%20y%20clientes.

Creswell, John.2014. *Research design*. California: Sage.

CSIRT. 2019. “Memorándum de entendimiento sobre cooperación de ciberseguridad, ciberdelito y ciberdefensa entre la República de Chile y la República Argentina”, ttps://www.csirt.gob.cl/media/2019/07/MOU-CHILE-ARGENTINA.pdf

CSIRT.EC. 2020. “Listado CSIRT EC”, https://csirt.ec/csirts-en-ecuador/listados/

Deloitte. 2018. “Ciberseguridad. Encuesta 2018 sobre Tendencias de Cyber Riesgos y Seguridad de la Información en Ecuador”, https://www2.deloitte.com/ec/es/pages/risk/articles/cyber-risk-2018.html

Diario Estrategia. 2019. “Delitos informáticos aumentan en Chile en un 74%”. *Diario Estrategia,* 09 de agosto. http://www.diarioestrategia.cl/texto-diario/mostrar/1499774/delitos-informaticos-aumentan-chile-74

Díaz, Laura, Uri Torruco, Mildred Martínez, y Margarita Varela. 2013. “La entrevista, recurso flexible y dinámico”. *Revista Investigación en educación médica* 2 (2013): 162 -167.

Dipres. 2019. “Balance de Gestión Integral año 2018”, http://www.dipres.gob.cl/597/articles-188333_doc_pdf.pdf

Doctor Ortiz, Javier Ulises y Doctora Claudia Fonseca 2017. "La Defensa Cibernética. Alcances estratégicos, proyecciones doctrinarias”, http://cefadigital.edu.ar/bitstream/1847939/1088/1/La%20defensa%20cibernetica_TI%20LRRII%202017_Ortiz_6.pdf

Dunne Tim, Milja Kurki y Steve Smith. 2013. *International Relations Theories*. Oxford: Oxford University Press.

Eissa Sergio, Gastaldi Sol, Iván Poczynok y Elina Zacarías. 2014. “El ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino”. *Revista de Ciencias Sociales de la Universidad Nacional de Quilmes* 6 (25): 181–197.

El Dínamo. 2018. “Superintendencia de Bancos y ciberataque a 20 entidades: “La mayoría de las tarjetas de crédito afectadas se encuentran inactivas””. 25 de julio. https://www.eldinamo.cl/nacional/2018/07/25/superintendencia-de-bancos-y-ciber-ataque-a-20-entidades-la-mayoria-de-las-tarjetas-de-credito-afectadas-se-encuentran-inactivas/

El telégrafo. 2014. “FF.AA. analizan crear un Comando Operacional de Ciberdefensa”. 09 de septiembre. https://www.eltelegrafo.com.ec/noticias/politica/3/ff-aa-analizan-crear-un-comando-operacional-de-ciberdefensa.

Enríquez, Carlos. 2012. “Estrategias internacionales para el ciberespacio”. En *El ciberespacio, Nuevo escenario de confrontación*, editado por el Ministerio de Defensa de España, 73- 116. España: Imprenta del Ministerio de Defensa.

Flick, Uwe. *Designing Qualitative Research*. Londres: Sage, 2007.

Flores, Jonathan. 2018. “Banco Consorcio pierde US$2 millones tras ciberataque y enciende alarmas en la industria financiera”. *Biobiochile*, 09 de noviembre. https://www.biobiochile.cl/noticias/economia/negocios-y-empresas/2018/11/09/banco-consorcio-pierde-us2-millones-tras-ciberataque-y-enciende-alarmas-en-la-industria-financiera.shtml

Fundación Jaime Guzmán. 2018. “Desafíos de la ciberseguridad”, https://www.fjguzman.cl/wp-content/uploads/2018/08/IP_254_ciberseguridad.pdf

García, Bertha. 2008. “La situación de seguridad en el Ecuador. Políticas y estrategias en un nuevo marco de interpretación”. En *El fortalecimiento de la cooperación en seguridad entre Bolivia, Brasil, Chile, Colombia, Ecuador y Perú. Hacia una comunidad en seguridad*, editado por Baeza et al, 95-111. Lima: Konrad Adenauer Stiftung.

Gobierno de Chile. 2017. Política Nacional de Ciberseguridad. Chile: Gobierno de Chile.

Gobierno Nacional de la República del Ecuador. 2014-2017. Plan Nacional de Seguridad Integral 2014-2017. Quito: El telégrafo.

Grathouse, Craig. 2014, “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?”. En *Cyberspace and International Relations. Theory, Prospects and Challenges*, editado por Jan-Frederik Kremer y Benedikt Muller, 59-76. Nueva York: Springer.

Guzzini Stefano y Anna Leander. 2006. *Constructivism and International Relations. Alexander Wendt and his critics*. Nueva York: Routledge.

Hansen Lene y Helen Nissenbaum. 2009. “Digital Disaster, Cyber Security, and the Copenhagen School”. *Revista International Studies Quarterly* 53: 1155-1175.

https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Infodefensa. 2015. “Ecuador pone los ojos en los sistemas de ciberdefensa brasileños”. 10 de junio. https://www.infodefensa.com/latam/2015/06/10/noticia-ecuador-sistemas-ciberdefensa-brasilenos.html

Infodefensa. 2017. “Chile y Ecuador firman un gran acuerdo se colaboración en Defensa”. 31 de octubre. Infodefeinfodefensa.com/latam/2017/10/31/noticia-chile-ecuador-firman-acuerdo-colaboracion-defensa.html#:~:text=Los%20Ministerios%20de%20Defensa%20de,colaboración%20en%20materias%20de%20defensa.&text=Para%20la%20parte%20chilena%2C%20este,hemos%20firmado%20con%20diversos%20países”

Infodefensa. 2018. “Chile crea un Comando Conjunto de Ciberdefensa”. 21 de marzo. https://www.infodefensa.com/latam/2018/03/21/noticia-chile-creara-comando-conjunto-ciberdefensa.html

International Telecommunication Union. 2019. “Percentage of Individuals using the Internet”, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Internet World Stats. 2019. “Internet Usage and Population in South America”, https://www.internetworldstats.com/stats15.htm.

Jarpa, Pedro. 2016. “De ciberseguridad a ciberguerra.”, https://www.acapomil.cl/postgrado/extension/pdf/5_DE%20CIBERSEGURIDAD%20A%20CIBERGUERRA_.pdf

Kaspersky. 2019. “Kaspersky registra 45 ataques por segundo en América Latina”, https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/

Kassab, Hanna. 2014. “In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare”. En *Cyberspace and International Relations. Theory, Prospects and Challenges*, editado por Jan-Frederik Kremer y Benedikt Muller, 59-76. Nueva York: Springer.

Keohane, Robert. 1986. *Neorealism and its critics*. New York: Columbia University Press.

Kiggins David. 2014. “US Leadership in Cyberspace: Transnational Cyber Security and Global Governance”, En *Cyberspace and International Relations. Theory, Prospects and Challenges*, editado por Jan-Frederik Kremer y Benedikt Muller, 59-76. Nueva York: Springer.

Kshetri, Nir. 2013. *Cybercrime and Cybersecurity in the Global South*. New York: Palgrave Mcmillan.

Kuehl, Daniel. 2009. “From Cyberspace to Cyberpower: Defining the Problem”. En *Cyberpower and National Security*, editado por Franklin Kramer, Stuart Starr y Larry Wentz, 24 - 42. Nebraska: Nebraska Press.

Lamont, Christopher. *Research Methods in International Relations*. Londres: Sage, 2015.

Merlo, Carmen. 2017. “Ecuadro es un país poco global”. *Gestión Digital,* 1 de diciembre. https://revistagestion.ec/economia-y-finanzas-analisis/ecuador-es-un-pais-poco-global

Ministerio de Defensa de Chile. 2020. “CIberdefensa”, https://www.defensa.cl/temas-de-contenido/ciberdefensa/

Ministerio de Defensa Nacional de Chile, 2017. *Libro de la Defensa Nacional 2017*. Chile: Ministerio de Defensa Nacional.

Ministerio de Defensa Nacional de Chile, 2018. *Doctrina Conjunta de Ciberdefensa*. República de Chile: Ministerio de Defensa Nacional

Ministerio de Defensa Nacional del Ecuador. 2018. *Política de la Defensa Nacional “Libro Blanco”*. Quito: Instituto Geográfico Militar.

Ministerio de Defensa Nacional. 2014. “Informe de rendición de cuentas 2014”, https://www.defensa.gob.ec/wp-content/uploads/downloads/2015/04/INFORME_RENDICION-CUENTAS_2014.pdf

Ministerio de Defensa Nacional. 2018. “Chile y Brasil firman acuerdo sobre Ciberdefensa y protocolo de Catalogación OTAN”, https://www.defensa.cl/noticias/chile-y-brasil-firman-acuerdo-sobre-ciberdefensa/

Ministerio de Defensa Nacional. 2018. “Chile y EE.UU. firman acuerdo de cooperación en Ciberdefensa”, https://www.defensa.cl/noticias/chile-y-ee-uu-firman-acuerdo-de-cooperacion-en-ciberdefensa/

Ministerio de Defensa. “Ciberdefensa”, https://www.defensa.cl/temas-de-contenido/ciberdefensa/

Ministerio de Defensa. 2014. *Acuerdo ministerial 281*. Quito: Ministerio de Defensa Nacional de la República del Ecuador.

Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador. 2017. “Ecuador y Chile refuerzan su cooperación con nuevos acuerdos en materia social, energética y ambiental”, https://www.cancilleria.gob.ec/ecuador-y-chile-refuerzan-su-cooperacion-con-nuevos-acuerdos-en-materia-social-energetica-y-ambiental/

Ministerio de Telecomunicaciones y de la Sociedad de la Información 2016. “Viceministra Álava destacó logros de TIC en Ecuador, en TIC Fórum 2016”, https://www.telecomunicaciones.gob.ec/viceministra-alava-destaco-logros-de-tic-en-ecuador-en-tic-forum-2016/

Ministerio del Interior y Seguridad pública y Ministerio de Defensa Nacional. 2015. *Base para una Política Nacional de Ciberseguridad*. Chile: Ministerio del Interior y Seguridad pública y Ministerio de Defensa Nacional.

Ministerio del Interior y Seguridad Pública. 2018. "Ministerio de Defensa Nacional aprueba Política de Ciberdefensa." *Diario Oficial de la República de Chile*, 9 de marzo., https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf

Mogollón, Francis. 2017. "Desafíos de la Ciberseguridad y respuestas Estatales: el caso del Estado ecuatoriano en el periodo 2008-2015". Tesis de pregrado, Pontificia Universidad Católica del Ecuador.

Molina, Sandra. 2017. "¿Qué busca el Estado con una política pública? Dinámica de las políticas públicas y los valores entre las instituciones estatales". *Revista IUSTA* 1(46): 63-84.

National Cyber Security Index. 2019. "Ranking of National Cyber Security", https://ncsi.ega.ee/ncsi-index/

Norwood, Kerry y Sandra Catwell. 2009. *Cybersecurity, Cyberanalysis and Warning*. New York: Nova Science Publisher.

Nye, Joseph. 2010. *Cyber Power*. Cambridge: Harvard Kennedy School.

Panam Post. 2014. "Ecuador denuncia ataques cibernéticos provenientes de Colombia", 17 de octubre. https://panampost.com/panam-staff/2014/10/17/ecuador-denuncia-ataques-ciberneticos-provenientes-de-colombia/

Quintero, Daniel. 2014. "Las políticas regionales sobre ataques informáticos y su incidencia en la vulnerabilidad de la Defensa de la UNASUR en el periodo 2009-2013". Tesis de maestría, Instituto de Altos Estudios Nacionales (IAEN)

Radu, Roxana. 2014. "Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace". En *Cyberspace and International Relations. Theory, Prospects and Challenges*, editado por Jan-Frederik Kremer y Benedikt Muller, 59-76. Nueva York: Springer.

Rodríguez, Javiera. 2019. "Secuestran servidores de un servicio público del Ministerio de Agricultura", https://www.meganoticias.cl/nacional/266685-ataque-cibernetico-ministerio-de-agricultura-ransomware-secuestro-de-datos-servidores.html

Salinas, Cristina. 2018. "Ciberdefensa en el Estado ecuatoriano periodo 2013-2016". Tesis de pregrado, Pontificia Universidad Católica del Ecuador.

Salomón, Monica. 2002. "La Teoría de las Relaciones internacionales en los albores del siglo XXI: Diálogo, disidencia, aproximaciones". *Revista electrónica de estudios internacionales* 4: 1-59.

Sandoval, Roberto. 2018. “Chile participa en la conducción del ejercicio PANAMAX 2018”. *Defensa*, 14 de agosto. https://www.defensa.com/chile/chile-participa-conduccion-ejercicio-panamax-2018

Santander, Christian. 2019. “La construcción cibernéticas de Ecuador y Uruguay”. Tesis de Maestría, Facultad Latinoamericana de Ciencias Sociales, FLACSO Ecuador.

Schmidt, Klaus. 2006. “El crecimiento económico de Chile”, https://www.researchgate.net/publication/28124371_El_Crecimiento_Economico_de_Chile

SEMPLADES. 2011. *Guía para la formulación de políticas públicas sectoriales*. Quito. SEMPLADES

Silva, Carlos. 2018. “Curso Ciberseguridad para Auditores Internos. Taller del Marco de Ciberseguridad del NIST”, Presentado en el *Seminario CAIGG 2018*, Ministerio Secretaría General de la Presidencia, Santiago, 18 de octubre.

Silva, Julio Soto. “En torno a las amenazas: Una aclaración conceptual”, https://www.anepe.cl/en-torno-a-las-amenazas-una-aclaracion-conceptual/#_edn1.

Soto, Lorena. 2018. “El desafío de ciberseguridad para las Fuerzas Armadas”. *Revista Armas y Servicios* 15: 28-29.

Souto, Breno. 2015. “La contribución de Simmel a la sociología reticular”. *Revista Estudios Sociológicos* 99: 527-551

Squella, Pamela. 2019. “Proyecto Marciano, avance en el plan de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas Chile”. *Defensa*, 08 de septiembre. https://www.defensa.com/chile/proyecto-marciano-plan-ciberdefensa-emco-busca-dar-respuesta

Subsecretaría de Defensa. 2019. “Cierre Ejercicio Conjunto en Ciberdefensa Chile – EE.UU. (23 de agosto)”, http://www.ssdefensa.gov.cl/n8963_26-08-2019.html

Unión Internacional de Telecomunicaciones. 2017. “Global Cybersecurity Index 2017”, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Universidad Complutense de Madrid. 2009. “Las Fuerzas Armadas de Chile y su proceso de integración a las operaciones de paz”, /data/cont/media/www/pag-72507/UNISCI%20DP%2021%20-%20PERRY.pdf

Universidad de Chile. 2020. “Diploma de postítulo en Ciberseguridad y Ciberdefensa”, https://www.uchile.cl/noticias/127652/postulaciones-abiertas

Universidad de Chile. 2020. “Diploma de Postítulo en Ciberseguridad”, https://postgrados.derecho.uchile.cl/diploma-ciberseguridad/

Vargas Robert, Luis Recalde y Rolando Reyes. 2017. “Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa”. *Revista URVIO* 20: 31-45.

Vargas, Guadalupe. 2009. “El realismo y el neorrealismo estructural”. *Revista Estudios Políticos* 30 (16): 113-124.

Vicepresidencia de la República del Ecuador. 2016. “Ecuador firma acuerdo comercial con la unión europea”, https://www.vicepresidencia.gob.ec/ecuador-firma-acuerdo-comercial-con-la-union-europea/.

Waltz, Kenneth. 1979. *Theory of International Politics*. Nueva York: Longman Higher Education.

Wendt, Alexander. 2005. “La anarquía es lo que los estados hacen de ella. La construcción social de la política de poder”. *Revista Académica de Relaciones Internacionales* 1: 1-47.

Woo, Eduardo. 2014. “Ataque a servidores de la Universidad de Chile complicaron entrega de resultados de sismos”, https://www.biobiochile.cl/noticias/2014/03/07/ataque-a-servidores-de-la-universidad-de-chile-complicaron-entrega-de-resultados-de-sismos.shtml

World Economic Forum. 2016. “The Global Information Technology Report 2016”, http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf