Política Nacional de Ciberdefensa

Revisión contrastada con la Guía de Ciberdefensa de la JID

Autor

Bárbara Horzella C.
Email: bhorzella@bcn.cl

Área Gobierno, Defensa y RR.II.

Nº SUP: 129949

Resumen

El 9 de noviembre de 2017 fue aprobada la primera Política de Ciberdefensa aplicable al sector en Chile, dando cumplimiento a uno de los cinco objetivos estratégicos emanados de la Política Nacional de Ciberseguridad (Abril, 2017).

Según se consigna en su considerando, la mentada política constituye "la respuesta del Estado de Chile a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, infraestructura y operaciones de defensa".

En términos formales, se trata de un documento breve, que se divide en seis capítulos. En las primeras secciones se entregan sucintamente los elementos de contexto y de diagnóstico, que hacen necesaria la adopción de una política de estas características. Seguidamente, se ahonda en los principios en los que se sostiene la Política de Ciberdefensa, poniendo énfasis en el respeto del marco institucional vigente, así como de los tratados internacionales firmados por Chile. El texto aborda, asimismo, las modificaciones a nivel institucional que tendrán lugar como resultado de la implementación de la política; a la vez que distribuye roles entre los distintos actores del Sector Defensa, para la plena ejecución de la misma. Finaliza con un breve glosario y disposiciones en materia de gasto.

Por su parte, la Guía de Ciberdefensa elaborada por la Junta Interamericana de Defensa, consiste en un documento de 113 páginas, que proporciona "un conjunto de principios para la planificación, diseño, desarrollo y despliegue de capacidades de ciberdefensa", en virtud del mandato emanado por la OEA, en orden "de facilitar la comunicación y la colaboración en ciberdefensa entre las Fuerzas Armadas y de Seguridad del Hemisferio Occidental".

Concretamente, se trata de una guía orientada a la misión operativa militar, haciendo uso de terminología predominantemente castrense, facilitando con ello "la integración de la ciberdefensa en la acción conjunta con otros ámbitos de operaciones".

De la revisión de ambos documentos, se desprende que se trata de textos de naturaleza y objetivos distintos. El primero consigna los grandes lineamientos de política que deberán implementarse por parte del Sector Defensa en Chile, en tanto que el segundo contiene una bajada operativa y doctrinaria en materia de ciberdefensa, que busca nivelar la transformación de las Fuerzas Armadas del Hemisferio

Introducción

El 9 de noviembre de 2017[1] fue aprobada la primera Política de Ciberdefensa aplicable al sector en Chile. La aprobación de la mentada directriz forma parte de una seguidilla de hitos en este ámbito, entre los cuales se pueden mencionar los siguientes:

- El Decreto Supremo Nº 533/2015, de 27 de abril de 2015, que crea el Comité Interministerial sobre Ciberseguridad;
- La Orden Ministerial Nº 2, de 9 de octubre de 2015, del Ministro de Defensa Nacional, que dispone iniciar el proceso de elaboración de una Política de Defensa en materias de ciberespacio; y
- El Instructivo Presidencial Nº 1/2017, de 27 de abril de 2017, que aprueba e instruye la implementación de la Política Nacional de Ciberseguridad.

La adecuación al nuevo contexto tecnológico, en términos de "la creciente incorporación de tecnologías de la información y las comunicaciones en los procesos cotidianos y críticos de la Defensa Nacional", a la vez que el surgimiento de nuevos riesgos y amenazas para la seguridad del sector, constituyen aspectos sobre los que se funda la directriz bajo análisis, configurando esta última "la respuesta del Estado de Chile a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, infraestructura y operaciones de defensa" (PNCD, 2017, Considerando).

Por su parte, durante el año 2020, la Junta Interamericana de Defensa (en adelante, JID), publicó un documento titulado "Guía de Ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar"[2], principalmente orientado a la misión operativa militar, haciendo uso, asimismo, de terminología predominantemente militar, facilitando con ello "la integración de la ciberdefensa en la acción conjunta con otros ámbitos de operaciones".

A continuación se presentará una síntesis de ambos textos, a modo de extraer ciertas diferencias y similitudes generales.

1. Estructura y síntesis de la Política de Ciberdefensa

En términos formales, se trata de un documento breve, que se divide en seis capítulos. El capítulo introductorio (Capítulo 1) aborda de forma general la rápida introducción las TIC en Chile y América Latina, tanto en las actividades privadas como en el sector público, así como el aumento de los ataques o incidentes sufridos por dichos sectores, dando cuenta de la creciente vulnerabilidad y dependencia que genera la utilización de este tipo de herramientas, lo que hace necesaria la adopción de una Política de Estado para hacer frente a estos nuevos riesgos y amenazas.

[1] Fue publicada en el Diario Oficial N° 42.003, del día 9 de marzo de 2018. Disponible en: https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf (Marzo, 2021).
[2] JID (2020). "Guía de Ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar". Disponible en: https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf (Marzo, 2020).

La Política Nacional de Ciberseguridad, aprobada el 27 de abril de 2017, encarna dicha directriz política, constituyendo “el primer instrumento del Estado de Chile que fija la carta de navegación sobre las medidas que se deben adoptar, tanto en el sector público como en el privado, para contar con un ciberespacio libre, abierto, seguro y resiliente”, consagrándose en ella cinco objetivos estratégicos de largo plazo, de los cuales se deriva, a su vez, la adopción de la Política de Ciberdefensa, como parte integrante de un sistema nacional de políticas nacionales.

De esta forma, la Política de Ciberdefensa viene a complementar a la de Ciberseguridad en aquellos aspectos relacionados directamente con la defensa de la soberanía del país, a través de las redes digitales; y de la infraestructura crítica de la información, por mencionar algunos, sustentándose sobre los principios del Derecho Internacional, al considerar que estos le son plenamente aplicables al ciberespacio, como objeto de protección.

En virtud de ello, este instrumento fija los objetivos a ser cumplidos gradualmente en un horizonte de cinco años (2017-2022), requiriendo que las instituciones de la Defensa avancen en su implementación.

El capítulo 2, titulado “Diagnóstico”, describe sucintamente el tipo de amenazas cibernéticas, desde el punto de vista de su periodicidad, sofisticación e impacto, al que están expuestas las instituciones del sector Defensa, proyectándose un aumento constante de aquellas a futuro.

También de forma breve, alude al carácter global y transfronterizo del ciberespacio, así como al crecimiento exponencial de dispositivos conectados a la red, complejizando su gestión por parte de la comunidad internacional, lo que trae aparejada la necesidad de contar con “un instrumento normativo de política pública para la planificación y empleo de la Defensa Nacional en materia de ciberdefensa, que asegure el cumplimiento del mandato constitucional de protección de la seguridad exterior del país, en este ámbito”.

El capítulo 3, en tanto, ahonda en los principios en los que se sostiene la Política de Ciberdefensa, poniendo énfasis en el respeto del marco institucional vigente, así como de los tratados y acuerdos internacionales firmados por Chile.

En virtud de ello, dispone que el sector Defensa debe procurar una infraestructura de la información robusta y resiliente frente a los incidentes de ciberseguridad, respetando los derechos de las personas en el ciberespacio.

Asimismo, debe velar por la promoción de una cultura de buenas prácticas y educación en este ámbito. En materia de cooperación internacional, se señala como objetivo la prevención de acciones cibernéticas ilícitas desde Chile a otros estados, en el campo de la Defensa.

Por su parte, la Política de Ciberdefensa, en tanto parte integrante de la Política de Defensa Nacional, reconoce a las operaciones de defensa en el ciberespacio como una “dimensión específica del espectro contemporáneo del empleo de las capacidades de defensa”, cuya planificación, conducción y ejecución debe estar ceñida al respeto del Derecho Internacional Público, con especial consideración al Derecho Internacional de los Derechos Humanos y al Derecho Internacional Humanitario.

Desde el enfoque local, se establece la necesidad de una estrecha cooperación con otros actores de la institucionalidad del Estado, la sociedad civil y entidades privadas, mediante la participación en diversas instancias para la toma de decisiones, así como para el intercambio y colaboración en el plano técnico y operacional.

Asimismo, se precisa que la cooperación internacional es "imprescindible para contar con un ciberespacio libre, abierto y seguro, sobre la base de una regulación internacional democrática, que preserve los derechos de las personas y regule la conducta de los estados en esta dimensión", relevándose en este sentido la estrecha cooperación que debe existir con el Ministerio de Relaciones Exteriores.

Otro de los pilares establecidos por la directriz bajo análisis, tiene relación con la relevancia que se otorga al desarrollo tecnológico en materia de TIC. En este sentido, se busca orientar tanto a la Política Militar como a la Política de la Industria de Defensa Nacional, en la promoción del desarrollo de una industria que le permita mantener un adecuado nivel de independencia y soberanía tecnológica.

En el cuarto capítulo, intitulado "Política de Defensa Nacional y su aplicación al ciberespacio", se abordan los efectos que puede tener un ciberataque, señalando que sus daños pueden ser comparables a los de un ataque armado, y por ello -en su derecho de legítima defensa, consagrado en el Artículo 51 de la Carta de las Naciones Unidas- el Estado chileno podrá hacer uso de los medios que estime necesarios para su respuesta, protección de infraestructura crítica de la información y correcta atribución de ataques, entre otros.

Seguidamente, en el apartado 4.2, se ahonda en las medidas que debe tomar el Sector Defensa para la promoción de la cooperación internacional, transparencia y confianza entre los estados, considerando la participación en los distintos foros internacionales que aborden la materia.

Asimismo, y según se consigna en el punto 4.3, el Estado de Chile desarrollará y mantendrá las capacidades necesarias para la autodefensa del país, a través de programas generales y especializados de formación y capacitación, para los que se define una serie de lineamientos, que harán necesaria la modificación de la malla curricular, así como los requisitos de ascenso, entre otros aspectos.

El mismo punto aborda los cambios institucionales surgidos a partir de esta política, como la creación de un Comando Conjunto de Ciberdefensa, bajo el mando del Jefe del Estado Mayor Conjunto; la formación de 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, también dirigido por el EMCO; la creación de un CSIRT por cada una de las ramas; así como la implementación de una Oficina de Ciberdefensa y Seguridad de la Información, en el Gabinete del Ministro de Defensa Nacional.

A continuación, el capítulo 5 dispone la elaboración de un plan para la implementación de la mentada política, distribuyendo los roles entre los distintos actores del sector Defensa. Asimismo, consagra un

periodo de revisión de cuatro años de la Política, o cuando las circunstancias lo ameriten, proceso que será coordinado por la Subsecretaría de Defensa.

Finalmente, en el capítulo 6 se dispone un glosario donde se definen los siguientes términos: Ciberataque, Ciberdefensa, Ciberespacio y Ciberseguridad. Adicionalmente, en un segundo artículo se establecen las disposiciones en relación al gasto que genere la ejecución de la política bajo análisis.

2. Guía de Ciberdefensa de la JID

La Guía elaborada por la JID, con el patrocinio del Gobierno de Canadá, consiste en un documento de 113 páginas, que proporciona "un conjunto de principios para la planificación, diseño, desarrollo y despliegue de capacidades de ciberdefensa", en virtud del mandato emanado por la Organización de Estados Americanos (OEA), en orden "de facilitar la comunicación y la colaboración en ciberdefensa entre las Fuerzas Armadas y de Seguridad del Hemisferio Occidental" (JID, 2020: 5).

En términos globales, como señala el General LaCroix, "el ciberespacio ya no es un dominio 'emergente', sino un potencial teatro de guerra, en el que todas las naciones soberanas podrían participar de manera activa y diaria", agregando que "las ciberamenazas a la seguridad del Hemisferio Occidental, son cada vez más frecuentes, complejas, destructivas y coercitivas". De ahí la necesidad de abordar este fenómeno de forma colectiva.

Por su parte, y según se consigna en la Introducción, la elaboración de esta Guía responde a los desiguales niveles de transformación de las Fuerzas Armadas para adaptarse al nuevo escenario estratégico, que contempla al ciberespacio como el quinto ámbito de operaciones.

De esta forma, el objetivo de la Guía es "proporcionar orientaciones para llevar a cabo esta transformación y desarrollar una capacidad de ciberdefensa militar de una manera integral y organizada, a todos los niveles necesarios" (JID, 2020:8).

Particularmente, se trata de una guía orientada a la misión operativa militar, haciendo uso asimismo de terminología predominantemente militar, facilitando con ello "la integración de la ciberdefensa en la acción conjunta con otros ámbitos de operaciones".

A modo de síntesis, el contenido de la guía se organiza en nueve unidades que, en su conjunto, aportan una aproximación integral:

> La unidad "ciberespacio" analiza el medio en donde se desarrollan las actividades de ciberdefensa; proporciona una representación práctica que facilita su comprensión, estudio y uso; y analiza la parte principal del ciberespacio (*internet*), incluyendo la *internet* más oculta.
>
> La unidad "ámbito de operaciones ciberespacial", detalla todos aquellos elementos fundamentales de un ámbito de operaciones militares desde la perspectiva ciberespacial, remarcando sus peculiaridades y diferencias con los ámbitos de operaciones convencionales.

> La unidad “ciberdefensa militar” aproxima la ciberdefensa al arte militar del empleo del ciberespacio y a las operaciones militares en el mismo (ciberoperaciones), proponiendo una taxonomía de los diferentes tipos de ciberoperaciones.
>
> La unidad “fuerza ciberespacial” detalla los aspectos a considerar en el proceso de desarrollo de la fuerza militar responsable del planeamiento y la conducción de las operaciones militares en el ciberespacio, junto con las capacidades básicas que debe tener para llevar a cabo sus cometidos con un mínimo de garantía.
>
> La unidad “ciberamenaza” analiza los principales retos actuales, las tendencias y, en particular, la principal amenaza asociada a los estados, las amenazas avanzadas persistentes y el modo de combatirlas.
>
> La unidad “principios doctrinales” analiza la aplicabilidad al ciberespacio de los principios tradicionales que guían la actuación de las fuerzas militares en las operaciones convencionales (principios fundamentales del arte militar y principios operativos).
>
> La unidad “ecosistema ciberespacial” pone en contexto la ciberdefensa militar y analiza las relaciones con sus entornos naturales fundamentales, la ciberseguridad nacional, la ciberseguridad internacional y el sector privado.
>
> La unidad “aspectos legales” analiza la situación actual de consenso en la aplicación del derecho internacional a las ciberoperaciones, tanto en tiempo de paz como en periodos de conflicto, zona de operaciones o misiones de paz, considerando aquellos aspectos más relevantes para la ciberdefensa militar (JID, 2020:8).

La Guía aporta también un convenio de uso del lenguaje específico del entorno ciberespacial y las definiciones de los términos más relevantes usados en ella, así como los acrónimos.