Publicado en la página web del CEEEP
Fecha: 18 de noviembre de 2021

Política Sectorial de Ciberdefensa: una necesidad impostergable

Ernesto Castillo Fuerman, General de Brigada del Ejército del Perú, especialista en Ciberseguridad y Ciberdefensa por la UNI-INICTEL, Doctor y Magister en Gestión y Desarrollo, así como Magister en Gestión Pública e Ingeniero Electrónico. El General Castillo ha sido director del Centro de Entrenamiento Táctico Computarizado de Ejército, fundador del Centro de Ciberdefensa del Ejército y jefe de operaciones de Ciberdefensa y Telemática del Ejército; asimismo, ha formulado el Manual de Guerra Electrónica y Ciberdefensa del Ejército. Actualmente, se desempaña como Comandante General de Ciberdefensa y Telemática del Ejército.

Resumen

Las infraestructuras críticas de un país, los sistemas de comando y control, así como los sistemas de armas cuentan con plataformas informáticas para su funcionamiento; sin embargo, como resultado de un ciberataque, estas plataformas podrían quedar inservibles y paralizar a un país, poniendo en riesgo la Seguridad, la Defensa y el Desarrollo Nacional. Por consiguiente, resulta imprescindible contar con una Política Sectorial de Ciberdefensa, cuyos objetivos y lineamientos permitan fortalecer el desarrollo de capacidades para neutralizar las amenazas y ataques en y mediante el ciberespacio, impulsando la cultura, la educación, así como la Investigación, Desarrollo e Innovación (I+D+i) en ciberdefensa entre las Instituciones Armadas. En este artículo se analiza la situación de la Ciberdefensa en el Perú y se propone el enunciado, así como los objetivos y lineamientos de la necesaria Política Sectorial de Ciberdefensa que el Estado peruano debería poseer.

Palabras Clave: Ciberataque, Ciberdefensa, Ciberespacio, Política Sectorial de Ciberdefensa.

Introducción

El incremento de amenazas en el ciberespacio, así como el uso de nuevas tecnologías para generar amenazas informáticas constituyen preocupaciones comunes en todos los países, dado que impactan de manera significativa en la seguridad de la información (en los ámbitos públicos y privados) e, inclusive, en los activos críticos nacionales y recursos claves de un Estado. En el Perú, la Ley N° 30999, Ley de Ciberdefensa, aprobada el 26 de agosto de 2019, define a la Ciberdefensa como la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio, cuando estos afecten la Seguridad Nacional[1]. Por lo tanto, el desarrollo de capacidades en las Fuerzas Armadas (FF. AA.) para enfrentar los ciberataques y la ciberguerra es una necesidad impostergable en el Estado peruano ya que, de lo contrario, se ponen en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y los recursos claves del Estado. Sin embargo, en el Perú, se carece de una Política Sectorial de Ciberdefensa que oriente el desarrollo de dichas capacidades en las FF. AA.

Tomando en cuenta la experiencia del autor al haberse desempeñado como Director de Política y Planeamiento Estratégico para la Defensa en el Ministerio de Defensa, en

este artículo se analiza la situación de la Ciberdefensa en el Perú y se propone el enunciado, así como los objetivos y lineamientos de la necesaria Política Sectorial de Ciberdefensa que el Estado peruano debe poseer.

El ataque cibernético a Estonia

El primer ataque cibernético de gran envergadura contra un Estado se realizó en abril de 2007 en Estonia. A consecuencia de ese ataque, las principales instituciones públicas y privadas de Estonia se vieron paralizadas por una avalancha de ciberataques que tuvieron como objetivos a numerosas instituciones, entre las cuales el Parlamento y varios ministerios, además de bancos, partidos políticos y medios de comunicación. Ante ello, Estonia tuvo que cortar toda la línea de internet y formatear todos sus sistemas.[2]

El ataque cibernético a Estonia reveló una nueva forma de hacer la guerra, pudiéndose asegurar que la dificultad para la identificación de quienes llevaron a cabo el ataque y la naturaleza de los medios empleados cambiaron la imagen de lo que serían los conflictos del futuro. Al respecto, el Director del Centro de Seguridad Informática de Estonia indicó que todo fue muy confuso en los días precedentes al ataque debido a que no entendían lo que estaba pasando; asimismo, afirmó que la magnitud y el impacto del ataque fueron mucho mayores de lo que podrían haber imaginado. Durante dichos eventos, los *hackers* atacaron sustituyendo los portales de las páginas oficiales por imágenes insultantes contra el Primer Ministro estonio. El tráfico en internet se disparó bruscamente hasta saturar los servidores y la población de Estonia salió a tomar las calles de la capital ya que sentían que su gobierno perdía poco a poco el control de la situación. Cuando el Ministerio de Defensa intentó averiguar lo que pasaba, descubrió que no solo las agencias de noticias habían sido atacadas sino, también, los grandes bancos comerciales lo que, en un país pequeño como Estonia, fue una gran preocupación a todo nivel. El ataque cibernético estuvo a punto de generar una revuelta, ya que los estonios de origen ruso invadieron el centro de la capital, mientras los sistemas informáticos se bloquearon, la distribución de la gasolina y del pan fueron interrumpidos y la anarquía se propagó por el país[3].

Como respuesta a este ataque cibernético, la Organización del Tratado del Atlántico Norte (OTAN) implementó en Tallin, la capital de Estonia, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, siendo considerado actualmente un referente en ciberdefensa a nivel mundial. Asimismo, en enero de 2008, la OTAN promulgó la Política de Ciberdefensa con el objetivo de mejorar la capacidad de la Alianza para proteger sus sistemas de información y comunicaciones, de importancia crítica frente a los ciberataques[4]. Posteriormente, en Varsovia, en julio de 2016, los Jefes de Estado y de Gobierno miembros de la OTAN se comprometieron -a través del documento *Cyber Defence Pledge*- a mantenerse alertas ante las ciberamenazas y a ser capaces de defenderse en el ciberespacio, tal y como ocurre en el dominio terrestre, aéreo y marítimo, reconociendo al ciberespacio como un nuevo dominio de las operaciones militares[5].

La ciberdefensa en el Perú

Tras el caso descrito, resulta indudable afirmar que el Estado peruano requiere crear el ambiente y las condiciones necesarias para brindar efectiva protección en el ciberespacio y enfrentar las amenazas que atentan contra su seguridad. En ese sentido, tomando en consideración que las FF. AA. requieren actuar de forma integral frente a las

amenazas cibernéticas, es necesario que el Perú cuente con una Política Sectorial de Ciberdefensa.

Al respecto, en el año 2017, la Dirección de Política y Planeamiento Estratégico para la Defensa del Ministerio de Defensa formuló un proyecto de Directiva que establecía las Políticas del Sector Defensa en Ciberdefensa. Este proyecto de Directiva –aunque no fue aprobado con Resolución Ministerial- fue tomado en consideración para la formulación del Plan Estratégico Sectorial Multianual (PESEM) 2017-2021, el mismo que para alcanzar su Objetivo Estratégico 1 (Garantizar la Defensa Nacional) contemplaba la implementación de la Acción Estratégico 1.7 (Desarrollar la Ciberdefensa protegiendo la infraestructura critica del Estado de ciberataques)[6]. Incluso, el Plan Estratégico Institucional (PEI) 2018-2020 del Sector Defensa contempla alcanzar el Objetivo Estratégico 6 (Desarrollar la Ciberdefensa institucional)[7]. Para ello, tanto el Comando Conjunto de las Fuerzas Armadas (CCFFAA) como las Instituciones Armadas han creado sus entidades de ciberdefensa, lográndose promulgar la Ley N° 30999, Ley de Ciberdefensa.

Al respecto, el 25 de marzo de 2019, el CCFFAA activó el Comando Operacional de Ciberdefensa (COCID), inaugurando sus instalaciones el 20 de enero de 2020[8]. El COCID cuenta con tres Componentes (terrestre, naval y aéreo). Por una parte, el Componente Terrestre lo conforma el Centro de Ciberdefensa del Ejército, inaugurado el 29 de octubre de 2018[9]. Por otra parte, el Componente Naval lo conforma la Comandancia de Ciberdefensa de la Marina de Guerra, inaugurado el 21 de febrero de 2019[10]. Asimismo, el Componente Aéreo lo conforma el Grupo de Operaciones en el Ciberespacio de la Fuerza Aérea, inaugurado el 21 de diciembre del 2019[11].

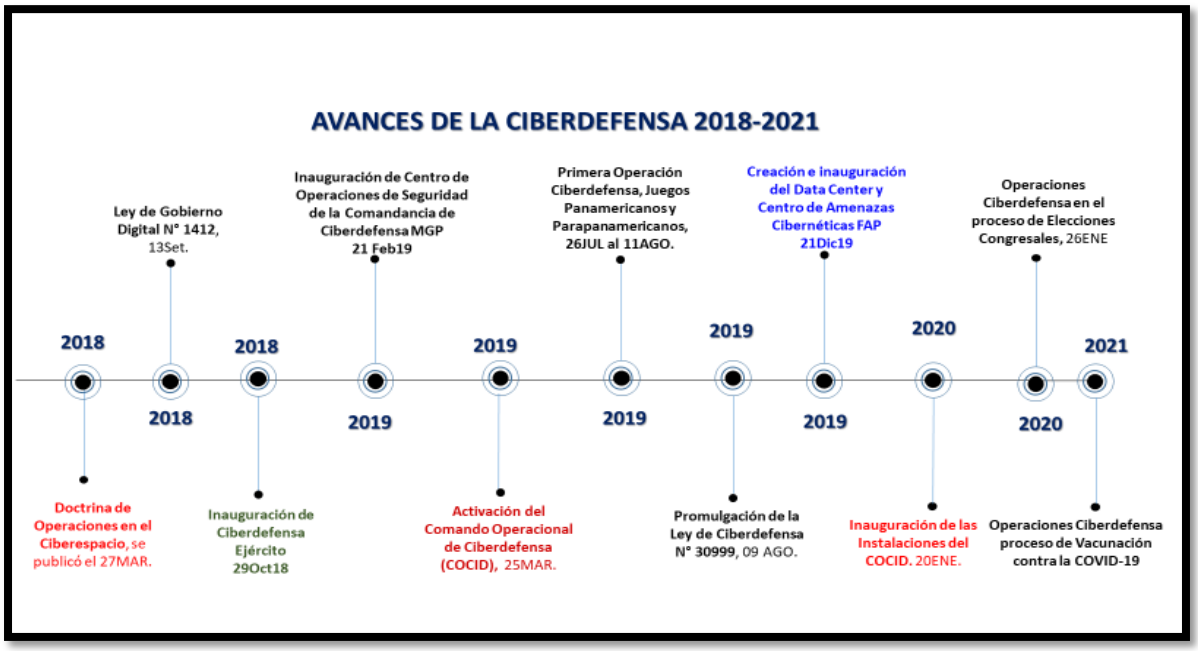

Figura 1. Línea de Tiempo de los Avances de la Ciberdefensa en el Perú (Elaboración propia)

A la fecha, el COCID ha realizado operaciones de ciberdefensa durante la realización de los XVIII Juegos Panamericanos y VI Juegos Parapanamericanos de Lima 2019, las Elecciones Congresales de enero de 2020 y la ejecución del Plan de Vacunación COVID-19 del año 2021. Todas estas experiencias han servido para conocer e identificar las debilidades del Estado Peruano en el entorno digital, sobre todo en los activos críticos

nacionales del sector público, lo que conllevaría a poner en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves del Estado.

En ese sentido, el Artículo 12 (sobre el control y la protección de los activos críticos nacionales y recursos claves) de la Ley N° 30999, Ley de Ciberdefensa, señala que "*el CCFFAA está a cargo de la Ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional*"[12]. Por consiguiente, para cumplir eficazmente esta función, el Gobierno debe asignar los recursos necesarios que permitan fortalecer y desarrollar capacidades en Ciberdefensa tanto del COCID, como de sus Componentes.

Asimismo, resulta imprescindible la formulación, aprobación e implementación de una Política Sectorial de Ciberdefensa que señale los objetivos y lineamientos que deberán ser alcanzados por el Sector Defensa. Para ello, a continuación, se brinda una propuesta del enunciado de dicha Política, así como de sus objetivos y lineamientos con la finalidad de brindar ideas y facilitar su necesaria formulación. En ese sentido, el enunciado de la Política de Ciberdefensa podría ser: "*Contar con FF. AA. con una capacidad de Ciberdefensa adecuada para hacer frente a las amenazas o ataques realizados en y mediante el ciberespacio, que pongan en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, considerando las debilidades del Estado en el entorno digital*".

Asimismo, tomando como referencia el proyecto de Directiva formulado por la Dirección de Política y Planeamiento Estratégico para la Defensa del Ministerio de Defensa y las experiencias obtenidas durante estos últimos años, los objetivos y lineamientos de la Política Sectorial de Ciberdefensa podrían ser los siguientes:

- **Objetivo 1:** "*Fortalecer la capacidad de Ciberdefensa de las FF. AA. para neutralizar las amenazas y ataques en y mediante el ciberespacio cuando afecten la seguridad nacional*", proponiéndose –para ello- los siguientes **Lineamientos**: (1) Fortalecer el COCID a fin de neutralizar la ciberamenazas y responder los ciberataques que atenten a la seguridad nacional. (2) Potenciar las capacidades militares de las organizaciones de ciberdefensa de las Instituciones Armadas, asegurando el ciberespacio que emplean las fuerzas terrestres, navales y aéreas, así como el ciberespacio de los activos críticos y recursos claves designados. (3) Mejorar las capacidades de las FF. AA. para contar con información oportuna ante una posible ciberamenaza, desarrollando alertas tempranas y apoyo a las operaciones ante ciberataques.

- **Objetivo 2:** "Impulsar la cultura y la educación en ciberdefensa en las FF. AA.", proponiéndose los siguientes **Lineamientos**: (1) Concientizar al personal que labora en el Sector Defensa de los riesgos derivados de las actividades en el ciberespacio, en busca de consolidar la cultura de ciberdefensa. (2) Desarrollar conocimientos, habilidades, experiencia y capacidades tecnológicas en las instituciones del sector para soportar y cumplir los objetivos de ciberdefensa, certificando la calidad educativa. (3) Impulsar la formación, capacitación, especialización del personal en cursos y programas de pre y post grado en Ciberdefensa.

- **Objetivo 3:** "Desarrollar Investigación, Desarrollo e Innovación (I+D+i) en Ciberdefensa colaborativa entre las FF. AA". Para ello, se proponen los siguientes **Lineamientos**: (1) Mejorar las Políticas para I+D+i en ciberdefensa a fin que sean adecuadas y oportunas.

(2) Implementar Infraestructura y equipamiento adecuado para la I+D+i en ciberdefensa. (3) Promover proyectos de I+D+i culminados en las FF. AA. (4) Fomentar la colaboración en I+D+i entre las Instituciones de las Fuerzas Armadas.

- **Objetivo 4:** "Impulsar la cooperación nacional e internacional a fin de contar con una seguridad cooperativa en el entorno digital", proponiéndose los siguientes **Lineamientos**: (1) Incrementar la presencia del Sector Defensa del Perú en organizaciones y foros internacionales en ciberdefensa. (2) Suscribir acuerdos con organizaciones nacionales e internacionales de países con quienes el Perú comparta intereses. (3) Fomentar la participación coordinada con otras instituciones públicas y privadas en simulacros y ejercicios internacionales de ciberdefensa. (4) Aumentar la cooperación con organismos nacionales e internacionales en materia de ciberdefensa, buscando la estandarización y alineamiento de procesos.

Conclusión

El que gane la guerra cibernética cumplirá lo expresado por Sun Tzu: "*Los generales expertos en mando siempre hacen a los ejércitos enemigos doblegarse sin batalla, esa es la máxima victoria*". En ese sentido, las infraestructuras críticas de un país, los sistemas de comando y control, así como los sistemas de armas cuentan con plataformas informáticas para su funcionamiento; sin embargo, como resultado de un ciberataque, estas plataformas podrían quedar inservibles y paralizar a un país, poniendo en riesgo la Seguridad, la Defensa y el Desarrollo Nacional.

Al respecto, la Política Nacional define el "qué hacer"; por consiguiente, resulta imprescindible contar con una Política Sectorial de Ciberdefensa, cuyos objetivos y lineamientos permitan fortalecer el desarrollo de capacidades para neutralizar las amenazas y ataques en y mediante el ciberespacio, impulsando tanto la cultura y la educación en ciberdefensa en las Fuerzas Armadas, como la Investigación, Desarrollo e Innovación (I+D+i) en ciberdefensa entre las Instituciones Armadas, así como la cooperación nacional e internacional a fin de contar con una seguridad cooperativa en el entorno digital.

Notas Finales

[1] *Ley Ciberdefensa*, art. 4, (09 de agosto de 2019) Ley N° 30999 Congreso de la República, https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678061-ley-n-30999

[2] "Los 10 ataques cibernéticos más importantes hasta la fecha," *Teinteresa* (19 de abril de 2013), http://www.teinteresa.es/mundo/ataques-ciberneticos-importantes-fecha_0_904110101.html (consultado el 18 de enero de 2017)

[3] *Ciber Guerrilla: Hackers, piratas y guerras secretas* (España, 2016), Documental canal Odisea

[4] *NATO Policy on Cyber Defence*, (C-M 2007)0120.

[5] https://www.nato.int/cps/en/natohq/official_texts_133177.htm, (consultado el 11 de octubre de 2021).

[6] Ministerio de Defensa, *Resolución Ministerial N° 2054-2017-DE/SG* (2017)

[7] Ministerio de Defensa, *Resolución Ministerial N° 2084-2017-DE/SG* (2017)

[8] "Ministro de Defensa inauguró instalaciones del Comando Operacional de Ciberdefensa," *Gob.pe plataforma digital única del Estado Peruano* (20 de enero de 2020), nota de prensa del Comando Cunjunto de las Fuerzas Armadas, https://www.gob.pe/institucion/ccffaa/noticias/505601-ministro-de-defensa-inauguro-

instalaciones-del-comando-operacional-de-ciberdefensa (consultado el 11 de octubre de 2021).

[9] "El Ejército del Perú inaugura su Comando de Ciberdefensa," *Maquina de combate* (30 de octubre de 2018), https://maquina-de-combate.com/blog/?p=58478 (consultado el 11 de octubre de 2021).

[10] "Inauguración del Centro de Operaciones de Seguridad de la Comandancia de Ciberdefensa," *Marina de Guerra del Perú Home Page* (21 de febrero de 2019), https://marina.mil.pe/es/noticia/inauguracion-del-centro-de-operaciones-de-seguridad-de-la-comandancia-de-ciberdefensa/ (consultado el 11 de octubre de 2021).

[11] "Fuerza Aérea presentó moderno Data Center y Centro de Monitoreo de Amenazas Cibernéticas," *Gob.pe plataforma digital única del Estado Peruano* (21 de diciembre de 2019), nota de prensa del Ministerio de Defensa, https://www.gob.pe/institucion/mindef/noticias/71274-fuerza-aerea-presento-moderno-data-center-y-centro-de-monitoreo-de-amenazas-ciberneticas (consultado el 11 de octubre de 2021).

[12] *Ley de Ciberdefensa*, art. 12, Ley N° 30999