URVIO, Revista Latinoamericana de Estudios de Seguridad
ISSN: 1390-3691
ISSN: 1390-4299
revistaurvio@flacso.edu.ec
Facultad Latinoamericana de Ciencias Sociales
Ecuador

Vargas Borbúa, Robert; Recalde Herrera, Luis; Reyes, Rolando

Ciberdefensa y ciberseguridad, más allá del mundo virtual:
modelo ecuatoriano de gobernanza en ciberdefensa

URVIO, Revista Latinoamericana de Estudios de Seguridad, núm. 20, 2017, pp. 31-45
Facultad Latinoamericana de Ciencias Sociales
Ecuador

DOI: https://doi.org/10.17141/urvio.20.2017.2571

Disponible en: https://www.redalyc.org/articulo.oa?id=552656641013

Tema central

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 31-45
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa

Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance

Robert Vargas Borbúa[1], Luis Recalde Herrera[2], Rolando P. Reyes Ch.[3]

Fecha de recepción: 11 de febrero de 2017
Fecha de aceptación: 19 de abril de 2017

Resumen

La ciberdefensa y ciberseguridad se han convertido en áreas claves de los estudios estratégicos. Su desarrollo actual coincide con el advenimiento de la sociedad de la información, las redes entre computadoras y el fenómeno "Internet", cuya expansión ha configurado la quinta dimensión de la guerra moderna y ha afectado sensiblemente la vida cotidiana de los diversos actores en el mundo global. De hecho, su estudio se convierte en una tarea obligada para la conducción político-estratégica de la defensa de las naciones. En el Ecuador, dichas temáticas (ampliamente discutidas) se han focalizado en una dimensión pragmática. El presente artículo, tras un examen analítico-conceptual de la seguridad y defensa en el ciberespacio, propone la configuración de un modelo local de gobernanza en ciberdefensa, inscrito en la normativa vigente. Los hallazgos muestran que la reflexión local es aún incipiente y se requieren esfuerzos interagenciales para su institucionalización.

Palabras clave: conducción de la defensa; Ecuador; estudios estratégicos; modelo de gobernanza.

Abstract

Cyber-defense and cybersecurity have become key areas of strategic studies. Its current development coincides with the advent of the information society, the networks between computers and the phenomenon "Inter-

1 Director del Centro de Investigación Científica y Tecnológica del Ejército (CICTE) en la Universidad de las Fuerzas Armadas (ESPE). Teniente Coronel de Estado Mayor del Ejército del Ecuador. Coordinador de la Maestría en Estrategia Militar Terrestre en la Academia de Guerra del Ejército. Master en Gestión de las Comunicaciones y Tecnologías de la Información, en la Escuela Politécnica Nacional, Quito-Ecuador. Master en Telemática, en la Universidad Politécnica de Cataluña, España. Correo: rbvargas@espe.edu.ec

2 Docente investigador del Departamento de Seguridad y Defensa de la Universidad de las Fuerzas Armadas ESPE. Mayor en Servicio Pasivo, Ingeniero Electrónico en Telecomunicaciones. Magister en Evaluación y Auditoría de Sistemas. Master en Administración de Empresas. Correo: llrecalde@espe.edu.ec

3 Investigador del Centro de Investigación Científica y Tecnológica del Ejército (CICTE) en la Universidad de las Fuerzas Armadas (ESPE). Coordinó la Jefatura de la Unidad de Tecnologías de la Información del Instituto de Seguridad Social de Fuerzas Armadas. Master en Electrónica con mención en Redes y Telecomunicaciones. Master en Software y Sistemas. Estudiante de doctorado en Software, Sistemas y Computación por la Universidad Politécnica de Madrid. Correo: rpreyes1@espe.edu.ec

net" whose expansion has shaped the fifth dimension of modern war and has significantly affected the daily life of the various actors in the global world. Indeed, its study becomes a task forced for the political-strategic conduct of the defense of the nations. In Ecuador these themes (widely discussed) have focused on a pragmatic dimension. This article, after an analytical-conceptual consideration of security and defense in cyberspace, proposes the configuration of a local model of governance in cyber-defense, inscribed in the current legislation. The findings show that local reflection is still incipient and interagency efforts are required for its institutionalization.

Keywords: conduction of defense; Ecuador; governance model; strategic studies.

Antecedentes

Después de los ataques terroristas en Francia, París se militarizó. Se sabía que podían existir más terroristas en su territorio. Los miembros de las fuerzas armadas, policía y otros servicios de seguridad, coparon las calles para proteger a sus conciudadanos, pues tenían que definir quién era el enemigo, quién podría participar directamente, quién podría proveer alojamiento, abrigo o comida, quién pudo coordinar los atentados y distribuir propaganda, entre otros. En este contexto, saber quién es combatiente y quién no, era difícil y ambiguo. Por ello, las concepciones tradicionales de seguridad, defensa, seguridad externa, seguridad interna, seguridad multidimensional, seguridad humana y otros, no solo que se traslapan, sino que se refuerzan y contraponen, abriendo la posibilidad a nuevas miradas teóricas y epistemológicas de la seguridad y la defensa, que sean capaces de dar cuenta del comportamiento de las amenazas y sus nuevas lógicas.

El concepto de *seguridad,* del latín *securitas* (Real Académica Española s.f.), inscribe varios sentidos y componentes, pero su connotación rectora se relaciona con la condición de confianza, de estar libre de riesgos y/o amenazas, peligros y daños. Es un logro colectivo, imprescindible para garantizar la libertad individual (Vargas 2008). De manera complementaria, *defensa* comprende las medidas (militares o no) que permiten resguardarnos de tales riesgos, amenazas, peligros y daños; por lo que estar o sentirse seguro implica no solo protección y conservación, sino también una capacidad de respuesta.

Se afirma que la estructura social y política del estado-nación actual es una respuesta a la seguridad, que necesariamente implica estar en condiciones de defenderse de amenazas, riesgos y peligros. Por ello, seguridad y defensa son inherentes a la supervivencia y desarrollo del hombre y la sociedad. En suma, el desarrollo de un Estado está íntimamente ligado a su condición de seguridad y a las acciones que se ejecuten para mantener esa condición, es decir, su capacidad de defensa (De Vergara 2009). Por ende, el conflicto, en sus variadas formas, también es inherente a la historia de la humanidad (Feliu 2013).

Existe una relación compleja de interdependencia entre seguridad, defensa y desarrollo (Díaz 2005). La intensidad de tal interdependencia ha sido matizada fuertemente por la influencia de diferentes intereses y percepciones, relaciones de poder o por intereses geopolíticos y estratégicos dadas en el tiempo, y desarrollos tecnológicos de la humanidad. Justamente, en la actualidad, cuando el desarrollo de las tecnologías de información y comunicaciones (TIC) empiezan a transformar la vida humana y sus estructuras sociales y políticas (Fridman 2013), la política nacional e internacional (Nye Jr. y Welch 2013), incluyendo las consideraciones de seguridad y defensa. La Internet, las redes de telecomunicaciones, las computadoras, el *software*, el uso

de las redes sociales, la interacción de las personas y las máquinas y las actuaciones que de estas se derivan, han impulsado a la creación un escenario virtual denominado ciberespacio (ISO/IEC27032 2012) que modifican las acepciones de seguridad y defensa (Government of Canada 2010, 2).

En el ciberespacio, más de 1,7 mil millones de personas están unidas intercambiando ideas y servicios. A diario se envían 294 mil millones de correos electrónicos, se generan 168 millones de *DVDs* de información, 22 millones de horas de TV y películas a través de *Netflix*[4], y 864.000 horas de vídeos se suben a *Youtube*[5] (Klimburg 2012, 33). Existen 31 millones de cuentas en *Skype*[6] (27 min/conversación) (Klimburg 2012, 33). La telefonía móvil ha penetrado en el 85% de la población mundial, el tráfico de mensajes por telefonía móvil genera $ 812.000 /min. Más del 20% de la población global actúa en redes sociales. De hecho, dos tercios de usuarios de Internet buscan productos y hacen negocios en línea y 2,5 mil millones de ciudadanos usan pago electrónico seguro (Klimburg 2012, 33). De su parte, las industrias cada vez utilizan más computadoras, sistemas operativos comunes, aplicaciones y protocolos de redes para reducir costos, mejorar la eficiencia y monitorear procesos.

Para el año 2020, se estima que la población mundial con acceso a Internet será de 5 mil millones (60% en línea), habrá aproximadamente 50 mil millones de dispositivos (10 equipos por persona) y una afectación a la economía mundial en más del 10% del producto interno bruto (PIB) mundial (Klimburg 2012, 33). Esto explica el por qué de las economías de los estados, de las compañías y de los propios individuos, dependen del ciberespacio (Government of Canada 2010, 2). Alvin y Heidi Toffler (1981, 18) puntualizaron que "nuestro modo de guerrear, refleja nuestro modo de ganar dinero". En resonancia, podríamos afirmar que si la economía y el bienestar están directamente relacionados con el mercado digital o el manejo de la información en el ciberespacio, nuestra seguridad y defensa deben estar también ligadas, cada vez más, al propio ciberespacio. Es decir, que las acciones para defendernos de riesgos, amenazas, peligros y daños virtuales, deben estar también orientadas a darnos confianza y certeza, tanto en el mundo real como en el virtual.

La seguridad del ciberespacio no solo constituye una necesidad individual o propia de las compañías, sino que también es un asunto de seguridad y soberanía nacional que influye en la gobernanza nacional (Choucri 2013), en la política nacional e internacional en diferentes grados (Nye Jr. y Welch 2013), en la integridad de la economía y en la protección de la información de sus ciudadanos (Government of Canada 2010). El Estado y sus instancias regionales deben afrontar el reto de la seguridad y defensa del ciberespacio, así como proteger y garantizar el acceso, uso y contenidos a la sociedad civil en el ámbito virtual, siendo conscientes de su repercusión local, nacional y global.

El académico australiano James Der Derian (2009) advierte cómo estas nuevas prácticas tecnológicas en el ciberespacio median y dominan las relaciones entre Estados y otros actores del mundo internacional. De hecho, dotan de una nueva materialidad a las rela-

4 Empresa comercial estadounidense de entretenimiento que proporciona mediante tarifa plana mensual *streaming* (flujo) multimedia (principalmente, películas y series de televisión) bajo demanda por Internet.

5 Sitio web en el cual los usuarios pueden subir y compartir vídeos.

6 Software que permite comunicaciones de texto, voz y vídeo sobre Internet (VoIP).

ciones de poder, por lo cual urge considerar factores asociados tales como: la simulación, la vigilancia y la velocidad, que exigen evaluar las implicaciones de lo que él denomina como *las nuevas tecno-deidades* (Der Derian 2009, 45). Para ganar claridad expositiva, esta revolución en el tratamiento de la información ha marcado nuevos ritmos en el balance del poder en el mundo entre individuos, organizaciones públicas y privadas, y los Estados, pero a la par ha generado competencia por su control, aprovechamiento y predominio.

Muchos casos nos permiten advertir su presencia y consecuencias. Durante la denominada "Primavera árabe", las redes sociales fusionaron diversas ideas que produjeron la participación de varias comunidades en actos disonantes en contra de sus gobiernos (Libia, Egipto, Marruecos, Argelia, Irak, entre otros), lo que derivó en cambio de autoridades y en la guerra misma. Otro caso, fueron las protestas del movimiento Zapatista en México, que recibieron apoyo y respaldo de personas alrededor del mundo, permitiendo a los activistas comunicarse directamente con millones de personas (Feenberg 2009).

Asimismo, las revelaciones de Snowden permitieron confirmar que la información secreta de los Estados y/o la información confidencial de individuos, es recopilada y almacenada, con el fin de obtener ventajas políticas y económicas, lo que evidencia la legitimación paulatina de la inteligencia como antidiplomacia (Cepik 2003). Los ataques virtuales de individuos o grupos dirigidos a objetivos nacionales, han producido grandes pérdidas económicas (Klimburg 2012) o la paralización del país en sí mismo, como lo sucedido en Estonia en el 2007.

Los eventos anteriormente nombrados, nos demuestran que los conflictos (inciertos e indefinidos aún) pueden generarse desde el mundo virtual. De acuerdo a Feenberg (Feenberg 2009, 77-83), las TIC tienen la habilidad de reunir a personas alrededor de redes (por su contexto colectivo), enrolando cada vez individuos y despoblando ciudades sin importar el área geográfica, lo que contribuye a crear ambigüedad en el conflicto y sus implicaciones. Esta es la razón por la que muchos países han entendido este fenómeno, definiendo al ciberespacio de distintas maneras: como un concepto orientado a ser una prioridad dentro de su estrategia en el desarrollo nacional (Presidencia del Gobierno de España 2013), como un nuevo dominio de la guerra (The Economist 2010) o como un nuevo campo de batalla sin fronteras y asimétrico (Caro Bejarano 2011).

Por ello, actualmente, para su tratamiento y análisis se ha creado una terminología propia. Este es el caso de la ISO/IEC 27032_2013, [7] que establece varios términos, entre ellos, *ciberataque,* que se refiere a los "intentos para destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo de información" de un estado, de sus organizaciones públicas o privadas, o de sus ciudadanos, en beneficio del atacante, que a su vez puede ser un Estado, una organización o simplemente un individuo. Asimismo, se establece el término *ciberseguridad* con dos acepciones diferentes. La primera, desde un ámbito más estratégico, en la que se identifica la condición de un ciberespacio libre de amenazas, peligros y daños, así como el nivel de riesgo al que están expuestos sus organizaciones y ciudadanos; y la segunda, más operativa, trata de preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, entre otros atributos.

7 Estándar internacional para ciberseguridad.

Finalmente, se establece el término c*iberdefensa*, que se orienta a las acciones de un Estado para proteger y controlar las amenazas, peligros o riesgos de naturaleza cibernética, con el fin de permitir el uso del ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía y la integridad territorial; sin soslayar que en los nuevos escenarios que plantea el ciberespacio, pueden incidir en el momento de trazar rutas estratégicas plausibles para el cumplimiento de las diversas misiones militares de ciberdefensa (Virilio 1995). No cabe duda que a futuro los Estados serán los encargados de decidir en el ámbito de la ciberdefensa, llegando a definir si un ataque virtual a un individuo u organización pública o privada puede comprometer el desarrollo y la supervivencia de la nación. Por ello, consideramos que la ciberseguridad y ciberdefensa han evolucionado de ser temas netamente técnicos, para convertirse en una capacidad estratégica clave en la conducción de un Estado dentro de los diversos niveles de decisión o niveles internacionales cuando se habla de proyectos de ciberseguridad regional (Samper 2015).

Problemática de ciberdefensa y ciberseguridad en el mundo

Como se mencionó anteriormente, los Estados, organizaciones regionales y órganos de seguridad y defensa, han empezado a realizar un cambio en su estrategia con el fin de lograr enfrentar las amenazas en el ciberespacio o al menos disminuir su impacto. Los ejemplos de acciones en cada país son innumerables, entre los que podemos citar: (1) Alemania, con el lanzamiento de su Estrategia de Seguridad Cibernética, la creación de su Centro Nacional de Ciberdefensa y la publicación de su Plan Nacional para la protección de Infraestructuras de información (NPIIP) en el 2011 (Acosta 2009); (2) España, que ha creado un Centro y un Plan Nacional de Protección de las Infraestructuras Críticas en el 2011 y también un Mando Conjunto de Ciberdefensa en el 2013 (Acosta 2009); y (3) Francia, que ha creado una Agencia de Seguridad para las Redes e Información (ANSSI) y una Estrategia de Defensa y Seguridad de los Sistemas de información en el 2011 (Acosta 2009). Algunos países en Latinoamérica no han sido la excepción, pues han realizado esfuerzos para aportar a su estrategia en ciberdefensa y ciberseguridad. Algunos ejemplos son: (1) Colombia, que ha creado el grupo de inteligencia para análisis del ciberespacio en el 2005, el *colCERT* en 2009 y la *Estrategia Integral para Ciberseguridad y Ciberdefensa CONPES* en el 2011 (Acosta 2009) (Ministerio de Defensa Nacional de Colombia 2009); y (2) Perú, que ha creado la *Coordinación de respuesta de Emergencia de Redes Teleinformáticas de Administración Pública peCERT* en 2009 y la *Política y Estrategia Nacional de Ciberseguridad y Ciberdefensa* en el 2013 (Acosta 2009).

Las organizaciones internacionales no se han quedado atrás. También se han esforzado de dotar con modelos o estrategias para la afrontar las amenazas de ciberdefensa y ciberseguridad a los Estados. Han publicado varios documentos o estándares, como la *Guía de la ciberseguridad para los países en desarrollo* (ITU 2007) o el *National Cybersecurity Strategy Guide* (ITU 2011).[8] Ambos son modelos de referencia basados en la valoración de activos,

8 Organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

capacidades, necesidades, amenazas y riesgos en sectores públicos y privados del Estado para construir y ejecutar una estrategia de ciberseguridad nacional. No podemos dejar de hablar de entidades de estandarización como la Organización Internacional de Normalización (ISO)[9], que con sus *Sistemas de Gestión de Seguridad de la Información (SGSI) contenidas en la ISO/IEC 27000, Tecnologías para la seguridad de la Información y Técnicas de Seguridad* pretende dar una propuesta más orientada a los aspectos específicos de seguridad en una entidad u organización (ISO 2012).

A pesar de todas estas propuestas, tanto países desarrollados como no desarrollados no han logrado adaptarse completamente a estos modelos. La razón es simple. Cada país posee diferentes capacidades, presupuestos, activos, infraestructura, gestión política, que de alguna manera no se adaptan adecuadamente a los modelos propuestos, quedando como simples referencias no aplicables.

Al respecto, en Ecuador (al igual que otros países) se evidencia la necesidad de implementar esta capacidad estratégica, lo que evidencia la oportunidad de establecer un modelo local y propio de gobernanza para la seguridad y defensa en el ciberespacio. Se alude al concepto de gobernanza debido a que la inserción de la sociedad de la información en Ecuador ha sido muy rápida en esta última década, integrando las nuevas tecnologías en todas su actividades e infraestructuras críticas, aumentando la dependencia de sus ciudadanos y del Estado a los sistemas de información y las redes -con alcance global-. Por esta razón, se exige una mirada estratégica para plantear un modelo de intervención, gestión y evaluación que permita controlar la seguridad de la información en los procesos, sistemas e infraestructuras que depende el Estado para su economía y desarrollo.

Problemática de ciberdefensa y ciberseguridad en el Ecuador

En Ecuador, el acceso al internet ha registrado un elevado incremento durante los últimos 5 años. Por ejemplo, los datos muestran que en el año 2012 la población ecuatoriana alcanzaba el 22,5% y que en el 2015 se alcanzó el 32,8%, según estadísticas del Instituto Nacional de Estadísticas y Censo (INEC 2016). Estos valores son palpables, cuando observamos que las organizaciones financieras y comerciales (ej. bancos, industrias, turismo, entre otros) han aumentado sus servicios en línea (ej. banca electrónica, transacciones electrónicas, entre otros). Incluso, en las entidades públicas han automatizado sus servicios (ej. pago predial, pago de impuestos, entre otros) y han aumentado la oferta de servicios y productos por Internet (ej. facturación electrónica, sitios de compras, entre otros).

Analizando el incremento mencionado, suponemos que podría deberse a varios motivos, tales como: (1) la creación del plan de gobierno electrónico 2014-2017 (COSEDE 2014), (2) el incremento de controles de calidad a las empresas que prestan servicios de internet por la extinta Supertel[10] (Delgado 2014), (3) la creación de redes comunitarias en zonas rurales (Ministerio Coordinador de Seguridad 2014), (4) las políticas de Gobierno para la transformación productiva y el desarrollo del Ecuador, entre otros. Es importante

9 Organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización.

10 Superintendencia de Telecomunicaciones.

recalcar que para el año 2015, el Ecuador se ubicó en el puesto 82 de 148 economías que aprovechan las TIC para la transformación productiva, desarrollo económico y bienestar de su población, superando a Argentina (100), país que ha sido un referente en avances TIC en América Latina en los últimos años (El Telégrafo 2014).

Esta innegable adopción de tecnologías ha devenido en desarrollo y, a su vez, en problemas de ciberseguridad. Al menos en Ecuador, las estadísticas referentes a violaciones a la seguridad han sido en su mayoría dentro del sistema financiero. Un incremento en sus cifras ha convertido a la ciberseguridad en un tema preocupante, especialmente para la banca ecuatoriana. Por ejemplo, en 2014 se registró un aumento de 37% de robos a la banca virtual, 14% en tarjetas de crédito y 46% en cajeros electrónicos (Ministerio Coordinador de Seguridad 2014). Pero no solo los problemas han sido en los sistemas de la banca. La prensa ecuatoriana también ha sido expuesta a varios ataques en sus sitios web que utilizan el "dominio.ec" (El Universo 2009), de la misma manera, ataques a sitios web del gobierno atribuidos al grupo Anonymous [11] (El Comercio 2012), ataques al sistema informático electoral del Ecuador (Andes 2013), supuestos ataques cibernéticos procedentes de Colombia, Estados Unidos, Rusia, China y Francia sobre cuentas o datos personales de ciudadanos ecuatorianos (El Comercio 2016), así como ataques a twitters y redes sociales de personajes públicos (La República 2014); y portales web de opinión libre (El Universo 2016), entre otros.

11 Seudónimo utilizado mundialmente por diferentes grupos e individuos para realizar en su nombre.

Estrategia propia de ciberseguridad y ciberdefensa

El Gobierno ecuatoriano, en su esfuerzo por minimizar estos problemas, tomó algunas decisiones de tipo político-coyuntural Por ejemplo, conformó un *Centro de Operaciones Estratégico Tecnológico*[12] que operó desde las 12AM del 4 de noviembre hasta las 21PM del 5 de noviembre de 2013, con el fin de realizar un monitoreo de ataques informáticos sobre los equipos de seguridad de varias instituciones públicas (Ministerio Coordinador de Seguridad 2014). Asimismo, se ejecutaron proyectos como: la implementación del Ecucert para el tratamiento de los incidentes Informáticos, iniciado a partir del año 2012.

También se promulgaron políticas más sustentables, como el Acuerdo Ministerial No. 166, emitido por la Secretaría Nacional de la Administración Pública, que obliga a las instituciones públicas (dependientes de la función ejecutiva) a la implementación del *Esquema Gubernamental de Seguridad de la Información (EGSI)*[13] a partir del año 2013 (Ecuador Universitario 2012), en dos fases. Además, dispone el uso obligatorio de las Normas Técnicas Ecuatorianas para la Gestión de Seguridad de la Información, las cuales contemplan un conjunto de directrices para viabilizar la implementación de la seguridad de la información en las entidades públicas. No obstante, han sido muy pocas las que han implementado en parte el esquema y sus medidas, que dan mediada confianza a los ciudadanos de la administración pública.

12 Proyecto adscrito a la Secretaría de Inteligencia encargando del monitoreo equipos de seguridad de varias instituciones y así detectar posibles ataques informáticos.

13 Esquema Gubernamental de Seguridad de la Información (INEN-ISO/IEC 27000/27002).

Paralelamente a lo estipulado en el *Plan Nacional de Seguridad Integral (PNSI) 2014-2017,* la Secretaría de Inteligencia incorpora en su *Plan Estratégico Institucional 2015-2017* el objetivo de "incrementar los mecanismos de ciberseguridad para los sistemas de comunicación estratégicos del estado y la integridad de la información" (Inteligencia 2014) . A la par de estos acontecimientos, el 12 de septiembre de 2014, por el Acuerdo Ministerial No. 281 se crea el *Comando de Ciberdefensa* dentro de las Fuerzas Armadas, con la misión de "proteger y defender la infraestructura crítica e información estratégica del Estado" (El Comercio 2014) mediante operaciones de protección del espacio cibernético, acciones de prevención, disuasión, explotación y respuesta ante eventuales amenazas, riesgos e incidentes (Freire 2016). Sin embargo, hasta el momento no existe un claro registro de la infraestructura crítica y, peor aún, de una definición de la información estratégica. En el mismo año, se anuncia la inclusión de la ciberdefensa como parte del currículo académico de la formación militar, sin concretarse hasta el día de hoy (El Universo 2014).

En esta ambigüedad, cada institución participante ha asumido diferentes aproximaciones o iniciativas basadas no solo en la complejidad de su infraestructura, la interconectividad, las aplicaciones y tecnologías asociadas, sino también en los recursos que se podrían manejar en favor de dichas instituciones. En suma, estos esfuerzos para mejorar la ciberseguridad, ya sean iniciativas puntuales de entidades públicas o políticas gubernamentales, han sido fragmentados, limitados y poco efectivos, generando vulnerabilidades expuestas y tácitas. Por lo tanto, a pesar de contar con una normativa legal específica en la materia y con instancias públicas para el efecto, aún no se tienen consensos y criterios técnico-metodológicos en torno al marco de trabajo o estándares en los que se apliquen los roles de los participantes, las metas y los procedimientos en el uso de tecnologías.

Un estudio previamente realizado por Delgado (2014), confirma que "a pesar de todos los esfuerzos, Ecuador no trabaja en ciberseguridad de manera sistemática con políticas definidas, no tienen un plan de acciones para todas las entidades del país y que todas las decisiones de qué hacer en ciberseguridad recaen en el administrador del sitio web". Esta afirmación llama la atención respecto de la necesidad de establecer lineamientos transversales, que permitan al Ecuador trabajar en forma coordinada entre sus diferentes niveles de decisión y en cada uno de sus sectores estratégicos, para hacer frente a este nuevo escenario. En suma, ha limitado la potencial institucionalización de una gobernanza nacional en ciberseguridad y ciberdefensa.

En este contexto, el debate en torno a la ciberseguridad y ciberdefensa en el Ecuador debe ser enfocado desde los conceptos fundamentales: el Estado, su seguridad, su desarrollo y defensa. Es imprescindible desarrollar una estrategia nacional de seguridad que incluya al ciberespacio y que agregue valor e influya a todos los niveles de decisión; y estos, a su vez, se conecten, de forma matricial, con las normas o estándares que son aplicables, con los sectores estratégicos involucrados, con el método de implementación y con los objetivos de seguridad que se van a plantear.

Aplicar una estrategia implica su inscripción de partida en el marco legal rector del país, que es la Constitución Política de la República del Ecuador, cuyos aspectos esenciales estipula: "garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral" (Art.3,

núm. 8); "el derecho al acceso universal a las tecnologías de información y comunicación" (Art. 16, núm. 16); y "garantizar la seguridad humana…. prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas se encargará a órganos especializados en los diferentes niveles de gobierno" (Art. 393). Posteriormente, analizando los mandatos -entre otros- recogidos en la Ley de Seguridad Pública y del Estado (LSPE) del 2010, la cual "prevé la protección y control de los riesgos tecnológicos y científicos, la tecnología e industria militar" (Art. 2), "es deber del Estado promover y garantizar la seguridad de todos los habitantes, comunidades, pueblos, además de la estructura del Estado(…) a fin de coadyuvar al bienestar colectivo, al desarrollo integral" (Art. 3) "ante circunstancias de inseguridad crítica que pongan en peligro o grave riesgo la gestión de las empresas públicas y privadas responsables de la gestión de los sectores estratégicos, el Ministerio de Defensa Nacional dispondrá a Fuerzas Armadas las protección de las mismas" (Art. 43).

No hay que olvidarnos que el cumplimiento de la Ley de Seguridad Pública y del Estado (2009), el Ministerio Coordinador de Seguridad del Estado, también promulga el Plan Nacional de Seguridad Integral (PNSI) 2014-2017. Este plan se enfoca en el ser humano y la naturaleza, garantizando los derechos humanos y las libertades de los ecuatorianos y, sobre todo, la soberanía y la seguridad nacional, orientación en la cual ya se incluye al ciberespacio. El PNSI apunta a la consolidación de un gobierno eficaz y transparente a través de plataformas tecnológicas, y el desarrollo de capacidades para proteger a sus ciudadanos y sus intereses vitales de ataques virtuales, planteando así el ciberespacio, como nuevo esquema de seguridad frente a las amenazas asimétricas y globales (transnacionales e interméstica). Esta misma Ley, crea el

Tabla 1. Propuesta de conformación del COSEPE

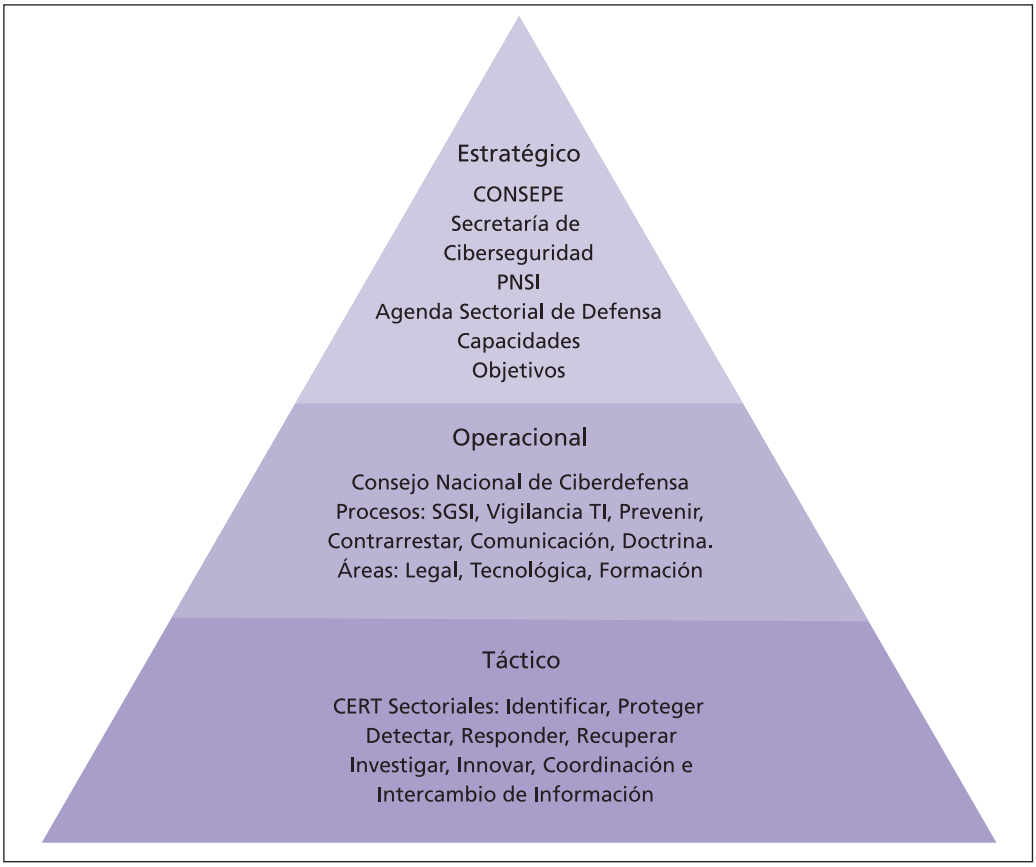
Miembros actuales	Miembros propuestos para tratar asuntos de ciberseguridad
• Presidente de la República • Vicepresidente de la República • Presidente de la Asamblea Nacional • Presidente de la Corte Nacional de Justicia • Ministro Coordinador de Seguridad • Ministro de Defensa Nacional • Ministro del Interior • Ministro de Relaciones Exteriores • Jefe del Comando Conjunto de las FF.AA. • Comandante General de Policía	• Ministerio Coordinador de Sectores Estratégicos • Ministro de Telecomunicaciones y Sociedad de la Información • Ministro de Electricidad y Energía renovables • Ministro de Recursos no renovables • Ministro Coordinador de la Política Económica • Ministro de Justicia, DD.HH y cultos • Secretario General de Gestión de Riesgos • Ministro Coordinador de Producción empleo y • competitividad • Ministro de Conocimiento y Talento Humano • Secretario Nacional de Comunicación • Secretario Nacional de la Administración Pública. • Agencia de Control y Regulación de las Telecomunicaciones • Proveedores de Telecomunicaciones y de Internet • Academia

Sistema de Seguridad Pública y del Estado y estipula la conformación del Consejo de Seguridad Pública y del Estado (COSEPE) para asuntos de Seguridad Nacional.

Ahora bien, consideremos como parte de nuestro planteamiento que para iniciar una discusión nacional de los temas de ciberseguridad y ciberdefensa, es necesario integrar al seno del mencionado Consejo (además de los miembros ya definidos en Ley- primera columna de la Tabla 1) a los representantes de distintas instituciones ecuatorianas (detallado en la segunda columna de la Tabla 1), considerando como énfasis que el ámbito de las TIC es transversal a las organizaciones públicas y privadas del Estado; y que las instituciones citadas en el planteamiento tiene gran relevancia en la gestión de los sectores estratégicos del país y son los órganos rectores de la política pública en sus respectivos ámbitos.

Sobre la base de una estructura piramidal, nuestra sugerencia es que se jerarquice la gestión de la ciberdefensa en tres niveles: nivel estratégico, nivel operacional y/o gerencial, y nivel táctico y/o técnico, tal como se muestra en la figura 1, que corresponde al direccionamiento estratégico de la ciberseguridad y la ciberdefensa en el Ecuador.

Figura 1. Direccionamiento estratégico de la ciberseguridad y ciberdefensa



Además, proponemos que, subordinado al COSEPE en el nivel estratégico, se cree un organismo permanente a nivel Secretaría: la Secretaría de Ciberdefensa, liderada por el Ministerio de Defensa, que será el órgano responsable de la ciberdefensa para el país, incluido en la seguridad nacional. La Secretaría de Ciberdefensa se constituirá como una entidad que se encargará de la planificación estratégica y de la aplicación de una política de investigación, prevención y reacción de defensa contra amenazas cibernéticas, para lo cual deberá cumplir principalmente 5 aspectos:

1) Proponer la organización y funcionamiento de la ciberdefensa, en las siguientes áreas: protección de las infraestructuras críticas, manejo de crisis, ciberterrorismo, ciberdefensa militar, inteligencia y contrainteligencia, y gobernanza en internet y ciberdelitos (Klimburg 2013).
2) Disponer de una red de expertos conformando "observatorios de seguridad de la información" tanto públicos como privados de manera coordinada con cada sector estratégico.
3) Coordinar las actividades de ciberdefensa entre el sector gubernamental, los sectores privados y la población en general, articulando un sistema de intercambio de información y comunicación de incidentes (ISO/IEC27032 2012).
4. Coordinar actividades de ciberdefensa con otros países, yentidades regionales mediante acuerdos y creando estructuras de información de ciberseguridad para propósitos de intercambio (establecido en la Agenda Política de la Defensa).
5. Orientar el desarrollo de políticas del COSEPE, basado en el levantamiento de las "debilidades, vulnerabilidades y riesgos actuales,y sobre los dilemas" (Klimburg 2012) existentes en cada ámbito, como son: estimular la economía versus mejorar la seguridad nacional, modernizar la infraestructura crítica o proteger la infraestructura crítica y protección de los datos o compartir información.

El análisis y la resolución de estos dilemas, permitirán establecer los objetivos de seguridad derivados de las necesidades nacionales mediante un balance entre los significativos de libre flujo de información y las necesidades de seguridad del sector público, sector privado y los ciudadanos en general. Como resultados del accionar de esta Secretaría de Ciberdefensa, se dictarán políticas y objetivos, alineados con el Plan Nacional del Buen Vivir y que deberán estar plasmadas en el PNSI y en las Agendas Sectoriales.

Bajo del nivel estratégico, se propone establecer un *nivel operacional* (ver figura 1) mediante la creación de un Centro Nacional de Ciberdefensa, que gestione los procesos de resiliencia para desarrollar las capacidades para la defensa cibernética; además, se desarrollaría la doctrina para el empleo de los ciber-defensores, apuntalándolos con los mandatos legales, de formación y desarrollo tecnológico. Por ello, el marco de trabajo de ciberseguridad y ciberdefensa debe ser pensado como una articulación de esfuerzos privados y públicos, civiles y militares, requeridos para asegurar un nivel aceptable de ciberseguridad del país. Para garantizar su efectividad, debe ser organizado de forma matricial, en donde un eje determine los niveles de decisión y trabajo, mientras se intercalan con los estándares, los sectores que deben atender, la metodología de aplicación y los objetivos de control que se deben aplicar. El citado alineamiento se esquematiza en la figura 2.

Figura 2. Metodología de aplicación y objetivos de control

Estrategia Nacional (Defensa)	Mejores Prácticas / Estándares Tecnología, Procesos, Gente	Componentes: O.S + Internet Servidores, servidores involucrados	Método de Aplicación	Funciones 4 metas: Crimen, e-commerce, CII, otros
Estrategia por Sector				
Operativo				
Táctico (Técnico)				

Finalmente, en el tercer nivel, nivel táctico (o técnico), se propone la creación de los Centros de Respuesta de Emergencias Informáticas (CERT, por sus siglas en inglés) Sectoriales (financiero, bancario, energía, telecomunicaciones, infraestructuras críticas y organismos públicos estratégicos) que se encargarán de identificar, proteger, detectar, responder, recuperar, investigar, innovar, coordinar e intercambiar información en cada una de las áreas críticas que potencialmente podrían ser afectadas por amenazas que aprovechen el anonimato en el ciberespacio, alineados con los estándares internacionales como: Norma ISO 27000, ISO 27032, ITU, norma de Ciberseguridad del NIST y normas de buenas prácticas como COBIT. En futuros trabajos de investigación, profundizaremos en la investigación y la discusión de los aspectos específicos de cada uno de los niveles planteados, realizando un estudio comparativo con la estructura de ciberseguridad y ciberdefensa de otros países. Desde la perspectiva planteada, se considera de vital importancia el establecimiento de esta metodología de trabajo (planeación-acción), que suponemos permitirá analizar el impacto en la economía, la seguridad pública, y otros servicios, así como también permitirá apalancar nuestras debilidades, sea a través de estándares o buenas prácticas, mejoras en ingeniería de software, inversión en formación, educación y entrenamiento continuo.

Discusión y conclusiones

De lo anotado, se puede desprender que las vulnerabilidades a los ciberataques se continúan ampliando, no solo porque internet se expande rápidamente con más servicios y usuarios, sino también porque el número y la sofisticación de los ciberataques aumenta en una proporción mayor. Si bien el modelo propuesto podría requerir pruebas para evaluar su efectividad, no es menos cierto que en este momento Ecuador requiere un modelo de gobernanza en ciberseguridad y ciberdefensa, que integre y materialice de manera efectiva los esfuerzos aislados, que a lo largo del tiempo no han supuesto una solución global al objetivo de la ciberdefensa y ciberseguridad en el Ecuador. Recordemos que, si bien la seguridad por teoría es tratada individualmente, no es eficiente si no se logra con la participación de todos.

Debemos considerar que el ciberespacio ya es un medio o dominio -militarmente hablando- que aún no se encuentra completamente definido. Nuevas tecnologías emergentes funcionan sobre el ciberespacio y otras continúan apareciendo tal y como ha sucedido con *cloud*

computing, *big data*, telefonía móvil e internet de las cosas. A la par nuevas generaciones de usuarios aparecen, las actuales generaciones evolucionan y otras desaparecen: todo ello, con tal de adaptarse a las plataformas instaladas y sus nuevos desarrollos.

Estas nuevas generaciones tienen que tener claro que acciones del mundo virtual tienen sus consecuencias en el mundo real. Un claro ejemplo, son los problemas causados por los ciberataques, así como las ideas que fluyen en internet, promoviendo percepciones que pueden alterar la paz colectiva y amenazar las soberanías y las estructuras organizacionales. Las redes sociales, hoy por hoy, han probado ser tecnologías emergentes que pueden organizar civiles alrededor de una misma meta, llegando incluso a construir o desorganizar estructuras sociales y políticas de forma impredecible, incontrolable y sin capacidad de anticipación. Con ello, la problemática de seguridad, como consecuencia del uso del ciberespacio, no solo se concentra en temas de técnicos de seguridad en dicho ámbito, sino que implica las consecuencias en el mundo real y sociedad actual, que socaban su continuidad. En suma, es insoslayable buscar soporte internacional para que esta nueva ola tecnológica no afecte objetivos nacionales, desuna pueblos, o atente aldeas o personas que buscan el mismo fin, o a quienes cambian su sentido de pertenencia y lealtad.

El fenómeno está en todos los países del mundo y no solo al nivel del Estado. Sin embargo, para el Ecuador, tras la insuficiente previsión gubernamental en relación al tema, se ha abierto la posibilidad de que se fortalezca la gestión tecnológica de infraestructura e información nacional desde el exterior hacia el país. De ahí que es imprescindible rediseñar la organización de la política de la ciberdefensa en todos sus niveles y la implementación de una S*ecretaría de Ciberdefensa* que permitirá una política de la privacidad y la gestión de la información en la sociedad ecuatoriana y con ello el mejoramiento de la seguridad en la infraestructuras críticas vitales para la propia existencia del Estado y la sociedad ecuatoriana en su conjunto.

Bibliografía

Acosta, Pastor. 2009. "Seguridad nacional y ciberdefensa", catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-Nº-6.pdf.

Andes. 2013. "Sistema informático electoral del Ecuador sufrió ciberataque desde un país del primer mundo", http://www.andes.info.ec/es/noticias/sistema-informatico-electoral-ecuador-sufrio-ciberataque-pais-primer-mundo.html.

Caro Bejarano, María José. 2011. "Alcance y ambito de la Seguridad Nacional en el ciberespacio". En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, coordinado por el Instituto Español de Estudios Estratégicos, 49-82. Madrid: Ministerio de Defensa Nacional – España.

Cepik, Marco. 2003 "Espionagem e democracia", http://professor.ufrgs.br/marcocepik/files/cepik_-_2003_-_fgv_-_espionagem_e_ democracia _21-apr-14_1.compressed.pdf.

Choucri, Nazli, y David Clark. 2013. "Who controls cyberspace?". *Bulletin of Atomic Scientists* 5 (69): 21-31.

COSEDE (Corporación del Seguro de Depósitos, Fondo de Liquidez y Fondo de Seguros Privados). 2014. "Plan de Gobier-

no Electrónico", http://www.cosede.gob.ec/?p=3677.

De Vergara, Evergisto. 2009. *Las diferencias conceptuales entre seguridad y defensa.* Argentina: Instituto de Estudios Estratégicos de Buenos Aires.

Delgado, Andrés. 2014. "Gobernanza de Internet en Ecuador: Infraestructura y acceso", repositorio.educacionsuperior.gob.ec/handle/28000/1579.

Der Derian, James. 2009. *Virtuous war: Mapping the military-industrial-media-entertainment-network*. Londres: Routledge.

Díaz, Fernando Hormazábal. 2005. *El libro blanco de Chile: el problema marítimo boliviano.* Chile: Ediciones Centro de Estudios Bicentenario.

Ecuador Universitario. 2012. "El contexto de la Ciberseguridad", http://ecuadoruniversitario.com/ciencia-y-tecnologia/el-contexto-de-la-ciberseguridad/.

El Comercio. 2014. "Ecuador implementará un Comando de Ciberdefensa". 09 de septiembre, http://www.elcomercio.com/actualidad/ciberdefensa-ecuador-comando-fuerzasarmadas-ministerioddefensa.html.

_____. 2012. "Anonymous inicio ataque a web oficiales en Ecuador". 11 de septiembre, http://www.elcomercio.com/actualidad/negocios/anonymous-inicio-ataque-a-web.html.

_____. 2016. "Hackers de Rusia, China, EE.UU. y Francia dirigen ataques a Ecuador". 29 de octubre, http://www.elcomercio.com/actualidad/hackers-rusia-ecuador-ciberataques-seguridad.html.

El Telégrafo. 2014. "Ecuador escala 9 puestos en ranking de aplicación de las TIC". 25 de abril, http://www.eltelegrafo.com.ec/noticias/tecnologia/30/ecuador-escala-9-puestos-en-ranking-de-aplicacion-de-las-tic.

El Universo. 2009. "Ciberataques a sitios web de Ecuador". 13 de mayo, http://www.eluniverso.com/2009/05/13/1/1431/82615AC354164A25ABE48FCDE222C48E.html.

_____. 2014. "Formación militar prevé ciberdefensa". 21 de mayo, http://www.eluniverso.com/noticias/2014/05/21/nota/2991356/formacion-militar-prevee-ciberdefensa.

_____. 2016. "Tres portales web de Ecuador denuncian ciberataques". 10 de mayo, http://www.eluniverso.com/noticias/2016/05/10/nota/5572110/tres-portales-web-ecuador-denuncian-ciberataques.

Feenberg, Andrew. 2009. "Critical theory of communication technology: Introduction to the special section". *The Information Society*: 77-83.

Feliu, Luis. 2013. *Aproximacion conceptual: Ciberseguridad y Ciberdefensa.* Seguridad Nacional y Cibedefensa. Madrid: Escuela Superior de Ingenieros de Telecomunicaciones.

Freire, Byron. 2016. "Aplicación de la Ciberdefensa en la Seguridad Nacional". *Revista Presencia la Asociación de Generales*: 59-65.

Fridman, Ofer. 2013 *The power of social media: Analyzing challenges and opportunities for the future military operations.* London: SEDTC.

Government of Canada. 2010. *Canada's cyber security strategy: for a stronger and more prospeous Canada*. Ottawa: Minister of public Safety.

INEC (Instituto Nacional de Estadísticas y Censo). 2016. "Tecnologías de la Información y Comunicaciones 2015", http://www.ecuadorencifras.gob.ec/...inec/Estadisticas.../2015/Presentacion_TIC_2015.pdf.

Inteligencia, Secretaría de. 2014. "Plan Estratégico Institucional 2015-2016", www.inteligencia.gob.ec/wp-content/…/05/PlanEstrategico2015-2017Aprobado.pdf.

ISO, 27000.es. 2012. "El portal de ISO 27001 en Español", http://www.iso27000.es/.

ISO/IEC27032. 2012. "Information technology - Security techniques - Guilines for cybersecurity", https://www.iso.org/standard/44375.html.

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

_____. 2011. "National Cybersecurity Strategy Guide", http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

Klimburg, Alexander. 2012. "National Cyber Security Framework Manual". Tallin: NATO CCD COE Publication.

_____. 2013. "National cyber security framework manual", http://https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

La República. 2014. "Ministerio denuncia -atentado a seguridad- de Correa tras ciberataque", http://www.larepublica.ec/blog/politica/2014/03/28/ministerio-denuncia-atentado-a-seguridad-de-correa-tras-ciberataque/.

Ministerio Coordinador de Seguridad. 2014. "Ciberseguridad escenarios y recomendaciones". Revista Digital del Ministerio Coordinador de Seguridad.

Nye Jr., Joseph S., y David A. Welch. 2013. *Understanding global conflict and cooperation: an introduction to theory and history. novena*. Nueva York: Upper Saddle River Pearson.

Presidencia del Gobierno de España. 2013. "Estrategia de ciberseguridad nacional. Madrid". Presidencia del Gobierno.

Real Académica Española. 2011. "Diccionario de la lengua española", http://dle.rae.es/?id=XTrIaQd.

Samper, Ernesto. 2015. "Ciberdefensa en Colombia". *Revisa de Defensa de Colombia* 12.

The Economist. 2010. "Cyberwar: war in the fifth domain", www.economist.com/node/16478792.

Toffler, Alvin, y Heidi Toffler. 1981. *Las guerras del futuro.* Barcelona: Plaza & Janés,

Vargas, Alejo. 2008. "¿Cómo entender la seguridad y la defensa?". *Democracia, seguridad y defensa* 29 (Mayo / Junio): 2-4.

Virilio, Paul. 1995. "Velocidad e información. ¡Alarma en el ciberespacio!", http://ateneu.xtec.cat/wikiform/wikiexport/_media/cursos/curriculum/interniv/dv36/paulvirilio.pdf.