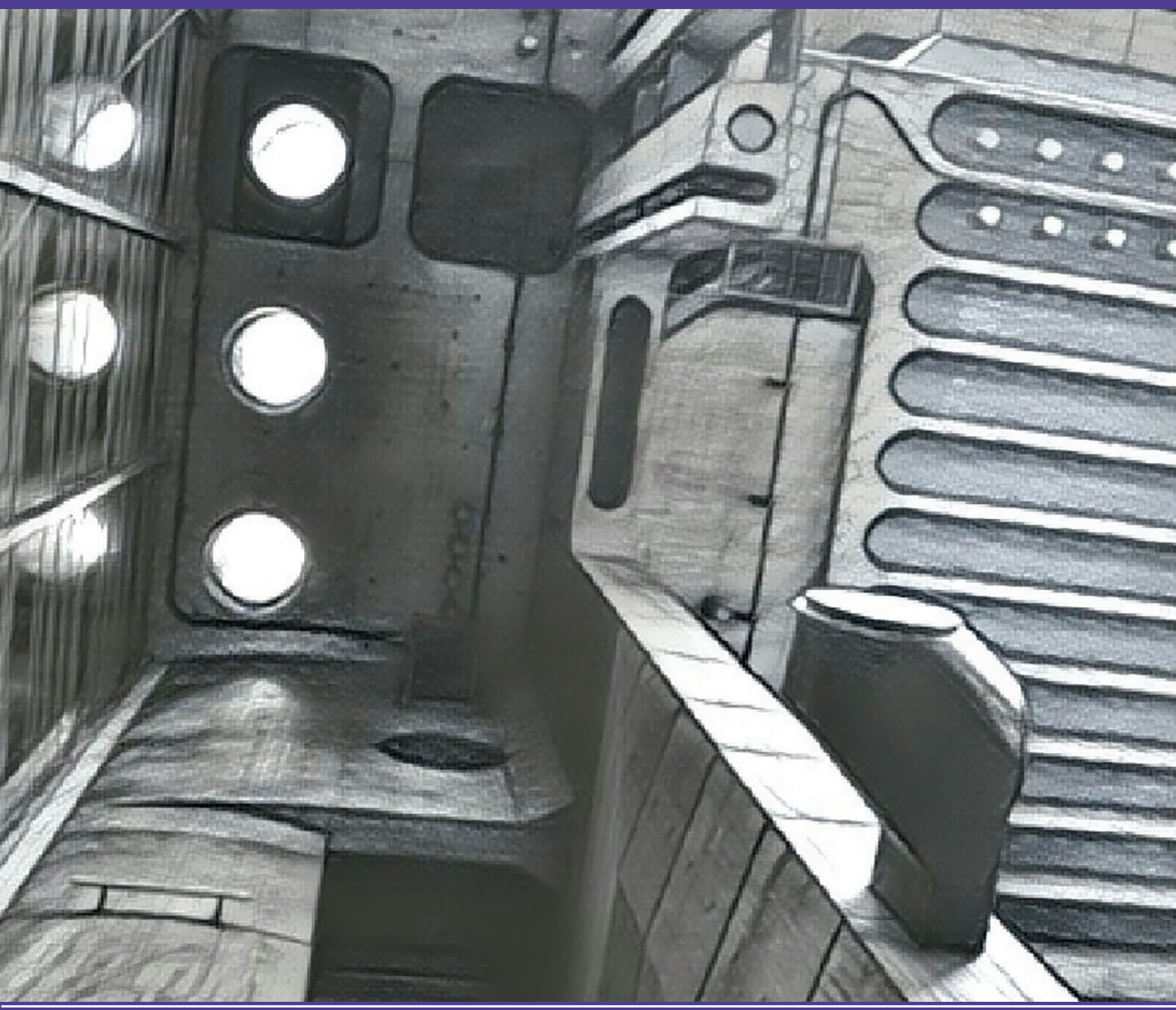
ISSN: 1390-4299
1390-3691

No. 20

URVIO

Revista Latinoamericana de Estudios de Seguridad



Ciberseguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
FLACSO Sede Ecuador • Junio 2017

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Junio 2017 - No. 20

URVIO está incluida en los siguientes índices, bases de datos y catálogos:

- Emerging Sources Citation Index (ESCI). Índice del Master Journal List de Thomson Reuters.
- ERIH PLUS, European Reference Index for the Humanities and the Social Sciences. Índice de referencias.
- JournalTOCS. Base de datos.
- Directory of Research Journals Indexing (DRJI). Directorio.
- Actualidad Iberoamericana. Índice internacional de revistas.
- CLASE, Citas Latinoamericanas en Ciencias Sociales y Humanidades. Base de datos bibliográfica.
- Directorio LATINDEX, Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal.
- DIALNET, Universidad de La Rioja. Plataforma de recursos y servicios documentales.
- EBSCO. Base de datos de investigación.
- FLACSO-ANDES, Centro digital de vanguardia para la investigación en ciencias sociales - Región Andina y América Latina - FLACSO, Ecuador. Plataforma y repositorio.
- REDIB, Red Iberoamericana de Innovación y Conocimiento Científico. Plataforma.
- MIAR (Matriz de Información para el Análisis de Revistas). Base de datos.
- LatAm Studies. Estudios Latinoamericanos. Base de datos.
- Google académico. Buscador especializado en documentación académica y científica.

FLACSO ECUADOR

RELASEDOR
Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada

URVIO, **Revista Latinoamericana de Estudios de Seguridad**
Número 19, diciembre de 2016
Quito - Ecuador

ISSN 1390-4299 (en línea) y 1390-3691

URVIO, Revista Latinoamericana de Estudios de Seguridad, es una publicación electrónica semestral de FLACSO, sede Ecuador, fundada en el año 2007. La revista constituye un espacio para la reflexión crítica, el debate, la actualización de conocimientos, la investigación y la consulta sobre temas vinculados con la seguridad, el delito organizado, la inteligencia y las políticas públicas sobre seguridad en la región.

Disponible en:
http://revistas.flacsoandes.edu.ec/index.php/URVIO
http://www.flacsoandes.org/urvio/principal.php?idtipocontenido=13

El Comité Editorial de URVIO decidirá la publicación o no de los trabajos recibidos, sobre los cuales no se comprometerá a mantener correspondencia. Los artículos serán sometidos a la evaluación de expertos mediante el sistema de doble ciego. Las opiniones y comentarios expuestos en los trabajos son de responsabilidad estricta de sus autoras y autores, y no reflejan la línea de pensamiento de FLACSO, sede Ecuador. Los artículos publicados en URVIO son propiedad exclusiva de FLACSO, sede Ecuador. Se autoriza la reproducción total o parcial de los contenidos siempre que se cite como fuente a URVIO, Revista Latinoamericana de Estudios de Seguridad.

Envío de artículos
revistaurvio@flacso.org.ec

FLACSO, sede Ecuador
Casilla: 17-11-06362
Dirección: Calle Pradera E7-174 y Av. Diego de Almagro. Quito, Ecuador
www.flacso.edu.ec
Telf.: (593-2) 294 6800 Fax: (593-2) 294 6803

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Junio 2017 - No. 20

Tema central

Misceláneo

Entrevista

Reseñas

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Junio 2017 - No. 20

Central topic

Miscellaneous

Interview

Books reviews

Tema central

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2859

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 8-15
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Ciberseguridad. Presentación del dossier

Cybersecurity. Introduction to Dossier

Carolina Sancho Hirare[1]

Fecha de recepción: 24 de marzo de 2017
Fecha de aceptación: 15 de mayo de 2017

La gobernabilidad de todo sistema político requiere al menos considerar tres factores: seguridad como condición, institucionalidad como medio y desarrollo como objetivo. En este contexto, la ciberseguridad constituye una condición para permitir que los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio como dimensión en la cual las relaciones sociales pueden efectuarse en forma más rápida y económica en comparación con otras formas conocidas de intercambio de información.

La ciberseguridad emerge ante el creciente uso del ciberespacio como nueva dimensión para la interacción social, resultado de la revolución de la tecnología de la información y comunicación (TIC), que ha acelerado el proceso de globalización y periódicamente sorprende con su constante innovación. Ejemplo de ello, lo encontramos en el incremento de la cantidad de aparatos conectados al ciberespacio, lo que ha dado origen a la denominada internet de las cosas. Asimismo, la gran cantidad de datos virtuales generados en el ciberespacio ha permitido el desarrollo de "big data" o grandes bases de datos que posibilitan almacenar ingentes cantidades de información y posibilitan el rápido análisis de grandes cantidades de datos de variable naturaleza o formato. El especialista a cargo de estas bases de datos es el "data scientist", un experto cada vez más demandado en el futuro, cuyo principal aporte es dar valor agregado a la información almacenada en "big data" a partir del análisis que puede efectuar en corto tiempo y con recursos limitados.

Estas nuevas tendencias se han potenciado por el aumento sostenido de personas conectadas al ciberespacio. Según cifras de la Unión Internacional de Telecomunicaciones (UIT), en 2015 a nivel mundial, la cantidad de usuarios de internet se ha estimado en un 40% de la población y los abonados a banda ancha móvil serían unos 3.500 millones de personas. Sin embargo, el creciente acceso a este recurso trae aparejado nuevos desafíos. Uno de ellos, es el efectivo uso de todo el potencial de internet, tal como indica la UIT (2016) en el reporte anual "Medición de la sociedad de la información":

1 Doctora en Conflictos, Seguridad y Solidaridad por la Universidad de Zaragoza. Profesora en la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) de Chile. Correo: csanchohirane@yahoo.es

Usuarios de internet con niveles educativos más altos utilizan servicios más avanzados, como los de cibercomercio y los servicios financieros y gubernamentales en línea, en mayor grado que los usuarios de Internet con niveles de educación e ingresos inferiores, quienes usan Internet sobre todo con fines lúdicos y comunicativos.

Por este motivo, no solo es necesario ofrecer acceso a internet, sino también se requiere que las autoridades encargadas de la elaboración de políticas aborden las desigualdades socioeconómicas generales y establezcan medidas que permitan a las personas adquirir las habilidades y competencias necesarias para el uso

Figura 1. Factores de riesgo en el Ciberespacio

Autoría	Objetivos	
	Gobierno	Sector Privado
Ataques patrocinados por otros Estados	Espionaje, ataques contra infraestructuras críticas, amenazas persistentes avanzadas (APT, por sus siglas en inglés)	Espionaje, ataques contra infraestructuras críticas, APT
Ataques patrocinados por privados	Espionaje	Espionaje
Terroristas, extremismo político e ideológico	Ataques contra redes y sistemas; contra servicios de Internet; infección con *malware*; contra redes, sistemas o servicios de terceros	Ataques contra redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Crimen organizado	Espionaje	Robo de identidad digital y fraude
Ataques de bajo perfil	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Ataques de personal con accesos privilegiados (*Insiders*)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT
Impacto	**Alto**	
	Medio	
	Bajo	

Fuente: Instituto de Ciberseguridad de España (2012).

pleno de Internet. La creciente consideración del ciberespacio e internet como un bien público, obliga al Estado a desarrollar acciones necesarias que garanticen condiciones mínimas de seguridad –según estándares internacionales- para que toda la población pueda usarla en forma confiable.

En este sentido, es necesario reconocer que el aumento en el uso del ciberespacio, ha generado ventajas y desventajas para los usuarios. Sus cualidades de facilidad en el acceso, rapidez en la transmisión de la información y bajo costo en la comunicación se ha visto afectado por la existencia de riesgos que han puesto en cuestión la conveniencia de su uso en forma única por parte de personas organizaciones e instituciones, los cuales son sistematizados en la figura 1.

En efecto, periódicamente los ciudadanos reciben información sobre nuevos ciberdelitos ante los cuales muchas veces están desprotegidos, como es el caso del robo de información en formato electrónico; el "phishing" o acceso fraudulento de información personal a través del engaño, como por ejemplo, una clave de acceso a una cuenta desde una página falsa; el "ransomware" o secuestro de datos en el ciberespacio, que para recuperarlos se cobra un monto de dinero, muchas veces en la moneda virtual "bitcoin".

Figura 2. Las principales familias de malware de 2014

Familia de Malware	Descripción
KEYGEN	Genera números de serie para entrar a los programas que requieren números de serie válidos para que los programas funcionen completamente
DUNIHI	Esta Familia de malware normalmente es malware VBS ofuscado que es capaz de propagarse infectando unidades removibles; puede llegar como archivo anexo del correo no deseado.
ACTIVATOR	Quiebra la aplicación y el usuario puede instalarla mutualmente. Sus rutinas le permiten a los usuarios evadir las técnicas de registro y protección de las aplicaciones. Esto les permite utilizar la versión registrada de las aplicaciones.
DOWNAD/ Conficker	Esta explota una vulnerabilidad del servicio del servidor que, cuando es explotada, permite que un usuario remoto ejecute el código arbitrario en el sistema infectado para propagarse a las redes.
CONDUIT	Se incluye en los paquetes de malware como un componente de malware, como un archivo entregado por otro malware, o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
PRODUKEY	Una aplicación que muestra la identificación del producto y la clave del CD de cierto software si se instala en el sistema afectado. Esta herramiento de hackeo puede ser instalada manualmente por el usuario.
SAFNUT	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que lo usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
AGENT	Normalmente trae consigo cargas o realiza otras acciones maliciosos, que van moderando desde moderadamente molestas hasta las irreparablemente destructivas. También pueden modificar las configuraciones del sistema para que se inicie automáticamente. Para restaurar los sistemas afectados podrían requerirse.
CROSSRDR	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
FAKEAV	Crea carpetas en los sistemas afectados y entrega varios archivos, incluyendo una copia de sí mismo y un archivo malicioso. Realiza varios cambios al registro, uno de los cuales permite que se ejecute cada vez que el sistema arranca.

Fuente: Organización de Estados Americanos (OEA) y *Trend Micro* (2015).

Este ilícito, afectó a organizaciones en diversos lugares del mundo en forma simultánea, las cuales no habían actualizado sus equipos con los parches que las empresas de software habían colocado recientemente a disposición de sus clientes.

Se adiciona a lo señalado, las frecuentes noticias sobre ciberataques a diversas organizaciones afectando su normal funcionamiento, por ejemplo, cuando se produce un ataque de denegación distribuida de servicio (DDoS) o cuando un malware del tipo APT afectan los sistemas de supervisión, control y adquisición datos (SCADA) en la infraestructura crítica, como ocurrió con el gusano informático en el sistema de control de los reactores nucleares de Natanz en Irán. La figura 2, permite ilustrar la variedad de malware existentes. En ella son descritas las principales familias de malware detectadas en 2014, las que se han incrementado por mutación o por la aparición de nuevos software maliciosos.

Situaciones como las descritas, obligan a reconocer la importancia de la seguridad en el ciberespacio y asumir su complejidad, pues las amenazas en el ciberespacio pueden tener diversos orígenes (estatal o no estatal), pero el mismo efecto de perjudicar a las personas, dañar a las organizaciones e impedir el normal funcionamiento de instituciones. Asimismo, la existencia de ciberdelito, ciberataques, ciberespionaeje y posiblemente, la ciberguerra (ver figura 3) –no hay consenso entre los expertos en este concepto-, obliga a las máximas autoridades nacionales a contar

Figura 3. Episodios destacados de ciberguerra

Fecha	Denominación	Resumen
1982	Explosión en el sistema de distribución de gas (Unión Soviética)	Los servicios de inteligencia estadounidenses introdujeron una *bomba lógica* en un software de control de infraestructuras gasísticas que había sido robado por espías soviéticos a una empresa canadiense.
2003 2005	Titan Rain	Conjunto de ataques coordinados contra empresas estratégicas e instituciones estadounidenses presumiblemente procedentes de China.
2007	Ciberataque contra Estonia	La retirada en este país de una estatua del período soviético desencadena un conjunto de graves ataques procedentes de Rusia que afectan a las instituciones estatales, bancos y medios de comunicación.
2007	Ciberataque contra Siria	La aviación israelí bombardea una instalación nuclear secreta. El ataque aéreo fue precedido de un ciberataque que engañó a los sistemas de defensa aérea e impidió detectar la incursión de los aviones en el territorio sirio.
2008	Guerra en Osetia del Sur	De manera paralela al conflicto hubo ciberataques coordinados desde Rusia contra sitios gubernamentales de Georgia que quedaron inutilizados y tuvieron que ser reubicados en servidores de otros países.
2010	Stuxnet	Un troyano provoca la destrucción de maquinaria del programa nuclear iraní.

Fuente: Torres (2013).

con políticas públicas que regulen el empleo del ciberespacio y ofrezcan seguridad en su uso, como también el respeto de los derechos de los ciudadanos, los cuales se han visto en cuestionamiento frente a una tecnología capaz de obtener muchos datos sensibles de las personas, pero incapaz de resguardarlos adecuadamente.

Junto a lo indicado, resulta urgente la formulación de políticas públicas y/o estrategias nacionales de ciberseguridad que permitan sistematizar los principales objetivos nacionales e internacionales en la materia, explicitar las acciones que permitirán alcanzarlos y las metas que permitirán constatar su logro. En efecto, los gobiernos de los países son responsables de elaborar políticas que promuevan y garanticen adecuados niveles de ciberseguridad según estándares internacionales, especialmente en lo que dice relación con la protección de la infraestructura crítica de la información a nivel nacional.

Resulta recomendable que tanto las políticas como la estrategia de ciberseguridad sean desarrolladas en un ambiente de participación que contemple al sector público, privado, académico y la sociedad civil, pues condicionará su legitimidad, aspecto fundamental en el éxito de su posterior implementación. Especial mención requiere la participación del sector privado debido a que, según el Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, elaborado en 2015 por la OEA y la empresa *Trend Micro*, "más del 80% de la infraestructura que potencia el Internet y administra los servicios esenciales es propiedad del sector privado y es operada por este".

No obstante, aparecen muchas dudas sobre la forma más adecuada de canalizar constructivamente la participación de los actores señalados. Sin embargo, la experiencia de países como Canadá, EE.UU, Reino Unido, España y Alemania, entre otros, con años de experiencia en el tema puede servir como modelo. Asimismo, buenas prácticas asociadas a la promoción de la coordinación interagencial y la cooperación internacional constituyen aspecto de especial interés en el estudio de caso sobre ciberseguridad.

Lo descrito, permite establecer una serie de problemas, dilemas, desafíos y buenas prácticas que es necesario identificar, analizar y compartir con la finalidad de colaborar en la discusión sobre el nivel de ciberseguridad requerido y el existente para reducir la brecha detectada. Ello cobra especial relevancia cuando se tiene en consideración que un incidente en el ciberespacio tarde o temprano le ocurrirá a todo usuario de éste. La diferencia estará dada por el tiempo demorado en detectarlo, la capacidad para enfrentarlo y la resiliencia para superarlo.

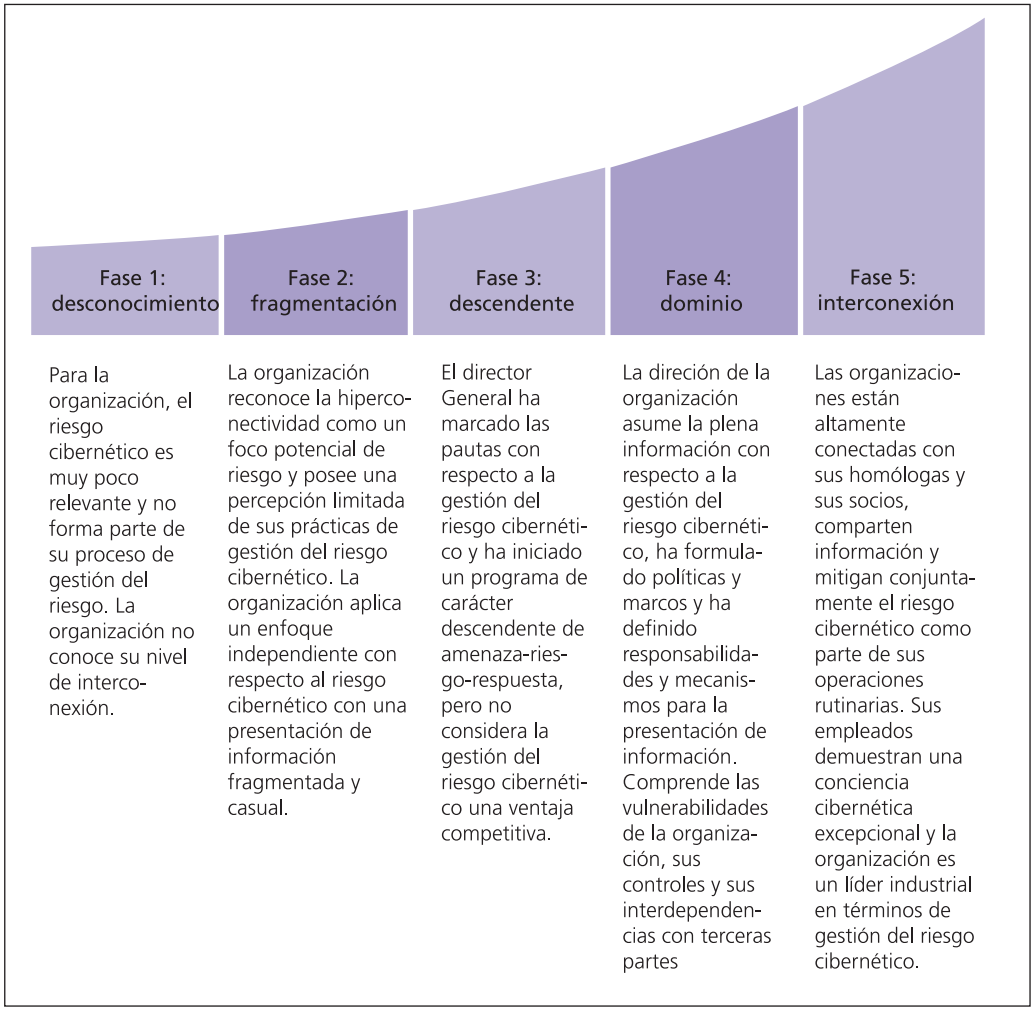
Por este motivo, la OEA, a través del *Comité interamericano contra el terrorismo* (CICTE), aborda los asuntos de Seguridad Cibernética. Ya en el año 2004, los Estados miembros aprobaron la "Estrategia interamericana integral para combatir las amenazas a la seguridad cibernética" en la resolución (AG/RES. 2004 XXXIV-O/04). Desde este organismo se "emplea un enfoque integral en la construcción de capacidades de seguridad cibernética entre los Estados miembros, reconociendo que la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio".

Destacan entre los objetivos que se han propuesto los siguientes:

El establecimiento de grupos nacionales de 'alerta, vigilancia y prevención', también conocidos como *equipos de respuesta a incidentes* (CSIRT) en cada país; crear una red de alerta Hemisférica que proporciona a formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas; promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio (OEA y CICTE 2017).

Ilustra la orientación del trabajo a desarrollar, la XVI Declaración CICTE denominada "Fortalecimiento de la Cooperación y del Desarrollo en la Seguridad Cibernética y la Lucha contra el Terrorismo en las Américas", efectuada en el año 2016. Ello ha justificado la elaboración de un número especial sobre

Figura 4. Modelo de madurez organizacional



Fuente: Foro Económico Mundial (2012).

ciberseguridad. Artículos específicos sobre diversas aristas del tema expuesto buscan ilustrar tanto la complejidad como la diversidad del fenómeno. En este sentido, a continuación, el lector encontrará siete artículos que pueden ser clasificados en dos categorías: por un lado, sobre temas amplios queabordan aspectos de la ciberseguridad que pueden ser aplicados a diferentes situaciones, como es el caso de los ciberdelitos vinculados al ciberterrorismo y la ciberinteligencia; por otro lado, es posible encontrar materias que analizan casos específicos de seguridad en el ciberespacio en países específicos como Ecuador (gobernanza en ciberdefensa), Brasil (política de ciberseguridad), México (video vigilancia en puebla), Venezuela (cibervictimización) y Argentina (ciberdefensa y regulación legal). Se destaca en cada uno de los artículos, la rigurosidad para tratar temas novedosos en los cuales hay poca bibliografía disponible, por lo que constituyen un valioso aporte en la construcción de un acervo de conocimiento con estándares académicos en ciberseguridad.

En síntesis, el ciberespacio es un ambiente de creciente interacción social, que desde una perspectiva política tiende a ser reconocido como un bien público y desde la Defensa ha sido considerado una nueva dimensión o dominio de la guerra. La existencia de riesgos y amenazas obliga a considerar la ciberseguridad como una condición que debe ser provista por el Estado. Los países Latinoamericanos no están eximidos de abordar este tema desde una perspectiva de política pública con la finalidad de ofrecer (garantizar) crecientes niveles de seguridad. Organismos multilaterales como la OEA han elaborado documentos para apoyar a los países en la materia con la finalidad de ayudar a promover la existencia de organizaciones e institucionales que sean maduras desde una perspectiva de ciberseguridad, tal como se ilustra en la figura 4.

Bibliografía

Foro Económico Mundial. 2012. "Asociación por la Resiliencia Cibernética", http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012_SP.pdf.

Karpesky. 2015. "Los riesgos futuros: protéjase", acceso el 5 de mayo de 2017, http://go.kaspersky.com/rs/802-IJN-240/images/APT_Report_ONLINE_AW_ES.pdf.

OEA (Organización de Estados Americanos) y CICTE (Comité Interamericano contra el Terrorismo). 2017. "Seguridad cibernética", https://www.sites.oas.org/cyber/Es/Paginas/default.aspx.

OEA (Organización de Estados Americanos) y Trend Micro. 2015. "Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas", https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf.

Sancho, Carolina. 2016. "Ciberespacio bien público mundial en tiempos de globalización: Política pública de ciberseguridad una necesidad imperiosa y la ciberdefensa como desafíos en el siglo XXI". Ponencia presentada en *XVII Conferencia de Directores de Colegios de Defesa Ibero*-americanos, Brasil, 3 y 7 de octubre.

Torres, Manuel. 2013. "Ciberguerra". En *Manual de Estudios Estratégicos y Seguridad In-*

ternacional, coordinado por Javier Jordán, 329-348. España: Plaza y Valdés.

UIT (Unión Internacional de Telecomunicaciones). 2014. "Medición de la Sociedad de la Información 2014. Resumen Ejecutivo", https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS_2014_Exec-sum-S.pdf.

_____. 2015. "Medición de la Sociedad de la Información 2015. Resumen Ejecutivo", https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-S.pdf.

_____. 2016. "Measuring the Information Society Report 2016. Key findings", acceso el 6 de mayo, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-KeyFindings.pdf.

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2576

URVIO, Revista Latinoamericana de Estudios de Seguridad. No. 20, Quito, junio 2017, pp. 16-30
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea)

La política brasileña de ciberseguridad como estrategia de liderazgo regional

The brazilian cybersecurity policy as a strategy of regional leadership

Luisa Cruz Lobato[1]

Fecha de recepción: 13 de febrero de 2017
Fecha de aceptación: 26 de abril de 2017

Resumen

El artículo analiza la estructuración de la política de ciberseguridad de Brasil entre los años de 2003 y 2016 como componente de su estrategia de inserción internacional y proyección de liderazgo en el Sul Global. El campo de la gobernanza de la Internet, de lo cual la ciberseguridad es parte, ofrece al país una oportunidad de relativo bajo costo de protagonismo en la elaboración de normas internacionales. Analizase documentos principales de esa política y argumentase que ella es parte de los esfuerzos de proyección del *soft power* del país en el campo de la seguridad internacional, pero que sus incoherencias pueden afectar y hasta mismo comprometer esta estrategia. Por fin, trazase breves proyecciones para esta política ante los cambios políticos en Brasil.

Palabras clave: Brasil; ciberseguridad; gobernanza de internet; liderazgo regional.

Abstract

The article analyzes the structuration of Brazil's cybersecurity policy between the years of 2003 and 2016 as a component of its strategy of international insertion and projection of leadership in the Global South. The Internet governance field, of which cybersecurity is a part, offers the country a relatively low-cost opportunity of protagonism in the elaboration of international norms. It analyzes cornerstone documents of this policy and argues that it is a part of the country's efforts to project its *soft power* in the field of international security, but that its incoherencies can affect and even compromise the strategy. Finally, it draws brief projections to this policy in face of political changes in Brazil.

Keywords: Brazil; cybersecurity; internet governance; regional leadership.

1Estudiante del Doctorado en Relaciones Internacionales de la Pontificia Universidad Católica de Rio de Janeiro (PUC-Rio) y Máster en Relaciones Internacionales con mención en Política Internacional por la misma institución. Investigadora visitante del grupo de práctica jurídica en Derechos Humanos del Centro Universitário do Pará (CESUPA). Correo: l.cruzlobato@gmail.com

Introducción

La "revolución digital" en Latinoamérica ha sido poco homogénea y significativamente desigual. Los principales desafíos comunes para la región incluyen la mejora de las condiciones de acceso a la red –apenas la mitad de la población está conectada a internet – y la poca atención dada a la ciberseguridad. Según el Banco Interamericano de Desarrollo, cuatro de cada cinco países latinoamericanos carecen de una estrategia de ciberseguridad (BID 2016). A diferencia de la mayor parte del subcontinente, en las últimas décadas se presenció el esfuerzo de Brasil para estructurar una política propia de ciberseguridad motivada en parte por las amenazas percibidas tras el exponencial crecimiento de usuarios de internet en el país y en parte por su envolvimiento activo con la agenda internacional de gobernanza de Internet.

La agenda de ciberseguridad se muestra bastante atractiva a los intereses estratégicos del país (Diniz, Muggah y Glenny 2014). Sin embargo, la política brasileña enfrenta significativos desafíos, tales como el problema de la especificación de las amenazas y la implementación y administración de esta política en la práctica. El objetivo de este artículo es analizar la arquitectura institucional y los principales instrumentos normativos de la política brasileña de seguridad cibernética para comprender su inserción en la estrategia de proyección internacional del país. Se argumenta, que por vía de la exportación de sus experiencias internas con ciberseguridad, Brasil ha intentado proyectar regional e internacionalmente su "soft power" en la agenda de la gobernanza de internet, pero las incoherencias en su política doméstica pueden afectar y hasta comprometer la estrategia.

El artículo se divide en cuatro partes. En la primera, se abordan los temas de gobernanza de internet y ciberseguridad en las relaciones internacionales, discutiéndose la relación entre ambas y argumentándose que la ciberseguridad es un componente fundamental de la gobernanza de Internet, pero posee lógicas de gestión propias (DeNardis y Raymond 2013). En la segunda parte, se analiza la arquitectura institucional y los principales instrumentos normativos que componen la política de ciberseguridad brasileña, señalando sus características y principales problemas. La metodología utilizada comprende un relevamiento de los principales instrumentos normativos y legales que estructuran la política, destacándose la "Estratégia Nacional de Defesa", la "Política Cibernética de Defesa" y la "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Adm*i*nistração Pública Federal (2015-2018)".

En la tercera parte, se analiza el lugar de la ciberseguridad en la estrategia de inserción internacional de Brasil, argumentándose que la política desarrollada internamente es vista como instrumento de proyección de su *soft power*, mediante la exportación de prácticas exitosas, lo que es auxiliado por la actuación del país en procesos de elaboración de normas/prácticas internacionales relativas a la gobernanza de Internet, así como por la respuesta de la estructura existente. En la cuarta y última parte, se traza una breve perspectiva para la ciberseguridad en Brasil tras los cambios políticos recientes en el país.

Gobernanza de Internet y ciberseguridad

En los últimos años, el creciente reconocimiento de la Internet, como una infraestructura básica de soporte económico y social de

las vidas, ha llamado la atención sobre cuestiones relativas a su gobernanza, lo que incluye las funciones, instituciones y sistemas técnicos necesarios para mantenerla operacional y segura (DeNardis y Musiani 2016). Lo que se comprende por gobernanza de Internet abarca desde las cuestiones de infraestructura, coordinación técnica y política relativas al intercambio de información por medio de la red, hasta las disputas y deliberaciones acerca de la manera como ella es coordenada, administrada y modelada para reflejar políticas (DeNardis 2009; Mueller 2010).

Tradicionalmente, el foco de la mayor parte de los estudios sobre el tema han sido el conjunto de instituciones e instrumentos políticos que comprenden la coordinación global del Dominio de Nombres y Números (DNS) y otras atribuciones de normas de configuración (van Eeten y Mueller 2012). Diversas investigaciones han prestado atención a las controversias sobre las tareas realizadas por la Corporación para Nombres y Números Asignados (ICANN), procesos en las Naciones Unidas, a ejemplo de la Cumbre Mundial sobre la Sociedad de la Información (WSIS) y del Fórum para la Gobernanza de Internet (IGF), y en disputas sobre el modelo (multisectorial o multilateral) más adecuado a toma de decisiones políticas para la Internet (Dutton 2015; DeNardis y Raymond 2013; Maciel y Souza 2011). Conceptualmente, la atención de la literatura a las instituciones, al Estado y a la regulación apunta hacia la fuerte influencia de investigaciones jurídicas y de relaciones internacionales en esos dichos estudios (Epstein, Katzenbach y Musiani 2016; Flyverbom 2016).

Definiciones como la de Mueller (2010), para quien la gobernanza de Internet se ha vuelto una plataforma para disputas sobre una gama de políticas informacionales y de comunicación, aclaran la manera de cómo las relaciones internacionales influencian la literatura de la gobernanza de Internet. El autor justifica el uso del término "gobernanza" en razón de su "debilidad" en relación con el concepto de gobierno y lo equipara a su uso en las relaciones internacionales:

> El término gobernanza, sin embargo, ganó circulación en las relaciones internacionales precisamente porque era más débil que gobierno; denota la coordinación y regulación de actores interdependientes en ausencia de una autoridad política global. En las relaciones internacionales, el término gobernanza global sugiere que existe alguna función de dirección y organización, pero que es menos jerárquica y autoritaria (Mueller 2010, 8-9).

Sin embargo, el término "gobernanza de Internet" puede ser engañoso al sugerir la idea de un proceso único (Dutton 2015). La especificidad de cada función de la gobernanza de la Internet, resulta en una forma propia de coordinación y en la participación de actores distintos en ella. Como argumentan DeNardis y Raymond (2013), el proceso de gobernanza de Internet comprende varias clases de tareas diferentes y lo que la mantiene operacional es una costosa coordinación administrativa entre los actores primarios envueltos en estas tareas. En la práctica, esto significa comprender que el control de los "recursos críticos" de la Internet, por ejemplo, el servicio de DNS, no opera de la misma manera que la gobernanza de la ciberseguridad o que la definición de los estandartes de la Internet. En el caso de la ciberseguridad, su operación incluye desde las actividades las compañías de *software* responsables por la corrección de vulnerabilidades en

sus productos hasta la operación de respuestas a problemas de seguridad, lo que incluye las actividades de los Centros de Estudio de Respuestas y Tratamiento de Incidentes (CERTS).

Es posible decir que la ciberseguridad es una de las funciones comprendidas por la agenda de la gobernanza de Internet (Mueller 2010; DeNardis y Raymond 2013; Oppermann 2014). No se limita a la protección y reacción contra amenazas perpetradas por medio del ciberespacio, lo que incluye el uso de una serie de medidas utilizadas para evitar que un sistema sea comprometido por terceros. También responde a problemas de seguridad en Internet, como ataques de denegación de servicio, asegura la protección de datos de la identidad y el correcto funcionamiento de los sistemas digitales (Nissenbaum 2005; Deibert y Rohozinsk 2010). De una perspectiva más técnica, la ciberseguridad aún abarca el desafío de asegurar las infraestructuras necesarias al funcionamiento de la Internet, lo que incluye, además de ofrecer respuestas a problemas de seguridad en Internet, el enrutamiento, la autenticación de sistemas y el DNS (DeNardis y Raymond 2013).

En las últimas décadas, el tema recibió vasta atención en la literatura de las relaciones internacionales (Barnard-Wills y Ashenden 2012; Dunn Cavelty 2008; 2012; 2015; 2016; Deibert 2011; 2013; Deibert y Rohozinski 2010; Eriksson y Giacomello 2009; Hansen y Nissenbaum 2009; Nissenbaum 2005). Una cartografía hecha por Dunn Cavelty (2016), sugiere que la mayor parte de la producción académica en la disciplina puede ser dividida en los siguientes grupos: un grupo de trabajos producidos por expertos enfocados a discutir la formulación de políticas, generalmente en el ámbito de los "think-tanks" (CSIS 2008; 2010; Ablon, Libicki y Golay 2014), estudios críticos enfocados en la relación entre información y poder (Day 2001), estudios sobre la producción de inseguridad en la Internet a partir de prácticas de vigilancia y censura (Deibert *et al.* 2010) y estudios sobre la constitución de amenazas en el ciberespacio (Dunn Cavelty 2008; Hansen y Nissenbaum 2009; Betz y Stevens 2013).

En determinados países, la recurrente asociación entre riesgos y vulnerabilidades digitales y la seguridad nacional, así como el constante énfasis en la posibilidad de ciberataques catastróficos, los cuales son simbolizados por escenarios donde las infraestructuras críticas de un país son comprometidas por ellos, han puesto las amenazas a la ciberseguridad en una condición de peligros calamitosos, inminentes y urgentes, llevando a un proceso de securitización de esas amenazas. Esa interpretación de las amenazas cibernéticas ha generado críticas por ser considerada extremamente improbable (Rid 2012), así como considerables preocupaciones con el recurso a la militarización del ciberespacio como respuesta a ellas (Dunn Cavelty 2012). Recientemente, se ha dado renovada atención al lazo entre gobernanza de Internet y la ciberseguridad, desde que los problemas de ciberseguridad han desafiado cada vez más las instituciones existentes de gobernanza de Internet, a ejemplo de los conflictos de jurisdicción y tentativas de control de diferentes Estados sobre los servicios de Internet (Mueller, Schmidt y Kuerbis 2013; Mueller y Klein 2014; Internet Governance Project 2016).

Es relevante establecer la asociación entre ciberseguridad y gobernanza de la Internet, pues ella proporciona un punto de partida para el análisis del desarrollo de la política de ciberseguridad en Brasil, así como resaltar sus características y principales problemas. Esto

porque comprender la ciberseguridad como una función de la gobernanza de Internet permite entender la participación de Brasil en esas agendas a partir de una estrategia amplia de inserción internacional puesta en práctica por el gobierno brasileño entre los años 2003 y 2015 y que ha priorizado las relaciones Sur-Sur y la proyección política de Brasil como un liderazgo regional y del "Sur Global". Esa estrategia y sus limitaciones, a su vez, pueden ser mejor explicadas y comprendidas tras un análisis cuidadoso de los principales puntos y características de la política brasileña de ciberseguridad.

La política de ciberseguridad de Brasil

La política de ciberseguridad brasileña se ha desarrollado en un contexto de creciente preocupación con el incremento en el número de ataques cibernéticos y por la capacidad del país de hacer frente a ellos, así como por la oportunidad de no quedar detrás de las principales potencias mundiales en el enfrentamiento de las amenazas cibernéticas (Abdenur 2014). Brasil está en la lista de los países más *atingidos* (golpeados) por el cibercrimen tanto por origen de actividades criminales, como por el número de víctimas de esas actividades (Muggah y Thompson 2015). En 2013, diversos sitios del gobierno federal fueron blancos de ataques cibernéticos y en el mismo año, el país se descubrió afectado por las actividades de espionaje en masa de los EEUU. Esos eventos fueron acompañados de un creciente número de individuos en el país con acceso a la Internet: hoy, cerca de 67.5% de su población se encuentra conectada (Internet World Stats 2016).

En función de ese escenario y del intenso envolvimiento de Brasil con las agendas internacionales de ciberseguridad y gobernanza de Internet, se vuelve importante comprender el proceso de desarrollo y las características de su política de ciberseguridad, así como señalar sus posibles incongruencias. Para este fin, el análisis se centra principalmente en tres documentos: la "Estratégia Nacional de Defesa" (END), la "Política Cibernética de Defesa" (PCD) y la "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (2015-2018)" (Estrategia de Ciberseguridad) y se utilizan también estudios sobre la estrategia de seguridad de Brasil para el ciberespacio como bibliografía secundaria.

Arquitectura institucional

Los esfuerzos de defensa y seguridad cibernéticas en Brasil suceden en un contexto de iniciativas de reestructuración interna y fortalecimiento de la capacidad de defensa nacional iniciada en 1999 con la creación del Ministerio de la Defensa (Abdenur 2014). La estructura de la ciberseguridad hoy es descentralizada, o sea, no hay un liderazgo central que coordine el tema en el gobierno, y orbita en torno de la distinción a nivel conceptual e institucional entre seguridad y defensa cibernéticas: la primera comprende la prevención y represión, mientras la segunda se refiere a las acciones operacionales de combates ofensivos (Mandarino Junior y Canongia 2010; Cruz Júnior 2013).

En el ámbito del Gobierno Federal se establece un sistema jerárquico para la toma de decisión estratégica desde la Presidencia de la República hasta el nivel operacional, cuyas acciones en materia de seguridad cibernética son coordinadas por el "Gabinete de Segu-

rança Institutional da Presidência da República" (GSI-PR), mientras la coordinación de la defensa queda a cargo del "Centro de Defesa Cibernética" (CDCiber), vinculado al Ejército brasileño y al Ministerio de la Defensa. A pesar de que ambos están jerárquicamente abajo de la Presidencia de la República, no existe una agencia propia responsable por la implementación de su estrategia y política de ciberseguridad, estando la competencia un tanto dividida entre órganos como el Consejo Nacional de Defensa, que coordina la política y estrategia de defensa nacional, el GSI-PR, el Ejército, mediante el CDCiber, la Agencia Brasileña de Inteligencia (ABIN) y el Ministerio de la Justicia, por medio de la Policía Federal.

El GSI-PR, extinto en 2015 y restablecido por fuerza de la ley 13.341 de 29 de septiembre de 2016, es responsable por prestar asistencia a la Presidencia de la República en asuntos militares y de seguridad, así como coordinar las actividades de inteligencia federal y seguridad de la información. El Departamento de Seguridad de Información y Comunicación (DSIC-GSI), órgano que compone el gabinete, es directamente responsable por la coordinación de acciones de seguridad cibernética, lo que incluye la operación y manutención de un centro de tratamiento de incidentes en las redes de la Administración Pública Federal (APF).

La Estrategia de Ciberseguridad estableció metas de mejoramiento de la seguridad y resiliencia de las infraestructuras críticas y servicios públicos nacionales para el período de 2015 a 2018. Entre los principales objetivos de la Estrategia, se encuentran el aumento del volumen de recursos presupuestarios de la ciberseguridad y una articulación y coordinación más orientadas para el tema en el ámbito de la administración pública. El CDCiber, creado en 2010, volviéndose operacional entre los años de 2011 y 2012. El centro se encuentra entre los niveles estratégico y operacional del gobierno, a vez que es subordinado al Ministerio de la Defensa, lo cual lo somete al GSI-PR. La estrategia del CDCiber incluye actividades cibernéticas en las áreas de la inteligencia, ciencia y tecnología, habilidades operacionales, doctrina y recursos humanos; su misión consiste en la protección de las redes militares y gubernamentales de ciberataques. Entre las actividades y proyectos del centro, están, por ejemplo, la administración de la seguridad de informaciones durante los megaeventos que tuvieran lugar en Brasil entre los años de 2014 y 2016 (Portal Brasil 2015).

La piedra angular de la política de defensa brasileña es la END, presentada por el Ministerio de la Defensa, aprobada por el Decreto nº 6.703 de 18 de diciembre de 2008, y revisada en 2012. El objetivo de la estrategia es elaborar un plan de defensa a medio y largo plazo y, así, modernizar la estructura nacional de defensa. La END ha establecido el ciberespacio, junto a los sectores aeroespacial y nuclear, como estratégico para el desarrollo y autonomía nacionales y ha delegado el liderazgo de la defensa cibernética al Ejército (la Armada y la Fuerza Aérea son encargadas de los programas nuclear y aeroespacial, respectivamente). La versión revisada del documento establece como prioridad el fortalecimiento del CDCiber para que este se convierta en el Comando de Defensa Cibernética de las Fuerzas Armadas. Además del CDCiber, del GSI-PR y de los otros órganos ya mencionados, agregan la política de protección cibernética brasileña: el Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad (CERT), del Servicio Federal de Procesamien-

to de Dados (Serpro), de centros de investigación en asociación con el gobierno y otros órganos responsables por la administración de sistemas.

La "securitización" de la ciberseguridad

La noción de "securitización" en la teoría de las relaciones internacionales dice respecto al movimiento de inserción de un determinado asunto en la agenda de seguridad a partir de su construcción como amenaza existencial o condición de emergencia frente al Estado (Buzan, Waever y Wilde 1998). Una vasta literatura ha discutido el proceso de securitización de la ciberseguridad de manera general (Dunn Cavelty y Jaeger 2015; Hansen y Nissenbaum 2009; Dunn Cavelty 2008; Bendrath, Eriksson y Giacomello 2007; Nissenbaum 2005) y de manera más específica en el caso brasileño (Lopes 2013; Diniz, Muggah y Glenny 2014). Aquí se utiliza el término para hacer referencia a un esfuerzo en curso que comprende desde la politización[2] de un tema hasta su eficaz inserción, o no, en la agenda de seguridad.

El desarrollo de la política de ciberseguridad en Brasil coincide con una serie de percepciones de las amenazas cibernéticas como una cuestión existencial de seguridad (Mandarino Junior y Canongia 2010). El documento oficial más importante en ese sentido, es la END, ya que incluye el asunto entre aquellos estratégicos para el desarrollo y defensa del país (Brasil 2008). La estrategia contextualiza esa necesidad en razón de las vulnerabilidades traídas por los avances tecnológicos de la información, y su adopción por diversos países en el mundo. Ilustran dicho escenario, la proyección de la ciberseguridad en foros internacionales sobre sociedad de la información y gobernanza de Internet, el aumento del número de ataques a redes gubernamentales, así como eventos de amplia repercusión como los ataques cibernéticos contra Georgia (2007) y Estonia (2008), y más tarde, el descubrimiento del *worm* Stuxnet que afectó las operaciones de instalaciones nucleares en Irán (2010).

Los principios de la política de ciberseguridad brasileña están en el Decreto nº 3.505/2000 que instituyó la política de seguridad de la información en entidades y organismos de la APF. El decreto atribuye como presupuestos básicos de la APF la capacitación tecnológica del país para uso de la criptografía en la seguridad y defensa del Estado, así como el fortalecimiento de la seguridad de información. Desde entonces, diversos mecanismos normativos han sido publicados con vista a la regulación de la seguridad de información en el ámbito de la APF hasta la inclusión del sector cibernético en la END y su atribución al Ejército.

El Ministerio de la Defensa aprobó en 2012 la Política Cibernética de Defensa (Portaria Normativa nº3.389/MD de 21 de Dezembro de 2012), que establece los principios, objetivos y directrices para las actividades en ese sector. El hecho de que dos de los tres principales documentos analizados están en el ámbito del Ministerio de la Defensa (y, por consecuencia, del Ejército) ha levantado críticas a un proceso visto como excesivamente militarizado. Uno de los principales argumentos en ese sentido

2 La relación entre securitización y politización comprende un *continuum* que abarca desde la ausencia de un asunto en las políticas estatales y debates públicos, hasta su inserción en estas agendas, cuando entonces el asunto se vuelve objeto de políticas públicas, y posible securitización, cuando el asunto entonces se vuelve amenaza a la existencia del Estado, demandando medidas de emergencia o la toma de decisiones fuera de las reglas ordinarias de los procedimientos políticos. Ver Buzan, Waever y Wilde (1998).

es la existencia de un desequilibrio en la balanza de amenazas y respuestas, lo que resulta en el manejo inapropiado de las amenazas cibernéticas, con un enfoque mayor en aquellas poco probables, como la guerra cibernética, en detrimento de una mejor preparación para enfrentar cuestiones más urgentes, como el cibercrimen (Diniz, Muggah y Glenny 2014).

La división entre seguridad y defensa cibernética desde los principios del tratamiento de Brasil sobre el tema también ha sido criticada. Se argumenta que la separación tiende a fragilizar la seguridad cibernética, pues esta pasa a depender de la afinidad y coordinación de los dirigentes del CDCiber/Ministerio de la Defensa y del GSI-PR, además de favorecer ambas sobre posición de tareas y brechas por indefinición de responsabilidades (Cruz Júnior 2013), lo que hace bastante confusa la arquitectura institucional de la ciberseguridad en el país. Mas aún, la separación institucional entre ciberseguridad (civil) y defensa (militar) no impidió la actuación del CDCiber en los Juegos Olímpicos y Paralímpicos en el país (Portal Brasil 2015).

Fuera del ámbito de la defensa, la Estrategia de Ciberseguridad del GSI-PR establece las principales metas y objetivos estratégicos para las áreas de seguridad de la información y ciberseguridad. Ella fue antecedida por el "Livro Verde sobre Segurança Cibernética no Brasil", que estableció las directrices estratégicas para una política de seguridad cibernética en el corto, medio y largo plazos. La estrategia contiene diez objetivos y se propone, en conformidad con los vectores propuestos en el documento que la procedió, la promoción de Brasil como actor protagonista en la ciberseguridad a partir de inversiones internos en tecnologías de información, la creación de empleos, el establecimiento de asociaciones con el sector privado, la reducción de la dependencia de tecnologías externas, mejorar la gestión de la ciberseguridad en el ámbito de la APF; así como promover la concienciación de la población acerca de la seguridad cibernética, entre otros.

La Estrategia de Ciberseguridad, al igual que los documentos orientados a la defensa ha traído una respuesta, aunque parcial, a la cuestión de que Brasil tenga o no una política de ciberseguridad. Esta respuesta no está libre de críticas, las cuales incluyen su imprecisión y poca consideración de principios de derechos humanos en su aplicación (Artigo 19 2016). Además, los objetivos de la estrategia no hacen referencia directa a su contraparte de defensa, señalando una intención de mantener la separación entre defensa y seguridad cibernética en el conjunto de la política de ciberseguridad brasileña. Por otra parte, tanto la estrategia cuanto su documento predecesor, llaman la atención para el deseo de Brasil, por medio de sus políticas de ciberseguridad, de volverse un jugador internacional en el área (Mandarino Junior y Canongia 2010; Brasil 2015).

Brasil, la ciberseguridad y las relaciones internacionales

En las últimas décadas se ha visto un esfuerzo por parte de Brasil para consolidarse como un jugador relevante en diferentes aspectos de la gobernanza global. El país es parte de un grupo que, en el mismo período, experimentó un crecimiento económico significativo y adquirió influencia política a un nivel internacional (Zakaria 2008; Alden, Morphet y Vieira 2010; Stuenkel 2015). Abrazando el concepto de "Sur Global", Brasil y otros países que pasaban por un proceso similar intentaron pro-

yectar como liderazgos en diferentes negociaciones multilaterales (Stuenkel 2015).

La relevancia de la ciberseguridad para la agenda política brasileña debe ser pensada a partir de su participación en procesos de toma de decisiones y elaboración de normas sobre la gobernanza de la Internet. Brasil ha acompañado el desarrollo del debate desde su principio, abogando por cambios en la arquitectura de la gobernanza de la Internet (Maciel, Zingales y Fink 2015). En la esfera internacional, la intensificación de los debates sobre el asunto acompañó el establecimiento del IGF tras el segundo encuentro de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), en 2005 (WSIS 2005).

Brasil ha participado activamente de todas las ediciones del IGF, habiendo sido su anfitrión en 2003, cuando tuvo lugar en Río de Janeiro y, en 2014, en João Pessoa. En ese proceso, ha defendido el fortalecimiento de un modelo multisectorial de gestión para la Internet (Opperman 2014; Maciel, Zingales y Fink 2015). El modelo multisectorial, comprende el reconocimiento del papel de actores de naturalezas distintas en la estructuración y gestión de la Internet y propone que las discusiones y debates ocurran en un nivel horizontal, en vez de jerárquico. La importancia de ese modelo se asocia al propio desarrollo histórico de la Internet, que al principio funcionaba como una red de comunicación académica entre institutos de investigación en los EEUU en los años de 1960, y más tarde, en los años 1990, vio la participación de actores comerciales y gobiernos aumentar exponencialmente (Castells 2010).

Para defender la agenda, Brasil ha utilizado su propia experiencia con debates multisectoriales en asuntos relacionados a la Internet. El Comité Gestor de la Internet (CGI.br), creado en 1995, es responsable por establecer las directrices para el uso y desarrollo de la Internet en el país, lo que incluye la asignación de dirección "IP" (Internet Protocol) y la administración del dominio de primer nivel ".br"[3], entre otras decisiones administrativas y operacionales. El CGI.br es un órgano de carácter multisectorial en su composición y proceso de deliberación, compuesto por 21 miembros: nueve representantes del gobierno, cuatro del sector empresarial, cuatro de la sociedad civil, tres de la comunidad científica y tecnológica, y un representante de notorio saber en asuntos de la Internet.

Ese compromiso con la agenda de gobernanza de la Internet, fue luego complementado por el crecimiento de la importancia de la ciberseguridad (considerada uno de los tópicos centrales de la gobernanza de Internet por el IGF) para la agenda política del país, y fue motivada por el aumento en el número de personas conectadas a la Internet, acompañado por el aumento en el número de ciberataques contra individuos y entes públicos, y por la proyección global de ese tipo de evento, a ejemplo de lo ocurrido en Georgia, Estonia e Irán. La ciberseguridad puede ser pensada como parte de una tendencia más amplia de expansión del significado de la seguridad internacional en las décadas posteriores a la Guerra Fría, quedándose frecuentemente en la categoría de amenazas no tradicionales (Abdenur 2014). Sin embargo, en las relaciones internacionales no hay consenso acerca de su definición o potencial transformativo, a vista de las discordancias sobre la dimensión de la real amenaza puesta por las amenazas cibernéticas (Abdenur 2014; Rid 2012). Además,

3 Para una relación de todas las atribuciones del CGI.br, ver el Decreto nº 4.829, de 3 de septiembre de 2003.

el reconocimiento del ciberespacio como sitio de conflicto entre naciones y su creciente importancia en las agendas de seguridad de los países (NATO, 2016), señalan la importancia de desarrollar recursos propios para su análisis y tratamiento.

Para Brasil, las tecnologías de la información pasaron a representar una oportunidad de redistribución de recursos para el desarrollo, posibilitando la reversión de la tendencia de concentración de renta por los países desarrollados (Fontenelle 2012; Cruz Júnior 2013; Keohane y Nye 1998). Las políticas de inclusión digital en el país resultaron en un aumento exponencial en el número de personas conectadas a la Internet, lo que no fue acompañado de una concientización de los usuarios sobre los riesgos digitales. Así, el empoderamiento digital ha moldado el ciberespacio brasileño, confiriéndole amplia escala y dinamismo, que incluye la dimensión que el cibercrimen adquirió en el país (Diniz, Muggah y Glenny 2014; Muggah y Thompson 2015).

La gobernanza global de la ciberseguridad es un proceso aún en curso y precisamente por eso, pone oportunidades y desafíos de defensa y política externa para potencias en ascensión que buscan mayor influencia global. La escasez de recursos para inversión, si comparada a la de las principales potencias mundiales y la competición interna con otras agendas políticas y de seguridad, son apuntados como dos de los principales problemas enfrentados en la consolidación de una agenda coherente para la ciberseguridad en Brasil, como en otras potencias en ascenso (Cruz Júnior 2013; Abdenur 2014). Además, se acredita que, por estar en una fase de desarrollo inicial también en el resto del mundo, el momento presenta una oportunidad para que el país se proyecte internacionalmente (Mandarino Junior y Canongia 2010; Cruz Júnior 2013). Si se comparan con los esfuerzos brasileños con otras áreas de la política internacional, como los gastos militares y las operaciones de paz, ambas la gobernanza de Internet y de ciberseguridad aún son percibidas como agendas menos costosas (Diniz, Muggah y Glenny 2014).

Abdenur (2014) nota que hace poco tiempo que las relaciones internacionales comenzaron a tratar de las cuestiones de poder producidas por la ciberseguridad. Sin embargo, la relación entre poder y tecnologías de la información, más ampliamente consideradas, es discutida por Keohane y Nye (1998). Los autores argumentan que esas tecnologías alteran patrones de interdependencia compleja al aumentar la cantidad de canales de comunicación en la política mundial y tienden a volverse importantes recursos de poder en la política mundial. Nye (2004) sostiene que la era de la información aumenta la relevancia del "*soft power*" y que este tenderá a tornarse menos una función de recursos materiales.

La estrategia de proyección del *soft power* es adoptada por Brasil en la agenda de gobernanza de Internet, particularmente considerándose sus esfuerzos para influenciar la elaboración de normas internacionales sobre asuntos que abarcan desde el cibercrimen, con su crítica abierta a la Convención de Budapest e iniciativa para discutir una convención global sobre el tema (Diniz, Muggah y Glenny 2014), hasta su defensa del modelo multisectorial en el IGF. Las revelaciones de Edward Snowden en 2013 acerca de la estrategia de espionaje global de los Estados Unidos, llevaran no solo a una intensificación de los esfuerzos del país para influenciar la elaboración de normas sobre o tema, a ejemplo de la iniciativa conjunta con Alemania de una resolución

sobre privacidad online ante la Organización de las Naciones Unidas, que ha resultado en la designación de un Relator Especial sobre el Derecho a Privacidad, como también en una mayor atención de Brasil para sus vecinos de América del Sur y en los BRICS (Brasil, Rusia, India, China, Sudáfrica). [4]

Regionalmente, se apunta para acuerdos de cooperación en el marco de la Unión de Naciones Suramericanas (UNASUR) y del Consejo de Defensa Suramericano (CDS), entre Brasil, Argentina y Chile (Justibró 2014). En esos acuerdos están incluidos esfuerzos para fortalecer la colaboración en el área cibernética, lo que comprende ampliar la capacitación en seguridad de información y criptografía, métodos y sistemas tecnológicos, así como el intercambio de integrantes de Equipos de Respuestas de Incidentes de Seguridad Informática (CSIRTs, en inglés) y de investigación científica.

Además de los acuerdos bilaterales, Brasil busca aún exportar para sus vecinos el aprendizaje con la actuación del CDCiber en la seguridad de los Juegos Olímpicos de Rio de Janeiro y de la Copa del Mundo de Fútbol. Por otra parte, el establecimiento de la Escuela de Defensa Suramericana (ESUDE) ha sido visto como una oportunidad para la ampliación de la colaboración con defensa cibernética en la región (Abdenur 2014; Ministério da Defesa 2016b). Sin embargo, para que las iniciativas de cooperación e integración regional en Latinoamérica sean exitosas, es relevante que Brasil busque acercarse a sus vecinos, en particular de los países miembros de UNASUR, a fin de construir una visión compartida acerca de las fuentes comunes de seguridad e inseguridad en Sudamérica y de superar los obstáculos a la cooperación para la ciberseguridad en la región (Justribó 2014).

Consideraciones finales

La intensa participación de Brasil en asuntos relacionados a la gobernanza de la Internet le ha otorgado una posición de actor protagonista en el campo. Una de las vías adoptadas por el país ha sido la proyección de políticas relacionadas a la Internet como una estrategia de *soft power*, entre las cuales se encuentra la ciberseguridad (Diniz, Muggah y Glenny 2014). Pero la posición brasileña con relación al asunto, es también influenciada por su condición de potencia en ascensión y por las contradicciones que de eso transcurren: hay una tentativa por parte del país de equilibrar sus aspiraciones de jugar un papel más amplio en la política internacional (particularmente en la seguridad), al mismo tiempo en que hay limitaciones significativas a su capacidad de actuar en el exterior (Abdenur 2014).

La estrategia brasileña para la ciberseguridad y gobernanza de Internet, tiene significativas contradicciones que resultan en gran parte de problemas institucionales y administrativos de sus políticas y de la adopción de prioridades equivocadas. Una división institucional como la establecida en la política brasileña y la falta de principios claros en la estrategia puede llevar a posiciones y actitudes contradictorias, como bien señala el caso de la vigilancia de la ABIN y del CDCiber sobre la población brasileña en ocasión de las protestas de 2013, en total contrapunto a las duras críticas hechas por la presidente brasileña al espionaje estadounidense. Las incohe-

4 Sin embargo, en el caso de los BRICS, la cooperación parece más costosa: paralizada desde 2015, la construcción de un cabo submarino alternativo fuera del occidente está siendo continuada por la China (Lee (2017).

rencias entre la política interna y la posición internacional de Brasil, pueden generar tres efectos: afectar significativamente la posición que el país viene intentando intenta construir internacionalmente para sí en la agenda de gobernanza de Internet, debilitar los esfuerzos existentes de integración y cooperación regional en Latinoamérica, y dejar su política de ciberseguridad más susceptible a cambios políticos internos y externos.

Tras los cambios políticos que resultaron de la destitución de la presidente Dilma Rousseff, hubo esfuerzos para reestructurar el sector de inteligencia bajo la coordinación del nuevo GSI-PR. La Estrategia de Ciberseguridad esta mantenida bajo la nueva coordinación del órgano, mientras que la política de defensa debe pasar por un proceso de revisión periódica en lo cual, al que todo indica, la ciberseguridad debe mantener su importancia estratégica (Ministério da Defesa 2016a). Asimismo, en noviembre de 2016, el GSI-PR y el Ministerio de la Defensa anunciaran estar en vías de construir una estrategia conjunta de cooperación interministerial para la seguridad y defensa, en la cual la agenda cibernética es considerada una de las prioridades. No hay indicativos de cambios sustantivos en la arquitectura institucional de la ciberseguridad en el gobierno al corto y mediano plazos y la tendencia es su manutención, con todos los problemas de atribución que la acompañan.

Es deseable que Brasil desarrolle una política de ciberseguridad más coherente con los problemas de seguridad que enfrenta y que esté más atenta al escenario regional, y que se coopere con el sector privado para reducir los costos del cibercrimen no solo para las empresas, también para el usuario de Internet. Superar la fragmentación en su arquitectura institucional es fundamental para que las iniciativas de ciberseguridad en el país y en cooperación con sus vecinos sean más coherentes. Investigaciones futuras en el área de ciberseguridad, deben considerar no apenas esfuerzos en ese sentido, como también las iniciativas de cooperación regional e internacional del país en materia de ciberseguridad, así como la participación del sector privado tanto en la estrategia nacional cuanto en la construcción de un papel global más protagonista para el país.

Bibliografía

Abdenur, Adriana. 2014. "Brazil and Cybersecurity in the Aftermath of the Snowden Revelations". En *International Security: a European-South American Dialogue*, 229-283. Río de Janeiro: Konrad-Adenauer-Stiftung.

Ablon, Lillian, Martin C. Libicki y Andrea A. Golay. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* Santa Mónica: RAND.

Alden, Chris, Sally Morphet y Marcos Antonio Vieira. 2010. *The South in World Politics.* Basingstoke: Palgrave Macmillan.

Artigo 19. 2016. *Brasil: Análise da Estratégia de Cibersegurança.* São Paulo: Artigo.

Balzacq, Thierry. 2011. "A theory of securitization: origins, core assumptions, and variants". En *Securitization theory: how security problems emerge and dissolve*. Nueva York: Routledge.

Barnard-Wills, David, y Debi Ashenden. 2012. "Securing Virtual Space: Cyber War, Cyber Terror and Risk". *Space and Culture*: 110-123.

Bendrath, Ralf, Johan Eriksson, e Giampero Giacomello. 2007. "From 'cyberterror-

ism' to 'cyberwar', back and forth: How the United States securitized cyberspace". *International Relations and Security in the Digital Age*, J. Eriksson y G. Giacomello, 57-82. Nueva York: Routledge.

Betz, David J., y Tim Stevens. 2013. "Analogical reasoning and cyber security". *Security Dialogue*: 147-164.

BID (Banco Interamericano de Desarrollo). 2016. "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?", https://publications.iadb.org/handle/11319/7449?locale-attribute=es&.

Brasil. 2015. *Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018.* Brasilia: Presidência da República.

_____. 2012. *Política Cibernética de Defesa.* Brasilia: Ministério da Defesa.

_____. 2008. *Estratégia Nacional de Defesa.* Brasilia: Ministério da Defesa.

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

Castells, Manuel. 2010. *The rise of the network society.* Malden: Blackwell.

Cruz Júnior, Samuel Souza da. 2013. *A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual.* Río de Janeiro: IPEA.

CSIS. 2010. *Cybersecurity two years later: a report of the CSIS Commission on Cybersecurity for the 44th Presidency.* Washington DC: Center for Strategic and International Studies.

CSIS. 2008. "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency". Center for Strategic and International Studies, Washington DC, 90.

Day, Ronald E. 2001. *The Modern Invention of Information: Discourse, History and Power.* Carbondale: Southern Illinois University Press.

Decreto nº4.829/2003, de 3 de setembro, dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil e dá outras providências (D.O.U de 4 de setembro de 2003).

Decreto nº3.505/2000, de 13 de junho, institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal (D.O.U de 14 de junho de 2000).

Deibert, Ronald J. 2013. *Black Code: inside the battle for cyberspace.* Oxford: Signal.

_____. 2011 "Tracking the emerging arms race in cyberspace". *Bulletin of the Atomic Scientists* 67 (1): 1-8.

Deibert, Ronald J., y Rafal Rohozinski. 2010. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology*: 15-32.

DeNardis, Laura, y Francesca Musiani. 2016. "Governance by infrastructure". En *The turn to infrastructure in Internet governance*, 3-24. Londres: Palgrave MacMillan.

DeNardis, Laura. 2009. *Protocol Politics: The Globalization of Internet Governance.* Cambridge: MIT Press.

DeNardis, Laura, y Mark Raymond. 2013. "Thinking Clearly about Multistakeholder Internet Governance". *Eighth Annual GigaNet Symposium*, 21 de Octubre.

Diniz, Gustavo, Robert Muggah y Misha Glenny. 2014. "Deconstructing cyber security in Brazil: Threats and responses". Strategic Paper 11: 3-32.

Dunn Cavelty, Myriam. 2012. "The Militarisation of Cyberspace: Why Less May Be

Better". *4th International Conference on Cyber Conflicts*, 141-153.

_____. 2016. "Cyber-security and private actors." Em *Routledge Handbook of Private Security Studies*, Abrahansen, Rita y Anna Leander. eds. Nueva York: Routledge.

_____. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* . London: Routledge.

_____. 2015. "The Normalization of Cyber-International Relations." Em *Strategic Trends 2015: Key Developments in Global Affairs*. CSS.

Dunn Cavelty, Myriam., y Mark Daniel Jaeger. 2015. "(In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous". *International Political Sociology*: 176-194.

Dutton, William H. 2015. "Multistakeholder Internet governance?". *Background Paper: Digital Dividends*.

Epstein, Dmitry, Christian Katzenbach, y Francesca Musiani. 2016. "Doing internet governance: practices, controversies, infrastructures, and institutions". *Internet Policy Review*.

Eriksson, Johan, y Giampero Giacomello. 2009. "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State". *International Studies Review*, 205-230.

Flyverbom, Mikkel. 2016. "Disclosing and concealing: internet governance, information control and the management of visibility". *Internet Policy Review, 30 de septiembre.*

Fontenelle, Alexandre S. 2012. "O Espaço Cibernético na Agenda Internacional". *ECEME, XI Ciclo de Estudos Estratégicos*.

Gonzaga, Alexandre. 2016. "Jungmann apresenta ao presidente Temer a revisão dos documentos de defesa", http://www.defesa.gov.br/noticias/24840-jungmann-apresenta-ao-presidente-temer-a-revisao-dos-documentos-da-defesa.

Hansen, Lene., y Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly*: 1155–1175.

Internet World Stats. 2016. "Internet usage and population in South America", http://www.internetworldstats.com/stats15.htm.

Justribó, Candela. 2014. "Ciberdefensa: una visión desde la UNASUR", http://www.congresos.unlp.edu.ar/index.php/CRRII/CRRIIVII/paper/view/1849/422.

Keohane, Robert., y Joseph Nye. 1998. "Power and Interdependence in the Information Age". *Foreign Affairs* 77 (5): 81-94.

Lee, Stacia. 2017. "The Cybersecurity Implications of Chinese Undersea Cable Investment". *The Henry M. Jackson School of International Studies*.

Lopes, Gills. 2013. "Securitizando o ciberespaço: um estudo comparativo sobre a defesa cibernética em sete países". *4º Encontro Nacional da ABRI.* Belo Horizonte.

Maciel, Marília Ferreira, y Carlos Affonso Pereira de Souza. 2011. "Multi-stakeholder participation on Internet governance: An analysis from a developing country, civil society perspective". *Association for Progressive Communications*.

Maciel, Marilia Ferreira, Nicolo Zingales, y Daniel Fink. 2015. "NoC Internet Governance Case Studies Series: The Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial) ". *SSRN*.

Mandarino Junior, Raphael, y Claudia Canongia. 2010. *Livro Verde: Segurança Cibernética no Brasil.* Brasília: GSIPR/SE/DSIC.

Ministério da Defesa. 2016a. "Defesa, MRE e GSI aproximam agendas internacionais e criam mecanismo de coordenação", http://www.defesa.gov.br/noticias/26193-defesa-mre-e-gsi-aproximam-agendas-internacionais-e-criam-mecanismo-de-coordenacao.

_____. 2016b. "XII CDMA: Ministro Jungmann defende cooperação regional nas fronteiras", http://www.defesa.gov.br/noticias/25195-xii-cmda-ministro-jugmann-defende-cooperacao-regional-nas-fronteiras.

Mueller, Milton, Andreas Schmidt, y Brenden Kuerbis. 2013. "Internet Security and Networked Governance in International Relations". *International Studies Review*, 86–104.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance.* Cambridge: MIT Press.

Mueller, Milton, y Hans Klein. 2014. "Sovereignty, National Security, and Internet Governance: Proceedings of a Workshop". Syracuse University: Georgia Institute of Technology School of Public Policy.

Muggah, Robert, y Thompson Nathan. 2015. "Brazil's Cybercrime Problem". *Foreign Affairs*.

NATO. 2016. "NATO Cyber Defense Fact Sheet", http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

Nissenbaum, Helen. 2005. "Where Computer Security Meets National Security." *Ethics and Information Technology*, 61-73.

Nye, Joseph. 2004. *Power in a global information age: from realism to globalization.* Nueva York: Routledge.

Oppermann, Daniel. 2014. "Internet governance and cyber security in Brazil". En *International Security: a European-South American Dialogue*, 167-182. Río de Janeiro: Konrad-Adenauer-Stiftung.

Portal Brasil. 2015. "Forças Armadas vão monitorar redes de Internet na Rio 2016", http://www.brasil.gov.br/defesa-e-seguranca/2015/09/forcas-armadas-vao-monitorar-redes-de-internet-na-rio-2016.

Rid, Thomas. 2012. "Cyber War Will Not Take Place". *Journal of Strategic Studies* 35(1).

Stuenkel, Oliver. 2015. *India-Brazil-South Africa Dialogue Forum (IBSA): The Rise of the Global South?* Londres: Routledge.

Van Eeten, Michel JG., y Milton Mueller. 2012. "Where is the governance in Internet governance?". *New Media & Society*: 720-736.

WSIS. 2005. "Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1)-E.", http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

Zakaria, Fareed. 2008. *The Post-American World.* Nova York: W. W. Norton & Company.

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

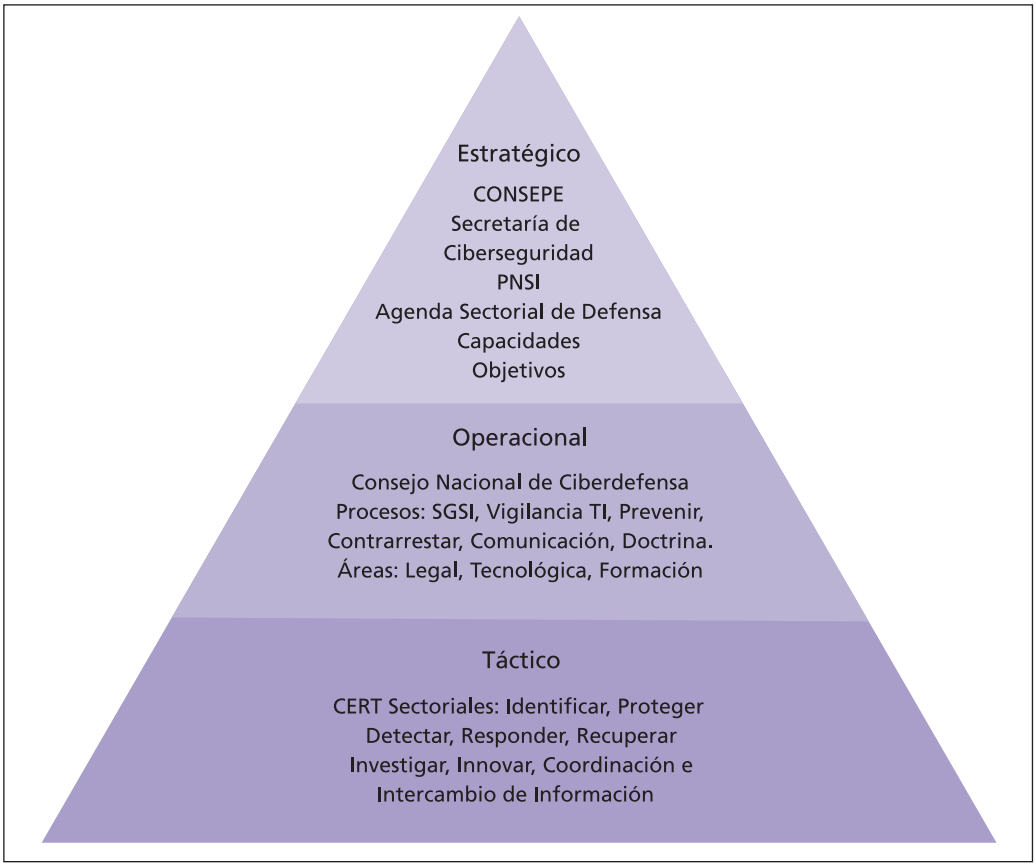
Miembros actuales	Miembros propuestos para tratar asuntos de ciberseguridad
• Presidente de la República • Vicepresidente de la República • Presidente de la Asamblea Nacional • Presidente de la Corte Nacional de Justicia • Ministro Coordinador de Seguridad • Ministro de Defensa Nacional • Ministro del 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.

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2601

Urvio, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 46-62
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

La ciberdefensa y su regulación legal en Argentina (2006-2015)

The ciberdefense and its legal regulation in Argentina (2006-2015)[1]

Silvina Cornaglia[2] y Ariel Vercelli[3]

Fecha de recepción: 20 de febrero de 2017
Fecha de aceptación: 30 de abril de 2017

Resumen

En el artículo se analiza qué lugar ocupa y cómo se desarrolló la ciberdefensa dentro del sistema de defensa de la República Argentina. Para ello, se relevan y analizan las normas que se han producido sobre la temática durante el período 2006 – 2015. El estudio permite observar que dos instituciones han sido las más activas: por un lado, se destacan las regulaciones del Ministerio de Defensa y, por el otro, las regulaciones de la Jefatura de Gabinete de Ministros. La investigación tiene una doble finalidad. En primer lugar, favorecer un mayor nivel de sistematicidad legislativa en materia de ciberdefensa. En segundo lugar, producir información sustantiva para la elaboración de políticas públicas y actividades regionales de colaboración. El artículo es parte de una investigación mayor abocada al análisis de las diferentes formas de regular el ciberespacio.

Palabras clave: ciberdefensa; ciberespacio; leyes; República Argentina.

Abstract

The article analyzes the place and how cyberdefense was developed within the defense system of República Argentina. To this end, the norms that have been produced on the subject during 2006 - 2015 are relieved and analyzed. The study shows that two institutions have been the most active: on one hand, stand out the regulations of the Ministerio de Defensa, and, on the other, the regulations of the Jefatura de Gabinete de Ministros. The research has a double purpose. Firstly, to favor a greater level of legislative systemacy in cyberdefense. Second, to produce substantive information for the elaboration of public policies and regional collaboration activities. The article is part of a larger investigation focused on the analysis of the different ways of regulating cyberspace.

Keywords: ciberdefense; cyberspace; laws; Republic Argentina.

1 La obra intelectual se desarrolló gracias al apoyo de la Escuela del Cuerpo de Abogados del Estado (ECAE), el Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), el Instituto de Estudios Sociales de la Ciencia y la Tecnología (IESCT) de la Universidad Nacional de Quilmes (UNQ) y Bienes Comunes A. C.

2 Especialista en Asesoramiento Jurídico del Estado de la Escuela del Cuerpo de Abogados del Estado (ECAE), Abogada de la Universidad de Buenos Aires (UBA), Miembro del Observatorio de Defensa de la Universidad de la Defensa Nacional (UNDEF). Correo: silvina_cornaglia@hotmail.com

3 Doctor en Ciencias Sociales y Humanas de la Universidad Nacional de Quilmes (UNQ), Investigador de CONICET con lugar de trabajo en el Instituto de Estudios Sociales sobre la Ciencia y la Tecnología (IESCT) y Presidente de Bienes Comunes A. C. Correo: arielvercelli@arielvercelli.org

Introducción: nuevos enfoques sobre la ciberdefensa

La ciberdefensa ha adquirido gran relevancia mundial en las últimas décadas. Los ataques cibernéticos anónimos se han convertido en una fuente constante de amenazas, pues además de atacar las infraestructuras críticas de los países, afectan de forma directa y simultánea a millones de personas (Pastor Acosta *et. al*. 2009; Amaral 2014). El tema se ha transformado en un tema público a través de varios casos resonantes, entre otros, el ataque contra sitios *web* de Estonia en 2007 (diarios, bancos, ministerios), los ataques sufridos en 2010 por las centrifugadoras nucleares iraníes en Natanz mediante el *malware Stuxnet* (Gibney 2016), las filtraciones realizadas por *Wikileaks* (Assange, 2013), las filtraciones sobre ciberespionaje global que realizó Edward Snowden en 2013 (Poitras 2014) o el ataque realizado a través del *ransomware WannaCry* en 2017, que afectó más de 150 países (Rusia, EE.UU., Reino Unido, China, Italia, etc.). Ya es habitual que los medios de comunicación hablen y discutan sobre conceptos técnicos, tales como cibercrimen, ciberterrorismo, ciberespionaje, hacktivismo o ciberguerra (Adkins 2001; Gastaldi 2014).

La importancia de los ataques producidos, las consecuencias imprevisibles que pueden generar, la dificultad de identificar a los autores de los mismos y la carencia de definiciones legales precisas, han puesto a los diferentes gobiernos y a la comunidad internacional a trabajar tanto en sus jurisdicciones como en el ámbito regional y global. Rápidamente, la ciberdefensa comenzó a formar parte de un nuevo escenario de luchas, tensiones, intereses y negociaciones: entre otros, la protección de todo tipo de infraestructuras críticas (redes, recursos y servicios que -en caso de sufrir un ataque- podrían causar gran impacto en la seguridad de la población), el diseño de políticas públicas orientadas fortalecer la seguridad de la información, [4] la soberanía territorial y su particular relación con el ciberespacio (Eissa *et al*. 2014; Gastaldi 2014) o el normal y pacífico funcionamiento administrativo y jurídico-político de los Estados (Ferrero 2013; Illaro 2014).

La ciberdefensa no ha sido ni es materia simple. Se la puede caracterizar por su complejidad y cambio constante. Este es uno de los principales desafíos con que se enfrentan los Estados. Aún no existen convenciones o tratados internacionales que establezcan normas claras sobre la materia. Incluso, en el ciberespacio las tecnologías digitales y las regulaciones se van co-construyendo a través del tiempo y es posible observar que se diseñan tecnologías para producir los efectos de las regulaciones (Vercelli 2009; 2015). Por ello, las estrategias nacionales de defensa y la necesidad de generar nuevas capacidades comenzaron a ser considerados temas centrales y estratégicos dentro de los Ministerios de Defensa y otras agencias gubernamentales. Al respecto, en poco más de una década, es posible observar la aparición de todo tipo de iniciativas e instituciones a nivel mundial[5]: entre otras, el na-

4 En la actualidad, la mayor parte de la información que gestionan los organismos del Estado es procesada digitalmente. La seguridad de la información (o ciberseguridad) bien puede ser considerado un ítem complementario de la ciberdefensa de un país/región. Para Feliu Ortega (2012), la ciberdefensa comprende todas las acciones y medidas necesarias para garantizar la ciberseguridad de todos los sistemas tanto militares como civiles.

5 La Organización del Tratado del Atlántico Norte (OTAN) aprobó en 2008 su política de ciberdefensa. En 2011 realizó una revisión de dicha política y un Plan de Acción de Ciberdefensa. En la Cumbre de Gales, realizada en septiembre de 2014, reconoció la aplicabilidad al ciberespacio de la legislación internacional (incluyendo la legislación internacional humanitaria y la Carta de las Naciones Unidas). La Unión Europea (UE) adoptó una Estrategia de Seguridad Cibernética en febrero de 2013. Los estados miembros de

cimiento de comandos militares, autoridades nacionales/regionales, manuales y protocolos de acción (por ejemplo, el Manual de Tallin[6]) e, incluso, la aparición de grupos de emergencias cibernéticas tanto civiles como militares.[7]

La República Argentina y la Unión de Naciones Suramericanas (UNASUR) no se han mantenido ajenas a estas nuevas dinámicas de problemas. El Consejo de Defensa de la UNASUR ha considerado esta problemática en sus Planes de Acción 2012, 2013 y 2014.[8] A su vez, se incorporaron actividades específicas respecto de políticas, mecanismos y capacidades regionales para hacer frente a las amenazas cibernéticas e informáticas en el ámbito de la defensa. En el Plan de Acción 2015 se incorporó la temática como Grupo de Trabajo Extra Plan de Acción, cuyo objeto fue continuar con el Grupo de Trabajo de ciberdefensa y coordinar con el COSIPLAN[9] la realización de un seminario.[10] Incluso, el 13 de septiembre de 2013, los ministros de Defensa de Argentina y Brasil expresaron en el marco de un encuentro bilateral la importancia de trabajar en conjunto en la materia: incluyeron la ciberdefensa en la Declaración de Buenos Aires[11], acordaron la cooperación en defensa cibernética y la creación de un subgrupo de trabajo bilateral específico.

El sistema de defensa y la ciberdefensa en la República Argentina

En el contexto específico de la República Argentina, es posible identificar abundante normativa y múltiples acciones orientadas a mejorar las capacidades en ciberdefensa. Debido a su alta complejidad, la ciberdefensa no es fácilmente clasificable. Se encuentra aún en una etapa de expansión regulativa, de flexibilidad interpretativa y de amplio debate. Por ejemplo, entre otros puntos salientes, aún no está del todo claro qué significa la ciberdefensa y qué relaciones mantiene con el sistema de defensa nacional (Libro Blanco 2015). En igual sentido, es importante avanzar sobre los siguientes cuestionamientos: ¿Qué actividades representan un ciberataque a nivel nacional, regional o internacional?[12], ¿Cuáles son las instituciones públicas y las autoridades competentes para su gestión? y ¿Cuenta la República Argentina con una legislación sistemática en materia de ciberdefensa? Por ello, en este

la Organización de Estados Americanos (OEA) adoptaron por unanimidad la Estrategia Interamericana Integral de Seguridad Cibernética y aprobaron una declaración sobre Fortalecimiento de la Seguridad Cibernética (OEA 2014).

6 El Manual Tallin, es un documento no oficial, abocado a describir como pueden aplicarse reglas del derecho internacional a la guerra cibernética. Fue elaborado en el Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN. Define el ciberespacio como el entorno formado por componentes físicos y no físicos, caracterizados por el uso de computadoras y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de redes informáticas (Schmitt 2013).

7 Por ejemplo, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia –colCERT- y la Dirección de Ciencia, Tecnología e Innovación –Ctel (Gallardo 2014).

8 Dentro del contexto de integración política, económica, social y cultural materializada en la UNASUR, se ha constituido el Consejo de Defensa Suramericano (CDS), organismo para favorecer el diálogo y la cooperación política en temas de defensa.

9 Consejo Suramericano de Infraestructura y Planeamiento de UNASUR.

10 Plan de Acción 2015 del Consejo Defensa Suramericano.

11 Convenio N° 62 del Ministerio de Defensa, Declaración de Buenos Aires de los Ministros de Defensa del Brasil y Argentina, Buenos Aires, 13 de septiembre de 2013.

12 Sobre el uso de la fuerza el Manual Tallin considera que los artículos 2 y 51 de la Carta de las Naciones Unidas, relativos a la prohibición del uso de la fuerza y la legítima defensa, respectivamente, resultan aplicables en materia cibernética: ver reglas 10 y 11 (uso de la fuerza y evaluación). No son criterios legales formales.

apartado se ofrece un marco interpretativo y sistémico sobre qué relación existe entre el sistema de defensa y las incipientes regulaciones sobre ciberdefensa.

El concepto de ciberdefensa en la República Argentina debe interpretarse dentro de la tradición institucional amplia de su sistema de defensa en caso de agresiones. Existe una profunda articulación entre los conceptos centrales de la defensa en agresiones tradicionales y las posibles interpretaciones que puedan hacerse sobre el concepto de ciberdefensa como un ámbito específico de protección a cargo del Estado. La concepción argentina en materia de defensa, en general, se funda en el reconocimiento de la importancia que detenta la cooperación interestatal y la dimensión multilateral de la defensa y seguridad como instrumentos complementarios de la política de defensa propia. El sistema de defensa argentino tiene a su cargo la protección del Estado en relación a aquellos ataques que puedan afectar su soberanía, su independencia e integridad territorial. El sistema exige, por lo tanto, que la agresión pueda afectar alguno de estos elementos y que tenga origen externo. La reglamentación, además, requiere que el agresor sea un actor estatal.

La Ley de Defensa Nacional N° 23.554 (B.O. 5/05/1988) "establece las bases jurídicas, orgánicas y funcionales para la preparación, ejecución y control de la defensa nacional". La ley define la defensa nacional como la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieren el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva, para enfrentar las agresiones de origen externo (Art. 2). Según el artículo nueve, "el sistema de defensa está integrado por el Presidente de la Nación; el Consejo de Defensa Nacional; el Congreso de la Nación; el Ministro de Defensa; el Estado Mayor Conjunto de las Fuerzas Armadas; el Ejército, la Armada y la Fuerza Aérea de la República Argentina; Gendarmería Nacional y Prefectura Naval Argentina; y el Pueblo de la Nación mediante su participación activa en los términos de la ley". El sistema de defensa está orientado a determinar la política de defensa nacional más adecuada a las necesidades del país (y su actualización). Dicha política debe surgir de la acción coordinada de los distintos miembros del sistema. La dirección de la defensa nacional y la conducción de las Fuerzas Armadas es competencia del Presidente de la Nación en su carácter de Jefe Supremo de la misma y Comandante en Jefe de las Fuerzas Armadas (Art. 10).

La reglamentación a la ley realizada mediante Decreto N° 727/2006 (B.O. 13/06/2006), establece en su artículo primero los requisitos para el empleo de las Fuerzas Armadas, los cuales consisten en la existencia de agresiones de origen externo perpetradas por fuerzas armadas pertenecientes a otro/s Estado/s. Asimismo, define la agresión de origen externo como "el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de nuestro país, o en cualquier otra forma que sea incompatible con la Carta de las Naciones Unidas". Uno de los puntos que queda expresamente establecido en la reglamentación es que el sistema de defensa argentino no podrá contemplar situaciones pertenecientes al ámbito de la seguridad interior, conforme la delimitación establecida en la Ley de Seguridad Interior N° 24.059 (B.O. 17/01/1992).[13]

13 Tanto la Ley N° 23.554 como la Ley N° 24.059 establecen una clara distinción jurisdiccional, orgánica y funcional entre la Defensa Nacional y la Seguridad Interior (diferencia

La Ley N° 24.948 (B.O. 8/04/1998) establece las bases políticas, orgánicas y funcionales fundamentales para la reestructuración de las Fuerzas Armadas, estableciendo en su artículo segundo que la política de defensa se sustenta en lograr consolidar e incrementar las capacidades espirituales y materiales que tornen eficaz una estrategia disuasiva, coadyuvando al mantenimiento de la paz y la seguridad internacionales. La Directiva de Política de Defensa Nacional, materializada en el Decreto N° 1714/ 2009 (B.O. 12/11/2009) y en su actualización conforme el Decreto N° 2645/2014 (B.O. 19/01/2015), inicia el planeamiento para la defensa nacional. De estos documentos derivan los principales lineamientos de la política de defensa y de la política militar de la República Argentina.

En este sentido, como pauta ordenadora del sistema,y como guía orientadora en materia de ciberdefensa, la Directiva destaca que el criterio esencial y ordenador sobre el cual se estructura nuestro sistema de defensa es el concepto de "legítima defensa", rechazando las políticas estratégicas de agresión en tanto se encuentran por fuera del marco jurídico internacional vigente. Al respecto establece que:

> La República Argentina sostiene una identidad estratégica de carácter 'defensivo', de rechazo y oposición a políticas, actitudes y capacidades ofensivas de proyección de poder hacia terceros Estados. Por lo tanto, la concepción y la disposición estratégica, la política de defensa y su consecuente política militar, así como el diseño de fuerzas y previsión de empleo y evolución del Instrumento Militar, se encuentran estructuradas según el principio de legítima defensa ante agresiones militares de terceros Estados (Decreto N° 2645/2014, Capítulo II, Política de Defensa Nacional).

En 2014, la actualización de la Directiva de Política de Defensa Nacional contempló de manera expresa la importancia del ciberespacio para el desarrollo de las operaciones militares y planteó la necesidad de adaptar los sistemas de defensa a estos nuevos componentes. La Directiva destaca que solo una parte de la amplia gama de operaciones cibernéticas, afectan el ámbito de la Defensa Nacional. Además, estableció que resulta sencillo desde el punto de vista fáctico determinar *a priori* y *ab initio* si la afectación se trata de una agresión militar estatal externa. Por tanto, es complejo determinar si una situación resulta competencia o no del sistema de defensa nacional. La inclusión de la ciberdefensa en la Directiva demuestra que las nuevas tecnologías de la información y las comunicaciones han adquirido un protagonismo estratégico en la defensa de la soberanía nacional.

El relevamiento normativo y su marco teórico-metodológico

En este apartado el trabajo de investigación se aboca al estudio exploratorio y al relevamiento de la normativa sobre ciberdefensa que se desarrolló en la República Argentina durante el período 2006 – julio de 2015. [14] Por un lado,

de naturaleza). La Ley N° 24.059 establece las bases jurídicas, orgánicas y funcionales del sistema de planificación, coordinación, control y apoyo del esfuerzo nacional de policía tendiente a garantizar la seguridad interior. Se define como seguridad interior a la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional.

14 El relevamiento realizado no alcanza las normativas posteriores al 10 de diciembre de 2015 (momento en el que se produce un cambio de gobierno en la República Argentina).

[1] se relevan las normativas sobre ciberdefensa que se han generado en la República Argentina durante el período 2006 – julio de 2015 y las actividades vinculadas. Por el otro, [2] se describen las normativas y el uso concreto del concepto de ciberdefensa que se presenta en las mismas. El relevamiento y descripción de las regulaciones comprendió tanto la normativa específica en materia de ciberdefensa como aquella vinculada a otros aspectos de la regulación del ciberespacio. Es decir, aquella que también resulta aplicable al objeto de estudio: por ejemplo, la normativa sobre seguridad de la información o la normativa sobre la regulación de Internet).

A continuación, se presenta el relevamiento de la normativa sobre ciberdefensa ordenada por organismos competentes. Del análisis realizado en el período, se destacan principalmente dos instituciones que han trabajado en la materia. Por un lado, [4] se describen las regulaciones públicas del Ministerio de Defensa: este Ministerio fortaleció sus políticas en ciberdefensa desde el año 2006 a partir de la constitución de su Comité de Seguridad de la Información. Por el otro, [5] se describe la normativa que vincula la ciberdefensa con las actividades de la Jefatura de Gabinete de Ministros (JGM): la Jefatura aportó abundante normativa vinculada al tratamiento seguro de la información. En la parte final, [6] se relevan otras normativas sobre la regulación de Internet que, por diferentes razones, también resultan relevantes en materia de ciberdefensa. En los siguientes apartados, con el objeto de facilitar la lectura, la normativa se presenta en orden cronológico.

Las normas vinculadas al Ministerio de Defensa

[a] Comité de Seguridad de la Información

Por Resolución del Ministerio de Defensa N° 364, del 12 de abril de 2006, se creó el Comité de Seguridad de la Información del Ministerio de Defensa.[15] El mismo se integró, entre otras, por las áreas con competencia en materia de política, planes y programas, presupuesto, tecnología, asuntos jurídicos, recursos humanos, administración y despacho (Art. 2). La coordinación del comité fue puesta a cargo del Subsecretario de Coordinación, de quien dependían las áreas de apoyo, conforme lo requerido en el artículo tercero de la Decisión Administrativa N° 669/2004. Este fue el primer antecedente normativo dentro del Ministerio de Defensa referido a uno de los aspectos de la ciberdefensa. Si bien solo se refiere a la seguridad de la información, puede considerarse el puntapié inicial. La norma ordena coadyuvar -desde las funciones propias del Ministerio- en el proceso de protección de infraestructuras críticas (proceso coordinado desde la Jefatura de Gabinete de Ministros).

[b] El ciberespacio para el sistema de defensa nacional

En el año 2010, la Secretaría de Estrategia y Asuntos Militares del Ministerio de Defensa constituyó un grupo de trabajo a los efectos de analizar, desde el punto de vista técnico y normativo, las implicancias del ciberespa-

15 La norma dio cumplimiento a lo establecido en la decisión administrativa N° 669/2004 (B.O. 22/12/2004) para los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 (B.O. 29/10/1992).

cio para el sistema de defensa nacional. [16] La necesidad de contar con un análisis sobre la temática surgió de la permanente expansión de las redes informáticas en el mundo. El estudio comprendía los aspectos estratégicos, doctrinarios y normativos, vinculados con la normativa establecida en materia de defensa nacional. La constitución de un grupo de trabajo específico (conformado por miembros del Ministerio de Defensa, del Estado Mayor Conjunto y de las Fuerzas Armadas) representa uno de los primeros antecedentes sobre la necesidad de un trabajo coordinado en la materia de defensa. Sin embargo, aún no es posible encontrar un concepto *stricto sensu* sobre ciberdefensa. El concepto primario que se buscaba explorar desde todos los aspectos posibles era el ciberespacio, como un nuevo espacio de interés para la actuación de los organismos vinculados a la defensa.

[c] Unidad de Coordinación de Ciberdefensa

La resolución del Ministerio de Defensa N° 385, del 22 de octubre de 2013, creó la Unidad de Coordinación de Ciberdefensa en el ámbito de la Jefatura de Gabinete del Ministerio de Defensa. Su función específica consistió en coordinar las políticas y el desempeño de los actores vinculados a la ciberdefensa en la jurisdicción. El principal fundamento para la creación del área fue la existencia en las Fuerzas Armadas de un proceso de generación de capacidades y unidades especializadas para emergencias tele-informáticas. La constitución de la Unidad de Coordinación se enmarca en un concepto de ciberdefensa asociado a la protección del ciberespacio.

Se establece que la ciberdefensa requiere de la participación de todos los miembros del sistema de la defensa e innovación tecnológica del país. Entre sus funciones se destacan: a) realizar un relevamiento exhaustivo de infraestructuras, redes, recursos humanos, procesos y actividades relativas a ciberdefensa; b) entender en el diseño, planificación estratégica e implementación de políticas; c) impulsar el desarrollo doctrinario; d) analizar la evolución normativa; e) intervenir en la implementación de la Resolución de la Jefatura de Gabinete de Ministros N° 580/2011 (B.O. 2/08/2011). Una tarea especialmente asignada a esta Unidad fue la de elaborar una propuesta de estructura orgánica que asuma las competencias relativas al desarrollo e implementación de las políticas de ciberdefensa en la jurisdicción del Ministerio de Defensa. El proyecto se vio materializado mediante el dictado de la Resolución del Ministerio de Defensa N° 343 del 14 de mayo de 2014, que dispuso la creación de un Comando Conjunto de Ciberdefensa y la Decisión Administrativa N° 15/2015 (B.O. 11/03/2015) que estableció la incorporación de la Dirección General de Ciberdefensa. La estructura orgánica desarrollada tiende a favorecer la coordinación entre organismos y áreas con capacidad en la materia. Se vincula a un concepto de ciberdefensa integrado por múltiples facetas que comprenden desde el planeamiento, la doctrina, el aspecto normativo y la seguridad de la información hasta los aspectos operacionales militares específicos.

[d] Comando Conjunto de Ciberdefensa

La Resolución del Ministerio de Defensa N° 343, del 14 de mayo de 2014, dispuso la creación de un Comando Conjunto de Ciberdefensa dependiente orgánica, funcional y ope-

16 Resolución de la Secretaría de Estrategia y Asuntos Militares del Ministerio de Defensa N° 8 de fecha 14 de abril de 2010, artículo primero.

racionalmente del Estado Mayor Conjunto de las Fuerzas Armadas (Artículo primero de la Resolución MD N° 343/2014 del 14 de mayo de 2014). Su competencia específica es ejercer la conducción de las operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional. [17] El Decreto N° 727/2006 (B.O. 13/06/2006) ha establecido que las operaciones militares son conducidas por el Estado Mayor Conjunto de las Fuerzas Armadas a través del Comando Operacional. Es por eso que la conducción de las operaciones en materia de ciberdefensa debe quedar a cargo de un órgano que se encuentre contenido en la estructura del Estado Mayor Conjunto y que mantenga vínculos permanentes de coordinación con las Fuerzas Armadas. La principal capacidad que debe desarrollar este nuevo comando es la de conjurar y repeler ciberataques contra infraestructuras críticas de la información y activos del Sistema de Defensa Nacional y de su Instrumento Militar.

Para definir su marco de actuación, se debe tener en cuenta que la misión principal del Instrumento Militar es conjurar y repeler toda agresión militar estatal externa contra los intereses vitales y estratégicos de la República Argentina. El país ha adoptado un modelo de defensa de carácter defensivo[18] que deberá guiar la generación de capacidades en la temática. La conducción del Comando se encuentra a cargo de un oficial superior en actividad del Ejército argentino que cuente con capacitación para la planificación y conducción de operaciones de ciberdefensa.

La conformación de este órgano específico dentro del Estado Mayor Conjunto responde a un concepto de ciberdefensa vinculado al ciberespacio no como un ámbito militar operacional específico, sino como una dimensión transversal a los ambientes operacionales tradicionales, por lo que se requiere un planeamiento militar conjunto, y una intervención también conjunta e integrada del Instrumento Militar. Queda también definida la principal función en materia de ciberdefensa, que es la conjurar y repeler ciberataques, función que en el caso específico del Instrumento Militar quedará limitada a aquellos que recaigan sobre infraestructuras críticas de la información y activos del Sistema de Defensa Nacional y de su Instrumento Militar. La norma aborda la ciberdefensa desde el punto de vista preventivo y defensivo, en concordancia con las políticas generales.

[e] Actualización de la Directiva de Política de Defensa Nacional

Mediante el Decreto N° 2645/2014 se aprobó una actualización contenida en el Decreto N° 1714/2009 (B.O. 12/11/2009). El documento reafirma los principios fundamentales del sistema de defensa y, en su Capítulo I, expresa:

> La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la "guerra real" y exige, por la di-

17 Este diseño institucional es acorde a lo establecido en el artículo quinto de la Ley N° 24.948 de Reestructuración de las Fuerzas Armadas, que establece que "tanto en las previsiones estratégicas como en la organización, el equipamiento, la doctrina y el adiestramiento, se dará prioridad al accionar conjunto y a la integración operativa de las fuerzas, así como con las fuerzas de seguridad en sus funciones de apoyo y con fuerzas del ámbito regional y las de los países que integren contingentes de paz por mandato de las Naciones Unidas".

18 Decreto PEN N° 1714 del 12 de noviembre de 2009 "Directiva de Política de Defensa Nacional", actualizada por Decreto PEN N° 2645 del 30 de diciembre de 2014.

> námica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también el ciberespacial.

Se destaca que, si bien los ciberataques se originan en el mundo virtual conformado por redes de comunicación y sistemas informáticos, sus consecuencias impactan en el mundo físico y pueden afectar las más diversas infraestructuras críticas: agua potable, medios de comunicación o sistemas bancarios. La Directiva destaca las dificultades fácticas para determinar *a priori* y *ab initio* si la afectación califica como una agresión militar estatal externa objeto del sistema de defensa nacional. También plantea la necesidad de desarrollar capacidades operacionales en la dimensión ciberespacial tendientes a adquirir competencias en los ambientes terrestres, naval y aéreo; así como el de incrementar la ciberseguridad de redes pertenecientes al sistema de defensa nacional y de los objetivos de valor estratégico.

La Directiva contiene un aporte fundamental para el análisis, pues incorpora una definición de ciberdefensa en el marco del sistema de defensa nacional. Al respecto, en el Capítulo III, Apartado A.II, Punto 9, establece que "se entenderá por ciberdefensa a las acciones y capacidades desarrolladas por el instrumento militar en la dimensión ciberespacial de carácter transversal a los ambientes operacionales terrestre, naval y aéreo". Esta definición se destaca por brindar el marco de actuación en la materia, no solo para el planeamiento y actividades futuras, sino que le da contenido a un conjunto de normas de diferente rango, previamente analizadas, que requerían de un concepto preciso para las funciones encomendadas. Este concepto se encuentra contenido en un decreto: es decir, tiene un rango normativo superior al resto de las regulaciones analizadas y sus criterios son obligatorios para todas aquellas normativas internas del Ministerio de Defensa.

[f] Dirección General de Ciberdefensa

El 4 de marzo de 2015 se aprobó la Decisión Administrativa N° 15/2015, por medio de la cual se crea dentro del Ministerio de Defensa la Dirección General de Ciberdefensa, dependiendo directamente de la Unidad Ministro. Esta nueva norma brinda una respuesta orgánica institucional a la necesidad de contar con un área responsable de la planificación, elaboración, supervisión y evaluación de políticas en materia de ciberdefensa para el Ministerio de Defensa y su Instrumento Militar dependiente. Tiene su fundamento en la tarea permanente de resguardar las redes, sistemas informáticos y activos.

La principal competencia de la Dirección General de Ciberdefensa consiste en intervenir en el planeamiento, formulación, dirección, supervisión y evaluación de las políticas específicas dentro del Ministerio de Defensa. Entre sus funciones destacan la coordinación con organismos y autoridades de los distintos poderes del Estado, la intervención en la orientación de las acciones de ciberdefensa ejecutadas por el Nivel Estratégico Militar, el control funcional sobre el Comando Conjunto de Ciberdefensa, la intervención en el diseño de políticas, normas y procedimientos de seguridad de la información y el fomento de políticas de formación de recursos humanos.

[g] Política de Seguridad

Por medio de la Resolución MD N° 781/2015 del 24 de julio de 2015 se aprobó la Política de Seguridad de implementación en la jurisdicción Ministerio de Defensa y organismos descentralizados en su órbita. Esta medida incorpora una 'Política de Seguridad de la Información' común e integrada que contempla las características propias de cada área u organismo. Tiene por objeto garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la jurisdicción. La Resolución también crea un Comité de Seguimiento de Seguridad de la Información integrado por las áreas con competencia en la materia y que tiene por función realizar el seguimiento de la implementación y avances de la Política tanto en el Ministerio como en sus organismos.

Las normas vinculadas a la Jefatura de Gabinete de Ministros (JGM)

[a] Comités de Seguridad de la Información

La Decisión Administrativa N° 669/2004 de la JGM tuvo por objeto elevar los niveles de seguridad de los sistemas de información de los organismos públicos. La competencia recayó en la Subsecretaría de la Gestión Pública, pues se buscaba definir las estrategias vinculadas a tecnologías de la información, comunicaciones asociadas y sistemas electrónicos de tratamiento de la información dentro de la Administración Pública Nacional. Se estableció que los organismos del Sector Público Nacional debían adecuar su política de seguridad a la Política de Seguridad Modelo que sería aprobada por el Subsecretario de la Gestión Pública. El artículo 2° de la norma creó el Comité de Seguridad de la Información y obligó a cada organismo a conformar su propio Comité.

[b] Política de seguridad de la información modelo

La Oficina Nacional de Tecnologías de la Información aprobó mediante Disposición N° 1/2015 (B.O. 25/02/2015) la "Política de Seguridad de la Información Modelo" (que a su vez, reemplazó la que fuera aprobada por Disposición N° 3/2013). Este documento constituyó la base para la elaboración de las políticas específicas de cada uno de los organismos del Sector Público Nacional. Puede considerarse un compendio de buenas prácticas en materia de seguridad de la información. La JGM tenía a su cargo el establecimiento de las políticas de seguridad para la protección de los sistemas de información de la Administración Pública Nacional. Dentro de ese marco la Oficina Nacional de Tecnologías de la Información, organismo dependiente, tenía bajo su responsabilidad la formulación de políticas relativas a la seguridad de la información digitalizada y electrónica del Sector Público Nacional. El Decreto del Poder Ejecutivo Nacional N° 1067 del 10 de junio de 2015 modificó la estructura de la JGM y asignó la facultad de aprobar la Política de Seguridad Modelo a la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad. Las políticas de seguridad de la información conforman procesos clave en materia de ciberdefensa.

[c] Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad

La JGM, por medio de la Resolución N° 580 del 28 de julio de 2011, creó, en el ámbito de la Oficina Nacional de Tecnologías de la Información el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad. El principal fundamento para el establecimiento de esta política es la consideración de las infraestructuras digitales como infraestructuras críticas, imprescindibles para el funcionamiento de los sistemas de información y comunicaciones. En el artículo segundo se establece que:

> La elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones definidas en el artículo 8° de la Ley 24.156 y sus modificatorios, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran, así como el fomento de la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías (Resolución N° 580 del 28 de julio de 2011).

La implementación de las políticas de seguridad se menciona de manera expresa en la normativa dictada por el Ministerio de Defensa, en especial la Resolución N° 385/2013, que manda a la Unidad de Coordinación de Ciberdefensa a intervenir en la implementación de la Resolución de la Jefatura de Gabinete de Ministros N° 580/2011.

[d] Aprobación de Estándares Tecnológicos

Por medio de la disposición de la Oficina Nacional de Tecnologías de la Información N° 3/2014 (B.O. 8/10/2014) se aprobaron los Estándares Tecnológicos para la Administración Pública Nacional Versión 2.0. Los mismos sustituyen los aprobados por la Disposición N° 1 del 24 de julio de 2013 y la Disposición N° 1 del 7 de julio de 2014 del mismo organismo. Los estándares son de aplicación en el Ministerio de Defensa y los organismos descentralizados en su órbita (la normativa comprende a toda la Administración Pública Nacional, centralizada y descentralizada, empresas de propiedad del Estado o en las que éste tenga mayoría accionaria, bancos oficiales y Fuerzas Armadas y de Seguridad, resultando exceptuados los organismos del sistema científico nacional).[19] La normativa fija estándares mínimos para compras y contrataciones de tecnologías de información y comunicaciones.[20] Desde el punto de vista de la ciberdefensa, la fijación de estándares mínimos de seguridad a toda la administración resulta una medida preventiva fundamental.

[e] Grupo de Trabajo ICIC – CERT (Computer Emergency Response Team)

En el marco de los objetivos establecidos en el Programa Nacional de Infraestructuras

19 Dentro del Ministerio de Defensa queda excluido de su aplicación obligatoria el Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF) por integrar el Sistema Nacional de Ciencia, Tecnología e Innovación creado por la Ley N° 25.467.

20 Es así que todo organismo durante la tramitación de un expediente para la adquisición o arrendamiento de bienes y servicios de carácter informático debe remitir en forma previa toda la información relativa a sus proyectos a la Dirección Nacional de Estandarización y Asistencia Técnica de Jefatura de Gabinete, que produce su dictamen técnico al respecto: Art. 5 del Decreto N° 856/98 (B.O. 22/07/98).

Críticas de Información y Ciberseguridad, se dictó la Disposición de la Oficina Nacional de Tecnologías de la Información N° 2/2013 (B.O. 3/09/2013), que creó una serie de grupos de trabajo a fin de desarrollar proyectos y propuestas que promuevan la protección de infraestructuras críticas de información y ciberseguridad. Entre ellos, se encuentra el grupo de trabajo "ICIC – CERT" que administra y asesora sobre incidentes de seguridad a los organismos del Sector Público Nacional que hubieren adherido al Programa. La existencia de esta instancia de coordinación resulta necesaria para una política conjunta en materia de seguridad de la información. La norma también crea un Grupo de Acción Preventiva (ICIC – GAP), uno de Infraestructuras Críticas de Información (ICIC – GICI) y uno de Internet Sano (ICIC – INTERNET SANO).

[f] Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad

El Decreto N° 1067/2015 (B.O. 12/06/2015) modifica la estructura orgánica de la JGM mediante la creación de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad en el ámbito de la Secretaria de Gabinete. La misma, tiene como objetivo principal entender en la elaboración de la estrategia nacional de protección de infraestructuras críticas de información y ciberseguridad. La norma dispone la transferencia del "Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad", dependiente de la Oficina Nacional de Tecnologías de Información, a la órbita de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad dependiente de la nueva Subsecretaría. El Subsecretario de Protección de Infraestructuras Críticas de Información y Ciberseguridad tendrá la facultad para aprobar la Política de Seguridad Modelo y dictar las normas aclaratorias y complementarias de la Decisión Administrativa N° 669/2004.

Otras normas vinculadas a la regulación de internet

[a] Comisión Argentina de Políticas de Internet

La Secretaría de Comunicaciones, con fundamento en la multiplicidad de áreas dentro del Sector Público Nacional con injerencia en temas vinculados a Internet, creó por Resolución N° 13/2014 (B.O. 23/04/2014) la Comisión Argentina de Políticas de Internet con el fin de articular la participación de los distintos actores en el diseño de una estrategia nacional sobre gobierno de Internet. Entre otras, la Resolución invitó a participar de la comisión a la Secretaría de Ciencia, Tecnología y Producción para la Defensa del Ministerio de Defensa. La medida se enmarcó en un escenario internacional lleno de expectativas ante la realización en Brasil de la Reunión Global de Múltiples Partes Interesadas sobre el Futuro de la Gobernanza de Internet – NETmundial (23 y 24 de abril de 2014 en San Pablo).

[b] Argentina Digital

La Ley N° 27.078 (B.O. 19/12/2014) declaró "de interés público el desarrollo de las tecnologías de la información y las comunicaciones, las telecomunicaciones, y sus recursos asociados", y estableció como finalidad de la misma garantizar el derecho humano a las comunicaciones y a las telecomunicaciones. La

ley creó su propia autoridad de aplicación, un organismo descentralizado y autárquico en el ámbito del Poder Ejecutivo Nacional, denominado Autoridad Federal de Tecnologías de la Información y las Comunicaciones (creados a su vez por el Decreto N° 677/2015, B.O. 29/04/2015). Esta normativa debe ser tenida en cuenta en materia de ciberdefensa puesto que se trata de una norma de orden público y que define, en el artículo 6, apartado b, los recursos asociados (es decir, infraestructuras físicas, los sistemas, los dispositivos, los servicios asociados con una red de telecomunicaciones o con un Servicio de Tecnologías de la Información y las Comunicaciones).

La ley no define el concepto de ciberespacio. Sin embargo, en su artículo 6 apartado g., se explica qué se entiende por tecnologías de información y comunicación: "conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permitan la compilación, procesamiento, almacenamiento y transmisión de información". En el artículo 62, inciso i, establece la obligación de atender los requerimientos en materia de defensa nacional y de seguridad pública formulados por las autoridades competentes.

Conclusiones: Hacia una mayor sistematización de la legislación en ciberdefensa

La ciberdefensa se ha transformado en un tema clave a nivel mundial. Desde hace varios años la red de redes puede ser considerada una fuente de amenazas para la defensa nacional/regional. Los avances científico-tecnológicos están cambiando -y adecuando- muchas de las tradicionales estrategias de defensa. El interés sobre ciberdefensa está expandiéndose rápidamente en Argentina y toda la región sur. En el período analizado es posible identificar que en Argentina se produjo un aumento significativo de la normativa específica. También se produjo un incremento de medidas de confianza mutua y cooperación tanto bilaterales como multilaterales en la región sur. Esto incluye el establecimiento de políticas comunes a través de órganos regionales: por ejemplo, el Consejo de Defensa Suramericano.

Específicamente, el estudio identifica que el concepto de ciberdefensa de la República Argentina, en el marco de la normativa que rige el sistema de defensa nacional, sigue un modelo de carácter defensivo y orientado al desarrollo de capacidades. Existe en la legislación Argentina una definición específica de ciberdefensa: la misma está contenida en la Actualización de la Directiva de Política de Defensa Nacional. El relevamiento también permite observar que, durante el período 2006 – julio 2015, se ha producido un aumento significativo en las regulaciones sobre la temática dentro del Estado Argentino. Éste se relaciona al crecimiento y desarrollo de nuevas amenazas provenientes del uso masivo de las tecnologías de información y comunicación. Como se ha resaltado durante el relevamiento, dicho crecimiento normativo no está exento de ambigüedades, interpretaciones y negociaciones: por ejemplo, qué significa el concepto de ciberdefensa, qué es y cómo se evalúa un ciberataque o, entre otros, qué criterios jurídico-políticos deben aplicarse.

La investigación también ha revisado cuáles fueron en el período las instituciones públicas argentinas competentes. Específicamente, la ciberdefensa ha sido regulada por el Ministerio de Defensa de la Nación a través de normativa de rango interno (resoluciones). También es posible destacar normativa del Poder Ejecutivo

Nacional (decretos). A esto se suman normativas vinculadas a seguridad de la información, infraestructuras críticas y regulaciones de Internet (por ejemplo, la Ley N° 27.078 de Argentina Digital). Sobre la temática también existen normas que otorgaron responsabilidades a la Jefatura de Gabinete de Ministros, y sus áreas dependientes, con el objeto de generar políticas comunes de aplicación a toda la Administración Pública Nacional.

Finalmente, la investigación permite concluir que el sistema legal argentino aún no dispone de una codificación general y sistemática sobre ciberdefensa. Una sistematización de los marcos jurídicos (y reglamentarios), así como una mayor definición de objetivos, competencias y funciones entre los diferentes organismos del Estado, podría ser de gran utilidad y ayudar a alcanzar múltiples objetivos estratégicos. Entre otros, [a] definir qué significa y cómo debe entenderse el concepto de ciberdefensa nacional / regional; [b] contribuir al diseño de tecnologías digitales orientadas a la defensa de los intereses nacionales / regionales; [c] favorecer procesos legislativos (del Congreso Nacional) que se orienten a regular tanto el sector público como las actividades críticas en manos del sector privado; [d] fortalecer la simetría y la correspondencia con las potenciales regulaciones regionales e internacionales sobre ciberdefensa; y [e] enriquecer los debates sobre ciberdefensa involucrando tanto actores de la política y las fuerzas armadas como de la academia, la sociedad civil y el sector privado nacional / regional.

Bibliografía

Adkins, Bonnie. 2001. "The spectrum of Cyberconflict. From hacking to information warfare. What is law enforcement´s role", http://handle.dtic.mil/100.2/ADA406949.

Amaral, Augusto César. 2014. "La amenaza cibernética para la seguridad y defensa de Brasil". *Revista Visión Conjunta* 10: 19-22. http://www.cefadigital.edu.ar/bitstream/123456789/32/3/VC%2010-2014%20AMARAL.pdf.

Assange, Julian. 2013. Criptopunks: La libertad y el futuro de Internet. Buenos Aires: Marea/Trilce.

Eissa, Sergio G, Gastaldi Sol; Iván Poczynok y Elina Zacarías Di Tullio. 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. http://www.unq.edu.ar/catalogo/330-revista-de-ciencias-sociales-n-25.php.

Feliu Ortega, Luis. 2012. "La ciberseguridad y la ciberdefensa". España: Ministerio de Defensa de España.

Ferrero, Julio Alberto. 2013. "La Ciberguerra, génesis y evolución". *Revista General de Marina* 264: 81-97. http://publicaciones.defensa.gob.es/pprevistas/49e78d6b-fb63-65ab-9bdd-ff0000451707/index.html.

Gallardo, Sara. 2014. "Más allá de las TIC en Mindefensa". *Revista Sistemas, ACIS* 130 (7). http://52.0.140.184/revsistemas1/index .php/ediciones-revista-sistemas/edicion-130/item/156-m%C3%A1s-all%C3%A1-de-las-tic-en-mindefensa.

Gibney, Alex. 2016. *Zero Days*. EE.UU.: Jigsaw Productions y Participant Media (Documental).

Gastaldi, Sol y Justifró Candela. 2014. "La seguridad y la defensa en el ámbito ciberespacial. Informe de Investigación. Escuela de Defensa Nacional", http://www.edena.mindef.gob.ar/sol_gastaldi.html

Ministerio de Defensa, Presidencia de la Nación y República Argentina. 2015. *Libro Blanco de la Defensa*. Argentina: Ministerio de Defensa. http://www.mindef.gob.ar/institucional/pdfs/libro_blanco_2015.pdf.

Illaro, Eguskiñe Lejarza. 2014. "Ciberguerra, los escenarios de confrontación". *Revista del Instituto Español de Estudios Estratégicos* 18: 1-20. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf.

OEA (Organización de los Estados Americanos). 2014. *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos*. Washington: Secretaría de Seguridad Multidimensional. https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Pastor Acosta, Oscar, José Antonio Pérez Rodríguez, Daniel Arnáiz de la Torre y Pedro Taboso Ballesteros. 2009. *Seguridad Nacional y Ciberdefensa*. Madrid: Cuadernos Cátedra ISDEFE. http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

Poitras, Laura. 2014. *Citizenfour*. Alemania, EE.UU, Reino Unido: Praxis Films/Participant Media/ HBO Films (Documental). https://citizenfourfilm.com/.

Schmitt, Michael, ed. 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare gen. Nueva York: Cambridge University Press.

Vercelli, Ariel. 2009. Repensado los bienes intelectuales comunes: análisis socio-técnico sobre el proceso de co-construcción entre las regulaciones de derecho de autor y derecho de copia y las tecnologías digitales para su gestión. Edición en PDF. http://www.arielvercelli.org/rlbic.pdf

_____. 2015. "Repensando las regulaciones de Internet: análisis de las tensiones políticas entre no-regular y re-regular la red de redes". *Revista Latinoamericana de Comunicación Chasqui* 129: 95–112. http://revistachasqui.org/index.php/chasqui/issue/view/129_2015.

Documentos

Carta de las Naciones Unidas. 1945. "Conferencia de las Naciones Unidas sobre Organización Internacional", http://www.un.org/es/charter-united-nations/index.html.

Convenio del Ministerio de Defensa. 2013, de 13 de septiembre, Declaración de Buenos Aires de los Ministros de Defensa del Brasil y Argentina, http://www.ceedcds.org.ar/Espanol/09-Downloads/DECLARACION_ARG_BRASIL.pdf.

Decisión Administrativa 669/2004, de 20 de diciembre, Política de Seguridad de la Información (B.O. 22/12/2004), http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/102188/texact.htm.

Decisión Administrativa 15/2015, de 4 de marzo, Estructura organizativa. Modificación (B.O. 11/03/2015), http://servi-

cios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/244566/norma.htm.

Decreto 727/2006, de 12 de junio, de Reglamentación de la Ley Nº 23.554 (B.O. 13/06/2006), http://servicios.infoleg.gob.ar/infolegInternet/anexos/115000-119999/116997/norma.htm.

Decreto 1714/ 2009, de 10 de noviembre, Directiva de Política de Defensa Nacional (B.O. 12/11/2009), http://servicios.infoleg.gob.ar/infolegInternet/anexos/160000-164999/160013/norma.htm.

Decreto 2645/2014, de 30 de diciembre, Directiva de Política de Defensa Nacional. Apruébase actualización (B.O. 19/01/2015), http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/240966/norma.htm.

Decreto 677/2015, de 28 de abril, de Argentina Digital. Autoridad Federal de Tecnologías de la Información y las Comunicaciones (B.O. 29/04/2015), http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/246354/norma.htm.

Decreto 1067/2015, de 10 de junio, Decreto N° 357/2002. Modificación (B.O. 12/06/2015), http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm.

Disposición de la Oficina Nacional de Tecnologías de la Información 2/2013, de 8 de agosto, Grupo de Trabajo "ICIC - CERT - Creación (B.O. 3/09/2013), http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219212/norma.htm.

Disposición de la Oficina Nacional de Tecnologías de la Información 3/2014, de 2 de octubre, Estándares Tecnológicos para la Administración Pública Nacional Versión 20.0 - Aprobación (B.O. 8/10/2014), http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/236037/norma.htm.

Disposición de la Oficina Nacional de Tecnologías de la Información 1/2015, 18 de agosto, Requerimientos para la Conformación de las Autoridades de Registro (B.O. 25/02/2015), http://servicios.infoleg.gob.ar/infolegInternet/anexos/250000-254999/250974/norma.htm.

Ley 23554/1988, de 13 de abril, de Defensa Nacional (B.O. 5/05/1988), http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm.

Ley 24.059/1991, de 18 de diciembre, de Seguridad Interior (B.O. 17/01/1992), http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/texact.htm.

Ley 24.156/1992, de 30 de septiembre, de Administración Financiera y de los Sistemas de Contabilidad del Sector Público Nacional (B.O. 29/10/1992), http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/554/texact.htm.

Ley 24.948/1998, de 18 de marzo, de Reestructuración de las Fuerzas Armadas (B.O. 8/04/1998), http://servicios.infoleg.gob.ar/infolegInternet/anexos/50000-54999/50229/norma.htm.

Ley 27.078/2014, de 16 de diciembre, de Argentina Digital (B.O. 19/12/2014), http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm.

Resolución de la Jefatura de Gabinete de Ministros 580/2011, de 28 de julio, Créase el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (B.O. 2/08/2011), http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm.

Resolución de la Secretaría de Comunicaciones 13/2014, de 22 de abril, Comisión Argentina de Políticas de Internet (B.O. 23/04/2014), http://servicios. infoleg. gob.ar/infolegInternet/anexos/225000-229999/229123/norma.htm.

Resolución del Ministerio de Defensa 364/ 2006, de 12 de abril.

Resolución del Ministerio de Defensa 385/ 2013, del 22 de octubre.

Resolución del Ministerio de Defensa 343/ 2014, del 14 de mayo.

Resolución del Ministerio de Defensa 781/ 2015, del 24 de julio.

Resolución de la Secretaría de Estrategia y Asuntos Militares del Ministerio de Defensa 8/2010, de 14 de abril.

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2583

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 63-79
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Actividades rutinarias y cibervictimización en Venezuela

Routine activities and cyber-victimization in Venezuela

Juan Antonio Rodríguez[1], Jesús Oduber[2] y Endira Mora[3]

Fecha de recepción: 14 de febrero de 2017
Fecha de aceptación: 3 de abril de 2017

Resumen

El ciberdelito ha aumentado significativamente a nivel mundial en estas últimas décadas. En tal sentido, la investigación sobre este fenómeno en Venezuela ha sido escasa, específicamente en lo que respecta a los factores asociados con la victimización en línea. En consecuencia, este estudio busca promover el análisis de los condicionantes del delito y la victimización en línea en la región. Para ello, se investiga un conjunto de variables derivadas de la *Teoría de las actividades rutinarias*. El propósito es observar su relación con la victimización por *hackeo* y acoso *online* en una muestra de 308 sujetos. Este estudio halló un grupo de variables que pueden estar relacionadas con la probabilidad de victimización cibernética, las cuales serán discutidas en términos empíricos, teóricos y prácticos.

Palabras clave: victimización; *hacking*; acoso en línea; actividades rutinarias; Venezuela.

Abstract

Cybercrime has significantly increased worldwide in the last decades. There has been very little research done regarding cybercrimes in Venezuela in comparison to other places, more specifically in regards to the factors related to online victimization. Thus, this study aims to encourage the analysis on the factors of crime and online victimization in the region. Therefore, a group of variables derived from the routine activity theory (Cohen and Felson 1979), is analyzed. The purpose is to observe its relation to hacking and online harassment in a sample of 308 individuals. This study found a group of variables that could be related to the likelihood of cyber victimization, which will be discussed in empirical, theoretical and practical terms.

Keywords: victimization; hacking; online harassment; routine activity; Venezuela.

1 Criminólogo y Doctor en Psicología Social por la Universidad de Santiago de Compostela (España). Profesor asociado y ex-director de la Escuela de Criminología de la Universidad de Los Andes (Venezuela). Investigador (adscrito al GIC y CENIPEC) acreditado por el ONCTI y el CDCHTA-ULA (Venezuela). Correo: jarodrig@ula.ve.

2 Criminólogo y abogado. Docente e investigador de la Escuela de Criminología de la Universidad de Los Andes (Venezuela). Correo: jesusoduber@hotmail.com.

3 Criminóloga, abogada y MSc. en Orientación de la Conducta. Maestrante de Derecho Procesal Penal y de Gestión Empresarial. Consultora jurídica e investigadora en Derecho Informático del CENDITEL. Correo: endiramorarojas@gmail.com.

Introducción

En las dos últimas décadas, el uso de internet se ha incrementado de manera sostenida en Latinoamérica. Cifras de la Comisión Económica para América Latina y el Caribe (CEPAL) señalan que el porcentaje de usuarios creció casi un 11% de forma interanual en el periodo 2000-2015 (CEPAL 2016). Esta Comisión, al igual que otros organismos como el Banco Interamericano de Desarrollo (BID 2016), afirma que alrededor del 55% de la población total de Latinoamérica y el Caribe utilizó en mayor o menor medida internet en el 2015. No hay duda de que las Tecnologías de la Información y la Comunicación (TIC) se han convertido en un medio fundamental tanto para el desarrollo de actividades comerciales y económicas como para el crecimiento de relaciones sociales en la región. Sin embargo, este mismo desarrollo tecnológico también ha subvertido la seguridad favoreciendo el aumento de nuevas oportunidades para la comisión de viejos delitos (pero ahora basados en modernos sistemas de información y comunicación) y la eclosión de formas muy novedosas de transgresión inmanentes al ciberespacio.

Los informes de organismos internacionales y empresas vinculadas a la seguridad informática reseñan un importante incremento de ataques cibernéticos contra personas físicas, corporaciones y gobiernos de Latinoamérica y el Caribe en el último quinquenio (BID 2016; ESET 2016; Kaspersky 2016; OEA 2013; Symantec 2014a), lo que significa para las finanzas de la zona cerca de 90.000 millones de dólares anuales (BID 2016). Los ciberdelitos con mayor ocurrencia (o al menos los más destacados en los informes de entidades públicas y privadas) son el acceso ilegal a datos (*hacking*) y la violación de la privacidad o confidencialidad, los cuales se encuentran muy relacionados a ataques con *malware* (ESET 2016; OEA 2013; Symantec 2014a).

Al respecto, Kaspersky Lab registró más de 398 millones de ciberataques con *malware* en América Latina durante los años 2015 y 2016, facilitados en parte por la navegación, la descarga de archivos y el ingreso a correos electrónicos fraudulentos o con adjuntos contaminados (Kaspersky 2016). En este sentido, el *crimeware* es otro caso característico de la ciberdelincuencia local. Los *hackers,* apoyados en técnicas como el *spamming* o *pharming,* buscan robar identidades, credenciales y datos financieros para ingresar en cuentas de banco *online* y substraer los fondos disponibles o para interceptar información de tarjetas de crédito y venderla en el mercado. Este tipo de amenazas bancarias basadas en navegadores son usuales en Latinoamérica, pero también han surgido nuevas modalidades como el ataque a dispositivos móviles para interceptar los mensajes de texto (SMS) enviados del banco a la víctima o los ataques con *malware* dirigido a cajeros automáticos (Symantec 2014a).

En Venezuela, las actividades ilegales vinculadas al ciberespacio presentan un patrón muy similar al resto de los países de América Latina y el Caribe. La empresa Symantec (2014b) destaca que el 4,2% de los ataques cibernéticos de la región ocurrieron desde este país en el 2013. Simultáneamente, Venezuela tuvo una tasa de infección por *malware* del 23.13% del total de computadoras analizadas por PandaLabs en ese mismo año (Symantec 2014a). Y además, se ubicó entre los 10 países de esta parte del continente más afectados por el *spear phishing* al sufrir el 5% del total de ataques registrados para Latinoamérica y el Caribe. En el caso concreto de las empresas, el laboratorio de investigación de ESET (2016)

conoció y desmanteló una campaña de propagación e infección de *malware* denominada *Operación Liberpy* en el año 2015. Esta *botnet* se dedicaba expresamente al robo de información de los usuarios. Este mismo reporte señala que 13% de las empresas en Venezuela fueron víctimas de *phishing* en ese mismo periodo.

En vista de este escenario, los organismos gubernamentales de Venezuela y del resto de América Latina han buscado fórmulas para contrarrestar la ciberdelincuencia, lográndose avances sustantivos en el mejoramiento de las capacidades tecnológicas, las políticas de prevención y, en especial, la sanción de leyes contra este tipo de delito[4] (Symantec 2014a; BID 2016). Ahora bien, estos intentos de prevenir y controlar dicho fenómeno son valiosos, pero para que ello tenga una mayor efectividad hay que conocer qué factores están relacionados al mismo. Sobre la base de lo anterior, se debe precisar que hasta el momento se ha desarrollado muy poca investigación sistemática tanto cuantitativa como cualitativa sobre el ciberdelito en Venezuela y el resto de los países de Latinoamérica. De aquí la imperiosa necesidad de dedicar mayor interés a su definición y clasificación, los niveles de perpetración/victimización, los predictores (individuales y ambientales) asociados a estos y los marcos explicativos plausibles para comprender este objeto de estudio a nivel local.

En este sentido, la presente investigación, por sus características, no tiene como finalidad analizar la prevalencia e incidencia de la victimización cibernética en una población determinada. Más bien constituye un análisis cuantitativo que permite mejorar la comprensión de los factores de riesgo y protección inherentes al uso de las TIC, los cuales pueden hacer a alguien vulnerable (o no) a un delito informático. Tomando en cuenta el apoyo alcanzado para este tipo de análisis, se ha decidido utilizar los conceptos y predictores enmarcados en la *Teoría de las actividades rutinarias* (en adelante TAR) propuesta por Cohen y Felson a finales de los años setenta. Un teoría que según Wikström y Treiber (2016) puede considerarse más como un modelo predictivo con el que se consigue definir dónde y cuándo es más probable que ocurra un delito. Así, el objetivo principal de este estudio es contrastar algunos predictores del *hackeo* y el acoso cibernético (*online harassment*) con la aplicación de medidas derivadas de la TAR en una muestra de estudiantes universitarios de Venezuela.

Cibervictimización y actividades rutinarias: desarrollos teóricos y empíricos

La victimización en línea se ha estudiado fundamentalmente en los países desarrollados en las dos últimas décadas. Con el propósito de recopilar información, evaluarla y, luego, tratar de predecir y explicar los delitos relacionados con las TIC, algunos trabajos se han dedicado a analizar el significado y la naturaleza

4 Venezuela cuenta con un marco legislativo que regula el ámbito informático conformado por la Constitución de la República Bolivariana de Venezuela del año 1999, el Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas del año 2001, la Ley de Interoperabilidad del año 2012, la Ley Orgánica de Telecomunicaciones del año 2014, la Ley de Infogobierno del año 2013 y la Ley Especial contra los Delitos Informáticos del año 2001. Se debe destacar que esta última Ley es la que regula las sanciones penales en la materia. En el ámbito institucional los cuatro organismos encargadas del control de los delitos informáticos en este país son: el Sistema Nacional de Gestión de Incidentes Telemáticos (VenCert), el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), el Centro Nacional de Informática Forense (CENIF) y la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) (BID 2016; Symantec 2014a).

de múltiples formas de ciberdelitos. Al punto que, en un marco de visibles desacuerdos, los expertos en el tema han propuesto diferentes definiciones de lo que puede entenderse por delito informático y creado a partir de ellas algunas tipologías (Gordon y Ford 2006; Wall 2005; Yar 2006). Por ejemplo, Gordon y Ford (2006, 14) definen el delito informático como "cualquier delito que es facilitado o cometido usando una computadora, red, o dispositivo hardware".

Sobre la base de esta definición, clasifican el ciberdelito en *tipo I,* que es básicamente de naturaleza tecnológica y *tipo II,* que tiene un componente humano más acentuado. Son delitos propios de la primera categoría, entre otros, el *phishing*, el *hacking*, el *ransomware,* el robo de identidad, los fraudes bancarios o de comercio *online* mediante información robada y los ataques de denegación de servicio (*DoS* y *DDos*). Por su parte, el acoso en línea (*online harassment, cyberbullying, cyberstalking*), el *gromming*, la pornografía infantil y el ciberterrorismo son ejemplos de la segunda categoría. En el presente estudio se analizan dos ciberdelitos enmarcados en cada una de estas tipologías, ellos son el *hacking* y el acoso en línea (*online harassment*). Ambas formas de victimización han sido analizadas empíricamente en la Criminología de países como Estados Unidos y España a la luz de la TAR pero nunca en algún país de Latinoamérica.

Citado más de 6850 veces en las últimas cuatro décadas (Google Scholar 2017), el artículo de Cohen y Felson (1979) titulado *Social change and crime rate trends: a routine activity approach* introduce las ideas centrales de la TAR. Para Cohen y Felson la probabilidad de que ocurra un delito es el resultado de una ecuación que incluye tres variables interdependientes: un delincuente motivado (capaz de perpetrar un delito), un objetivo/víctima adecuado[5] y un guardián eficaz (cuya presencia disuada el delito y su ausencia lo facilite). Concretamente, estos autores predicen que las oportunidades delictivas se dan cuando convergen estos tres elementos en un momento y lugar determinado. Según este enfoque, sin una oportunidad en estos términos es mucho menos probable que suceda el delito; por ello, la oportunidad constituye la causa principal de la victimización delictiva.

Ahora bien, la noción de actividades rutinarias hace referencia a modos de vida que constituyen patrones regulares en la sociedad, los cuales están relacionados con la familia, el trabajo o el entretenimiento y buscan satisfacer necesidades individuales y colectivas. La TAR sostiene que la organización social moderna, afectada por la evolución tecnológica, determina en cierta medida los estilos de vida, hábitos y actividades diarias de las personas, hasta el punto de que puede tener una influencia en las oportunidades que promueven el delito. La evolución tecnológica y social ha significado un aumento de nuevos espacios de oportunidad delictiva porque incrementa la convergencia de un posible delincuente motivado, un objetivo idóneo y la ausencia de un guardián eficaz (Cohen y Felson 1979).

A simple vista, las TIC son un buen ejemplo de transformación tecnológica que han tenido una incidencia importante en el día a día de la sociedad contemporánea. Por esta razón, no es un error suponer que las oportunidades delictivas en torno a las TIC han aumentado por los cambios de las actividades rutinarias modernas y que las personas actúan en respuesta a estas oportunidades. Probablemente,

5 Un objetivo será más o menos adecuado dependiendo de cómo un delincuente lo perciba en función de su valor, inercia, visibilidad y accesibilidad (Cohen y Felson 1979).

teniendo esto en mente, un número creciente de estudios teórico-empíricos ha analizado los correlatos de la victimización *online* usando como marco de referencia la TAR (Bossler y Holt 2009; Bossler, Holt y May 2013; Choi 2008; Holt y Bossler 2009; Leukfeldt y Yar 2016; Marcum, Higgins y Ricketts 2010; Miró 2013; Ngo y Paternoster 2011; Reyns, Henson y Fisher 2011; Tillyer y Eck 2009; Yar 2005).

Las primeras discusiones teóricas se centraron en si las predicciones y explicaciones formuladas por Cohen y Felson, pensando en rutinas y circunstancias muy particulares del mundo físico, como el momento y lugar, son válidas para analizar la victimización por delitos cibernéticos (Eck y Clarke 2003; Grabosky 2001; McGuaire 2007; Miró 2011; Tillyer y Eck 2009; Yar 2005). En el marco de este debate, varios investigadores se han mostrado más o menos de acuerdo con la adaptación de los conceptos originales de la TAR al ciberespacio (Miró 2011 y Yar 2005). Algunos reconocen conceptual y analíticamente cierta correspondencia entre el contexto físico y el contexto virtual donde se pueden manifestar los tres elementos clave de la teoría (delincuente motivado, objetivo adecuado y ausencia de un guardián capaz). Por ejemplo, para estos investigadores una persona puede ser igualmente un *blanco adecuado* si enseña dinero en una taquilla de pago o si ofrece información en *Facebook* sobre el banco donde lo ahorra y un antivirus puede ser un *guardián* tan *capaz* como el vigilante de seguridad que cuida la tienda donde se vende este tipo de *software*. En definitiva, algunos autores sostienen en apoyo a la TAR que la organización del hecho delictivo es equivalente en escenarios físicos y virtuales y, en consecuencia, la cibervictimización puede ser tratada apropiadamente a la luz de la propuesta de Cohen y Felson (Yar 2005).

A la par de este valioso debate, varios estudios han intentado probar empíricamente la TAR en el contexto cibernético analizando muestras de estudiantes universitarios. Por ejemplo, Choi (2008) encontró a favor de esta teoría que los *estilos de vida en línea* imprudentes (como, por ejemplo, abrir adjuntos y enlaces web enviados por correos electrónicos desconocidos o ingresar en mensajes *pop-up*) aumentan la probabilidad de victimización por infección de virus. Y, al contrario, disponer de un *guardián digital* (programas antivirus, antispyware y firewall), disminuye tal probabilidad. En esta misma dirección, Marcum *et al.* (2010) también hallaron cierta evidencia a favor de las predicciones de Cohen y Felson.

En concreto, algunas prácticas *online* que hacen más probable la exposición a delincuentes motivados (uso de correo electrónico, mensajería instantánea, salas de chat y redes sociales) y la idoneidad del objetivo (información personal compartida en redes sociales) se relacionaron con la victimización por exposición a material sexual, acoso (no sexual) y proposición sexual no deseados. Sin embargo, las medidas de protección tecnológicas (uso de *software* de bloqueo) no evitaron este tipo de victimización; aunque, sí lo hicieron otras tácticas como el monitoreo de terceros y los controles parentales.

Otro grupo de investigaciones han encontrado poco o ningún apoyo empírico a la TAR en este tipo de muestras. En su estudio, por ejemplo, Bossler y Holt (2009) concluyen que las compras u operaciones en banca por internet y la vigilancia eficaz operacionalizada como habilidades informáticas y uso de antivirus no tienen una relación con el robo de datos por infección de *malware*. En otra inves-

tigación publicada ese mismo año, estos autores reportan que el acoso en línea (*harassment*) no tiene ninguna correspondencia con la mayoría de los indicadores de la TAR, especialmente con programas de seguridad y con rutinas como el tiempo conectado a internet, uso de correo electrónico y compras en línea. Reyns *et al.* (2011) analizaron el acoso *online* persistente (*cyberstalking*) y determinaron que los indicadores de exposición en línea no presentaron ninguna asociación significativa con este tipo de ciberdelito.

Solo la variable *agregar a personas desconocidas* se relacionó con este modo de hostigamiento. Con respecto a los indicadores de vigilancia, la medida de rastreo de perfil, al contrario de lo esperado, aumentó el riesgo de victimización. Finalmente, Ngo y Paternoster (2011) analizaron la capacidad predictiva de la TAR en un grupo amplio de formas de victimizaciones *online* (*harassment* por parte de extraños y conocidos, infección por virus, *phishing*, pornografía no deseada, solicitud de sexo y difamación) pero sus resultados tampoco consiguieron brindarle respaldo empírico a la teoría; incluso, en la mayoría de los casos se observaron relaciones en el sentido contrario a las predicciones de Cohen y Felson.[6]

Dado el interés que a nivel internacional han despertado las ideas de Cohen y Felson, se prevé que la TAR puede ser analíticamente útil para predecir la victimización cibernética en nuestra región. Así, la pregunta central que guía este estudio es ¿qué actividades cotidianas de las que se experimentan dentro y fuera de Internet se relacionan con la probabilidad de victimización por *hacking* y por acoso en línea (*online harassment)*? Para dar respuesta a esto, el propósito de esta investigación es hallar, a partir de los conceptos y medidas de la TAR, algunas variables individuales y ambientales asociadas a la cibervictimización. En concreto, se analizará estadísticamente si la exposición a un delincuente motivado, la idoneidad del objetivo/víctima y la falta de vigilancia efectiva tienen correspondencia con el *hacking* y al acoso en línea de universitarios venezolanos. Los resultados obtenidos pueden mejorar el conocimiento sobre los correlatos de la victimización cibernética y sobre la validez de la TAR para la predicción y explicación de este fenómeno.

Método

Participantes

Los datos de la muestra provienen de estudiantes universitarios venezolanos adscritos a la Facultad de Ciencias Jurídicas y Políticas de la Universidad de Los Andes. Esta es una muestra por conveniencia y en total fueron analizados 308 sujetos. En términos generales, el 63% (*N*=193) de la muestra es de sexo femenino y el 37% (*N*=113) masculino. En este grupo hay universitarios entre 17 y 56 años de edad y la media es de 25,94 años (D.T 0,09 años). El 68,2% de los sujetos cuenta con edades comprendidas entre 17 y 26 años, por lo tanto, puede señalarse que la muestra está conformada en su mayoría por estudiantes jóvenes. De este grupo de universitarios, un 17,9% (*N* =55) se encuentran estudiando primer año, 28,6% (*N* =88) segundo año, 16,9% (*N* =52) tercer año, 22,7% (*N*=70) cuarto año y un 13,3% (*N*=41) el quinto año de la carrera.

6 En este estudio solo el uso de mensajería instantánea se relacionó con el acoso en línea en la dirección propuesta por la TAR.

Medidas

Victimización en línea (Variable criterio)

La variable criterio se operacionalizó mediante dos formas de victimización por delitos informáticos.[7] La primera es el *hacking,* que se entiende como el acceso y posterior uso de un dispositivo o sitio de la red con fines nocivos, sin el debido consentimiento del usuario o titular al que pertenece. Esta definición se midió por medio del *hackeo* de correo electrónico y cuentas en redes sociales. La segunda es la cibervictimización por acoso en línea u *online harassment*, que se refiere a actos de hostigamiento en internet (Miró 2013). En esta investigación el acoso en línea se midió con tres ítems: suplantación de identidad, uso de imagen sin autorización y contacto repetido no deseado. Para cada una de las preguntas planteadas se usó un tipo de respuesta dicotómica en la que 0 representa "no" y 1 "sí".

Actividades rutinarias (Variables predictivas)

Las variables predictivas se diseñaron sobre la base de lo propuesto por la TAR (Cohen y Felson 1979) y en algunos de los estudios citados en párrafos anteriores. El *objetivo adecuado en línea* son aquellos comportamientos en el uso de internet que hacen a una persona o cosa un blanco probable para el delito. Este constructo se midió con los siguientes indicadores: 1) ¿Por medio de la mensajería instantánea (*Whatsapp, Line, BlackBerry Messenger*, etc.) tiene contacto con personas que no conoce? 2) ¿Abre o descarga enlaces o archivos enviados por desconocidos a través del correo electrónico? y 3) ¿Facilita información personal real a través de las redes sociales? La respuesta a cada una de estas preguntas fue de tipo binaria (0= no y 1= sí).

La *exposición a un delincuente motivado en línea* se operacionalizó como el conjunto de actividades que hace a un individuo más visible ante un ciberdelincuente cuando se conecta a internet. Los 5 indicadores usados para medir este constructo fueron el número de horas de conexión a internet, el uso de correo electrónico, el uso de redes sociales (*Twitter, Facebook*), la descarga de archivos y el uso de la banca *online.* En el caso del primer indicador se le preguntó al encuestado por la cantidad de horas que se conecta al internet durante una semana típica. Con relación a los otros cuatro indicadores, se consultó al encuestado ¿con qué frecuencia utiliza los siguientes servicios de internet a la semana? La categoría de respuesta se planteó como una escala tipo Likert que va de 0 (nunca) a 4 (siempre). En este caso, para efectos de los análisis multivariante se dicotomizaron las variables uso de correo electrónico, redes sociales y descarga de archivos como 0=poco y 1=mucho. En el caso de la variable uso de la banca *online* la categoría "no" se codificó con 0 y "sí" con 1.

Por último, el *guardián capaz* se operacionalizó como aquellas personas, tácticas individuales y herramientas tecnológicas que pueden evitar un potencial ciberdelito. Así, partiendo de este concepto, se han incluido en este estudio medidas sobre prácticas o hábitos del propio usuario que lo protegen del ciberdelito. Al respecto se preguntó: 1) ¿se conecta a internet desde computadoras de uso público (laboratorios de computación, cibercafés, etc.)?, y 2) ¿nos puede indicar si ha solicitado en alguna ocasión

7 Se decidió analizar estos delitos informáticos tomando como base la Constitución de la República Bolivariana de Venezuela de 1999, el Código Penal (2005) y la Ley Especial contra los Delitos Informáticos de 2001, dado que son conductas y acciones que van en contra de lo establecido en estas normas jurídicas (Venezuela 1999; 2001; 2005).

que borren o cancelen sus datos personales de algún registro en internet? Desde un punto de vista tecnológico, se requirió información sobre los programas de protección instalados en la computadora o dispositivo móvil, en concreto, por *software* antivirus y *antimalware*. Cada una de estas respuestas fue planteada de forma dicotómica. Así, en el caso de la variable relacionada con la conexión en equipos públicos el código 1 representa la presencia de la condición y en el resto de los indicadores se reservó para identificar la ausencia.

Tipo de estudio y procedimiento

Los informes de las empresas de ciberseguridad (Symantec, Kaspersky, ESET, etc.) o de las organizaciones públicas o privadas (OEA, BID, etc.) pueden ser un recurso útil para conocer los niveles de ocurrencia de la ciberdelincuencia en distintos lugares; pero la estadística utilizada es meramente descriptiva. En tales estudios no hay ningún intento de analizar relaciones entre variables que permita comprobar, por ejemplo, bajo qué condiciones una persona es vulnerable al ciberdelito. Es decir, entre muchos otros elementos, estos trabajos prescinden del uso de estadística bivariada y multivariante.

Evidentemente, con un nivel de análisis descriptivo es difícil tener un referente teórico acerca de la cibervictimización, lo que hace necesario plantearse otras estrategias de investigación. Es por ello que se ha decidido llevar a cabo un estudio correlacional, de corte transversal, basado en la encuesta de victimización como método de medición. El diseño de esta encuesta giró en torno a un conjunto de preguntas para recabar información sobre los delitos cibernéticos sufridos por el encuestado y algunas variables de orden teórico como el caso de las actividades cotidianas que se suelen desarrollar cuando se hace uso de las TIC.

En términos operativos, luego del diseño de la encuesta se solicitó el permiso a cada profesor en horas lectivas para su aplicación y así contar con su apoyo en el control del alumnado. Se aplicó el instrumento a un total de 11 secciones, las cuales tenían un número de alumnos que oscilaba entre 15 y 70 sujetos por aula al momento de la actividad. Antes de dar inicio a la aplicación del instrumento, los estudiantes fueron informados del contenido general, extensión, forma de llenado y anonimato del mismo. Se hizo hincapié en que cualquier duda sobre algún punto del contenido podría ser consultada al encuestador. El llenado de la encuesta tomó un tiempo promedio de 25 minutos. Finalmente, se utilizó el paquete estadístico SPSS versión 20 para el vaciado y análisis de los datos.

Estrategia de análisis estadístico

En principio se desarrolló un análisis univariado para examinar las características principales de la muestra. Luego se efectuaron algunas pruebas de X^2 y se calcularon coeficientes de correlación *Phi* para determinar los niveles de independencia y asociación entre las variables predictivas y los indicadores de cibervictimización.[8] Finalmente, se utilizó la regresión lógistica binaria debido a la escala de medida de las variables criterio que en este caso fue nominal con dos valores (dicotómica). De esta manera, se pusieron a prueba cinco modelos de regresión por separado para cada indicador de cibervictimización.

8 Por razones de espacio no se presentan los resultados de los análisis bivariados. Si hay algún interés en ellos pueden solicitárselos a los autores.

Resultados

Estadística descriptiva

Según los resultados de la tabla 1, el 20% de la muestra (*N*= 61) fue víctima del acceso no autorizado a su correo electrónico y el 15% sufrió el *hackeo* de una cuenta de red social como *Twitter, Facebook, Instagram*, etc (*N*= 45). Con respecto al acoso en línea (*online harassment*), el 17% de la muestra (*N*= 52) reportó haber sido víctima de suplantación de identidad, el 20% reveló que usaron su imagen sin autorización (*N*= 60) y un 62% experimentó acoso repetidamente luego de haber prohibido un nuevo contacto (*N*= 184).

Con relación a las actividades rutinarias, el 19% de los universitarios (*N*= 58) trató con desconocidos mediante mensajería instantánea, el 12% abrió vínculos y descargó archivos extraños (*N*= 37) y un 33% proporcionó información personal en Internet (*N*= 98). Los indicadores de exposición en línea señalan que estos jóvenes se conectaron a internet, por término medio, 20,08 horas a la semana. El 68% de la muestra (*N*= 206) utilizó con mucha frecuencia el correo electrónico y las redes sociales y esa misma proporción realizó operaciones financieras en la banca *online*. En cuanto a los hábitos de protección, el 81% mencionó que tiene instalado un software antivirus en sus dispositivos (*N*= 233) y 9% algún programa *antimalware* (*N*= 26). Finalmente, el 52% de la muestra (*N*= 158) reportó haberse conectado a internet en computadoras de sitios públicos y un 42% solicitó varias veces que borraran o cancelaran sus datos personales de algún registro en internet (*N*= 120).

Tabla 1. Estadística descriptiva

	Min-Max	M (DT)
Variable		
Victimización en línea		
Hacking de correo electrónico	0-1	0,20 (0,40)
Hacking de cuenta red social	0-1	0,15 (0,36)
Suplantación de identidad	0-1	0,17 (0,38)
Uso de imagen sin permiso	0-1	0,20 (0,40)
Contacto repetido no deseado	0-1	0,62 (0,49)
Objetivo adecuado en línea		
Comunicación con extraños	0-1	0,19 (0,39)
Abrir/descargar enlaces/ archivos desconocidos	0-1	0,12 (0,32)
Proporcionar información personal	0-1	0,33 (0,47)
Exposición a delincuente motivado en línea		
Número de horas en Internet (Semana)	1-150	20,08 (24,32)
Uso correo electrónico	0-1	0,68 (0,47)
Uso redes sociales	0-1	0,68 (0,47)
Descargar archivos	0-1	0,56 (0,50)
Banca *online*	0-1	0,68 (0,47)
Guardián eficaz (tecnológico y humano)		
Software antivirus	0-1	0,81 (0,39)
Software antimalware	0-1	0,09 (0,28)
Conectarse a Internet en computadoras públicas	0-1	0,52 (0,50)
Solicitar eliminación/ cancelación datos	0-1	0,42 (0,49)
Variables de control		
Sexo (Hombre)	0-1	0,37 (0,48)
Edad	17-56	25,94 (0,09)

Análisis de regresión logística binaria

Hacking

Los resultados de los análisis multivariante basados en la técnica de regresión logística binaria se resumen en la tabla 2. Estos resultados señalan para el Modelo 1 y 2 que la mayoría de las medidas referentes a los tres elementos conceptuales de la TAR no fueron predictores significativos del *hacking.* En concreto, ninguna de las variables que conforman el constructo *objetivo adecuado en línea* tuvo correspondencia con los dos indicadores de acceso no autorizado a correos y cuentas en redes sociales.

Solo una medida de *exposición a un delincuente motivado*, en este caso el uso de banca *online,* mostró una relación estadísticamente significativa con el *hackeo* de correo electrónico pero de forma negativa (Modelo 1). En el caso del constructo *guardián eficaz*, solicitar la eliminación y cancelación de datos en registros de internet (OR=2.41) fue un predictor significativo del *hackeo* de correos electrónicos y esa misma variable (OR=2.35) junto al uso de antimalware (OR=4.55) se relacionaron con el acceso no autorizado a cuentas de redes sociales (Modelo 2). En este caso, no usar *antimalware* aumenta 83% el riesgo de *hackeo* de cuentas en *Twitter, Facebook, Instagram*, etc. Por el contrario, el uso de antivirus presentó un efecto inverso sobre el *hacking* de cuentas de redes sociales (Modelo 2).

Acoso en línea (Online harassment)

De manera muy similar al *hacking*, la Tabla 2 muestra que un gran número de medidas no presentaron una relación significativa con el acoso en línea. Específicamente, en el caso de la dimensión *objetivo adecuado en línea,* abrir o descargar enlaces/archivos desconocidos se relacionó con la probabilidad de ser victimizado por suplantación de identidad pero, en esta oportunidad, con signo negativo. Con respecto a la *exposición a un delincuente motivado,* el número de horas en internet es un predictor significativo del acoso en línea en los Modelos 4 y 5. En el caso de la victimización por uso de imágenes no autorizadas y por contacto reiterado no consentido, el mayor número de horas en internet aumenta 50% el riesgo de acoso.

Usar tanto el correo electrónico como las redes sociales se relacionó negativamente con el contacto reiterado no consentido y la suplantación de identidad. En referencia al concepto de *guardián eficaz* únicamente la variable solicitar la eliminación y cancelación de datos en registros de Internet tuvo una relación significativa (OR=2.41) con el acoso por uso de imágenes personales sin autorización (Modelo 4) y con el acoso por contacto reiterado no deseado (Modelo 5). En el primer caso disminuyó un 72% el riesgo de este tipo de acoso y en el segundo caso lo redujo un 80%. Asimismo, hay que destacar que en los Modelos 3 y 4, conectarse a internet en computadoras públicas presentó una relación negativa con las respectivas variables criterio.

En conjunto, estas medidas parecen predecir mejor el acoso por contacto repetido no deseado (R^2= 28%) que se analizó en el Modelo 5. Además, la variable solicitar la eliminación y cancelación de datos de algún registro en internet parece ser una variable clave en la predicción de los diferentes tipos de cibervictimización, dados los patrones de relación significativa que presentó en casi todos los modelos. Finalmente, las medidas usadas para operacionalizar el constructo *objetivo adecua-*

Tabla 2. Modelos de regresión logística binaria para victimización por *hacking* y *harassment* (N= 308)

	Hacking 1 (Correo electrónico) **MODELO 1**			*Hacking 2* (Cuenta red social) **MODELO 2**			*Harassment 1* (Suplantación de identidad) **MODELO 3**		
Variable	B	Wald	OR	B	Wald	OR	B	Wald	OR
Objetivo adecuado en línea									
Comunicación con extraños (Si=1)	-0.02	0.00	0.97	-0.48	0.88	0.62	-0.29	0.38	0.74
Abrir/descargar enlaces/archivos desconocidos (Si=1)	-0.59	1.08	0.56	0.13	0.04	1.14	-1.06	**3.59***	0.34
Proporcionar información personal (Si=1)	-0.62	2.71	0.54	-0.14	0.11	0.87	-0.39	0.95	0.68
Exposición a delincuente motivado en línea									
Número de horas en Internet (Semana)	-0.00	0.75	0.99	-0.01	0.67	0.99	0.01	1.58	1.01
Uso correo electrónico (Si=1)	-0.88	3.44[a]	0.41	-0.89	2.36	0.41	-1.12	**4.37***	0.33
Uso redes sociales (Si=1)	0.12	0.07	1.12	0.14	0.07	1.15	-1.02	3.09	0.36
Descargar archivos (Si=1)	-0.05	0.02	0.94	0.06	0.02	1.06	0.46	1.06	1.58
Banca *online* (Si=1)	-0.99	**4.23***	0.37	-0.65	1.54	0.52	-0.23	0.27	0.79
Guardián eficaz (tecnológico y humano)									
Software antivirus (No=1)	0.48	0.78	1.61	-0.99	**4.12***	0.37	-0.68	1.96	0.51
Software antimalware (No=1)	0.45	0.51	1.57	1.52	**6.11***	4.55	0.35	0.26	1.41
Conectarse a Internet en computadoras públicas (Si=1)	-0.71	**3.34**[a]	0.49	-0.73	2.62	0.48	-1.22	**7.64****	0.30
Solicitar eliminación/cancelación de datos (No=1)	0.88	**5.50***	2.41	0.86	**4.00***	2.35	0.31	0.59	1.36
Variables de control									
Sexo (Hombre = 1)	0.40	0.84	1.49	0.28	0.34	1.33	0.03	0.00	1.04
Edad	0.01	0.20	1.01	-0.01	0.12	0.99	0.01	0.36	1.02
2 Log-likelihood	192,63			158,43			174,19		
Modelo X^2	25.20* (df=14)			22.87[a] (df=14)			28.01*(df=14)		
Nagelkerke R^2	17%			17%			20%		

Nota: $^*p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$; $^{a}p < 0.06$

do en línea resultaron las más débiles del conjunto. En este caso, prácticamente todos los indicadores no tuvieron correspondencia con ninguna de las variables de cibervictimización analizadas y la única medida que presentó una relación significativa lo hizo con signo negativo. Esto, junto a las escasas y contradictorias relaciones encontradas en el resto de las dimensiones, ofrece un débil apoyo empírico a las hipótesis de Cohen y Felson.

Discusión y conclusiones

El objetivo principal de este estudio (quizá inédito en la región) fue identificar algunos predictores de la victimización cibernética en una muestra de estudiantes universitarios. Para ello, se ha medido un conjunto de indicadores vinculados a los tres conceptos teóricos básicos de la TAR (delincuente motivado, objetivo adecuado y falta de vigilancia eficaz) para

Tabla 2. Continuación...

	Harassment 2 (Uso de imagen sin permiso) **MODELO 4**			*Harassment 3* (Contacto repetido no deseado) **MODELO 5**		
Variable	B	Wald	OR	B	Wald	OR
Objetivo adecuado en línea						
Comunicación con extraños (Si=1)	-0.59	1.74	0.55	-0.54	1.24	0.58
Abrir/descargar enlaces/archivos desconocidos (Si=1)	-0.17	0.10	0.84	-1.07	3.13	0.34
Proporcionar información personal (Si=1)	-0.51	1.92	0.60	-0.43	1.61	0.65
Exposición a delincuente motivado en línea						
Número de horas en Internet (Semana)	0.02	**6.12***	1.02	0.02	**4.06***	1.02
Uso correo electrónico (Si=1)	-0.28	0.45	0.75	-0.77	**4.48***	0.46
Uso redes sociales (Si=1)	0.61	2.07	1.85	-0.77	**4.25***	0.46
Descargar archivos (Si=1)	0.27	0.44	1.30	0.12	0.11	1.12
Banca *online* (Si=1)	-0.72	2.72	0.49	-0.07	0.04	0.93
Guardián eficaz (tecnológico y humano)						
Software antivirus (No=1)	-0.59	1.61	0.56	0.33	0.65	1.39
Software antimalware (No=1)	-0.69	0.90	0.50	-0.48	0.66	0.62
Conectarse a Internet en computadoras públicas (Si=1)	-0.95	**5.89***	0.39	-0.60	3.26	0.55
Solicitar eliminación/cancelación de datos (No=1)	0.97	**7.29****	2.65	1.36	**15.35*****	3.89
Variables de control						
Sexo (Hombre = 1)	-0.08	0.04	0.92	-0.14	0.14	0.87
Edad	0.00	0.00	1.00	-0.00	0.19	0.99
2 Log-likelihood	201,57			245,11		
Modelo X^2	30.44**(df=14)			60.00*** (df=14)		
Nagelkerke R^2	20%			28%		
Nota: $^{*}p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$; $^{a}p < 0.06$						

tratar de responder a la pregunta: ¿qué actividades cotidianas de las que se experimentan dentro y fuera de Internet se relacionan con la probabilidad de cibervictimización? A continuación se discuten algunos resultados en el marco de esta interrogante.

Un rasgo muy notorio de estos resultados es que gran parte de las medidas analizadas no estaban relacionadas significativamente con las diferentes formas de cibervictimización. Además, el patrón de predicción y la fuerza de las pocas relaciones significativas encontradas variaban según el tipo de variable criterio analizada. El *guardián eficaz* mostró tener el efecto más fuerte y estable sobre las distintas formas de victimización cibernética, en especial sobre las de acoso en línea.

En este caso, al menos una de las medidas de este concepto se relacionó significativamente con casi todos los modos de victimización.

La *exposición a un delincuente motivado* presentó un patrón de predicción más modesto e inestable. En este caso, ninguna de las medidas utilizadas predijo el *hacking* de cuentas de redes sociales. El efecto más débil sobre la cibervictimización lo mostró el *objetivo adecuado en línea* cuyos indicadores, casi en su totalidad, no se relacionaron significativamente con las cinco variables criterio observadas. Enseguida se discuten con más detalle algunos elementos de este patrón de resultados.

En primer término, solo se hallaron tres medidas estadísticamente relacionadas con algunos de los cinco indicadores de cibervictimización conforme a las expectativas de la TAR. Concretamente, los universitarios que pasaron más tiempo en internet (lo cual debe aumentar la probabilidad de *exposición a un delincuente motivado en línea*) fueron más propensos a ser victimizados por acoso *online*. Estos resultados van en el mismo sentido de los reportados por Holt y Bossler (2009) y Ngo y Paternoster (2011) y contrarios a los obtenidos por Reyns *et al.* (2011). Las otras dos variables incluidas en la dimensión *guardián eficaz* son el uso de software antimalware (que actuó como factor de protección del *hackeo* a cuentas de redes sociales) y la solicitud de eliminación de datos en registros de Internet (la cual disminuyó el riesgo tanto de *hacking* como de *online harassment*).

En relación con esto, el efecto del *antimalware* se corresponde con lo reportado en otras investigaciones y demuestra que el uso del mismo reduce la posibilidad de que existan en el dispositivo electrónico programas maliciosos destinados a conseguir claves y datos personales. Aun cuando el efecto del *antimalware* sobre el *hacking* ha sido poco estudiado en muestras de universitarios, este hallazgo confirma su relevancia e, incluso, como lo mencionan Ngo y Paternoster (2011), lo importante de medir de manera separada los distintos indicadores de protección tecnológica (antivirus, antimalware, *firewall*) y no de forma compuesta.

Sumado a esto, el hecho de que la fuerza del efecto y el tipo de factores de riesgo/protección varíen según el indicador de victimización observado, permite especular que los correlatos y las causas de la cibervictimización pueden ser diferentes dependiendo de la naturaleza del delito que se pretenda predecir. Por ejemplo, el *hacking* que es un delito (*tipo I*) *centrado* en la computadora tal vez responda mejor a variables de carácter tecnológico (programas *antimalware*) y el acoso en línea que es un delito (*tipo II*) *asistido* por las TIC se relacione principalmente con variables de interacción social (v. gr. uso de redes sociales). Quizás este tipo de hallazgos contradice a la TAR como posible teoría *general* y sugiere el uso de enfoques específicos o tipologías para predecir y explicar mejor diversas formas de cibervictimización.

En segundo lugar, casi todos los indicadores de la dimensión *objetivo adecuado en línea* no resultaron predictores significativos de la cibervictimización. Si bien esto se logra explicar por la manera en cómo se operacionalizó este concepto en el presente estudio, también es posible que existan otro tipo de efectos que, dados los objetivos de partida, no fueron evaluados como, por ejemplo, los de mediación. Es decir, la relación que se observó en los análisis bivariados entre los indicadores del *objetivo adecuado* y la cibervictimización, puede estar influenciada por alguno de los otros conceptos de la TAR (delincuente motivado y/o guardián eficaz). De no existir tal efecto mediador, el comportamiento estadístico de las medidas de este concepto que, cabe señalar, en otras investigaciones han mostrado tener una relación significativa con la cibervictimización (Choi 2008; Marcum

et al. 2010; Reyns *et al.* 2011), puede refutar la capacidad de la TAR para predecir y explicar la victimización en el mundo virtual.

En tercer lugar, se observaron algunas relaciones estadísticamente significativas contrarias a las predicciones de las TAR. Este es el caso, por ejemplo, de abrir/descargar enlaces/archivos desconocidos, usar correo electrónico y redes sociales, conectarse a internet en computadoras públicas y disponer de antivirus. Esta última variable, en concreto, presentó una relación que está en sintonía con los hallazgos reportados por Ngo y Paternoster (2011). Una lectura somera de estas relaciones haría suponer que, por ejemplo, no usar correos electrónicos o tener instalado un antivirus contribuye a estas formas de cibervictimización. Sin embargo, este tipo de relaciones con signo contrario a las expectativas de la TAR puede ser consecuencia de la naturaleza transversal de los datos. Es decir, puesto que en este estudio no se controló el orden temporal de las relaciones es plausible sostener que una persona que ha sido víctima de ciberdelito decide, posteriormente, restringir su ingreso a páginas extrañas, limitar el uso de redes sociales y correos electrónicos o instalar un antivirus.

Queda claro que estos resultados en conjunto ofrecen, provisionalmente, poco apoyo a la aplicabilidad de la TAR para la compresión de la cibervictimización. Pero, cabe señalar que los mismos pueden tener alguna utilidad en términos preventivos. En principio, la TAR determina qué condiciones son casi siempre necesarias para aumentar la probabilidad de delito y sostiene que la ausencia de cualquiera de los tres elementos es una condición suficiente para evitar que ocurra la victimización. En este estudio se observó una mejor capacidad predictiva del elemento *guardián eficaz* en el que, concretamente, *usar programas antimalware* y *solicitar la eliminación de información personal en la red* disminuyen el riesgo de cibervictimización. Los hallazgos aquí presentados confirman la importancia del propio usuario para un control efectivo. Quien utiliza los servicios de las TIC parece desempeñar un rol básico en la cibervictimización al definir qué dispositivos tecnológicos de vigilancia (*antimalware*) y estrategias de protección no electrónicas lo convierten en un autoguardián (eficaz) de su seguridad informática.

Estos hallazgos permiten llegar a la misma conclusión de Choi (2008) con respecto a que la vigilancia efectiva puede ser el elemento fundamental de la TAR e, inclusive, por el que hay que interesarse más de cara a la prevención situacional. Si las hipótesis de Cohen y Felson son válidas, tal vez garantizando la sola presencia de este elemento situacional se consiga desestimular la decisión de cometer delitos por parte de un sujeto motivado. Dado el aparente alcance que tiene el *guardián eficaz*, las políticas y campañas de disminución de la cibervictimización (desplegadas tanto por entidades públicas como privadas) deben ir orientadas a estimular la educación y habilidades de los usuarios para una adecuada autoprotección que les permita modificar el ámbito de oportunidades delictivas en el ciberespacio.

Para concluir, aun cuando estos resultados hacen un modesto aporte a la investigación sobre la cibervictimización, hay varias limitaciones que se deben considerar. Una de las más importantes es, precisamente, la transversalidad de los datos. Sería importante en futuras investigaciones contar con datos longitudinales para desentrañar las relaciones causales entre las variables de estudio, especialmente para poder identificar si el uso de medidas de protección como el antivirus se da antes o

después de un episodio de cibervictimización. Otra limitación fue la naturaleza de la muestra que, en esta ocasión, se limitó al ámbito universitario. En este caso, analizar en futuros estudios muestras representativas de otras poblaciones permitirá mejorar la generalización de los resultados. Finalmente, la tercera limitación de esta investigación tiene que ver con la validez de los indicadores escogidos.

Sería útil en próximas investigaciones utilizar otro tipo de medidas para operacionalizar los conceptos básicos de la TAR. Incluso, se pueden probar otras técnicas de recolección de información como la metodología de viñetas basada en encuestas factoriales (Wikström, Oberwittler, Treiber y Hardie 2012, como ejemplo de este método en Criminología). Esta técnica consiste en presentarle al encuestado una situación o escenario hipotético inspirado en la vida real y evaluar las decisiones en situaciones concretas cuando se usa Internet. La finalidad de esta metodología es observar la relación de dichas decisiones o valoraciones con las variables teóricas de base y, desde luego, con la probabilidad de cibervictimización. Todo esto podría dar como resultado datos más robustos que permitan apoyar o rechazar la aplicabilidad de esta teoría criminológica para el estudio de la ciberdelincuencia y, por consiguiente, el diseño de métodos más precisos para su prevención y control.

Bibliografía

BID (Banco Interamericano de Desarrollo). 2016. *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016.* Washington: Observatorio de la Ciberseguridad en América Latina y el Caribe.

Bossler, Adam, y Thomas Holt. 2009. "Online activities, guardianship, and malware infection: An examination of Routine Activities Theory". *International Journal of Cyber Criminology* 1: 400-420.

Bossler, Adam, Thomas Holt y David May. 2013. "Predicting online harassment victimization among a juvenile population". *Youth & Society* 44 (4): 500-523.

CEPAL (Comisión Económica para América Latina y el Caribe). 2016. "Estado de la banda ancha en América Latina y el Caribe 2016. Santiago de Chile: Naciones Unidas", http://www.cepal.org/es/publicaciones/40528-estado-la-banda-ancha-america-latina-caribe-2016.

Choi, Kyung-shick. 2008. "Computer Crime Victimization and Integrated Theory: An Empirical Assessment". *International Journal of Cyber Criminology* 2 (1): 308–333.

Cohen, Lawrense y Marcus Felson. 1979. "Social change and crime rate trends: A routine activity approach". *American Sociological Review* 44: 588-608.

Eck, John y Ronald Clarke. 2003. "Classifying common police problems: A Routine activity approach". *Crime Prevention Studies* 16: 7-39.

ESET. 2011. "Aumenta el hacktivismo en América Latina", http://www.eset-la.com/centro-prensa/articulo/2011/aumenta-hacktivismo-america-latina/2572.

_____. 2016. "ESET Security Report. Latinoamérica 2016", http://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf.

Gordon, Sarah y Richard Ford. 2006. "On the definitions and classification of cybercrime". *J. Comput. Virol* 2 (1): 13-20.

Grabosky, Peter. 2001. "Virtual criminality: old wine in new bottles?". *Social and legal studies* 10 (2): 243-249.

Holt, Thomas y Adam Bossler. 2009. "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization". *Deviant Behavior* 30 (1): 1–25.

Kaspersky. 2016. "Internautas en América Latina sufren 12 ataques de malware por segundo", http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/2016/internautas-en-america-latina-sufren-doce-ataques-de-malware-por-segunda-revela-kaspersky-lab.

Leukfeldt, Eric y Majid Yar. 2016. "Applying Routine Activity Theory to Cibercrime: A Theoretical and Empirical Analysis". *Deviant Behavior* 37 (3): 263-280.

Marcum, Catherine, George Higgins y Melissa Ricketts. 2010. "Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory". *Deviant Behavior* 31 (5): 381–410.

McGuaire, Michael. 2007. "*Hypercrime: A geometry of virtual harms*". Londres: Routledge.

Miró, Fernando. 2011. "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la Teoría de las actividades cotidianas para la prevención del cibercrimen". *RECPC* 13-07: 1-55.

_____. 2013. "La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio". *Revista española de investigación criminológica* 5 (11): 1-35.

Ngo, Fawn y Raymond Paternoster. 2011. "Cybercrime victimization: An examination of individual and situational level Factors". *International Journal of Cyber Criminology* 5 (1): 773–793.

OEA (Organización de Estados Americanos). 2013. "Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos", http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf.

Reyns, Bradford, Billy Henson y Bonnie Fisher. 2011. "Being pursued online. Applying cyberlifestyle-routine activities theory to cyberstalking victimization". *Criminal Justice and Behavior*, 38 (11): 1149–1169.

Symantec. 2014a. "Tendencias de seguridad cibernética en América Latina y el Caribe", https://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends.

_____. 2014b. "Latin American + Caribbean 2013 in numbers", http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc-annex.pdf.

Tillyer, Marie y John Eck. 2009. "Routine Activities". En *21st century criminology: A reference handbook,* editado por Mitchell Miller, 279-287. Thousand Oaks: Sage.

Venezuela. 1999. "Constitución de la República Bolivariana de Venezuela". Gaceta Oficial de la República Bolivariana de Venezuela. N° 36860 del 30 de Diciembre de 1999.

_____. 2001. "Ley Especial contra Delitos Informáticos (2001)". Gaceta Oficial de la República Bolivariana de Venezuela. N° 37313 del 30 de Octubre de 2001.

_____. 2005. "Código Penal". Gaceta Oficial de la República Bolivariana de Venezuela. N° 5768E del 13 de Abril de 2005.

Wall, David. 2005. "The Internet as a conduit for criminal activity". In *Information Technology and the Criminal Justice System*, editado por April Pattavina, 77-98. EE.UU: Sage.

Wikström, Per-Olof, Dietrich Oberwittler, Kyle Treiber y Beth Hardie. 2012. *Breaking rules: The social and situational dynamics of young people's urban crime*. Oxford: University Press.

Wikström, Per-Olof, y Kyle Treiber. 2016. "Situational Theory: The Importance of Interactions and Action Mechanisms in the Explanation of Crime". En *The Handbook of Criminological Theory*, editado por Alex Piquero, 415-444. EE.UU: Wiley Blackwell.

Yar, Majid. 2005. "The novelty of cybercrime: An assessment in light of routine activity theory". *European Journal of Criminology* 2 (4): 407-427.

_____. 2006. *Cybercrime and Society*. Londres: Sage.

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2563

Urvio, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 80-93
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad

Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity

Vicente Pons Gamón[1]

Fecha de recepción: 7 de febrero de 2017
Fecha de aceptación: 26 de abril de 2017

Resumen

El artículo tiene como objetivo analizar la visión que tienen diversos autores sobre la aparición del ciberdelito en materia de terrorismo (ciberterrorismo) y la respuesta de las naciones en defensa cibernética. En primer lugar estudiamos el nacimiento de un nuevo espacio delictivo el "ciberespacio" y todas sus amenazas, en una segunda parte vemos la reacción que este fenómeno ha provocado en las naciones y organizaciones internacionales en dirección a determinar y estudiar todos estos delitos, sus causas, métodos y reacciones, para poder combatirlos desde el aspecto legal (legislación española, europea e internacional) y a partir de aquí finalizar mostrando la visión estratégica de defensa de los estados, estudiando como ejemplos las líneas de actuación que utiliza España y Europa para contrarrestar su efecto destructivo en la sociedad actual.

Palabras clave: Ciberespacio; Cibercrimen; Ciberdelincuencia; Ciberdelito; ciberterrorismo; ciberataque; ciberdefensa.

Abstract

This article aims to analyze the view of different authors about emergence of cybercrime in the terrorism area (cyberterrorism) and the nations cyber-defense response. In a first time we study the birth of a new criminal space "cyberspace" and all its threats, in a second part we see the reaction that this phenomenon has provoked to nations and international organizations in order to determine and study all these crimes, methods and reactions, so as to be able to combat them from the view legal point (Spanish, European and internacional legislation) then finish, showing the strategic vision of states defense, studying as examples the lines of action used by Spain and Europe to counteract its destructive effect on today's society.

Keywords: Cyberspace; Cybercrime; Cyberdelinquency; cyberterrorism; cyberattack; cyberdefense.

1 Licenciado por la Universidad de Valencia y Posgrado en la Facultad de Ciencias Económicas y Empresariales Universidad Nacional de educación a distancia (UNED). Máster en Seguridad y Doctorando en Derecho y Ciencias Sociales por la UNED (España). Correo: vp@infurma.es

Introducción

La aparición de internet y los sistemas informáticos supuso un antes y un después en el modo que las personas acceden a los sistemas de información, donde cada acción se encuentra reflejada, pues "la red es un nuevo espacio donde los roles de los diferentes agentes se construyen, evolucionan y cambian día a día" (Alonso García 2015, 18). También se comenzaron a evidenciar los comportamientos delictivos en torno a estos nuevos paradigmas y herramientas cibernéticas. Durante estos periodos de crecimiento de las redes informáticas, los llamados ciberdelincuentes avanzaron a pasos agigantados desarrollando técnicas y métodos para vulnerar unos sistemas de seguridad, aún inmaduros, tomando ventaja sobre las autoridades y su escasa preparación para abordar este nuevo problema.

Esta investigación se centra en las acciones delictivas en el ciberespacio, que hoy por hoy, preocupan a las naciones y a sus cuerpos de seguridad, más aún si provienen de grupos u organizaciones terroristas. Partimos, como idea clave, del nuevo concepto de ciberespacio, y veremos, entre otras, las definiciones de ciberdelincuencia y ciberterrorismo, las ventajas y las técnicas de los ciberataques. Posteriormente, se tratará de conocer la reacción y líneas de acción de naciones y organizaciones, con especial referencia a España.

Nacimiento de un nuevo espacio delictivo: el "ciberespacio"

Históricamente, comenzamos a hablar del nacimiento del internet en 1969. Desde su surgimiento, la conocemos como el conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP (trasmisión control protocol/internet protocol), que garantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcance mundial. Es interesante recordar que "la red de redes nació de la idea y de la necesidad de establecer múltiples canales de comunicación entre ordenadores" (Chicharro Lázaro 2009, 4), y que "el advenimiento de internet y su expansión han demostrado ser una de las revoluciones tecnológicas más importantes de la historia contemporánea" (Carlini 2016, 3).

Este fenómeno es tan revolucionario que en unos pocos años se produce un enorme incremento en el número de usuarios de internet, "en 1993 se estimaba que había 14 millones y en julio de 2014 rondaban los 2900 millones" (Carlini 2016, 3). En la actualidad, todos los ciudadanos y las sociedades que conforman, tienen una dependencia casi total de los sistemas informáticos para todos los procesos económicos y sociales, que además están íntimamente relacionados. Este rápido y acelerado crecimiento de las tecnologías de información abrió espacios para el delito, poniendo un arma de gran calibre en manos de los delincuentes y terroristas.

Así, desde esta misma óptica, siguiendo a Curtis (2011), podemos describir al espacio cibernético, o ciberespacio, como un dominio artificial construido por el hombre, diferenciado de los otros cuatros dominios de guerra (tierra, aire, mar y espacio); aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa. Además, el ciberespacio no está aislado sino profundamente vinculado y apoyado por medios físicos, por ejemplo las redes eléctricas. Si se ataca a esta interconexión puede tener repercusiones graves sobre

las estrategias de seguridad, nacionales e internacionales.

A partir del desarrollo acelerado de la internet, también emerge el lado oscuro y surgen nuevos términos como *cibercrimen, ciberdelito o ciberdelincuencia*, que describen de forma genérica los aspectos ilícitos cometidos en el ciberespacio y que tienen cuatro características específicas: "se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas" (Subijana Zunzunegui 2008, 171).

Centrándonos en el origen y aparición de los ciberataques, y posteriormente, ciberterrorismo, Ponce (2012) considera que "el advenimiento de la Web 2.0 revoluciona el concepto de red", donde todos compartimos información que es actualizada constantemente; y también menciona que "la Web 2.0 se ha llamado en muchas ocasiones a la Web social y los medios de comunicación que ofrece, también han incorporado este adjetivo, denominándose Medios Sociales o Social Media".

Como indica Urueña Centeno (2015) "el ataque se puede realizar desde cualquier parte del mundo, lo que ofrece al ciberdelincuente varias ventajas". Si analizamos estas ventajas podemos indicar lo siguiente: el ciberatacante se siente seguro, ya que no se expone físicamente a su víctima ni mucho menos a la posible intervención de las fuerzas de seguridad, dado que su acción delictiva se realiza *a distancia*; sensación de cómoda impunidad, al saber que hay lagunas legislativas a nivel internacional, por lo que muchos de los delitos cometidos no *se castigan*. Además, el delincuente aprovecha el anonimato de sus ciberacciones al ser complicado identificar al atacante; cualquier usuario que tenga un equipo informático y conexión a internet, con unos conocimientos técnicos que están al alcance de cualquiera y con una inversión económica no elevada, puede ejecutar un ciberataque; cualquier ciberataque conlleva un efecto de vulnerabilidad y falta de protección individual; y por último estos ataques sacuden la opinión pública y tiene gran difusión en los medios digitales de todo el mundo.

Entre los delitos tipificados como ciberdelincuencia encontramos: *el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos*. Con las últimas modificaciones legislativas, se han introducido otros delitos que emplean las tecnologías de la información y la comunicación, tales como el acoso electrónico contra la libertad de personas, el descubrimiento y revelación de secretos, la interferencia ilegal de información o datos, los delitos contra la propiedad intelectual y los abusos con fines sexuales a través de internet u otros medios de telecomunicación a menores. En el gráfico 1 se resume en series temporales, datos entre los años 2011 a 2015, que corresponden a la actividad registrada por las Fuerzas y Cuerpos de Seguridad del Estado Español (Guardia Civil y Policía Nacional) y la Policía Foral de Navarra. También se incluyen datos de los cuerpos de policía local que facilitaron estadísticas al Sistema Estadístico de Criminalidad durante el año 2015. Como se puede apreciar la tendencia al alza es continua, produciéndose un incremento de más de 10.000 delitos en 2015 con respecto a 2014.

Gráfico 1. Cibercriminalidad y principales tipologías penales cometidas con las nuevas tecnologías

Grupos delictivos	2011	2012	2013	2014	2015
Acceso e interceptación ilícita	1.492	1.701	1.805	1.851	2.386
Interferencia en los datos y en el sistema	228	298	359	440	900
Falsificación informática	1.860	1.625	1.608	1.874	2.361
Fraude informático	21.075	27.231	26.664	32.842	40.864
Delitos sexuales	755	715	768	974	1.233
Contra la propiedad industrial/intelectual	222	144	172	183	167
Contra el honor	1.941	1.891	1.963	2.212	2.131
Amenazas y coacciones	9.839	9.207	9.064	9.559	10.112
Total	**37.412**	**42.812**	**42.403**	**49.935**	**60.154**

Fuente: Ministerio del Interior, España (2016).

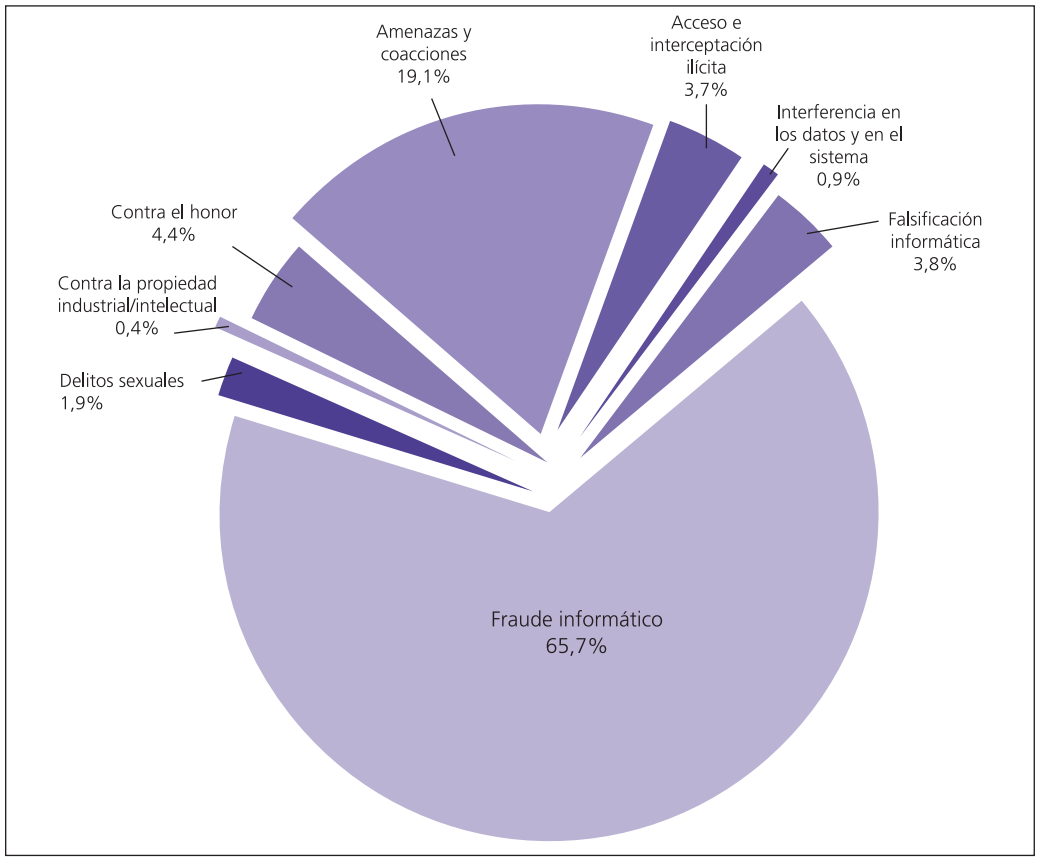
En el gráfico 2 se observa la distribución porcentual de los ciberdelitos en 2015, de los cuales podemos indicar que el fraude informático (65,7%) es el principal delito cometido en la actualidad, seguido de las amenazas y coacciones (19,1%) y la falsificación informática (3,8%).

Centrándonos ahora en los instrumentos o técnicas que se utilizan en los ciberataques de mayor o menor intensidad y siguiendo a Urueña Centeno (2015, 4-5) y el último informe de la Agencia europea para la Seguridad de las Redes y de la Información (ENISA), hacemos referencia a las quince amenazas más relevantes: *Malware*; ataques basados en el uso de la web; ataques basados en aplicaciones web; denegación de servicio; *botnets*; *phishing*; correo basura (*spam*); *ransomware*; amenaza interna; daños físicos, robos o pérdidas; kit de explotación de vulnerabilidades; violación de datos; robo de identidad; fuga de información; y ciberespionaje.

El *malware* es el nombre que agrupa a distintos *software* maliciosos como virus, gusanos o caballos de Troya, que crecen rápidamente y afectan a los contenidos de los sistemas informáticos al que accede. En relación con los ataques basados en el uso de la web, hay que indicar que existe gran variedad, como por ejemplo, las web que visita el usuario y compromete a su equipo, abren puertas traseras y vulneran su navegador. También se usan ataques a través de una aplicación web, quedando expuestos o vulnerables sectores importantes como la administración pública.

Los ataques por denegación de servicio (DDoS, *Denial of service*) hacen que sea imposible el acceso a los propios recursos y servicios de una organización o empresa y posteriormente solicitan un rescate para detener los ataques. El "*bot*" es otro programa malicioso utilizado para tomar el control de un equipo informático, sin que sea detectado fácilmente. El *phishing* es el término informático que se utiliza cuando el atacante intenta suplantar la identidad de cualquier víctima para adquirir su información confidencial. El conocido de forma universal como spam o correo basura, centra su acción en el envío de correos a un gran número de usuarios perjudicando al receptor.

Gráfico 2. Porcentaje de tipos penales relacionados con la cibercriminalidad en España (2015)



Fuente: Ministerio del Interior, España (2016).

El *ransomware* es otro software malicioso que infecta y le da al atacante la posibilidad de bloquear su equipo informático y controlar sus datos. En relación con la amenaza interna hay que indicar que se trata de una persona o agente, normalmente empleado o funcionario de una institución que tiene acceso a los programas informáticos de la organización para causar un incidente grave de seguridad. El robo o pérdida de material sensible, también se considera como una amenaza que afecta a la fuga de datos y robos de identidad. Si se tiene un conocimiento y habilidades especiales, se puede desarrollar un kit de explotación de vulnerabilidades de seguridad para tener una posición dominante sobre los competidores tanto económicos como institucionales, esas habilidades pueden proporcionar una brecha o violación de datos de carácter confidencial, robar la identidad, violar los datos correspondientes a registros personales, o realizar operaciones de espionaje cibernético a gran escala.

Cabe esperar, por su grado de importancia, que las autoridades mundiales encargadas de defender y aplicar leyes enciendan motores, para evitar y perseguir este tipo de delitos.

Analizando los alcances e implicaciones de los medios informáticos en acciones delictivas, podemos hacer un recorrido por la definición de *ciberterrorismo*, partiendo que "delito informático o ciberdelincuencia, es toda aquella acción ilegal que se da por las vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet" (Urueña Centeno 2015, 2). Muchos de esos delitos, aún no están tipificados como tales en la ley y se definen actualmente como abusos informáticos. La forma más destructiva de ciberdelincuencia es el ciberterrorismo donde convergen el ciberespacio y el terrorismo, por lo que esta forma de acción utiliza las tecnologías de la información para conseguir sus fines, intimidando, atemorizando y causando daño a sus víctimas. Actualmente, para la preparación y ejecución de casi la totalidad de acciones terroristas están apoyadas cibernéticamente o utilizan en algún momento medios cibernéticos en su realización bien para comunicación o acción.

Chicharro Lázaro (2013) define ciberterrorismo como "el uso de las nuevas tecnologías con fines terroristas". Los terroristas pueden usar las herramientas informáticas como objeto de ocasionar daños, lanzando ataques de cualquier tipo contra equipos informáticos, redes o información recogida en ellos. También, pueden ejecutar atentados a través del empleo de cualquier acción de las contempladas anteriormente contra los sistemas individuales y de redes, causando daños físicos, y por último, pueden servirse de internet para su propaganda, incitación, amenazas, hacer proselitismo, financiar sus ataques y reclutar a nuevos simpatizantes que con un poco de entrenamiento y consignas estarán en condiciones de servir a la causa terrorista.

Si nos referimos al uso que los terroristas hacen en este nuevo ciberespacio, hay que indicar, tal y como refiere Conway (2006, 7), que internet tiene la capacidad de conectar no solo a miembros de las mismas organizaciones terroristas, sino también a miembros de diferentes grupos. Así por ejemplo, existen cientos de sitios "yihadistas" en todo el mundo que expresan su apoyo al terrorismo, y en estas web y foros conexos que permiten a terroristas en lugares tan lejanos como Chechenia, Palestina, Indonesia, Afganistán, Turquía, Irak, Malasia, Filipinas y Líbano intercambiar no solo ideas y sugerencias, sino también información práctica sobre cómo construir bombas, establecer células terroristas y, en última instancia, perpetrar ataques.

El Consejo de Europa define el ciberterrorismo como al "terrorismo que utiliza las tecnologías de la información para poder intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos" (Subijana Zunzunegui 2008). La ciberdelincuencia y el ciberterrorismo buscan desestabilizar las estructuras sociales establecidas. España fue el tercer país, tras Estados Unidos y Reino Unido, que mayor número de ataques cibernéticos sufrió en 2014. Según declaraciones del ministro de Asuntos Exteriores, existieron más de 70.000 ciberincidentes de los que no detalló la gravedad (González 2015). Los crímenes del ciberterrorismo, cuando tienen intención de causar pánico colectivo, una alarma social generalizada, responden a una motivación ideológica determinada, conllevan implicaciones más graves que los delitos comunes para la seguridad nacional y la política de defensa.

Determinando que el origen del ciberterrorismo radica intrínsecamente en su misma raíz como *espacio cibernético*, escenario dónde se desarrollan las amenazas cibernéticas. Si tomamos como base la conceptualización emanada del Departamento de Defensa de los

Estados Unidos (2016), el ciberespacio sería "un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores". Estas nuevas ventajas son usadas por las organizaciones terroristas para el cumplimiento de sus objetivos estratégicos, el funcionamiento de cuidadosas estrategias de marketing, una adecuada utilización de redes sociales virtuales, y así conseguir recursos económicos y otros, con el fin de realizar su cruzada armamentista.

Existe un consenso alrededor de esto, y es que los ciberataques, en sus diferentes modalidades, entre las que se encuentra su máxima expresión, el ciberterrorismo, representan la mayor amenaza no solo para el individuo, sino también para la sociedad en su conjunto. Se considera que los "ciberataques son hoy en día la estrategia de guerra más poderosa" (Urueña Centeno 2015). A raíz de esto, el Consejo de Europa, en su Convenio sobre la ciberdelincuencia promulgado el 23 de noviembre de 2001 en Budapest, y ratificado por España el año 2010, engloba las actuaciones de ciberdelincuencia y tipifican las diversas actividades realizadas en el ciberespacio, dirigidas a diversos objetivos, que por su naturaleza serían constitutivos de delito. Entre estas, podemos encontrar delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos (acceso ilícito, interceptación ilícita, interferencia en datos, interferencia en el sistema y abuso de dispositivos); delitos informáticos (falsificación informática o fraude informático); delitos relacionados con el contenido (pornografía infantil: producción, puesta a disposición, difusión, adquisición o posesión de la misma por medio de un sistema informático); y delitos relacionados con infracciones de propiedad intelectual y de derechos afines (Instrumento de Ratificación 2001).

Analizando las ciberamenazas terroristas, se presupone que las consecuencias más significativas de este tipo de delitos son económicas y de imagen, aunque por supuesto, no debemos quitar importancia a los relacionados con el contenido. Los ataques son cada vez más sofisticados y afectan redes informáticas que en teoría disponen de niveles de seguridad extremos, es entonces cuando a este análisis de las implicaciones de los ciberataques, el factor económico aparece con un elemento que definido como "inteligencia económica como el conjunto de acciones coordinadas de investigación, tratamiento y distribución de la información para tomar decisiones en el orden económico" (Olier Arenas 2013, 9). Estas acciones se focalizan en el ámbito de economía nacional y también a menor nivel en sectores pequeños sectores empresariales, dada la globalización de los mercados que pone también en riesgo a las compañías menores.

En el mismo orden de ideas aparece otro fenómeno delictivo, *el ciberespionaje*, que afecta de manera obvia a la seguridad de la información, tiene amplia incidencia en el sector económico, debido a que "las grandes empresas multinacionales sufren igualmente el acoso de espías electrónicos, en busca de información sobre nuevos proyectos de desarrollo, en un entorno altamente globalizado y competitivo" (Ruiz Díaz 2016, 14). Una vez definido el nuevo espacio virtual donde se cometen determinados delitos, gracias a las ventajas sobre la forma tradicional que realizan los delincuentes o terroristas, y conocidos los grupos delictivos tipificados en la legisla-

ción española como ciberdelincuencia, hemos comprobado la tendencia al alza de manera continua durante los últimos años, y además, se ha tratado de determinar la definición de ciberterrorismo, por lo que podemos pasar al siguiente apartado para analizar la reacción defensiva que este fenómeno ha provocado en las naciones, para poder combatirlo desde la legalidad.

Reacción de naciones y organizaciones

Desde la aparición de los ciberataques realizados por delincuentes, por el crimen organizado o por terroristas, las naciones y organizaciones han ido reaccionando de forma progresiva para enfrentarse contra esta amenaza global. De esta forma, se han creado estrategias y sistemas de respuesta para garantizar la seguridad de sus ciudadanos y empresas. Así, se han ido modificando y adaptando la legislación de los distintos países y organizaciones. En el ámbito jurídico internacional, siguiendo el *ius ad bellum* de la Carta de las Naciones Unidas (ONU), este tipo de ataques cibernéticos de un Estado contra otro, tienen la siguiente consideración: podrían ser considerado como "uso de la fuerza" y pueden provocar un conflicto armado internacional; el Estado atacado tendría derecho a defenderse legítimamente mediante un ataque armado; de forma general el Consejo de Seguridad considera estos actos como de agresión y amenaza a la paz, por lo que podría intervenir para restablecer la paz y la seguridad internacional.

Carlini (2006, 8) indica que "para entender mejor los ataques cibernéticos como *uso de la fuerza* tendría que tenerse en consideración el instrumento, el objeto y un enfoque basado en los efectos". Igualmente el trabajo realizado por el Grupo de Expertos del Centro de Excelencia de la OTAN (Organización del Tratado del Atlántico Norte, *North Atlantic Treaty Organization NATO*) para la Ciberdefensa de Tallín, menciona que el derecho internacional vigente es de aplicación a las operaciones cibernéticas y los Estados podrán ejercer el derecho de la legítima defensa (CCDCOE 2013).

Este tipo de actos y la dificultad para su tipificación en materia jurídica ha obligado a las naciones a actualizar los conceptos de seguridad y defensa, debido a las diversas razones que han producido un incremento del riesgo.[2] Entre estas, encontramos "la diversificación de actores (o activos que son potenciales objetivos), dentro de la seguridad y la defensa (organizaciones públicas, civiles y militares, organizaciones privadas y ciudadanos)"; y la "diversificación y aumento de las amenazas (los terroristas y las organizaciones criminales, las naciones hostiles, personal descontento, catástrofes naturales y el simple ciudadano que persigue notoriedad)" (Pastor Acosta *et. al*. 2009).

Este incremento de riesgos está asociado a las vulnerabilidades de los sistemas, de acuerdo a la Escuela de Altos Estudios para la Defensa Española, que lo define como "cualquier debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas". Las vulnerabilidades no solo son características inherentes a la naturaleza de sus activos, pues también se considera una vulnerabilidad la presencia de errores de diseño, implementación, operación o administración de un sistema de información pudiendo ser explotados,

2 Riesgo: estimación del grado de exposición a que una amenaza se materialice, a través de las vulnerabilidades, sobre uno o más activos causando daños o perjuicios sobre los mismos.

y deriven en un efecto no deseado o no esperado que comprometa la directiva de seguridad del sistema (Ministerio de Defensa 2014).

Para contrarrestar los riesgos y vulnerabilidades, los Estados toman las medidas necesarias, pero estos no pueden tomar acciones fuera de pactos internacionales, si nos atenemos al artículo 2 (párrafo 4) de la Carta de la ONU sobre el "uso de la fuerza". Aun así, los Estados afectados deben responder mediante su Derecho Penal nacional antes de tomar en consideración una intervención del Consejo de Seguridad, para preservar la paz y la seguridad. Además, hay que tipificar los delitos graves suficientemente para que se puedan enjuiciar y sancionar estas conductas terroristas descritas, de forma que quede debidamente reflejada la gravedad del delito. Las acciones terroristas constituyen el máximo exponente de nuevas amenazas que el terrorismo internacional plantea a las sociedades abiertas, que pretenden poner en riesgo los pilares en los que se sustenta el Estado de Derecho y el marco de convivencia de las democracias del mundo (Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo).

El terrorismo internacional, concretamente el yihadista, se caracteriza ser el que más emplea la red para la divulgación de sus ideas y sus métodos de ataques, así incorporan nuevas formas de agresión, sobre todo orientadas a la captación, adiestramiento o adoctrinamiento en el odio, que no tendrán reparaos en emplear de manera cruel contra sus enemigos. Los Estados deben, combatir esta amenaza con todos sus instrumentos legales a su alcance.

Si particularizamos en el caso español, las herramientas legales son de diversa índole, su legislación relacionada con la Seguridad Nacional y Ciberdefensa, se encuentra recogida en la Ley 36/2015, de 28 de septiembre de Seguridad Nacional, en la Estrategia de Seguridad Nacional de 2013, la Estrategia de Ciberseguridad Nacional de 2013 (Consejo de Seguridad Nacional 2013), y concretamente, en un conjunto de artículos del Código Penal español y Leyes tratan directa o indirectamente el tema del terrorismo: Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo.

Además, el Estado español modificó sus estructuras, en varios ministerios, para dar respuesta a las ciberamenazas y ciberterrorismo, por ejemplo se creó el Instituto Nacional de Ciberseguridad (INCIBE)[3], la Oficina Nacional de Seguridad (ONS), el Centro Criptológico Nacional (CCN), el Mando Conjunto de Ciberdefensa, el Centro Nacional para la protección de las Infraestructuras Críticas (CNPIC), o unidades especializadas dentro de los cuerpos de seguridad como el Grupo de Delitos Telemáticos y Grupo de Ciberterrorismo de la Guardia Civil.

En el seno del INCIBE opera el centro de respuesta a incidentes de ciberseguridad (*ComputerEmergency Response Team* CERT) de Seguridad e Industria (CERTSI)[4], que por Acuerdo del Consejo Nacional de Ciberseguridad de 29 de mayo de 2015 es el CERT Nacio-

3 El INCIBE es un organismo que trabaja en la prevención y protección frente a incidentes de seguridad de la información que colabora con iniciativas de colaboración público-privadas para mejorar los niveles de ciberseguridad en España.

4 El CERTSI es un centro de respuestas a incidentes derivados de las tecnologías de la información de las infraestructuras críticas ubicadas en España y actúa como la primera línea estratégica de acción que incrementa la capacidas de prevención, detección, investigación y respuesta ante las ciberamenazas.

nal competente en la prevención, mitigación y respuesta ante incidentes de ciberseguridad. El CERTSI ofrece capacidad tecnológica y de coordinación, de forma continuada 24 horas al día, 7 días a la semana, en tres ámbitos diferenciados: ciudadanos y empresas; Instituciones afiliadas a la RedIRIS; y operadores estratégicos y de infraestructuras críticas.

La experiencia de lucha contra el terrorismo en España permite contar con una legislación penal eficaz que ya dio respuesta al terrorismo protagonizado por extintas bandas armadas como ETA (*Euskadi Ta Askatasuna*) o el GRAPO (Grupo de Resistencia Antifascista Primero de Octubre). El eje del tratamiento penal del terrorismo era la definición de la organización o grupo terrorista y la tipificación de aquellas conductas que cometían quienes se integraban en ellas o prestaban su colaboración. El Código Penal español no debe perder esa perspectiva de tipificación de las conductas articuladas en torno a organizaciones o grupos terroristas.

Estas nuevas amenazas exigen la actualización de la normativa para dar cabida al fenómeno del terrorismo individual y a conductas que constituyen la principal preocupación de la comunidad internacional, en línea con la Resolución 2178 del Consejo de Seguridad de Naciones Unidas. La Ley Orgánica 2/2015, modificó el Código Penal, de tal forma que, actualmente, hay una respuesta penal frente a crímenes de terrorismo ya conocidas y los procedentes de nuevas amenazas.

En concreto, en el ordenamiento jurídico español existen normas procesales de aplicación directa sobre el ciberterrorismo, que deben seguir unas reglas legales, como se refiere Subijana (2008, 182), cuando dice que:

> Una primera norma significativa en materia de ciberterrorismo es la referida a la extensión de potestad jurisdiccional de los órganos judiciales que conforman el Poder Judicial. La función jurisdiccional, en cuanto ejercicio de uno de los poderes del Estado (el de juzgar y hacer ejecutar lo juzgado), requiere normalmente, cuando se trata del ejercicio del *ius puniendi*, de la existencia de conexión entre infracción y Estado.

En este sentido, la jurisdicción de los órganos judiciales y los espacios o territorios indicará el lugar donde pueden juzgar y deben ejecutar lo juzgado. Para ello, debe de haber una conexión entre la infracción y estado que puede ser de territorio, nacionalidad o protección de intereses y concretamente en el fenómeno ciberterrorismo se puede aplicar el principio de jurisdicción universal que permite al Estado actuar fuera de su territorio, independientemente de la nacionalidad de autores o víctimas.

En resumen, hemos comprobado que la aparición de las nuevas formas criminales, como la ciberdelincuencia y el ciberterrorismo, han hecho que organizaciones como la ONU y la Unión Europea (UE), y países como España, hayan tenido que adaptar su ordenamiento jurídico para garantizar la seguridad de los ciudadanos. Estas modificaciones y adaptaciones legislativas tienen que ir acompañadas de otras líneas de acción concretas, que implican crear y organizar nuevas estructuras que bajo la dirección ejecutiva de los gobiernos van poniéndose en marcha dentro de un plan estratégico integral.

Líneas de acción de España y Europa

Para finalizar este artículo haremos un resumen de las líneas de acción cibernética de países como España, que se están llevando a cabo en el ámbito de la UE. El capítulo cuarto de

la Estrategia de Seguridad Nacional española (Departamento de Seguridad Nacional, España. 2013), establece doce ámbitos prioritarios de actuación. En el ámbito de la lucha contra el terrorismo, establece diferentes líneas de acción: actuar contra el terrorismo desde su origen (prevención); disminuir nuestras vulnerabilidades (protección); hacer frente a la actividad terrorista (persecución); y preparar la respuesta para restablecer la normalidad (resiliencia). Por otra parte, en el ámbito de la ciberseguridad, marca seis líneas de acción, que van desde el incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas, hasta la intensificación de la colaboración internacional.

Por ejemplo la Estrategia de Ciberseguridad española de 2013 detalla ocho líneas de acción (Consejo de Seguridad Nacional 2013), entre las que destacamos: incrementar la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas; garantizar y fortalecer la seguridad de los sistemas de información, redes e infraestructuras críticas; potenciar las capacidades para nvestigar y perseguir las actividades terroristas; e intensificar la colaboración internacional. Tal y como indica Pastor Acosta (2009), la UE ha realizado diversos y contundentes esfuerzos en ciberdefensa, de un lado, se ha centrado en defender las infraestructuras críticas, poniendo en marcha un programa específico con el programa europeo para la protección de las infraestructuras críticas (PEPIC), apoyado con una red de alerta de las infraestructuras criticas (*critical infraestructue warninig information network*, CIWIN); y de otro lado, en la mejora de la protección de los sistemas de información y desarrollo de una vertiente legislativa que tratara de estandarizar las leyes de los países que componen la unión europea.

Así se reflejó después de los atentados de Madrid, en marzo de 2004, la primera acción en ciberdefensa, y la Comisión Europea adoptó la Comunicación sobre protección de infraestructuras críticas sobre la que España, en mayo de 2007, aprobó el Plan Nacional de Protección de Infraestructuras Críticas, creando posteriormente el CNPIC. De los esfuerzos realizados por España, específicamente en ciberdefensa, los más destacados son la labor realizada por el CCN para incrementar la Seguridad de la Información en la Administración pública, y la participación del Ministerio de Defensa como miembro del Centro de Excelencia de Ciberdefensa Cooperativa (CCD COE) de la OTAN, ubicado en Estonia.

De esta manera, como consecuencia de estos compromisos, España participa activamente en el Centro de Excelencia de Ciberdefensa Cooperativa *(CooperativeCyberDefence Centre of Excellence, CCD COE)* que la OTAN estableció en Tallín, Estonia, tras firmar el *MoU* del 14 de mayo de 2008. El CCD COE es una organización multinacional que proporciona I+D[5] y servicios de formación a la OTAN, entre otras. Además, abierta a la participación de todos los miembros de la OTAN, y con la posibilidad de firmar acuerdos con organizaciones ajenas a la OTAN, como universidades, empresas, centros, etc., centrará su trabajo en las siguientes áreas fundamentales en ciberdefensa: desarrollo de doctrinas y conceptos; formación y concienciación; investigación y desarrollo; análisis y lecciones aprendidas y consulta.

También, en el marco de la UE, se creó el Centro Europeo de Cibercrimen (EC3), de-

5 El término I+D, (en inglés R&D, research and development), se refiere a la investigación y desarrollo, que persiguen las organizaciones públicas y privadas para desarrollar nuevos productos o mejorar los existentes por medio de la investigación científica.

pendiente de Europol, que se ocupa de los delitos relacionados con ciberterrorismo, desde enero de 2013, centrándose principalmente en delitos de fraude económico, los relacionados con ataques informáticos a empresas o infraestructuras críticas y explotación sexual infantil, así como a la recogida de información de inteligencia, de gran variedad de fuentes tanto públicas como privadas a fin de alimentar una base de datos policiales, que permita facilitar información a los países miembros (Ruiz Díaz 2016). Por último, hay que indicar que este resumen de las líneas de acción que realiza España en el ámbito de la Unión Europea, tiene que realizarse con la colaboración y coordinación de todas las instituciones, tanto públicas como privadas que además tienen que estar en continua actualización y contar con el amparo legislativo necesario, si queremos hacer frente de forma global a todas las amenazas emergentes, especialmente las ciberamenazas.

Conclusiones

Con la aparición del ciberespacio, el hábitat delictivo ha crecido exponencialmente, pues la era de la información multiplica las oportunidades de los delincuentes. El ciberterrorismo, y en particular, el yihadista, se aprovecha de la existencia del ciberespacio para magnificar sus ataques y se ha convertido en la mayor pesadilla para la seguridad de las naciones occidentales. Tiene unas características tan amplias y destructivas que exige una respuesta inmediata, contundente, unida, continuada e incansable de las naciones. Nacen tantas amenazas desde cualquier lugar del mundo, la mano es tan larga y puede ser tan destructiva, que los Estados deben responder a tanto y tan rápido, que de no hacerlo, se podrían causar daños humanos, sociales y económicos irreparables.

Una vez determinados los nuevos delitos y sus penas, podemos decir que las leyes deben estar atentas a los cambios constantes de las amenazas, porque de no hacerlo los delincuentes sacarían un gran partido de ello. Así la UE y sus miembros, siguen la línea de estandarizar todo lo posible los delitos y sus legislaciones propias antiterroristas, para en consecuencia poder combatir de forma compacta y unida este germen llamado ciberterrorismo. De forma seguida, al análisis legislativo y hablando ya de las directrices defensivas, tras nuestro análisis, intuimos que para el éxito en la lucha contra el ciberterrorismo, no sirve un sistema de defensa nacional simple y convencional, además de la tecnología más moderna, se necesita un conjunto de sistemas de defensa que a su vez se unen a otros, creciendo según aumentamos fronteras, esto nos hace concluir que la ciberdefensa es un gran entramado mundial de sistemas defensivos. La UE y la OTAN tratan de marcar las directrices de esta lucha en Europa.

España como ejemplo descrito, cuenta con experiencia de años en el marco terrorista (las desarticuladas ETA y GRAPO), unas líneas estratégicas y unos marcos de cooperación con la UE, OTAN y la comunidad internacional, que son plausibles y que le permiten defenderse contundentemente dentro de sus fronteras. Tras el análisis conjunto de toda la información recopilada en este artículo, podemos decir que apoyado en la ley, el mundo civilizado ha creado un gran sistema u organigrama defensivo que crece, actualizándose continuamente, en medios económicos, humanos y tecnológicos para poder mantenerse efectivo y contrarrestar el poder destructivo de los ciberdelincuentes.

Bibliografía

Alonso García, Javier. 2015. *Derecho penal y redes sociales*. Madrid: Aranzadi.

Carlini, Agnese. 2016. "Ciberseguridad: Un nuevo desafío para la comunidad internacional", http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO67-2016_Ciberseguridad_Desafio_ComunidadInt_ACarlini.pdf

Carta de las Naciones Unidas. 26 de junio de 1945, http://www.un.org/es/sections/uncharter/chapter-i/index.html.

CCDCOE. 2013. "NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual Process", https://ccdcoe.org/tallinn-manual.html.

Consejo de Seguridad Nacional. 2013. "Estrategia de Ciberseguridad Nacional de 2013", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf.

Conway, Maura. 2006. "Terrorism and the Internet: New Media–New Threat?". *Parliamentary Affairs 59* (2): 283-298.

Curtis E. Lemay Center. 2011. "Introduction to cyberspaceoperations", https://doctrine.af.mil/download.jsp?filename=3-12-D01-CYBER-Introduction.pdf.

Chicharro Lázaro, Alicia. 2009. "La labor legislativa del consejo de Europa frente a la utilización de internet con fines terroristas". *Revista de Internet, Derecho y Política* 9 (2009): 1-14. https://dialnet.unirioja.es/servlet/articulo?codigo=3101795

_____ 2013. "La violencia terrorista en el ciberespacio: Riesgos y normativa europea sobre ciberterrorismo". En *La Sociedad Ruido/ Entre el dato y el grito*, editado por Javier Herrero et al, 80-81. La Laguna (Tenerife): Sociedad Latina de Comunicación Social. http://www.revistalatinacs.org/068/cuadernos/cac53.pdf

Departamento de Defensa, USA. 2016. "Dictionary of Military and Associated Terms. Joint Publication 1-02", https://fas.org/irp/doddir/dod/jp1_02.pdf.

Departamento de Seguridad Nacional, España. 2013. "Estrategia de Seguridad Nacional. Un proyecto compartido", http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional.

ENISA. 2017. "European Union Agency for Network and Information Security. Threat Landscape Report 2016", https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.

Europol. 2013. "European Cybercrime Centre-EC3", https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

González, Miguel. 2015. "España es, tras EEUU y Reino Unido, el país que sufre más ciberataques". *El País*, 5 de febrero. http://politica.elpais.com/politica/2015/02/05/actualidad/1423136881_175042.html.

IEEE (Instituto Español de Estudios Estratégicos). 2010. "Ciberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio", http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf.

Instrumento de Ratificación 2001, de 23 de noviembre, del convenio sobre la ciberdelincuencia (BOE núm. 226 de 17 de septiembre de 2010). https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf.

Ministerio de Defensa, España. 2014. "Documentos de Seguridad y Defensa 60. Estrategia de la información y seguridad en el ciberespacio. Escuela de Altos Estudios de

la Defensa", http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/060_ESTRATEGIA_DE_LA_INFORMACION_Y_SEGURIDAD_EN_EL_CIBERESPACIO.pdf.

Ministerio del Interior, España. 2016. "Anuario estadístico del Ministerio del Interior 2015", http://www.interior.gob.es/documents/642317/1204854/Anuario-Estadistico-2015.pdf/03be89e1-dd38-47a2-9ce8-ccdd74659741.

Olier Arenas, Eduardo. 2013. "Inteligencia estratégica y seguridad económica". *En la inteligencia económica en un mundo globalizado*, editado por Secretaría General Técnica del Ministerio de Defensa, 9-31. Madrid: Ministerio de Defensa. Recuperado de:http://www.ieee.es/Galerias/fichero/cuadernos/CE_162_La_inteligencia_economica_en_un_mundo_globalizado.pdf

Pastor Acosta, Óscar, José Antonio Pérez Rodríguez, Daniel Arnáiz de la Torre y Pedro Taboso Ballesteros. 2009. *Seguridad nacional y ciberdefensa*. Cuadernos Cátedra ISDEFE-UPM 6. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones. http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

Ponce, Isabel. 2012. "Monográfico: Redes Sociales", http://recursostic.educacion.es/observatorio/web/ca/internet/web-20/1043-redes-sociales?showall=1.

Ruiz Díaz, Joaquín. 2016. "Ciberamenazas: ¿el terrorismo del futuro?", http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf.

Subijana Zunzunegui, Ignacio José. 2008. "El ciberterrorismo: Una perspectiva legal y judicial". Eguzkilore, 22 (2008): 169-187. http://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf.

Urueña Centeno, Francisco Javier. 2015. "Ciberataques, la mayor amenaza actual", http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf.

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2577

Urvio, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 94-109
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

The new era of information as power and the field of Cyber Intelligence

La nueva era de la información como poder y el campo de la ciberinteligencia

Camila Gomes de Assis[1]

Date of receipt: February 13, 2017
Date of acceptance: April 20, 2017

Abstract
This article seeks to describe the interference of cybernetics as a key intervening factor in the consolidation of information as a power resource in the 21st century. Aware that information is the main substrate for the practice of intelligence, the studies carried out also seek to understand the transformations generated by the inclusion of cyberspace in this practice, highlighting how the particular characteristics of this domain are responsible for generating new demands to States in terms of defense and security. In order to achieve the proposed objectives, this paper is structured into three main discussion topics. The first one will hold a brief discussion about the particular characteristics of this new domain and its political significance to International Relations. The second topic will deal directly with the issues of intelligence and an evaluation of the interference of cyberspace in the intelligence practice will be carried out focusing on the study of the North American - dedicating a third topic to such discussion. In methodological terms it is a descriptive work; therefore, it will be guide by the analysis of international events that approach this subject, as well as by the literature that dedicated to such discussions. This article does not seek to end with such questions, but to present itself as a north to future discussions on this subject.

Keywords: Cyberspace; Cyber-Intelligence; International Relations; Power.

Resumen
Este artículo pretende describir la interferencia de la cibernética como un factor clave para la consolidación de la información como recurso de poder en el siglo XXI. Conscientes de que la información es el principal soporte para la práctica de la inteligencia, los estudios realizados también buscan comprender las transformaciones generadas por la inclusión del ciberespacio en esta práctica, destacando cómo las características particulares de este ámbito son responsables por generar nuevas demandas a los Estados en términos de defensa y seguridad. Con el fin de lograr los objetivos propuestos, este documento se estructura en tres temas principales de discusión. La primera tendrá una breve discusión sobre las características particulares de este nuevo dominio y su significado político para las Relaciones Internacionales. El segundo tema abordará directamente las cuestiones de inteligencia. Una evaluación de la interferencia del ciberespacio en la práctica de inteligencia se llevará a cabo centrándose en el estudio de los norteamericanos - dedicando un tercer tema a dicha discusión. En términos metodológicos es un trabajo descriptivo; por lo tanto, será guiado por el análisis de los eventos internacionales que abordan este tema, así como por la literatura dedicada a tales discusiones. Este artículo no pretende terminar con tales preguntas, sino presentarse como un norte a discusiones futuras sobre este tema.

Palabras clave: Ciberespacio; Ciber-Inteligencia; Relaciones Internacionales; Poder.

1 Master's Degree in International Relations for the Postgraduate Program Santiago Dantas (Unesp, Unicamp, PUC-SP - Brazil). Graduated in International Relations from Universidade Estadual Paulista (UNESP), Brazil. Researcher at the Defense and International Security Studies Group (Gedes). E-mail: camilagomesdeassis@gmail.com

Introduction

In June 2013, Edward Snowden, a former employee of the US National Security Agency (NSA), reported, with contribution from the journals *Washington Post* and *The Guardian,* confidential information responsible for reveal a national and international surveillance scheme carried out by the US government. This surveillance was implemented through the usage of a program entitled PRISM.[2] This program was responsible for conducting a rigorous monitoring of the North American citizens and the international community through internet access. Counting for this with the collaboration of large social media companies like *Facebook, Microsoft, Apple, Google* and *Youtube*.[3]

According to information disclosed, the volume of data in the possession of the US government is huge. Almost all of the information exchanged on the Internet, such as emails, videos, photos, and browsing history were under the disposition of the United States government. The statement that international leaders were also under US surveillance, like the Brazilian president Dilma Rousseff and the German Chancellor Angela Merkel, generated a great international repercussion.[4]

Multilateral forums such as the UN were place within which gained relevance the discussion about the need to devise new mechanisms that would allow States to protect information considered confidential and strategic to maintain their stability and promoting their interests in an international environment. The discussion about the need to preserve human rights in this new domain also gained prominence.[5] In a resolution signed in November 2013, under the coordination of Brazil and Germany, during the UN General Assembly, was declared that

> […] illegal surveillance of communications, their interception, as well as the illegal collection of personal data constitute a highly intrusive act that violates the right to privacy and freedom of expression and may threaten the foundations of a democratic society (UN 2013, 2)

Reaffirming:

> the human right of individuals to privacy and not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, and the right to enjoy protection of the law against such interferences and attacks, and recognizing that the exercise of the right to privacy is an essential requirement for the realization of the right to freedom of expression and to hold opinions without interference, and one of the foundations of a democratic society (UN 2013, 1).

Based on the above mentioned, it is observed that the episode in question, and the international convulsion generated by it highlighted

2 This information has been removed from: Black, Ian. 2013. "NSA spying scandal: what we have learned". The guardian, 10 june. https://www.theguardian.com/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned.

3 This information has been removed from: Greenwald Glenn, Ewen MacAskill y Laura Poitras. The 2013. "Edward Snowden: the whistleblower behind the NSA surveillance revelations". The guardian, 11 june. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

4 This information has been removed from: Ball, James. 2013. "NSA monitored calls of 35 world leaders after US official handed over contacts". The Guardian, 25 october. https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

5 This information has been removed from: BBC News, 2013. The UN General Assembly adopts anti-spy resolution.,http://www.bbc.com/news/world-latin-america-25441408.

a fundamental question: the fact that the practice of collecting confidential information in order to build strategies favorable to a given State is not a new practice, however, its use through cyberspace is. Leading, consequently, to transformations *in the manner in which* and *in the intensity with which* this activity is performed (Nye 2010, 3). Conducing to the emergence of new challenges to States in all fields, including security and defense issues (Lopes 2013). In this way, it can be affirmed that the Information Revolution of the 20th century, based on rapid technological advances in computers and communications, only collaborated to consolidate information as a fundamental strategic asset to the States, reshaping the use of this resource (Minc y Nora 1981; Libick 2009; Kello 2012).

The Information Revolution described was responsible, therefore, for promoting extraordinary declines in the costs of creating, processing, transmitting and searching information (Nye 2014). Leading not only to changes in the forms of social and individual interaction as pointed out by sociologists Manuel Castells (1999) and Pierry Lévy (1999), but also in the dynamics of interstate relations, such as Nye (2010), Clark and Knake (2010), John Arquill a and David Ronfeldt (1993) and Libicki (2009)[6] pointed out. The changes associated with the emergence of these new technologies conduce to the conformation of a new domain: cyberspace, within which international practices will be remodeled in terms of power (Libicki 2009).

In this sense, as the Information and Communication Technologies (ICTs) revolution spreads around the globe, it modifies the way we do business and conduct policy between and among nations, changing, according to Nye (2010), the nature of Intelligence, opposition politics and war. The present article will focus on the studies of this interference within intelligence activities. In this way the central objective of this work is to describe the influence of the so-called New Technologies of Information and Communication (NICT), represented here by the inclusion of cyberspace, within the National Intelligence Services, presenting the new challenges and threats imposed to the practice of intelligence, and therefore to the role played by information as an instrument to exercise power in the 21st century.

In general terms, it is intended to briefly conceptualize what cyberspace is, its general impact on international dynamics, and, finally, to focus on the issues that debate its interference in the practice of intelligence. In view of the intentions presented, the article is structured into three main discussion topics. The first one will hold a brief discussion

6 For a better understanding of the interference of cyberspace to the practice of International Relations it is recommended to verify such authors: (I) Joseph Nye in his work "*Cyberpower*" (2010) seeks to describe what cyberpower comes to be and how this kind of power, with particular characteristics, inserts within the struggle between nations in international environment.. (II) Clark and Knake wrote the book "*Cyber War: the nex threat to national security and what to do about it*". This work is centralized in the discussion about the incorporation of cyberspace to North American policy, focusing on the interference of this element within the practices of defense and security policies. (III) The book ""*Cyberwar is coming!*" written by John Arquilla and David Ronfeldt (1993) manifests itself as one of the primary literatures in addressing cyberspace in International Relations. The focus given to the author is on the interference of the cybernetic element in the conduct of war practice. (IV) Finally, Martin Libicki (2009) in his book "Cyberdeterence and Cyberwar" carried out an in-depth analysis of the interference of cyberspace with the practice of defense and war by states. Behaving as an author of fundamental importance to those who want to dwell on such studies.

about the particular characteristics of this new domain and its political significance to International Relations. The second topic will deal directly with the issues of intelligence and third topic will be dedicated to an evaluation of the interference of cyberspace in the intelligence practice focusing on the study of the North American case.

The choice of The United States as an object of analysis is justified due to the country's tradition in using technological means as an instrument to construct offensive and defensive power in the international arena (Bretton 1991; Almeida 2006). The United States is one of the first countries to give relevance to cyberspace highlighting even the interference conducted by this new domain into intelligence practice (Clark y Knake 2010). According to the official US document entitled *International Strategy for Operating in Cyberspace* (2011), the north American perception of vulnerability and opportunities imposed by the cyber domain highlights the need to employ new operational concepts of defense, including a more active cyber defense (capable for protecting the networks) allied with the development of more expressive cyber intelligence departments able to meet the new demands imposed by technological transformations in world (United States 2011, 1).

So, the relevance of the proposed discussion is evidenced, mainly due to the growing importance attached to the use of electronic communication and, therefore of cyberspace, as a primary tool to purchase Intelligence and attacking the opponent's decision-making power without the use of force within the contemporary international scene (Hare 2009). Regarding the choice of theoretical contribution, the realistic perspective was chosen to guide the reflections proposed by this paper. The realists, from classics to neorealist, usually understand international relations in a deterministic way having as a key concept to their interpretation the idea of power (Herz 1951). Among the central foundations of realism, we can also mention (i) the perception of the predominance of competition and the conflictive dimension on all forms of relations between international actors, and (ii) the concern for security as one of the great conductors of states's action (Morgenthau 1985; Vigevani, Veiga y Mariano 1994). In this way, states towards the international structure live "in the shadow of war" (Aron 1986, 52). This implies a constant contest for power, especially in the form of military power, although other forms are also possible.

The focus on the political-military dispute therefore places activities such as the practice of Intelligence by States in a position of fundamental relevance to understanding the dynamics of international relations. This practice, therefore, highlights the role of power, the need for competition, and the needs for change through the promotion, for example, of technological advancement. It is known that the Realism has interpretative gaps, since it neglects social, cultural or even economic aspects, giving exacerbated value to political-military aspects; however, is exactly this simplification that leads us to choose such theoretical side. The choice of a theoretical strand that prioritizes the political-military element helps us understand the inclusion of cybernetic issues in International Relations. Due to the current relevance of this theme and the multiple factors surrounding its understanding, it is believed that focusing on an approach that prioritizes power, and military aspects, is positive for the proposed goal. So, understanding cybers-

pace by the realistic theoretical side, allows us to interpret this as a new operational domain within which states systematically seek to increase their cybernetic capacities with a view to maximizing their Power (Acacio y Lopes 2012).

The construction of a new domain: the cyberspace

According to a technical definition, cyberspace corresponds to an operational domain marked by the use of electro-electronics and the electromagnetic spectrum for the purpose of creating, storing, modifying and exchanging information by interconnected and interdependent networks (Kuehl 2009, 29). Based on this is possible to affirm that telegraph networks, amateur radio, mobile telephony and satellite television shaped cyberspace long before the advent of the Internet (Blumenthal y Clark 2009, 206). However, it is since the scientific-technological revolution of the 1970s that such networks started to rely on information and communication technologies (ICTs) focused on computing, among which the advent of the internet stands out (Castells 1999).

Over the years, through Internet's popularization, it has become not only the main network that makes up the cyberspace, but the platform to which other technologies have converged (Bretton 1991). In this sense, when we argue about cyberspace, we often refer to the transformations caused by the inclusion of the Internet in its scope, which was responsible for eliminating the physical limitations of time and space, including in conducting military attacks (Gama Neto y Lopes 2014, 29). According to Nye (2014) the key characteristic of this recent information revolution, and consequently of this new domain, is not the speed of communications but the considerable and very significant reduction of costs for transmit, process and access information.

For all practical purposes, transmission costs have become negligible leading to a significant increase of the amount of information that can be transmitted worldwide. The cheapening of these processes made possible an expressive increase in the number of individuals that have access to this system. The popularization of this technology has undeniable political implications (Nye 2014). In the field of International Relations, we observe that the internet empowered individuals in previously unimaginable ways. Conducing, in consequence, to an increase in the number of actors responsible for influencing the international political game (Arquilla y Ronfeld 1993; Nye 2010; Hare 2009).

In contrast to the physical world, where states have the legitimate monopoly of violence and attacks are extremely costly because of the high cost of resources used, the cyber world allows overcome this physical limitations of time and space, allowing actions and attacks be executed with effectiveness and to lower costs for anyone who has an internet-connected device (Nye 2010). In a practical assessment of the international scene, focusing our evaluation on episodes that specifically involve the use of information as a transforming aspect to the power game, we can identify a series of new actors. Wikileaks, the Anonymous movement and the self-styled "the jester"-people who act alone thanks to their advanced technological mastery- often have technological capabilities comparable to many countries, presen-

ting an undeniable directly or indirectly relevance in international politics (Kuhl 2009). The inclusion of new actors, makes the international dynamic even more complex and uncertain, generating new demands for the national defense, security and intelligence sectors (Libicki 2009).

Another transforming feature of international dynamics, is the fact that cybernetics knows no boundaries, so attacks can come from distant, undisclosed locations. This, in turn, renders the international environment more "uncertain" given the difficulty in assuming responsibility for the acts practiced in this fild (Nye 2010; Libicki 2009). It happens because "most of the suggestions regarding nation states involvement in cyberattacks against other countries are generally inferred from circumstantial rather than direct, factual and conclusive evidence" (Kshetri 2014, 4). Or even if such origins are established many questions arise regarding the attribution of responsibilities. For example, if an individual in the North American territory attacks the physical infrastructure of a particular country through their computer, how is possible to determine whether it was an individual attitude or even a state-funded? This difficulty in assigning responsibilities, inevitably leads to more insecurity once they break with the constraints.

In addition, authors such as Nye (2010, 1) affirm that the ease access to cyberspace can lead to a possible change in the balance of power, because it can promote the reduction of power differences between countries, promoting a greater diffusion of the potential for state acting in the international system. It is imperative to point out that this diffusion of the potential of international action does not necessarily translate into an equality of power between nation-states. Countries such as United States continue to occupy a privileged position within international dynamics, adding to their kinetic military resources the use of technological instruments in the promotion of their economic and military power (Nye 2010).

Also based on the technical aspects involved in the conformation of the cyberspace, it is known that this in opposition to the other domains - terrestrial air and sea - is not a natural domain but created by man himself (Sheldon, 2014). This space differs from others in relation to interconnectivity. For Ventre (2011), the cybersapce transcends all the others. Through this argument, Ventre (2011) explains that there are several access points to the cyber space in the other geographical spaces, and in a similar way, according to the author, through cyberspace influence can be exerted on the other domains. In this way, actions performed in a virtual environment can generate consequences in physical environments. This possibility of diffusion of power from the virtual medium to the physical is called transversality (Ventre 2011).

Transversality as a particular feature of the fifth domain –cyberspace- is responsible to allow the projection of cybernetic power and its reflections on other domains of state action: land, sea, air and space). On the basis of the foregoing, there is now a growing vulnerability of the physical domain of states to cybernetics, since the safety and effectiveness of the operation of a wide variety of critical and strategic national infrastructures such as energy, finance, transportation, banking negotiations, communications and intelligence and security services are directly linked to and dependent on this domain (United States 2011).

Recent episodes from Estonia (2007)[7] and Georgia (2008)[8], illustrate this fragility, evidencing the strong impact of the transversality of the cyberspace in national physical infrastructures. It is observed, therefore, that the broad technological development can also lead to disadvantages. The more technologically developed nations with greater potential for cyber attack, also become the most vulnerable, since they have a greater dependence on the technological element. In light of this, cybernetics provides to states not only a greater variety of instruments to be used as resources of power, but also increases the vulnerability and instability present in the international system (Sommer y Brown 2011; Nye 2010).

Authors like Clarke and Knake (2010) affirm, from a realistic conception of this phenomenon, the undeniable presence of the possibility of new forms of conflict in the cyberspace, giving rise to the so-called "cyber wars". According to these authors: (i) cyber war is real; (ii) cyber war happens at the speed of light; (iii) cyber war is global; (iv) cyber war skips the battlefield, and (v) cyber war has begun (Clarke y Knake 2010, 30-31). On the other hand, authors like Peter Sommer and Iann Brown (2013) maintain that the great variety of events classified as cyber war represent an wrong use of the concept, since there will hardly be a purely cybernetic conflict. Despite the divergent opinions on the possibility of a purely cybernetic war, nowadays, it is possible observe, with some homogeneity, the importance attributed to cyberspace and its associated practices. Numerous countries have attached importance to these issues within their defense and security policies.

Using as an example the North American case, we observe an increasing valuation of cybernetics -and cyberspace- as a fundamental strategic component in promoting the interests and preservation of US national sovereignty since Obama's administration. At the same time is possible to identify an intensification of a discourse within which cybernetic is detected as a threat, affirming the character of urgency and danger directly associated with those issues (Jentlenson 2010). As can be seen in the section to be presented, the US government puts itself in a position of vulnerability, evidencing, after analysis, the strong deficiencies present in the defense structures and cybernetic security characteristic of the US:

> The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. . Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations (United States 2009, 1).

7 On 27 April 2007, Estonia suffered a series of cyber attacks through the DoS - denial of service attack. The Estonian government accused Russia of having motivated this attack. The allegations against the Russian government have not been proven because of the unknown origin of the attacks. The attack on Estonia's infrastructure is considered the first major cyberattack within the international relations. For more information access: Shetter, L. 2007. "Estonia Accuses Russia of" Cyber Attack "to the Country". BBC, May 17. Available in <http://www.bbc.co.uk/en/reporterbbc/story/2007/05/070517_estoniaataquesinternetrw.shtml>

8 In 2008, during a period of tension between Russia and Georgia, hackers promoted DDoS Attack (Short for Distributed Denial of Service) in order to overload Georgia's Web sites and servers in the weeks leading up to the military invasion. In the region. For more information about the épisodio consult. LEE, D. 2014. Russia and Ukraine wage "cyber-duel". BBC Brazil, 7 March. Available in http://www.bbc.co.uk/portuguese/noticias/2014/03/140307_russia_ucrania_bg.

So it is not surprising that governments express their intention to defend the strategic assets and interests of their countries in this area, seeking to acquire greater offensive and defensive power within this domain, in particular by reformulating their intelligence and Counterintelligence affecting directly the politics of security and defense of States (Gagnon 2008; Lopes 2013). The new demands imposed on states in political and military terms translate, therefore, into an increasing preoccupation to promote a cybersecurity and cyberdefense policies. Cybersecurity, as Gills Lopes (2013, 27) points out, "refers to the combat and prevention of so-called cybercrimes in the sphere of public security, and is therefore under the responsibility of police forces or even public ministries".

Cyberdefense, on the other hand, refers to the military sector, being "the set of defensive, exploratory and offensive actions in the context of a military planning, carried out in cyberspace" (Carvalho 2011, 8; Lopes 2013). It is assumed, then, that cybernetic defense means, according to Lopes (2013) to safeguard national security against cyber existential threats. Both cybersecurity and cyberdefense rely on intelligence and information security practices. In this way the changes generated by this domain become fundamental to describe the new configuration of the International Relations.

Intelligence in International Relations

Before entering the debate about the interference of cyberspace in the practice of Intelligence, we need to rescue its role in International Relations. As mentioned earlier, since the earliest times information has played a fundamental role in the struggle for power among nations, so intelligence has always been playing a fundamental role for the States in the process of conquering their interests and objectives. In general, the practice of Intelligence can be defined as:

> [..] that component of the struggle among nations that deals with information. Intelligence seeks to learn all it can about the world. But intelligence can never forget that the attainment of the truth involves a struggle with human enemy who is fighting back and that truth is not the goal but rather only a means toward victory (Shulsky 1992, 197).

When we look at the literature that deals with the role of Intelligence applied to the international scene, we can understand this activity through three different meanings: a type of information, a peculiar activity or as a type of organization (Costa Júnior 2011, 13). As outstanding Michael Herman:

> Inteliggence in government is bade on the particular set of organizations with that name: (i)"the intelligence services" or "intelligence community". Intelligence activity is what they do(ii), and intelligence knowledge, what they procude (iii) (Herman 1996, 2).

In terms of conceptual definition, intelligence as an organization is defined as a sort of state agency based on secrecy and which product, although it rewards the benefit of society, is not accessible to the citizens (Costa Júnior 2011). As important as understanding the definition of such concept is identify its usefulness in practical terms in state policies. Thus, taking over Cepik's

(2003) and Costa Júnnior's (2011) studies, one can conclude that governments have national intelligence services with the purpose of supplying eight utilities, namely (1) contributing to transform the governmental decision-making process more realistic and rational; (2) establish a process of interaction between decision makers and intelligence officers with cumulative effects; (3) give support to defensive planning capabilities and the development of the acquisition of systems and weapons; (4) obtain relevant information through diplomatic negotiations in various areas; (5) ability to subsidize military planning and the preparation of war plans; (6) anticipation of possible counterattacks by alerting civilian and military officials; (7) monitoring of priority targets and external environments, thereby reducing uncertainty and increasing knowledge and confidence; (8) preserving secrecy about the informational needs of its adversaries.

When we talk about intelligence as (ii) a type of information we can describe intelligence as all information collected, organized, analyzed and submitted to a special process of elaboration that aims to meet the demands of a decision maker (Cepik 2003; Sims 1995). Through this definition we can deduce that the basic objective of intelligence is the production of a specific knowledge for decision makers who aim to increase the probability of a correct decision and therefore the advantages over the opponent (Sims 1995, 4).

As an activity, intelligence will act in an environment where secrecy behaves as a fundamental factor, marking the competition between those states that don't want their knowledge, activities or actions to be discovered while, at the same time that they seek to acquire as much as they can about other states confidential information. So, "Intelligence as an activity may be defined as that component of struggle between adversaries that deals primarily with information" (Shulsky 1992, 2). It is, therefore, envisaged that intelligence activities simultaneously seek to obtain information from other actors at the same time as it is necessary to protect and neutralize the enemy's abilities to obtain relevant information about the functioning of the state in question. In this way, it is essential to maintain the security of a wide range of sensitive information by governments, in this context gained relevance the practice of information security (Herman 1996, 165). As Cepik points out:

> [...]The information security area seeks to protect information that, once obtained by an adversary or enemy - for example through the intelligence operations of a foreign government - could render the state and citizens vulnerable and insecure (2003, 20).

Thus, the Intelligence refers not only to espionage activities or information, but to certain types of information that are related to the defense of the State; Counterintelligence and other organizations that are responsible for conducting and coordinating this activity at the state level(Sims 1995). Being characterized, therefore, by the acquisition, analysis, processing, production and dissemination of data that are used in the area of foreign policy and national defense. The focus of this work is precisely to point out how a greater dependence on technology -with the inclusion of cyberspace- allows at the same time a greater efficiency by the States in practicing Intelligence - being able to enter more easily through computer programs in confidential files of other countries-, and either the expan-

sion of their vulnerabilities due to imposing new challenges to the practice of counterintelligence, because the opposite also happen with them, it means other states can access their system easily. Such issues will be further explored in the subsequent topic. In this way, the influence that cyberspace will exert on this practice and on its utilitarian effects on the State is visible. So, the aim of this paper is precisely to point out these transformations, focusing more precisely in the definition of Intelligence as a practice (ii).

The intelligence services in the face of technological transformations: the cyber intelligence

Throughout the centuries, the use of secrecy, or in other words, the information in a confidential way, was considered a fundamental element for the art of governing (Bessa 1996). Important strategists such as Sun Tzu, since long ago, have highlighted information as a key factor for States achieve victory in the War. In his classic work *The art of War* Sun Tzu (2007) obviousness the importance of the employment of spies. According to the Chinese general:

> […] what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. That is, knowledge of the enemy's dispositions, and what he means to do. This foreknowledge cannot be elicited from spirits, and cannot be obtained inductively from experience, nor by any deductive calculation. Knowlegde of the enemy's dispositions can only be obtained from other men […] (Sun Tzu 2007, 150).

However, over the years, is possible to notice a transformation in the role of information as a power resource to states. In a historical perspective, the end of World War II and the emergence of an ideological political dispute during the Cold War led the activity of Intelligence from the level of practice merely focused on military campaigns to a resource with fundamental importance for the security and development of states (Dandoneli, Giovani de Paula y Souza 2012). Giving to information a political meaning that transcends the battlefield (Andrew 1998). During this period was possible to observe the creation of ministries and services dedicated exclusively to the execution of such practice (Fernandes 2012, 22).

Permeating this transformations, technology has always been linked to the Intelligence activity being responsible for allowing a greater access to privileged information as well as greater effectiveness in the formulation of strategies to those who obtain a high technological development (Dandoneli, Giovani de Paula y Souza 2012, 120). The emergence of the computer, for example, is associate to the power struggle between nations (Brito 2011, 21). The creation of the first prototype by Alan Turing - the father of computer science and artificial intelligence - relates to British intelligence efforts to decipher, at the time of World War II, the messages generated by the German Enigma machine. The aim was to decode the German messages in order to take knowledge of the Germany strategies in war and consequently take actions that enables the allies to win.

The creation of ARPANet, a forerunner to the Internet, is also associated with the strategic importance of technological development in the international power struggle held during the Cold War, through the US Agency

for International Development (DARPA) (Bretton 1999). This enterprise arose from the need to create a network of communications inviolable to possible Soviet attacks. Allowing the United States to preserve, within its Intelligence Services, information considered fundamental to the promotion of its interests and the maintenance of national security (Bretton 1999; Castells 1999; Lojkine 1995; Minc y Nora, 1980).

In the face of these findings, Intelligence must be understood as a complex adaptive system in which the processes of construction, production and management of information and knowledge are able to be optimize through the technological increment at the domestic and international (Dandoneli, Giovani de Paula y Souza 2012). Therefore, the role played by cyberspace can not be denied as an important element in the practice of Intelligence. In this scenario, it is observed the emergence of new information access strategies, such as the Computer Network Exploitation (ERC) practice, as well as new mechanisms capable of compromising the technological tools of the opposing Intelligence systems, undermining their ability to collect information considered fundamental to the promotion of security and the projection of their national interests (Machado 2010).

As a result of the emergence of these new doors of vulnerability, States are obliged to maintain the integrity of their computer networks and systems not by means of physical defenses, such as the use of the armed forces, but by reducing vulnerabilities in their systems to protect their data (Bajaj 2010, 2). Among the cyberweapons used to carry out such a practice are (i) the use of viruses responsible for contaminating executable files of the critical infrastructures of adversary states; (ii) SQL Injection, defined as changing the database access commands; Denial of Service attacks, which are responsible for rendering a system's resources unavailable to its users and, finally; (iii) the Computer Network Attack (ARC) responsible for damaging, denying, corrupting, degrading or destroying critical infrastructure of adversary countries, as well as the information contained therein or the systems controlled by them (Gama Neto y Lopes, 2014).

In addition to these procedural factors, the emergence of a growing demand for more efficient processes of information sorting and storage, caused mainly by the increase of the information flow and the ease access to information, made possible by the Internet connection, generate new problems to be faced by the State (Dcaf Backgrounder 2008, 3). This new challenge appears because intelligence and security services have generated a lot of data to be classified. However, the collection of information does not automatically translate into better results in the decision-making process. Even when important information is available, locating them and recognizing their importance in time to prevent disasters can be a challenge (Nye 2010).

An example, is the transformations in the treatment of the ostensive sources, or open sourcers intelligence (OSINT). This kind of intelligence derives from obtaining public information about political, military and economic aspects of the internal life of other countries or targets in a legal, direct and non-clandestine way through the monitoring of the media (newspapers, like BBC/ Le Monde Diplomatic and other national and local journals; radio and television). The advent of the Internet and the greater connectivity generated by it, generating even more information

to be processed and transformed into intelligence (Machado 2010).

There is, therefore, a clear transformation of Intelligence into its operational process, that is, as a data collection and search procedure, since the effectiveness of the intelligence services is directly related to the process of development and improvement in the production, procurement, management and transmission of informations considered strategic to the States (Cepik 2003; Gama Neto y Lopes, 2014). However, obtaining information about the States, the organizations or the individuals is not limited merely to public and OSINT. The activity of intelligence also included access to confidential informations (Cepik 2003). So, the cyberspace also opening space for the intensification and transformation of the espionage practices. The international conjuncture itself evidences this process. The denunciations by Julian Assange and Edward Snowden emphasizes the use of this new instrument as a transformer of the use of an old resource to the International Relations: the information.

Recapping these episodes, the Wikileaks website, founded in 2006 by Australian cyberactivist Julian Paul Assange, gained international visibility by publishing a series of secret documents produced by the US government (Harding y Leigh 2001). The so-called *Cablegate project* made public about 251,287 diplomatic communications from 247 US embassies around the world. Among the various accusations was the charge about espionage practice by the US government, such as Secretary of State Hilary Clinton's requests to 33 embassies and consulates for diplomats doing a vigorously monitoring of the representatives of Various UN countries (Assange, Appelbaum, Maguhn y Zimmermann 2013).

In 2013 it was Edward Snowden's turn as mentioned at the beginning of this article. The episode in question was responsible for generating a great tension between the United States and the international community, especially with Germany and Brazil, as these countries obtained the privacy of their heads of government, Chancellor Angela Merker and President Dilma Rouseff, respectively, violated by US intelligence agencies. In view of this, there is, therefore, a constant attempt to improve security in this domain, gaining relevance due to this the practice of Information Security, defined as an activity responsible for protecting information considered strategic to the State and which, if obtained by its opponents or enemies, may make the country and its citizens vulnerable (kent 1967, 9).

This practice consists of three practically autonomous activities: Counter Intelligence, Security Countermeasures (SCM) and Operations Security. The emergence of a new domain and resource to be used by the states (cyberspace) makes it fundamental, in turn, the association of these activities with the implementation of a cyber-security, defined, according to the Technical Group on Cyber Security, linked to the Security Office (Brazil 2011, 45) as the "art of ensuring the existence and continuity of the Information Society of a Nation, guaranteeing and protecting, in the Cyber Space, its information assets and its infra- Structures". Countries such as Brazil and the United States have already moved toward implementing national cyber security systems (Miles 2016; Machado 2010).

The United States, the major world power in the world, has identified as necessary create a new Intelligence Agency entitled *Cyber Tread Intelligence Integration Center (CTIIC)*, dedicated exclusively to the practice of cyber

security. CTIIC will work seamlessly with other US intelligence services, such as the FBI, the CIA and the NSA, with the primary goal of ensuring cyber security in the country (United States, 2011). Finally, it is important to consider that the interference of the technological element within the practice of Intelligence leads to an intensification of the use of information as a soft power resource by the countries , given the greater speed in the transmission of information and the connectivity provided by the Internet.

These operations are called covert operations and it aim to influence a foreign "audience" which could be a government, government leaders, the population of a nation, a segment of the population or even non-state groups like terrorist organizations, to do something (or fail to do something) according to the interests of the foreign policy of a particular country, creating a change of behavior (Cepik 2003). This kind of Intelligence to be effective demands that activities conducted are viewed as legitimate by the target audience. In the field of cybernetics, this practice takes place through secret intrusions into computer databases for the purpose of altering or destroying computer hardware, software, or information (Miles 2016; Arquilla y Ronfeldt 1993).

Differentiating, therefore, from secret invasions that aim only to learn what information consists of, without altering or corrupting the data (Cepik 2003). Countries such as the United States, for example, are often able to be present through public diplomacy, propaganda, psychological campaigns with greater ease in a greater number of countries, intervening in a direct way about the capacity of perception of the reality of one people or of rulers considered opponents. In this context, once again the Internet has gained prominence in giving greater speed and scope to the political and cultural subversion practiced by these intelligence agencies. Accelerating the impact of policies across the globe.

Conclusion

Face of the reflections made during all this paper, we conclude that the influence of cyberspace on the practice of Intelligence in the 21st century is relevant. Due to the particular characteristics of this domain, marked by a greater number of actors, the ease access in this field, its transversality and at the same time the difficulty in imputing responsibilities, a new number of challenges and opportunities rise to modify an old practice, which is the use of information in order to purchase power. Faced with this new scenario, not only States but also individuals and organizations can become a threat to be faced, because everyone with a computer can be a potential enemy. All this new structure of the relations derived by the cyberspace, is responsible for generating several questions that are still little explored and that don't have precise answers.

One of the question which could be made is: *How we could differentiate the so-called information war, presents since the most remote times, of the so-called cyberwars, a new form of conflict originated from cyberspace?* The States itself treat these issues in a still very confusing way, but we can not disregarding the political intention by this way of acting. Some countries like United States is safeguarding the right of an offensive stance, in the face of cyberspace, hidden, however, by a defensive discourse (Jentlenson 2010). The insecurity

attributed to this domain sets the precedent for this country to legitimize more assertive actions, under the pretext of defending national interests and sovereignty, following the Weberian maxim of the legitimate use of force for the preservation of the nation-state (Lopes 2013; Machado 2010). All this just show us the relevance of cybernetics in the International Relations and as presented by this paper the undeniable relevance of this new domain to the practice of Intelligence.

References

Acácio, Igor, y Gills Lopes. 2012. "Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespao?". *Encontro Anual da Anpocs* 36.

Almeida, Fernando C. 2006. "Poder americano e Estados Nacionais: uma abordagem a partir das esferas econômica e militar" (tesis de maestria de la Universidade Federal de Uberlândia).

Andrew Christopher, 1998. "Intelligence and International Relations in the Early cold War". *Review of International Studies*: 321-330.

Aron, Raymond. 1986. *Paz e guerra entre as nações.* Brasília: UNB.

Arquilla, John, y David Ronfeldt.1993. "Cyberwar is coming!". *Comparative Strategy* 12 (2): 141-165.

Assange Julian, Jacob Appelbaum, Andy Müller-Maguhn y Jérémie Zimmermann. 2013. *Cyberpunks: Liberdade e o Futuro da Internet*. São Paulo: Boitempo.

Bajaj, Kamlesh. 2012. *Cyberspace as Global Commons: The Challenges*. India: Dataquest India.

Bessa, António Marques. 1996. *A Arte de Governar. Ensaios sobre a Classe Dirigente e a Fórmula Política.* Lisboa: SCSP.

Blumenthal, Majory S., y David Clark. 2009. "The future of the Internet and cyberpower". En *Cyberpower and National Security*, editado por Franklin Kramer, Stuart H. Starr y Larry Wentz, 206-240. Washington, D.C.: National Defense University Press.

Brasil. 2012. *Livro Branco de Defesa Nacional*. Brasília: Presidência da República. http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf.

Bretton, Philippe.1991. *História da Informática.* São Paulo: Editora da Unesp.

Clarke, Richard, y Robert K. Knake. 2012. *Cyberwar: The Next Treat to National Security and What to Do About It*. Nova Iorque: Harper Collins.

Carvalho, Paulo Sergio M. de. 2011. "A defesa cibernética e as infraestruturas críticas nacionais". *Ciclo de Estudos Estratégicos* 10.

Castells, Manuel. 1999. *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*. Reino Unido: Wiley-Blackwell.

Cepik, Marco. 2003. *Espionagem e Democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência.* Rio de Janeiro: Editora FGV.

Costa Júnnior, Arnaldo. 2011. "A história da Agência Brasileira de Inteligência: A contra-inteligência organizacional" (tesis de maestria, Universidad de Brasília). http://bdm.unb.br/bitstream/10483/2307/1/2011_ArnaldoMonteiroCostaJunnior.pdf.

Dandolini Aparecida, Giovani de Paula y João Artur Souza. 2012. "Tecnologia da Informação e Comunicação e as atividades de inteligência". *Revista Ordem Pública* 5 (1): 119-136.

DCAF Backgrounder 2008. "Contemporary Challegens for the Intelligence Community Geneva Center for the Democratic Control of Armed Forces", http://www.dcaf.ch/publications/kms/series_backgrounders.cgm?lng=en&size269=20& page269=0.

Gagnon, Benoît. 2008. "Cyberwars and Cybercrimes". En *Technocrime: technology, crime and social control,* editado por Stéphane Leman Langlois, 46-65. Londres: Willan Publishing.

Gama Neto, Ricardo, y Gills Lopes. 2014. "Armas cibernéticas e Segurança Interna-cional". En *Segurança e Defesa Cibernética: da fronteira física aos muros virtuais,* editado por Medeiros Filho, Ferreira Neto y Gonzales. Recife: Editora UFPE.

Harding Luke, David Leigh. 2011. *Wikileaks: A Guerra de Julian Assange contra os Segredos do Estado*. Sao Paulo: Campinas.

Hare, Forrest. 2009. "Borders in Cyberspace: Can Sovereignty adapt to the challenges of Cyber Security?". En *The virtual battlefield: Perspectives on cyber Warfare,* editado por Christian Czosseck y Kenneth Geers. Estonia: Cryptology and Information Security.

Herman, Michael. 1996. *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

Herz, John. 1951 *Political Realism and Political Idealism. A Study in Theories and Realities*. Chicago: The University of Chicago Press.

Jentlenson, Bruce W. 2010. *American Foreign Policy: The Dynamics of Choice in the 21st Century*. Nova Iorque: Norton & Company.

Kello, Lucas. 2012. *Cyber disorders: Rivalry & Conflict in a Global Information Age*. Cambridge: International Security Program/ Belfer Center for Science/ International Affairs, Harvard Kennedy School.

Kent, Sherman.1967. *Informações Estratégicas.* Rio de Janeiro: Bibliex.

Kshetri, Nir. 2014. "Cybersecurity and International Relations: The U.S engagement with China and Russia", http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf.

Kuehl, Daniel. 2009. "From Cyberspace to Cyberpower: Defining the Problem". En *Cyberpower and National Security,* editado por Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, 24-42. University of Nebraska Press.

Levy, Pierre. 1999. *Cibercultura.* São Paulo: Editora 34.

Libicki, Martin. 2009. *Cyberdeterrence and Cyberwar.* Santa Monica: Rand.

Libicki, Martin. 2012. "Cyberspace Is Not a Warfighting Domain". *I/S: A Journal of Law and Policy* 8 (2): 321-336.

Lojkine, Jean.1995. *A revolução informacional*. São Paulo: Cortez Editora.

Lopes, Gills. 2013. "Reflexos da digitalização da Guerra na política internacional do XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá" (tesis de Maestria, Universidade Federal de Pernambuco).

Machado, Jussara de Oliveira. 2010. "Inteligência e Ciberespaço: Desafios do Século XXI" (tesis de Maestria, Escola Superior do Ministério Público de Minas Gerais).

Miles, Anne Daugherty. 2016. *Intelligence Speding: In Brief*. Washigton, Dc: Library of Congress.

Minc, Alain, y Simon Nora. 1981. *The Computerization of Society.* Massachusetts: Mit

Press. Congressional Research Service Report.

Morgenthau, Hans. 1985. *Política entre las naciones. La lucha por el poder y por la paz*. Buenos Aires: Grupo Editor Latinoamericano.

Nye Joseph. 2010. *Cyberpower*. Harvard Kennedy School: Belfer Center for Science and International Affairs.

Nye, Joseph S. 2014. "The Information Revolution and Soft Power". *Current History* 113 (759): 19-22.

Sheldon, John. 2014. "Geopolitics and Cyber Power: Why Geography Still Matters?". *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy* 36 (5): 286-293.

Shulshy, Abram. 1992. *Silent warfare: understanding the world of intelligence.* Nueva York: Brassey's.

Sims, Jennifer. 1995. "What is intelligence? Information for decision makers". En *U.S intelligence at crossroads: agendas for reform*, editado por Roy Godson. Nueva York: Brassey's.

Sommer, P. Ian Brown. 2010. *Study: unlikely there Will ever be a pure "cyberwar"*. Inglaterra: University of Oxford.

Sun Tzu. 2007. *A arte da guerra: os treze capítulos originais.* São Paulo: Jardim dos Livros.

United States. The White House. 2011. "International Strategy for Operating in Cyberspace, Washington, Dc.

United Sates. 2009. "Cyberspace Policy Review", https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf.

Ventre, Daniel. 2012. "Ciberguerra". Ponencia presentada *XIX Curso Internacional de Defensa*, Jaca, España, 26 de septiembre.

Vigevani, Tullo, Paulo Veiga y Karina Mariano. 1994. "Realismo versus globalismo nas relações internacionais". *Lua Nova* 34: 5-26.

Misceláneo

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2578

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 111-125
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

La vinculación entre geopolítica y seguridad: algunas apreciaciones conceptuales y teóricas

The link between geopolitics and security: a conceptual and theoretical assessment

Lester Cabrera Toledo[1]

Fecha de recepción: 13 de febrero de 2017
Fecha de aceptación: 15 de abril de 2017

Resumen

El presente artículo establece una discusión teórica sobre la vinculación que existe entre la geopolítica y la seguridad. En este sentido, la discusión se aprecia desde un punto de vista en torno a la evolución que ha tenido la relación entre geopolítica y seguridad, particularmente sobre la forma en que se comprenden tanto los procesos conflictivos y los actores que se ven involucrados. Así, se establece la vinculación desde comienzos del siglo XX hasta la actualidad, donde se percibe la necesidad de comprender tanto a la geopolítica como a la seguridad desde otros puntos de vista en los que incluso sus elementos básicos se ven cuestionados. Se concluye que se requiere una comprensión holística de ambas perspectivas para entender y explicar los nuevos fenómenos conflictivos, sin descartar la totalidad de los postulados clásicos.

Palabras clave: Geopolítica; Seguridad; Estado; Teoría.

Abstract

The present article seeks to establish a theoretical discussion about the link between geopolitics and security. In this sense, the discussion is seen from a point of view on the evolution of the relationship between geopolitics and security, particularly on the way in which both conflicting processes and the actors involved are understood. Thus, it is established the linkage from the beginning of the twentieth century to the present, where it is perceived the need to understand both geopolitics and security from other points of view, in which even its basic elements are questioned. It concludes that a holistic understanding of both perspectives is required to understand and explain the new conflicting phenomena, without ruling out the totality of the classical postulates.

Keywords: Geopolitics; Security; State; Theory.

1 Licenciado en Ciencias Políticas y Administrativas, Universidad de Concepción, Chile. Magister en Seguridad y Defensa, ANEPE-Chile. Doctor (c) en Estudios Internacionales, FLACSO-Ecuador. ORCID ID: http://orcid.org/0000-0003-0307-1528. Correo: cabrera.lester@gmail.com

Introducción

En el campo de los estudios internacionales y, especialmente, en el área de los estudios estratégicos, la concepción clásica de la geopolítica tiene una fuerte vinculación con una condición de las capacidades que el Estado puede –o debe tener- para lograr determinados objetivos. En este plano, la consecución de objetivos, siempre en el plano internacional, establece a su vez una directa relación en torno a un eventual aumento en los niveles de seguridad. Por lo tanto, la condición geopolítica ayudaría a determinar las cualidades sobre las cuales el Estado y sus tomadores de decisión en el ámbito político, deberían poseer para lograr una mejor percepción de seguridad. Sin embargo, aquello refleja una realidad que era propia del siglo XX y no necesariamente es un parámetro a considerar en la actualidad. Es por ello que resulta necesario establecer, dentro de los planos conceptual y teórico, las vinculaciones que se tienen, como también los alcances que se pueden visualizar, entre ambas disciplinas, constituyéndose, esto último, en el principal objetivo del presente trabajo.

El objeto de estudio es analizar, desde una perspectiva histórica amplia, la evolución de los conceptos de seguridad y geopolítica, así como cuáles son sus vinculaciones teóricas sin dejar de lado los preceptos que fueron parte de su construcción en el siglo pasado. Sin embargo, y pese de que aquella perspectiva radica principalmente en una descripción, se desea al mismo tiempo entender cuáles son los elementos y aspectos que relacionan a la seguridad y a la geopolítica, como una manera de lograr puentes teóricos. Sobre este punto, resulta clave la incorporación de nuevas concepciones desde el punto de vista conceptual como teórico, para así entender qué aspectos, eventualmente, se modifican o se mantienen en la relación entre ambas disciplinas, con vistas a lograr una mejor comprensión sobre el objeto que abarcan y determinar sus alcances y límites

Uno de los elementos que también se busca atender en el presente trabajo, es la falta de rigurosidad académica de los conceptos mencionados. En este sentido, se establece que si bien se puede apreciar, en un primer momento, que existe una directa relación entre la seguridad y la geopolítica, aquello no se puede interpretar como un aspecto absoluto y homogéneo. La incorporación de diferentes elementos teóricos, así como también la propia modificación del contexto internacional, no determinan cambios en la manera en que se entienden ambas disciplinas, sino que también abre desafíos, principalmente para la academia, en la forma de teorizar y comprender la aplicación de estos conceptos, para, a su vez, entender y explicar distintos fenómenos de alcance internacional, así como sus repercusiones en un ámbito nacional. En este plano, se requiere profundizar el debate de los alcances y límites que tienen ambas disciplinas por separado y, particularmente, cuáles serían sus implicancias en temas vinculados a la planificación estratégica de los países, como también al logro de los objetivos internacionales. Pero incluso, en el plano mencionado, también debe considerarse cuál es el rol que le cabe al Estado en la generación de condiciones de seguridad y en la interpretación de sus parámetros geopolíticos.

Seguridad y geopolítica en el siglo XX

Simon Dalby, en su libro *Creating the Second Cold War, The Discourse of Politics*, realiza un extenso análisis de las vinculaciones que tie-

ne el discurso político, particularmente en aquellos temas relacionados con lo militar, y la forma en que los tomadores de decisión perciben las amenazas que afectan, en mayor o menor medida, a la consecución de objetivos por parte del Estado. Pero tal vez más relevante que lo mencionado, es la vinculación que realiza el autor con respecto a la imaginación geopolítica de los personeros de gobierno y las medidas que toman en el plano de la política exterior, manifestándose esto último en un determinado discurso político. La idea principal de Dalby (1990) en dicha obra, es cómo el plano político "representa" y "hace real", su propia concepción de seguridad, lo cual es, de manera subyacente, un aspecto intrínseco a la persona y sus reglas tanto morales como éticas, al tiempo que es altamente subjetivo, ejemplificándose en el discurso del Presidente de los Estados Unidos Ronald Reagan, sobre una segunda etapa en la Guerra Fría.

Una perspectiva similar es la que establecen John Agnew y Gearoid O'Tuathail (1992), en el hecho de evidenciar que las amenazas a la seguridad de los países pasa principalmente por la capacidad de interpretación que de las mismas tengan los tomadores de decisión en los ámbitos estratégicos, como también en la política exterior. Pero incluso más allá, dicha interpretación queda en nada si no se manifiesta dentro de un plano imaginario, el cual sería, para los mencionados autores, el espacio en el que se unen geopolítica y seguridad, debido a que es por medio de la geopolítica en que los tomadores de decisión "espacializan" sus amenazas, así como también la posibilidad de contrarrestarlas, a través de decisiones concretas, las que se manifiestan en políticas de seguridad sobre un fenómeno u objeto en particular.

Paralelamente, esta visión que expresan tanto Simon Dalby, como Agnew y O'Tuathail sobre la geopolítica y la seguridad es contrastada con la perspectiva más clásica de ambas disciplinas. En efecto, para Klaus Dodds (2000) la visión tradicional y clásica de la geopolítica, que colocaba al Estado como la principal unidad de análisis, tiene una alta vinculación con la perspectiva realista de las Relaciones Internacionales, principalmente a la concepción territorial que ambas visiones poseen. Por un lado, la geopolítica para el mencionado autor posee un elemento territorial, que es la propia esencia de la disciplina, la que a su vez influye en la manera en cómo los países establecen su política exterior hacia el sistema internacional. Por otro lado, la concepción realista se transformaría en el sustento teórico sobre el cual la geopolítica, desde un punto de vista clásico, lograría plasmar sus realidades.

En definitiva, para Klaus Dodds, la geopolítica y el realismo van de la mano, siendo uno de los elementos claves la política exterior de los países, pues es una forma de maximizar sus condiciones de seguridad frente a un sistema internacional anárquico. Este punto de vista es también compartido por Henry Kissinger. Particularmente, en su obra *La Diplomacia*, establece a la geopolítica como una forma de comprender los conflictos de poder que se dan entre países en el sistema internacional, aunque cabe mencionar que, pese a que el mencionado autor establece la validez del concepto, jamás lo define, lo que a su vez crea una forma altamente subjetiva de comprenderlo clara y objetivamente, y lo coloca como una forma de entender el balance de poder que existía en plena Guerra Fría entre las grandes potencias (O'Tuathail 1994).

Sin embargo, a juicio de Phil Kelly (2016), la unión entre geopolítica y seguridad no es tal. Esto se produce como consecuencia de una errónea vinculación entre geopolítica y

seguridad a través de algunos de los principales preceptos que establece la visión teórica del realismo. Para el autor, la geopolítica descansa sobre el posicionamiento espacial de los países, regiones y recursos que pueden afectar la política exterior de los mismos y las acciones vinculadas a la misma, siempre desde una visión clásica. Mientras que el realismo se basa, fundamentalmente, en los balances de poder que se generan entre los Estados, por diferentes razones, y que se expresan en la configuración del sistema internacional. Así, si bien es cierto que el realismo podría considerar relevante la vinculación entre poder y geografía, aquello se daría en el plano de que las características geográficas le generen un aumento en sus capacidades de poder, tanto materiales como relativas, y una protección a sus intereses. Pero la geopolítica no posee un interés claro en aquello, preocupándose en mayor medida en el impacto que puede generar el posicionamiento espacial de los Estados en las política y comportamiento internacional de estos actores (Kelly 2016).

Finalmente, y desde un punto de vista del desarrollo de la geopolítica en América Latina, se posee un claro posicionamiento sobre la base de la necesaria unión entre la geopolítica y la seguridad. Esto último se explicaría desde el argumento de que el estudio de la geopolítica en la mencionada región, se aprecia en mayor medida como parte de la formación de los oficiales de las diferentes ramas de las Fuerzas Armadas de la región (Dodds y Atkinson 2001; Child 1979). No obstante aquello, que evidencia un fuerte componente realista en la base teórica de las explicaciones geopolíticas, lo cierto es que la geopolítica queda supeditada a la visión de Defensa más que de seguridad, entendiendo en este plano a la Defensa como algo más concreto y restringido que la seguridad. Así, la geopolítica estaría ligada a la forma en cómo se planifican y concretan los denominados "objetivos nacionales permanentes", indicando al mismo tiempo la factibilidad de la realización de los mismos, y las eventuales amenazas que se ciernen sobre ellos (von Chrismar 2010), y la importancia del actuar de los cuerpos armados en su ejecución.

Las diferentes perspectivas que existen sobre la vinculación entre geopolítica y seguridad pueden tener una explicación sobre la base de los planteamientos clásicos de la propia geopolítica, así como también su posterior evolución y aplicación. En este sentido, observando las bases teóricas y ontológicas de los clásicos, es posible encontrar grandes diferencias en la comprensión de la geopolítica y, por ende, su relación con la seguridad. En primer lugar, si bien se considera que los planteamientos clásicos tuvieron su desarrollo de la mano de geógrafos, lo cierto es que el concepto de geopolítica como tal fue impuesto por un abogado y politólogo, Kjellen, que si bien toma las concepciones teóricas de Darwin, muy populares por fines del siglo XIX, su análisis se enfoca en el Estado (Cohen 2015). Distinto es el caso de los geógrafos, como el propio Ratzel, que establecían principios sobre la misma base teórica, pero su aplicación se relacionaba íntimamente con el entorno que iba más allá de las fronteras de los países (Dodds y Atkinson 2000). Lo anterior es un claro ejemplo de la carencia de una única forma de interpretación de la geopolítica, tomando a los autores clásicos y fundadores de la disciplina.

Siguiendo el planteamiento anterior, si se analiza lo mencionado por autores como Mackinder, Spykman o Haushofer, a juicio de determinados autores (Kelly 2016, Grygiel 2006), esta forma de interpretación geopolíti-

ca no es tal, debido a que mezcla por un lado elementos de supervivencia de los Estados, o de determinadas regiones, mientras que por otro toma aspectos relativos a la capacidad de hegemonía en otros espacios territoriales. Se hace una clara vinculación entre la concepción geopolítica y lo que se entiende por geoestrategia, siendo esta última perspectiva la que se identifica con los temas de seguridad. Por ende, si bien para algunos especialistas, la geopolítica en un sentido clásico, se vincula directamente al realismo y a la seguridad de los países, aquello va a depender de la perspectiva sobre la que identifiquen a los actores, como también a la propia interpretación que le otorguen a la geopolítica.

Sin perjuicio de lo anterior, pese a que en un principio se observa una vinculación entre geopolítica y seguridad, aquello respondería principalmente a una concepción positivista, donde elementos como el territorio se observan como absolutos. Y, al mismo tiempo, visualiza al Estado como la principal, si no es la única unidad de análisis, tomando los preceptos realistas al respecto; es decir, el principio de unidad, el actor racional y que lucha por su supervivencia en un contexto internacional anárquico. Aquello, producto de la irrupción de otros puntos de vista, tanto en la geopolítica como en los estudios de seguridad, dan cabida a otra forma de comprender una eventual vinculación entre ambas disciplinas, incluso considerando una variación en el objeto a analizar.

La vinculación teórica contemporánea

Los fenómenos internacionales vinculados a los estudios estratégicos, debido a la configuración de múltiples puntos de vista, tanto epistémicos como teóricos, han proliferado luego del fin de la Guerra Fría. Pero aquello no solamente se debe a la propia evolución del conocimiento, sino que también se puede extraer una eventual explicación debido a los propios fenómenos que se dieron en el sistema internacional, y que afectaron diferentes realidades sociales. En este sentido, la propia concepción de una de las unidades básicas del sistema internacional, como lo es el Estado, ha quedado en tela de juicio incluso en sus elementos constitutivos (Harvey 1990).

Es así como la concepción territorial de los países ha dado paso a que el concepto de "territorio", producto de las consecuencias del fenómeno de la globalización, no sea el más apto para entender las actuales problemáticas, tanto en término de seguridad, como también para la geopolítica (Hassner 2006). Esto se debe a que la concepción absoluta del territorio, como algo impenetrable e incluso inamovible, sea deja de lado, debido a los avances tecnológicos. Es por ello que el "espacio" no solo se convierte en una perspectiva más dinámica para entender las fluctuaciones de los procesos sociales, sino que va más allá de la figura del Estado, incorporando incluso a otros actores y factores, tanto materiales como simbólicos, que antes estaban disminuidos bajo la presencia del Estado.

El contexto mencionado altera de manera considerable la forma en que se comprende el panorama de la seguridad, debido a que uno de los factores que eran claves para el diseño de las estrategias, tanto en el ámbito de la política exterior de los países como en la Defensa de los mismos, se encuentra en una evolución e incluso, en una comprensión limitada. El siglo XXI no solamente trajo la necesaria incorporación de otros actores, que van más allá de la figura del Estado, en la conformación de las

amenazas, sino que incluso el propio objeto de la seguridad se ha modificado (Paris 2001).

En un comienzo, la concepción de amenaza estaba dada por actores estatales, los cuales eran altamente visibles en cuanto a sus intenciones, como también en sus prácticas para confrontar un determinado conflicto, lo que puede entenderse desde una visión del conflicto regular o de amenaza tradicional. Sin embargo, en la actualidad aquello no se evidencia de tal forma. Los conflictos irregulares, es decir, entre un Estado y un actor (o varios) no estatales, se ha transformado en la tónica de los enfrentamientos armados. Y en aquella relación, el actor no estatal se evidencia con una alta capacidad de influencia en los temas de seguridad, especialmente en aquellos segmentos en los que tiene una libertad de acción considerable, particularmente por la falta de presencia del Estado dentro de la sociedad (Gray 2012).

Siendo así, los elementos que sostenían a la perspectiva clásica de la geopolítica, no pueden considerarse como inmutables o libres de algún cambio. Al contrario, los aspectos que vinculan a la geopolítica con la seguridad son múltiples, pero no necesariamente obedecen al actuar del Estado o, en su defecto, al condicionamiento geográfico que se pueda visualizar en torno a la seguridad. Es cierto, como bien sostiene Robert Kaplan (2012), los elementos geográficos no van a pasar de moda ni tampoco van cambiar de un momento a otro, pero es la interpretación que se les da a los mismos, como también el grado de afectación que pueden establecer en una localidad más reducida que el Estado, lo que otorga una clara modificación a las formas de comprender en este caso, a la geopolítica (Agnew 2005). Y si a lo anterior se le suma el hecho de que los elementos simbólicos ligados a la geografía generan un grado de influencia en el comportamiento exterior tanto de grupos vinculados al Estado como al propio Estado en sí, las características objetivas de la geopolítica también quedan en duda, como lo mencionado con respecto al territorio (Font y Rufí 2001).

Sin embargo, ¿aquellos aspectos reducen la vinculación entre la geopolítica y la seguridad? No necesariamente, e incluso dependiendo del punto de vista con el cual se trate, amplían la relación entre ambas disciplinas, pero dejando de lado los parámetros netamente positivistas y/o realistas. Al momento de modificarse las condiciones de comprensión de la geopolítica, dejando de lado una visión inamovible del territorio como también de los factores geográficos que influyen en el comportamiento exterior de los países, se amplía la forma de evaluar los fenómenos que, de alguna u otra forma, afectarían a la seguridad, no solo del Estado, sino de las sociedades en general (Roe 2013).

En este sentido, la geopolítica permitiría evidenciar la importancia de fenómenos transnacionales que no necesariamente poseen una concepción territorial (Agnew 1994). Al mismo tiempo, al establecer nuevos parámetros de compresión en torno, por ejemplo, a las amenazas no tradicionales o nuevas amenazas, el objeto de la propia seguridad se modifica. La visión Estado-céntrica, si bien ayudó en su momento a explicar el proceso de la seguridad (de por sí altamente subjetivo) en el contexto de la Guerra Fría, no es representativa de la realidad que viven las sociedades. Por ende, al tomar medidas sobre los fenómenos o procesos conflictivos, se tiene que tener una base de explicación distinta, para poder superar los desafíos que se presentan (Manwaring 2011).

El mismo Simon Dalby (1997) logra establecer la vinculación entre un concepto como lo es el de geopolítica crítica y la seguridad,

tomando como base la utilización del discurso como forma de deconstruir las realidades socialmente aceptadas, incluyendo en este plano, la validez del territorio como base de comprensión de los fenómenos de seguridad asociados al Estado. Sin embargo, el mencionado autor también deja patente el hecho de que esta manera de acercarse a los nuevos fenómenos que afectan la seguridad, hace necesario un nuevo punto de vista para tratar dichos aspectos. En otras palabras, el foco no se encuentra en los propios acontecimientos, sino en la mente y comportamientos de los actores asociados a los procesos de toma de decisión, especialmente en el ámbito de la seguridad. Con ello, se logra identificar cuáles serían los patrones que están detrás de cada decisión, al tiempo que se busca conocer los elementos que formarían vínculos con aspectos de identidad, como una forma de entender una nueva dimensión de los procesos de seguridad (Agius 2013).

Cuando se cambia el foco de acontecimientos a procesos, los factores culturales adquieren en mayor medida una importancia considerable, teniendo en cuenta que es gracias a dichos elementos que se establecería una unión entre identidad y seguridad, relevando a un segundo plano la integridad territorial como aspecto a resguardar en el plano internacional del Estado. Es más, de acuerdo a Paul Roe (2013), en múltiples ocasiones son las propias localidades ubicadas al interior del Estado, las que no logran un grado de compatibilidad entre la identidad y lo cultural con dicha institución, lo que da como consecuencia una serie de conflictos entre las partes involucradas. Pero incluso más, la visión cultural y de identidad no solamente reafirmaría una condición geopolítica determinada de una localidad, sino que, al mismo tiempo, lograría evidenciar que, en múltiples ocasiones, el Estado basa su propia concepción de seguridad en aspectos netamente simbólicos, lo que no solo da como resultado una clara incongruencia en los parámetros tradicionales de comprender a la geopolítica y a la seguridad, sino que, al mismo tiempo, devela los aspectos subyacentes que se esconden detrás de una eventual realidad (O'Tuathail 1996).

Es decir, ¿cómo se puede explicar, desde una perspectiva realista y clásica tanto de la geopolítica como de la seguridad, que los "intereses nacionales" sean en buena manera elementos simbólicos y que, en términos pragmáticos, se observen como representaciones de aquellos que toman decisiones en el ámbito estratégico del Estado? En una eventual respuesta, el discurso juega un papel clave, considerándose este como una herramienta que permite la elaboración de patrones sociales, los cuales a su vez son reconocidos y legitimados por la población. Lo señalado puede considerarse como uno de los elementos sustanciales de la perspectiva constructivista, en el ámbito de las Relaciones Internacionales (Santa Cruz 2009; Kubálková 2001).

El impacto de las tecnologías de la información es otro de los elementos que necesariamente deben ponderarse, para entender la concepción contemporánea de la geopolítica y la seguridad. Si bien es cierto que dichas tecnologías han tenido una influencia en la forma de evidenciar una "disminución" de las distancias entre los diferentes espacios territoriales del planeta, también es cierto que dichas tecnologías han incrementado los espacios de vulnerabilidad de las sociedades (Ayoob 1997). Incluso, desde un punto de vista estratégico, la aparición de las nuevas tecnologías de la información, han dado como consecuencia la aparición de una nueva dimensión de la

estrategia, la cual es el ciberespacio (Dunn Cavelty 2013). Sobre este punto, la perspectiva clásica de la geopolítica no permitiría otorgar explicaciones ni respuestas a las eventuales interrogantes planteadas por dicho fenómeno, el que, sin perjuicio de ello, tiene importantes implicaciones en el tema de la seguridad. Un ejemplo de aquello, es la interconexión que poseen las denominadas "infraestructuras críticas" dentro de un país, a un determinado sistema informático. En términos de afectación tanto económica como social, los ataques informáticos poseen un alto impacto tanto para los propios Estados como para las entidades privadas que se encuentran en dicho espacio territorial.[2]

Tanto para Peter Taylor como para Colin Flint (2002), las vinculaciones entre el imaginario geopolítico y las amenazas que se perciben a la seguridad, ya sea del Estado o bien de las propias sociedades, se debe principalmente a la diferenciación entre los sistemas de producción, y particularmente, por la manifestación de aquellas diferencias en espacios territoriales. Así, la división entre centro y periferia, pese a que fue elaborada y desarrollada dentro la primera parte de la segunda mitad del siglo XX, aún mantiene una vigencia geopolítica. Es así como Peter Taylor y Colin Flint concibieron, siguiendo los parámetros teóricos de Inmanuel Wallerstein, que los países establecen un posicionamiento geopolítico no solo de acuerdo a los procesos de producción que imperaban dentro de su geografía, sino también por el grado de influencia política que pueden tener, a través de los mismos, en el sistema internacional. Aquello les permitiría tener una posición que se evalúa tanto en términos económicos como políticos y, particularmente, geográficos. Por lo tanto, las amenazas quedarían visibles desde otras perspectivas, más allá de las concepciones tradicionales de seguridad, en el sentido de que un proceso puede interpretarse como amenaza, cuando afecte la sustentabilidad de un modelo económico, y que a su vez atente contra la visión geopolítica de un país. Y aquello no tiene una visión territorial clásica, lo que requeriría ampliar el espectro de las herramientas que se utilizarían para lograr dicha percepción de amenaza.

Como se mencionó en su momento, la cultura juega un papel central dentro de la construcción, ya sea real o simbólica, de los elementos que configuran patrones de seguridad desde una visión geopolítica crítica. Pero incluso en este plano, de acuerdo a lo establecido por Martin Müller (2008), si bien el discurso ayuda a generar patrones sociales, aquello puede ser a su vez interpretado como un absolutismo, especialmente cuando se habla de geopolítica. Así, cuando se toman las nuevas perspectivas de la geopolítica desde una visión crítica y, como producto de su bajo nivel de comprensión y dominio, se tiende a mezclar con lineamientos muy cercanos al propio análisis crítico del discurso, con lo que, a juicio del mencionado autor, se amplía el rango de discusión de la geopolítica, incluso dejando a un lado la naturaleza misma de la disciplina. Por lo tanto, no todos los elementos o procesos culturales, poseen una vinculación con la geopolítica, ni

2 Un ejemplo de lo anterior puede reflejarse en las declaraciones emitidas en octubre del año 2012 por el entonces Secretario de Defensa, Robert Panetta, el cual declaró que el país se encuentra ad portas de un "Pearl Harbor cibernético", debido a que "podría causar destrucción material como también la pérdida de vidas. Un ataque que podría paralizar a la nación y crear un profundo sentimiento de vulnerabilida"d. Véase al respecto *Panetta Warns of Dire Threat of Cyberattack on U.S.*, disponible en: http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

menos con la seguridad, así como también la geopolítica como tal, debe ser apreciada desde determinados parámetros, para no desnaturalizar su objeto de estudio. Entre dichos parámetros, se encuentra la concepción espacial y territorial de los problemas, los que pueden ser vinculados a perspectivas de seguridad. Es por ello que se requiere tener una comprensión más amplia de los procesos mencionados, como el de seguridad y la geopolítica, con el fin de encontrar aquellos elementos en común y que permitan dilucidar y explicar de una mejor forma, aquellos fenómenos conflictivos de la actualidad.

Hacia una comprensión holística

Phil Kelly (2006) expone un planteamiento central que, según su perspectiva, debiera ser incorporado en la totalidad de los eventuales análisis geopolíticos que se realicen: no necesariamente lo antiguo es malo y debe desecharse, ni tampoco lo nuevo debe reemplazar a lo antiguo. Para el mencionado autor, siempre desde la óptica de la geopolítica, los nuevos enfoques, como lo son la propia geopolítica crítica, como aquella perspectiva que se deriva de la Economía Política Internacional, tienen la virtud de complementar de una buena manera, las antiguas formas de análisis geopolítico. Incluso, la complementariedad se da particularmente en el plano del objeto a analizar, mencionando que el territorio debe ser el elemento clave para que un problema sea, o no, de carácter geopolítico (Kelly 2006).

En línea con lo mencionado por el autor mencionado, tanto John Agnew (2005) como Klaus Dodds (2000) y Colin Flint (2007), desde diferentes concepciones, no estandarizan a la geopolítica desde una visión única, al tiempo que abogan por una complementariedad, principalmente por las herramientas conceptuales que se visualizan desde los nuevos enfoques de la geopolítica, en línea con los parámetros argumentativos de la geopolítica clásica. Es así como el propio Phil Kelly (2016) señala de manera explícita que los criterios para entender el posicionamiento geopolítico de un país, deben ser relacionados con su contexto como también por los intereses y amenazas que evidencia. Y para lograr aquello, no solo se requiere una matriz de pensamiento que se derive, exclusivamente, de los clásicos, sino que incorpore otras visiones más contemporáneas.

En un plano muy similar, determinados autores relacionados con la temática de la seguridad, propugnan mantener, especialmente en el plano conceptual, una serie de elementos y factores que determinan la existencia de un problema de seguridad, desde el plano estratégico (Nunn 2011; Griffiths 2007). Así, una correcta interpretación de dichos elementos, permitiría generar los alcances y límites necesarios para hablar de problemas y fenómenos que se vinculan en mayor medida a la seguridad, pese a que posean una raíz donde el desarrollo sea un factor de explicación. Siendo así, se dejarían de lado en una importante magnitud, conceptos como el de seguridad humana y sus múltiples variaciones.

Pese a lo mencionado, también existe una concordancia en que el cambio en el foco de protección de la seguridad es uno de los fenómenos necesarios para la propia evolución del concepto, estando en línea con el contexto internacional. Por lo tanto, si bien la nueva concepción de la seguridad ha impregnado los parámetros analíticos en la manera de comprender los fenómenos conflictivos, al mismo tiempo se requiere considerar una base sobre

la que se permita realizar observaciones y otorgar medidas objetivas, a fin de solucionar o enfrentar los desafíos impuestos por el nuevo contexto (Gray 2007).

Considerando el panorama señalado es que se hace necesario una mixtura entre los dos enfoques, para lograr finalmente una mejor visualización tanto del entorno en el que se desenvuelve el Estado, la naturaleza de los procesos conflictivos, y los procesos de toma de decisión en el interior de los países, como una forma de comprender la "imaginación geopolítica" de los procesos conflictivos señalados (Agnew 2005). Siendo así, se requiere la incorporación de nuevas formas de pensamiento que, unidas a las estructuras clásicas (como el propio Estado), ayudarían a mejorar la comprensión de los fenómenos. Pero sin perjuicio de un posterior análisis sobre las categorías señaladas, se hace necesario conocer el grado de cercanía o lejanía que tienen cada una de las posturas mencionadas, tanto en el plano de la geopolítica como de la seguridad, las cuales se exponen en el cuadro 1.

En el cuadro anterior, se expone, sobre la base de cinco categorías, las similitudes y diferencias que, de acuerdo a la literatura que versa sobre las temáticas analizadas, se dan entre la geopolítica y la seguridad. Por ejemplo, desde la perspectiva que entregan los niveles de análisis, tanto la geopolítica clásica como la seguridad clásica, comparten que se visualizan de una mejor forma los fenómenos si se toma en consideración la estructura que envuelve a los principales actores, los que son los Estados. Mientras que las otras dos perspectivas, es decir, la geopolítica crítica y los nuevos enfoques de seguridad toman perspectivas que comparten algún grado de similitud. Por ejemplo, si bien la geopolítica crítica se enfoca en el proceso de toma de decisión, y específicamente en el ámbito de la política exterior, y los nuevos enfoques en temas de seguridad le otorgan relevancia al proceso de agencia, aquello se deriva en una conjunción de temas, debido a que el proceso de toma de decisión debe a su vez considerar una eventual capacidad de agencia por parte del Estado, para que sea un proceso exitoso.

Existe una directa relación entre las categorías de "base epistémica", por un lado, y el "objeto de estudio", por otro. Si se toma en

Cuadro 1. Vinculaciones entre los enfoques clásicos y contemporáneos de la geopolítica y la seguridad

Categorías	Geopolítica Clásica	Seguridad Clásica	Geopolítica crítica	Nuevos enfoques de seguridad
Niveles de Análisis	La estructura	La estructura	El proceso de toma de decisión	Agencia
Base epistémica	Positivista	Positivista	"Posmoderna"	"Reflectivista"
Objeto de estudio	Vinculación entre territorio y la política exterior	El Estado y las amenazas convencionales	Las intenciones dadas a través de un discurso	La percepción de inseguridad en la sociedad
Actores	El Estado	El Estado y el sistema internacional	Múltiples	Múltiples
Finalidad	Conocer y prever dinámicas de poder	Prever amenazas y disuadirlas	Deconstruir realidades socialmente aceptadas	Analizar la naturaleza del proceso conflictivo

Fuente: Elaboración propia a raíz de los antecedentes recopilados

consideración que la base epistémica de la geopolítica y seguridad, desde la perspectiva clásica es positivista, su objeto de estudio tiene que ser un elemento relativamente objetivo, como se evidencia en el cuadro 1. Distinta situación sucede con las otras dos perspectivas. En este plano, cabe destacar que dentro de la categoría de "base epistémica", ambas visiones contemporáneas se encuentran entre comillas.

Esto se debe a que no existe una visión exclusiva ni única sobre este tema, el cual se encuentra en plena discusión, debido a que dichos enfoques aún son relativamente novedosos. Pese a lo anterior, la mayoría de los estudiosos consideran las mencionadas perspectivas epistémicas para cada una de las disciplinas en cuestión. Pero más allá de aquello, existe una directa relación entre dicha categoría y el "objeto de estudio", tanto para la geopolítica crítica como para los nuevos enfoques de seguridad. Ambas visiones son altamente subjetivas y resulta compleja su medición a diferencia de las perspectivas clásicas. Es por ello que se hace necesario una mayor cantidad de información para clarificar dicho objeto de estudio, al tiempo que también se requiere otro tipo de entradas disciplinarias para comprender el fenómeno en cuestión.

Las categorías antes mencionadas se relacionan directamente con los "actores" a los que cada una de las perspectivas establece una importancia. En este sentido, las visiones clásicas toman al Estado como el actor principal sobre el cual establecen sus análisis; mientras que las visiones más contemporáneas no necesariamente consideran al Estado como el actor relevante, sino que existen otros actores que deben ser tomados en cuenta y que, en determinadas circunstancias, su importancia es mayor a la del propio Estado. No obstante dicha lógica, desde las visiones más contemporáneas, no existe una claridad sobre un único actor. Esto puede explicarse por la amplitud y subjetividad que ambas poseen en su objeto de estudio, como también por el hecho de que son corrientes relativamente nuevas, y aún no establecen un campo definido.

La última categoría, la propia "finalidad" de cada una las corrientes en cuestión, las visiones clásicas encuentran puntos de convergencia, tomando en cuenta la necesidad de "previsión" que ambos enfoques propugnan, aunque desde distintos puntos de vista. Sin embargo, logran una conjunción en términos de poseer un conocimiento previo sobre dinámicas que puedan influir, en un sentido positivo como negativo, en el desarrollo del Estado. Mientras que las posturas más contemporáneas se enfocan en determinar la naturaleza de los procesos conflictivos (seguridad), como en la deconstrucción de las realidades socialmente aceptadas (geopolítica). Pese a que en un principio no existiría una directa vinculación entre ambas, lo cierto es que la hay. Para poder entender la naturaleza de los procesos conflictivos, las que no necesariamente están asociadas a una visión de amenazas convencionales, se debe entender el proceso en sí desde una visión diferente. Aquella perspectiva la otorgaría la geopolítica crítica a través de la deconstrucción de aquellas realidades que se consideran absolutas y no permitirían visualizar el fenómeno de una forma más amplia.

De las características dadas por cada una de las categorías, es posible evidenciar tres aspectos de alta relevancia para poder establecer un enfoque holístico en la vinculación entre geopolíticas y seguridades. En primer lugar, la figura del Estado, pese a que es mencionada tácitamente por las nuevas corrientes de la geopolítica y la seguridad, es uno de los elementos en los que las cuatro visiones se unen.

Si bien es cierto que las nuevas perspectivas no colocan al Estado como una unidad principal de análisis, tampoco lo descartan como tal, por lo que el Estado puede ser considerado como un aspecto en donde los mencionados enfoques confluyan.

En segundo lugar, si bien es cierto que las nuevas corrientes de la geopolítica y la seguridad poseen elementos altamente subjetivos, resulta necesario otorgar un grado de objetividad a los procesos en cuestión, con el objetivo de comprobar y medir dentro de lo posible, los impactos y consecuencias que los mismos pueden ocasionar. Por ende, se requiere de una base definida para luego descomponer los elementos que se derivan de aquella, lo que se daría en la vinculación entre las corrientes clásicas y contemporáneas de la geopolítica y la seguridad. Y, finalmente, si los enfoques clásicos buscan "prever", los enfoques contemporáneos pueden ayudar en dicho objetivo, tomando en cuenta que la deconstrucción de las realidades generaría nuevos enfoques de comprensión de un mismo fenómeno, con lo que a su vez se detectarían eventuales debilidades y posibles vulnerabilidades, tomando en cuenta el o los objetos a resguardar.

La vinculación entre los enfoques clásicos y contemporáneos no solo se explica desde las categorías mencionadas, sino también desde aspectos sobre los cuales se puede analizar un determinado fenómeno. Es por eso que se establecen tres aspectos en los que las perspectivas señaladas pueden complementarse para un mejor entendimiento de un fenómeno o problema dado, los cuales, de acuerdo a lo mencionado en su momento, son el contexto sobre el cual se desenvuelve el Estado, la naturaleza de los procesos conflictivos, y los procesos de toma de decisión que generan una "imaginación geopolítica" de los fenómenos analizados.

Al considerar al Estado como unidad de análisis, debe considerarse como base, mas no como la perspectiva que propugna la teoría realista. Es decir, si bien el Estado existe, no debe analizarse como el actor unitario y racional. Esto da como consecuencia una ampliación de los fenómenos que afectarían al Estado y el aumento en el número de actores que intervienen en los fenómenos, con su diferente ponderación. Pero al mismo tiempo, al intervenir nuevos actores, el contexto en el cual el Estado se relaciona no es único: la visión territorial se amplia y la perspectiva de fronteras se aplicaría tanto en un ámbito interno como externo, lo que modifica la visión de los peligros como de las amenazas, tanto en su lógica como en los actores que intervienen.

Derivado del punto anterior, se comprende la importancia de entender la naturaleza de los procesos o fenómenos conflictivos. En múltiples ocasiones, la respuesta que otorgan las instituciones se contradice con la real naturaleza del conflicto, lo que da como consecuencia un agravamiento del mismo, o bien que se tome en cuenta solamente una parte del fenómeno. Por ende, una concepción más amplia de la seguridad, tanto en los actores como en los procesos, da como resultado una complejidad no menor. Más aún, si se establece que la naturaleza de los actuales procesos conflictivos es difusa, tanto en su actuar como en los actores que intervienen. Por eso que no se puede considerar al Estado como "la" unidad de análisis, ni tampoco a las herramientas clásicas de la seguridad, para lograr una situación de resguardo de los intereses. Y es en aquel plano en donde la geopolítica crítica puede ayudar a mejorar la comprensión de los fenómenos e, incluso, a delimitar si los mismos poseen una naturaleza en el ámbito de la seguridad o no.

La modificación y aumento de los fenómenos y actores que influyen en la visión de amenaza o peligro para el Estado, así como también su propia naturaleza de características difusas, hacen que los procesos de toma de decisión sean más complejos a la hora de calificar y/o cuantificar el fenómeno en sí y su impacto para los actores que se ven afectados. Es por ello que los responsables de tomar las decisiones, ya sea al interior del Estado o en su política exterior, cumplen un rol crucial, debido a que es de la forma en cómo perciban, se realizará el tratamiento para lograr el menor grado de afectación, lo que se deriva en una "imaginación geopolítica". Dicha "imaginación" resulta de una ponderación entre puntos fuertes, puntos débiles y la propia afectación o emocionalidad que pueda tener el tomador de decisión frente a aquellos fenómenos. La comprensión y deconstrucción de aquellas perspectivas, en parámetros más objetivos, ayudaría a determinar y a clarificar tanto a los actores que intervendrían, los elementos que son parte del fenómeno en sí, como también las consecuencias que una determinada política o decisión traería para el Estado, tomando en cuenta el contexto en el cual se desenvuelve.

Conclusiones

La geopolítica y la seguridad son elementos que, en un principio, se consideran como partes totalmente vinculadas, especialmente en el plano teórico, como una forma de entender el comportamiento de los Estados o, en su defecto, como una manera de explicar la necesidad de contar con un marco que permita argumentar medidas de seguridad sobre una base geopolítica. Aquello, si bien encuentra una forma de manifestación a través del realismo, también se considera en gran parte como inexacto, debido a las diferentes propuestas que se visualizan tanto en el ámbito de la seguridad, como también de la geopolítica. Incluso, analizando la evolución de ambos conceptos, resulta inadecuado señalar que, en la actualidad, la geopolítica y la seguridad poseen un puente únicamente a través del realismo, e incluso si es que tienen un grado de conexión como tal, tomando como referencia al respecto una eventual orientación epistémica en ambos conceptos.

Como se evidenció a través de los propios conceptos y contextos, la geopolítica contemporánea, como también los nuevos enfoques de seguridad, poseen múltiples puntos en común, y su adecuada comprensión permite una mejor explicación sobre los fenómenos que, hoy por hoy, intervienen en la percepción de amenaza tanto de los Estados como de las sociedades. La mezcla y vinculación entre los preceptos clásicos de la geopolítica y la seguridad, y la visión contemporánea de las mismas, no solamente establecen un panorama más diverso de los fenómenos, sino también una complejidad para aquellos que analizan dichas perspectivas, ya que de por sí, el contexto de la propia explicación se amplía.

En este plano, el desafío está tanto en la utilización de ambas visiones. Es decir, la clásica y la contemporánea, como un conjunto único, como también en teorizar y desarrollar perspectivas prácticas, tomando en cuenta que los contextos de inseguridad y los actores que participan en los mismos, son los que marcan las diferencias. Por ende, la realización de trabajos de investigación que desarrollen desde una visión teórica los planteamientos vinculados a la geopolítica y la seguridad, son altamente necesarios para una mejor comprensión de los fenómenos que afectan negativamente a las sociedades.

Bibliografía

Agius, Christine. 2013. Social Constructivism. En *Contemporary Security Studies*, editado por Alan Collins, 87-103. Nueva York: Oxford University Press.

Agnew, John, y Gearoid O'Tuathail. 1992. "Geopolitics and discourse: Practical geopolitical reasoning in American foreign policy". *Political Geography* 11: 190-204.

Agnew, John. 1994. "The Territorial Trap: The Geographical Assumptions of International Relations Theory". *Review of International Political Economy* 1 (1): 53-80.

_____. 2005. *Geopolítica. Una re-visión de la política mundial*. Madrid: Trama Editorial.

Ayoob, Mohammed. 1997. "Defining Security: A Subaltern Realist Perspective". En *Critical Security Studies. Concepts and Cases,* editado por Keith Krause y Michael C. Williams, 121-148. Londres: UCL Press.

Child, John. 1979. "Geopolitical Thinking in Latin America". *Latin American Research Review* 14 (2): 89-111.

Cohen, Saul. 2015. *Geopolitics. The Geography of International Relations*. Nueva York: Rownman & Littlefield

Dalby, Simon. 1990. *Creating the Second Cold War. The Discourse of Politics*. Londres: Pinter Publishers.

_____. 1997. "Contesting an Essential Concept: Reading the Dilemmas in Contemporary Security Discourse". En *Critical Security Studies. Concepts and Cases,* editado por Keith Krause y Michael C. Williams, 3-32. Londres: UCL Press.

Dodds, Klaus. 2000. *Geopolitics in a Changing World*. Nueva York: Prentice Hall.

Doods, Klaus, y David Atkinson. 2000. Introduction to geopolitical traditions: a century of geopolitical thought. En *Geopolitical Traditions: A century of Geopolitical Thought*, 1-24. Nueva York: Routledge.

Dunn Cavelty, Myriam. 2013. "Cyber-Security". En *Contemporary Security Studies*, editado por Alan Collins, 362-378. Nueva York: Oxford University Press.

Flint, Colin. 2006. *Introduction to Geopolitics*. Nueva York: Routledge.

Font, Joan, y Joan Rufí. 2001. *Geopolítica, Identidad y Globalización*. Barcelona: Ariel.

Gray, Colin. 2007. *War, Peace and International Relations. An Introduction to Strategic History*. Nueva York: Routledge.

_____. 2012. *Categorical confusion? The strategic implications of recognizing challenges either as irregular or traditional*. Washington DC: Strategic Studies Institute/Army War College.

Griffiths, John. 2007. "Seguridad Hemisférica en América Latina. Alcances y Proposiciones". *Revista Globalización, Competitividad y Gobernabilidad* 1 (1): 88-104.

Grygiel, Jakub. 2006. *Great Powers and Geopolitical Change*. Baltimore: John Hopkins University Press.

Harvey, David. 1990. *The Condition of Posmodernity: An Enquiry into the Origins of Cultural Change*. Oxford: Blackwell.

Hassner, Ron. 2006. "The Path to Intractability Time and the Entrenchment of Territorial Disputes". *International Security* 31 (3): 107-138.

Kaplan, Robert. 2012. *The Revenge of Geography. What the Map tells is about coming conflicts and the battle against fate*. Nueva York: Random House.

Kelly, Phil. 2006. "A Critique of Critical Geopolitics". *Geopolitics* 11: 24-53.

_____. 2016. *Classical Geopolitics. A New Analytical Model*. Stanford: Stanford University Press.

Kubálková, Vendulka. 2001. "Foreign Policy, International Politics and Constructivism". En *Foreign Policy in a Constructed World,* editado por Vendulka Kubalkova, 15-37. Nueva York: M.E. Sharpe.

Manwaring, Max. 2011. *The Strategic Logic of the Contemporary Security Dilemma*. Washington DC: Strategic Studies Institute/ U.S. Army War College.

Müller, Martin. 2008. "Reconsidering the concept of discourse for the field of critical geopolitics: Towards discourse as language and practice". *Political Geography* 27: 322-338.

Nunn, Frederick. 2011. *Relaciones Militares Civiles Sudamericanas en el Siglo XXI*. Santiago: Academia de Guerra del Ejército de Chile.

O'Tuathail, Gearoid. 1994. "Problematizing Geopolitics: Survey, Statesmanship and Strategy". *Transactions of the Institute of British Geographers*, *New Series* 19 (3): 259-272.

_____.1996. *Critical Geopolitics. The Politics of Writing Global Space*. Londres: Routledge.

Paris, Ronald. 2001. "Human Security: Paradigm Shift of Hot Air?". *International Security* 26 (2): 87-102.

Roe, Paul. 2013. "Societal Security". En *Contemporary Security Studies,* editado por Alan Collins, 176-189). Nueva York: Oxford University Press.

Santa Cruz, Arturo. 2009. "Introducción". En *El constructivismo y las relaciones internacionales*, editado por Arturo Santa Cruz, 9-40. Ciudad de México: Colección Estudios Internacionales CIDE.

Taylor, Peter, y Colin Flint. 2002. *Geografía Política. Economía mundo, Estado-Nación y Localidad*. Madrid: Trama Editorial.

Von Chrismar, Julio. 2010. *Los Objetivos Nacionales, Base de la Política Nacional de los Estados*. Santiago: Academia de Guerra del Ejército de Chile.

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2459

Urvio, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 126-144
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

La construcción de confianza Estado-policías-comunidad, un problema de diseño institucional

Constructing Trust on State-Police-Community relationships, a problem of Institutional Design

Basilio Verduzco Chávez[1]

Fecha de recepción: 30 de septiembre de 2016
Fecha de aceptación: 15 de abril de 2017

Resumen

Este artículo presenta una lectura de la situación de inseguridad en la que se destaca la incapacidad del Estado para integrar soluciones organizacionales e institucionales que proporcionen seguridad a los agentes de los cuerpos policiales, ayuden a construir relaciones de confianza entre policías y sociedad, incrementen la legitimidad de las actuaciones policiales y, en consecuencia, reduzcan los índices de criminalidad observados. Se analiza la experiencia mexicana para estudiar la falta de confianza y el pobre desempeño de la policía como resultados de fallas de diseño institucional. Los problemas de diseño institucional persisten debido a errores de interpretación de la racionalidad de los actores y de los procesos de cambio social registrados en el país, malos diagnósticos de los problemas de seguridad, problemas al distinguir entre estructuras de implementación y poblaciones objetivo, al diseñar políticas públicas que forman parte de una estrategia de soberanía graduada que ofrece protección desigual a los ciudadanos.

Palabras clave: cambio institucional; control de confianza; México; policía; seguridad.

Abstract

This article presents an interpretation of insecurity, highlighting the lack of capacity of the State to integrate organizational and institutional solutions aimed at providing protection to police officers, building trust on police-society relationships, increasing police legitimacy and, therefore, reducing crime rates. Based on the analysis of the Mexican experience, this article looks at the lack of trust and the poor performance of police corps, consequences of institutional design failures. Such failures persist due to erroneous readings of actors´ rationalities and social change processes observed in the country, poor diagnostics of security problems, and confusion of implementation structures and target populations in public policies that integrate a graduated sovereignty strategy through which the state offers different levels of police protection to its citizens.

Keywords: Trust control; police; security; México; institutional change.

1 Profesor de la Cátedra Doctoral de Políticas Públicas y Desarrollo en el Departamento de Estudios Regionales-INESER en la Universidad de Guadalajara. Es Doctor en Planeación Urbana y Desarrollo de Políticas por la Universidad Rutgers en donde fue Becario Fulbright. Correo: basiliomapas@gmail.com.

Introducción

La desconfianza Estado-policías-ciudadanos es un rasgo del totalitarismo (Arendt 1976) y puede estar asociada a la corrupción, la impunidad y a los arreglos institucionales inadecuados para predecir los cursos de acción que seguirán los actores involucrados en los sistemas de seguridad (Bergman y Flom 2012; Ratton y de Alencar 2009).[2] En las últimas décadas, en México impera un clima de desconfianza en el sistema de seguridad pública. Según el Instituto Nacional de Estadística y Geografía (2016), la percepción de inseguridad se ha mantenido desde 2013 en cifras superiores al 67 por ciento, alcanzando en 2014, el 72 por ciento.[3] Esta percepción se refuerza por los altos índices de inseguridad en varias regiones y ciudades con cifras registradas en 2015 de 2,016 por cada 100 mil habitantes en el estado de Guerrero, 2,070 en el estado de México, 1,017 en Jalisco y 993 en Sinaloa (SESNSP 2016).

Este artículo analiza la desconfianza Estado-policías-comunidad como problema de diseño institucional y explora el vínculo entre diseños institucionales y estrategias más amplias de organización del Estado y el control ejercido sobre el territorio. Para tal efecto, se revisan ejemplos de la agenda de cambio institucional seguida en México (Barrachina y Hernández 2012; Hernández y Zepeda 2015) en donde, a diferencia de lo que ocurre en otros países como Chile o Costa Rica (Oviedo 2007), ha sido necesario partir de altos niveles de desconfianza. Esta agenda, seguida por los gobiernos del presidente Felipe Calderón (2006-2012) y el presidente Enrique Peña Nieto (2012-2018), se ha impulsado con un discurso geopolítico que simplifica en exceso el problema de desconfianza cuando identifica como responsables directos del problema a los agentes del sistema de impartición de justicia destacando la responsabilidad de las instituciones policiales de la federación, las entidades federativas y los municipios.

El gobierno mexicano ha optado por un enfoque de protección contra el crimen que puede caracterizarse como soberanía graduada, la cual abarca reorganización de las agencias responsables de los sistemas de seguridad, así como diseños institucionales para regular las fuerzas policiales de orden federal, estatal y municipal. Las reformas procuran una mayor centralización de las agencias policiales y vulneran la seguridad laboral de los agentes de policía. Se usan pruebas de control de confianza como principal mecanismo para depurar los cuerpos de policía y mejorar la confianza que tiene en ellos la ciudadanía (Barranchina y Hernández 2012). Un ejemplo de ello, es la reforma constitucional aprobada el 29 de enero de 2016, la cual incluyó entre las sanciones el despido injustificado, dando lugar a un debate público en torno a la necesidad de una contrarreforma para reestablecer la seguridad laboral de dichos agentes.

Los diseños institucionales son analizados como objetos estructurados a partir de elementos observables empíricamente como son: problemas a resolver, poblaciones objetivo, estructuras de implementación, reglas, supuestos y racionalidades (Schneider e Ingram 1997). En una democracia, algunos problemas de diseño pueden ser la estigmatización de poblaciones objetivo, simplificación de

2 La desconfianza se origina en la dificultad de predecir comportamientos, no en la designación de funciones preventivas o de reacción para los agentes de policía.

3 Población de 18 años y más que reside en las ciudades estudiadas que consideran es inseguro vivir actualmente en su ciudad (INEGI 2016).

problemas a resolver, o el uso inadecuado de herramientas de estímulo y sanción. Los diseños institucionales influyen en la construcción de confianza si ayudan a determinar en forma subjetiva las probabilidades de cursos de acción,a reducir en consecuencia la incertidumbre y los costos de transacción (Ratton y de Alencar 2009).

Hay por lo tanto una relación entre construcción de confianza, certidumbre institucional y seguridad en las comunidades (Oviedo 2007; Campoy-Torrente, Chelini y Soto-Urpina 2016). El proceso involucra cooperación y desarrollo de creencias y convenciones compartidas (Tyler y Fagan 2008); un comportamiento ético y responsable basado en el convencimiento y no solo en la coerción (Candina 2006), así como transparencia en las agencias de policía, reconocimiento de errores, de sanciones a conductas inadecuadas en forma expedita y participativa, y uso del poder en forma responsable a la vez que se atienden demandas ciudadanas (U.S. Department of Justice 2007).

Partiendo de una discusión del concepto de soberanía graduada como estrategia general de protección, en este trabajo se propone el concepto de "proceso local de construcción de confianza" para hacer referencia a situaciones de interacciones recurrentes entre representantes del Estado, policías y ciudadanos, en los que cada involucrado ajusta sus estrategias y sus expectativas a partir de los resultados en el comportamiento observado de otros involucrados. El trabajo concluye con una propuesta de seis pasos para lograr diseños que ayuden a construir confianza Estado-Policías-Ciudadanía.

La estrategia de soberanía graduada basada en soluciones organizacionales e institucionales centralistas

El tipo de reformas policiales introducidas en México y otros países de América Latina sigue una estrategia según la cual un Estado incapaz de ofrecer seguridad a todos, cambia las atribuciones de la policía (Rodríguez 2012), escoge merecedores y no merecedores y responde mejor a las necesidades de ciertos lugares y grupos sociales. Aihwa Ong (2000) denomina a dicha estrategia como de soberanía graduada la cual es usada para responder a presiones internacionales y domésticas mientras se intenta crear entornos económicos competitivos. El Estado focaliza sus acciones en el control de la migración, el flujo comercial, la vigilancia de instalaciones estratégicas, carreteras y sitios de valor comercial, turístico o de comunicación internacional. Para controlar, el Estado dirige operativos a sitios donde hay disputas territoriales entre bandas criminales o donde se registran eventos de inseguridad. En una sociedad en transición como la mexicana, la estrategia no resuelve la desconfianza porque no logra borrar los vestigios de autoritarismo e informalidad y no puede garantizar justicia (Rivera 2012).

Soberanía graduada, desconfianza y reforma policial en México

La policía en México nunca ha gozado de confianza plena, pero el alto grado de desconfianza registrado en los últimos años es propio de una economía en proceso de apertura económica y transición política con altos niveles de desigualdad. En la transición, la desconfianza

se basa en la experiencia del régimen anterior y se alimenta de eventos y situaciones adversas como haber sido víctima o testigo de un abuso policial, o vivir en un barrio de bajos ingresos (Bergman y Flom 2012). Hay eventos con un alto impacto en los niveles de confianza (CIDAC 2016). La pérdida de confianza revela la existencia de una sociedad dividida, con antecedentes autoritarios y un mal desempeño de la policía (Goldsmith 2005).

La falta de confianza en los cuerpos de seguridad es un problema circular y acumulativo pues la falta de confianza reduce la capacidad del Estado para garantizar seguridad y resta legitimidad a las actuaciones policiales, produciendo en consecuencia un menor desempeño y mayor desconfianza (Goldsmith 2005; Dammert 2005). La transición abre oportunidades para un mayor respeto a los derechos humanos, el uso de mecanismos de control o mayor participación y empoderamiento ciudadano (Costa y Neild 2007); pero la desconfianza se fortalece por la infinidad de cambios organizacionales e institucionales que acompañan la transformación del régimen político, la misma que abarca cambios en el peso de los partidos políticos, mayor influencia de los medios, distribución de triunfos electorales por partido y por región, debilitamiento relativo del ejecutivo y pérdida de influencia de grupos de poder (Shaw 1995; Felix Azogu 2013; Savelsberg y McElrath 2014).

El Estado mexicano ha procurado instaurar un régimen de justicia y protección contra el crimen para responder a tres procesos internacionales que influyen en la relación Estado-sociedad y en las percepciones que tienen agentes externos sobre la seguridad en México. Estos son: la globalización, que ha convertido la protección contra el crimen en un factor de competitividad internacional y ha revivido dilemas sobre el tipo de protección y las poblaciones a proteger; el surgimiento de una ciudadanía global conformada por organismos cívicos internacionales, líderes experimentados y vínculos con grupos de activistas mexicanos con una agenda internacional interesados en monitorear los avances del país en aspectos clave de seguridad y derechos humanos; y la expansión del crimen organizado y sus disputas territoriales.

Desde finales de los años ochenta, pero particularmente desde el año 2000, con el arribo de la alternancia partidista a nivel federal, el Estado mexicano enfrenta también procesos domésticos que influyen en la configuración de la geografía del crimen y en las relaciones intergubernamentales orientadas a disminuir las condiciones que hacen posible la comisión de delitos. Estos procesos son: la transformación productiva regional y el mayor peso de flujos internacionales de comercio e inversión extranjera, personas y mercancías que tienen lugar en zonas metropolitanas, corredores industriales, sitios turísticos, regiones fronterizas, áreas de cultivo de productos agrícolas de exportación, puertos, aeropuertos, autopistas y zonas costeras; la democratización y proliferación de grupos que trabajan en múltiples agendas de interés público, entre los que se destacan temas de seguridad y desempeño de policías; y la conformación de contextos situacionales locales (Pacheco y Verduzco 2015) que hacen posible la comisión de delitos entre los que se encuentran procesos de planificación urbana, decisiones de localización de infraestructuras, privatización del espacio público.

La oferta de protección que ofrece el Estado mexicano ante los cambios anteriores abarca cambios organizacionales e institucionales con orientaciones geopolíticas de corte

centralista y punitivo. Según Alvarado y Zaverucha (2010), una de sus manifestaciones es la creciente presencia del ejército en todo tipo de tareas de vigilancia y represión. En las reformas prevalece la idea de corregir desde arriba a los cuerpos de seguridad, sobre todo los del ámbito municipal. La revisión de cambios presentada por Meyer (2014) muestra una búsqueda disfuncional de reformas a los sistemas de seguridad. Una lista no exhaustiva de cambios incluye la creación del Sistema Nacional de Seguridad Pública en 1995, que es vigilado por el Consejo Nacional de Seguridad Pública; la creación en 1998 del Fondo de Aportaciones para la Seguridad Pública; la Policía Federal Preventiva (PFP), que absorbió entre otros a elementos de la Policía Federal de Caminos, la Policía Fiscal. En el periodo 2000-2006, la PFP fue puesta bajo la supervisión de la Secretaría de Seguridad Pública y se creó la Agencia Federal de Investigación como parte de la Procuraduría General de la República. En el Gobierno de Calderón se firmaron pactos internacionales de cooperación en seguridad como la Iniciativa Mérida, firmada con Estados Unidos, y se introdujeron cambios al sistema de procuración de justicia y reformas adicionales a los cuerpos de seguridad. En ese periodo se iniciaron operaciones militares para combatir al crimen organizado y se propuso una iniciativa para crear un mando único policial a nivel de Estados, pero con posibilidades de mayor centralización a nivel federal. En el gobierno del presidente Peña Nieto (2014-2018) se han continuado esas iniciativas y creado otros cuerpos de seguridad como la Gendarmería.

Lo que Carrión (2007) denomina nueva doctrina de reformas, en México ha contribuido a debilitar las condiciones laborales de los agentes de seguridad (Olivares 2010).[4] En el proceso se ha sembrado desconfianza al sugerir que es imposible tener cuerpos de seguridad y agentes confiables y capaces si no se introducen sistemas de control de confianza, soluciones organizacionales centralizadas y amenazas creíbles de pérdida de empleo para los agentes de seguridad (Ángel 2016; Piñeiro 2016; Secretaría de Gobernación 2016). Los agentes se sienten vulnerables pues se les puede dar de baja si no aprueban un examen o incluso en forma arbitraria.[5] Las medidas centralizadoras debilitan a los gobiernos locales y confunden a la ciudadanía con distribuciones de competencias poco claras. La centralización da lugar a un círculo vicioso que asigna funciones de policía local a la policía federal o incluso al Ejército, y eso genera más debilidad de policía local (Meyer 2014).

Confianza, legitimidad social y seguridad

Soberanía, confianza y seguridad ofrecida por el Estado a sus ciudadanos son fenómenos interconectados (Perekh 2008; Hayden 2009; Ong 2000). Para avanzar en legitimidad, debe existir confianza y no se puede dejar a sectores desprotegidos. Los estudios de capital social y de gobernanza (Solís 2016; Aguirre 2016) proponen la importancia de mejorar la seguridad ciudadana cuando se convive en un contexto de bajo capital social. Confianza y legitimidad influyen en el desempeño policial y en la reducción de índices delictivos en un país.

4 Los conceptos de condiciones laborales o seguridad laboral se refieren a salarios, prestaciones y condiciones de contratación, promoción y permanencia.

5 El despido arbitrario contemplado en la reforma constitucional de 2016, replica en México el argumento de que no puede haber errores en el trabajo de ser policía (Ozimek 2014).

Ratton y de Alencar (2009) sugieren que hay confianza cuando un sujeto puede predecir, con alta probabilidad, el comportamiento de otros. La confianza es un patrón de relaciones socialmente aprendido que no se produce por decreto. Para Goldsmith (2005) la confianza en las labores realizadas por los organismos y agentes de seguridad e impartición de justicia es necesaria para incrementar la legitimidad social de las prácticas policiales, y ambas son cruciales para mejorar el desempeño.

El modelo de soberanía graduada abarca aspectos como la construcción discursiva del temor, la responsabilidad y el respeto a los derechos de otros; pero son las soluciones organizacionales e institucionales que produce, las que influyen en la desconfianza. La distribución de competencias entre los distintos órdenes de gobierno, entre distintos poderes y entre distintas agencias, son vistas con desconfianza por los individuos cuando hay fallas de coordinación. Los arreglos que regulan las interacciones entre agentes del Estado y los ciudadanos pueden generar desconfianza si no abordan en forma adecuada las racionalidades y comportamientos de los actores o si ofrecen distintos niveles de protección.

El Estado mexicano enfrenta problemas para construir confianza porque insiste en soluciones incompatibles con la aspiración social de protección como bien público de cobertura universal. Dichas soluciones son insuficientes para proteger derechos humanos, inadecuadas para dar legitimidad al ejercicio del monopolio de violencia, ineficaces para lograr una coordinación intergubernamental eficiente en un marco constitucional republicano y un régimen democrático, y adversas a la construcción local de relaciones de confianza entre agentes de seguridad y ciudanía. La siguiente sección profundiza en el problema de los diseños institucionales y su orientación a la centralización del poder y el uso de estrategias punitivas de corte militar.[6]

Orientaciones institucionales e interdependencia de problemas a resolver

La literatura sobre diseños institucionales enfatiza la importancia de procurar coherencia entre los elementos del diseño y los grandes objetivos a resolver en el ámbito público (Schneider e Ingram 1997). El análisis de los diseños de instrumentos de política, como reformas constitucionales o protocolos de actuación policial, es útil para identificar su orientación al logro de objetivos como la mejoría de las condiciones laborales de los agentes de seguridad, la confianza de la ciudadanía hacia el Estado y sus agentes, la prevención de delitos, y el respeto a derechos humanos y libertades.

En México, los diseños de política dirigidos a inspirar confianza y mejorar el desempeño policial tienden a corregir a la policía y concentrar el poder para combatir la penetración del crimen organizado en las agencias de policía. Para lograr respaldo social a estas políticas se usan datos y hechos que alimentan una construcción social de los policías como agentes esencialmente corruptos, violentos, y hasta criminales. Los instrumentos favoritos son reformas constitucionales, leyes nacionales y legislaciones estatales.

Un caso ejemplar es la reforma constitucional publicada el 29 de enero de 2016 a la Fracción XIII del apartado B del artículo 123 constitucional. Dicha fracción establece que:

6 En esa dirección queda la iniciativa de Ley de Seguridad Interior que se discutía en el Congreso de la Unión al momento de escribir este trabajo.

> "Los militares, marinos, personal del servicio exterior, agentes del Ministerio Público, peritos y los miembros de las instituciones policiales, se regirán por sus propias leyes".[7]

En el diseño se destacan algunas herramientas correctivas de posibles comportamientos adversos, cuando se indica que:

> "Los agentes del Ministerio Público, los peritos y los miembros de las instituciones policiales de la Federación, las entidades federativas y los Municipios, podrán ser separados de sus cargos si no cumplen con los requisitos que las leyes vigentes en el momento del acto señalen para permanecer en dichas instituciones, o removidos por incurrir en responsabilidad en el desempeño de sus funciones. Si la autoridad jurisdiccional resolviere que la separación, remoción, baja, cese o cualquier otra forma de terminación del servicio fue injustificada, el Estado sólo estará obligado a pagar la indemnización y demás prestaciones a que tenga derecho, sin que en ningún caso proceda su reincorporación al servicio, cualquiera que sea el resultado del juicio o medio de defensa que se hubiere promovido.[8]

Este mandato constitucional deja en manos de autoridades de los tres órdenes de gobierno la creación de sistemas complementarios de seguridad. Otros arreglos institucionales también contemplan recomendaciones correctivas de prácticas policiales, pero buscan generar confianza mediante la oferta de un servicio de calidad. El Artículo 13 del Reglamento para Vigilar la Actuación de los Elementos de la Dirección General de Seguridad Pública de Guadalajara, contempla como faltas graves diversas acciones que dañan directamente a la ciudadanía tales como ocultar sus datos oficiales al público, utilizar rigor innecesario, salirse de su área para cometer delitos o ilícitos; escandalizar ebrio o bajo la influencia de estupefacientes, actuar con negligencia en el uso del armamento, poner en riesgo a los particulares; revelar asuntos secretos o reservados, obligar o sugerir entregas de dinero o cualquier tipo de dádivas; realizar detenciones sin causa justificada, atentar en contra de los bienes y derechos de los particulares o contra la integridad física de las personas en situaciones que no impliquen legítima defensa, proferir amenazas en contra de los particulares o dar motivo razonable de pérdida de confianza.[9]

Estos instrumentos institucionales presentan problemas, como son estructuras de implementación de corte jerárquico con espacios para el abuso de poder al interior de los órganos de policía; baja participación de la ciudadanía en la definición de objetivos y acciones contempladas para restaurar la confianza en los cuerpos de seguridad; uso de herramientas inadecuadas para facilitar la transparencia. Estos errores no ayudan a crear incentivos a converger en comportamientos dentro de un marco de legitimidad comúnmente construido y aceptado. Un análisis de reformas constitucionales y protocolos de actuación ilustra las confusiones y errores de diseño.

En la fracción XIII, del artículo 123, apartado B, los agentes de seguridad son poblaciones objetivo, pero se les puede tratar como parte de la estructura de implementación que comprende agencias empleadoras y demás organizaciones involucradas en implementar las medidas dirigidas a corregir a los cuerpos de seguridad como son los centros de evaluación y control de confianza.[10] Ellos

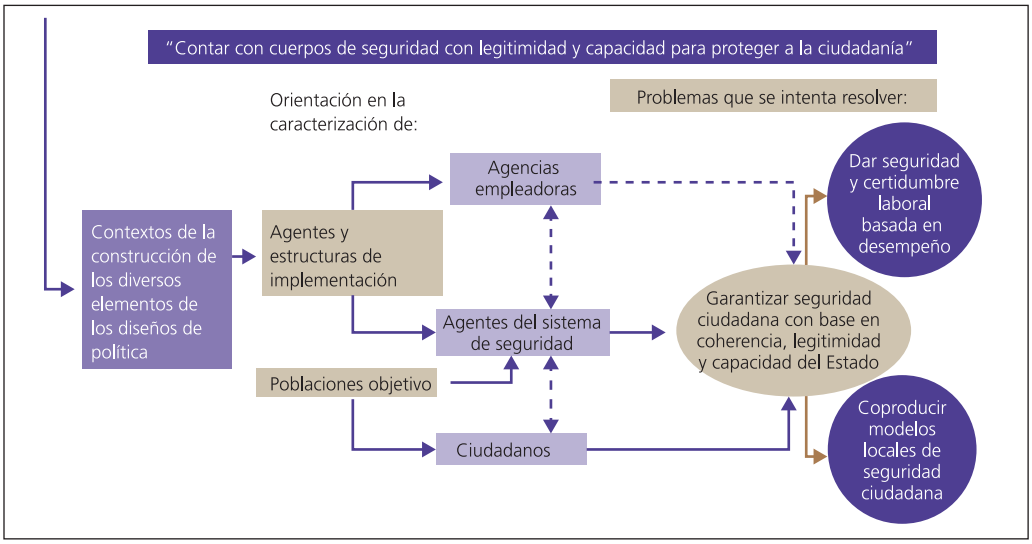
7 Párrafo reformado, DOF, 29-01-2016.

8 Párrafo reformado DOF 29-01-2016.

9 Situaciones simplificadas del original.

10 Los Centros de Evaluación y Control de Confianza fueron institucionalizados en 2010. Su funcionamiento es mo-

Figura 1. Un modelo simplificado para ofrecer seguridad basado en coherencia, legitimidad y confianza



reciben en forma directa el costo de mayor vulnerabilidad del nuevo marco institucional. Los ciudadanos son poblaciones objetivo de segundo orden que recibe los posibles beneficios generados por la reforma organizacional y la introducción de sistemas centralizados de control de confianza.

El Reglamento para Vigilar la Actuación de los Elementos de la Dirección General de Seguridad Pública de Guadalajara, intenta regular la actuación de los policías para "proteger a la ciudadanía". La meta es el mejoramiento en los niveles confianza y de seguridad. En este caso, la población objetivo inmediata es la ciudadanía. Los cuerpos de seguridad son parte clave de una estructura de implementación que abarca al gobierno municipal como agencia empleadora. El reglamento define acciones dirigidas a mejorar la relación sociedad-agentes de seguridad.

nitoreado por el Centro Nacional de Certificación y Acreditación.

Junto con este tipo de cambios institucionales, han proliferado políticas públicas que buscan fortalecer las capacidades de acción y respuesta punitiva de los organismos de seguridad tales como compra de equipamiento, armas, sistemas de vigilancia y programas de entrenamiento. Por otro lado, se ha insistido en acciones como "operativos", "inspecciones de rutina", "reacción a situaciones de crisis" y "patrullaje preventivo", entre otros. Estos ejemplos ilustran la necesidad de diseños más adecuados al objetivo de construir confianza Estado-Policías-Ciudadanía. La figura 1 presenta las características de un modelo participativo alterno que cubren cuatro aspectos de la construcción de confianza:

a) **Conocimiento del contexto.** Análisis transparente de información, diálogo y consultas, los involucrados generan un conocimiento compartido del contexto en el que se diseñan las políticas públicas.

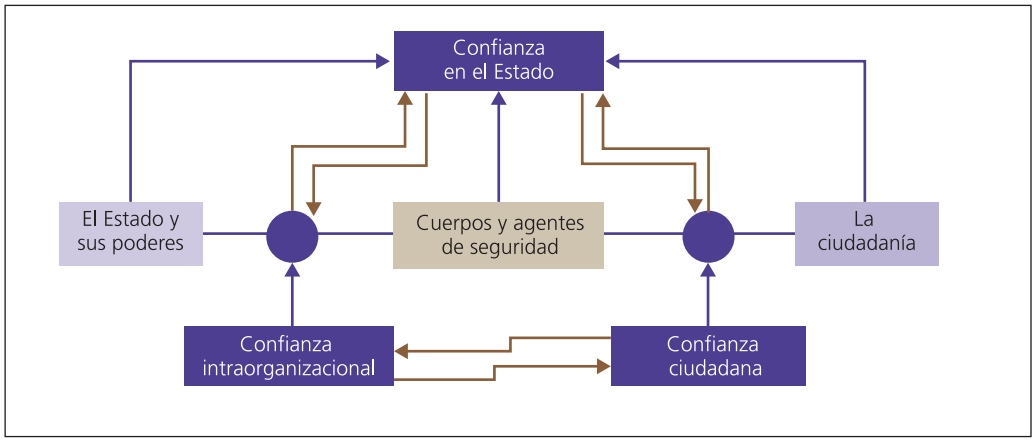
b) **Objetivo claro.** Los involucrados conocen y comparten el objetivo general de contar con cuerpos de seguridad con legitimidad y capacidad para proteger a todos los ciudadanos.
c) **Claridad del problema a resolver y de objetivos.** Los involucrados establecen por acuerdo el objetivo de lograr una oferta de seguridad ciudadana con base en coherencia, legitimidad y capacidad del Estado y en certidumbre laboral para los policías.
d) **Distinción clara de estructuras de implementación y poblaciones objetivo.** Los arreglos institucionales distinguen claramente cuándo los policías son población objetivo de una política –como la reforma constitucional que regula su relación laboral con el Estado- y cuándo son estructura de implementación –responsable de proveer el servicio de protección respetando libertades y respetando derechos humanos.

La estructura propuesta se basa en el reconocimiento de la interdependencia entre la desconfianza imperante y las interacciones negativas con la ciudadanía como acciones de corrupción, abuso de autoridad o violación de derechos humanos.

Cambio institucional, confianza y desempeño de los cuerpos de seguridad

En una transición política, es difícil lograr cambios institucionales con diseños promotores de relaciones de confianza entre Estado, policías y población. La transición no elimina el uso de construcciones sociales dominantes sobre aspectos como la discrecionalidad en el uso del poder del Estado, la definición del mandato de una policía para servir a los poderosos o la noción de peligrosidad asociada a variables de ingreso, etnicidad y edad. Corrupción e impunidad tienden a perdurar. La transición a la democracia hace necesario tratar en forma integral las múltiples relaciones existentes entre Estado policías y ciudadanía. La figura 2 sugiere la existencia de tres esferas de confianza a considerar en los diseños institucionales del sistema de seguridad.

Figura 2. La interdependencia de las relaciones de confianza en el sistema de seguridad pública



a) **La confianza en el Estado.** Tiene que ver con el grado de legitimidad alcanzado por un Estado. Abarca aspectos como la confianza en la procuración del bienestar social, la provisión de bienes colectivos y la protección universal de los derechos y seguridad de la población.
b) **La confianza intra-organizacional.** Asociada a relaciones duraderas, mejor desempeño y más valor de las organizaciones (Chien y Wu 2006). Tiene que ver con la confianza entre agentes de seguridad y sus jefes superiores; y con el respeto del Estado y los superiores inmediatos por el cumplimiento de las funciones básicas de los agentes de seguridad.
c) **La confianza ciudadana en la seguridad.** Es decir, confianza en la integridad de los agentes, su compromiso con su trabajo, la mejora de su desempeño y su renuncia a comportamientos y conductas adversas a su misión de proteger a la ciudadanía. Esta confianza es vital para establecer lazos de trabajo y cooperación con las comunidades (Dammert y Lunecke 2004).

En la construcción de confianza entre sociedad (principal) y agentes, son importantes las señales emitidas, la propensión al riesgo de los participantes en la relación y la capacidad de cumplir con lo prometido. Confianza y desconfianza son patrones de relaciones (Ratton y de Alencar 2009) que pueden ser alterados drásticamente por eventos o sucesos inesperados, o por esfuerzos deliberados o intencionados. Para crear certidumbre, los diseños institucionales deben reducir la discrecionalidad de acción fuera de un rango socialmente aceptado.

Los responsables de ofrecer protección pueden lograr confianza si demuestran tener compromisos efectivos con la ciudadanía. Para ello es necesario desarrollar propiedades intrínsecas tales como habilidades efectivas, motivaciones generadas por la internalización de normas y la benevolencia o interés en favorecer a otros, las cuales pueden hacer de un agente un ente confiable en sí mismo. También se puede lograr confianza cuando existen incentivos contextuales que inducen comportamientos dignos de confianza (Riegelsberger, Sasse y McCarthy 2004; Banks 2014).

Los incentivos contextuales son mezclas de construcciones discursivas y recompensas tangibles que definen escenarios de costos, así como compensaciones o reconocimientos por desempeño en el cumplimiento de la misión solicitada por un principal a un agente. Los incentivos son situacionales y se refieren a la posibilidad de permanecer o salir del juego por factores como incumplimiento, interés por cuidar la reputación social o la existencia de árbitros externos. Incentivos o sanciones pueden realizarse a nivel personal u organizacional y los criterios de evaluación de desempeño se establecen en función de las aspiraciones de una sociedad.

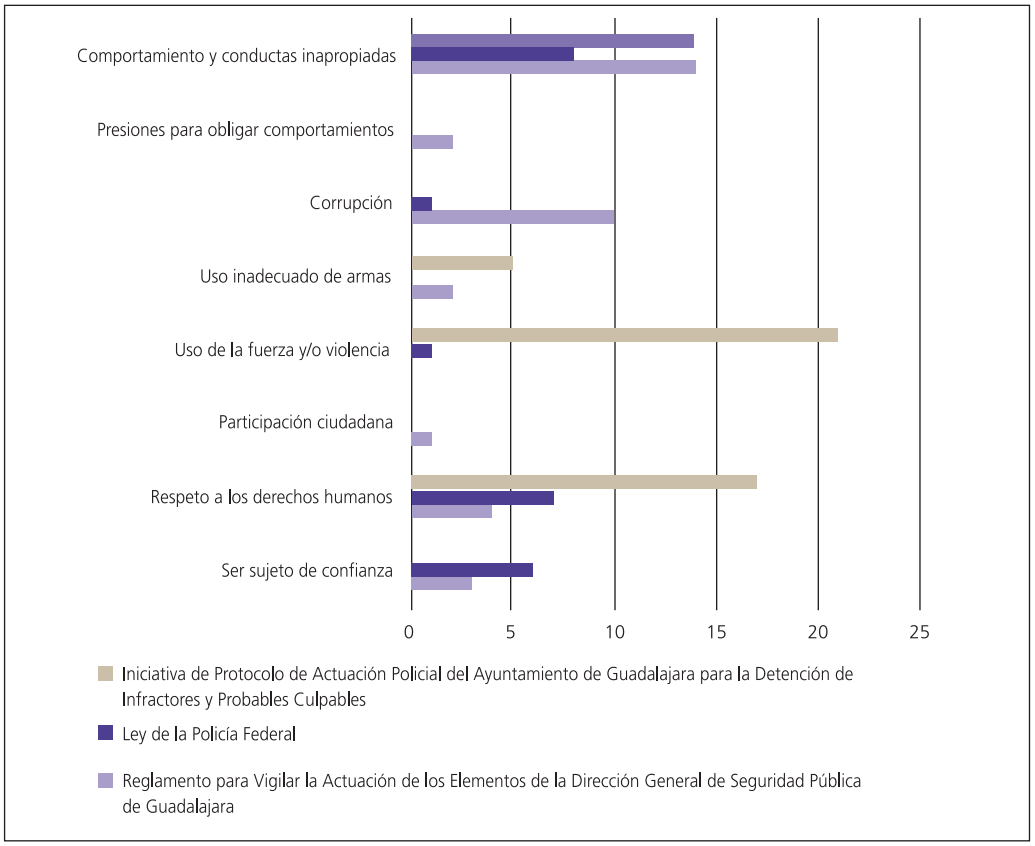
En México, las reformas insisten en sistemas de control de confianza estancados en el plano de los incentivos contextuales y no se logran avances en la creación de propiedades intrínsecas entre los agentes que conduzcan a relaciones de confianza más estables. Algunas explicaciones posibles de la situación, son los problemas de politización de las decisiones, el mal entendimiento de la profundidad de las reglas informales aplicadas por agentes de seguridad, la corrupción de los mandos superiores, o la escasa continuidad del cambio institucional. Al reformar desde arriba se pierden de vista que las dinámicas de diseño institucional son socialmente construidas y reflejan los valores e interpretaciones de los diseñadores y la

influencia de los grupos de interés (Schneider e Ingram 1997).

Un ejemplo específico de la construcción discursiva de las relaciones de confianza, lo ofrece la exposición de motivos de la regidora María Candelaria Ochoa, al presentar al Ayuntamiento de Guadalajara la *Iniciativa de Protocolo de Actuación Policial del Ayuntamiento de Guadalajara Para la Detención de Infractores y Probables Culpables.* La propuesta de abril de 2014, identifica conductas inapropiadas de los policías como el factor que pudo haber influido en un enfrentamiento entre policías y asistentes a un partido de futbol. La regidora Ochoa señala:

> "Existen testimonios de personas que asisten regularmente a este tipo de eventos masivos en donde señalan las prácticas de hostigamiento de los elementos de la policía de Guadalajara, lo que se traduce en ´insultos, golpes, escupitajos y hasta racismo por parte de la autoridad, lo que desemboca en

Gráfico 1. Aspectos considerados en la regulación dirigida a incrementar la legitimidad y desempeño de la acción policial.



Fuente: construcción propia con lectura de contenido de los ordenamientos señalados*.

*Para determinar la frecuencia se realizaron búsquedas de palabras clave analizándose el contexto en el cual se usaban. Se omitieron del conteo referencias a nombres de dependencias públicas o a títulos de apartados del ordenamiento y menciones en cuadros y gráficos. Las menciones de actos que constituyen comportamientos o acciones independientes, se tomaron como menciones separadas.

> arrestos masivos dentro o fuera de los estadios de futbol" (Iniciativa de Protocolo de la Regidora Candelaria Ochoa 2014).

El gráfico 1, compara tres diseños y sugiere que los diseñadores plasman en cada instrumento su interpretación sobre ocho aspectos la relación entre agentes y ciudadanía. En ella se observan tres temas dominantes: "uso de la fuerza y/o la violencia", "el respeto a los derechos humanos" y "el comportamiento y las conductas inadecuadas" por parte de la policía. Estos temas se plasman como una generalidad o como un interés basado en comportamientos particulares ocurridos durante algún evento.

La frecuencia de menciones indica la relevancia de dichos temas en la orientación general del arreglo institucional revisado y su posible contribución a la mejora de la relación de confianza. En los tres casos, el tema de la participación ciudadana es poco mencionado, aunque se reconoce que en el reglamento de Guadalajara hay un apartado especial que regula el Consejo Consultivo de Seguridad Ciudadana y establece reglas para su integración, funcionamiento y actividades a realizar. En ninguno de los documentos se percibe un trato claro a la interdependencia de relaciones de confianza en el sistema de seguridad pública o un rompimiento con la cultura organizacional prevaleciente (Cantú 2014) o con las preferencias centralistas de los actores públicos (Sánchez 2015).

Insistir en el modelo de control de confianza de mandos policiales diseñados y coordinados por autoridades superiores es un acto geopolítico. Dicho acto intenta consolidar relaciones de poder centralistas y autoritarias (Olivares 2010). Para el agente de seguridad, los resultados de las pruebas de control de confianza son potencialmente arbitrarios en manos de mandos superiores con prejuicios e intereses propios que no necesariamente buscan mejorar las condiciones de seguridad de la población. En el estudio realizado por Causa en común (2015) los entrevistados reportan desconfiar en la utilidad de los exámenes, critican los gastos incurridos, señalan la participación de personas incompetentes en su aplicación, e identifican sesgos para despedir a quienes no son bien vistos por los jefes.

La existencia de tres esferas de relaciones de confianza en el diseño de nuevos arreglos institucionales plantea la necesidad de avanzar en la construcción simultánea de relaciones de confianza en cada una de ellas. En esta perspectiva, la seguridad laboral de los agentes, entendida como respeto a derechos laborales básicos y a prestaciones adecuadas al trabajo que realizan, se vuelve indispensable para mejorar la seguridad ciudadana ya que se relaciona buen desempeño de agentes con la existencia de incentivos intrínsecos para optar por comportamientos adecuados.

La revisión de problemas de diseño institucional sugiere que México necesita transitar hacia modelos locales de seguridad ciudadana basados en la legitimidad, la confianza y el desempeño de los agentes de seguridad. Procesos en el sentido sugerido por Tyler y Fegan (2008) donde funcionarios electos, policías y ciudadanos participan en procesos interactivos repetidos que son sometidos a revisión, pero los involucrados tienen grados de libertad para acoplar sus acciones a lo legítimamente esperado por los demás involucrados.

La coproducción de modelos locales de seguridad ciudadana

La revisión de arreglos institucionales presentada en la sección anterior permite identificar

una ruta de cambio institucional de seis pasos hacia mejores relaciones de confianza y mejor desempeño de los cuerpos de seguridad.

Paso 1. Entender mejor la racionalidad de los agentes y actores sociales

Las políticas de reforma policial se han basado en supuestos equivocados sobre la racionalidad de los agentes y los actores sociales. Por un lado, en vez de ver la violencia, y la inseguridad como una relación social (Dammert y Lunecke 2004), las reformas confían en reducir transgresiones incrementando las sanciones. Eso es poco viable en condiciones de impunidad e incertidumbre institucional provocada por cambios recurrentes. Por otro lado, la idea construir relaciones de confianza desenraizando las organizaciones policiales de sus entornos locales no tiene fundamento teórico o empírico. Ambos supuestos son debatibles.

Los agentes construyen la racionalidad de su actuación en el marco de sus propias relaciones laborales y de la confianza que tienen en sus mandos o en el Estado. La racionalidad de los agentes no está guiada solamente por el tamaño de la sanción sino por la probabilidad de que se ejecute. La política de mando único policial ha avanzado con lentitud (Ángel 2016) y es criticable por las inconsistencias de su adopción y la mala interpretación sobre la racionalidad de los actores públicos y su relación con la ciudadanía. La estrategia de desarraigo y el control centralizado del mando policial no garantiza efectividad en la construcción de confianza si los policías del mando único incurren, como es el caso, en comportamientos que alimentan la desconfianza.

Los estudios sobre el tema sugieren que es más fácil construir confianza y legitimidad en entornos familiares de tipo local dada la existencia de marcadas diferencias en las expectativas de las comunidades (Jackson 2015). El estudio de Sánchez (2015), muestra que los actores públicos participantes en la tarea de ofrecer seguridad, siguen estrategias adaptativas en sus elecciones institucionales. Ellos entienden que los arreglos institucionales favorecen ciertos intereses y distribuyen beneficios en forma desigual. Su estudio con grupos focales reveló que quienes más apoyan el mando único son quienes están más cerca del poder central. Su apoyo no se basa en la efectividad de una fuerza policial centralizada, sino porque esperan que arroje dividendos políticos y económicos construidos en estructuras políticas verticales.

El institucionalismo ha demostrado que las reglas definen incentivos y los incentivos inducen comportamientos. De conformidad con el modelo de interdependencia de las esferas de confianza entre Estado, agentes y ciudadanía, se necesitan nuevos arreglos institucionales que ofrezcan incentivos a todos los involucrados a cooperar en un juego multilateral cuyos beneficios son una mayor seguridad laboral para agentes y una mayor protección para la ciudadanía.

Paso 2: Reconstruir geopolíticamente a las agencias de seguridad como entidades dignas de confianza

La introducción de pruebas de control de confianza es la piedra angular del nuevo esquema de certificación de policías en México. La desconfianza en ellos ha crecido debido a su construcción social como organizaciones que funcionan como carteles institucionalizados que defienden sus propios intereses y los de sus aliados en las redes del crimen or-

ganizados (Alvarado 2008), y porque se ha construido un aura de temor y vulnerabilidad ante el crimen. En las reformas policiales, los agentes de seguridad han sido convertidos en poblaciones objetivo etiquetados como no dignos de confianza y merecedores de sanciones de tipo laboral y penal. Dicha construcción social presenta la incertidumbre laboral de los agentes de seguridad como una estrategia de "limpieza" de las agencias de policía, para hacerlas más eficientes y responsables y respetuosas de los derechos de los ciudadanos. Las propuestas de cambio institucional presentan a la sociedad el falso dilema de elegir entre contar con policías honestos y capaces o tener agentes de seguridad con garantías laborales que son deseables en cualquier otro empleo.

La reconstrucción geopolítica de las agencias de seguridad como entidades dignas de confianza necesita un discurso que pueda integrar la búsqueda de una mayor eficiencia en la organización de los cuerpos de policía, con mejoras de sus condiciones laborales y el logro de niveles de seguridad ciudadana en los distintos entornos de convivencia social. Más que un marco jurídico laboral de corte punitivo para los agentes de seguridad, se necesita construir con la ciudadanía un marco institucional que ofrezca incentivos y sanciones para mejorar las prácticas policiales y estímulos a la cooperación ciudadanía-agentes de policía. Como se infiere del estudio sobre el trabajo de Hannah Arendt (Perekh 2008), los arreglos institucionales deben ofrecer incentivos también a la ciudadanía para embarcarse en relaciones de confianza con la policía y con el Estado, lo cual puede incluir un mayor poder de toma de decisiones sobre seguridad y sobre el uso de recursos públicos.

Paso 3. Inducir procesos compartidos para crear seguridad y confianza

La construcción de confianza y legitimidad es un camino de doble sentido (Jackson 2015). Las reformas institucionales deben abrir las puertas a formas participativas para redefinir la misión de los agentes de seguridad. Los diseños deben alentar formas de cooperación incluso en condiciones críticas de interacción, como ocurre en erupciones de violencia, y deben ser flexibles para adaptarse a necesidades específicas de la población, aun en situaciones de tensión social.

Cuando se ignora la participación de ciudadanos en los procesos de diseño institucional y en la prevención del delito, se ignora también el carácter situacional del mismo destacado en las nuevas corrientes de la criminología (Pacheco y Verduzco 2015). Imponer diseños desde arriba conduce a fallas en la prevención y a violaciones a leyes y procedimientos. Sin participación pública crecen las dudas sobre su legitimidad de la acción del Estado y su compromiso con los intereses de la ciudadanía.

Paso 4. Reconocer que toda la seguridad es local

El diseño de reformas constitucionales y de protocolos de actuación debe transformar la exposición al contexto internacional de las regiones del país en retos locales de provisión de seguridad. Los representantes de los tres órdenes de gobierno pueden jugar un papel distinto en la creación de escenarios locales de seguridad. La incorporación de ciudadanos contribuye a crear entornos locales de confianza y seguridad ciudadana.

La estrategia de graduación de soberanía basada en soluciones organizacionales centralizadas diseñadas para cubrir la necesidad de

personas, bienes y lugares estratégicos deja en manos del mercado la provisión de seguridad al resto de las necesidades sociales. Dicha alternativa ignora los hallazgos institucionalistas sobre los beneficios del policentrismo según los cuales, la diversidad de centros de poder produce sistemas eficientes de seguridad (Pérez-Ducy 2013), y la división del trabajo entre distintas instancias de gobierno es necesaria para establecer mandatos y jerarquías con claridad (Ostrom, Parks y Whitaker 1978).

Las diversas formas de contratación de seguridad privada revelan preferencias sociales sobre modelos escalables de seguridad como respuesta a necesidades sociales. Es necesario estudiar esas formas de contratación para diseñar instituciones y organizaciones policiales públicas competentes y confiables. Los nuevos diseños institucionales deben resolver en forma integral los problemas de desconfianza que ocurren en las tres esferas identificadas en la sección 3. Como lo sugiere Ralston (2006), la confianza intra-organizacional se construye interviniendo en factores que están afuera de los individuos. Las múltiples quejas sobre los sistemas de control de confianza, señaladas antes, son evidencia de que la desconfianza en dichos sistemas refleja la falta de confianza de sociedad y agentes de seguridad en el propio Estado.

Paso 5. Rediseñar incentivos tomando en cuenta el papel de la información y la transparencia en la construcción la confianza

En un mundo dominado por las tecnologías de información y comunicación, eventos aislados de confrontación ciudadanía–agentes de seguridad, alimentan la desconfianza incluso en sociedades con democracias consolidadas. Para presumir una trayectoria de comportamientos y conductas adecuadas, es necesario contar con procesos permanentes de monitoreo basados en información objetiva. Al diseñar instrumentos de transparencia es preciso entender el papel de la información verídica y los rumores en la construcción de percepciones sociales. Esto significa que es necesario insistir en la claridad de los incentivos y en la definición de fronteras socialmente aceptables para el comportamiento de los agentes de seguridad. Ciudadanos y policías deben contar con criterios objetivos para determinar cuándo se incurre en fallas sancionables y el repertorio de sanciones aplicables.

La aplicación de los exámenes de control de confianza basados en umbrales para demostrar capacidad y confiabilidad arroja el resultado paradójico de incrementar la desconfianza cada vez que un agente aprobado incurre en un comportamiento sancionable según la legislación vigente. El error del sistema de umbrales es aprobar personas en un momento fijo, no en construir procesos dinámicos de (prevención-monitoreo-mitigación-compensación) dirigidos a la construcción de confianza que cuenten con el consentimiento social.

Para generar confianza en los procesos, los diseños deben contemplar lineamientos dirigidos a transparentar la información sobre agendas de trabajo, actividades de rutinas y reportes de actividades de los agentes de seguridad. Además de regular aspectos como el uso de la fuerza y las armas en las interacciones ciudadanos-agentes, es necesario un monitoreo cercano y permanente del comportamiento de los agentes, y mayor transparencia sobre sus actividades rutinarias o extraordinarias. La proliferación de sistemas privados de monitoreo usados por las redes sociales ha puesto en manos de la ciudadanía una solución a ese problema, pero cada video mostrando malas

prácticas policiales incrementa la desconfianza entre la ciudadanía y se pierde legitimidad sobre la seriedad de las reformas y de las soluciones organizacionales.

Paso 6. Instaurar un sistema eficiente y participativo de manejo de crisis

El trabajo de las organizaciones y agentes de seguridad está expuesto con frecuencia a situaciones de crisis que ponen a prueba las relaciones de confianza y generan interacciones que nutren la desconfianza. Los diseños institucionales no han cubierto plenamente esa situación. Los casos reportados de abuso o violación de derechos contribuyen a retroalimentar la desconfianza entre la ciudadanía y a limitar el desempeño que se puede alcanzar en el marco institucional y organizacional existente. Por ello es necesario establecer un sistema expedito de atención y manejo de crisis y conflictos ciudadanía-cuerpos de seguridad que, entre otros objetivos, permita reducir sustancialmente los costos de transacción en los que incurre la ciudadanía y las victimas que resulten de eventos críticos. La aprobación de la Ley General de Víctimas en 2013 es un buen paso en ese sentido, pero de acuerdo con Flores (2014) quedan dudas sobre la transparencia de las burocracias creadas por dicha ley, la capacidad presupuestal para reparar daños y la pertinencia misma de las ponderaciones de los derechos de las víctimas para lograr una reparación del daño.

Conclusiones

El objetivo de crear confianza Estado-policías-comunidad en un país en transición como México, demanda mejores arreglos institucionales para generar incentivos a la cooperación y hacer posibles procesos locales de construcción de confianza. La interdependencia de las esferas de relaciones de confianza, influye en los avances que se pueden alcanzar en cada una de ellas. Para incrementar la legitimidad social de la protección policial y mejorar el desempeño en las labores policiales es necesario incrementar la confianza de los agentes de policía en sus relaciones laborales con los distintos órdenes de gobierno.

Concentrar el mando policial y crear soluciones organizacionales centralizadas son acciones coherentes con la estrategia de soberanía graduada, pero no responde a necesidades sociales de protección que podrían atenderse mejor con soluciones policéntricas y en protocolos de actuación consensuados socialmente, certidumbre laboral, seguridad física y jurídica de todos los agentes y mayor cooperación policías-ciudadanos. Las preferencias de los ciudadanos siguen siendo importantes en la procuración de sistemas eficientes y confiables de seguridad. Sin ser socialmente óptima, la proliferación de empresas privadas de seguridad demuestra que los ciudadanos prefieren un control cercano sobre quién los protege y decidir sobre las condiciones de trabajo de quién los protege. Esa preferencia choca con el discurso geopolítico que ha dominado el diseño de reformas policiales en el periodo de transición a la democracia y la globalización de la economía mexicana. Las reformas emprendidas en los últimos años tienen fallas de diseño y de implementación. Es importante reconocer lo anterior para dirigir la búsqueda hacia diseños institucionales alternativos que puedan crear relaciones de confianza en las tres esferas de interacción Estado-policías-ciudadanos y en los espacios locales donde ocurren las situaciones de inseguridad.

Bibliografía

Aguirre Sala, Jorge Francisco. 2016. "La prevención comunitaria del delito a través de la gobernanza local". *OBETS. Revista de Ciencias Sociales* 11 (2): 383-418.

Alvarado, Arturo, y Jorge Zaverucha. 2010. "La actuación de las fuerzas armadas en la seguridad pública en México y Brasil, una visión comparada". En *Los grandes problemas de México, XV seguridad nacional y seguridad interior*, coordinado por Arturo Alvarado y Mónica Serrano, 227-268. México: El Colegio de México.

Alvarado, Arturo. 2008. "El Acceso a la justicia en una sociedad en transición". En *La reforma de la justicia en México*, editado por Arturo Alvarado, 31-94. México: El Colegio de México.

Ángel, Arturo. 2016. "Mando único cumple 6 años sin aprobarse; mil 200 municipios siguen sin policías", 15 de junio de 2017, http://bit.ly/1sGjmwG.

Arendt, Hannah. 1976. *The Origins of Totalitarianism*. Orlando: Harcourt, Inc.

Banks, Richard. 2014. "Dialogues: Trust in Design". En *Trust, Computing and Society*, editado por Richard H. R. Harper, 250-271. Cambridge: Cambridge University Press.

Barrachina, Carlos, y Juan Ignacio Hernández. 2012. "Reformas del sistema nacional de seguridad en México (2006-2011)". *URVIO, Revista Latinoamericana de Seguridad Ciudadana* 11: 79-92.

Bergman, Marcelo, y Hernán Flom. 2012. "Determinantes de la confianza en la policía: una comparación entre Argentina y México". *Revista Perfiles Latinoamericanos* 20 (40): 97-122.

Campoy-Torrente, Pedro, Ariel Chelini, y Carles Soto-Urpina. 2016. "Evaluación de la policía de proximidad en la ciudad de Santa Fé". *URVIO, Revista Latinoamericana de Seguridad Ciudadana* 19: 70-89.

Candina, Azun. 2006. *Comunidad y Seguridad: una guía para la prevención a nivel local*. Santiago de Chile: Centro de Estudios en Seguridad Ciudadana, Instituto de Asuntos Públicos, Universidad de Chile. https://www.cesc.uchile.cl/publicaciones/mc_02_comyseg.pdf.

Cantú, Edwin. 2014. "La cultura organizacional y el modelo de policía en México". *Ciencia UANL* 17 (67): 21-25. http://cienciauanl.uanl.mx/?p=1677.

Carrión, Fernando M. 2007. "Reforma policial: ¿Realidad ineludible de una nueva doctrina de seguridad?". *URVIO, Revista Latinoamericana de Estudios de Seguridad Ciudadana* 2: 5-22.

Causa en común. 2015. "Informe ejecutivo de resultados Encuesta ¿Qué piensa la policía? 2015", acceso el 13 de mayo de 2017, http://bit.ly/2jttgBb.

Chien, Shu-Hua y Jyh-Jeng Wu. 2006. "The Influence of Intra-organizational Trust and Interaction on Marketing Capability and Performance". *Asia Pacific Management Review* 11 (2): 123-132.

CIDAC. 2016. "La democratización de la desconfianza", acceso el 13 de mayo de 2017, http:bit.ly/277IBrM.

Costa, Gino, y R. Neild. 2007. "La reforma policial en Perú". *URVIO, Revista Latinoamericana de Seguridad Ciudadana* 2: 112-126.

Dammert, Lucía y Alejandra Lunecke. 2004. *La prevención del delito en Chile. Una visión desde la comunidad*. Santiago de Chile: Centro de Estudios en Seguridad Ciudadana. Instituto de Estudios Públicos, Universidad de Chile. http://bit.ly/2o17XFd.

Dammert, Lucía. 2005. "Reforma policial en América Latina". *Quórum Revista de Pensamiento Iberoamericano* 12: 53-64.

Felix Azogu, Adigwe. 2013. "Democratic Transition and Crime in Nigeria". *IOSR Journal of Humanities and Social Science* 14 (2): 62-71.

Flores Ramos, Alejandra. 2014. "Análisis de la Ley General de Víctimas, en cuanto a la reparación del daño por violaciones a los derechos humanos" (Tesis de maestría, FLACSO México).

Goldsmith, Andrew. 2005. "Police Reform and the Problem of Trust". *Theoretical Criminology* 9 (4): 443–470.

Hayden, Patrick. 2009. "From Exclusion to Containment: Arendt, Sovereign Power, and Statelessness". *Societies Without Borders* 3 (2): 248-269.

Hernández, F. Francisco, y Darío G. Zepeda, G. 2015. "El plan estatal de prevención social de la violencia y la delincuencia para el estado de Aguascalientes: la participación ciudadana, la función policial preventiva y la confianza institucional". *Archivos de Criminología, Seguridad Privada y Criminalística* 3 (V), agosto-diciembre.

Instituto Nacional de Estadística y Geografía (INEGI). 2016. Boletín de Prensa Núm. 151/2016. 6 de abril de 2016. http://bit.ly/1RM23zX.

Jackson, Brian A. 2015. "Respect and Legitimacy —A Two-Way Street Strengthening Trust Between Police and the Public in an Era of Increasing Transparency". *Perspective, Expert Insights on a Timely Policy Issue*. Santa Monica, CA: Rand Corporation. http://bit.ly/2dt5Om1.

Meyer, Maureen. 2014. "Mexico´s Police: Many Reforms, Little Progress". WOLA, Washington Office on Latin America. http://bit.ly/2opsHtx.

Olivares Ferreto, Edith. 2010. *Análisis político: condiciones sociolaborales de los cuerpos policiales y seguridad pública.* México: Friedrich Ebert Stiftung. http://bit.ly/2opnQc0.

Ong, Aihwa. 2000. "Graduated Sovereignty in South-East Asia". *Theory Culture and Society* 17 (4): 55-75.

Osorio, Chong. 2016. "Creación del mando único policial permitirá contar con instituciones fuertes: Osorio Chong", acceso el 27 de julio de 2016, http://bit.ly/2dvHjoe.

Ostrom, Elinor, Roger. B. Parks y Gordon P. Whitaker. 1978. *Patterns of Metropolitan Policing*. Cambridge: Balinger Publishing Co.

Oviedo, Enrique. 2007. "Modernización policial: el caso de los carabineros de Chile". *URVIO, Revista Latinoamericana de Seguridad Ciudadana* 2: 71-84.

Ozimek, Adam. 2014. "Making the police less powerful", acceso el 28 de noviembre de 2014, http://bit.ly/2ajW6QE.

Pacheco, Angélica, y Basilio Verduzco. 2015. "Prácticas socioespaciales y análisis situacional del delito". En *Cada quien su imperio: preferencias institucionales y patrones territoriales de inseguridad,* coordinado por Basilio Verduzco Chávez, 160-186. Guadalajara, Jalisco: Universidad de Guadalajara.

Perekh, Serena. 2008. *Hannah Arendt and the Challenge of Modernity: A Phenomenology of Human Rights*. Nueva York: Routledge.

Pérez-Ducy, Ellen. 2013. Coproducción de la paz social: la elevación de las penas para adolescentes vistas según las teorías de Elinor Ostrom. *Revista Ciencia y Sociedad* 38 (2): 195-214.

Piñeiro, Arturo. 2016. "El dilema del mando único", acceso el 13 de Junio de 2016, http://bit.ly/2o11xWM.

Ralston, Ekaterina S. 2006. "Structure of Organizational Trust in Military-Type and Civilian Organizations: Validation of the Organizational Trust Questionnaire". *Retrospective Theses and Dissertations*. Paper 1873. http://lib.dr.iastate.edu/rtd/1873/.

Ratton, José Luiz, y Eduardo de Alencar. 2009. "Construyendo un programa de investigación sobre grupos de exterminio: desconfianza, mercados de protección privada y organizaciones criminales en Brasil". *URVIO, Revista Latinoamericana de Seguridad Ciudadana* 8: 88-97.

Riegelsberger, Jens, Angela Sasse y John. D. McCarthy. 2004. "Depending on the Kindness of Strangers? Trust Relationships in Ambient Societies". Trabajo presentado en *CHI 2004 Workshop on Trust in Ambient Societies*, Vienna, Austria, 26 de abril. http://bit.ly/2dbxAS4.

Rivera, Marien. 2012. "Sistema de justicia: la asignatura pendiente". En *Repensar México, un enfoque multidisciplinario*, coordinado por Blanca Alcalá Ruiz, 233-250. San Andrés Cholula: Iexxe Editorial.

Rodríguez, F. Octavio. 2012. "La Policía Federal y el Nuevo Modelo de Policía: análisis legislativo y consideraciones generales". En *Policía Federal: una nueva institución para México*, coordinado por David Arellano y Juan Salgado, 11-34. México: SSP-CIES. http://bit.ly/1SYsrZH.

Sánchez Orozco, Víctor Manuel. 2015. "Las racionalidades de los actores públicos en torno al mando único policial". En *Cada quien su imperio: preferencias institucionales y patrones territoriales de inseguridad*, coordinado por Basilio Verduzco Chávez, 105-141. Guadalajara, Jalisco: Universidad de Guadalajara.

Savelsberg, Joachim J. y Suzy. McElrath. 2014. "Crime, Law, and Regime Change". *Annual Review of Law and Social Science* 10 (1): 259-279.

Schneider, Anne L. y Helen Ingram. 1997. *Policy Design for Democracy*. Lawrence: University of Kansas Press.

SESNSP (Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública). 2016. "Tasas por cada 100 mil habitantes 1997-2016", acceso el 27 de julio de 2016, http://bit.ly/29RV7UE.

Shaw, Mark. 1995. "Towards Safer Cities?: Crime, Political Transition and Chancing Forms of Policing Control in South Africa". *African Security Review* 4 (5): 4-11.

Solís Moreira, Julio. 2016. "Incidencia de la seguridad comunitaria en el capital social de barrios urbanos en San José, Costa Rica". *URVIO, Revista Latinoamericana de Estudios de Seguridad* 19: 90-110.

Tyler, Tom R. y Jeffrey Fagan. 2008. Legitimacy and Cooperation, Why Do People Help the Police Fight Crime in Their Communities? *Ohio State Journal of Criminal Law* 6: 231-275. http://bit.ly/2oM1aE7

U.S. Department of Justice. 2007. *Building Trust Between the Police and the Citizens They Serve*. Washington: DOJ, Office of Community Oriented Policing Services. http://www.theiacp.org/portals/0/pdfs/buildingtrust.pdf.

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2748

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 145-165
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Evaluación de las instituciones del sistema de justicia penal de la República de Panamá desde un enfoque de seguridad ciudadana (2004-2014)

Evaluation of the Institutions of the Criminal Justice System of the Republic of Panama from the perspective of Citizen Security (2004-2014)

Roberto Rodríguez-Rodríguez[1]

Fecha de recepción: 13 de marzo de 2017
Fecha de aceptación: 26 de abril de 2017

Resumen

En este artículo se expone una parte de los resultados de la investigación sobre la Evaluación de la Seguridad Ciudadana en la República de Panamá durante los periodos de gobierno 2004-2009 y 2009-2014. Se presentan, concretamente, los resultados de la evaluación de las Instituciones del Sistema de Justicia Penal estudiadas: Policía Nacional, Ministerio Público, Órgano Judicial y Sistema Penitenciario; además de los resultados de los aspectos organizacionales considerados para esta evaluación institucional: Presupuestos, Recursos Humanos, Modernización, Transparencia y Rendición de Cuentas, y Atención Ciudadana. Se identifican y evalúan las características, diferencias y similitudes en el desarrollo de las Instituciones del Sistema de Justicia Penal y las distintas acciones de gobierno que inciden en su funcionamiento, a través de un Modelo de Evaluación de la Seguridad Ciudadana en el marco de la política general de seguridad de cada gobierno.

Palabras clave: entidades del Sistema de Justicia Penal; seguridad ciudadana; evaluación; modelo de evaluación; funcionamiento; periodo de gobierno; valoración; aspectos institucionales.

Abstract

This article presents the results of the evaluation research of the Citizen Security in the Republic of Panama during the Government periods 2004-2009 and 2009-2014. In particular, the results of the evaluation of the institutions of the criminal justice system: Police, Prosecutors, Judiciary and Prison System; and the results of the evaluation of the organizational aspects considered for this institutional evaluation: budgets, human resources, modernization, transparency and accountability, and citizen attention. The characteristics, differences and similarities in the development of the institutions of the criminal justice system and the different actions of the Governments that affect its operation are identified and evaluated through a model of evaluation of Citizen Security within the framework of the general security policy of each Government.

Keywords: Institutions of the Criminal Justice System; Citizen Security; evaluation; evaluation model; operation; period of Government; valuation; institutional aspects.

1 Licenciado en Relaciones Internacionales por la Universidad de Panamá. Máster en Gobierno y Administración Pública por la Universidad Complutense de Madrid y candidato a Doctor por el Instituto Universitario de Investigación Ortega y Gasset y la Universidad Complutense. Investigador del Programa Nacional de Excelencia de la Secretaría Nacional de Ciencia y Tecnología de Panamá (SENACYT). Correo: robrod01@ucm.es

Introducción: El resurgimiento de la importancia de las instituciones

El Estado, como instancia político-social, ha sido uno de los objetos de estudio dentro de las ciencias sociales y políticas más estudiados a lo largo de la historia. La carrera por su comprensión se remonta tradicionalmente a los escritos de Maquiavelo en el siglo XVI, y a otros autores que a partir de esa época se ocupan de examinarlo. Durante el siglo XX se realizan importantes estudios que abordan la temática estatal desde distintas ramas de la ciencia.[2] Pero el interés científico por el Estado también entra durante este siglo en una fase de receso, que es superada a partir de su segunda mitad, principalmente en la década de los ochenta, como consecuencia del esfuerzo colectivo de las distintas ciencias sociales que retoman la mirada hacia el Estado, ya sea como agente regulador, generador de fallas del sistema, asignador y defensor de derechos, agente estabilizador del sistema, distribuidor y activador del desarrollo económico o como generador de clases, etc. (Valencia Agudelo 2011).

A la par de esto, tiene lugar el surgimiento de nuevas teorías[3] y debates en torno al desarrollo económico-social y el impacto que las instituciones públicas y democráticas pudieran tener en el desenlace de ese desarrollo (Alonso 2005; Barreda 2006; Alonso y Garcimartín 2010). Teorías y visiones que, desde una perspectiva económica, insisten en la relevancia que los marcos normativos y las instituciones tienen en la promoción del progreso, al definir una especie de código de instrucciones para la sociedad, condicionando "la habilidad que una sociedad tiene para poner en pleno uso sus factores productivos y someterlos a una más intensa dinámica de acumulación y mejora" (Alonso y Garcimartín 2010). Estas perspectivas de estudio se encuadran dentro de la corriente de pensamiento del Neoinstitucionalismo, que enfatiza la importancia de las instituciones y de la democracia en el desarrollo y la trayectoria de progreso de los países (Barreda 2006; Rivas Leone 2003; Ayala y González 2001).

A partir de la exposición de estos debates y enfoques teóricos economicistas que el Estado y sus dinámicas se vuelven importantes para la comprensión de los problemas de desarrollo, ocurre lo que según García Fernández (2004) abre paso a la idea de que la pobreza y el subdesarrollo, enlazadas a la ausencia de democracia, no se podían superar sin una transformación de las instituciones políticas que asegurasen una gestión pública más participativa y eficaz, emergiendo con esto la noción de gobernabilidad como paradigma de buenas prácticas en la gestión de los asuntos públicos. Por otra parte, Ruiz López y Cuellar Martín (2013), identifican una serie de transformaciones[4] a escala internacional que han venido cambiando la forma y el quehacer de los gobiernos y las administraciones públicas, así como todos los procesos y actividades que las conforman, quedando sometidas a una serie de reformas y procesos de modernización que comienzan en los paí-

2 Según Beobide y Gordillo (2012), la complejidad del Estado y sus diferentes formas de concebirlo explican que haya sido objeto de estudio por parte de diversas ciencias: la Ciencia Política, el Derecho, la Historia, la Ciencia del Gobierno, la Filosofía y la Sociología.

3 Barreda (2006) sostiene que a partir de la Segunda Guerra Mundial se comienza a tomar conciencia de la relación entre los conceptos de democracia y desarrollo gracias a las aportaciones de la teoría de la modernización.

4 Fenómenos o nuevos paradigmas como la globalización, la revolución tecnológica, el cambio de una sociedad industrial a una sociedad del conocimiento.

ses de la Organización para la Cooperación y el Desarrollo Económico (OCDE); pero que se han ido extendiendo en las últimas décadas a Latinoamérica, bajo el influjo del paradigma de la Nueva Gestión Pública en el que la gestión de la calidad, la eficacia y la eficiencia representan estrategias y principios que marcan la orientación de la administración pública contemporánea.

Es así que, dentro de este proceso de reforma y modernización, se vienen realizando cambios en áreas y aspectos específicos de la organización y el funcionamiento de las administraciones públicas que van desde la evaluación de políticas públicas; "la descentralización política-administrativa; las nuevas relaciones de la Administración con el ciudadano; la rendición de cuentas; el combate a la corrupción, la ética en el servicio público; el control y la evaluación de la Administración Pública; las nuevas modalidades para la prestación de servicios públicos; las nuevas tecnologías para la Administración Pública; el fortalecimiento de los gobiernos locales"; hasta la profesionalización de la administraciones públicas; etc. (Ruiz López y Cuellar Martín 2013), con lo que tales transformaciones y reformas se enmarcan dentro del proceso de interés por la mejora del funcionamiento del Estado y sus instituciones públicas.

Enfoques institucionales en los estudios de justicia y seguridad ciudadana

La seguridad ciudadana, como problema complejo, representa una temática de proporciones amplias, ya sea por los diversos factores que intervienen en su dinámica y composición. Además, por la diversidad de actores y sujetos que intervienen en su dinámica, por los diferentes enfoques de solución y mejora del problema y la dificultad que representa su articulación o por la diversidad de impactos que produce en diferentes áreas de la sociedad. Según Ramos García y Flores (2013, 34) los estudios, propuestas e intervenciones que se vienen realizando acerca de la problemática se caracterizan por la diversidad de enfoques de análisis en su abordaje. Este planteamiento es respaldado también por Fuentes Saavedra (2011), para quien la producción académica asociada al tema de la seguridad ciudadana se ha venido desarrollando en tres grandes líneas: el análisis de las instituciones públicas de seguridad, los factores de la violencia, y la vinculación entre percepciones sociales y política de seguridad.

El estudio de la seguridad ciudadana desde la perspectiva de las instituciones del sistema de justicia penal que integra organismos públicos como la Policía, el Ministerio Público, las Cárceles y los Tribunales, etc., ha experimentado un desarrollo significativo en la última década. Prieto (2003, 129) señala que los estudios y evaluaciones institucionales que se vienen realizando a los sistemas de justicia a nivel latinoamericano comprenden áreas que presentan debilidades tradicionales como "la lentitud de los procesos, dificultades de acceso a la justicia y excesiva litigiosidad, ineficiencia e ineficacia de las organizaciones judiciales, baja productividad y despilfarro, deficiencias de calidad, falta de eficacia en la ejecución de las sentencias, elevados costes privados y sociales, etc.". Por tanto, se entiende que tales investigaciones se enfoquen en temas como la reforma de las instituciones policiales, judiciales y los sistemas carcelarios desde las distintas dimensiones que los componen (normativa,

estructural-organizacional, estratégica, comunicacional, política, etc.).

En este sentido, a nivel de América Latina, se han realizado diferentes estudios que abordan el funcionamiento de las entidades del Sistema de Justicia Penal y sus distintas problemáticas. De esta forma, se han realizado estudios sobre la reforma de los sistemas policiales y el proceso democratizador en Latinoamérica (Fruhling 2005; Tudela 2007; Dammert 2007; Ruiz 2004; Baracaldo 2004). Igualmente, se han estudiado los procesos de reforma de los sistemas de justicia, policía, carcelario y de los métodos procesales (Vanderschueren *et. al*. 2004; Baytelman y Duce 2003; Duce y Pérez Perdomo 2005). Unas investigaciones han estudiado el impacto y el desempeño de la Policía (BID 2013; Zepeda Lecuona 2010), mientras que otras se han enfocado, por ejemplo, en estudiar el gasto en justicia, la eficacia y eficiencia en el funcionamiento de la administración de justicia (Alas de Franco 2016, 42; Zepeda Lecuona 2005; Pásara 2011; Pastor Prieto 2003). También se ha incursionado en temáticas que plantean metodologías de análisis que buscan determinar la eficacia, la eficiencia, la percepción y la calidad de estos sistemas a través de diagnósticos, evaluaciones y casos de estudio que analizan el funcionamiento de las instituciones de justicia (Zepeda Lecuona 2005; Basabé Serrano 2013; Rivera et. al. 2010; Pastor y Maspóns 2004; Rebuffi 2012; García España 2013; Ramos Rollón 2005; Ortega 2014); además de otras investigaciones que han hecho contribuciones en el campo de la evaluación de los sistemas penitenciarios (Zepeda Lecuona 2013; Coca Muñoz 2007; BID 2013; UNODC 2010).

En Panamá, algunos estudios e iniciativas ciudadanas, principalmente provenientes de organizaciones no gubernamentales han abordado los problemas de la justicia panameña a través de ejercicios de evaluación de la corrupción judicial (Fundación para el Debido Proceso 2007); la evaluación de la implementación del Sistema Penal Acusatorio (UNODC-CEJA 2015); así como estudios que analizan la situación del Poder Judicial en Panamá a través de componentes como la autonomía de los jueces, la independencia judicial, el desempeño judicial, la transparencia y rendición de cuentas, el acceso a la justicia, el compliance o Poder (ejecución de sentencia) (Castillo *et. al*. 2001). Otras iniciativas de evaluación de la justicia, provienen a través de técnicas como la auditoria social, encuestas de opinión, veedurías ciudadanas que buscan detectar los principales fallos y problemas de la administración de justicia, y estudios para el mejoramiento en la gestión gerencial de Despachos Judiciales (Benavides y Rodríguez 2006).

El funcionamiento de las organizaciones de justicia-penal y sus diferentes componentes estructurales se vienen estudiando como parte de los procesos de reforma y mejora de las administraciones públicas, fundamentalmente, con la incorporación de las reformas de segunda generación implementadas en los países de América Latina a partir de los noventa. Estas reformas están enfocadas en aspectos como la racionalidad funcional y organizativa del Estado, el fortalecimiento del aparato estatal para hacer más eficiente y transparente su desempeño. Además, centradas en las estructuras organizativas, en los recursos humanos y financieros buscando una mejor gobernabilidad a través del fortalecimiento institucional (Ramírez Brouchoud 2009), ya que "el aumento de su capacidad a través del desarrollo institucional es una de las herramientas para asegurar el éxito de los procesos de moderni-

zación del Estado en la región, como parte de la agenda más amplia que busca crear las condiciones para el fortalecimiento y profundización de una democracia que genere desarrollo sostenible" (Mejía Lira 2005).

Esto representó para el Estado "hacerse responsable de asuntos tales como la prevención de la criminalidad y la delincuencia, el mejoramiento de las prisiones, la provisión de una justicia penal fiable, implicando un desarrollo institucional y un fortalecimiento de capacidades estatales" (Ramírez Brouchoud 2009). Es así que, como parte de este proceso de mejora de las administraciones públicas latinoamericanas, se han venido desarrollando actuaciones de gobierno cuyas prácticas y resultados han generado análisis e investigaciones que se abordan desde las diferentes "dimensiones fundamentales de las organizaciones públicas" (Ramió 1999), analizándose los aspectos, características y problemas relacionados con las estructuras administrativas, los recursos humanos, los recursos tecnológicos, financieros y materiales, los procesos administrativos, etc.

En este sentido, algunos estudios han profundizado los temas de gestión y desarrollo de los recursos humanos en las organizaciones públicas (Salvador Serna 2003; Pliscoff 2008; Pocoví 2009; Briones Gamarra 2006); otros han tratado los aspectos comunicacionales y de información de las organizaciones desde las premisas de la transparencia y la rendición de cuentas (Ochoa y Montes de Oca 2004; Conejero Paz 2014; Moreira Corrêa y Claussen Spinelli 2011; Naessens 2010; Perramon 2013; Cerrillo i Martínez 2011; García Hernández 2011). Igualmente, las cuestiones presupuestales han sido ampliamente estudiadas (Barea Tejeiro *et. al*. 2014; Martínez Álvarez y García Martos 2013; Granados *et. al.* 2009; Gutiérrez Lara 2015; Manning 2008; Marcel 2008), mientras que otras investigaciones han abordado el aspecto de la atención hacia los ciudadanos desde el enfoque de la calidad de los servicios públicos y la satisfacción de los ciudadanos (Méndez Juez 2014; Sancho Royo 2007; Vicher-García 2012; Blanco Dopico *et. al.* 2006; Moyado Estrada 2002; Ruiz López y Cuellar Martín 2013). También destacan aquellos estudios que abordan los aspectos clave en los procesos de modernización de las administraciones públicas, principalmente los relacionados con la incorporación de recursos tecnológicos (TIC) y la implantación del e-Gobierno y la mejora de los procesos de gestión (Rodríguez-Arana 2001; Gil Gómez et. al. 2010; Criado y Gil García 2013; Ramió Matas 2012; De la Nuez et. al. 2015; Ballestero Díaz y Font Jaume 2004, Lillo L. 2010; Contini y Velicogna 2010).

Consideraciones metodológicas

La investigación consiste en evaluar la seguridad ciudadana de la República de Panamá en los periodos de gobierno 2004-2009 y 2009-2014 a través de un Modelo que adopta un enfoque institucional cualitativo acotado de la seguridad ciudadana que se circunscribe al análisis y evaluación de tres dimensiones específicas de la seguridad y de la política general gubernamental en esta materia, y en la que se consideran entidades, aspectos e instrumentos de control, administración, sanción y prevención de la violencia y la criminalidad. Las dimensiones consideradas para este estudio son las siguientes: dimensión de las Instituciones del Sistema de Justicia Penal, dimensión Regulativa de la Seguridad Pública, y la dimensión

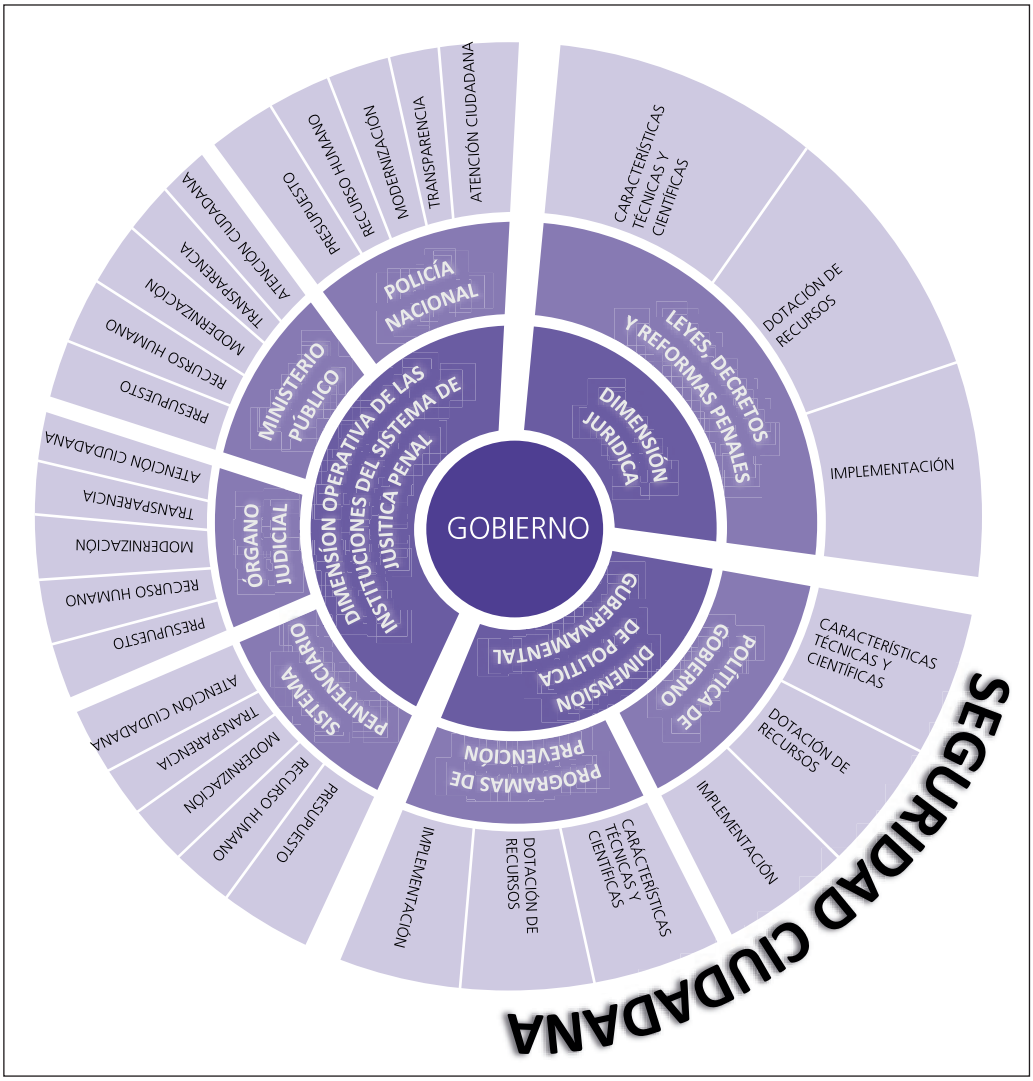
de las Estrategias de Política Gubernamental y de Programas Preventivos. En este artículo, describiremos y presentaremos los resultados de la evaluación de la primera dimensión del modelo de análisis planteado.

En este sentido, las evaluaciones y sus distintas tipologías son herramientas de gestión pública poco empleadas y desarrolladas en la administración pública panameña, por lo que las instancias públicas en general carecen de una cultura evaluativa sistemática que permita dar un seguimiento al funcionamiento, los procesos, las respuestas, los resultados e impactos de la actuación de los distintos poderes del Estado y sus dependencias. Junto a estas carencias evaluativas, se aprecia igualmente un desarrollo insuficiente y débil de la transparencia y rendición de cuentas que se observa, para el caso que nos interesa, en la escasa, incontinua y baja calidad de la información y datos de gestión y funcionamiento con que cuentan las diferentes entidades y aspectos considerados en esta investigación.

Este punto nos lleva precisamente a buscar metodologías de estudio que nos ayuden a complementar esta carencia de datos objetivos y cuantitativos en las diferentes áreas e instituciones que conforman la seguridad y la justicia panameña, por lo que la investigación y la metodología, así como los instrumentos y técnicas que la sustentan, pretenden incorporar herramientas de apoyo metodológico que refuercen y complementen estos vacíos de información. Por lo anterior, la evaluación se basa en la interpretación de la información cualitativa recogida en las entrevistas realizadas, pero que también toma en cuenta la revisión y el análisis documental y estadístico disponible y la contrastación de la información de estos instrumentos y fuentes. En este sentido, el núcleo de la investigación se refiere a la evaluación del funcionamiento de las dimensiones institucionales que hemos considerado como un conglomerado de áreas afines a la seguridad ciudadana, que como ya hemos mencionado están integrada por las instituciones del Sistema de Justicia Penal, el marco legislativo penal aprobado en cada periodo, y las estrategias y políticas preventivas de gobierno. Las tres dimensiones se descomponen en las entidades y aspectos (que representan las variables) que hemos considerado para la evaluación general de la seguridad y de la política tal como se muestra en el diagrama, tal como muestra la figura 1.

De esta forma, para determinar cómo fue el funcionamiento de las dimensiones y aspectos institucionales se optó por un diseño metodológico evaluativo que pudiera, en primer lugar, extraer información acerca del nivel de funcionamiento y nivel de desarrollo de las variables consideradas en base a la experiencia y conocimiento de un grupo de expertos entrevistados, estableciéndose de forma cualitativa valoraciones y juicios en escala; y en segundo lugar, transformando estas valoraciones a cuantitativas, para a través de un modelo obtener una evaluación cualitativa y cuantitativa de la seguridad ciudadana desde la perspectiva de los expertos sobre el funcionamiento y desarrollo de las dimensiones institucionales de la seguridad panameña. En el campo de la Ciencia Política a nivel de Latinoamérica y España se han venido haciendo algunos estudios con enfoque de evaluación apoyadas en metodologías basadas en encuestas de opinión o en cuestionarios y entrevistas realizadas específicamente a un conjunto de expertos informados (Mendoza, Prieto y Barreto 2012; Cabero y Llorente 2013; Escobar y Cuervo 2008; Escobar 2011; Ahumada, Farren y Williamson 2008).

Figura 1. Esquema conceptual de evaluación de la seguridad ciudadana



El fin de estas es evaluar distintas características y aspectos de alguna dimensión del gobierno o de los sistemas políticos aprovechando el conocimiento de las fuentes en la materia. En este sentido, para Cabero y Llorente (2013) "la evaluación mediante el juicio de experto consiste en solicitar a una serie de personas la demanda de un juicio hacia un objeto, un instrumento, o su opinión respecto a un aspecto concreto". Igualmente, para Escobar y Cuervo (2008) "el juicio de experto se define como una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones".

Evaluación de la dimensión: Instituciones del Sistema de Justicia Penal de la República de Panamá

Esta dimensión está integrada por cuatro entidades del Sistema de Justicia Penal[5], tal como muestra la figura 2: la Policía Nacional, el Ministerio Público, el Órgano Judicial y el Sistema Penitenciario. A su vez, estas entidades se descomponen en un conjunto de aspectos institucionales: Asignación Presupuestaria, Recursos Humanos, Modernización, Transparencia y Rendición de Cuentas, y Atención ciudadana, que van a caracterizar de forma general el funcionamiento y nivel de desarrollo de cada entidad y cuyas valoraciones representan los indicadores que determinan la evaluación de las mismas.

La evaluación general utiliza la valoración e información cualitativa y cuantitativa que proporcionan los expertos en una entrevista con cuestionario, acerca de los cinco aspectos institucionales y de las cuatro entidades del Sistema de Justicia Penal que son consultados. En términos prácticos, representan evaluaciones individuales de los aspectos y entidades que serán luego articuladas para establecer valoraciones definitivas por aspecto, entidad y periodo. La entrevista se basó en la aplicación de un cuestionario para medir la valoración de los expertos sobre varios componentes e indicadores del funcionamiento de las instituciones del Sistema de Justicia Penal, que combina preguntas estructuradas, en su mayor parte, y no estructuradas. Las preguntas estructuradas fueron de tipo cerrada-múltiples en las que el entrevistado debía escoger una sola respuesta (cerrada) entre varias opciones (múltiples) en escala de categorías.

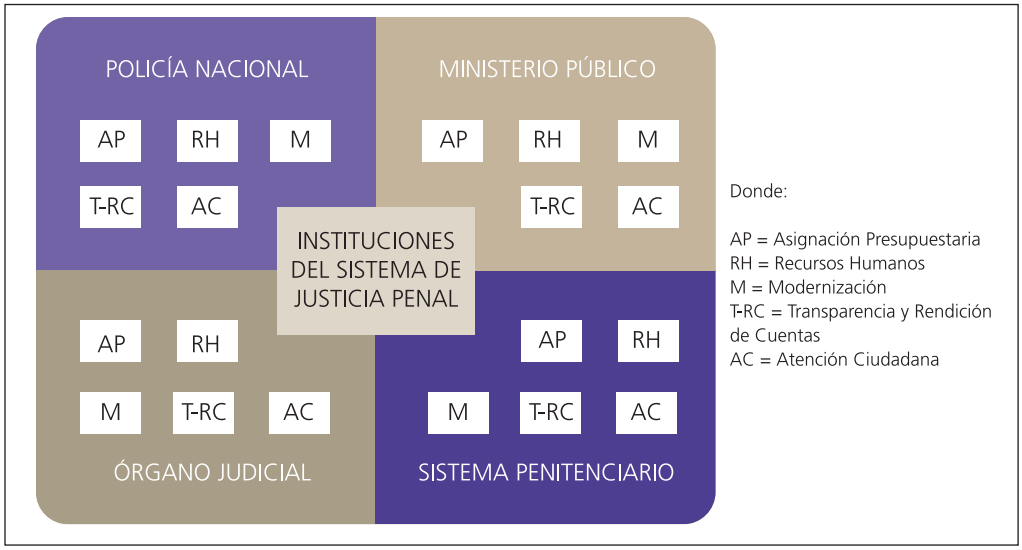
5 Según UNODC (2010), los principales componentes del Sistema de Justicia Penal lo conforman instituciones como la Policía, el Ministerio Público, los Tribunales y las Cárceles.

El muestreo se hizo de forma intencional. Se seleccionaron sujetos e informantes clave, con conocimiento y experiencia profesional y académica en materia de seguridad pública y temas afines. Por tanto, se escogieron personas con perfil de expertos o conocedores profesionales en materia de seguridad ciudadana, justicia, políticas públicas, asuntos policiales y criminológicos en la República de Panamá, aplicando un procedimiento de revisión y clasificación de distintos perfiles y líneas de investigación, así como en el área de gestión y administración de los sujetos, optando por aquellos expertos que en materia de investigación mantuvieran líneas especializadas en el funcionamiento de las instituciones de justicia penal, y por la calidad y cantidad de sus publicaciones. Mientras, los profesionales del sector fueron escogidos por la importancia de las posiciones que ocuparon o dirigieron, y su pertenencia y antigüedad en algunas de las entidades estudiadas. La muestra final fue de 16 sujetos, pero en la práctica pudo aplicarse a 12 expertos en total.

Procedimientos y pasos de la evaluación

A continuación, se describe la metodología y los pasos para determinar la evaluación de las cuatro entidades tal como se aprecia en la figura 3. En este sentido, se ha considerado utilizar cinco aspectos fundamentales de la organización, administración y funcionamiento de las organizaciones públicas: la asignación presupuestaria, los recursos humanos, la modernización, la transparencia y la rendición de cuentas, y la atención ciudadana (Figura 2). Estos componentes, a través de sus características, atributos, debilidades y fortalezas refle-

Figura 2. Esquema conceptual de las instituciones y los aspectos de análisis del modelo de evaluación.



jadas en la valoración experta, nos proporcionan una indicación de su grado de desarrollo particular, e igualmente en conjunto, del grado de desarrollo de la entidad.

Previo a la aplicación del cuestionario, se establecen y discuten entre el entrevistador y el entrevistado los criterios de valoración y las características, cualidades y rasgos principales de cada aspecto institucional por periodo de gobierno. Luego de este procedimiento, los expertos dieron cada uno su valoración concluyente para cada aspecto por entidad empleando la escala de categorías: Muy bueno, bueno, regular, malo, muy malo. Adicionalmente, para obtener una medida jerárquica de la importancia que puede tener cada uno de los cinco aspectos institucionales para el funcionamiento adecuado y eficaz de una entidad del Sistema de Justicia Penal frente al problema de inseguridad, y establecer qué entidades pudieran estar mejor dotadas de recursos, capacidades y desarrolladas para actuar de forma más eficaz ante la demanda del problema de inseguridad, se les pidió a los expertos que dieran a cada aspecto, en una escala de 1 a 10 (donde uno es mínima importancia y 10 es máxima importancia) su nivel de importancia y de influencia en el funcionamiento adecuado de cada entidad, cuyo resultado determina el peso que tiene cada aspecto en el funcionamiento adecuado de cada entidad.

En este sentido, el peso institucional viene a ser el porcentaje de importancia que tiene un determinado aspecto con relación a los demás dentro del adecuado funcionamiento de una entidad del Sistema de Justicia Penal. Igualmente, y como paso previo, la validez del instrumento (entrevista y cuestionario) se determinó mediante el procedimiento de juicio de expertos, aplicando una primera versión del cuestionario a un grupo de especialistas diferentes, a los expertos que respondieron el cuestionario final, pero cumpliendo los crite-

Figura 3. Modelo y pasos de la evaluación de las instituciones del Sistema de Justicia Penal

rios de selección. Por ejemplo, se les pidió que valoraran la comprensión y redacción de cada uno de los ítems (pertinencia del tiempo que toma la aplicación del cuestionario, sencillez y claridad de las preguntas, orden y secuencia, cantidad de preguntas, formato y calidad de la presentación del cuestionario, etc.) en una escala de 1 a 10, donde una valoración inferior a 8 representó que se debían modificar las preguntas, y una valoración igual o superior a 8 significó que eran aceptados (Manzano 2011). A continuación, se describen los pasos indicados en la figura 3.

Paso 1. Aplicación del Cuestionario a la muestra

Se aplica el cuestionario a la muestra representativa de expertos recogiendo la información cualitativa necesaria sobre las variables e indicadores que se quieren conocer y medir en torno al funcionamiento de las cuatro entidades del sistema de justicia penal seleccionadas para esta investigación. En esta sección del cuestionario se realizaron 20 preguntas idénticas por periodo de gobierno (2004-2009, 2009-2014) que se dividen en cinco preguntas (una por cada aspecto institucional) para cada una de las cuatro entidades evaluadas, lo que hace un total de 40 preguntas sobre los aspectos institucionales sumando los dos periodos de gobierno. La determinación experta de la valoración dada a cada aspecto institucional, debido a su grado de desarrollo por entidad y periodo, se fijó sobre la base de la escala cualitativa: Muy bueno, Bueno, Regular, Malo y Muy malo, que corresponden al grado de desarrollo y fortaleza de cada aspecto según el juicio de los expertos.

Paso 2. Valoración y transformación cuantitativa de los aspectos institucionales

Hechas las valoraciones individuales por los expertos, se procede a ordenar y clasificar los datos y las valoraciones en una matriz según aspecto, entidad y periodo para transformar la valoración cualitativa a escala numérica donde Muy bueno equivale a 5, Bueno a 4, Regular a 3, Malo a 2 y Muy malo equivale a 1. Una vez transformados estos valores se calculan los promedios de cada aspecto institucional.

Paso 3. Valoración de la importancia y determinación del peso de cada aspecto institucional

Este nivel consistió en la valoración de la importancia de cada uno de los aspectos institucionales. Las variables fueron operacionalizadas de la siguiente forma:

Asignación presupuestaria (i_1). "Asignaciones aprobadas en el presupuesto anual para el cumplimiento de las actividades y proyectos a su cargo, de acuerdo a los objetivos institucionales determinados para un año fiscal" (Ministerio de Economía y Finanzas 2015). Se valoró si el presupuesto otorgado a la entidad fue suficiente tanto para cubrir sus gastos operativos como de inversión.

Los recursos humanos (i_2). Funcionarios públicos que desempeñan labores administrativas, técnicas, de asesoría, etc., que por medio de sus competencias y capacidades permiten el funcionamiento y desarrollo de las entidades del Sistema de Justica Penal. Se valoran los criterios de profesionalización y competencias del recurso humano, entendido como los niveles de preparación técnico-educativa para desempeñar los puestos, las oportunidades de capacitación, entendidas como la formación continua del funcionario para la mejora de su desempeño individual y colectivo dentro de la entidad.

Modernización (i_3). La adecuación o adaptación de las entidades del Sistema de Justicia Penal a los nuevos lineamientos, procesos y técnicas de gestión y administración que buscan hacer más eficaz y eficiente el funcionamiento de estas entidades, conllevando el ofrecimiento de servicios de mejor calidad y resultados que impacten de forma positiva en las expectativas ciudadanas de justicia y seguridad ciudadana. Se valoran criterios como la creación e implementación de algún programa general o concreto de modernización de la entidad, la implantación de TIC en los procesos de administración y funcionamiento de las entidades (adopción de páginas web institucionales y mecanismos tecnológicos que permitan la tramitación electrónica de algunos servicios), implantación de técnicas e instrumentos de gestión para lograr mayor economía, eficacia y eficiencia en el funcionamiento de las entidades, mejoramiento de las infraestructuras y los recursos materiales de la entidad.

Transparencia y Rendición de Cuentas (i_4). Se determina, sobre la base de las estipulaciones de la Ley Nº 6 de 22 de enero de 2002, que dicta normas para la transparencia en la gestión pública de la República de Panamá. Se valora el grado en que la entidad cumple con los criterios de transparencia y Rendición de Cuentas que establece la Ley, principalmente aquellos relacionados con la exposición de información y datos de carácter obligatorio en los sitios web de la entidad.

Atención ciudadana (i_5). Hace referencia a los criterios de calidad de los servicios y la satisfacción del ciudadano con respecto al servicio y trato que recibe y las formas o mecanismos que emplea la entidad y sus funcionarios para ofrecer los servicios a la ciudadanía. Se valora la aplicación de una política institucional basada en la correcta atención a los usuarios, la costumbre o la manera en la

que los funcionarios de una entidad suelen atender a los ciudadanos, la implementación de modalidades de atención al público que faciliten y agilicen los trámites (centros de atención telefónica o electrónica, ventanilla única, disposición de canales para quejas, reclamos y sugerencias, implementación de Guías explicativas de los procedimientos y pasos a seguir para la realización de los tramites, la participación ciudadana a través de la implementación de hojas para la evaluación ciudadana del servicio).

Al igual que en los pasos previos, la información utilizada para la evaluación de la importancia de cada aspecto institucional se extrajo del cuestionario. Concretamente, se estableció una pregunta específica en el instrumento para determinar el nivel de importancia que tiene cada uno de los cinco aspectos según el criterio de los expertos dentro del adecuado funcionamiento del conglomerado de entidades del Sistema de Justicia Penal, utilizando una escala de 1 a 10 para dicha valoración, donde uno es mínima importancia y 10 es máxima importancia para luego proceder a determinar el promedio de las valoraciones expertas. Se determinan, por tanto, los pesos de los aspectos institucionales, tal como muestra la tabla 1, y determinar así, el orden de importancia de dichos aspectos para el adecuado funcionamiento de la entidad según la valoración de los expertos.

Tabla 1. Ecuaciones para el cálculo de los Pesos de los aspectos institucionales

Indicador	Descripción	Ecuación
IA1	Peso del presupuesto	
IA2	Peso del recurso humano	
IA3	Peso de la modernización	
IA4	Peso de la transparencia y rendición de cuentas	
IA5	Peso de la atención ciudadana	

Paso 4. Evaluación de la institución

Una vez determinadas las valoraciones expertas por cada aspecto (paso 2) y los pesos de los aspectos institucionales (paso 3), se procede a determinar la evaluación de la institución, de acuerdo a la ecuación[6]:

$$i1xIA1+i2xIA2+i3xIA3+i4xIA4+i5xIA5$$

Para los efectos de la validación de la metodología, se realizó una triangulación de fuentes y datos (Valencia, 2000), para corroborar que existiera concordancia entre los resultados del modelo y los datos estadísticos disponibles sobre las instituciones estudiadas y en particular, de los aspectos evaluados.

Resultados

Los pesos de los aspectos institucionales de las entidades del Sistema de Justicia Penal

Una vez valorados los cinco aspectos institucionales por los expertos, se logró determinar la importancia (en una escala) que tienen estos aspectos para el funcionamiento adecuado de las entidades analizadas según las valoraciones de todos los expertos. En este sentido, la tabla 2 muestra las valoraciones que obtienen los aspectos estudiados que significa el peso que tiene el aspecto institucional con relación al resto de aspectos dentro del funcionamiento de la entidad.

6 EI = Evaluación institucional por periodo; i_1, i_2, i_3, i_4, i_5 = valoración promedio de los aspectos institucionales, por entidad y periodo; y I_{A1}, I_{A2}, I_{A3}, I_{A4}, I_{A5} = Peso de los aspectos institucionales.

Tabla 2. Transformación de variables de importancia por aspecto institucional

Aspecto	Valoración experta	Porcentaje en la valoración total
Asignación presupuestaria	9,75	20.5%
Recurso humano	9,42	19.8%
Modernización	9,17	19.3%
Transparencia y rendición de cuentas	9,58	20.2%
Atención ciudadana	9,58	20.2%
Sumatoria		

Evaluación de los aspectos administrativos y de funcionamiento por Entidad del Sistema de Justicia Penal

Una vez valorados los cinco aspectos institucionales para cada entidad del Sistema de Justicia Penal por los expertos, se logró determinar la valoración de cada aspecto por institución y periodo de gobierno en una escala de 1 a 5 (Muy bueno, bueno, deficiente/regular, malo, muy malo). En este sentido, el grafico 1 muestra las valoraciones que obtienen los aspectos de cada entidad estudiada.

Evaluación de las Entidades del Sistema de Justicia Penal

Las entidades del Sistema de Justicia Penal de la República de Panamá, obtuvieron, según el modelo de evaluación, diversas valoraciones

Gráfico 1. Evaluación de las Instituciones del Sistema de Justicia Penal (Períodos 2004-2009 y 2009-2014)

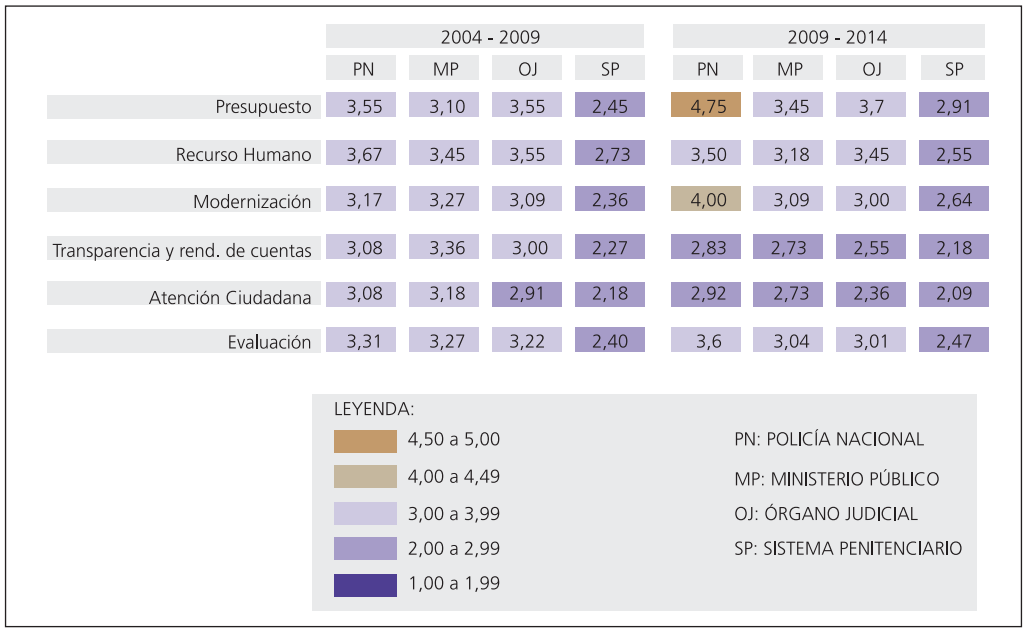
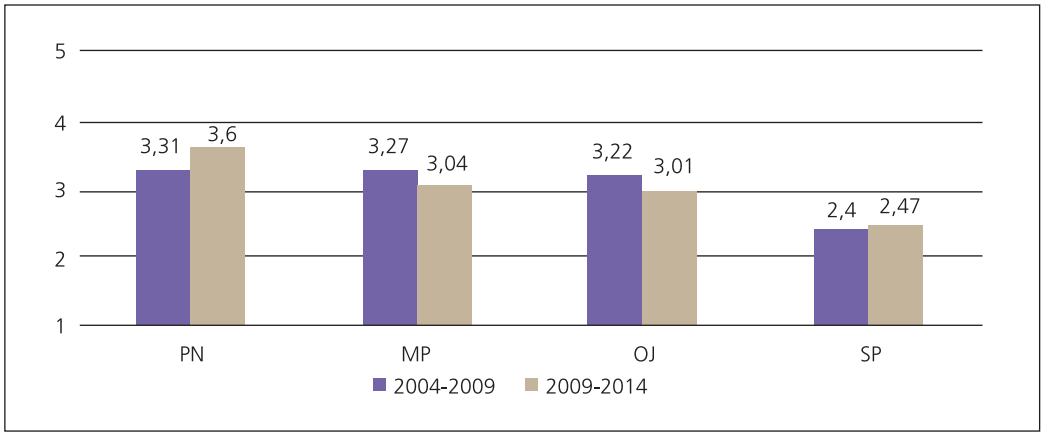


Grafico 2. Evaluación general de las entidades del Sistema de Justicia Penal



Fuente: Elaboración propia.

PN: Policía Nacional, MP: Ministerio Público, OJ: Órgano Judicial, SP: Sistema Penitenciario.

(ver Gráfico 2). La Policía Nacional fue evaluada con 3,31 en el periodo 2004-2009 y 3,6 en el periodo 2009-2014, en una escala de 1 a 5; el Ministerio Público fue evaluado con 3,27 en el periodo 2004-2009 y 3,04 en el periodo 2009-2014, en una escala de 1 a 5; el Órgano Judicial fue evaluado con 3,22 en el periodo 2004-2009 y 3,01 en el periodo 2009-2014 en una escala de 1 a 5; y el Sistema Penitenciario fue evaluado con 2,4 en el periodo 2004-2009 y 2,47 en el periodo 2009-2014 en una escala de 1 a 5.

Conclusiones

En cuanto al peso de las variables (aspectos institucionales), el Modelo de Evaluación indica que el presupuesto es el aspecto institucional de mayor peso en el funcionamiento de las Instituciones del Sistema de Justicia Penal de la República de Panamá durante el periodo de estudio (2004-2014), seguido de la Atención Ciudadana y la Transparencia y Rendición de Cuentas en segundo lugar, mientras que los aspectos de Recursos Humanos y Modernización, ocupan un tercer y cuarto lugar, respectivamente. Sin embargo, la diferencia entre el aspecto institucional de presupuesto y el de modernización es de apenas 1.23 puntos porcentuales, por lo que se concluye que no existen mayores diferencias en el peso que tiene un determinado aspecto en el funcionamiento de las entidades con relación a los otros aspectos según el modelo de evaluación.

PN: Policía Nacional, MP: Ministerio Público, OJ: Órgano Judicial, SP: Sistema Penitenciario.

Sin embargo, la diferencia entre el aspecto institucional de presupuesto y el de modernización es de apenas 1.23 puntos porcentuales, por lo que se concluye que no existen mayores diferencias en el peso que tiene un determinado aspecto en el funcionamiento de las entidades con relación a los otros aspectos según el modelo de evaluación. Igual-

mente, de acuerdo a la evaluación, en todas las entidades en el periodo 2004-2009, el aspecto institucional mejor evaluado en cada una de ellas fue el recurso humano. Aun así, el mismo fue evaluado como regular (deficiente) en términos generales en todas las instituciones estudiadas, excepto en el Sistema Penitenciario donde, a pesar de haber sido el aspecto mejor valorado, fue evaluado como malo en términos comparativos con el resto de entidades, mientras que para el período de gobierno 2009-2014 en todas las entidades el aspecto institucional mejor evaluado fue el presupuesto.

En cuanto a la evaluación general de las entidades del Sistema de Justicia Penal, según el modelo de evaluación, concluimos que la Policía Nacional arroja valoraciones deficientes en ambos períodos de gobierno. Estas deficiencias están más acentuadas en el período 2004-2009, donde toda la valoración de los distintos aspectos institucionales es deficiente (entre 3.00 y 3.99 en una escala de 1 a 5). Cabe destacar que en la Policía Nacional solamente destacan dos aspectos institucionales que fueron evaluados como buenos, ambos en el período de gobierno 2009-2014: la asignación presupuestaria (4.75 en una escala de 1 a 5) y la modernización (4.00 en una escala de 1 a 5), observándose que los aspectos presupuestarios y de modernización de la Policía Nacional fueron los mejor evaluados dentro de todos los aspectos considerados de las cuatro entidades evaluadas de los dos períodos de gobierno.

El Ministerio Público refleja valoraciones deficientes en todos los aspectos institucionales de ambos períodos de gobierno. Sin embargo, cabe destacar que los aspectos de Transparencia y Rendición de Cuentas y Atención Ciudadana registraron una leve mejor valoración en el período 2004-2009, en comparación con la mala valoración que registraron en el período 2009-2014. El Órgano Judicial no tiene grandes variaciones en el desarrollo de sus aspectos institucionales comparativamente entre los dos períodos de gobierno, ya que el modelo arroja valoraciones deficientes muy similares entre ambos períodos. Sin embargo, aspectos institucionales como la atención ciudadana registran valoraciones malas en ambos períodos de gobierno, al igual que la transparencia y rendición de cuentas que también arroja valoraciones bajas en ambos períodos (3.00 para el período 2004-2009 y 2.54 para el período 2009-2014).

El Sistema Penitenciario es evaluado como malo en ambos períodos de gobierno: 2.40 y 2.47, en escala de 1 a 5, respectivamente. Todos los aspectos institucionales del Sistema Penitenciario son valorados como malos (entre 2.00 y 2.99 en una escala de 1 a 5), siendo la entidad peor evaluada comparativamente con el resto de instituciones del Sistema de Justicia Penal en ambos períodos de gobierno según el modelo de evaluación. En cuanto a la evaluación comparativa de las cuatro entidades del Sistema de Justicia Penal, el modelo de evaluación señala que la Policía Nacional y el Sistema Penitenciario son las entidades mejor (Policía Nacional) y peor (Sistema Penitenciario) evaluadas en ambos períodos de gobierno.

Sin embargo, y a pesar de este resultado, en términos generales, las cuatro entidades en ambos períodos son valoradas como deficientes (entre 3.00 y 3.99 en una escala de 1 a 5), exceptuando el Sistema Penitenciario que es valorado como malo (entre 2.00 y 2.99 en una escala de 1 a 5) en ambos períodos. Cabe destacar que únicamente la Policía Nacional, en términos comparativos, entre un período y otro, registra una leve diferencia en su valora-

ción de 0.29 puntos de diferencia producto de su mejor evaluación en el período de gobierno 2009-2014. Por último, según los expertos, los cinco aspectos institucionales evaluados tienen una importancia similar entre sí para el funcionamiento adecuado de las entidades del Sistema de Justicia Penal de la República de Panamá, lo que indica que, por ejemplo, a pesar de que el aspecto presupuesto presentó diferencias (inversión significativa) entre un periodo de gobierno y otro, principalmente en la Policía Nacional, el mismo no fue suficiente para que esta entidad lograra obtener una evaluación positiva, pues otros aspectos no tradicionales como la transparencia y rendición de cuentas, así como la atención ciudadana que presentaron valoraciones deficientes, influyeron negativamente en la evaluación de esta entidad, lo que refleja el grado de paridad entre los cinco aspectos institucionales según el criterio de los expertos.

Bibliografía

Ahumada, Alejandra, Diego Farren y Bernardita Williamson. 2008. *Encuesta de opinión de jueces: Evaluación de las medidas cautelares personales y otros temas relacionados*. Santiago de Chile: Fundación Paz Ciudadana.

Alas de Franco, Carolina. 2016. *Aumento de recursos y algunos resultados en seguridad y justicia, 2008-2015*. El Salvador: Estudios Económicos.

Alonso, José Antonio. 2005. "Instituciones y Desarrollo Económico: El caso de América Latina". En *Gobernanza. Dialogo Euro-Iberoamericano sobre el Buen Gobierno*, coordinado por Vidal Beltrán y Joan Prats I Catalá, 109-117. Madrid: Editorial Colex.

Alonso, José Antonio, y Carlos Garcimartín. 2010. "Calidad de las instituciones, equidad y pacto fiscal". *Cuadernos Económicos de ICE* 78.

Ayala Espino, José, y Juan González. 2001. "*El neoinstitucionalismo, una revolución del pensamiento económico"*. Comercio Exterior 1 (51).

Ballestero Díaz, Fernando, y Andrés Font Jaume. 2004. "El despertar del e-procurement en las administraciones públicas", http://www.revistasice.com/CachePDF/ICE_813_73-88__9762FAF8AC3306090227B01C619F80B6.pdf.

Baracaldo, Estela. 2004. "La reforma policial en Colombia". En *Memoria del proyecto Política Pública de Seguridad Ciudadana*, compilado por Oswaldo Jarrín, 189-195. Quito: FLACSO.

Barea Tejeiro, José, José Antonio Martínez Álvarez y Ana Belén Miquel Burgos. 2014. *El presupuesto como instrumento de gestión pública eficaz. La implantación del presupuesto base cero en la Administración Pública española*. España: Instituto de Estudios Fiscales.

Barreda, Mikel. 2006. "Instituciones Democráticas y Desarrollo en América Latina: La impronta de la desigualdad y la informalidad". En *El Desafío de la globalización en América Latina. Claves para una interpretación*, compilado por Jorge Aromando, 155-186. Buenos Aires: Ediciones Jorge Baudino.

Basabé Serrano, Santiago. 2013. "Sistema de información, de administración y gestión de justicia para la seguridad ciudadana en el distrito metropolitano de Quito". En *Estudios de Seguridad Ciudadana, 2010-2012*, compilado por OMSC, 99-137. Quito: Distrito Metropolitano.

Baytelman, Andrés, y Mauricio Duce. 2003. *Evaluación de la Reforma Procesal Penal: Estado de una reforma en marcha*. Santiago de Chile: Universidad Diego Portales.

Benavides, Víctor, y Edgar Rodríguez. 2006. "Mejoramiento en la Gestión Gerencial del Despacho Judicial" (ponencia en seminario, Santa Cruz, Bolivia).

Beobide Ezpeleta, Ignacio, y Luis I. Gordillo Pérez. 2012. *La naturaleza del Estado. Origen, tipología y lógica de actuación política y social.* Madrid: Tecnos.

BID (Banco Interamericano de Desarrollo). 2013. "Evaluación del impacto de la nueva Policía Metropolitana de la Ciudad Autónoma de Buenos Aires", https://publications.iadb.org/handle/11319/5943?locale-attribute=es&scope=123456789/11&thumbnail=false&order=desc&rpp=5&sort_by=score&page=1&query=estacionamiento&group_by=none&etal=0.

Blanco Dopico, María Isabel, Beatriz Guzmán y Cristina Guzmán. 2006. "La gestión de la calidad total en el sector público local: estudio de un caso" (ponencia presentada en *IX Jornada de Contabilidad Pública ASEPUC*, Logroño, La Rioja, 23 y 24 de febrero).

Briones Gamarra, Oscar. 2006. "Modernización y gestión del personal: el caso de la administración autonómica de Galicia". *RIPS, Revista de Investigaciones Políticas y Sociológicas* 1 (5): 65-82.

Cabero Almenara, Julio, y María del Carmen Llorente Cejudo. 2013. "La Aplicación del Juicio de Experto como Técnica de Evaluación de las Tecnologías de la Información y Comunicación (TIC)". *Revista de Tecnología de Información y Comunicación en Educación*, 2 (7) Julio-diciembre.

Castillo, Magaly, Gina De La Guardia, Aida Jurado Zamora y Margarita Arosemena. 2010. "Administración de justicia en Panamá 2000-2009", http://estadonacion.or.cr/files/biblioteca_virtual/centroamerica/004/Castillo_et_al_2010.pdf.

Cerrillo i Martínez, Agustí. 2011. "Transparencia administrativa y lucha contra la corrupción en la Administración local", http://repositorio.gobiernolocal.es/xmlui/bitstream/handle/10873/1255/16_Cerrillo_Transparencia.pdf?sequence=1.

Coca Muñoz, José Luis. 2007. "*El sistema penitenciario mexicano: a un paso del colapso*". IUS, Revista del Instituto de Ciencias Jurídicas de Puebla 19, 168-187.

Conejero Paz, Enrique. 2014. "Rendimiento, evaluación y rendición de cuentas de las administraciones públicas en España". RIPS 2 (13): 77-101.

Contini, Francesco, y Marco Velicogna. 2010. "Del acceso a la información al acceso a la justicia: diez años de e-justice en Europa". *Publicación semestral del Centro de Estudios de Justicia de las Américas, CEJA* 16: 30-47.

Criado, Ignacio, y Ramón Gil-García. 2013. "Gobierno electrónico, gestión y políticas públicas Estado actual y tendencias futuras en América Latina". *Gestión y Política Pública*, volumen temático: 3-48.

Dammert, Lucia. 2007. "Reforma policial en América Latina. Perspectivas y dilemas de la seguridad ciudadana en América Latina". *Ciudadanía y Violencias* 2: 105-118.

Escobar, Modesto. 2011. "La calidad democrática. Una propuesta para su medición por expertos". *Reis* 133, enero-marzo: 59-80.

Escobar Pérez, Jazmine, y Ángela Cuervo-Martínez. 2008. "Validez de contenido y juicio de expertos: una aproximación a su utilización". *Avances en Medición* 6: 27–36.

Fundación para el Debido Proceso. 2007. "Controles y descontroles de la corrupción judicial. Evaluación de la corrupción judicial y de los mecanismos para combatirla en Centroamérica y Panamá", http://www.dplf.org/sites/default/files/1196091551.pdf.

García Fernández, Javier. 2004. "Estrategias horizontales de intervención en la cooperación española: el desarrollo institucional". Quórum: Revista de Pensamiento Iberoamericano 8: 239-262.

García Hernández, Joaquín. 2011. "La transparencia en México: ventajas y desventajas", https://www.uaeh.edu.mx/investigacion/productos/5069/xvii_congreso_clad_transparencia.pdf.

García España, Elisa. 2013. *"La calidad de la justicia penal en España. Indicadores de calidad del CGPJ"*. Revista de derecho penal y criminología 10: 553-582.

Gil Gómez, Hermenegildo, Martín Darío Arango Serna y Amadeo Lleó Calás. 2010. "Modernización de los procesos en la administración pública en la era digital". *Revista Avances en Sistemas e Informática* 1 (7). http://www.bdigital.unal.edu.co/23617/1/20609-69645-1-PB.pdf.

Granados, Sergio, Fernando Larraín y Jorge Rodríguez. 2009. "Planificación y presupuesto como herramientas de política pública", http://www.cieplan.org/media/publicaciones/archivos/324/Paper.pdf.

Gutiérrez Lara, Abelardo. 2015. "*Gasto público y Presupuesto Base Cero en México"*, http://www.elcotidianoenlinea.com.mx/pdf/19203.pdf.

De la Nuez, Elisa, Carlota Tarín y Rafael Rivera. 2015. "*Innovaciones en la prestación de servicios públicos"*, https://publications.iadb.org/bitstream/handle/11319/6912/ICS_DP_Los_servicios_en_l%C3%ADnea_como_derecho_ciudadano.pdf?sequence=1.

Duce, Mauricio, y Rogelio Pérez Perdomo. 2005. "La seguridad ciudadana y la reforma del sistema de justicia penal en América Latina". En *Crimen y violencia en América Latina*, editado por Hugo Frühling, Joseph S. Tulchin y Heather A. Golding, 91-116. Bogotá: Fondo de Cultura Económica.

Fruhling, Hugo. 2005. "La reforma de la policía y el proceso de democratización". En *Crimen y violencia en América Latina*, editado por Hugo Frühling, Tulchin y Golding, 29-62. Fondo de Cultura Económica.

Fuentes Saavedra, Claudio. 2011. Reflexiones sobre los determinantes políticos de la seguridad ciudadana. Seguridad Ciudadana en América Latina: Miradas críticas a procesos institucionales. Chile: Instituto de Asuntos Públicos/Centro de Estudios en Seguridad Ciudadana/Universidad de Chile.

Ley 6, de 22 enero de 2002, "Que dicta normas para la transparencia en la gestión pública y establece la acción de habeas data y dicta otras disposiciones", Gaceta Oficial, 24476.

Lillo L., Ricardo. 2010. "Indicadores de CEJA: El rol de las TIC en una justicia para ciudadanos". *Publicación semestral del Centro de Estudios de Justicia de las Américas, CEJA* 16: 6-7.

Manning, Nick. 2008. "Presupuesto en base a información de resultados en América Latina: Experiencias y oportunidades", http://www.coplac-gprd.org/images/stories/Publicaciones/Presupuesto/Presupuesto_basado_en_resultados_CD.pdf.

Manzano, Alberto. 2011. "Diseño y validación de un cuestionario para analizar la calidad

en empleados de servicios deportivos públicos de las mancomunidades de municipios extremeñas". *E-balonmano.com. Revista de Ciencias del Deporte*, 7 (3): 181-192.

Marcel, Mario. 2008. "Presupuesto por resultados: ¿Moda burocrática o nuevo paradigma en gestión pública?", http://www.coplacgprd.org/images/stories/Publicaciones/Presupuesto/Presupuesto_basado_en_resultados_CD.pdf#page=41.

Martínez Álvarez, José Antonio, y María Dolores García Martos. 2014. "Presupuesto base cero: una herramienta para la mejora de las finanzas públicas". Crónica Tributaria 149: 7-31.

Mejía Lira, José. 2005. "La evaluación como herramienta para una gestión pública orientada a resultados. La práctica de la evaluación en el ámbito público mexicano". CLAD.

Méndez Juez, Marta. 2014. "Un camino hacia la excelencia en la prestación del servicio público autonómico: los grupos de mejora de la administración de la Comunidad de Castilla y León". *Revista jurídica de Castilla y León* 34: 1-40.

Mendoza Tolosa, Henry Antonio, William Orlando Prieto Bustos y Carlos Alberto Barreto Nieto. 2012. "Encuesta de opinión para la evaluación de la gestión pública en Colombia: una propuesta de medición", http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-63462012000200004.

Moreira Corrêa, Izabela, y Mário Vinícius Claussen Spinelli. 2011. "Políticas de transparencia en la administración pública brasileña". *Revista del CLAD, Reforma y Democracia* 51: 129-152.

Moyado Estrada, Francisco. 2002. "Gestión pública y calidad: hacia la mejora continua y el rediseño de las instituciones del sector público", http://unpan1.un.org/intradoc/groups/public/documents/CLAD/clad0043302.pdf.

Naessens, Hilda. 2010. "Ética pública y transparencia", https://halshs.archives-ouvertes.fr/halshs-00531532/document.

Ochoa Henríquez, Haydée y Yorberth Montes de Oca. 2004. "Rendición de Cuentas en la Gestión Pública: Reflexiones teóricas". *Revista Venezolana de Gerencia* 27: 455-472.

Ortega, Daniel. 2014. "Incentivos electorales, capacidad del Estado y legitimidad". En *Por una América Latina más segura. Una nueva perspectiva para prevenir y controlar el delito*, editado por CAF, 211-238. Bogotá: CAF.

Pásara, Luis, ed. 2011. "El funcionamiento de la justicia del Estado", http://www.justicia.gob.ec/wp-content/uploads/downloads/2012/07/1_El_fucionamiento_de_la_justicia_del_Estado.pdf.

Pastor Prieto, Santos. 2003. "Dilación, eficiencia y costes. ¿Cómo ayudar a que la imagen de la justicia se corresponda mejor con la realidad?", http://www.fbbva.es/TLFU/dat/DT_2003_05.pdf.

Pastor, Santos, y Liliana Maspóns. 2005. "Cifrar y Descifrar. Indicadores judiciales para las Américas", http://biblioteca.cejamericas.org/bitstream/handle/2015/3843/cifrar-descifrar2-esp.pdf?sequence=1&isAllowed=y.

Perramon, Jordi. 2013. "La transparencia: concepto, evolución y retos actuales". *Revista de Contabilidad y Dirección* 16: 11-27.

Pliscoff, Cristina. 2008. "Modernización de la Gestión Pública en el Primer Tiempo: Avances y retrocesos", http://agendapublica.uchile.cl/n11/CristianPliscoff.pdf.

Pocoví, María Estela. 2009. "Gestión y desarrollo de recursos humanos: Clave para la transformación y la modernización de la administración pública. El caso de la Provincia de Santa Fe", http://www.scielo.org.ar/pdf/daapge/n12/n12a05.pdf.

Ramió, Carles. 1999. *Teoría de la Organización y de la Administración Pública*. Madrid: Tecnos.

Ramió Matas, Carles. 2012. "E-administración y renovación institucional para la mejora de los servicios públicos". Ponencia presentada en *XVII Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública*, Cartagena, 30 de octubre y 2 de noviembre.

Ramírez Brouchoud, María. 2009. "Las reformas del Estado y la administración pública en América Latina y los intentos de aplicación del New Public Management". *Estudios Políticos* 34: 115-141.

Ramos García, José María, y Mariana Flores. 2013. "Gobernanza, Seguridad Ciudadana y Desarrollo Local. Gobernanza y prevención transversal en la frontera norte de México". En *Gobernanza y prevención transversal en la frontera del norte de México*, editado por José María Ramos García y Alberto Villalobos Pacheco, 17-50. México: Centro de Alta Dirección Pública.

Ramos Rollón, Marisa. 2005. *Sistemas judiciales y democracia en Centroamérica: La perspectiva de los jueces*. Barcelona: CIDOB Edicions.

Rebuffi, Ana Clara. 2012. "Herramientas para evaluar la eficiencia judicial en la provincia de Salta (Argentina)", http://www.ief.es/documentos/recursos/publicaciones/revistas/cuadernos_formacion/2012_14_4.pdf.

Rivas Leone, José Antonio. 2003. "El neoinstitucionalismo y la revalorización de las instituciones". *Reflexión política* 5 (9): 37-44.

Rivera-Cira, Tirsa, Milena Sánchez de Boado y David Varela. 2010. "Las Instituciones de La Justicia Penal", http://siteresources.worldbank.org/INTLAC/Resources/Sp_Volume_II_Crime_and_Violence_Central_America.pdf.

Rodríguez-Arana, Jaime. 2001. "El proceso de modernización administrativa en las Comunidades Autónomas", http://idpbarcelona.net/docs/public/iccaa/2001/2_parte/modernizacion.pdf.

Ruiz, Juan Carlos. 2004. "Policía exitosa, policía indolente: nuevas tendencias en Seguridad Ciudadana". En *Política Pública de Seguridad Ciudadana, Primera Fase*, editado por Oswaldo Jarrín, 119-127. Quito: FLACSO.

Ruiz López, Joaquín y Eloy Cuellar Martín. 2013. "La Gestión de Calidad en las Administraciones Públicas Españolas. Balance y perspectivas. Gestión y Análisis de Políticas Públicas", http://e-archivo.uc3m.es/bitstream/handle/10016/19187/gestion_ruiz_GAPP_2013.pdf?sequence=2.

Salvador Serna, Miquel. 2003. "Instituciones y políticas públicas en la gestión de los recursos humanos de las comunidades autónomas" (tesis doctoral, Universitat Pompeu Fabra).

Sancho Royo, David. 2007. "La prestación del servicio público: ¿Qué es lo que el ciudadano entiende por calidad?", http://justicia.gencat.cat/web/.content/documents/arxius/prestacion_royo.pdf.

Tudela, Patricio. 2007. "Sociedad y Policía: Desarrollo y retos de la función policial en las democracias latinoamericanas". *Revista de Estudios Policiales* 7: 74-107.

UNODOC (Oficina de las Naciones Unidas contra la droga y el delito). 2010. "Medidas privativas y no privativas de la libertad. El sistema penitenciario: Manual de instrucciones para la evaluación de la justicia penal", https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/The_Prison_System_Spanish.pdf.

UNODOC-CEJA. 2015. "Evaluación de la implementación del Sistema Penal Acusatorio",http://biblioteca.cejamericas.org/bitstream/handle/2015/5493/informefinal _evaluaciondelaimplementaciondelsistemapenalacusatorio_panama.pdf?sequence=1&isAllowed=y.

Valencia Agudelo, German. 2011. "Contribuciones de las políticas públicas al estudio del Estado". *Semestre Económico* 30: 87-104.

Valencia, María Mercedes. 2000. "La triangulación metodológica: sus principios, alcances y limitaciones". *Investigación y educación en enfermería* 18 (1): 13-26.

Vanderschueren, Franz, Michel Marcus, Alejandra Lunecke y Jean Paul Buffat. 2004. *Políticas de seguridad ciudadana en Europa y América Latina, lecciones y desafíos*. Santiago de Chile: Ministerio del Interior.

Vicher-García, Mónica. 2012. "Utilidad o futilidad: calidad e ISOs en la administración pública". UAEM 60 (septiembre-diciembre): 205-228.

Zepeda Lecuona, Guillermo. 2005. "Los retos de la eficacia y la eficiencia en la seguridad ciudadana y la justicia penal en México: Mejorar la seguridad ciudadana y la justicia penal en México a través de una intensa reforma y del uso racional y eficiente de los recursos disponibles", http://cidac.org/esp/uploads/1/Los_retos_de_la_eficacia_y_la_eficiencia_en_la_seguridad_ciudadana_y_la_justicia_PDF.pdf.

_____. 2010. "La policía mexicana dentro del proceso de reforma del sistema penal", http://cidac.org/esp/uploads/1/La_polic__a_mexicana_dentro_del_proceso_de_reforma_del_sistema_penal_PDF.pdf.

_____. 2013. *Situación y desafíos del sistema penitenciario mexicano*. México: Centro de Análisis de Políticas Públicas.

Entrevista

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2860

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 167-173
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Regionalismo de seguridad, la dinámica de la amenaza y el uso de la fuerza armada en América Latina[1] Entrevista a Jorge Battaglino

Regionalism of security, the dynamics of the threat and the use of armed force in Latin America Interview to Jorge Battaglino

Marco Vinicio Méndez-Coto[2]

El día 27 de septiembre de 2016, en las instalaciones de la Universidad Torcuato Di Tella (UTDT) de Argentina, se llevó a cabo una entrevista académica con el Dr. Jorge Battaglino, experto en política latinoamericana, relaciones civiles militares y seguridad internacional, quién además se desempeñó como Director de la Escuela de Defensa Nacional (actual Facultad de la Defensa de la Universidad de la Defensa Nacional) que depende del Ministerio de Defensa argentino. A continuación, se presentan las principales contribuciones analíticas para el debate sobre el regionalismo de seguridad y sus principales cambios políticos durante la posguerra fría en América Latina.

En términos de la amenaza y uso de la fuerza en el continente, ¿cómo caracterizaría la dinámica en el siglo XXI?

En los últimos treinta años, la zona de paz sudamericana ha modificado su naturaleza al modificar sus fundamentos. Esta afirmación podría extenderse también a Latinoamérica. Al hecho de que la región ha tenido durante gran parte del siglo XIX un elevado nivel de paz interestatal, se suma la resolución de gran parte de los conflictos limítrofes, el impacto de la democratización y el incremento de las relaciones económicas que han mejorado

1 Entrevista académica resultado de la investigación doctoral "Enfrentando agresiones externas. Estados pequeños y complejos regionales de seguridad: los casos de Costa Rica y Ecuador" dirigida por el Dr. Fredy Rivera Vélez, Facultad Latinoamericana de Ciencias Sociales (FLACSO) – Ecuador.

2 Candidato a Doctor en Estudios Internacionales por FLACSO-Ecuador. Premio de estudios de posgrado de la Organización de Estados Americanos, período 2016-2018. Cuenta con una Maestría en Derechos Humanos y Educación para la Paz y una Licenciatura en Relaciones Internacionales, ambos de la Universidad Nacional de Costa Rica. Ha publicado libros y más de una decena de artículos en revistas científicas indexadas. Correo:marco.mendez.coto@gmail.com / mvmendezfl@flacso.edu.ec

sustantivamente los fundamentos de la paz. Aunque la paz interestatal convive en algunos casos con un importante nivel de conflictividad interna, tampoco esa inestabilidad ha favorecido el estallido de conflictos bélicos entre Estados, como pareció que iba a ser el caso en los momentos de máxima tensión entre Venezuela, Colombia y Ecuador.

La región, y específicamente América del Sur, se acerca a una situación inédita en su historia: gran parte de los conflictos territoriales que existían hasta hace poco años se han resuelto; además, una de las dinámicas (el conflicto colombiano) que favorecía altos niveles de violencia interna que derramaban sobre los países limítrofes, está a punto de resolverse. Aunque la región padece de graves problemas como la desigualdad, el crimen organizado y el narcotráfico, entre otros; no es evidente ni inminente que estas cuestiones tengan el potencial de afectar la paz interestatal. Sin embargo, estos datos empíricos no logran responder la interrogante de ¿por qué la región es una zona de paz? que es mucho más compleja y difícil de responder. Ciertamente, lo que nos distingue de otras partes del planeta es que los latinoamericanos no hemos elegido la guerra para resolver conflictos. Aunque existen excelentes trabajos sobre la paz regional, como los de Arie Kacowicz, por ejemplo, aún es necesario continuar investigando las fuentes o determinantes de la paz regional.

En nuestra investigación en FLACSO Ecuador, publicamos un artículo[3] en el que se analizan todos los países latinoamericanos en términos de Constituciones políticas y de documentos programáticos de la defensa para indagar la prevalencia de la agresión externa como una amenaza. Lo que encontramos es que el 67% de los países latinoamericanos, incluyendo los del Cono Sur, aun en documentos normativos y programáticos, se mantiene la idea de una hipótesis de conflicto interestatal. ¿Cómo se podría explicar frente a estos cambios geopolíticos que aun en las normas y en instrumento programáticos aun persista esta idea de la agresión externa?

Las razones por las que eso sucede son muy diversas y no hay una explicación única, me inclino por comenzar por el caso de la Argentina. En este país, existe una legislación que es muy estricta. Aquí tenemos una Ley de Defensa que prohíbe a los militares llevar a cabo misiones de seguridad interna. Por ejemplo, los militares no pueden hacer inteligencia en cuestiones relacionadas con el crimen organizado, el terrorismo y, menos aún, pueden participar directamente. Para eso están las policías y las llamadas fuerzas intermedias. Toda la doctrina militar de Argentina y la misión de nuestras Fuerzas Armadas se reducen a enfrentar agresiones de origen externo y estatal. El supuesto es que la intervención doméstica de las fuerzas armadas es peligrosa por muchas razones: porque los militares no están entrenados para llevar a cabo ese tipo de función, porque no deberían estar entrenados para ello porque deben preservarse exclusivamente para enfrentar el máximo nivel de fuerza posible, que es el de otra fuerza armada. Los militares no son policías, porque si intervienen, se politizan y se corrompen. Sin embargo, el problema que tiene Argentina y otros países de la región, es que sectores de la opinión pública,

3 Méndez-Coto, Marco V. (2017). Prácticas de seguridad en América durante la posguerra fría (1992-2010): ¿Complejos regionales o Comunidades pluralistas de seguridad? *Revista de Relaciones Internacionales, Estrategia y Seguridad* 12 (1): 75-106.

de la política y de las mismas fuerzas armadas buscan la intervención militar en la lucha contra el narcotráfico o el crimen organizado. Lo paradójico es que estas misiones no hacen más que debilitar al extremo la defensa nacional.

Existen varios países de la región que han identificado una misión tradicional para sus militares, sin que ello signifique reflotar las viejas hipótesis de conflictos con los países vecinos. Argentina no tiene enemigos externos. Brasil y Chile han dejado de serlo. Tenemos, por supuesto, a Gran Bretaña que está ocupando ilegalmente las Islas Malvinas, pero la estrategia de recuperación de las islas es pacífica (aunque considero indispensable incorporar a tal estrategia la dimensión de la defensa). En el caso de Brasil en la Estrategia de Defensa del 2008 se hace mención a que las fuerzas armadas tienen que estar preparadas para enfrentar la amenaza de "una potencia mayor", no se habla allí de un Estado de manera explícita, pero es claro que se hace referencia a una potencia extrarregional.

Otros países, como Uruguay o Chile, intentan evitar que sus militares intervengan en cuestiones de seguridad interna y una estrategia para hacerlo, es identificar misiones externas para sus militares. Chile ha resuelto su histórico conflicto marítimo con Perú, lo cual incentiva el desmonte de la hipótesis de conflicto con ese país. Entonces, en la región se ha producido una transformación cuya importancia no siempre es captada por los académicos y los políticos. Los Estados han comenzado a identificar amenazas, riesgos a su defensa o posibilidades de despliegue de sus militares de alcance extrarregional. Un dato de relevancia es que los dos países de mayor peso relativo en América del Sur, Argentina y Brasil, han identificado en sus estrategias o documentos de la defensa amenazas estatales de origen extra regional.

Esa percepción de la amenaza cambia mucho, incluso dependiendo del partido de gobierno. Actualmente en Argentina, con Macri, parece que hay más acercamiento con Gran Bretaña, disminuye la percepción de amenaza…

Exacto.

En su trabajo se ha señalado que en el continente ha mermado la amenaza y el uso de la fuerza, particularmente en el Cono Sur. Pero aun en la dinámica de las relaciones interestatales latinoamericanas hay ocasiones donde los Estados denuncian que enfrentan una "agresión externa"... Esta idea de la agresión externa en el discurso político es bastante recurrente en muchos países, ¿cómo podríamos interpretar este gesto, esta acción de que un Estado denuncie que enfrenta una agresión externa?

Esto es el resultado de una larga tradición en la región. Kacowicz sostiene que la cultura de resolución pacífica de las controversias es fundamental para comprender la paz regional y ello se evidencia en la densidad de las instituciones regionales, en la enorme predisposición a recurrir a mediaciones de terceros países y organismos para resolver conflictos. No es casual entonces que la región sea una productora de Derecho Internacional. En este sentido, la lógica de la resolución de los conflictos suele iniciarse con una denuncia de agresión, no es más que una manera de activar el sistema de gestión de los conflictos regional e internacional. La denuncia de la agresión no se efectúa para escalar militarmente, sino que es una forma de pedir auxilio para que la comunidad regional e internacional se active e intervenga.

La categoría de la agresión externa, es una categoría jurídica enmarcada en el Derecho Internacional, empezando por la Carta de Naciones Unidas, pero cuando se analiza la práctica del Consejo de Seguridad en toda su historia solo diez veces se ha invocado el artículo 39 y nunca se ha mencionado un Estado latinoamericano. Entonces, la pregunta es que este uso de la idea de la agresión externa no subyace a un fundamento jurídico sino más bien por una connotación de carácter político.

Creo que los textos de la ONU, que definen qué es una agresión, están pensando en situaciones de conflictos bélicos tradicionales donde se quiebra la soberanía de un Estado mediante una invasión. En América Latina los casos de agresión armada se han vinculado, en su gran mayoría, con escaramuzas fronterizas, incursiones armadas o con demostraciones de fuerza militar.

De hecho, esto evidencia que Naciones Unidas piensa una cosa, pero los países latinoamericanos piensan otra, porque si denuncias una agresión, ¿por qué no recurren al Consejo de Seguridad?

Aunque es necesaria más investigación sobre este tema, puedo aventurar el argumento de que en la región la denuncia de la agresión cumple un objetivo político: llamar la atención. Por esa razón, no puede explicarse como la antesala de una acción militar.

Los estudios sobre las disputas interestatales militarizadas y el uso de la fuerza hacen referencia a que en el continente tenemos instituciones sólidas para prevenir el escalamiento de las crisis. En los últimos años, se ha visto un profundo cuestionamiento a los pilares de la arquitectura interamericana: el Tratado de Río, que para Argentina quedó desacreditado y, en los últimos años, los países de la Alianza Bolivariana para los Pueblos de Nuestra América (ALBA) lo han denunciado formalmente, e incluso Colombia ha denunciado el Pacto de Bogotá. Entre una percepción de instituciones sólidas y otra percepción de procesos de cuestionamiento de dichas instituciones, ¿cuál podría ser la situación de seguridad colectiva en el hemisferio en este momento?

Este momento es particular, porque hay un cambio político importante en Brasil [Temer] y en Argentina [Macri] y todavía no se sabe que van a hacer estos países con toda la institucionalidad que se construyó en los últimos años (UNASUR, Consejo de Defensa, etc). Es aventurado realizar afirmaciones tajantes al respecto porque aún falta evidencia para fundamentarlas. Sin embargo, es importante enfatizar que la discusión sobre la solidez institucional debería partir de un sólido marco teórico que permita identificar la tradición en la que se funda, algo que no se ve a menudo en los trabajos sobre el tema que se escriben en nuestros países. En muchas ocasiones, los argumentos naturalizan la experiencia de la Unión Europea sin problematizar su pertinencia para nuestra región. Si se adopta acríticamente esa perspectiva es imposible sostener la idea de que existen instituciones en Latinoamérica y menos aún de que son sólidas. Por el contrario, las instituciones que tenemos responden a tradiciones propias: tienen escasa burocracia, se manejan a nivel de la diplomacia presidencial, o de altos funcionarios… la supranacionalidad no cae muy bien en estas tierras. Por ello, la construcción regional de

América Latina, y sobre todo de América del Sur es distinta, mucho más gradual, mucho más inclusiva tanto de numerosos Estados como también de los intereses de todos los Estados y, por eso, es mucho más lenta y más propensa a ser tildada de ineficiente o de no provocar cambios de magnitud.

La Unión de Naciones Suramericanas (UNASUR) responde a este modelo que en algunas dimensiones ha sido muy eficiente. Además, no tenemos que olvidar la cercanía con los EEUU que dificulta aún más cualquier intento de construir cualquier tipo de institucionalidad regional que no lo contemple como actor predominante. En este sentido, la posibilidad de construcción de instituciones regionales en América Central es más limitada, mientras que América del Sur tiene más margen de autonomía.

Dentro de sus reflexiones académicas para entender estas dinámicas de seguridad en el continente, ¿cuál es la capacidad que ha tenido la teoría de los complejos regionales de seguridad? En América del Sur, ¿qué reflexión ha hecho en ese sentido?

Distintos estudios han trabajado mucho la idea de las dos regiones diferenciadas en Sudamérica: el Cono Sur y la región Andina. Hay dinámicas de seguridad diferentes en ambas regiones. La diferencia principal a mi entender es que en el Cono Sur ha desaparecido la competencia militar. Ello no implica que existan sectores en los tres países que sigan percibiendo a los vecinos como rivales militares. Pero la mayoría de los actores políticos y de las fuerzas armadas no se perciben de esta forma, sino que construyen la relación en términos de cooperación y búsqueda de beneficios mutuos. Por el contrario, en la región Andina persiste la competencia militar. Sin embargo, la persistencia de rivalidad militar entre países vecinos en un contexto de resolución casi absoluta de los conflictos limítrofes, puede colocar a los militares en una situación de déficit de amenazas que favorezca la reducción del presupuesto de defensa y su transformación en policías con alto poder fuego. Por eso, esta razón es fundamental en la construcción política de la idea de la defensa regional contra amenazas extrarregionales, es lo único que permitirá que los militares sigan siéndolo, que continúen siendo una fuerza armada.

En nuestra investigación de FLACSO Ecuador tratamos de estudiar en qué medida el Complejo Regional de Seguridad incide en la forma en que el Estado pequeño prioriza sus preferencias. En el tema de regionalismo de seguridad y estudios estratégicos, ¿cuál ha sido el rol o la posición que en estas reflexiones han tenido los Estados pequeños?

En mi trabajo básicamente me focalicé en América del Sur, y los Estados pequeños que analicé con profundidad son Ecuador y Uruguay. En mi criterio, los Estados pequeños son fundamentales en el sentido de que permiten dar cuenta de ciertas dinámicas de seguridad que son distintivas y, en ese sentido, Ecuador y Uruguay presentan algunas diferencias. Uruguay es uno de los principales contribuyentes del mundo en misiones de paz, mientras que Ecuador no lo hace en la misma medida. En este sentido, el rol histórico de los militares, la magnitud de la problemática de la delincuencia organizada y el narcotráfico, la fortaleza de la sociedad civil, o el marco normativo de la defensa y la seguridad, son factores que permiten explicar porque Estados pequeños adoptan posturas disimiles en su defensa.

Allí hay un tema de investigación muy interesante y poco desarrollado, me refiero a los determinantes y conductas de los Estados pequeños en el área de la defensa y la seguridad. Cuando analicé las zonas de paz no presté demasiada atención al tamaño de los Estados, en gran medida porque mi variable dependiente no se alteraba por ello. Quiero decir, que el tamaño no era predictor de conflictividad estatal en América del Sur. Sin embargo, creo que la variable "tamaño" merece mayor atención e investigación, sobre todo a partir de contemplar factores explicativos que se dejan de lado en estudio comparativos que mezclan estados grandes con pequeños.

De hecho, la idea del riesgo moral se estuvo estudiando justamente porque las instituciones sólidas que impiden la guerra pueden ser una motivación para la militarización de una disputa…

Esto tiene que ver con la experiencia de cada país, la respuesta general que daría es que hay una cultura de resolver pacíficamente los conflictos. Desde esta perspectiva, la guerra no le conviene a nadie. Además, es necesario estudiar el peso de las culturas políticas civilistas. En América Central, el caso de Costa Rica es importante porque ha desarrollado tradiciones políticas muy distintas a las de algunos de sus vecinos. El civilismo de Costa Rica tiene un peso enorme y es inevitable su impacto en la política exterior.

En sus publicaciones, es muy importante recuperar a la democracia, que esta implica un cambio en la forma en la que se constituyen las relaciones interestatales en términos del uso de la fuerza. ¿Cómo dialoga su planteamiento con la tesis de la paz democrática?

La teoría de la paz democrática ha sido muy criticada y en muchos casos con argumentos de peso. Es arriesgado plantear la hipótesis de que la democracia es la causa de la paz. Sin embargo, en América del Sur existe una sólida asociación entre el proceso de democratización y la progresiva resolución pacífica de las disputas interestatales. Hasta los años ochenta, la región estuvo plagada de regímenes militares y de hipótesis de conflicto que pusieron a la mayoría de los países al borde de la guerra en algún momento. Con la difusión regional de la democracia los diferendos se han resuelto en un reducido lapso de tiempo. Los teóricos de la paz democrática dirían que ello se debe a la predisposición a la negociación de los líderes democráticos.

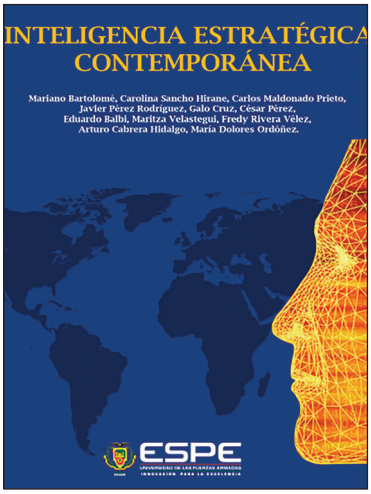
Sin embargo, es necesaria mayor investigación empírica y de identificación de los mecanismos causales que hacen que la democracia favorezca la paz. En el caso de los Estados débiles, existen otras variables a ser tomadas en cuenta, por ejemplo, el cálculo estratégico por lo que representa una guerra en términos de gasto fiscal en países donde no abundan los recursos, porque la victoria no puede garantizarse o debido a que la geografía no favorece la ofensiva. Sin embargo, no es evidente y requiere mayor indagación porque estas variables, y otras que no fueron mencionadas, deberían ser específicas de los Estados pequeños.

Ese es un tema que resulta interesante porque tanto en las crisis Ecuador-Colombia (por Angostura) y de Costa Rica-Nicaragua (por Harbour Head) no se tuvo repercusiones de índole comercial ya que todo se centró en el nivel político, lo que es una particularidad de la región muy destacable.

Es que las variables tipo de régimen e intensidad del vínculo económico deberían tomarse

con sumo cuidado cuando se analiza la paz. Quiero decir que durante gran parte del siglo XX predominaron en América del Sur regímenes militares y bajos niveles de intercambio que, sin embargo, alteraron la continuidad de la paz. Un planteo más mesurado es el que sostiene que la democracia impacta favorablemente en la calidad de la paz. La paz en América del Sur existe desde hace mucho tiempo, lo nuevo son sus fundamentos, muchos más sólidos que los del pasado.

Reseña



DOI: http://dx.doi.org/10.17141/urvio.20.2017.2858

Inteligencia estratégica contemporánea: perspectivas desde la región suramericana[1]

Jyefferson Figueroa[2]

Esta publicación está dirigida a las personas interesadas en aumentar su conocimiento sobre inteligencia estratégica (I.E.), tomadores de decisiones o investigadores que buscan revisar una mirada contemporánea y ajustada al contexto suramericano, en temas como la seguridad, la cooperación, la estrategia militar y la inteligencia. Hablar de I.E. implica reunir diferentes aspectos que hasta hace poco tiempo habían estado en manos exclusivamente de personal militar y policial, generando una mínima producción académica y científica, pues se entendía como tema de alta confidencialidad. En Suramérica no se ha trabajado de forma tan amplia, por lo que la producción sigue estando limitada a esferas cercanas al poder político y militar en los países de la región.

La Universidad de las Fuerzas Armadas decidió realizar esta compilación para entender las nociones más básicas de la inteligencia estratégica, permitiendo que cualquier persona pueda investigar y profundizar sus posturas sobre la temática. Si bien este es un tema poco explorado desde la mirada suramericana, el texto condensa grandes aportes de especialistas cuyo trabajo se centra en las especificidades históricas, contextuales e interpretativas de la región, con discusiones de alta complejidad, como el abordaje de escenarios, casos y propuestas propias de esta parte del continente.

La publicación se divide en tres apartados. En primer lugar, un sondeo del escenario de la I.E. en la región titulado "Perspectivas para una inteligencia estratégica desde la región suramericana". En segundo lugar, una serie de propuestas de fortalecimiento y comprensión del tema en la región, llamado "Conflictividad contemporánea e inteligencia estratégica". Y, por último, algunas reflexiones de orden académico y teórico: "Inteligencia estratégica de la teoría a la práctica: una mirada crítica a los sistemas".

El primer apartado contiene tres artículos. Para generar un acercamiento al tema, Mariano Bartolomé presenta una síntesis del panorama del desarrollo del concepto de I.E. en la seguridad internacional, focalizándose en Sudamérica. El autor expone, en un principio, la categoría de I.E., argumentando que

1 Bartolomé, Mariano, Carolina Sancho Hirane, Carlos Maldonado Prieto, Javier Pérez Rodríguez, Galo Cruz, César Pérez, Eduardo Balbi, Maritza Velastegui, Fredy Rivera Vélez, Arturo Cabrera Hidalgo, María Dolores Ordóñez. 2016. *Inteligencia estratégica contemporánea: perspectivas desde la región suramericana.* Quito: Universidad de las Fuerzas Armadas (ESPE).

2 Sociólogo de la Universidad Santo Tomás de Bogotá, Colombia. Maestrante en Relaciones Internacionales con mención en Seguridad y Derechos Humanos por la Facultad Latinoamericana de Ciencias Sociales (Flacso), sede Ecuador. Correo: edufigueroa21@gmail.com

en los trabajos desarrollados hasta ahora en el continente, los expertos han asumido definiciones demasiado clásicas o simplemente han obviado esta discusión. Posteriormente, presenta cinco puntos claves sobre lo que debería ser la I.E. en la región suramericana, dando forma a una propuesta muy cercana al contexto particular del continente. Concluye Bartolomé planteando los retos para consolidar un modelo común de I.E. en la región, debido a la heterogeneidad de los países que la conforman, sin embargo, invita a pensar en la posibilidad de reformular algunos principios del campo estudiado, con miras a fortalecer su papel en el escenario de la democracia, para hacer del tema una política de estado capaz de fortalecer la toma de decisiones en la región.

Los artículos posteriores abordan, en primer lugar, los retos de la inteligencia estratégica en escenarios de cooperación internacional, desde un punto de vista enfocado en la necesidad de construir lazos de acercamiento y coordinación inter-agencial, de cara a modelos como la Unión de Naciones Suramericanas (Unasur). En segundo lugar, se hace referencia a la necesidad de "profesionalizar" el campo de la inteligencia estratégica en función de los intereses de estado, de tal manera que dicho campo no esté únicamente al servicio de los gobiernos de turno. Al acercarse al estudio de la I.E. como campo de investigación, los artículos de la primera sección del libro constituyen una herramienta clave para la comprensión del fenómeno en la región. En primer lugar, se presentan los retos de la inteligencia estratégica y su comprensión en el contexto latinoamericano; en segundo lugar, una visión liberal de la I.E. y, por último, un estudio de casos suramericanos.

La segunda sección, compuesta por cinco artículos, presenta una propuesta metodológica interesante y diversa sobre la I.E. y su papel en los nuevos retos y conflictos que enfrentan los Estados en la dinámica contemporánea. Debates sobre el papel de la inteligencia en los nuevos conflictos desde el concepto de nuevas guerras de Mary Kaldor, la inteligencia para el posconflicto colombiano, la inteligencia marítima en el Ecuador y el lavado de activos, narcotráfico y el crimen transnacional, son trabajados a lo largo de este apartado desde posturas realistas, hasta estudios de caso.

De esta sección, es esencial resaltar el artículo escrito por Eduardo Balbi, titulado "Anticipación estratégica: clave para la prevención y la gestión de riesgos". El texto presenta una propuesta metodológica basada en la transformación de la forma en la que se hace I.E., incluyendo la prospectiva como eje fundamental de estudio, con miras a la prevención y la gestión del riesgo. Según el autor, la I.E. abarca en esencia tres aspectos fundamentales: al gobierno, la defensa y la seguridad; además busca anticipar los riesgos y disminuir la "conducta reactiva". Ahora bien, su aspecto central debe ser la posibilidad de anticipar o descubrir de manera previa las amenazas del Estado.

Para Balbi, la inclusión de la prospectiva contribuye plenamente a "la búsqueda de eliminación o mitigación del clásico stress de la incertidumbre (que condiciona fuertemente los procesos decisionales y la elaboración de políticas y estrategias) [a su vez] es un requerimiento de alto rango y fuerte desafío" (Bartolomé *et al*. 2016, 109). En este orden de ideas, para el autor es importante insertar una etapa de pre-inteligencia con el fin de abandonar la idea de la resolución de conflictos a posteriori. La implementación de la gestión de riesgo y la anticipación estratégica son fundamentales para los sistemas de inteligencia de la región.

En resumen, el segundo apartado presenta algunas discusiones focalizadas en los nuevos retos de la I.E. en la región suramericana, abordando aspectos teóricos y metodológicos que brindan perspectivas para un abordaje específico de la temática. El tercer y último apartado, está compuesto por tres artículos con visiones más críticas en torno a la I.E., que permiten una exploración un poco más profunda de la temática. Fredy Rivera presenta una reflexión histórica titulada "Inteligencia estratégica e inteligencia política: los claro-oscuros del caso ecuatoriano", en la que evidencia la influencia estadounidense en el desarrollo de la inteligencia estratégica en los países suramericanos. El autor advierte que las labores de inteligencia han estado unidas de forma inexorable a la labor política, argumentando que "la inteligencia era asumida como una herramienta estratégica de prevención y desarticulación de amenazas" (Bartolomé *et al*. 2016, 137) privilegiando los fines políticos y militares en torno a la construcción del enemigo.

La creación en 2009 en Ecuador de la Secretaría Nacional de Inteligencia (SENAIN) apartó a la inteligencia entendida como labor política heredera de la Guerra Fría. Sin embargo, en palabras de Rivera, esta concepción,apetecida por los gobiernos, retrasó en gran medida la especialización de los sistemas de inteligencia en el país y la región. Concluye el autor planteando la interrogante de cuál es el punto actual de la I.E. en Ecuador, si existen avances significativos o, por el contrario, si el país está presenciando el retroceso de la I.E.

En los dos artículos posteriores, se invita a reflexionar sobre una mirada epistemológica de la I.E., ya que hasta ahora sigue siendo entendida desde una visión totalmente anglosajona, lo cual genera una suerte de dependencia del sur hacia el norte. Se plantea, además, una discusión mucho más ontológica en términos de la ética de la inteligencia estratégica, estableciendo una relación entre conocimiento (entendido como información) y poder en las relaciones sociales, frente al tema que ocupa el texto entre Estado y sociedad.

En general, el libro presenta un buen espectro de la I.E. planteando desde las perspectivas más generales de exploración, hasta discusiones de orden epistémico sobre el abordaje de este tema. Es una publicación rica en ejemplos y casos de investigación, que representa una gran contribución al campo de estudio. Quienes participan en la producción de estos textos, desde sus puntos de vistas, muestran experticia en los temas trabajados, constituyendo la publicación como una herramienta de trabajo fundamental para los investigadores y estudiosos que quieren acercarse al tema de la I.E. Este texto es una nueva contribución al campo de la seguridad, las Relaciones Internacionales y los estudios estratégicos desde una perspectiva suramericana ajustada al contexto y la realidad que estos países atraviesan y afrontan, contemplando sus matices y los nuevos retos que cada vez se complejizan más.

Revista URVIO agradece a las siguientes personas por su colaboración
en la realización del presente número:

Alexis Colmenares

Andrés de Castro

Aracelly Camacho de Casanova

Carolina Sancho

Gilda Guerrero

Jenny Torres

Jorge Francisco Aguirre Sala

José Manuel Ugarte

Juan Ignacio Plaza

Juan Manuel R. Mosso

Lester Cabrera

Luis Octavio Coimbra

Manuel Gazapo

María de Vianey Peralta Buendía

María Eugenia Suárez de Garay

Nicolás Comini

Rafael Rodríguez Prieto

Verónica Barrios

Política Editorial

URVIO, Revista Latinoamericana de Estudios de Seguridad, es una publicación internacional especializada de FLACSO, sede Ecuador, fundada en el año 2007. La revista busca ser una herramienta de debate, actualización, investigación y consulta para académicos y decidores de políticas y opinión pública, tanto en Ecuador, como en América Latina y el mundo en general.

La revista URVIO es de publicación semestral. Cada número presenta un *dossier* enfocado en un tema específico relacionado con la problemática de la violencia y la seguridad en la región. Las demás secciones (misceláneos, reseñas, entrevistas) desarrollan diferentes temáticas en torno a la seguridad.

Las opiniones y comentarios expuestos en los trabajos son de responsabilidad estricta de las autoras y autores, y no reflejan la línea de pensamiento de FLACSO, sede Ecuador. Los artículos publicados en URVIO son propiedad exclusiva de FLACSO, sede Ecuador. Se autoriza la reproducción total o parcial de los contenidos siempre que se cite como fuente a URVIO, Revista Latinoamericana de Estudios de Seguridad.

Normas de publicación de URVIO

Las personas interesadas en escribir para URVIO, Revista Latinoamericana de Estudios de Seguridad, deberán subir su artículo a la plataforma de la revista y además, enviar una copia del documento a la dirección de correo electrónico:
revistaurvio@flacso.edu.ec, siempre respetando las siguientes normas:

1. El Comité Editorial de URVIO se reserva el derecho de decidir sobre la publicación de los trabajos, así como el número y la sección en la que aparecerán.
2. URVIO se reserva el derecho de realizar la corrección de estilo y los cambios editoriales que considere para mejorar el trabajo.
3. Las investigaciones y artículos de los autores y autoras deberán ser inéditos, escritos preferentemente en español y no estar aprobados o publicados en otras revistas.
4. Todos los artículos e investigaciones deben incluir un resumen en español e inglés, no mayor a 10 líneas (un párrafo donde se especifique los objetivos de trabajo y los contenidos), y un listado de palabras clave utilizadas. Esta norma no se aplica a la sección Reseñas.
5. Los títulos de los trabajos no podrán ser mayores a 10 palabras, y deberán estar traducidos al inglés.
6. Todos los trabajos deberán ser presentados en letra 12 Times New Roman, a espacio sencillo.
7. Todos los trabajos deberán ser enviados con una referencia del nombre de su autora o autor, grado académico, lugar de trabajo o adscripción académica. Además deberán incluir la fecha de envío y dirección de correo electrónico. Para citas y referencias bibliográficas, se deberá utilizar el Manual de Chicago Deusto.

8. Los artículos presentados para la sección Reseñas deben incluir toda la información bibliográfica del libro que se reseñe.
9. La extensión de los trabajos variará según las secciones:

Secciones	Extensión máxima	Extensión mínima
Tema Central	8000 palabras	5000 palabras
Misceláneo	8000 palabras	5000 palabras
Reseñas	2000 palabras	1500 palabras

Las referencias bibliográficas estarán acorde al Manual de Estilo Chicago Deusto, formato establecido en FLACSO Ecuador:

Estructura Básica de una cita en el cuerpo del texto

En el sistema autor-año, la referencia en el texto normalmente aparece entre paréntesis y contiene solo los dos primeros elementos que se hacen constar en la lista de referencias: el autor y el año de publicación, sin puntuación entre ellos. Además, se puede añadir el número de la página u otro elemento de localización, después de una coma. En ningún caso utilizar op. cit., ibid., ibídem.

Ejemplo:

(Cox 2010)
(Cox 2010, 91)

Entradas de la lista de referencias con el mismo autor o autores y el mismo año

Las obras de un mismo responsable (con independencia que sea autor, editor, compilador o traductor) y del mismo año se deben diferenciar con la edición de a, b, c, etc. y se ordenan alfabéticamente por el título. Las citas en el texto consignan el autor y el año con la letra.

Ejemplo:

Chaume Varela, Frederic. 2004a. Cine y traducción. Cátedra: Madrid
__ 2004b. "Modelos de Investigación en traducción audiovisual". *Íkala, Revista de lenguaje y Cultura* 9 (15): 351-365.
(Chaume Varela 2004b, 356)
(Chaume Varela 2004a, 45-46)

Orden cronológico para los nombres repetidos en una lista de referencias

Cuando se repite el autor (es), traductor(es), editor(es), o compilador(es) en varias entradas seguidas, el nombre (los nombres) se remplaza por una raya tras la primera aparición. No se escribe tras la raya el signo de puntuación que sigue habitualmente al elemento omitido (aquí, el punto). Las entradas se disponen cronológicamente por año de publicación en orden ascendente, no alfabetizadas por título. Los trabajos sin fechar (marcados como s. f.) o en prensa van después de los trabajos fechados.

Ejemplo:

Segura Munguía, Santiago. 2005. *Los jardines en la Antigüedad*. Bilbao: Universidad de Deusto.
__ 2007. *Diccionario por raíces del latín y de las voces derivadas*. Bilbao: Universidad de Deusto.
__ 2010. *Nuevo diccionario etimológico latín –español y de las voces derivadas.* Bilbao: Universidad de Deusto.

Libro de un autor o editor único

Ejemplo:

Duch, Lluís. 1998. *Mito, interpretación y cultura*. Barcelona: Harder
(Duch 1998, 99-100)

Libro de dos o tres autores

En el caso de libros con dos autores, en la lista de referencias solo se invierte el primer nombre:

Ejemplo:

León, Orfelio e Ignacio Montero. 1993. *Diseño de investigaciones: Introducción a la lógica de la investigación en psicología y educación.* Madrid: Mc Graw- Hill/ Interamericana de España.
(León y Montero 1993, 25)

Libro con tres autores

Ejemplo:

Borrego Nieto, Julio, José J. Gómez Asencio y Emilio Prieto de los Mozos.1986. *El subjuntivo. Valores y usos*. Madrid: SGEL.
(Borrego Nieto, Gómez Ascencio y Prieto de los Mozos 1986)

Más de cuatro autores

Si el libro tiene cuatro o más autores, se incluye a todos ellos en la entrada de referencias (bibliografía). El orden y la puntuación son los mismos que en el caso de los libros con dos o tres autores. En el texto, sin embargo, se da el apellido del autor que aparece en primer lugar, seguido de et al.

Ejemplo:

(Lago et. al. 2008, 118-19)

Libro publicado electrónicamente

Si el libro está disponible en más de un formato, citen la versión con la que han trabajado. En los libros consultados en línea hay que añadir el URL.

Libro electrónico obtenido de una biblioteca o librería

Muchos libros editados electrónicamente pueden tener un equivalente impreso. Pero dada la posibilidad de que existan diferencias, aconsejamos indicar el formato en el que lo han consultado.

Ejemplo:

Austen, Jane. 2008. *Pride and Prejudice*. Nueva York: Penguin Classics. Edición en PDF. URL.

Capítulo de un libro

Ejemplo:

Gómez Mendoza, Josefina. 2009. "Ecología urbana y paisaje en la ciudad". En *La ciudad del futuro*, editado por Antonio Bonet Correa, 177-217. Madrid: Instituto de España.

Artículos de revista científica

Los elementos que deben constar en la entrada son los siguientes: Nombre complete del autor o autores, año de publicación, título y subtítulo del artículo, nombre de la publicación periódica,

información sobre volumen, número, fecha; indicación de la página cuando es necesario, incluir el URL o el DOI cuando estén disponibles.

Ejemplo:

Bernárdez, Enrique. 2000. "Estrategias constructivistas de la descripción oral". *Revista Española de Lingüística* 30 (2): 331-356.

Artículo en periódicos y magacines en la lista de referencias

Ejemplo:

Lafuente, Javier.2015. "Venezuela da la espalda al chavismo". *El País*, 7 de diciembre. http://internacional.elpaís.com/internacional/2015712/077america/1449454340_373673.html.

Artículo sin firma tomado de periódicos o magazine en internet

Ejemplo:

Mundo Diner. 2014. "Japón, una nación que combina la modernidad con tradiciones y costumbres ancestrales". 29 de diciembre de 2014. http://www.revista-mundodiners.com/?p=4509

Documentos electrónicos en página web

Ejemplo:

Senescyt. 2011. "Becas docentes universitarios", http://programasbecas.educacionsuperior.gob.ec/becas-para-docentes-universitarios/.

Ponencia presentada en un seminario, conferencias y otros

Ejemplo:

Castro Gómez, Santiago. 2013. "El Dasein como Design: sobre el concepto de antropotécnica en Peter Sloterdijk". Ponencia presentada en el *Coloquio Poder, vida y subjetivación*, Universidad Nacional, Bogotá, 14 de abril.

Tesis, tesinas

Ejemplo:

Black, John. 1999. "The making of an Indigenous Movement". Tesis de maestría, Universidad de Nuevo México.

Normas jurídicas

Las normas jurídicas se citan indicando los siguientes elementos: tipo de norma, número y fecha 8 empezando por el año, separado del número por una barra9, seguidos, sin espacio intermedios, del día y el mes entre comas, nombre completo de la norma tal y como figura en la publicación original; lugar y fecha de publicación. Al citar las más habituales para cada área se puede incluir, ya en la primera mención, sea en el cuerpo del texto o en la nota, la abreviatura por la que se la mencionará en las siguientes citas.

Ejemplo:

Ley Orgánica 8/ 1980, de 22 de septiembre, de Financiación de las Comunidades Autónomas (BOE núm.236 de 1 de octubre de 1980), a partir de ahora LOFCA. Ley 14/2007, de 26 de noviembre, del Patrimonio Histórico de Andalucía (BOJA núm. 248 de 19 de diciembre de 2007).

Entrevistas inéditas y comunicaciones personales

Ejemplo:

Nombre real o ficticio (cualquier elemento identificativo relevante al contexto de la entrevista: ejemplo cargo/ocupación/residencia), día, mes y año. No tiene que estar la entrevista en bibliografía. Con su entrada en el texto es suficiente.

(Manuela Ambas, Barrio Miraflores, Perú, 2 septiembre 2010).
(Manula Ambas, entrevista, 2 septiembre 2010)

Respecto a siglas, la primera vez que aparezcan deberá escribirse su significado completo y su sigla entre paréntesis, luego solamente la sigla.

Código de ética

El Consejo Editorial y el Comité Asesor Internacional de URVIO, Revista Latinoamericana de Estudios de Seguridad, velarán que editores, revisores pares y autores respeten los principios éticos durante todas las fases del proceso editorial. A continuación, detallamos nuestras normas.

Sobre autores y autoría:

- Los artículos que envíen a URVIO deben **ser originales e inéditos**.
- **Abstenerse del envío múltiple/repetitivo** de artículos a publicaciones o editoriales diferentes. Ésta es una conducta reprobable en la difusión de investigaciones académicas.
- Respeto a las **fuentes originales** que consulta en su artículo. Las referencias bibliográficas deben estar señaladas de manera correcta y completa.
- **Errores en los artículos publicados**. Cuando el autor/a identifica en su trabajo un error o inexactitud, deberá informar al equipo editorial de URVIO y facilitarle la información necesaria para las correcciones.
- Se comprometen a **revisar la literatura académica más actual y prominente** sobre el tema que investigan.
- **Ordenar la firma autoría de acuerdo al nivel de responsabilidad e implicación** en el artículo.

Sobre revisores pares:

- **Informar si existen conflictos de intereses**. Cuando un evaluador o revisor tenga alguna opinión o interés de tipo personal o financiero que pudiera afectar su objetividad en su evaluación, debe abstenerse de participar en el proceso editorial.
- **Anonimato**. Los revisores nunca conocerán a los/as autores/as (solo a través del código del OJS) y tampoco tendrán conocimiento sobre la identidad del otro par ciego.
- **Confidencialidad**. Una vez terminado el proceso evaluativo, el revisor se abstendrá de divulgar lo leído a agentes externos a URVIO.
- **Respeto de los tiempos pactados con la revista**. El revisor tiene la responsabilidad de notificar a los editores en caso de existir inconvenientes para entregar la evaluación a tiempo.

Sobre responsabilidad de los editores:

- **Honestidad**. Garantizar la transparencia en los procesos de evaluación, edición y publicación de cada número.
- **Confidencialidad**. El equipo editorial mantendrá el anonimato entre revisores y autores durante todo el proceso.
- **Responder inquietudes vía correo electrónico**. Las consultas y aclaraciones solicitadas por autores, revisores o cualquier persona interesada en URVIO serán contestadas con prontitud.
- **Facilitar rectificaciones**. Se publicarán correcciones o aclaraciones correspondientes a través de la página web de la revista.
- **Difusión**. El número publicado se difundirá a repositorios, bases de datos y redes sociales.
- **Proceso de publicación**. Los editores seleccionarán con apreciación crítica a los revisores más capaces.

ÍCONOS 58
REVISTA DE CIENCIAS SOCIALES

Año 21
No. 58
Mayo de 2017
Cuatrimestral

Número anterior:
ICONOS 57: Pensamiento social latinoamericano y caribeño

Número siguiente:
ICONOS 59: Etnografías experimentales: repensar el trabajo de campo

Íconos. Revista de ciencias sociales está incluida en los siguientes índices científicos: Academic Search Premier, Directory of Publishing Opportunities (CABELL'S), Clasificación Integrada de Revistas Científicas (CIRC), Citas Latinoamericanas en Ciencias Sociales (CLASE), DIALNET, Directory of Open Access Journal (DOAJ), Emerging Source Citation Index (ESCI) Web of Science Thomson Reuters, FLACSO Andes, Fuente Académica Plus, Hispanic American Periodical Index (HAPI), International Bibliography of the Social Science (IBSS), Informe Académico Thompson Gale, International Institute of Organized Research (I2OR), LatAm-Studies, LATINDEX-catálogo, MIAR, Political Science Complete, REDALYC, REDIB, Sociological Abstracts, Social Science Jornals. Sociology Collection, Ulrich's Periodical Directory, Worldwide Political Science Abstracts (WPSA).

FLACSO ECUADOR

Revista de la Facultad Latinoamericana de Ciencias Sociales - Sede Ecuador

Información y colaboraciones: (revistaiconos@flacso.edu.ec)
Revista Íconos: www.revistaiconos.ec

mundosplurales

Revista Latinoamericana de Políticas y Acción Pública • ISSN: 1390-9193
Volumen 3 • Número 2 • noviembre 2016

Vol. 3 / Nº 2

FLACSO ECUADOR

Encuéntrela en: http://www.flacsoandes.edu.ec

EUTOPÍA-10

Revista de Desarrollo Económico Territorial - N.º 10 - diciembre 2016

TERRITORIOS RURALES: ENTRE CRISIS Y PERSPECTIVAS DE DESARROLLO

ISSN: 1390 5708
Disponible en: http://revistas.flacsoandes.edu.ec/eutopia/index

FLACSO ECUADOR