

URVIO

Revista Latinoamericana de Estudios de Seguridad



Amenazas híbridas

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 - Diciembre 2019 - No. 25

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.
- SciELO Ecuador. Biblioteca electrónica.
- Redalyc. Red de Revistas Científicas de América Latina y el Caribe, España y Portugal.
- 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 25, diciembre de 2019
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>

Información estadística sobre tasas de aceptación e internacionalización en Urvio #25

- Número de trabajos recibidos: 11 manuscritos.
- Número de trabajos aceptados publicados: 7.
- Índice de aceptación de manuscritos: 63,63%
- Índice de rechazo de manuscritos: 36,36%.
- Número de revisores internacionales: 22
- Número de revisores nacionales: 2
- Número total de revisores por países: 6 (Argentina, Colombia, México, Chile, España y Ecuador).
- Internacionalización de autores: 4 países (Argentina, España, Costa Rica y México).

Redes sociales

 @revistaurvio

 @revista_URVIO

 Blog: <https://revistaurvio.wordpress.com/>

 Academia.edu: <https://flacso.academia.edu/RevistaUrvio>



FLACSO
ECUADOR



RELASEDOR
*Red Latinoamericana de Análisis de Seguridad
y Delincuencia Organizada*

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.

Editor Jefe (Editor in Chief)

Doctor Fredy Rivera Vélez, Facultad Latinoamericana de Ciencias Sociales (FLACSO), sede Ecuador

Editor Asociado (Associate Editor)

- Dra. Grace Jaramillo, University of British Columbia, Canadá.
- Mg. Liosday Landaburo Sánchez, Facultad Latinoamericana de Ciencias Sociales (Flacso), sede Ecuador.

Asistente Editorial

Mg. Martin Scarpacci, Universidad Federal de Río de Janeiro, Brasil

**Consejo Científico Internacional
(International Scientific Council)**

- Dra. Adele Norris, University of Waikato, Nueva Zelanda.
- Dr. Alejandra Otamendi, Universidad de Buenos Aires, Argentina.
- Dr. Gustavo Díaz Matey, Universidad Complutense de Madrid, España.
- Dra. Sara Makowski Muchnik, Universidad Autónoma Metropolitana, Unidad Xochimilco, México.
- Dr. Marco Cepik, Universidad Federal de Rio Grande do Sul (UFRGS), Brasil.
- Dra. Julia Pulido Gragera, Universidad Europea de Madrid, España.
- Dr. Markus Gottsbacher, Universidad de Viena, Austria.
- Dr. Andrés de Castro García, University of Kurdistan Hewler, Iraq.
- Dr. Daniel Pontón, Instituto de Altos Estudios Nacionales, Ecuador.
- Dr. Haluk Karadag, Universidad de Baskent, Turquía.

**Consejo Internacional de Revisores
(International Review Board)**

- Dr. Geoffrey Pleyers, Universidad de Lovaina, Bélgica.
- Dr. Marco Méndez, Universidad Nacional de Costa Rica, Costa Rica.
- Dra. Karina Mouzo, Instituto de Investigaciones Gino Germani, Universidad de Buenos Aires, Argentina.
- Dr. Cristián Doña-Reveco, University of Nebraska at Omaha, Estados Unidos.
- Dra. Ana J. Bengoa, Universidad de Valparaíso, Chile.
- Dra. Gracia M. Imberton, Universidad Autónoma de Chiapas, México.
- Dr. Guillem Colom, Universidad Pablo de Olavide, España.
- Dr. Carlos Brito, Universidad Complutense de Madrid, España.
- Mg. Nicolás Alvarez, Center for Higher National Studies, Ministry of Defense, Uruguay.
- Dr. Lester Cabrera, Facultad Latinoamericana de Ciencias Sociales (Flacso), Ecuador.
- Dr. Iván Poczynok, Universidad de Buenos Aires, Argentina.

- Dra. Carolina Sancho, Universidad Autónoma de Chile, Chile.
- Dra. Ainhoa Vázquez, Universidad Nacional Autónoma de México (UNAM), México.
- Dra.(c) Nelly E. Reséndiz, Universidad Nacional Autónoma de México (UNAM), México.
- Dr.(c) Daniel Sansó-Rubert, Universidad de Santiago de Compostela, España.
- Dra. Laura Loeza, Universidad Nacional Autónoma de México (UNAM), México.
- Dra. María Eva Muzzopappa, Universidad Nacional de Río Negro, Argentina.
- Dra. Rut Diamint, Universidad Torcuato Di Tella, Argentina.
- Dra.(c) Liudmila Morales Alfonso, Universidad de Salamanca, España.
- Dr. Juan Antonio Rodríguez, Universidad de los Andes, Venezuela.
- Dra.(c). Viviana García Pinzón, Universidad de Marburg, Alemania.
- Dra. Jenny Torres Olmedo, Escuela Politécnica Nacional, Ecuador.
- Dra. Tania Rodríguez Morales, Universidad de Santo Tomás, Colombia.
- Dra. Alma Trejo Peña, Universidad Nacional Autónoma de México (UNAM), México.
- Dr. Juan Carlos Sandoval, Universidad de Alicante, España.
- Dra. Alice Martini, Scuola Superiore Sant'Anna, Italia.
- Dra. Evelyn Louyse Godoy Postigo, Universidade Federal de São Carlos, Brasil.
- Dr. Pedro Díaz Polanco, Universidad Austral, Chile.
- Dr. Freddy Crespo, Universidad de los Andes, Venezuela.
- Dra. Rita Gradañlle Pernas, Universidad de Santiago de Compostela, España.
- Mg. Alejandro Romero Miranda, Universidad La República, Chile.
- Dr. Sergio Gabriel Eissa, Universidad de Buenos Aires, Argentina.
- Dr. Luis Ignacio García Sigman, Universidad de Belgrano, Argentina.
- Dr(c). Luiz Coimbra, Organización de Estados Americanos (OEA), Estados Unidos.
- Dra. Beverly Estela Castillo Herrera, Universidad Nacional Autónoma de Nicaragua.
- Dr. Sergio Salazar Araya, Universidad de Costa Rica.
- Dra. Mariana Albuquerque Dantas, Universidade Federal Rural de Pernambuco, Brasil.
- Dr. Johan Avendaño Arias, Universidad Nacional de Colombia.
- Dra. Roberta Camineiro Baggio, Universidade Federal do Rio Grande do Sul, Brasil.
- Dra. María Eugenia Suárez de Garay, Universidade de Guadalajara, México.

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELA SEDOR)
y FLACSO Sede Ecuador

ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

Tema central

- Amenazas y conflictos híbridos: características distintivas,
evolución en el tiempo y manifestaciones preponderantes. 8-23
Mariano Bartolomé
- Hechos ciberfísicos: una propuesta de análisis para ciberamenazas
en las Estrategias Nacionales de Ciberseguridad 24-40
Juan-Manuel Aguilar-Antonio
- Reconceptualizando la relación entre tecnología, instituciones y guerra 41-56
Alfredo-Leandro Ocón y Aureliano da Ponte
- El componente social de la amenaza híbrida y
su detección con modelos bayesianos 57-69
Ana-María Ruiz-Ruano, Jorge López-Puga y Juan-José Delgado-Morán

Misceláneo

- Narcomenudeo y control territorial en América Latina. 71-86
Sebastián Saborío
- La Guardia Nacional y la militarización de la seguridad pública en México 87-106
Gerardo Hernández y Carlos-Alfonso Romero-Arias

Estudios Globales

- El tratamiento informativo de la guerra híbrida de Rusia 108-121
Javier Miguel-Gil
- Política editorial. 122-140

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELA SEDOR)
y FLACSO Sede Ecuador

ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

Central topic

- Hybrid Conflicts and Threats: Main Features, its Evolution
across Time and Preponderant Forms 8-23
Mariano Bartolomé
- Cyber-physical Facts: A Proposed Analysis for Cyber Threats
in the National Cybersecurity Strategies 24-40
Juan-Manuel Aguilar-Antonio
- Reconceptualizing the Relationship between Technology, Institutions and War 41-56
Alfredo-Leandro Ocón y Aureliano da Ponte
- The Social Component of the Hybrid Threat and its
Detection with Bayesian Models 57-69
Ana-María Ruiz-Ruano, Jorge López-Puga y Juan-José Delgado-Morán

Miscellaneous

- Small Scale Drug Trafficking and Territorial Control in Latin America 71-86
Sebastián Saborío
- The National Guard and the militarization of public security in Mexico 87-106
Gerardo Hernández y Carlos-Alfonso Romero-Arias

Global Studies

- The Informative Treatment of the Russian Hybrid War 108-121
Javier Miguel-Gil
- Política editorial 122-140

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELA SEDOR)
y FLACSO Sede Ecuador

ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

Tema central

- Ameaças e conflitos híbridos: características distintivas, evolução
ao longo do tempo e manifestações predominantes. 8-23
Mariano Bartolomé
- Fatos ciber-físicos: uma proposta de análise para ameaças cibernéticas
nas Estratégias Nacionais de Segurança Cibernética 24-40
Juan-Manuel Aguilar-Antonio
- Reconceituando a relação entre tecnologia, instituições e guerra 41-56
Alfredo-Leandro Ocón y Aureliano da Ponte
- O componente social da ameaça híbrida e sua detecção com modelos bayesianos 57-69
Ana-María Ruiz-Ruano, Jorge López-Puga y Juan-José Delgado-Morán

Diversos

- Varejo de drogas e controle territorial na América Latina 71-86
Sebastián Saborío
- A Guarda Nacional e a militarização da segurança pública no México 87-106
Gerardo Hernández y Carlos-Alfonso Romero-Arias

Estudos Globais

- O tratamento informativo da Guerra híbrida russa 108-121
Javier Miguel-Gil
- Política editorial. 122-140



Tema central

Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes

Hybrid Conflicts and Threats: Main Features, its Evolution across Time and Preponderant Forms

Mariano Bartolomé¹

Recibido: 16 de julio de 2019

Aceptado: 30 de septiembre de 2019

Publicado: 2 de diciembre de 2019

Resumen

Dentro del campo de análisis de la seguridad internacional contemporánea, ocupa un lugar de importancia la “hibridación” de los conflictos armados y las amenazas transnacionales, cuestión que demanda la constante atención de los especialistas. El presente artículo aborda tanto la amenaza que constituye un actor que plantea modos de combate híbridos como la resultante de la combinación sinérgica de al menos dos amenazas diferentes, que pueden darse de manera autónoma. Se presenta un panorama actualizado sobre el tema, que refleja su estado del arte, incluyendo versiones ajenas a Occidente. El primer objetivo consiste en establecer dónde radica la singularidad de los conflictos híbridos respecto a las formas precedentes de contienda armada, subsanando así los inconvenientes que plantean tanto un empleo poco riguroso de los términos como cierta proliferación semántica. El segundo objetivo, complementario del primero, apunta a identificar los formatos más relevantes que adoptan las amenazas híbridas en la actualidad. Las conclusiones indican si se registra la presencia de conflictos y amenazas híbridas en América Latina, y en caso afirmativo, cuáles son sus manifestaciones, así como el grado de preparación de los Estados frente a ellas.

Palabras clave: amenazas híbridas; amenazas transnacionales; conflictos armados; conflictos híbridos; guerra híbrida; seguridad internacional

Abstract

In the field of contemporary international security, the “hybridization” of armed conflicts and transnational threats has a high level of priority, demanding constant attention from specialists. This article analyzes threats coming from actors that choose hybrids ways of warfare, and also

¹ Universidad del Salvador (USAL), Argentina, mariano.bartolome@usal.edu.ar,  orcid.org/0000-0002-6409-0880



the combination of at least two different and autonomous threats. An updated framework about this issue, which reflects the state of the art, including nonwestern views, is presented. The first objective is to identify the singularity of hybrid conflicts, and its differences with previous forms of armed conflicts, fixing the problems produced both by an unrestricted use of concepts and certain semantic proliferation. The second objective, which complements the former, seeks to identify the most common expressions of hybrid threats in today's international relations framework. The conclusions address if hybrid conflicts and threats are present in Latin America and, in an affirmative case, what is the degree of preparation of the States to fight these problems.

Key words: armed conflicts; hybrid conflicts; hybrid threats; hybrid wars; international security; transnational threats

Introducción

Desde hace casi tres lustros, la cuestión de la “hibridación” de los conflictos armados ocupa un lugar de importancia dentro del campo de análisis de la seguridad internacional, entendido como un recorte disciplinar de las Relaciones Internacionales cuyo objeto de estudio son las amenazas que se ciernen sobre los actores del sistema internacional, y los efectos que esta situación genera (Bartolomé 2017). De forma aún más específica, el tema adquirió particular relevancia en el marco de los contrapuntos sobre la fisonomía de los conflictos armados contemporáneos, área de incumbencia específica de la polemología, que no es otra cosa que “el estudio objetivo y científico de la guerra como fenómeno social susceptible de observación” (Bouthoul 1984, 60). Precisamente, la fisonomía de los conflictos armados constituye una de las cuestiones centrales de la agenda

de la seguridad internacional contemporánea, cuyos contenidos se ampliaron a lo largo de las últimas décadas, como correlato directo de los impactos recibidos desde la teoría de las Relaciones Internacionales (Bartolomé 2016). Comparten esa prioridad temática, en un listado no exhaustivo, la solidez institucional del Estado, las mal llamadas “nuevas amenazas” y la legitimidad de las intervenciones armadas individuales o colectivas (Bartolomé 2018).

El concepto de hibridación rápidamente se hizo extensivo al estudio de las amenazas, aunque en este caso su uso registra escaso rigor metodológico y cierta ambigüedad. Por un lado, la referencia apunta a la heterodoxa forma de conflicto que plantea un eventual oponente que abandona los cánones tradicionales e integra diversas formas de combate. En ese sentido, como se verá con mayor detalle en pasajes posteriores, a mediados del decenio pasado la organización chiíta libanesa *Hezbollah* constituyó (y probablemente continúa siendo) una amenaza híbrida para Israel y su aparato militar. Por otra parte, la amenaza puede ser híbrida en sí misma, en función de sus características intrínsecas, con independencia de su circunstancial protagonista. *A priori*, puede decirse que una amenaza híbrida combina, en cierto grado, características propias de al menos dos amenazas en su formato “puro”, o de una amenaza en estado puro y otro fenómeno o situación, de ribetes claramente diferenciados.

Con este breve marco contextual, el presente artículo aborda la cuestión de las amenazas híbridas en su doble acepción: como amenaza que constituye un actor que plantea modos de combate de ese tipo (*v.g.* amenaza de conflicto híbrido), y como amenaza cuyas características resultan de algún tipo de combinación entre al menos dos amenazas diferentes, que pueden presentarse de manera

autónoma, o de al menos una amenaza y un fenómeno de otro tipo.

El propósito del texto consiste en presentar un panorama actualizado sobre el tema, que refleje su estado del arte, incluyendo versiones ajenas a Occidente, surgidas al calor de otras circunstancias históricas y culturales. En concreto, se propone como primer objetivo establecer dónde radica la singularidad de los conflictos híbridos respecto a las formas precedentes de contienda armada, subsanando así los inconvenientes que plantean tanto un empleo poco riguroso de los términos como cierta proliferación semántica. El segundo objetivo, complementario del primero, consiste en identificar los formatos más relevantes que adoptan las amenazas híbridas en la actualidad.

El artículo se estructura en dos partes principales, además de esta introducción. En la primera parte se describirán las características iniciales de los conflictos híbridos, y la evolución del concepto hasta la adopción de nuevos formatos. En la segunda se atenderán las amenazas cuyas características resultan de la combinación sinérgica de al menos dos amenazas diferentes, que pueden presentarse de manera autónoma. Los niveles de análisis del texto fluctúan entre los planos descriptivo y explicativo; se basan en información cualitativa y las fuentes empleadas son todas de tipo secundario.

Una aproximación a los conflictos híbridos y su evolución

La bibliografía existente considera a los denominados conflictos híbridos como fenómenos dotados de características particulares, que constituyen un estadio relativamente reciente en el marco de un proceso evolutivo del con-

flicto armado a lo largo del tiempo, en el cual este muda su fisonomía. Recurriendo a un cliché de uso recurrente, los conflictos híbridos expresan una “metamorfosis de la violencia” que irrumpe en el escenario internacional en el año 2006, momento en que sus rasgos son suficientemente nítidos para permitir su identificación y la consecuente elaboración de una tipología. La ocasión para esa novedad fue la llamada Segunda Guerra del Líbano, denominación que se aplica usualmente a la Operación Recompensa Justa, ejecutada por Israel contra la organización chiíta *Hezbollah* en suelo libanés. Sin embargo, antes de ese acontecimiento, especialistas estadounidenses ya estimaban que cualquier actor que en el futuro quisiera enfrentarse en el plano armado a la superpotencia, debería echar mano a inusuales combinaciones de tecnologías y tácticas, para compensar, en parte, la abrumadora superioridad del oponente (Bartolomé 2016).

Los estudios pioneros de Hoffmann (2007, 38) sobre el caso libanés conceptualizaron como guerra híbrida a “una combinación de la letalidad de la guerra estatal con el fanatismo de la guerra irregular”. En otras palabras, a la conjunción de modos de combate clásicos e irregulares, por parte de actores no estatales, en su enfrentamiento con instrumentos militares más poderosos, con el objetivo de lograr efectos favorables, no solo físicos, sino también psicológicos.

En análisis ulteriores, le autor opinó que la tipificación de ciertas contiendas armadas como asimétricas es insuficiente y engañosa. Se asemejaría más a lo que se concibe como un conflicto multimodal, en el que al menos uno de los contendientes utiliza de forma simultánea y complementaria los formatos asimétricos y simétricos, en aras de una mayor letalidad de sus acciones (Hoffmann 2009). De esa lectu-

ra merece subrayarse no solo la idea de multimodalidad, sino la clara diferenciación entre conflictos asimétricos y conflictos híbridos asociada con ella, pues en los primeros el armamento sofisticado y la tecnología avanzada suelen estar monopolizados por el protagonista estatal, mientras la contraparte, al decir de Münkler (2003, 18), encontró su símbolo en un vehículo civil, la *pick-up* Toyota. La diferenciación entre conflictos híbridos y asimétricos resulta fundamental en términos analíticos, pues permite subsanar el error en el cual incurren algunos analistas, que entienden que se aplican denominaciones diferentes para hacer referencia a la misma cosa (García 2013).

Así, la guerra híbrida nos muestra una doble faz. Por un lado, procura fusionar la letalidad de los conflictos interestatales con el fervor de las guerras irregulares. Por el otro, exhibe mayor velocidad y letalidad que las guerras irregulares del pasado, debido a la difusión de tecnologías avanzadas (Tello 2013). En ese sentido, la visión de Colin Gray (2004, 131) fue premonitory, al advertir, años antes de la Segunda Guerra del Líbano, que la alta volatilidad que caracterizaría a los conflictos armados del Siglo XXI obedecería a la combinación de nuevas tecnologías y ancestrales divisiones religiosas y étnicas.

También en este caso surgieron lecturas de los conflictos híbridos alternativas a la original, esbozada por Hoffman. Una de ellas incorpora dentro de sus características centrales a la criminalidad organizada, entendiendo que esta novedad, sumada al empleo de tecnologías avanzadas, marcaría una diferencia nítida con otras formas de conflicto en el pasado. En síntesis, tomando como referencia los avances doctrinarios estadounidenses (plasmados en el año 2011), serían conflictos en los que “al menos uno de los contendientes combina

operaciones convencionales, guerra irregular, acciones terroristas y conexiones con el crimen organizado” (Schnauffer 2017, 18). Otra lectura de conflictos híbridos alude, bajo esa idea, a episodios armados que tienen una doble dimensión regional e interna, en referencia a inestabilidades y tensiones entre Estados que se inflaman por la violencia subestatal originaria de uno de ellos, la cual se expande a través de las fronteras. Por ejemplo, cuando flujos transfronterizos de migrantes, bienes ilícitos o combatientes irregulares generados en un país agravan la crisis en otro (Scheier 2008).

El planteo de este especialista estadounidense es particularmente interesante, pues abre la puerta a considerar híbridos aquellos conflictos expresados en diferentes niveles de agregación geográfica, que parten del plano local y pueden llegar (al menos teóricamente) al global. Así, inesperadamente se combinan los conceptos de hibridez y glocalidad, neologismo este que refiere a un escenario local que registra el efecto de las múltiples interconexiones con el plano global. Sería híbrido, entonces, un conflicto como el sirio, precisamente calificado de glocal por incluir entre sus principales elementos las pujas entre clanes tradicionales; las cuestiones petroleras; una lógica revolucionaria anti-Assad; elementos salafistas procedentes de Occidente; rivalidades históricas entre sunnitas y chiítas, y yihadismo global (Liogier 2017).

Entre las interpretaciones de los conflictos híbridos alternativas a la original, la que más ha perdurado y en mayor medida se ha profundizado sostiene que, más allá de la violencia física, estos acontecimientos pueden expresarse en varios planos simultáneos, entre ellos el económico, legal, cibernético, comunicacional y mediático. Sobre la relevancia de los dos últimos, oportunamente ha

dicho John Gray (2004, 109) que “el ataque contra las Torres Gemelas demuestra que Al Qaeda entiende que las guerras del siglo XXI son pugilatos espectaculares en los que la difusión mediática de las imágenes constituye una estrategia capital”. Por otra parte, resultan el componente clave de procesos comunicativos conformados según una posición o conducta que el emisor desea que adopte el receptor, actuando sobre su intelecto y emociones (Pizarroso Quintero 2004). En ese contexto, ocupan un lugar central tanto la creación de “empatía moral” (Ignatieff 1999) como la “fabricación de consenso” (Torres Soriano 2011) en el público seleccionado.

Como se ha planteado en otras oportunidades (Bartolomé 2017), la incorporación de los planos comunicacional y mediático a los nuevos formatos de conflicto híbrido implica su vinculación con las llamadas Guerras de Cuarta Generación (4GW, por sus siglas en inglés), cuyas primeras teorizaciones datan de la década de 1980. En esencia, refieren a conflictos que reconocen muchas de las características que signan a las Nuevas Guerras, incluyendo su asimetría, su carácter difuso y su asincronía; pero a diferencia de ellas, les otorgan una especial importancia a las operaciones psicológicas y al manejo de los medios masivos de comunicación. Ese énfasis permaneció vigente tras la actualización teórica que se produjo luego de los atentados terroristas del 11S y las campañas militares de Afganistán e Irak, primeros jalones de la así llamada Guerra contra el Terrorismo. Esto ratificó que el uso de los medios de comunicación y las redes informáticas ocupa un lugar central en la transmisión de mensajes a distintos segmentos de una audiencia que se sabe fragmentada.

En cuanto al plano cibernético, cabe destacar que un conflicto híbrido por excelencia,

desde el momento en que combina entornos y daños reales y virtuales, es la llamada ciber guerra, definible de manera simplificada como “un conflicto bélico en el que el ciberespacio y las tecnologías de la información son el escenario principal” (Quintana 2016, 42). Respecto a las formas tradicionales de combate, las ciber guerras imponen cuatro importantes novedades. La primera de ellas es que el campo de batalla es el ciberespacio. Aunque el uso común del término refiere al entorno virtual de información e interacciones entre las personas, en sentido estricto refiere a un “dominio global y dinámico compuesto por infraestructuras de tecnología de información, las redes y los sistemas de información y telecomunicaciones” (Quintana 2016, 45). Tal vez de manera algo exagerada, Kissinger (2016, 347) indica que este dominio ha colonizado el espacio físico, aunque sin dudas acierta al indicar que se ha vuelto estratégicamente indispensable, y que demanda un nuevo cuerpo teórico y doctrinario, abocado a la forma y al grado de las respuestas “cinéticas” a agresiones cibernéticas.

La segunda novedad de las ciber guerras apunta a su formato en red, que refiere tanto a una forma de actuar como de organizarse, valiéndose de las posibilidades que proporciona la tecnología. Un tercer hecho novedoso apunta a la incorporación de actores de diferente tipo. El cuarto y último tiene que ver con la forma de lucha, que suele priorizar el ataque a las llamadas infraestructuras críticas, es decir, “sistemas, máquinas, edificios o instalaciones relacionados con la prestación de servicios esenciales” (Quintana 2016, 95). En rigor de verdad, la heterogeneidad de actores involucrados también es una nota distintiva de las Nuevas Guerras, por lo que puede decirse lo mismo de los formatos en red respecto al fenómeno terrorista.

Simultáneamente a la incorporación de nuevas dimensiones, la renovada perspectiva sobre conflictos híbridos dejó de lado el supuesto implícito según el cual, en el contexto de una contienda, la multimodalidad corre por cuenta de un actor no estatal, o lo que es lo mismo, se consideró que un Estado también podía articular sus recursos y capacidades de manera tal que pueda proponer una forma híbrida de conflicto a un eventual oponente. Más aun, se planteó que las formas evolucionadas de conflicto híbrido serán libradas predominantemente por Estados o entidades tras las cuales se registra un sólido respaldo estatal, habida cuenta de las elevadas capacidades (sobre tecnológicas) que demanda su aplicación, así como la sólida organización con que debe contarse para planificarlo y conducirlo (Sánchez Erráes 2014). Desde la perspectiva de Occidente, además del Estado Islámico (*Daesh*) específicamente en lo atinente a la multidimensionalidad del conflicto, casos principales en ese sentido serían Rusia, a partir de su accionar respecto a Crimea y el oriente de Ucrania, y China, en su exterior cercano, particularmente en su frente marítimo.

El carácter híbrido del conflicto armado que planteó desde el comienzo el Estado Islámico es claro. Como ya se explicó en detalle (Bartolomé 2017), aplicó diferentes formas de combate, en una gama que abarcó desde ataques terroristas de baja sofisticación perpetrados contra la ciudadanía en general (particularmente en Europa), por “lobos solitarios”, pasando por actos terroristas a gran escala, hasta formas de combate convencionales que incluyeron el empleo de unidades de infantería motorizada y mecanizada, caballería blindada y artillería pesada. La compleja maquinaria bélica de esta organización llegó a contar con hasta 40 000 efectivos, en su gran

mayoría exsoldados profesionales iraquíes y sirios, con experiencia de combate.

Al mismo tiempo, el Estado Islámico incurrió en prácticas propias de la criminalidad organizada, al comercializar en los mercados ilegales “antigüedades de sangre”, en referencia a piezas arqueológicas y libros antiguos pertenecientes al patrimonio cultural de Irak y Siria, para financiar su lucha armada y otras actividades de la entidad (Bartolomé y Anguita Olmedo 2019). Finalmente, se valió de internet, YouTube y las redes sociales como herramientas de propaganda, en una suerte de “yihadismo digital” (Avilés Farré 2017, 207) que incluyó terribles escenas de violencia perpetrada contra propios y ajenos. En el contexto de la actual vorágine informativa, la difusión de esos contenidos ha sido explicada como una “propaganda del miedo”, diseñada para captar la atención de la audiencia global de manera mucho más efectiva que los sermones religiosos (Napoleoni 2015, 19).

Aun antes de la derrota de Estado Islámico como entidad territorial, acontecimiento que tendría lugar en marzo de 2019 con la caída de su último baluarte en Siria (la aldea de Baghouz), los especialistas descartaron su desaparición definitiva, vaticinando una nueva hibridación de la organización, en este caso hacia formatos plenamente terroristas (Avilés Farré 2017).

Al contrario que en el asunto del Estado Islámico, las referencias a China y Rusia se relacionan con estrategias estatales de hibridación de conflictos, echando mano a recursos heterogéneos. Esas estrategias involucraron acciones en el límite de lo permitido por el Derecho Internacional, a la vez que incluyeron formatos reñidos con los tiempos de paz, todo lo cual invita a replantear el contenido y los límites del concepto de paz vigente (Mora-

les Morales 2017). La rusa ha sido caratulada como una novedosa versión de guerra no lineal, signada por dos características. Por un lado, su ya referido desarrollo simultáneo en los planos legal, económico, comunicacional, cibernético y mediático (Schnauffer 2017). Por otro, la deliberada creación de confusión y fragilidad en los adversarios, a través de campañas psicológicas sustentadas en herramientas tecnológicas de avanzada. También es conocida como doctrina Gerasimov, en referencia a quien habría sido su creador, el actual jefe del Estado Mayor de las Fuerzas Armadas rusas, y a los contenidos de su discurso pronunciado en enero de 2013 ante la Academia de Ciencias Militares.

Este personaje describe la nueva forma de guerra como “un medio para alcanzar la dirección estratégica y efectos geopolíticos deseados, usando primordialmente abordajes no militares” (Schnauffer 2017, 20). Agrega que en los conflictos contemporáneos ya no existen frentes de combate claros, ni una distinción entre zonas geográficas aliadas y enemigas, y que en la actualidad tienden a diluirse los límites claros entre paz y guerra. En ese marco, le otorga una alta importancia a las capacidades no militares de un actor que persigue un objetivo político o estratégico, subrayando que en un conflicto externo se aplican cuatro veces más medidas no militares que militares. Entre ellas se encuentran represalias económicas, propaganda, subversión política y operaciones psicológicas. Por tanto, para alcanzar el triunfo, resulta indispensable la previa obtención de la supremacía en el ámbito del manejo de la información y la comunicación estratégica (Morales Morales 2017).

La doctrina Gerasimov postula que la ventaja que reporta la ejecución de acciones de carácter híbrido es que dificulta la identifica-

ción de la agresión, por parte del oponente. Precisamente, en torno a los límites difusos de la paz y la guerra es que los Estados pueden amenazarse y agredirse sin echar mano, en primera instancia, al instrumento militar. Este podría incorporarse en una segunda etapa, capitalizando los avances logrados por las medidas económicas, políticas, comunicacionales y de otro tipo (Morales Morales 2017).

La aplicación de esa conducta por Moscú, sea como guerra no lineal o doctrina Gerasimov, incluye el ataque cibernético a Estonia en 2007, y la breve guerra de Georgia en torno a Osetia del Sur, un año más tarde. Empero, el caso icónico fue la crisis desatada en Ucrania en el año 2014, que culminó con la anexión de Crimea, ocasión en la cual el Kremlin explotó intensamente los planos psicológico y mediático (incluyendo las redes sociales). Así, alcanzó con eficacia una serie de metas: desacreditar a su oponente y erosionar su imagen internacional; explotar los clivajes étnicos para fragmentar el cuerpo social ucraniano; maximizar los éxitos de los rebeldes prorrusos en el oriente del país, y envolver en un halo de misterio las acciones de sus propias unidades de combate. De manera simultánea y complementaria, se desarrollaron acciones bélicas que estuvieron ejecutadas por unidades propias de operaciones especiales, o milicias locales (Pomerantsev 2015). En los términos de la estrategia militar rusa, los hechos detallados se enmarcarían dentro del concepto *maskirovka* (traducido como “enmascaramiento”), que alude a operaciones de engaño y distracción que optimizan las acciones militares propias, capitalizando el “factor sorpresa”, al tiempo que se confunde al oponente (Ash 2015).

En sentido inverso, Rusia también acusa a Occidente, y de manera más específica a Estados Unidos, de ejecutar en contra suya y de

sus aliados novedosas modalidades de guerra no convencional, que encuadrarían en formatos de guerra híbrida. Daniel Estulin realiza una detallada descripción de esas formas de enfrentamiento, cuyo objetivo sería propiciar cambios de regímenes políticos en los países-blanco, a través del colapso de su aparato estatal desde dentro, a expensas del bienestar de la población local. El abanico de opciones a las que echan mano los países que protagonizan la agresión incluyen la generación de inestabilidad interna; la presión externa al régimen para impedir que use la fuerza en el restablecimiento del orden; la asistencia militar y económica a insurgencias o grupos armados opositores y, eventualmente, si lo anterior no fuera suficiente, el uso de la fuerza militar (Estulin 2015).

Siempre en tal línea argumental, la externalidad de esta forma de conflicto híbrido, tras la cual hay velados intereses geopolíticos, por lo general vinculados a recursos naturales o ubicaciones estratégicas, consiste en las llamadas “revoluciones de colores”. La idea remite a la generación de disturbios en los países-blanco, en muchos casos en torno a un color simbólico. Una zaga de eventos de dicha naturaleza incluiría la Revolución Amarilla contra Ferdinand Marcos (1986); el derrocamiento de Slobodan Milosevic (2000); la Revolución de las Rosas en Georgia, que llevó al poder a Mijail Saakashvili (2003); la Revolución Naranja en Ucrania (2004-2005); la Revolución de los Cedros en el Líbano (2005); la Revolución de los Jazmines en Túnez (2011) y finalmente el capítulo sirio de la llamada Primavera Árabe (2012) (Estulin 2015, 181-182).

Todos esos episodios, a los cuales podrían agregarse las revoluciones acaecidas en Kirguistán y Uzbekistán, en ambos casos en el año 2005, son interpretados en Rusia como acontecimientos con fuerte respaldo exógeno

a las facciones prooccidentales, en el marco de una estrategia que apuntaría a evitar su consolidación como potencia euroasiática (Gutiérrez del Cid 2016). Empero, se ha alegado que la principal amenaza de esas presuntas revoluciones para el Poder Ejecutivo ruso no radicaba tanto en cuestiones geopolíticas, enlazadas con la amenaza a su influencia regional, sino en el riesgo de que se repitan en su propio territorio (Welsh 2017). De hecho, se sostiene que las jornadas revolucionarias de Uzbekistán habrían constituido el punto álgido a partir del cual no solo Rusia, sino también China, habrían decidido neutralizar estas formas híbridas y no convencionales de agresión (Gutiérrez del Cid 2016). Otras lecturas (Friedman 2010), en cambio, sitúan el punto de quiebre en la ya mencionada Revolución Naranja, interpretada como un intento de Estados Unidos de llevar a Ucrania a la Organización del Tratado del Atlántico Norte (OTAN) y asfixiar a Rusia, cuyo gobierno relanzó a partir de ese momento una doctrina de “esferas de influencia” en su espacio cercano exterior.

La versión china de guerra híbrida difiere tanto de la concepción rusa como de la practicada por el Estado Islámico. Su rasgo más notorio consiste en que hasta el momento ha excluido el empleo de la violencia directa. El nombre que ha merecido el fenómeno en Occidente es el de guerra irrestricta, traducción no literal del título de un libro redactado en 1999 por los coroneles Qiao Ling y Wang Xiangsui.² Casi tres lustros después de su publicación, los contenidos de la obra se transformaron en doctrina oficial, cuando el Ejército Popular de Liberación (PLA) adoptó

² La traducción correcta del título original del libro sería “Guerra sin ataduras” (war without bounds).

el concepto de “tres guerras”, en referencia a la coordinación de operaciones psicológicas, manipulación mediática y planteos jurídicos para influir en las percepciones, estrategias y conductas del oponente (Raska 2015).

Los autores sostienen que, simultáneamente a la reducción relativa de la violencia militar que se observa en el tablero internacional, se incrementa la violencia en los ámbitos político, económico y tecnológico. Es una violencia que suele ejercerse a través de la desinformación y del control de sectores sensibles para una sociedad. Dicho de otra manera, en la guerra contemporánea, las acciones bélicas son desplazadas de su rol principal y directriz, en beneficio de otras modalidades de actuación (Morales Morales 2017). Qiao y Wang recogen el postulado de Sun Tzu, “el supremo arte de la guerra es someter al enemigo sin luchar”. Entienden que, en un mundo signado por la interdependencia, en el cual los límites y las fronteras se relativizan, es preciso combinar un “gran método de guerra” que incluya todas las dimensiones militares y no militares (Sánchez Erráez 2014). La heterogénea variedad de medios involucrados incluye obviamente el instrumento militar. Se agrega que su alto costo aconseja su empleo en operaciones cortas y precisas, pero lo excede para incorporar también herramientas legales (el llamado *lawfare*), económicas y psicológicas, así como las redes informáticas (*network warfare*) e incluso el cometimiento de acciones terroristas (Bartolomé 2017).

En términos empíricos, una guerra irrestricta sería la que Pekín libra contra algunos de sus vecinos (y eventualmente contra Estados Unidos) en sus mares adyacentes, enormes reservorios de recursos naturales energéticos y paso obligado de innumerables líneas marítimas de comunicación. Allí ha respalda-

do sus reclamos de soberanía sobre algunos de sus sectores, con la construcción de islas artificiales, el despliegue de fuerzas aeronavales de consideración y la amenaza de sanciones económicas a quienes no reconozcan sus derechos, al tiempo que debate en el plano jurídico con sus contendientes.

Las amenazas híbridas

Ya se anticipó en los pasajes introductorios que una amenaza puede ser híbrida en sí misma, con independencia de su circunstancial protagonista, en la medida en que combina características propias de al menos dos amenazas diferentes, o de una amenaza y otro fenómeno o situación, de ribetes claramente diferenciados. Las amenazas transnacionales, protagonizadas por actores de naturaleza no estatal, presentan adecuadas condiciones para su hibridación, teniendo en cuenta que tienden a adoptar formatos similares, fuertemente influenciados por la revolución registrada en las postrimerías del siglo pasado, en el campo de las Tecnologías de la Información y las Comunicaciones (TIC). En concreto, se trata de la organización en redes flexibles y descentralizadas, muy adaptables y con un manejo optimizado de la información en los procesos de tomas de decisiones: la llamada “guerra en red” (*netwar*), entendida como “el uso de formas de red de organización, doctrina, estrategia y tecnología de acuerdo a la Era de la Información” (Arquilla, Ronfeldt y Zanini 2000, 180).

En el mencionado campo de las amenazas transnacionales, el fenómeno terrorista se presenta particularmente permeable a dinámicas hibridizantes, debido a las imprecisiones en torno a sus límites y contenidos. Esto ha llevado a asegurar que no es un método, sino una

lógica (Brito Gonçalves y Reis 2017); que es más una dinámica que una estructura, y que es menos una definición técnica que moral (Silva 2017). Una de las formas de hibridación del terrorismo lo emparenta con la guerra contemporánea, dado que ambos fenómenos comparten un “cambio de escala” en términos de violencia, aplicándola contra masas civiles a partir de justificaciones vinculadas a la noción de “responsabilidad colectiva” (Ruggiero 2009). Sobre ese punto, Brito Gonçalves y Reis (2017) alegan que, cada vez más, el terrorismo se aproxima en intensidad a una guerra, justificando acciones de Estados que en otras épocas hubieran sido inaceptables.

La criminalidad organizada también se muestra proclive a la hibridación con otros fenómenos. En principio, esa permeabilidad parece ser notoria en el caso del narcotráfico, una de sus principales manifestaciones. Así, el llamado narcoterrorismo sería un claro resultado de la combinación con el terrorismo. Sohr (2000, 177) destaca su naturaleza bidireccional, indicando que puede aludir tanto al empleo de tácticas terroristas por parte de narcotraficantes como a grupos terroristas (o insurgentes) que se involucran de alguna manera con el tráfico de narcóticos. El involucramiento puede abarcar servicios de protección o tránsito, o la amenaza a plantadores o traficantes que operan en el territorio que ellos controlan, por lo general a cambio de dinero. Otro caso de hibridación entre terrorismo y crimen organizado, elaborado a partir de *Al Qaeda* y con puntos de contacto con la idea de “guerra en red”, refiere a la adopción de estructuras celulares propias de los carteles de la droga, por parte de grupos terroristas, según John Gray (2004).

Pese a la bidireccionalidad indicada por Sohr, la idea de narcoterrorismo suele referir

al involucramiento de organizaciones terroristas o insurgentes en el tráfico ilegal de drogas. Esta tesis tendría cierto respaldo empírico. El fenómeno inverso, basado inicialmente en la experiencia mexicana, se conoce como insurgencia criminal. Ya se indicó que, en estos casos, la búsqueda de ganancias económicas ocupa el lugar que en otras circunstancias corresponde a la ideología, la religión o la etnia. El fenómeno erosiona y socava las instituciones políticas y las sociedades de los Estados democráticos, no solo a través de la corrupción, sino también mediante el ejercicio de la violencia, en aras de preservar sus negocios, enfrentando a la fuerza pública y estableciendo áreas geográficas donde poder desplegar sus actividades ilegales en forma irrestricta. A tal efecto, echa mano a verdaderos ejércitos privados, con gran especialización y adecuadamente equipados (Bartolomé 2013). La última cuestión ha sido entendida también como una “paramilitarización” de las estructuras criminales, que facilita el empleo del instrumento militar en la articulación de la respuesta estatal, dada la eventual insuficiencia de los medios policiales o de las fuerzas de seguridad (Sansó-Rubert Pascual 2017).

Desde el punto de vista analítico, la hibridación entre terrorismo y crimen organizado ha sido explicada a partir de una progresiva “convergencia motivacional” entre ambos fenómenos, que se presenta como un amplio espectro, entre cuyos extremos existen diferentes posibilidades de interacción (Makarenko 2004). Sea en un sentido o en otro de ese continuo, resulta claro que la hibridación entre terrorismo y crimen organizado no consiste en una mera transformación de uno en otro, sino en la evolución hacia una estructura que otorgue importancia a características de ambos fenómenos, a partir de un giro político de la

organización criminal, o un giro pragmático del grupo terrorista (De la Corte y Giménez Salinas Framis 2015).

Un enfoque alternativo sobre los procesos de hibridación entre terrorismo y crimen organizado, surgido a comienzos del presente decenio (Farah 2011), enfoca su atención en la existencia de redes que semejan “ductos” por donde se mueven productos ilegales, dinero, armas y personas. Las redes son operadas por facilitadores, que actúan en las sombras y son particularmente hábiles en explotar las debilidades de las estructuras legal y económica internacionales. En esa dinámica, los actores terroristas y criminales no son necesariamente aliados, y de hecho suelen enfrentarse, pero establecen alianzas transitorias de conveniencia, que se sustentan en la habilidad de cada participante para proporcionar algún servicio o beneficio clave a la contraparte. Los abordajes tempranos al funcionamiento de esos ductos evolucionaron hacia la idea de convergencia, en relación con la proliferación y diversificación a escala global de redes de tráficos ilícitos para cuyo funcionamiento convergen los intereses de diferentes actores terroristas y criminales.

Estas redes ilegales, en la visión de Miklaucic, Brewer y Barnabo (2013), configuran verdaderas cadenas de suministros transcontinentales, que conectan mercados ilícitos de los más variados bienes y servicios, cuyos “nodos” (*hubs*) suelen ubicarse en áreas geográficas con escaso control gubernamental. Los actores no estatales que las dinamizan incluyen en sus metodologías el uso de la violencia. Parte de ellos, por un principio de especialización, han desarrollado una notable habilidad para eludir las medidas de seguridad y protección del Estado, cuyas debilidades y oportunidades explotan a su favor.

La alta capacidad de adaptación y diversificación horizontal de los actores que convergen en las redes híbridas les permite acceder a vastos recursos financieros. Adquieren una gran capacidad para corromper a funcionarios públicos, desconocer las leyes vigentes, proveer a la ciudadanía bienes y servicios (incluida la seguridad), reemplazando al Estado en esa función, y operar a través de las fronteras nacionales como si estas no existieran. Para preservar este estado de cosas, se arman y entrenan en un grado superior a las instituciones públicas que deben enfrentar, combinándose y potenciándose entre sí en una suerte de “sinergia negativa”, al tiempo que exhiben una alta capacidad de adaptarse y transformarse según las demandas del entorno, razón por la cual es dificultosa su derrota y desarticulación.

La criminalidad organizada es el elemento central de otro proceso de hibridación, en este caso con el Estado, que da lugar a un nuevo tipo de actor dentro del subsistema de seguridad internacional. Esta es la tesis que sostiene Naím (2012), en referencia a lo que denominó inicialmente Estado Mafioso y luego Estado Criminal. En su visión, la figura es el resultado de una penetración criminal a las estructuras estatales en un grado sin precedentes, corolario de largos procesos de criminalización, que reconocen diferentes estadios. Los funcionarios se enriquecen a sí mismos, y a sus familias y amistades, a través de la explotación de dinero, poder, influencia política y conexiones del con el crimen organizado, que constituye la principal prioridad. Dicho de otra manera, las actividades ilegales no son realizadas solamente por profesionales de ese rubro, sino también por funcionarios públicos.

En esa línea de pensamiento, en el Estado Mafioso o Criminal es difícil diferenciar los cálculos geopolíticos estatales de los motivos

y ganancias de los criminales. En suma, en cierto modo se borran las líneas demarcatorias entre Estado y actor no estatal, lo cual genera una nueva forma híbrida de actor internacional, consistente en una gran empresa criminal con fachada de aparato estatal. Se configura un actor híbrido orientado a las actividades ilícitas, que combina la flexibilidad y adaptabilidad de las redes criminales con la protección legal y los privilegios que pueden proporcionar los aparatos estatales (Naím 2012; Miklaucic y Naím 2013). *A priori*, el modelo de nuevo actor internacional que plantea el escritor y columnista venezolano podría hacerse extensivo a otras tipologías semejantes al Estado Mafioso. Un ejemplo sería el de la “captura (criminal) del Estado”, situación en la cual la elite política se torna en un grupo criminal que utiliza los recursos y estructuras estatales en su propio beneficio (Farah 2011). Otra muestra estaría dada por los llamados Narcoestados, casos extremos de criminalización en los que la economía del país depende básicamente de los ingresos procedentes de las actividades criminales (en este caso, el narcotráfico) (De la Corte y Giménez Salinas Framis 2015).

Conclusiones

El análisis presentado confirma que, más allá de una notable proliferación semántica en lo referente a la definición de los conflictos armados actuales, y a pesar del uso poco riguroso de la terminología disponible, los conflictos híbridos gozan de un importante grado de singularidad respecto a otras manifestaciones polemológicas contemporáneas. La singularidad de los conflictos híbridos es consecuencia directa de su especificidad, que se detecta ya

en las acciones llevadas a cabo por Hezbollah en la llamada Segunda Guerra del Líbano. Tal especificidad marcó una ruptura respecto a los formatos vigentes, consistentes en la combinación de modos de combate clásicos e irregulares. O dicho de otro modo, de formas encuadradas en el modelo clausewitziano de guerra verdadera, con otras que signaron la primera década posterior a la Guerra Fría, muchas veces englobadas bajo el rótulo genérico de Nuevas Guerras.

Así planteados, los conflictos híbridos asumen el atributo de la asimetría, propio de las Nuevas Guerras, aunque lo trascienden al incorporar otras formas de combate, en su multimodalidad. En ese sentido, conflictos híbridos y conflictos no son la misma cosa, ni los primeros representan la mera evolución de los segundos. Queda claro que los conflictos híbridos pusieron en crisis el consenso existente durante el primer decenio posterior a la Guerra Fría, en cuanto a la escasa complejidad tecnológica que caracterizaría el accionar de los actores no estatales, asimetría mediante.

También se concluye que la mera idea de conflictos híbridos, lejos de permanecer estática y refractaria al cambio, ha experimentado un importante salto cualitativo, cuyo dato central es su ejercicio por parte de actores estatales. En esos casos, la multimodalidad continúa vigente, aunque su sentido cambia. Mientras en las concepciones iniciales la novedad radicó en la incorporación de formas de combate tradicionales por actores asociados apriorísticamente con conductas asimétricas, en este segundo caso se asiste a lo contrario.

Lo que podría considerarse entonces un segundo tipo de conflictos híbridos, en el cual el Estado recupera su protagonismo, exhibe de manera accesoria otras diferencias cuantitativas y cualitativas respecto al tipo inicial.

En cuanto a lo primero, un empleo más intenso de tecnología avanzada, que se explica en el hecho de que los Estados tienen mayores y mejores capacidades en ese rubro que sus contrapartes no estatales. En lo cualitativo, se observa la incorporación de dimensiones otrora soslayadas, entre ellas la legal, la comunicacional y la cibernética. Los conflictos híbridos de segundo tipo no son solo multimodales, sino además multidimensionales. Incluso, no es desacertado considerarlos también “multidominio”, a partir de la incorporación del dominio cibernético a los tres tradicionales. Es posible prever que este aspecto incrementará su importancia, de la mano de la expansión de las TIC y la complejización de las modalidades de ciber guerra.

La idea de conflictos híbridos, en su segundo tipo, no se circunscribe a Occidente. Encuentra fuertes puntos de contacto con doctrinas ajenas a ese ámbito geográfico y, lo que es aún más importante, de diferentes tradiciones. Los conflictos no lineales de Rusia, también englobados en la llamada Doctrina Gerasimov, y la guerra irrestricta que se postula desde China constituyen ejemplos por demás elocuentes.

Frente al concepto de conflictos híbridos, la idea de amenazas híbridas exhibe una originalidad mucho menor, puesto que básicamente consiste en encuadrar de manera conceptual una situación usual, consistente en la combinación de dos o más amenazas, por lo general de características transnacionales, protagonizadas por actores no estatales, o de una amenaza y otro fenómeno. Resulta útil recordar en este punto que, aunque desde el punto de vista académico las mencionadas amenazas suelen ser estudiadas de manera aislada, en la realidad suelen combinarse de diferentes maneras, a menudo potenciándose sinérgicamente.

En un contexto facilitado por la adopción de formatos de red, el terrorismo exhibe una alta permeabilidad a dinámicas hibridizantes, con el crimen organizado en general, y en especial con el narcotráfico. El narcoterrorismo y la insurgencia criminal son elocuentes ejemplos, aunque en el modelo teórico de Makarenko exhiben aproximaciones opuestas.

En todo ese contexto, la debilidad del Estado y sus déficits de gobernabilidad ocupan un lugar central. Por un lado, su pérdida de control territorial efectivo y del monopolio de la violencia facilitan la aparición o consolidación de amenazas híbridas cuyo potencial de daño no quedaría limitado dentro de sus fronteras, sino que podrían excederlas para alcanzar al menos el plano regional. Por otro lado, el propio aparato estatal puede verse involucrado en diversos grados de hibridación con el crimen organizado, derivando en diferentes cuadros de captura por parte de ese flagelo. En teoría, puede llegar al extremo de constituir un Estado Mafioso o Estado Criminal. Esto confirma la conclusión planteada en otras ocasiones (Bartolomé 2018): a partir de cierto grado de intensidad, los cuadros de debilidad estatal y déficit de gobernabilidad dejan de concernir solo a los habitantes de un país, y se transforman en cuestiones de seguridad regional o eventualmente internacional.

Nada indica que América Latina constituya una región exenta de la ocurrencia de conflictos híbridos o de la presencia de amenazas híbridas, aunque diferentes elementos indican que es más factible lo segundo que lo primero. *In extenso*, no se detectan actores no estatales con la capacidad de realizar una exitosa combinación entre modos de combate convencionales afines al modelo clausewitziano, con formatos asimétricos no convencionales. Tampoco se tiene conocimiento de Estados

regionales que hayan desarrollado esas formas no convencionales de conflicto. Incluso apelando a la licencia de presuponer su existencia, no se registran situaciones de conflictividad interestatal que puedan precipitar su implementación.

Sin embargo, dentro del espacio latinoamericano proliferan fenómenos de hibridación entre criminalidad y terrorismo, sea de manera permanente o como convergencias coyunturales y transitorias, que se benefician de la debilidad estatal. Un amplio rango de actores podría quedar involucrado en una tipología sobre estos casos. En un listado que en modo alguno pretende ser exhaustivo, podría incluirse al Primer Comando de la Capital (PCC) de Brasil; a los elementos residuales de Sendero Luminoso, basados en la selvática zona del valle de los ríos Apurímac, Ene y Mantaro (VRAEM) peruano, volcados al negocio de las drogas; a algunos de los cárteles mexicanos, en particular la Federación de Sinaloa, los Zetas y el Cartel de Jalisco Nueva Generación (CJNG); a algunos colectivos venezolanos; y al heterogéneo universo de organizaciones que han surgido en el espacio geográfico colombiano, aunque sus acciones son claramente transnacionales –las bandas criminales constituidas tras la desmovilización de los paramilitares, las disidencias de las Fuerzas Armadas Revolucionarias de Colombia (FARC) e incluso el Ejército de Liberación Nacional (ELN)–.

De cara a la aparición, consolidación y expansión de amenazas híbridas, ya sea que se las identifique como tales o no, las naciones latinoamericanas han desarrollado estrategias y doctrinas disímiles, que constituyen el objetivo de habituales controversias por parte de especialistas. El encuadre de estas situaciones en el campo de la seguridad pública o de la

defensa, y los debates en torno al empleo o no del instrumento militar, constituyen apenas dos aristas de un debate que excede los objetivos de este artículo. Empero, no puede concluirse sin subrayar que tales estrategias y doctrinas brillan por su ausencia –al menos, hasta donde conoce el autor– al momento de contemplar, siquiera de modo prospectivo y en el plano especulativo, enfrentamientos con oponentes estatales que puedan plantear una forma de conflicto multimodal, multidimensional y multidominio. He aquí una tarea pendiente.

Bibliografía

- Arquilla, John, David Ronfeldt, y Michele Zanini. 2000. "Information-Age Terrorism". *Current History* 636 (99): 179-185.
- Ash, Lucy. 2015. "How Russia outfoxes its enemies". *BBC News*, 29 de enero, <https://www.bbc.com/news/magazine-31020283>
- Avilés Farré, Juan. 2017. *Historia del Terrorismo Yihadista: de Al Qaeda al Daesh*. Madrid: Editorial Síntesis.
- Bartolomé, Mariano. 2013. "Más allá del crimen organizado: la reformulación del concepto de insurgencia y su impacto en el entorno estratégico sudamericano". *Austral: Revista Brasileira de Estratégia e Relações Internacionais* 2 (3): 47-77.
- Bartolomé, Mariano. 2016. "Algunas aproximaciones a la agenda de la Seguridad Internacional contemporánea y la influencia teórica en sus contenidos". *Política y Estrategia* 128: 101-134.
- Bartolomé, Mariano. 2017. "El empleo actual del concepto 'Guerra' en las Relaciones Internacionales". *Revista de Relaciones Internacionales, Estrategia y Seguridad* 12 (2): 43-66.

- Bartolomé, Mariano. 2018. "La Seguridad Internacional contemporánea: contenidos temáticos, agenda y efectos de su ampliación". *Relaciones Internacionales* 55: 123-145.
- Bartolomé, Mariano, y Concepción Anguita Olmedo. 2019. "La destrucción de bienes culturales en el marco de conflictos armados, en la agenda de la Seguridad Internacional contemporánea". *Studia Politicae* 46: 35-67.
- Bouthoul, Gastón. 1984. *Tratado de Polemología. Sociología de las guerras*. Madrid: Ediciones Ejército.
- Brito Gonçalves, Joanival, y Marcus Reis. 2017. *Terrorismo. Conhecimento e combate*. Niteroi: Impetus.
- De la Corte Ibañez, Luis, y Andrea Giménez Salinas Framis. 2015. *Crimen.Org*. Barcelona: Ariel.
- Estulin, Daniel. 2015. *Fuera de Control*. Buenos Aires: Planeta.
- Farah, Douglas. 2011. "Terrorist-Criminal Pipelines and Criminalized States". *Prism* 2 (3): 5-32.
- Friedman, George. 2010. *The Next 100 Years. A Forecast for the 21st Century*. Nueva York: Anchor Books.
- García, Caterina. 2013. "Las nuevas guerras del siglo XXI. Tendencias de la conflictividad armada contemporánea". *Institut de Ciénces Politiques i Socials, Working Paper* 323.
- Gray, Colin. 2004. *How has War Changed since the End of the Cold War?* Washington DC: Global Trends Project / US National Intelligence Council.
- Gray, John. 2004. *Al Qaeda y lo que significa ser moderno*. Buenos Aires: Paidós.
- Gutiérrez del Cid, Ana. 2016. "El debate actual sobre la visión de Mackinder en la perspectiva de Brzezinski y Alexander Dugin: el regreso de la geopolítica". En *La Geopolítica del Siglo XXI*, coordinada por Graciela Pérez Gavilán Rojas, Ana Gutiérrez del Cid y Beatriz Pérez Rodríguez, 33-57. México DF: Universidad Autónoma Metropolitana.
- Hoffmann, Frank. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.
- Hoffmann, Frank. 2009. "Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict". *Strategic Foru*, 240: 1-8.
- Ignatieff, Michel. 1999. *El Honor del Guerrero. Guerra étnica y conciencia moderna*. Madrid: Santillana.
- Kissinger, Henry. 2016. *Orden Mundial*. Barcelona: Debate.
- Liogier, Raphael. 2017. *La Guerra de Civilizaciones no tendrá lugar. Coexistencia y violencia en el Siglo XXI*. Salamanca: Comunicación Social.
- Makarenko, Tamara. 2004. "The Crime-Terror Continuum: Tracing the Interplay between Transnational Organized Crime and Terrorism". *Global Crime* 6 (1): 129-145.
- Miklaucic, Michael, Jacqueline Brewer, y Gary Barnabo. 2013. *Convergence. Illicit Networks and National Security in Age of Globalization*. Washington DC: National Defense University Press.
- Miklaucic, Michael, y Moisés Naím. 2013. "The Criminal State". En *Convergence. Illicit Networks and National Security in Age of Globalization*, compilado por Michael Miklaucic, Jacqueline Brewer y Gary Barnabo, 149-170. Washington DC: National Defense University Press.
- Morales Morales, Samuel. 2017. "El futuro de la naturaleza de los conflictos arma-

- dos”. *Instituto Español de Estudios Estratégicos, Documento Marco* 17/2017, 23 de noviembre.
- Münkler, Herfried. 2003. “The Wars of the 21st Century”. *International Review of the Red Cross*, 85 (849): 7-22.
- Naím, Moisés. 2012. “Mafia States. Organized Crime Takes Office. *Foreign Policy*, mayo-junio, <https://www.foreignaffairs.com/articles/2012-04-20/mafia-states>
- Napoleoni, Loretta. 2015. *El Fénix Islamista*. Barcelona: Paidós.
- Pomerantsev, Peter. 2015. “Brave New War. A New Form of Conflict emerged in 2015, from the Islamic State to the South China Sea”. *The Atlantic*, 29 de diciembre, <https://www.theatlantic.com/international/archive/2015/12/war-2015-china-russia-isis/422085/>
- Pizarroso Quintero, Alejandro. 2004. “Guerra y comunicación. Propaganda, desinformación y guerra psicológica en los conflictos armados”. En *Culturas de Guerra*, coordinado por Fernando Contreras y Francisco Sierra, 17-56. Madrid: Cátedra.
- Quintana, Yolanda. 2016. *Ciberguerra*. Madrid: Catarata.
- Ruggiero, Vincenzo. 2009. *La violencia política*. Barcelona: Antrophos.
- Sánchez Errás, Pedro. 2014. “La nueva Guerra Híbrida: un somero análisis estratégico”. *Instituto Español de Estudios Estratégicos, Documento de Análisis* 54/2014, 29 de octubre.
- Sansó-Rubert Pascual, Daniel. 2017. *Democracias bajo presión*. Madrid: Dykinson.
- Schear, James. 2008. “Defusing Conflicts in Unstable Regions”. En *Strategic Challenges*, compilado por Stephen Flanagan y James Schear, 110-148. Washington DC: National Defense University / Potomac Books.
- Schnauffer, Tad. 2017. “Redefining Hybrid Warfare: Russia’s Nonlinear War against the West”. *Journal of Strategic Security* 10 (1), 17-31.
- Silva, Luis. 2017. *Vidas armadas*. Santiago de Chile: Planeta.
- Sohr, Raúl. 2000. *Las guerras que nos esperan*. Santiago de Chile: Ediciones B.
- Tello, Ángel. 2013. *Escenarios mundiales. Situaciones y conflictos*. La Plata: Universidad de La Plata.
- Torres Soriano, Manuel. 2011. “Los medios de comunicación globales y la acción exterior del Estado”. En *La Seguridad más allá del Estado. Actores no estatales y Seguridad Internacional*, compilado por Javier Jordán, Pilar Pozo y Josep Bacqués, 93-112. Madrid: Plaza y Valdés.
- Welsh, Jennifer. 2017. *The Return of History. Conflicts, Migration and Geopolitics in the Twenty-First Century*. Toronto: Anansi Press.

Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad

Cyber-physical Facts: A Proposed Analysis for Cyber Threats in the National Cybersecurity Strategies

Juan-Manuel Aguilar-Antonio¹

Recibido: 3 de junio de 2019
Aceptado: 22 de agosto de 2019
Publicado: 2 de diciembre de 2019

Resumen

El artículo presenta la categoría de hechos ciberfísicos, una propuesta para el análisis y la delimitación de amenazas en el régimen híbrido del ciberespacio. Se propone la hipótesis de que América Latina, y en particular México, no comprenden en sus Estrategias Nacionales de Ciberseguridad (ENCS) la naturaleza de las ciberagresiones ni la posibilidad de que una crisis surgida en el ciberespacio salte al espacio físico o material. Para probarla se presenta el contexto de la ciberseguridad en la región y se realiza una crítica de la ENCS de México. Después se hace un análisis comparativo de cinco casos de interés y referencia entre los estudios de ciberseguridad, para introducir el concepto de hecho ciberfísico. Por último, se aplica la propuesta a un estudio de caso y se muestra su utilidad para las ENCS, así como su grado de impacto en la esfera de la seguridad pública y nacional.

Palabras clave: crisis política; internet; protección de datos; seguridad cibernética; seguridad del Estado

Abstract

The article introduces the category of cyber-physical facts, a proposal for the analysis and delimitation of threats in the hybrid regime of cyberspace. The research objective is to test the hypothesis that Latin America, and Mexico in particular, do not understand in their National Cybersecurity Strategies (NCSS) the nature of cyber-attacks, nor the possibility that a crisis arising in cyberspace will jump into the physical or material ground. To prove this, the context of cybersecurity in the region is presented and also a critique of the NCSS of Mexico. Then, the

¹ Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México (UNAM), México, alchemistfvii@hotmail.com,  orcid.org/0000-0002-4686-685X



article makes a comparative analysis of five cases of interest and reference in cybersecurity studies to introduce the concept of cyber-physical fact. Finally, this proposal is applied to a case study, and its usefulness to the NCSS is shown, as well as its degree of impact in the sphere of public and national security.

Keywords: cybernetics security; data protection; internet; political crises; State security

Introducción

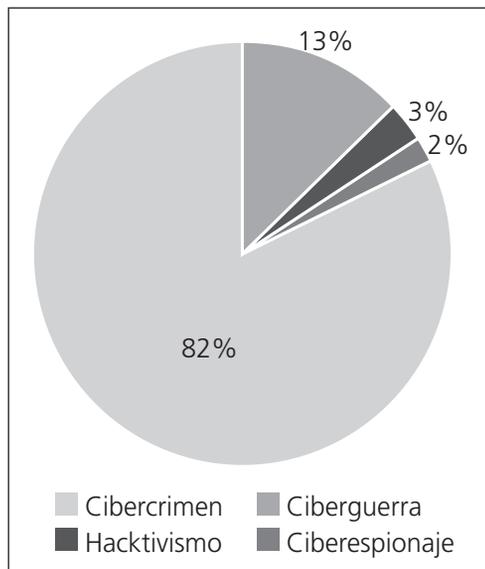
La agenda de ciberseguridad es un reto entre las naciones de Latinoamérica, dada la velocidad de la evolución del ciberespacio. Entre los esfuerzos conjuntos de cooperación regional destaca el papel de la Organización de los Estados Americanos (OEA), con la publicación de la Estrategia Interamericana Integral de Seguridad Cibernética (2004) y la declaración de Fortalecimiento de la Seguridad Cibernética en las Américas (2012). En el plano unilateral, países como México, Argentina, Brasil, Colombia y Jamaica han estructurado Estrategias Nacionales de Ciberseguridad (ENCS), con importantes avances para consolidar una política de ciberseguridad, que forman parte de una tendencia creciente de la importancia del tema en la región (Cornaglia y Vercelli 2017).

Sin embargo, la creación de políticas de ciberseguridad enfrenta dificultades ante el incremento de ciberamenazas. Tan solo en el bienio 2012-2013 los ciberataques a entidades o sitios de internet públicos y privados crecieron más del 61 % (OEA y Symantec 2014). En 2014, países como Ecuador, Guatemala, Bolivia, Perú y Brasil se incluyeron entre las diez principales naciones con más computadoras infectadas por *malware*. Se sumaron Uruguay, Colombia y Chile, que estuvieron

por encima de la media mundial de infección, situación que colocó a la región, junto a Asia, en las tasas más altas de virus maliciosos a escala global (PandaLabs 2015).

Las principales ciberamenazas en América Latina son ataques dirigidos por *malware* para robo de información sensible o confidencial. Las técnicas más utilizadas son el *spear-phishing* (correo electrónico diseñado para infectar un computador personal), y el *watering-hole* (infiltración de sitios web legítimos para mandar a través de ellos códigos maliciosos) (OEA y Symantec 2014). También, desde 2015 los troyanos dirigidos al fraude bancario han presentado un incremento considerable; se estima que el 92 % de las entidades financieras ha sufrido un ciberataque; 37 % del total resultaron exitosos (OEA 2018). Ese panorama presenta que las ciberamenazas se concentran en el sector y los usuarios privados. Situación que está en sintonía con las tendencias globales, como

Gráfico 1. Motivaciones detrás de ciberataques a escala global (2018)



Fuente: Pessiri (2019).

parte de las cuales las actividades relacionadas con el cibercrimen son mayores (77,9% del total) que otras vinculadas a instituciones públicas o gubernamentales, como el ciberespionaje o hacktivismo (Pessiri 2019) (gráfico 1).

Es importante destacar que en América Latina no se ha presentado un ciberataque importante que involucre a actores privados con gubernamentales, con fines o motivaciones políticas, como el ataque de negación de servicio (DoS/DDoS²) acontecido en Tallin (2007) y Georgia (2008) o ataques enfocados al daño de Infraestructura Nacional Crítica (INC), como el de Stuxnet (2010).

En ese sentido, partimos de la hipótesis de que la región y sus ENCS no están preparadas para un ataque de tal naturaleza, y no consideran la posibilidad de que una crisis surgida en el ciberespacio pueda saltar al espacio físico o material. Para probar esto, utilizamos la metodología de estudio de caso para analizar la ENCS de México y hacemos una crítica a sus carencias y debilidades en el contexto actual de ciberamenazas. Posteriormente, hacemos un estudio comparativo de cinco casos de trascendencia en los estudios de seguridad, para presentar la categoría de hecho ciberfísico y su esquema de analítica para ciberamenazas.

Crítica a la ENCS de México

En México la penetración de internet representa el 60 % de la población, lo que significa 71,3 millones de cibernautas. La edad de los usuarios de internet se concentra entre los 18 y 34 años (83,4 %). Asimismo, el principal me-

² Un ataque DDoS tiene como objetivo inhabilitar un servidor, un servicio o una infraestructura. Puede hacerse por saturación del ancho de banda del servidor para dejarlo inaccesible, o por agotamiento de los recursos del sistema de la máquina.

dio de acceso es a través de teléfonos inteligentes (89,7 %), y computadora de escritorio y portátil (34 %) (INEGI 2018). Durante 2017 las pérdidas económicas en ciberseguridad alcanzaron una cifra de 7,7 billones de dólares (Norton 2018). También, en el periodo 2013-2016 los ciberincidentes mostraron un incremento del 300 %, al pasar de 20 000 a 60 000, a la par de que se detectaron 5000 páginas de ciberfraude en el país (Parraguez 2018).

El principal medio de infección de computadores es a través de *malware* (98 %) y el resto se da a través de *spear-phishing* (Espinosa 2015). Resalta el incremento anual de efectividad de ambas modalidades de ciberinfección en 2015, con una tasa de crecimiento de 323 % para el *malware* y 409 % para *spear-phishing* (OEA y Symantec 2014). Norton (2018) resalta que los usuarios de internet gastaron 55,1 horas en promedio al año en resolver problemas vinculados a infecciones o amenazas provenientes del ciberespacio.

Ciberseguridad en el marco de la ENCS

La ciberseguridad es un tema posicionado en la agenda del gobierno de México. Desde 2013 existen al menos tres documentos que contemplan el tema y son clave para el diseño de políticas públicas: el Plan Nacional de Desarrollo (2013-2018), el Programa de Seguridad Nacional (2014-2018) y el Programa Nacional de Seguridad Pública (2014-2018). Asimismo, en 2017 se creó la Estrategia Nacional de Ciberseguridad (ENCS), con lo cual México se convirtió en el octavo país en Latinoamérica en crear un documento de esta naturaleza.

Hasta 2018 la ENCS fue coordinada por múltiples instituciones, como la Comisión Nacional de Seguridad (CNS), la Secretaría

de Gobernación (Segob), la Policía Federal (PF), con División de Policía Científica, la Secretaría de la Defensa Nacional (SEDENA) y la Secretaría de Marina (SEMAR). Datos de la Policía Científica destacan que hasta 2017 se atendieron 51 000 denuncias ciudadanas, más de 200 000 incidentes cibernéticos, se desactivaron 17 000 sitios fraudulentos y se emitieron más de 2000 alertas de ciberseguridad (ENCS México de 2017).

También, esta división de la PF gestiona el Equipo de Respuesta de Incidentes Informáticos (*CERT³ MX*), el cual es miembro del Foro Global para Equipos de Respuesta a Incidentes y Seguridad (*FIRST⁴*). Por otra parte, las agencias gubernamentales utilizan el Manual Administrativo General de Gestión de Tecnologías de la Información, Comunicaciones y Ciberseguridad, de estándares ISO 27001. El Instituto Nacional Mexicano de Acceso a la Información, Transparencia y Protección de Datos Personales (INAI) colabora en esfuerzos por una mayor transparencia y disponibilidad de información y sensibiliza a los ciudadanos de sus derechos como usuarios de internet.

En indicadores internacionales, la Unidad de Inteligencia Económica de la Consultora Booz Allen Hamilton, que evalúa el ciberpoder entre las naciones que conforman el Grupo de los 20 (G20), posicionó a México en 11° lugar, a través de una medición de 39 indicadores en atributos que contemplan aspectos como el marco legal, regulatorio, económico y social, la tecnología implantada y la aplicación industrial (García 2018). Asimismo, el Índice

Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT) posicionó a México en el lugar 18, de un total de 29, respecto a sus capacidades de acción y resiliencia en ciberseguridad (UIT 2014). A pesar de que esas mediciones consideran que el país detenta capacidades intermedias en cuestiones de ciberseguridad, es necesaria una crítica para mejorar la capacidad de acción de la ENCS y su capacidad de enfrentar ciberamenazas.

Revisión de la ENCS de México

El objetivo general de la ENCS de México es:

Fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las Tecnología de Información de la Comunicación (TIC) de manera responsable para el desarrollo sostenible del Estado Mexicano (ENCS de México 2017).

El enunciado anterior contiene múltiples elementos vinculados a la creación de capacidades de resiliencia en el ciberespacio: su comprensión multidimensional (en la esfera social, económica y política) y la coordinación y cooperación de entidades públicas o privadas. Sin embargo, en su segunda parte es visible cómo la estrategia del país está concentrada en incrementar la penetración del internet y consolidar su uso como un derecho universal, más que en crear capacidades de resiliencia ante ciberamenazas. Esa conclusión es más visible al revisar su estructura:

Objetivos estratégicos: sociedad y derechos, economía e innovación, instituciones públicas, seguridad pública, seguridad nacional.

³ CERT, del inglés *Computer Emergency Response Team*, es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

⁴ Siglas en inglés de *Forum of Incident Response and Security Teams*.

Principios rectores: perspectiva de derechos humanos, enfoque basado en gestión de riesgos, colaboración multidisciplinaria y de múltiples actores.

Ejes transversales: cultura de ciberseguridad, desarrollo de capacidades, coordinación y colaboración, investigación, desarrollo e innovación TIC, estándares y criterios técnicos, infraestructuras críticas, marco jurídico y autorregulación, medición y seguimiento.

La ENCS sostiene que sus objetivos estratégicos y principios rectores se concentran en aumentar el uso de internet en México. Esta visión se vincula al concepto de brecha digital, que representa la separación entre las personas que utilizan las TIC como una parte de su vida diaria y quienes no tienen acceso a ellas o no saben cómo utilizarlas (Gómez et al. 2018). La aún baja penetración de internet en México explica el énfasis del documento en mejorar su uso y acceso. Una primera crítica a la ENCS se basa en esta condición, dado que la reducción de la brecha digital entre usuarios y no usuarios corresponde a otro tipo de política pública.

Por otra parte, el apartado de la ENCS más vinculado al desarrollo de capacidades de resiliencia en el ciberespacio se concentra en sus ejes transversales. Entre estos destacan: a) desarrollo de capacidades, b) coordinación y colaboración, c) infraestructuras críticas y d) marco jurídico y autorregulación. No obstante, la ENCS se presenta más como un documento en construcción que una política de ciberseguridad que contemple protocolos o mecanismos para consolidar capacidades de acción y reacción en materia de ciberseguridad.

Los apartados de desarrollo de capacidades, coordinación y colaboración contienen oraciones ambiguas que no se concretan en indicado-

res, metas concretas o cuantificables. A la par, estas secciones deben incluir un organigrama de la política de cooperación entre las instituciones del gobierno encargadas de la ciberseguridad, como la División Científica, SEDENA, SEMAR, Segob, etc., en el que destaquen las facultades de cada una en la ENCS (Espinosa 2015). Una tarea pendiente es identificar los vínculos y actores de la industria privada interesados en colaborar con el gobierno. En ese sentido, resalta que durante 2017, el mismo año de la publicación de la ENCS, la Cámara Nacional de la Industria Electrónica, Telecomunicaciones y Tecnologías de la Información (CANIETI) presentó un informe relacionado con el tema, en que solicitó al gobierno el establecimiento de una Agencia Nacional de Ciberseguridad que coordine la ENCS entre actores gubernamentales y privados, y establezca una ruta crítica para la gobernanza de internet en México (Parraguez 2018).

Un aspecto de interés es que en el eje transversal de INC se cita la Ley Nacional de Seguridad como documento rector de la política de ciberseguridad (ENCS de México 2017). Sin embargo, no se destacan acciones fundamentales para su protección, como la actualización del catálogo de INC de México, así como la diferenciación entre cuáles deben ser administradas por entidades públicas y privadas. Del mismo modo, no se sugiere la elaboración de guías y estándares para su protección (Calderón 2018?).

Por último, en el eje de marco jurídico y autorregulación, destacamos la necesidad de actualizar las legislaciones nacionales que engloban al ciberespacio, con base en lo establecido en el Convenio de Budapest (García 2018), una actualización sobre la clasificación de ciberdelitos punibles (Espinosa 2015) y la armonización de todas las leyes sobre delitos

informáticos (Parraguez 2018). Entre las normativas se encuentran: el art. 16 (referente a la inviolabilidad de las comunicaciones y la protección de los datos personales), de la Constitución Política de los Estados Unidos Mexicanos; los artículos 167 (sanción por la interrupción, interferencia e intervención de comunicaciones electrónicas), 202 (almacenamiento y difusión de pornografía infantil por medios electrónicos) y 211 Bis (acceso ilícito a equipos y sistemas de informática) del Código Penal Federal. También el Título IV, Capítulo IV (de regulación de la copia, alteración y reproducción de software y bases de datos) de la Ley Federal del Derecho de Autor y el Art. 298 (de pena al bloqueo del servicio de internet; interceptación de la información transmitida en redes públicas y no adopción de medidas para garantizar la confidencialidad y privacidad de comunicaciones) de la Ley Federal de Telecomunicaciones y Radiodifusión.

La crítica realizada a la ENCS de México devela que existe una marcada distancia entre el entorno actual de ciberamenazas a escala global y su contenido. Asimismo, no existe una concordancia o revisión para el aprendizaje de experiencias internacionales, para comprender el potencial del ciberespacio como un instrumento para vulnerar la seguridad pública o nacional, a escala local, nacional o internacional, que tome en cuenta que las crisis surgidas en esta arena pueden brincar del espacio virtual al material. Cómo propuesta de análisis para la promoción de una agenda de ciberseguridad, se presenta la categoría de hecho ciberfísico, que explicaremos a través de un estudio comparativo de cinco casos de interés para los estudios de ciberseguridad.

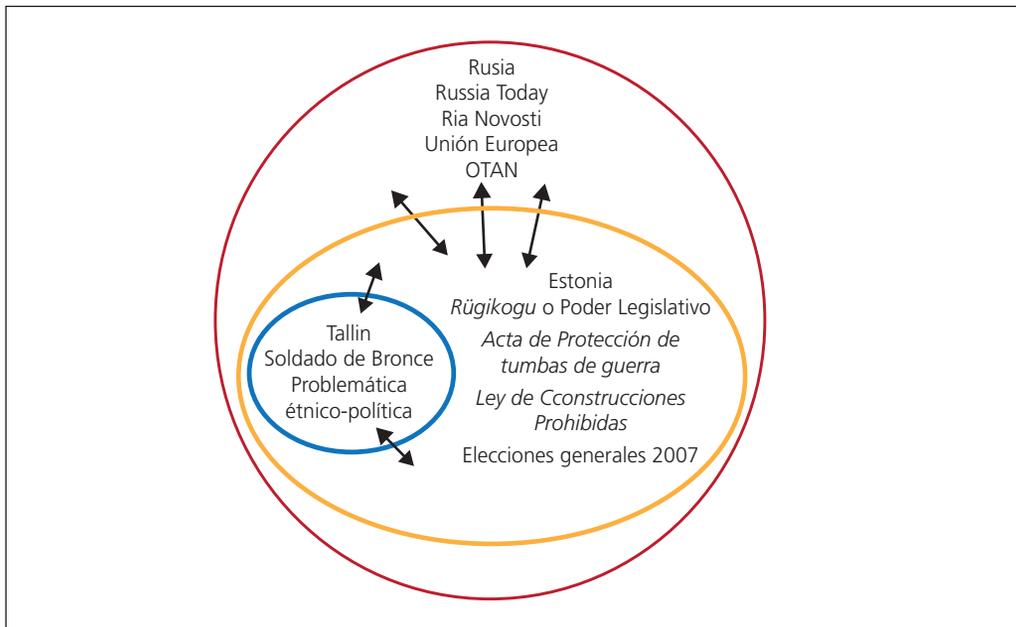
Revisitando Tallin: interpenetración de la escala local, nacional e internacional

Existe un consenso generalizado entre los estudios de ciberseguridad en señalar a los ataques de Tallin, Estonia (2007), como el primer caso de trascendencia que involucra a internet como un instrumento capaz de vulnerar la seguridad nacional de un Estado. La relevancia del caso hizo que se hablara de internet como un mecanismo capaz de promover una revolución en la política internacional (Kello 2013), que se señalara al ciberespacio como una nueva arena de confrontación e influencia de las naciones (Hughes 2010), que necesita la construcción de la securitización para su uso y regulación (Hansen y Nissenbaum 2009).

Una particularidad que presentan los análisis centrados en Tallin es abordar el evento desde la óptica de la seguridad nacional, con implicaciones para la soberanía de Estonia. En este análisis se proponen tres escalas para su comprensión, que explican un hecho ciberfísico, y se muestra cómo una ciberamenaza puede moverse a diferentes escalas y esferas. La figura 1 refleja cómo se superponen los niveles; dentro de cada esfera existen actores y factores que influyeron en la crisis de Tallin.

Escala local-nacional. La crisis de Tallin empieza con una motivación local, que es la reubicación de un monumento soviético denominado “Soldado de Bronce”. En primera óptica, su remoción se interpreta como un problema étnico-político que confrontó a dos sectores de la población, uno con raíces culturales estonias y otro de origen ruso-soviético (Schmidt 2013). Desde la perspectiva de la seguridad pública, el malestar político y civil que podía causar el evento no es menor, dado que 350 000 habitantes (26,5 % del total de

Figura 1. Interpenetración de escalas de seguridad en el ciberataque de Tallin (2007)



Fuente: elaboración propia.

la población del país) tenía algún grado de parentesco o filiación con Rusia o el periodo de dominación soviética. Tallin concentra una tercera parte de la población y era susceptible de sufrir fuertes disturbios.

La reubicación del monumento fue un tema central de la agenda parlamentaria desde enero de 2017 (BBC News 2007). De hecho, durante los meses previos a su remoción, el parlamento o *Riigikogu* legisló dos iniciativas para su reubicación: El Acta de Protección de Tumbas de Guerra, el 10 de enero, y la Ley de Construcciones Prohibidas, el 15 de febrero. Ese año el país celebró sus primeras elecciones generales que utilizaron el voto electrónico, hecho que formaba parte del proyecto de modernización tecnológica *X-Road*, cuyo objetivo era volver electrónicos todos los servicios del gobierno para 2015 (Detlefsen 2015).

En ese contexto, la confrontación entre un partido europeísta (Partido Reformista) y un partido cercano a Rusia (Partido del Centro) promovió que la reubicación se aplazara hasta después de las elecciones, el 4 de marzo (BBC 2007). No fue hasta después de la victoria del candidato reformista, Andrus Ancip, que el tema se retomó dentro del parlamento. Por último, se destaca que un discurso de Ancip, con comentarios despectivos hacia el monumento soviético, el 24 de abril, fue lo que detonó la convocatoria de protestas y consecuentes disturbios.

Escala nacional-internacional. Hasta la convocatoria de protestas en contra del gobierno, la crisis del “Soldado de Bronce” no se había transformado en un problema de ciberseguridad. Los disturbios del 26 de abril se consideraron la peor crisis de seguridad pública del país desde su independencia, pero no formaban parte de una problemática de

este tipo. El ataque cibernético se reveló al gobierno cuando este convocó a una reunión del Comité de Crisis para atender los disturbios de seguridad pública y los escenarios de inestabilidad política. Fue en esa reunión que las autoridades de Estonia recibieron la notificación de que los sitios gubernamentales habían empezado a recibir un tráfico inusual de datos, que causó problemas en los portales en línea y servicios estatales, evento que fue el inicio del ataque DDoS (Nguyen 2013).

El ciberataque perjudicó por completo la operatividad de todos los sitios del gobierno. También, portales privados y de noticias se vieron imposibilitados de compartir contenido. En el caso de los bancos, el ataque impidió operaciones como transacciones bancarias y el uso de cajeros electrónicos durante cuatro días. En este punto, resalta el papel de las agencias de noticias extranjeras, principalmente de origen ruso, que sí podían compartir información durante las protestas, mientras otros sitios no tenían esta capacidad. Eso generó desinformación (Detlefsen 2015).

En la vinculación de Estonia con el extranjero, una de las primeras acciones que ejecutó el CERT para reducir el flujo de información de *bots* fue bloquear todos los sitios de internet del extranjero, con especial énfasis en los provenientes de Rusia, ya que el 99 % de excesos de información de *bots* era de ese país (Schmidt 2013). Con estas acciones, el 30 de abril, el CERT y la policía de Tallin contuvieron el ciberataque y los disturbios en las calles. No obstante, la crisis de seguridad pública y nacional tomaría una nueva forma, al transformarse en una crisis diplomática y de política exterior, debido a las agresiones que recibió la embajadora Marina Kaljurand, en la embajada de Estonia en Moscú, que derivaron en la retirada de la diplomática de Rusia (Finn 2007).

El gobierno estonio presentó el tema de los ciberataques en su agenda de organismos multilaterales para pedir la asistencia y solidaridad de otros países. Lo hizo en la Unión Europea (UE), el 17 de mayo, durante la cumbre UE-Rusia (Martínez 2007) y, de forma unilateral, ante la Secretaría General de la Organización del Atlántico Norte (OTAN), en la que proclamó el artículo 5 de la alianza y exigió que los ciberataques fuera considerado una agresión contra todos sus miembros. La acción resultó exitosa, dado que impulsó la creación del Centro Cooperativo de Ciberdefensa de Excelencia (NATO CCDCOE por sus siglas en inglés), con la finalidad de mejorar la capacidad, cooperación e información de la OTAN ante ciberamenazas (Tamkin 2017).

Escala local-nacional-internacional. Esta escala muestra la interpenetración de la crisis del “Soldado de Bronce” en los tres niveles. La figura 2 presenta cada escala: problemáticas, actores involucrados y temporalidad de los sucesos. Expone cómo los sucesos detonadores de cada tema de seguridad difieren en cada nivel. Sin embargo, la interconexión entre la crisis de seguridad pública, el ataque DDoS como problema de seguridad nacional y la crisis diplomática y agenda de política exterior muestra una interrelación entre cada evento.

La importancia del análisis es señalar que la crisis de Tallin, al inicio, no correspondía a un problema de ciberseguridad. En un primer nivel se refería a un tema de seguridad pública en un espacio físico. Sin embargo, las condiciones y el contexto político permitieron la injerencia de actores extranjeros para utilizar la problemática local, en una plataforma (internet) que se consideraba una fortaleza de Estonia.

Por otra parte, el punto más álgido del caso de Tallin es cuando se combina la crisis de seguridad pública (en el espacio físico) y el

Figura 2. Escala local-nacional-internacional de la crisis del Soldado de Bronce y los ciberataques de Tallin (2007)

<p>LOCAL TALLIN</p> <p>Catalizador: Reubicación del Soldado de Bronce</p> <p>Problemáticas: Conflicto étnico-político Protestas y vandalismo Crisis de seguridad pública</p> <p>Actores involucrados: Policía y Alcaldía Tallin</p> <p>Temporalidad: 10 enero- 30 abril 2007</p>	<p>NACIONAL ESTONIA</p> <p>Catalizador: Comentarios del 1er Ministro Andrus Ansip</p> <p>Problemáticas: Ataque DDoS a servidores gubernamentales y privados de Crisis de seguridad Nacional</p> <p>Actores involucrados: Gobierno Estonio y Comité de Crisis, Banca Privada y Medios de Comunicación</p> <p>Temporalidad: 26 abril - 30 abril 2007</p>	<p>INTERNACIONAL ESTONIA-RUSIA-UE-OTAN</p> <p>Catalizador: Agresiones de bots de origen ruso a sitios web de Estonia y agresión a Embajadora estonia en Moscú</p> <p>Problemáticas: Crisis diplomática Estonia-Rusia</p> <p>Actores involucrados: Estonia, Rusia, UE y OTAN</p> <p>Temporalidad: 30 abril - mayo 2007</p>	<p>Escala de acción</p>
<p>Étnico-político Seguridad Pública Opinión Pública</p>	<p>Seguridad Nacional Banca Privada Economía Opinión Pública Acceso a Información</p>	<p>Diplomacia Seguridad Nacional Seguridad Regional Seguridad Internacional</p>	<p>Espacios de superposición o interpenetración</p>

Fuente: elaboración propia.

ataque DDoS a todos los servicios electrónicos del gobierno y a entidades privadas (canales de noticias e instituciones bancarias). Es en ese punto de desequilibrio que las autoridades policiales y el CERT realizan las acciones clave, en aras de encontrar una solución a ambas problemáticas.

Posteriormente, la escala local-nacional se enlaza en el ámbito internacional por las tensiones diplomáticas entre Rusia y Estonia, dado el origen de los *bots* y las agresiones que recibió la misión diplomática estonia. En conclusión, la crisis de Tallin muestra cómo los eventos del espacio físico pueden brincar al ciberespacio para vulnerar diferentes niveles de seguridad de un actor estatal, característica que define a los hechos ciberfísicos.

Cinco casos de los estudios de ciberseguridad y el régimen híbrido del ciberespacio

En este apartado se discute cómo una ciberamenaza, desde la comprensión de una ENCS, es aquella que tenga implicaciones, consecuencias o impacto tanto en el espacio físico o material como en el virtual.

Para esto, se añaden al caso de Tallin otros cuatro casos de interés para los estudios de ciberseguridad: 1) el *Cablegate* de los papeles del Departamento de Estado de los Estados Unidos (Farrel y Finnemore 2013; Medcalf 2011); 2) el uso de redes sociales durante la Primavera Árabe (Auragh 2012; Bachrach 2011); 3) el gusano *Stuxnet*, que atacó la base nuclear de

Tabla 1. Hechos ciberfísicos, narrativa virtual, material y espacios de interpenetración

Casos de análisis	Narrativa virtual	Narrativa material	Espacios de interpenetración
1. Ciberataques de Tallin (2007)	a. Ataque DDoS a todos los sitios gubernamentales y de empresas privadas. b. Interrupción de servicios bancarios y noticias.	a. Conflicto étnico-político entre estonios y rusos y protestas sociales. b. Traslado del Soldado de Bronce.	Seguridad pública y nacional. Ciberseguridad. Economía. Opinión pública.
2. Cablegate (2010)	a. Extracción de 251 a 287 documentos del Departamento de Estado. b. Publicación de los primeros 291 cables en cinco diarios internacionales y publicación del resto.	a. Tensión diplomática entre EEUU y países referidos en los cables. b. Atención en medios de comunicación y publicaciones de <i>The Guardian</i> , <i>The New York Times</i> , <i>El País</i> , <i>Le Monde</i> y <i>Der Spiegel</i> , y quejas diplomáticas.	Política nacional y diplomacia. Seguridad nacional. Ciberseguridad. Opinión pública
3. Uso de redes sociales en la Primavera Árabe.	a. Uso libre, sin restricciones de libertad de opinión, de la internet en Egipto y Túnez. b. Promoción de debates sociales respecto al régimen autoritario en Twitter y Facebook. c. Organización de protestas a través de redes sociales.	a. Protestas sociales en contra del régimen autoritario y la represión policiaca y militar contra civiles. b. Renuncia de los mandatarios o jefes de Estado y reestructuración política.	Política nacional. Seguridad pública y nacional. Ciberseguridad. Opinión pública.
4. Stuxnet (2010)	a. Planeación y diseño de un ciberataque entre actores estatales (EEUU e Israel) y no estatales (Microsoft). b. Creación de un <i>malware</i> con capacidad de afectar las centrífugas Siemens S7-315, y afectación de más de 1000 sistemas informáticos en la Central Nuclear Natanz, Irán.	a. Daños a las centrífugas de la central nuclear de Natanz, Irán. b. Retraso de tres años del programa nuclear iraní.	Seguridad nacional. Infraestructura crítica. Ciberseguridad.
5. LuzlSec (2011)	a. Protesta cibernética en contra de PayPal y Master Card. b. Convocatoria, amenaza y realización de ciberataques a sitios gubernamentales y empresas por 50 días.	a. Imposibilidad de usar redes públicas (FBI y CIA) y privadas (Sony y AT&T). b. Interrupción de comunicaciones y servicios gubernamentales y pérdidas económicas de la empresa.	Seguridad privada y gubernamental. Ciberseguridad. Hacktivismo económico.

Fuente: elaboración propia.

Natanz, Irán (Detlefsen 2015; Lagner 2013) y 4) el conjunto de ciberataques a empresas privadas y portales gubernamentales del grupo hacktivista *LulzSec* (DiSanto 2015; Thaw 2013). En la tabla 1 se presenta el resumen del análisis, las implicaciones o consecuencias de la narrativa virtual y material, y los espacios de superposición e interpenetración.

La tabla 1 muestra al menos tres esquemas de análisis para cada caso de estudio: a) las escalas de seguridad (local, nacional o internacional); b) la interdependencia y cooperación de los actores o partes interesadas, que pueden ser gubernamentales o públicos (gobiernos nacionales o locales, instituciones policíacas) y privados (empresas, medios de comunicación, bancos, etc.); y c) la materialización de los efectos de una ciberagresión tanto en el ciberespacio como en el espacio físico.

Hechos ciberfísicos en el régimen híbrido del ciberespacio

El concepto de hecho ciberfísico representa una categoría de análisis para delimitar eventos, casos o unidades de estudio en que las dinámicas o procesos sociales tienen repercusiones, impactos o consecuencias que vinculan a internet y al espacio material. Pretende servir a los estudios de ciberseguridad y a los creadores de políticas de ciberdefensa y ciberseguridad. El argumento central de los hechos ciberfísicos es exponer que existen eventos que tienen efectos tanto en el mundo material como en el virtual. Asimismo, al manifestarse dentro de un espacio sin fronteras (como internet), estos pueden saltar a diferentes niveles e incluir a múltiples actores gubernamentales, nacionales o privados.

El concepto contempla cualquier canal de comunicación de la sociedad y sus actores (po-

lítica, economía, comercio, cooperación internacional, etc.). En ese sentido, responde a la noción de que el ciberespacio es un régimen híbrido con características materiales e inmateriales, cuyos componentes físicos y virtuales coexisten en el mundo real, y con capacidad de impacto en las dinámicas sociales (Nye 2010; Demchak 2012).

La comprensión de lo ciberfísico como esquema de análisis híbrido de un fenómeno social puede mejorar con la comparación de conceptos semejantes como lo glocal y el enfoque de seguridad interdoméstico. El término glocal fue utilizado ampliamente dentro de la teoría social a finales del siglo XX, para analizar fenómenos y dinámicas sociales derivados del proceso de globalización, en que la reducción de fronteras (económicas, financieras, políticas, etc.) cambió las características típicas de los espacios locales y globales, entre los que era cada vez más indisociable determinar los límites de lo provincial e internacional. Así, glocal es un neologismo que combina ambas categorías. Fue utilizado para describir el incremento de la interacción de las fuerzas de la economía global con las respuestas de las comunidades locales y regionales, noción que promovió una nueva escala de análisis de la organización socio-territorial del Estado nación (Taylor 1996). Posteriormente, se usó para explicar fenómenos como los procesos de integración económica (Keeling 2004), las dinámicas financieras y multiculturales de grandes urbes (Curtis 2011; Sidaway 2006) y los fenómenos derivados de la migración (Hoerder 2010; Van Wijk y Bolhuis 2017).

Por otra parte, el enfoque de seguridad interdoméstica surgió como una categoría de análisis en el período posterior a la Guerra Fría. En ese momento se consideró obsoleta la visión de la seguridad nacional centrada en la

integridad territorial, frente a nuevas amenazas y retos para la seguridad nacional (Lindstrom y Luijff 2012). Sirvió para la creación de los complejos regionales de seguridad en América, con lo que promovió una reinterpretación del concepto de seguridad más allá del aspecto militar, para incluir amenazas de diverso tipo o no tradicionales (Buzan, Waever y De Wilde 1998). Acuerdos de cooperación regional y procesos de integración económica incluyeron en su agenda asuntos como crimen organizado, narcotráfico, estabilidad política, migración, ecología y terrorismo (Benítez 2005).

Ambos términos ejemplifican cómo lo ciberfísico responde a una reconceptualización para abordar fenómenos de características híbridas, como los que competen a los estudios de ciberseguridad. En la figura 3 se representa el régimen de análisis mixto que distingue a los hechos ciberfísicos, emparentado con ambos términos citados.

Interacción, cooperación y conflicto en el ciberespacio: actores y partes interesadas

La interacción de los actores del ciberespacio es otro asunto de interés dentro de la propuesta

de los hechos ciberfísicos, dada la necesidad de enmarcar a los protagonistas del ciberespacio y localizar unidades de estudio que permitan utilizar la categoría. Esta acción es necesaria para que los estudios del ciberespacio puedan crear y operacionalizar estrategias dirigidas a construir una agenda de ciberseguridad.

La comprensión de los protagonistas del ciberespacio, desde el enfoque de la seguridad nacional, corresponde a una visión que pone en el centro al Estado nación y a los actores gubernamentales. No obstante, esta visión de seguridad acepta que, para promover una estrategia efectiva para crear protocolos o estrategias de ciberseguridad, es necesaria la participación de actores privados y no estatales. Una propuesta sólida en esa óptica es la de las partes interesadas (*stakeholders* en el texto en inglés), que clasifica a los actores del ciberespacio en tres grandes grupos (Klimburg y Healey 2012).

El primero son los actores estatales, en concreto, Estados nación e instituciones gubernamentales. Son entidades con los mejores y sofisticados recursos para influir en el ciberespacio, dada la capacidad de componer grandes equipos de seguridad informática y al hecho de que poseen infraestructura en telecomunicaciones. Entre las ventajas que los distinguen está ser entidades de gran tamaño

Figura 3. Categorías de análisis híbrido: seguridad interdoméstica, glocal y hechos ciberfísicos de Tallin (2007)



Fuente: elaboración propia con base en (Buzan, Waever y De Wilde 1998; Beck 1998).

y abarcar múltiples unidades de gobierno (locales, regionales o nacionales), así como diferentes esferas de influencia (política, educativa, comercial, etc.). Es muy complicado que una ciberamenaza afecte la totalidad de sus componentes. Otra fortaleza es que detentan un marco de normas legales e instituciones de justicia para someter a un ciberagresor. Entre sus desventajas está su lenta capacidad de reacción, dada la gran cantidad de unidades gubernamentales que deben coordinar. En esa clasificación se incluyen actores como Estados nación, organismos internacionales o regionales y gobiernos subnacionales.

El segundo grupo son los actores no estatales organizados. Comprende a las entidades fuera del Estado nación y de carácter privado con un nivel mínimo de organización. Entre estas se encuentran los creadores del *hardware* y *software* utilizado en el ciberespacio. Son las principales víctimas de ciberagresiones y delitos, a la vez que ejecutan la mayoría de las ciberoperaciones de internet, ya sea por intereses particulares o para apoyar a un gobierno. Los estudios de ciberseguridad ponen especial atención en estos actores, dado que poseen una capacidad de reacción más rápida que los actores estatales. Entre ellos se encuentran empresas de *software*⁵ (Microsoft, Linux, etc.), empresas de seguridad informática (McAfee, Norton) y prestadores de telecomunicaciones (AT&T, Vodafone...), al igual que los más peligrosos grupos de ciberdelincuentes (mafias y delincuencia organizada). Este grupo engloba: empresas transnacionales y de *software*, portadores de telecomunicaciones, ONG, grupos criminales y grupos terroristas.

⁵ Son empresas que diseñan *software* o soporte lógico de un sistema informático, lo cual comprende los componentes que hacen posible la realización de tareas específicas y todas las funciones que permite un ordenador.

El tercer grupo son los actores no estatales no organizados, que realizan operaciones o campañas de bajo nivel en el ciberespacio. Ese tipo de acciones son conducidas por pequeños grupos de individuos, sin nivel de jerarquía, o por actores individuales. Una característica suya es la ausencia de una autoridad o cadena de mando, que limita su nivel de operación y capacidad de daño. A diferencia de las grandes organizaciones criminales o grupos delictivos bien estructurados, este tipo de actores no desempeñan actos de cibercrimen de alto valor, además de que sus campañas son de corta duración. La clasificación engloba: hacktivistas, pequeños grupos criminales e individuos autónomos.

Por otra parte, un proceso de interacción en el ciberespacio supone dos vías: la cooperación o el conflicto. De acuerdo con Kello (2013), esta dinámica se presenta en cuatro escenarios.

- Estatal a estatal: corresponde a una acción en el ciberespacio ejecutada por un actor estatal o gobierno hacia otro actor de las mismas características.
- Privado a estatal: representa los ciberataques u operaciones de actores no estatales organizados o no organizados, dirigidos a activos estratégicos de Estados o gobiernos.
- Privado a privado: señala los procesos de cooperación o agresión entre dos entidades no estatales, ya sean estas organizadas o no organizadas.
- Estatal a privado: define la colaboración o agresión de un gobierno o actor estatal con una entidad privada, ya sea organizada o no organizada.

Estudio de caso: comprensión de los ataques al SPEI desde los hechos ciberfísicos

El marco de análisis de los hechos ciberfísicos puede aplicarse al caso concreto de México, y la crítica a su ENCS, en dos importantes ciberataques al Sistema de Pagos Electrónicos Interbancarios (SPEI) del Banco de México (BM), en 2018. El primero fue detectado a finales del mes de abril e involucró a tres bancos privados, una casa de bolsa y una caja de ahorro popular. Se estima que hubo pérdidas de alrededor 300 000 000 de pesos (Valdelamar 2018).

El segundo fue ejecutado en octubre de 2018, a través de la aseguradora AXA, institución privada mediante la cual los agresores infiltraron el SPEI y realizaron múltiples operaciones anómalas. Tras ese ataque, tres instituciones gubernamentales —el BM, la Secretaría de Hacienda y Crédito Público (SHCP)

y la Comisión Nacional Bancaria y de Valores (CNBV)— elevaron a rojo el nivel de alerta de seguridad informática en las operaciones del SPEI (Estañol 2018). Posteriormente, la firma de ciberseguridad *Fire Eye* expresó que el culpable del ciberataque fue el equipo de hackers APT38, una cédula norcoreana encargada de ejecutar ciberataques a bancos de naciones extranjeras para obtener recursos para su país, famosos por haber vulnerado 16 instituciones bancarias en 11 países y haber extraído 100 000 000 de dólares (Lara 2018).

Los ataques al SPEI presentan una importante área de oportunidad para consolidar una agenda de ciberseguridad y delimitar el nivel de impacto de las ciberamenazas, en la cual se puede utilizar el esquema de los hechos ciberfísicos, dada la importante afectación que sufrieron el BM y las partes interesadas, que no contempla la ENCS de México. En la tabla 2 se presenta un análisis desde esta propuesta.

Tabla 2. Análisis de ataques al SPEI como hechos ciberfísicos

Caso de análisis	Narrativa virtual	Narrativa material	Escalas	Partes Interesadas	Tipo de ataque
Ataques al SPEI en México (2018)	A. 1er ataque en abril: involucró a tres bancos privados, una casa de bolsa y una caja de ahorro popular.	A. El prestigio de los bancos, clientes y activos se vio afectado, con pérdidas de 300 000 000 de pesos.	A. Escala local-nacional: dado que afectó a instituciones bancarias locales y nacionales.	A. Actores estatales: BM, SHCP y CNBV. Actores no estatales organizados: casa de bolsa, caja de ahorro popular y APT38.	A. Privado a Estado; privado a privado. B. Privado a Estado Estado a Estado.
	B. 2do ataque en octubre: a través de AXA, por quien se infiltraron el SPEI.	B. El BM, la SHCP y la CNBV elevaron a rojo el nivel de alerta de seguridad informática en las operaciones del SPEI, afectando todas sus operaciones.	B. Escala nacional-internacional: dado que afectó al BM y a una aseguradora de origen francés. Asimismo, los atacantes eran de Corea del Norte, Estado agresor.	B. Actores estatales: BM, SHCP, CNBV. Actores no estatales organizados: APT38, <i>Fire Eye</i> y AXA.	

Fuente: elaboración propia.

Conclusiones

Las ENCS en América Latina y México están alejadas de la comprensión actual de las ciberamenazas y el potencial del ciberespacio para vulnerar la seguridad pública y nacional. Esta distancia explica el alto grado de incremento anual de ciberagresiones entre los Estados de la región y el hecho de que detente las tasas globales más altas de infección por virus maliciosos y ciberataques a instituciones bancarias, junto con Asia.

El análisis devela que las ENCS no contemplan protocolos que involucren diferentes escalas de análisis (local, nacional e internacional), así como protocolos de acción o vinculación entre las partes interesadas del ciberespacio (actores estatales, actores no estatales organizados y no organizados) para la prevención de ciberamenazas.

La ausencia de vínculos entre actores públicos y privados ha incrementado los ciberataques a bancos y actores privados. La poca presencia de ataques de corte político como ciberespionaje, hacktivismo o ataques a INC ha hecho que las ENCS no tengan protocolos concretos en contra de este tipo de agresiones. Otro aspecto importante es que no existe una acción de aprendizaje, estudio o análisis de casos de trascendencia que involucren al ciberespacio y su impacto en el espacio material y virtual, para crear una ENCS y determinar los grados de impacto de una ciberagresión.

En México, la ENCS es ambigua y confunde la disminución de la brecha digital entre la población con la necesidad de poseer una política de ciberseguridad y el desarrollo de capacidades de resiliencia. Es necesario crear un organigrama de responsabilidades y atribuciones de las instituciones públicas y privadas encargadas de la ciberseguridad y homologar las

legislaciones nacionales vinculadas al ciberespacio. El gobierno mexicano debe aprovechar la disposición de la industria privada para crear una Agencia Nacional de Ciberseguridad, a la par de actualizar su catálogo de INC, con división de responsabilidades de su administración entre entidades públicas y privadas.

La propuesta de análisis de los hechos ciberfísicos sirve para comprender cómo una amenaza surgida en el ciberespacio se traslada al espacio físico, y viceversa. También ayuda a delimitar las partes interesadas que construyen una ENCS efectiva, los niveles y esferas de impacto, y los tipos de clasificaciones para los diferentes ciberataques. Después de la revisión de los cinco casos seleccionados, se considera que la propuesta se ajusta al análisis de los ataques al SPEI en México (2018), y puede ser replicada a otro estudio de caso en materia de ciberseguridad.

Bibliografía

- Auoragh, Miriyam. 2012. "Social Media, Mediation and the Arab Revolutions." *TripleC* 10 (2): 518-36.
- Bachrach, Judy. 2011. "Wikihistory: Did the Leaks Inspire the Arab Spring?". *World Affairs* 174 (2): 35-44.
- BBC News. 2007. "Tallinn tense after deadly riots". 28 de abril, <http://news.bbc.co.uk/2/hi/europe/6602171.stm>
- Beck, Ulrich. 1998. *¿Qué es la globalización?* Barcelona: Paidós.
- Benítez, Raúl. 2005. "Defensa y seguridad hemisférica hacia el siglo XXI: el desafío de la cooperación multinacional". En *Seguridad Hemisférica: debates y desafíos*, editado por Raúl Benítez, 11-31. México: UNAM/CISAN.
- Buzan, Barry, Ole Wæver, y Jaap de Wilde. 1998. "Security: A New Framework for Analysis". Boulder: Lynne Rienner.

- Calderón, José. 2018?. "Infraestructura crítica en México: el enfoque hacia el futuro", 3 de mayo, <https://bit.ly/2KBqepW>
- Cornaglia, Silvina, y Ariel Vercelli. 2017. "La ciberdefensa y su regulación legal en Argentina (2006-2015)". *Urvio. Revista Latinoamericana de Estudios de Seguridad*, 20: 46-62. doi.org/10.17141/urvio.20.2017.2601
- Curtis, Simon. 2011. "Global Cities and the Transformation of the International System". *Review of International Studies* 37 (4): 1923-1947.
- Demchak, Chris. 2012. "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure." *Journal of Comparative Policy Analysis: Research and Practice* 14 (3): 254-269.
- Detlefsen, William. 2015. *Cyber Attacks, Attribution, and Deterrence: Three Case Studies*. Leavenworth: US Army Command and General Staff College.
- DiSanto, Philip. 2015. "Blurred Lines of Identity Crimes: Intersection of the First Amendment and Federal Identity Fraud". *Columbia Law Review* 115 (4): 941-82.
- ENCS (Estrategia Nacional de Ciberseguridad) de México. 2017. 31 de mayo de 2019, <https://bit.ly/2AEvAtU>
- Espinosa, Iván. 2015. "Hacia una estrategia nacional de ciberseguridad en México". *Revista de Administración Pública* 50 (1): 115-147.
- Estañol, Adrián. 2018. "La aseguradora AXA sufre un ciberataque en el Sistema de Pagos Electrónicos". *Expansión*, 23 de octubre, <https://expansion.mx/empresas/2018/10/23/axa-sufre-un-ciberataque-en-el-spei>
- Farrell, Henry, y Martha Finnemore. 2013. "The End of Hypocrisy: American Foreign Policy in the Age of Leaks". *Foreign Affairs* 92 (6): 22-26.
- Finn, Peter. 2007. "Protesters in Moscow Harass Estonian Envoy Over Statue". *The Washington Post*, 3 de mayo, <https://wapo.st/2Kv0Y61>
- García, Arturo. 2018. *Ciber México: voluntades y acciones en el ciberespacio*. S.L.: IUS Ediciones.
- Gómez Navarro, Dulce Angélica, Raúl Arturo Alvarado López, Marlen Martínez Domínguez, y Christian Díaz de León Castañeda. 2018. "La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México". *Entreciencias: Diálogos en la Sociedad del Conocimiento* 6 (16): 49-64.
- Hansen, Lene, y Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly* 53 (4): 1155-1175.
- Hoerder, Dirk. 2010. "Recent Methodological and Conceptual Approaches to Migration: Comparing the Globe or the North Atlantic World?". *Journal of American Ethnic History* 29 (2): 79-84.
- Hughes, Rex. 2010. "A Treaty for Cyberspace". *International Affairs* 86 (2): 523-541.
- INEGI (Instituto Nacional de Estadística y Geografía). 2018. "Comunicado de Prensa Núm. 105/18". <https://bit.ly/2MWpoab>
- Keeling, David. 2004. "Latin American Development and the Globalization Imperative: New Directions, Familiar Crises". *Journal of Latin American Geography* 3 (1): 1-21.
- Kello, Lucas. 2013. "The meaning of the Cyber Revolution: Perils to Theory and Statecraft". *International Security* 38 (2): 7-40.
- Klimburg, Alexander, y Jason Healey. 2012. "Strategic Goals and Stakeholders". En *National Cyber Security Framework Manual*, editado por Alexander Klimburg, 66-107. Tallin: NATO/CCD/COE.
- Lara, Paul. 2018. "Atacaron al SPEI crackers norcoreanos, asegura firma de EU". *Excelsior*, 4 de octubre, <https://bit.ly/2ySnW08>
- Langner, Ralph. 2013. "To Kill a Centrifuge-A Technical Analysis of What Stuxnet's Creators Tried to Achieve." Hamburgo: The Lagner Group.

- Lindstrom, Gustav, y Eric Luijff. 2012. "Political Aims & Policy Methods. En *National Cyber Security Framework Manual*, editado por Alexander Klimburg, 66-107. Tallin: NATO CCD COE.
- Martínez, Ricardo. 2007. "Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE". *El País*, 18 de mayo, https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html
- Medcalf, Rory. 2011. "Diplomacia, transparencia y opinión pública". *Política Exterior* 25 (141): 114-121.
- Nguyen, Reese. 2013. "Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare". *California Law Review* 101 (4): 1079-129.
- Norton. 2018. "Norton Cyber Security Insights Report Global Results", <https://symc.ly/2G8VNnU>
- Nye, Joshep. 2010. *Cyber Power*. Cambridge: Harvard University Press.
- OEA (Organización de los Estados Americanos). 2018. "Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe", <https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf>
- OEA (Organización de los Estados Americanos) y Symantec. 2014. "Tendencias de Seguridad Cibernética en América Latina y el Caribe", <https://symc.ly/2Ownq0i>
- PandaLabs. 2015. "Informe Anual 2014". <https://bit.ly/2GYRy08>
- Parraguez, Luisa. 2018. "Quo Vadis? Mexico's National Cybersecurity Strategy", Wilson Center, 31 de mayo, <https://bit.ly/2TpovYY>
- Pessiri, Paolo. 2019. "2018: A Year of Cyber Attacks". *Hackmageddon*, 15 de enero, <https://bit.ly/2Da7k7d>
- Schmidt, Andreas. 2013. "The Estonian Cyberattacks". En *The fierce domain. Conflicts in cyberspace 1986-2012*, editado por Jason Healey, 168-193. Washington, D.C.: Atlantic Council.
- Sidaway, James. 2006. "On the Nature of the Beast: Re-Charting Political Geographies of the European Union". *Geografiska Annaler. Series B, Human Geography* 88 (1): 1-14.
- Tamkin, Emily. 2017. "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?". *Foreign Policy*, 27 de abril, <https://bit.ly/2HCvY4H>
- Taylor, J. Peter. 1996. "Embedded Statism and the Social Sciences: Opening up to New Spaces". *Environment and Planning* 28 (11): 917-928.
- Thaw, David. 2013. "Criminalizing Hacking, Not Dating: Reconstructing The CFAA Intent Requirement". *The Journal of Criminal Law and Criminology (1973-)* 103 (3): 907-948.
- UIT (Unión Internacional de Telecomunicaciones). 2014. "Índice mundial de ciberseguridad y perfiles de ciberbienestar", <https://bit.ly/2H0e6xL>
- Valdelamar, Jassiel. 2018. "5 entidades y 300 mdp, involucrados en ciberataque: Banxico". *El Financiero*, 16 de mayo, <https://elfinanciero.com.mx/economia/5-entidades-fueron-afectadas-por-ciberataque-banxico>
- Van Wijk, Joris, y Maarten Bolhuis. 2017. "Awareness Trainings and Detecting Jihadists among Asylum Seekers: A Case Study from The Netherlands". *Perspectives on Terrorism* 11 (4): 39-49.

Reconceptualizando la relación entre tecnología, instituciones y guerra

Reconceptualizing the Relationship between Technology, Institutions and War

Alfredo-Leandro Ocón¹ y Aureliano da Ponte²

Recibido: 2 de junio de 2019

Aceptado: 25 de julio de 2019

Publicado: 2 de diciembre de 2019

Resumen

El estudio de la guerra y la capacidad de generar categorías o tipologías inmunes a la crítica ha sido un desafío histórico en el que persisten importantes debates. El presente artículo, de carácter cualitativo descriptivo, presenta un análisis histórico conceptual que indaga sobre la interacción entre la tecnología y las instituciones, así como su impacto en la forma de hacer la guerra, a fin de distinguir las condiciones estructurales de aquellas contingentes. La hipótesis planteada es que las convenciones y la tecnología son dimensiones estructurantes en cuanto a las opciones estratégicas de los actores al momento del choque de intereses. Como resultado, se evidencian factores que hacen novedosa la praxis de la guerra, pero en esencia se mantienen rasgos distintivos permanentes, más allá de la coyuntura histórica.

Palabras clave: convencionalidad; guerra; instituciones; tecnología; asimetría

Abstract

The study of war and the ability to generate categories or typologies immune to criticism has been a historic challenge in which important debates persist. This qualitative article presents a conceptual historical analysis of the interaction between technology and institutions, and their impact on the way of making war, aiming to differentiate the structural conditions from those of a contingent nature. The hypothesis stated is that conventionality and technology are structuring dimensions in terms of the strategic options of the actors at the time of the clash of interests. The results show factors that make the practice of war novel, but some permanent distinctive features beyond the historical juncture are essentially maintained.

Keywords: conventionality; institutions; asymmetry; technology; war

1 Universidad de la Defensa Nacional, Argentina, leandro.ocon@gmail.com,  orcid.org/0000-0002-6731-566X

2 Universidad de la Defensa Nacional, Argentina, aureliano.daponte@gmail.com,  orcid.org/0000-0003-4529-1772



Introducción

A lo largo de los últimos 30 años, el escenario de la seguridad internacional contemporánea ha experimentado importantes transformaciones (Bartolomé 2017). El tradicional panorama signado por conflictos armados interestatales, instrumentados a través de instituciones militares, ha sido alterado por el incremento cuantitativo de contiendas de difícil categorización, dada la variedad cualitativa de actores involucrados.

Las diferentes propuestas de denominación de los eventos armados, preponderantes, aunque no exclusivos en la post Guerra Fría, redundaron en una nutrida “proliferación semántica”: nuevas guerras, conflictos de cuarta (quinta, sexta, etc.) generación, ciberguerra, pequeñas guerras y/o guerras moleculares. A este listado, que en modo alguno pretende ser exhaustivo, se agregó más recientemente la idea de “guerra híbrida”, surgida en el marco de la llamada Segunda Guerra del Líbano, de 2006.

Las primeras teorizaciones sobre el concepto, correspondientes a Frank Hoffman (2007; 2009), colocaron el foco de la hibridación en dos variables que operan de manera autónoma, sin ser mutuamente excluyentes: la combinación entre modos simétricos y asimétricos de ejercicio de la violencia; y entre protagonistas estatales y no estatales dentro de un mismo bando en pugna. Elaboraciones posteriores situaron la clave en la utilización de medios militares de manera abierta o encubierta, con el empleo intensivo de los medios de comunicación y el desarrollo de operaciones en el dominio cibernético. El empleo de la violencia, en tanto elemento racional de política, se alejó de los cánones convencionales para dar lugar a lo que actualmente se denomina “asimetría”.

Los conflictos actuales proponen un desafío intelectual: ¿qué tienen de común entre sí y con otros tantos de la historia de la humanidad? ¿Qué los hace novedosos? Por un lado, el rol de la tecnología, factor que ha modificado profundamente su dinámica. Por otro lado, el tipo de actor involucrado y sus características intrínsecas, insertas en un contexto determinado, ponen de manifiesto otra dimensión relevante: la convencionalidad. En todo caso, se registra un contingente académico que reconoce que la guerra, ante todo, es un fenómeno que responde a las realidades históricas.

Desde las denominadas Ciencias Militares, las Relaciones Internacionales y la Ciencia Política, los intentos por revelar el futuro de la guerra han propuesto una amplia variedad de alternativas. El denominador común ha sido la proliferación conceptual, anclada a la aspiración prognóstica del futuro de la guerra en el paradigma de que la “guerra cambia”. Este punto es, en muchos aspectos, cierto, pero esencialmente discutible. Es diferente afirmar que no cambia, en lugar de que lo que cambia es la forma de hacer la guerra.

La complejidad del estudio de la guerra y la capacidad de generar categorías o tipologías inmunes a la crítica ha sido un desafío histórico en el que persisten importantes debates (Aznar Fernández-Montesinos 2015a; 2015b). Parte de la literatura reciente que ha estudiado sus cambios y transformaciones se concentra no solo en la coyuntura histórica, sino también en los cambios tecnológicos.

Sin embargo, los resultados de los conflictos no se encuentran necesariamente vinculados al simple cálculo de victoria por superioridad tecnológica. La respuesta de actores inferiores, en términos de instrumentos militares y grado de desarrollo tecnológico, han sido en muchos casos una lúcida articulación

estratégica y táctica, que les ha permitido convertir las debilidades en fortalezas. La convencionalidad comenzó a ser una variable prioritaria en los estudios contemporáneos.

A grandes rasgos, se pueden distinguir dos grandes corrientes, con sus propios debates internos y divergencias, en lo que respecta a la reflexión sobre la guerra. La primera, que se podría denominar holística, profundiza en su naturaleza y esencia, e identifica atributos generales que trascienden la coyuntura histórica. Ejemplo de ello son autores clásicos como Sun Tzu, con su obra *El arte de la Guerra*, y Carl von Clausewitz, con *De la Guerra*. En cambio, la segunda corriente entiende que el fenómeno se encuentra en constante cambio y responde exclusivamente a una serie de peculiaridades histórico-coyunturales, por lo que es posible tipificarlo en función de los climas de época y sus propias características. Esa racionalidad se sustenta en una amplia gama de variables, desde “las causas de la guerra” hasta “los rasgos distintivos epocales”. Lo ilustran las guerras napoleónicas, las guerras coloniales e incluso “las guerras del siglo XXI”.

De la segunda corriente surge una serie de trabajos y conceptos anclados en una mirada “teleológica”, que demarca la existencia de generaciones de conflictos cuyo principal impulsor es la tecnología. Los principales exponentes de esa visión son Lind et al (1989) y Van Crevelde (1991). Las advertencias de Lind et al (1989) a raíz de muchos de los fenómenos registrados en la realidad, particularmente desde la Guerra de Vietnam y luego el atentado de las torres gemelas, han puesto en perspectiva hasta qué punto la superioridad del instrumento (en calidad y cantidad) conlleva la victoria militar o una mejor seguridad nacional.

El objetivo de este artículo es contribuir a superar las dificultades conceptuales y los re-

duccionismos académicos a partir de demostrar que existe una interacción histórica entre la tecnología y las convenciones, que da forma *ex post* a la dinámica de cómo se hace la guerra. En todo caso, la firma de convenciones, su respeto y la tecnología disponible son todas opciones estratégicas de los actores a la hora de abordar un conflicto.

La investigación tiene carácter descriptivo. El abordaje metodológico es cualitativo y se apoya en el análisis histórico conceptual y la utilización de fuentes secundarias. El artículo se divide en cuatro apartados, más las conclusiones. El primero indaga en la problemática conceptual, metodológica y lingüística de la palabra guerra, que es en definitiva el objeto de estudio. En los siguientes apartados se analizan de forma cualitativa las variables mencionadas arriba y su incidencia. El segundo enfoca la atención en la convencionalidad, sus límites y alcances, así como su impacto en el estudio y la conceptualización del fenómeno. El tercero incorpora al análisis el rol del factor científico-tecnológico. El cuarto considera la interacción entre ambas variables. Por último, se sintetizan los principales hallazgos en el marco de reflexiones integradoras.

Guerra: significados, significantes y categorías

La palabra guerra proviene del antiguo germánico *werra* –y no del latín *bellum*–, que da origen a la acepción sajona *war*, que significa pelea, desorden o disputa. En la primera página de la obra maestra de Clausewitz (2009, 13) se define a la guerra, en esencia, como un duelo en una escala más amplia. Para el autor, “la guerra constituye un acto de fuerza que se lleva a cabo para obligar al adversario a acatar nuestra voluntad”.

Un gran estudioso de Clausewitz como Foch (1920), en función de sus experiencias de la conflagración franco-prusiana, describe cómo esta muta en su célebre *Los principios de la Guerra*. Tal vez de ahí nace su paradójica contribución conceptual y la tensión subyacente entre lo estructural y lo contingente. Dicho de otra manera, aquello que varía, pero que contiene a su vez una serie de principios generales.

Los aportes de Abluso, Alcántara y Tutusaus (2014, 174) ponen de manifiesto la problemática sobre las definiciones de guerra, ya que “la forma de hacer, de pensar y, por ende, de estudiar la guerra, ha variado a lo largo de la historia”. Para los autores, es como un “verdadero camaleón”, que cambia a lo largo del tiempo. Esa visión se suma a la de Bartolomé (2017, 61-62), quien señala que en la actualidad “la rigidez del concepto guerra ha disminuido, en la medida en que se flexibilizaron los contornos de la seguridad internacional, lo que ha incorporado nuevos enfoques y perspectivas”.

Recuperando la propuesta teórica de Foucault (2010), quien entiende que los cambios históricos conceptuales obedecen en gran medida a un problema inherente al lenguaje del hombre como objeto y sujeto de las ciencias humanas o, en los términos del autor, a la relación de las palabras y las cosas (Foucault 1968), ¿existe tal cosa como la “esencia de la guerra”? O en cambio ¿estamos sujetos a un sinnúmero de significados subsumidos a las cambiantes coyunturas históricas?

Ambas preguntas revelan una importante tensión metodológica, puesto que, si la guerra se transforma ante los cambios en las coyunturas históricas, las convenciones y la tecnología, ¿por qué dos eventos bélicos entre los que median 2000 años, tales como las Guerras del Peloponeso y la Segunda Guerra Mundial responden a un mismo vocablo? Por lo ge-

neral, la literatura escrita en inglés diferencia conceptualmente la guerra, *war*, de cómo se hace o práctica, *warfare*. Las traducciones de ambas palabras en español se reducen a una. Por ejemplo, cuando se habla de guerras de 4ta generación, en realidad se alude a *warfare* y no a *war*.³

De esta forma, se pueden observar dos abordajes simultáneos en el estudio y la aproximación a la guerra: por un lado, el que en esencia cree que se modifica y, por otro, el que sostiene que el principio esencial se mantiene inmutable, a diferencia de sus manifestaciones.

Aun así, la literatura anclada en el paradigma “de la guerra siempre cambiante” no solo ha inundado al pensamiento militar, estratégico y político de categorías, sino que apela a la búsqueda de tendencias futuras creando profundas confusiones lógico-epistémicas. Los debates sobre las guerras futuras adquieren un sentido paradójicamente esencialista y tajante: ¿cuál será la guerra del futuro?, asumiendo que esta se encuentra en permanente evolución. El campo epistémico se ha tornado una carrera futurológica de especialistas que buscan definir el presente con nuevas palabras, para poder pronosticar el futuro. La contradicción yace, pues, en una teleología conceptual que niega de alguna manera rasgos generales de la guerra y, sin embargo, apela a establecer una categoría general a una serie de conflictos contemporáneos al momento de la observación.

Almäng (2019) se acerca al abordaje de la guerra y la paz, con las dificultades que ello conlleva. Para el autor, el principal problema descansa en la vaguedad de dichos conceptos.

³ Dicha situación es observable también en el caso del idioma alemán, en el cual se distingue *krieg* de *Kriegsführung*, que responden a las respectivas acepciones anglosajonas de *war* y *warfare*. El francés sufre de la misma “desventaja” del español, ya que *war* y *warfare* se traducen como *guerre*.

Considera que cualquier tipo de lineamiento para definir recae constantemente en un problema lógico-empírico. De esa forma, destaca la dificultad de las definiciones de guerra y de paz, producto de la paradoja de sorites. A fin de resolver el dilema, adopta los aportes de Raffman (2014) sobre la imprecisión de las palabras, en particular guerra y paz, para proponer una nueva tipología de conflictos. En definitiva, agrega más categorías a las existentes.

La problemática señalada no es novedosa en las ciencias sociales. Weber ya advertía acerca de la importancia, pero también de las debilidades, de la utilización de tipos ideales (Alfaro 1990; Eliaeson 2000). Otra contribución es la propuesta de Sartori (1979) en la llamada escala de abstracción, en particular porque el idioma español utiliza el mismo significante (guerra) para referirse a una amplia gama de significados. A mayor abstracción, más generalidad y extensión; a mayor precisión empírica pierde generalidad, pero gana intención y precisión.

Siguiendo esa línea argumentativa, si la guerra cambia y la forma de entenderla también, podemos estar frente a dos problemas metodológicos: (a) estiramiento y malformación conceptual y/o (b) la noción de guerra ha mutado sucesivamente, por lo que carece de esencia conceptual. Consecuentemente, no existen características universales históricas.

Por otro lado, muchos enfoques contemporáneos son reduccionistas, ya que asumen que cada período de la historia está dominado por un solo modelo. El problema con ese supuesto es, sin embargo, que la evidencia empírica histórica demuestra que diversos tipos de guerra convivieron en un determinado período con otros, es decir, que pueden existir en paralelo (Tuck 2018). En ocasiones, las estrategias y tácticas “no preponderantes” fueron consideradas

obsoletas, propias de actores marginales, rudimentarias e incluso indecorosas. Esas circunstancias generaron un caos tipológico de difícil comensurabilidad. De hecho, aquellas nuevas categorías orientadas a explicar las nuevas guerras, en virtud de ese atributo, son capaces de ofrecer argumentos razonables para comprender enfrentamientos armados pasados, contribuyendo al desorden generalizado.

Los aportes de Almäng (2019) favorecen un punto fundamental: los actores involucrados en una contienda reconocen la existencia de instituciones o convenciones que, en muchos casos, optan por articular estrategias o tácticas estructuradas con base en la vaguedad de los conceptos y las normativas, en los espacios ontológicos intermedios entre las nociones de guerra y paz.

Si bien las “causas” de legitimidad que justifican una acción bélica pueden haber sido sujetos de cambios históricos, cada coyuntura ha estado marcada por un serie de convenciones (formales e informales) que los actores involucrados consienten, pero que pueden optar por respetar o no. Con la existencia de las Naciones Unidas en la actualidad, el *ius ad bellum* es un concepto inseparable de *ius in bello*, es decir, las motivaciones y las causas que conllevan una guerra legítima o justa, que de forma simultánea son inseparables de cómo se debe practicar. Esas convenciones e instituciones demarcan un “deber ser”. Por lo general no son respetadas por los actores internacionales, tal es el caso del continuo avance ruso sobre territorio ucraniano, sobre todo en Crimea, en el año 2014. Paradójicamente, el “retorno” de Crimea a Rusia es, para los rusos, una legítima anexación de un territorio que sociopolíticamente es considerado propio.

Este episodio colaboró con el incremento de atención a la literatura de Oriente prove-

niente de países como China y Rusia, que ha puesto de manifiesto interpretaciones alternativas a las teorías de la guerra de corte occidental. Por ejemplo, el concepto de guerra irrestricta de Qiao Liang y Wang Xiangsui (1999) puede considerarse en muchos aspectos un paralelismo a la noción de guerra híbrida producida en academias occidentales. Las estrategias híbridas de la gestión estratégica-militar de Putin, desde la perspectiva occidental, son lo que Nathan Dubovitsky denomina “guerra no-lineal”. La percepción geopolítica entre la polemología liberal-occidental y la nueva práctica rusa se apoya justamente en el abordaje y la aproximación estratégica frente al entramado institucional global anclado en organizaciones como la ONU. Sin embargo, como lo demuestran D’Anieri y Kuzio (2018), pese a que muchas de las herramientas utilizadas por Rusia son novedosas, la estrategia puede remontarse a la época soviética, cuando se combinaban tácticas de *dezinformatsiya*, operaciones especiales y fuerzas regulares, descripción que hoy respondería a la categoría novedosa de “híbrido”.

Así las cosas, no solo nos encontramos frente a una influencia circunstancial, sino a una estrategia política que puede oscilar a la par de los actores en una situación dada. Según Salgado y Barreiro (2018), los estudios estratégicos no se encuentran libres de instrumentalización y subjetividad. De esa forma, es necesario profundizar en aspectos que no solamente implican el accionar de actores en un campo de “vaguedad”, sino en el rol de las convenciones, sus límites y alcances. En todo caso, ¿es la guerra aquello que las convenciones e instituciones definen?

Incluso cabe señalar un problema de circularidad causal: si las instituciones son el resultado del accionar de actores, entonces resulta pertinente indagar cómo los actores estatales

y no estatales influyen tanto la estructuración como en el funcionamiento de las convenciones. Sobre esto, Rosa Brooks (2016, 218) afirma que la guerra es cualquier cosa que los Estados poderosos dicen que es.

En definitiva, las convenciones importan, pero no como un elemento determinante, sino como eje de referencia de obediencia y/o trasgresión. ¿Por qué un actor habría de transgredir o manipular las convenciones? La respuesta a primera vista es sencilla: la obediencia es perjudicial para sus fines político-estratégicos. De allí la famosa frase de Henry Kissinger: “El ejército convencional pierde si no gana. La guerrilla gana si no pierde”.

El problema conceptual de la simetría y la convencionalidad

“*Civitas filia temporis*”. Una interesante frase de Norberto Bobbio (2008), rescatada por parte de Federico Aznar Fernandez-Montesinos, que alude al célebre adagio latino “*veritas filia temporis*”: cada época tiene no solo su verdad, tal y como se señala en el original, sino también sus instituciones (Aznar Fernandez-Montesinos 2015a; 2015b)

Los intentos por establecer reglas de “conducta” y regulación de los comportamientos en la guerra, a través de convenciones, adoptaron diversas modalidades a lo largo de la historia. Ejemplos de ello son el Tratado de Kadesh entre el imperio egipcio y el hitita (data aproximadamente del año 1259 a.C.) y el *Pax Dei, Treuga Dei* que fue proclamado en el año 989 d.C., como un intento de proteger los bienes de Iglesia Católica, al campesinado y cualquier individuo inocente desarmado.

La particularidad de muchos de los conflictos contemporáneos que mezclan una gran

variedad de actores en cuanto a naturaleza, herramientas y tácticas conlleva la tradicional rotulación de “no convencional”. La adjetivación asume que existe tal cosa como la convencionalidad y, por ende, todo aquello que se aparta de los parámetros por ella establecidos es “no convencional”.

Ahora bien, el primer interrogante que se plantea es ¿qué es la convencionalidad? No se trata de una creación contemporánea, aunque a lo largo del tiempo ha ido modificándose. En ese sentido, el punto central es que la no-convencionalidad ha sido siempre una opción para aquellos actores dispuestos a asumir los costos de la ruptura con la convencionalidad.

La convencionalidad moderna se encuentra fuertemente arraigada a la construcción de la estatalidad y los acuerdos derivados de ese proceso. La construcción de nociones tales como “asimetría”, “(no)convencional”, “fuerzas (ir)regulares” e incluso “guerras híbridas” surge no solo de un saber convencional, sino de la estructura misma de la convencionalidad vigente, instaurada sobre un conjunto de entendimientos, arreglos, leyes e instituciones internacionales e intergubernamentales. El entramado de conceptos, significantes y significados de muchas de las discusiones recientes se ha edificado con base en una serie de convenciones modernas.

Tal como la raíz de la palabra lo indica, una convención es un compromiso, acuerdo, práctica o norma aceptada entre distintas partes. La convencionalidad de un conflicto yace en los usos y costumbres “aceptados” por los actores involucrados en la guerra, como resultado de tratados, acuerdos y leyes internacionales. Establece cuestiones como el uso del uniforme, los instrumentos o las prácticas permitidas y prohibidas, el rol de los comba-

tientes y no combatientes, el tratamiento de prisioneros de guerra, el empleo de cierto tipo de armamentos, etc. Estos puntos, entre tantos otros, se encuentran regulados por arreglos que aspiran a establecer cómo debe practicarse la guerra, con el fin de evitar daños innecesarios, víctimas inocentes o excesos moralmente condenables.

La “no convencionalidad” es justamente aquello que se aparta de la norma o las convenciones. Comportamientos o tácticas “irregulares” pueden observarse en diferentes contextos, cuando uno o más actores involucrados en una contienda optan por salirse de las convenciones.⁴ En general, al observar conflictos violentos, se asocia la no convencionalidad con la asimetría.

De esa forma surge un segundo interrogante: ¿cómo se vinculan las convenciones con la simetría en la guerra? La respuesta demanda al menos una definición de qué es “simetría”. Inicialmente, no parece haber acuerdo en la literatura respecto a este punto. El diccionario Merriam-Webster brinda una definición ambigua, puesto que reduce la asimetría en la guerra a la diferencia entre el poder de fuego de dos fuerzas, que generalmente involucra el uso de tácticas no convencionales por parte del más débil. Entonces, vale la pena preguntarse si el uso de tácticas no convencionales es una condición necesaria de la definición de asimetría.

Aunque en ocasiones resulta intuitiva la relación entre asimetría y no convencionalidad, es adecuado destacar que cada una tiene su propia racionalidad. Dicho de otro modo,

⁴ Es pertinente apuntar que comportamientos aislados (fuera de la norma) no necesariamente responden a una concienzuda maniobra o estrategia que busque la no convencionalidad. Es por ello que solo se considera no convencional todo aquel comportamiento sistémico y organizado que responde a una estrategia planificada.

son dos conceptos diferentes, lo que exige un análisis empírico que contemple las diferencias y no asuma patrones predeterminados. Ello incluso demuestra un problema conceptual de mayor envergadura: la definición de conflictos centrada en la visión de un actor. Por ejemplo, tal y como se puede observar en *Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict* de Andrew Mack (1975), la definición de pequeña guerra para la nación más poderosa no hace que la guerra sea pequeña para la más débil. Tal es el caso de la Segunda Guerra Indochina, que para Vietnam de ninguna manera fue percibida como “pequeña”, sino todo lo contrario. En términos actuales, desde la perspectiva vietnamita, coincide con nociones tales como guerra irrestricta o guerra total, en la que todos los medios y recursos disponibles son movilizados con el fin de destruir al enemigo.

En definitiva, el presente problema conceptual es producto de la no tan evidente conexión entre la asimetría de fuerzas y la necesidad del más débil de recurrir a acciones e instrumentos no convencionales, si desea tener oportunidades de vencer a su oponente. Esa cuestión es desarrollada excepcionalmente por Ivan Arreguín-Toft (2001) en *How the Weak Win Wars*.

En síntesis, la simetría y la convencionalidad son dos categorías independientes. Se observa una dificultad conceptual derivada de la delimitación y los atributos asignados a cada una, cuyo epicentro está vinculado a la interacción real de los actores con las instituciones existentes. Es decir, el acto deliberado y estratégico de no cumplir las convenciones es, para muchos actores, una opción estratégica con costos y beneficios.

La tecnología, la industria y la guerra

La evolución de los armamentos y su incidencia en los conflictos bélicos (en particular, su impacto sobre la estrategia y la táctica) ha sido abordada en el marco de numerosos estudios (Fernandes 2010; Cayuela Fernandez 2000; Van Creveld 1991; Lind et al. 1989). En los últimos años, dicha literatura ha ocupado un lugar cada vez más dominante, sobre todo desde 1970, cuando comenzó a desarrollarse en los países industrializados, fundamentalmente en los Estados Unidos, una propensión a la fabricación de sistemas de armas. A ese proceso lo acompañaron los intereses corporativos del llamado complejo militar-industrial (Dagnino 2010).

Como sustento intelectual para dar justificación académica, surgió en la literatura el concepto de Revolución de los Asuntos Militares (RAM), que coloca a la tecnología militar como la variable determinante para la predominancia nacional en el sistema internacional (Bitzinger 2009). Eso ha puesto el énfasis en una lógica que impone la necesidad de contar con los sistemas “último modelo” y, si ello no es posible, la derrota posiblemente esté asegurada (Scheetz 2011). En esa línea, Sempere (2006, 32) dice que

hoy en día, la presión tecnológica es tan elevada que en ciertas naciones se desarrollan, sin pausa, nuevas armas y sistemas para incorporar los últimos avances” en contraposición a la tentación de usar equipo de segunda calidad, que puede ser bueno en tiempo de paz pero no en la guerra.

La infraestructura científica, tecnológica y productiva, habitualmente identificada como base industrial y tecnológica –no solo de defensa– es aquella que permite explicar la ca-

pacidad de autonomía, desarrollo y poder instrumental de las fuerzas militares y/o de seguridad (Ocón y da Ponte 2016). Este es uno de los principales ejes de asimetría convencional, es decir, *ceteris paribus*: en un escenario con dos fuerzas que se enfrentan militarmente, ganaría la más “poderosa”.

Los sucesos transcurridos a partir del año 2001, en particular los atentados a las torres gemelas, pusieron de manifiesto la debilidad de dicho pensamiento paradigmático. La fuerza más poderosa del planeta, en aquel entonces Estados Unidos, fue atacada en su propio territorio por una fuerza no estatal con dispositivos técnicos no militares –aviones comerciales–. Esa circunstancia revela lo que Max Boot (2006) ha denominado “paradoja de la tecnología militar”.

A partir de entonces han proliferado los estudios acerca de las nuevas amenazas, sobre todo el uso de tácticas y tecnologías no militares para fines militares o violentos, y especialmente la noción de guerras y/o amenazas híbridas (Harris 2016; Tranchemontagne 2016; Bonavena 2006; Schaper 2002). A ello se suma una nueva dimensión: el ciberespacio ha dado lugar a nuevos debates, dinámicas y fenómenos. El crecimiento de producción académica orientada a él ha sido notable en la última década. Trabajos como los de Libicki (2009; 2012; 2016), Rid (2013) y Nye (2010; 2011) han marcado tendencia en los debates en torno al ciberpoder y al ciberespacio.

Ahora bien, parece poco convincente comprender las asimetrías contemporáneas en cuanto al poder duro de las naciones, en función de la comparación exclusiva de su instrumento militar. El activo diferencial es el constante desarrollo de nuevas capacidades. La RAM no es otra cosa que esa capacidad: la carrera constante por mantenerse en la vanguardia de la tecnología de aplicación para

la guerra. Esta solo es posible a partir de una estructura científica-tecnológica-productiva capaz de sostener los procesos inherentes.

Es decir, más allá de las capacidades tácticas y la creatividad de los comandantes en el campo de batalla, el choque de voluntades en la guerra pone de manifiesto una estructura anterior al momento del conflicto: las capacidades adquiridas hasta entonces. Todo instrumento, técnica y aprendizaje depende en gran medida de un proceso de mediano y largo plazo, que demuestra su nivel de efectividad en el teatro de operaciones. La asimetría, desde el punto de vista convencional, revela una racionalidad contundente: ante el choque de voluntades, quien posee mayor poder de fuego y la infraestructura tecnológica-industrial más desarrollada posee más poder y, por ende, es más proclive a imponer su voluntad.

De allí surge la asimetría no convencional. Si la voluntad de pelea se mantiene a pesar de la asimetría científica-tecnológica-productiva, la opción estratégica de los débiles es recurrir a tácticas e instrumentos no convencionales (Arreguín-Toft 2001), o que atentan contra los mandatos institucionales existentes: objetivos civiles con repercusión mediática, bombas caseras (artefactos explosivos improvisados), bombas sucias, robo de material químico o bacteriológico, etc. La falta de infraestructura genera visiones estratégicas alternativas: la toma de instalaciones capaces de producir armas nucleares, radiológicas, químicas o biológicas (NRQB) o incluso el robo de insumos que permitan la adquisición de dicho material (Guillemin 2005; Holle 2000; Purver 1996)

Eso está lejos de implicar que los más poderosos no recurran a mecanismos no convencionales. La simetría puede generar como opción estratégica recurrir a la no convencionalidad, sobre todo cuando las convenciones

vigentes fomentan el *statu quo* y uno de los actores busca romper dicho equilibrio.

En perspectiva histórica, existe un aspecto sobresaliente de la no convencionalidad que cabe destacar: el momento en que una innovación aún no posee regulación. Este es el caso de la bomba atómica en 1945, el uso de drones en los primeros años del siglo XXI e incluso el debate sobre el ciberespacio como dominio militar en la actualidad. Todos son ejemplos de ausencia de convencionalidad, como resultado de la innovación.

En la edad contemporánea, industrial y postindustrial, la estructura científica, tecnológica y productiva permite explicar simetrías y asimetrías entre actores en conflicto. Sin embargo, no necesariamente explica el comportamiento de ellos. El desarrollo tecnológico y militar no es una variable explicativa del resultado final de un conflicto o una guerra, tal como lo demuestra Arreguín-Toft (2001). En cambio, lo que sí permite explicar la estructura científica-tecnológica y la base industrial de los actores es cuál es su capacidad inicial, en un escenario con determinadas convenciones. De ahí que la existencia de múltiples tratados en contra del empleo de armas de destrucción masiva se constituyera en mera formalidad, en virtud de su utilización por Estados con capacidad de fabricarlos. La utilización de bombas racimo y fósforo blanco en el Medio Oriente ilustra el punto. La ruptura de las convenciones es una opción estratégica que todos los actores suelen preservar.

Sudhir (2008) afirma que David tuvo que apelar a la ingeniosidad y a sus propias habilidades para hacer frente a Goliat, no en los términos de Goliat, sino en los propios. Las alternativas del actor “asimétrico” para equilibrar la balanza son: la adquisición de alta tecnología militar (armas de destrucción masiva, etc.) o el uso de baja tecnología (dispositivos improvisados, etc.).

La relación entre tecnología y convencionalidad: aceptación, innovación y/o transgresión

Resulta evidente la relación entre convencionalidad y tecnología, pues en los supuestos antes referidos existen tres opciones factibles: (a) la aceptación de la convenciones, con la utilización de medios existentes, (b) el desarrollo de nuevas tecnologías, que permita superar la convencionalidad, a partir de la adquisición de dispositivos y/o sistemas que carecen de regulación institucional y/o (c) el uso de tecnologías no convencionales, con lo cual se transgrede el sistema normativo vigente.

En la actualidad, el concepto de armas no convencionales se puede referir a dos tipos: armas de destrucción masiva, encuadradas en las siglas NQBR o armas “improvisadas”, que son objetos que no fueron concebidos originalmente para ser utilizados como armas, pero se utilizan o se diseñan mecanismos para hacerlo. Por ejemplo, el uso de “armas” químicas, o en específico, de instrumentos, objetos y hasta personas por sus características o circunstancias “químicas”, para fines violentos, es un tema que data desde la antigüedad, siempre cargado de controversia. El uso de personas enfermas, cadáveres y hasta proyectiles envenenados ha sido una táctica documentada por los hititas. Constituye uno de los primeros registros escritos de Guerra Química (Trevisanato 2007). Ya cerca del mundo moderno, Leonardo da Vinci habría propuesto la utilización de polvo de sulfuro de arsénico como arma química (Gupta 2009).

En 1672, el obispo de Münster, Christoph Bernhard von Galen, utilizó *Atropa belladonna* durante un asedio en Groningen. No resulta extraño que tres años después se haya firmado en Strasburgo el primer tratado moderno que

prohíbe el uso de armas químicas. Dicho documento es un antecesor en muchos aspectos de las Convenciones de la Haya (1899-1907), respecto al uso de armas químicas. Convenciones que fueron violadas tanto por Francia como Alemania en la Primera Guerra Mundial (PGM).

Frente a los sucesos de la PGM, surgió la iniciativa de establecer mayores regulaciones. En lo referido al control de armas, se estableció en 1925 el Protocolo de Ginebra, también denominado “Protocolo sobre la prohibición del empleo en la guerra de gases asfixiantes, tóxicos o similares y de medios bacteriológicos”.

Faltaban 13 años para que la fisión nuclear de los átomos fuese descubierta por Otto Hahn y Fritz Strassmann, a partir del trabajo desarrollado por el propio Hahn junto a Lise Meitner durante años anteriores. Era inimaginable la bomba atómica y, por lo tanto, no se podía regular aquello aún inexistente. Solo después de la Segunda Guerra Mundial (SGM) se originó una dinámica inédita. Dicho de otro modo, fue luego de su empleo que se prohibió tanto su uso como su fabricación, para la inmensa mayoría de los países, a excepción de las potencias. El Tratado de No Proliferación tuvo sus primeros firmantes en 1968, mucho tiempo después de la bomba de Hiroshima y Nagasaki.

El uso de armas improvisadas y la aplicación de *modus operandi* del tipo “irregular” es el resultado claro de dos procesos interrelacionados: la firma intensiva de tratados internacionales dedicados al control de armas y la consolidación de las “industrias de defensa” en el mercado internacional (Anderson 1992). Proceso que aún persiste y continúa ampliándose, tal como se advierte con el tratado de comercio de armas que entró en vigor en el año 2014.

El establecimiento normativo y convencional de líneas divisorias entre lo que es “militar” y lo que es “civil” (aplicaciones, fabricación y usos permitidos y prohibidos de determinado instrumentos) es lo que paulatinamente ha generado una línea imaginaria institucional de “cómo debe practicarse la guerra”. Sobre todo, cuál instrumento es convencional y cuál no.

Los armas no convencionales del tipo “improvisadas” son elementos juzgados *a priori* por su fin al momento de la fabricación o venta, y no por su utilización como instrumento para el ejercicio de la violencia. Bombas de tubo, bombas molotov, cuchillos improvisados (*shiv*), etc... son algunos ejemplos de armas “caseras” o fabricadas con objetos adquiribles en cualquier supermercado.

Al componente del “arma no convencional improvisada” se le suma por lo general el “quién” fabrica o utiliza dicho armamento. Se presume que un soldado regular no necesita fabricar bombas de tubo, ya que dispone de dispositivos o sistemas convencionales como granadas u otros tipos de explosivos, que cuentan con adecuadas medidas de seguridad y para los cuales está adiestrado.

La no convencionalidad de armas caseras proviene de la regulación del derecho internacional que separa lo militar de lo civil, y dota a determinado tipo de individuo (no a otros) del derecho y la capacidad de portar y utilizar determinados tipos de armas. Esto, siempre y cuando la utilización de las armas convencionales se haga de acuerdo con lo establecido también por ley.

Ahora bien, cuando el escenario exhibe (*a priori*) las características de asimetría, en función de una diferencia notable en las capacidades instrumentales, militares y de infraestructura de un actor por sobre otro, pero no debido a la existencia de fuerzas irregulares, las condiciones están dadas para la preeminencia

del más fuerte por sobre el más débil, asumiendo que se cumplen las reglas convencionales.

Como demuestra Ivan Arreguín-Toft (2001), la asimetría es una opción estratégica de los débiles. La diferencia que generalmente revela la asimetría *a priori* no es solo la vanguardia tecnológica del instrumento, sino la infraestructura de Ciencia, Tecnología y Producción (CTP) de un adversario con respecto al otro. El “grande”, el “poderoso” es quien posee una infraestructura mayor, que además se apoya en una serie de convencionalidades, cuya interrelación con el poder ha sido demostrada por una amplia literatura.

Retomando los argumentos de Brooks (2016), existe una notable relación entre el poder de determinadas naciones y su capacidad de establecer ciertas convenciones a su favor, dotando de capacidad estratégica a los que posean mayor infraestructura, debido a su capacidad de sobresalir de las convenciones. En nuestros días, los drones y la actividad en el ciberespacio carecen de regulación adecuada y son tecnologías o espacios tecnológicos que requieren infraestructura.

Se pueden observar dos formas de estar fuera de las convenciones: el camino de la innovación y/o el camino de la transgresión. El primero consiste en superar las barreras con prácticas o instrumentos novedosos, que no estén sujetos a regulación, debido a un descubrimiento o a la creatividad de estrategias y decisores. Es decir, existe un paradigma donde se articulan las ideas y las nociones para identificar, categorizar y hasta comprender las guerras actuales. Es fundamental comprender que, si bien la convencionalidad en los conflictos ha sido siempre una constante, los comportamientos regulados y particularmente la tecnología disponible dependen de la coyuntura histórica.

Hoffman (2018) propone una construcción heurística del conflicto, basada principalmente en los aportes de un conjunto de autores que retoman la propuesta inicial de Kennan (Harlow y Maez 1990; Barno y Bensahel 2015) con respecto a las llamadas “zonas grises del conflicto”. De acuerdo con la noción inaugurada por Kennan en una serie de seminarios en el Colegio Nacional de Guerra, a fines de la década de 1940, existe “guerra” (warfare) del tipo político. Esa figura conceptual, hoy traducida como “conflictos de zona gris”, alude a aquellas formas en la cual la manifestación de la guerra es elusiva en términos convencionales. Es claro que no existe una clara definición de la no convencionalidad, pero sí existen acuerdos en cuanto a tácticas y estrategias de determinados actores para mantenerse en los límites (y por fuera) de lo convencional, con el fin de tener mayor ventaja.

Es importante considerar que, durante un mismo conflicto, la convencionalidad no suele variar, ya que son reglas de juego establecidas *a priori*, pero en lo que sí es necesario centrar la atención es en cómo los actores involucrados pueden y/u optan por salirse de la convencionalidad en un momento dado. Puede ocurrir desde el principio del conflicto o durante este.

En definitiva, existe un paradigma de la convencionalidad contemporánea, construido históricamente con base en la estatalidad y en una serie de hechos y procesos que han ido siempre detrás de las innovaciones tecnológicas, intentando establecer patrones, normas y prácticas aceptables a partir de una serie de preceptos éticos, morales e instrumentales, que son sujetos de varianza histórica.

Cómo los actores abordan el conflicto depende en gran medida de la infraestructura tecnológica, del instrumento disponible y

de la voluntad de transgredir convenciones establecidas, asumiendo los riesgos correspondientes. Lo interesante de los comportamientos de actores como Rusia en su conflicto con Ucrania, desde el año 2014, tiene que ver con la forma en que un actor con más poder militar encontró los mecanismos tecnológicos para vulnerar convenciones en espacios de vacío legal, utilizando tácticas híbridas y combinando transgresión con innovación.

Reflexiones finales

El estudio de la guerra, desde la perspectiva de las metanarrativas enraizadas en las estructuras institucionales, registra definiciones cuya amplitud apela a una generalidad que atraviesa las realidades históricas. Este punto de partida resulta fundamental para toda observación y análisis que, junto a otras características, sea capaz de distinguir las condiciones estructurales de aquellas contingentes respecto a un fenómeno complejo por su propia naturaleza. Salonio (2019) señala que los vocablos “complejo” y “complicado” suelen tratarse como sinónimos, pero, advierte, no lo son: para referir a algo difícil o de difícil comprensión, es apropiado diferenciarlos conceptualmente. En ese sentido, precisa que lo complicado admite la individualización de causas “con subsistemas controlables”, lo cual favorece una eventual solución permanente. Por el contrario,

un sistema complejo resulta de una red de múltiples causas interactuantes que no pueden ser distinguibles en su totalidad, que requieren ser tratadas como un sistema porque pequeñas alteraciones pueden resultar en resultados desproporcionados y los problemas que presentan no pueden ser resueltos de manera definitiva (Salonio 2019, 2).

Planteado en otros términos, no se pretende soslayar el rol de las instituciones, sino incorporarlo como variable explicativa, a fin de comprender lo que cambia y lo que no.

El acto de regulación del conflicto, inherentemente político, se encuentra con su contraparte bélica ya que, en términos *clauswitzianos*, la guerra es la continuación de la política por otros medios. De esa manera, la voluntad de lucha y de oposición, pero por sobre todas las cosas, la anteposición del interés del actor por mejorar su situación en un arreglo institucional que puede ir en detrimento de sus posibilidades, plantea la obediencia/transgresión a las convenciones como una opción estratégica, observable no solo de forma contemporánea, sino a través de la historia.

Parece adecuado sostener que uno de los indicadores más precisos de la posición y capacidad de los actores al momento del choque de voluntades se constituye en gran medida en función de su habilidad de canalizar al esfuerzo bélico los activos de su base científico-tecnológica y su estructura productiva. En efecto, el desarrollo de capacidades de infraestructura depende de un proceso que abarca diversas dimensiones: educación, iniciativas de política científica, tecnológica e industrial. Pese a que los efectos suelen cristalizar a mediano plazo, el momento de la guerra pone de manifiesto los atributos de las estructuras existentes a corto plazo. Es por eso que los actores “poderosos” son aquellos que pueden utilizar un mayor abanico de opciones, entre ellas la innovación. Por el contrario, los actores “débiles”, en relación asimétrica, suelen recurrir a mecanismos no convencionales.

Las denominadas nuevas guerras ¿son realmente nuevas? Pese al interrogante, no puede dejar de reconocerse que la tecnología y las convenciones han ido ampliándose y que eso

delimita e influye en el comportamiento de los actores respecto a las formas de practicar la guerra, es decir, el *warfare* o *kriegsführung*. No obstante, resulta necesaria una reflexión sistémica, que permita brindar argumentos consistentes para establecer qué es lo nuevo.

Ahora bien, la guerra como acto político por medios violentos implica tomar decisiones estratégicas con respecto a la aceptación o no de las convenciones frente al escenario de conflicto, el respeto a estas, la innovación en la tecnología militar y las maniobras que apelan al engaño, la acción psicosocial o la utilización de actos aberrantes como fin político-militar. Pertinente es apuntar que esas decisiones no son, de ninguna forma, novedosas, sino que es factible encontrar numerosos ejemplos históricos.

Tal y como se analizó en el presente artículo, existen al menos dos formas de evadirse de la convencionalidad. La primera es por medio de la innovación. La segunda, a través de la transgresión. Para el camino de la innovación, es necesaria una base científico-tecnológica e industrial, que generalmente poseen los países más desarrollados. Sin embargo, la transgresión no deja de ser una opción para este grupo de países.

En definitiva, la llamada guerra híbrida, que implica la combinación de formas de hacer la guerra por medio de maniobras e instrumentos convencionales y no convencionales, refiere a estratégicas y tácticas en las cuales un actor está dispuesto a empeñarse, pese a los costos de sus transgresiones. El desafío al marco institucional contemporáneo es, en todo caso, una puja de poder que se encuentra inserta en la dinámica de la guerra, y subsumida a los intereses de los actores de imponer su voluntad.

Bibliografía

- Abluso, Federico, Matías Alcántara, y Julián Tutasaus. 2014. "Definiendo la guerra". *Cuadernos De Martes Revista Latinoamericana de Sociología De La Guerra* (5) 7: 161-193.
- Alfaro, Daniel Adán. 1990. "Acercamiento a la metodología de Max Weber". *Revista de Sociología* (5): 129-146.
- Anderson, David G. 1992. "The International Arms Trade: Regulating Conventional Arms Transfers in the Aftermath of the Gulf War". *American University International Law Review* 4 (7): 749-805.
- Arreguín-Toft, Ivan. 2001. "How the Weak Win Wars: A Theory of Asymmetric Conflict". *International Security* (26) 1: 93-128.
- Aznar Fernandez-Montesinos, Federico. 2015a "Las generaciones de guerras. Guerras de primera generación (I)". *DIEEEA* (54): 1-14.
- Aznar Fernandez-Montesinos, Federico. 2015b. "Las generaciones de guerras. Guerras de segunda y tercera generación (II)". *DIEEEA* (59): 1-22.
- Almäng, Jan. 2019. "War, vagueness and hybrid war". *Defence Studies* 2 (19): 189-204. doi.org/10.1080/14702436.2019.1597631
- Bartolomé, Mariano. 2017. "El empleo actual del concepto guerra en las relaciones internacionales". *Revista de Relaciones Internacionales, Estrategia y Seguridad* 2 (12): 43-66.
- Barno, David, y Nora Bensahel. 2015. "Fighting and Winning in the 'Gray Zone'. War on the rocks", <https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/>

- Bitzinger, Richard. 2009. *The Modern Defense Industry: Political, Economic, and Technological Issues*. Estados Unidos: Praeger Security International Imprint Of ABC-CLIO.
- Bobbio, Norberto. 2008. *El problema de la guerra y las vías de la paz*. Madrid: Gedisa.
- Bonavena, Pablo. 2006. "Reflexiones sobre la doctrina de la Guerra asimétrica". *En Aportes para una Sociología de la Guerra*, editado por Flabián Nievas, 31-56, Buenos Aires: Proyecto Editorial.
- Boot, Max. 2006. "The Paradox of Military Technology". *The New Atlantis* (14): 13-31.
- Brooks, Rosa. 2016. *How Everything Became War And The Military Became Everything. Tales from the Pentagon*. Nueva York: Simon & Schuster.
- Cayuela Fernández, José Gregorio. 2000. "Guerra, industria y tecnología en la edad contemporánea". *Estudios históricos* (18): 179-199.
- Dagnino, Renato. 2010. *A indústria de defesa no governo Lula*. São Paulo: Expressão Popular.
- D'Anieri, Paul, y Taras Kuzio. 2018. *The Sources of Russia's Great Power Politics: Ukraine and the Challenge to the European Order*. Bristol: E-International Relations Publishing.
- Eliason, Sven. 2000. "Max Weber's methodology: An ideal type". *The History of Behavioral Science* (36) 3: 241-263. doi.org/10.1002/15206696(200022)36:3<241::AID-JHBS3>3.0.CO;2-C
- Fernandes, Luiz. 2010. "Ciencia, tecnología y soberanía nacional". *Cuadernos de Actualidad en Defensa y Estrategia* 5.
- Foch, Ferdinand. 1920. *The Principles of War*. Nueva York: H. Holt and Company.
- Foucault, Michel. 1968. *Las palabras y las cosas: una arqueología de las ciencias humanas*. Argentina: Siglo XXI editores.
- Foucault, Michel. 2010. *Nacimiento de la biopolítica: curso en el Collège de France (1978-1979)*. México: Fondo de Cultura Económica.
- Guillemin Jeanne. 2005. *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism*. Nueva York: Columbia University Press.
- Gupta, Ramesh. 2009. *Handbook of Toxicology of Chemical Warfare Agents*. India: Academic Press.
- Harlow, Giles D. y George C. Maez. 1990. *Measures Short of War: The George F. Kennan Lectures at the National War College, 1946-47*. Washington, DC: NDU Press.
- Harris, Elisa. 2016. *Governance of dual-use Technologies. Theory and Practice*. Cambridge: American Academy of Science and Arts.
- Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.
- Hoffman, Frank G. 2009. *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*. Washington, DC: Institute for National Strategic Studies.
- Hoffman, Frank G. 2018. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges". *Prism* 4 (7): 30-47.
- Holle, Juan Atilio. 2000. *La protección contra los agentes químico de guerras: elementos básicos*. Buenos Aires: Impresión Gráfica.
- Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.
- Libicki, Martin C. 2012. *Crisis and Escalation in Cyberspace*. Santa Monica: RAND Corporation.
- Libicki, Martin C. 2016. *Cyberspace in Peace and War*. Maryland: Naval Institute Press.
- Lind, William S, Keith Nightengale, John F Schmitt, Joseph W Sutton, y Gary I. Wil-

- son. 1989. "The Changing Face of War: Into the Fourth Generation". *Marine Corps Gazette* 73 (10): 22-26.
- Liang, Qiao, y Wang Xiangsui. 1999. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House.
- Mack, Andrew. 1975. "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict". *World Politics* (27) 2: 175-200. DOI: 10.2307/2009880
- Nye, Joseph S. 2010. *Cyber Power*. Cambridge: Bedfer Center for Science and International Affairs.
- Nye, Joseph S. 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5 (4): 18-38.
- Ocón, Alfredo L., y Aureliano da Ponte. 2016. "La industrialización como problema de defensa. Debates y "saber convencional"". En *Industria y Defensa. Economía política, pensamiento estratégico y autonomía tecnológica*, editado por Alfredo Ocón y Aureliano da Ponte, 27-70. Buenos Aires: 1884 Círculo Militar.
- Purver, Ron. 1996. *Chemical and Biological Terrorism. New threat to public safety?* Reino Unido: RISCT.
- Raffman, Diana. 2014. *Unruly Words: A Study of Vague Language*. Oxford: Oxford University Press.
- Rid, Thomas. 2011. "Cyberwar Will Not Take Place". *Journal of Strategic Studies* (35): 5-32. <https://doi.org/10.1080/01402390.2011.608939>
- Salgado Espinoza, Raúl, y Daniela Barreiro. 2018. "Estudios estratégicos: entre la rigurosidad y la subjetividad. *URVIO. Revista Latinoamericana de Estudios de Seguridad* 22: 8-23. doi.org/10.17141/urvio.22.2018.3324
- Sudhir, M.R. 2008. "Asymmetric War: A Conceptual Understanding". *CLAWS Journal*: 58-66.
- Salonio, Pablo L. 2019. *El entorno operacional futuro: un marco conceptual a partir del fenómeno de la complejidad en el siglo XXI*. Manuscrito no publicado. Escuela Superior de Guerra Conjunta.
- Sartori, Giovanni. 1979. *La política lógica y método en las Ciencias Sociales*. México: Fondo de Cultura Económica.
- Schaper, Annette. 2002. "Nuclear Terrorism: Dirty Weapons". *The World Today* 1 (58): 18-19.
- Scheetz, Thomas. 2011. "Teoría de la gestión económica de las Fuerzas Armadas". EDENA Documento de Trabajo 7.
- Sempere, Carlos Martí. 2006. *Tecnología de la Defensa, análisis de la situación española*. Madrid: IUGM.
- Tranchemontagne, Marc. 2016. "The Enduring IED Problem: Why We Need a Doctrine". *Joint Force Quarterly* 1 (80): 153-160.
- Trevisanato, Siro Igino. 2007. "The 'Hittite Plague', an Epidemic of Tularemia and the First Record of Biological Warfare". *Med Hypotheses* 6 (69): 1371-1374. doi.org/10.1016/j.mehy.2007.03.012
- Tuck, Christopher. 2018. "The Future of Land Operations: The Role and Challenges of Technology". *Revista de Ciencias Militares* 2 (6): 477-492.
- Van Creveld, Martin L. 1991 *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*. Nueva York: The Free Press.
- Von Clausewitz, Karl. 2009. *On war*. Maryland: Wildside Press, United States.

El componente social de la amenaza híbrida y su detección con modelos bayesianos

The Social Component of the Hybrid Threat and its Detection with Bayesian Models

Ana-María Ruiz-Ruano¹, Jorge López-Puga²
y Juan-José Delgado-Morán³

Recibido: 2 de junio de 2019
Aceptado: 31 de julio de 2019
Publicado: 2 de diciembre de 2019

Resumen

Las sociedades contemporáneas están cada vez más condicionadas por el desarrollo de la tecnología informática. Esa tendencia deja entrever un panorama en el que cada ser humano se identifica por el binomio persona-computadora, mientras que la mayor informatización de la vida civil está generando ingentes cantidades de datos que son susceptibles de ser gestionados con fines bélicos. El objetivo de este artículo es abordar la utilidad potencial de las redes bayesianas como herramientas destinadas a la monitorización y detección temprana de ataques híbridos de carácter social a escala global. Como conclusión, planteamos que el uso de la inferencia y las redes bayesianas es útil para monitorear, detectar y supervisar el componente social de las amenazas híbridas a escala global por medio del análisis de las redes sociales.

Palabras clave: inferencia estadística; inteligencia artificial; redes informáticas; redes sociales; seguridad de los datos

Abstract

Contemporary societies are increasingly conditioned by the development of computer technology. This trend suggests a picture in which each human being is identified by the person-computer binomial while greater computerization of civil life is generating huge amounts of data that are likely to be managed for war purposes. The objective of this article is to address the potential utility of Bayesian networks aimed at monitoring and early detection of hybrid attacks of a global nature. We conclude that the use of inference and Bayesian networks is useful for monitoring, detection and supervision of the social component of hybrid threats globally through social network analysis.

Keywords: artificial intelligence; computer networks; data protection; social networks; statistical inference

1 Universidad Católica de Murcia, España, amruiz@ucam.edu,  id/0000-0002-7260-0588

2 Universidad Católica de Murcia, España, jpuga@ucam.edu,  orcid/0000-0003-0693-0092

3 Universidad Católica de Murcia; miembro de la Cátedra Nebrija-Santander en Gestión de Riesgos y Conflictos y miembro del Grupo Nebrija de Relaciones Internacionales, Cooperación e Integración en Áreas Regionales (RICINTAR) de la Universidad Antonio de Nebrija, España, jjdelgado@ucam.edu,  orcid/0000-0002-9945-8235



Introducción

Es un hecho constatado que el mundo contemporáneo está ampliamente interconectado. El desarrollo que han experimentado las telecomunicaciones a lo largo del último siglo ha facilitado que sea cuestión de segundos ponerse en contacto con una persona que se encuentra en las antípodas. Podemos transferir texto, imágenes, sonido y video como nunca fue posible. La tecnología 5G plantea muchas más posibilidades para el presente, así como para el futuro.

Todo ese desarrollo científico-técnico ha tenido consecuencias positivas para la economía y para el desarrollo humano en general. Sin embargo, la sofisticación de las redes informáticas, así como las potencialidades que nos ofrecen coexistiría con la posibilidad de ser atacadas por agentes que pretenden desestabilizarlas. Este asunto ha sido, y sigue siendo, objeto de profundo análisis por parte de las ciencias de la computación. Sin embargo, la estabilidad y seguridad digital se enfrenta a nuevos retos.

Entre los desafíos actuales de la humanidad podríamos destacar aquellos relacionados con las amenazas **híbridas**. Este artículo tiene como objetivo principal aproximarnos a la caracterización conceptual de lo que podríamos llamar componente social de la amenaza híbrida. Se trata de un componente mediado principalmente por el aspecto social que caracteriza a la organización humana. Por tanto, se presenta una conceptualización y se analiza **cómo puede ser** monitoreado usando la inferencia bayesiana.

La primera parte del artículo aborda la conceptualización del componente social de la amenaza híbrida utilizando una metodología basada en la revisión bibliográfica. En la

segunda parte, y como objetivo secundario, presentamos una introducción a lo que denominamos inferencia bayesiana comparándola, básicamente, con la inferencia estadística clásica. La tercera parte refleja, a través de un ejemplo ilustrativo y limitado en el número de variables, el uso potencial de una red bayesiana para modelar un caso concreto de amenaza híbrida. Nos proponemos mostrar la lógica que subyace a este tipo de herramientas estadísticas en el contexto de la seguridad frente a amenazas híbridas. Por último, presentamos nuestras conclusiones y los derroteros que debería tomar el trabajo de prevención o detección del componente social de las amenazas híbridas.

El componente social de la amenaza híbrida

No existe una definición amplia y universalmente aceptada de amenaza híbrida (Ducaru 2016). Siguiendo a Colom (2019), podemos indicar que el término “guerra híbrida” fue utilizado por primera vez en un documento oficial producido por Estados Unidos por el año 2005. En cualquier caso, existe un conjunto de elementos hostiles que pueden asociarse con los ataques híbridos. Por ejemplo, las estrategias militares o no militares que están destinadas a desestabilizar organizaciones sociales legítimamente estructuradas de manera deliberada y sincronizada pueden considerarse ataques híbridos. Los ataques o intentos de desestabilización tienen como objetivo obtener influencia política, social o económica sobre la organización social que está siendo atacada (p. e., Ducaru 2016; Hoffman 2009; Lanoszka 2016). Este tipo de ataques híbridos, que inicialmente pueden no tener un

marcado o claro componente militar, siempre han existido y la historia está plagada de ellos. El “caballo de Troya” y la Guerra Fría son claros ejemplos (uno clásico y otro sostenido en el tiempo) de ataques híbridos.

El interés particular de este artículo es un aspecto concreto de los ataques híbridos contemporáneos: el componente social-virtual. Lo que denominamos componente social del ataque híbrido contemporáneo está asociado con una idea de seguridad informática que no se circunscribe a la integridad de la información electrónica (von Solms y van Niekerk 2013). Más bien está relacionado con la veracidad de la información difundida en la red de redes con el ánimo de auspiciar, incrementar o desarrollar ataques híbridos.

Como es bien sabido, gran parte del mundo está conectado por medio de dispositivos informáticos. Cada vez es más frecuente que las personas dispongan de un móvil inteligente que es, en definitiva, una computadora. De hecho, esas “minicomputadoras personales” son claramente más potentes de lo que lo fueron sus ancestros tecnológicos hace solo dos o tres décadas. Una gran proporción de la población que reside en lo que vulgarmente se denomina “mundo desarrollado” dispone de uno o más dispositivos móviles o portátiles que superan con creces la capacidad de cómputo de la que se disponía domésticamente hace tan solo unas décadas. Según predice la Ley de Moore, la tendencia será la misma en el futuro, máquinas cada vez más baratas y más potentes.

Las computadoras actuales no son solo más potentes y tienen mayor capacidad de almacenar información, sino que cada vez están más interconectadas. Conceptos como “el internet de las cosas” o el “coche autónomo” serán pronto una realidad, según los medios de comunicación de masas y las revistas cien-

tíficas especializadas. Esa conexión globalizada o conectividad globalizadora está ideada, al menos en teoría, para mejorar las vidas de las personas, pero también surgen ciertos problemas éticos que la humanidad tendrá que afrontar. Por ejemplo, ¿quién será responsable de un accidente que se produzca vinculado a la actividad de un coche autónomo?

En ese caldo de cultivo y desarrollo tecnológico, la cantidad de información que se va a producir parece abrumadora. Si las estimaciones son correctas, en pocos años la información electrónica que existirá, en términos de bytes, superará al número de estrellas que existen en el universo conocido (Butler 2016). Por ello, han sido acuñados conceptos como el de “Big Data”, cuyo desarrollo es espectacular desde el punto de vista académico o científico, para poder acomodarnos a la realidad computacional que se nos avecina (Cloud Security Alliance 2012).

Todo ello plantea ciertos desafíos a las sociedades democráticas legítimamente constituidas en aras de preservar el orden social y político, en relación con posibles ataques híbridos de naturaleza informática (Lafuente 2015). Como indican algunos autores, este tipo de delitos u otros de carácter informático tenderán a ser cada vez más frecuentes, más sofisticados y más destructivos (Taddeo y Floridi 2018). En tal contexto se ubica lo que hemos denominado “componente social del ataque híbrido”. Un componente que podría vincularse a lo que Reboloso (1994) denomina clásicamente comportamiento colectivo o conducta de masas.

Es bien sabido que el comportamiento colectivo o de masas favorece la consecución de objetivos sociales deseables y positivos. Sin embargo, las masas o ciertos movimientos colectivos pueden llevar a cabo comporta-

mientos destructivos y lesivos para la propia sociedad o estructura social (Lilienfeld, Lynn, Namy y Woolf 2011). Independientemente de si los fines perseguidos son legítimos o buscan la defensa de valores positivos, la organización social tumultuosa y los amotinamientos suelen provocar consecuencias deletéreas para la propia sociedad. En el ámbito de los ataques híbridos, este tipo de comportamientos colectivos se dan cada vez más en la red, a través de, por ejemplo, sistemas de mensajería instantánea. Merecería la pena preguntarse si en esas situaciones se pone en peligro o en riesgo la seguridad ciudadana o la seguridad de la estructura social establecida.

En el ámbito de las ciencias de la computación se han desarrollado herramientas que pueden ser potencialmente utilizadas para predecir el componente social de los ataques híbridos. Por ejemplo, los modelos estocásticos altamente estructurados, como los sistemas expertos probabilísticos (Cowell et al. 1999, 37). Este tipo de modelos han surgido en el seno de la inteligencia artificial (IA) y se están postulando como herramientas eficientes para gestionar iniciativas destinadas a vulnerar la seguridad de los Estados, naciones, democracias o estructuras sociales legítimamente establecidas (Anwar y Hassan 2017; Ruiz-Ruano y Puga 2018).

Los métodos bayesianos pueden considerarse herramientas apropiadas para tomar decisiones en situaciones de incertidumbre, teniendo en cuenta el conocimiento borroso que tenemos de las variables implicadas en el problema de decisión (Edwards y Fasolo 2001). Por ello, planteamos que este tipo de herramientas estadísticas podrían ser ideales para desarrollar sistemas de monitorización del componente social en las amenazas híbridas. De hecho, la utilización de técnicas

matemático-estadísticas no es nueva y algunas organizaciones gubernamentales como la CIA (Central Intelligence Agency) de los Estados Unidos de América se han apoyado en ellas para gestionar conflictos bélicos o relacionados con la seguridad (CIA 1968; Das 1999; Fisk 1994; Somiedo 2018). En cualquier caso, pese a que en este artículo defendemos que el uso de herramientas computacionales es esencial para detectar el componente social de la amenaza híbrida, tenemos que tener en cuenta sus limitaciones (Castelvecchi 2019).

En el epígrafe siguiente presentamos una escueta descripción de algunos de los elementos de los métodos bayesianos que creemos útiles para detectar el componente social de la amenaza híbrida. Presentamos nuestras conclusiones respecto a la utilidad y viabilidad de este tipo de herramientas para detectar y monitorizar amenazas de seguridad a gran escala.

Inferencia bayesiana

Los métodos de inferencia bayesiana son usualmente contrastados o confrontados con la inferencia clásica o frecuentista (Alonso y Tubau 2002; Cowell et al. 1999; O'Hagan y Luce 2003; Serrano 2003). Se considera que la estadística bayesiana tiene su origen en un trabajo atribuido al reverendo Thomas Bayes (1763), publicado a título póstumo. En esta sección presentaremos algunas de las características más sobresalientes de la estadística bayesiana, siguiendo algunos puntos de O'Hagan y Luce (2003).

En primer lugar, los métodos bayesianos o incluso los híbridos-bayesianos asumen que existe un componente subjetivo relevante en los problemas que han de ser resueltos. Desde esas ópticas se asume como normal la subjeti-

vidad y se trata de modelarla estadísticamente. Dicho de otro modo, se considera que existen incertidumbres en los planteamientos de los problemas que han de resolverse y ello es modelado estadísticamente por medio de, por ejemplo, distribuciones de probabilidad. Hacer esto supone una perspectiva humilde frente a la resolución de cualquier problema, dado que se está asumiendo que existe conocimiento incompleto sobre el aspecto de la naturaleza que se está estudiando. El conocimiento incierto sobre la realidad de un problema es, entonces, modelado o incluido en este, utilizando el conocimiento subjetivo que se tiene. Por ello, los métodos bayesianos se caracterizan por ser técnicas que asumen cierta subjetividad en la resolución de los problemas. Es más, se suele decir que asumen que la probabilidad en sí misma es un elemento más subjetivo que objetivo. Así, en vez de considerar que la probabilidad de ocurrencia de un fenómeno es algo real que existe como tal, se considera que las estimaciones de probabilidad son producto de la naturaleza cognitiva humana. Es decir, que las estimaciones de probabilidad son, en cualquier caso, subjetivas.

Como señala Dixon (1970), la probabilidad de ocurrencia de un fenómeno no sería una propiedad que pertenece al sistema o al evento observado, sino que, más bien, sería una propiedad o una característica que depende del observador del sistema. Creemos conveniente hacer aquí una sublime apreciación que ya sugería Jeffreys (1931), quien ha sido considerado uno de los máximos exponentes de la inferencia bayesiana. El hecho de que las estimaciones de probabilidad puedan ser consideradas algo subjetivo no implicaría necesariamente que la mente humana sea la que crea la realidad (Berger y Luckmann 1968). Más bien, se diría desde un enfoque bayesia-

no, que se acepta la idea de que habría ciertas estimaciones de probabilidad que encajan mejor o peor con los datos experimentales. Por tanto, la misión de las personas que resuelven problemas de probabilidad consiste en ir acomodando creencias y experiencias con base en los datos empíricos u observados.

Podríamos decir que los métodos bayesianos combinan información previa (denominada en el contexto estadístico “distribuciones *a priori*”) con información observada (también denominada datos o distribución de verosimilitud), para producir distribuciones posteriores o actualizadas (también denominadas “distribuciones *a posteriori*”) del problema estudiado. Sobre las distribuciones posteriores se suelen llevar a cabo procesos de inferencia estudiando, por ejemplo, datos estadísticos de tendencia central (media, mediana o moda, por ejemplo) o identificando intervalos de credibilidad bayesianos.

Los métodos bayesianos son técnicas que se asemejan mucho al razonamiento natural humano (Anscombe 1961; Bolstad 2007; Puga, Krzywinski y Altman 2015). Por ejemplo, en el ámbito de estudio de la psicología y la neurociencia, estudios de principios de este siglo sugieren que el razonamiento humano, principalmente el causal, se asemeja mucho a lo que cabría esperar si se estuviese utilizando inferencia bayesiana (véanse, por ejemplo, los trabajos de Glymour 2001, 2003; Gopnik et al. 2004, 2001, experimento 3; Gopnik y Schulz 2004; Sobel, Tenenbaum y Gopnik 2004, experimento 3). Dicho de otro modo: cuando observamos el aprendizaje humano y tratamos de modelarlo formalmente, se hacen predicciones que son muy congruentes con lo que postula la estadística bayesiana.

Mientras que la estadística frecuentista se centra, desde un punto de vista probabilísti-

co, en estimar la probabilidad de que unos datos muestrales (D) provengan de cierta distribución hipotética (H), es decir, $P(D|H)$, la estadística bayesiana está más interesada en conocer la credibilidad o verosimilitud de las hipótesis planteadas en función de los datos empíricos observados, $P(H|D)$. De ese modo, usando el teorema de Bayes y considerando que los parámetros poblacionales son entes que se distribuyen aleatoriamente (no como la estadística frecuentista o clásica, que considera a estos como entes fijos), los métodos bayesianos permiten actualizar los modelos probabilísticos a medida que se van recogiendo u observando datos muestrales frente a la resolución de problemas.

El Factor de Bayes o FB está recibiendo un considerable interés en los últimos tiempos en un amplio abanico de disciplinas científicas tanto teóricas como aplicadas (Held y Ott 2018; Hoijtink, van Kooten y Hulsker 2016; Jarosz y Wiley 2014; Jeon y De Boeck 2017; Morey y Rouder 2011; Morey, Wagenmakers y Rouder 2016). Es un estadístico que estima la medida en que una hipótesis es más probable que otra, teniendo en cuenta los datos muestrales o las evidencias disponibles (Kass y Raftery 1995). Matemáticamente, el Factor de Bayes (FB_{AB}) resulta de dividir la probabilidad de que ocurra una hipótesis (pongamos, A) entre la probabilidad de que ocurra otra (digamos, B), teniendo en cuenta cuán probables son a la luz de los resultados observados empíricamente. Dado que este factor es una fracción o proporción, puede ser interpretado de forma comparativa atendiendo a la verosimilitud de una hipótesis respecto a otra, habiéndolas condicionado a los datos observados. Por tanto, cuando el Factor de Bayes es igual a uno, podríamos decir que ambas hipótesis son igualmente probables a la luz de

los datos muestrales observados. Por su parte, cuando $FB_{AB} > 1$ diríamos que la hipótesis A es más probable que la hipótesis B , teniendo en cuenta los datos observados empíricamente. La magnitud de ese estadístico indicaría cuánto más probable es la hipótesis A frente a la B . Por ejemplo, un factor de Bayes igual a 20 indicaría que la hipótesis A es 20 veces más probable que la B . Por el contrario, y de manera análoga, cuando $FB_{AB} < 1$, la conclusión a la que podemos llegar es que la hipótesis más probable teniendo en cuenta los datos observados es la B .

Los Factores de Bayes son estadísticos muy útiles en la toma de decisiones porque alumbran o clarifican los caminos a seguir frente a situaciones de incertidumbre. Dado que su naturaleza es comparativa y confrontan la verosimilitud de unas hipótesis frente a otras, pueden ser utilizados para dar más o menos relevancia a las creencias que tenemos sobre las soluciones hipotéticas que planteamos ante los problemas. Aunque existen varias formas de interpretar los Factores de Bayes (Kass y Raftery 1995), vamos a presentar, con propósitos ilustrativos, los puntos de cortes que propuso Jeffreys (1948). Según este autor, existe una evidencia anecdótica en los datos en favor de una hipótesis frente a la otra cuando el Factor de Bayes está comprendido entre 1 y 3. Si, por su parte, la fracción de verosimilitud se encuentra entre 3 y 10, se podría considerar que la evidencia es substancial. Si el valor del factor está entre 10 y 30, diríamos que la evidencia registrada frente a la primera de las hipótesis es fuerte. Por último, si el factor está comprendido entre 30 y 100, diríamos que la evidencia empírica que apoya a una hipótesis frente a la otra es muy fuerte. Cuando estuviese por encima de 100, podríamos decir que es decisiva.

Un ejemplo de la aplicación de métodos bayesianos

En esta sección vamos a presentar un ejemplo muy sencillo que ilustra cómo podrían utilizarse los métodos bayesianos para detectar o monitorizar el componente social de las amenazas híbridas. Utilizamos un modelo de red bayesiana porque permite ilustrar fácilmente cómo se puede organizar la información existente sobre un problema y cómo se puede utilizar de cara a su resolución estratégica. Estas herramientas han sido utilizadas anteriormente tanto con fines militares como en el ámbito de la detección inteligente de delitos (Das 1999; Garbolino y Taroni 2002; Oatley y Ewart 2003). Un ejemplo mucho más profundo y elaborado que este es el modelo de Análisis de Riesgos Adversarios (Ríos, Ríos y Banks 2012), sobre cómo los sistemas expertos probabilísticos y los diagramas de influencia pueden ser utilizados para la modelización de toma de decisiones bajo incertidumbre. Ese modelo, que podría perfectamente acomodarse al estudio de la amenaza híbrida, representa un paradigma que combina simultáneamente la teoría de juegos y el análisis de riesgos, frente a la toma de decisiones bajo incertidumbre.

Las redes bayesianas son modelos multivariados que permiten representar tanto la dimensión cuantitativa como cualitativa de un problema (Cowell et al. 1999). La dimensión cualitativa es lo que se conoce como Gráfico Dirigido Acíclico o GDA. Esto es, una estructura gráfica que conecta variables (representadas por nodos o vértices) por medio de aristas dirigidas (representadas por flechas). Como su nombre indica, los ciclos o *loops* no están permitidos en los grafos de una red bayesiana. Las flechas que conectan las variables tienen sentido estadístico dado que representan o indican que una variable

depende de otra o que una variable está influenciada por otra u otras. Por su parte, la dimensión cuantitativa del modelo quedaría determinada por un conjunto de funciones de probabilidad condicional que especifican las relaciones probabilísticas definidas por los enlaces presentes en el grafo. Tanto las características gráficas del modelo como las funciones de probabilidad son usadas por el teorema de Bayes para actualizar la probabilidad de ocurrencia de los eventos del modelo y, por tanto, para tomar decisiones respecto a la resolución de problemas.

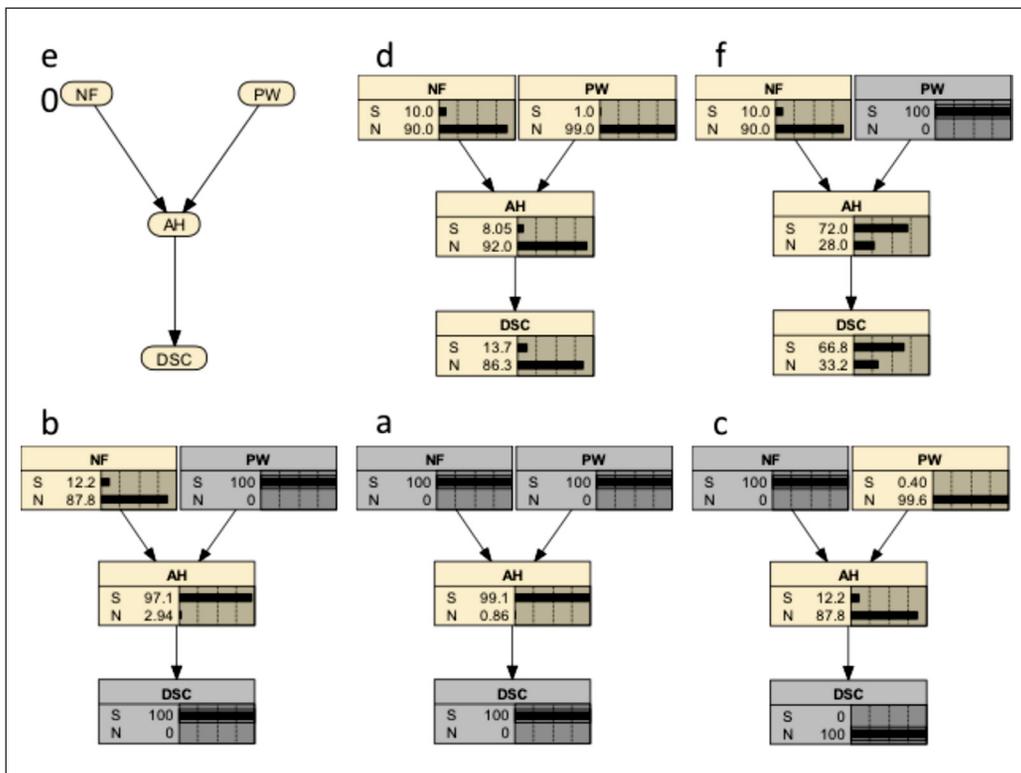
Supongamos que estamos monitoreando la aparición del componente social de la amenaza híbrida. Para referirnos al evento “se está perpetrando algún tipo de hostilidad vinculada con el componente social de la amenaza híbrida” vamos a utilizar las letras *AH*. Es decir, vamos a considerar que la amenaza híbrida es una variable que puede estar presente con cierta probabilidad. Si atendemos a los planteamientos de Lanoszka (2016), podríamos identificar algunas señales que se vinculan con el inicio de la ocurrencia de amenazas híbridas. Por ejemplo, la presencia de noticias falsas que pueden radicalizar o polarizar a la sociedad, el asalto de páginas webs oficiales o institucionales y la debilitación de la sociedad civil son eventos que se han asociado tradicionalmente con estadios iniciales de ataques híbridos (Grinberg et al. 2019). Por tanto, vamos a considerar que todos esos eventos son variables estadísticas y las vamos a modelar como variables dicotómicas que asumirán dos valores posibles: “se está produciendo el evento en cuestión” y “no se está produciendo el evento en cuestión”. Además, vamos a representar las noticias falsas con las letras *NF*, el asalto o pirateo a páginas webs con las letras *PW* y la debilitación de la sociedad civil con la expresión *DSC*.

Para ilustrar cómo se podría modelar este problema vamos a utilizar el software Netica en su versión 6.05. Aunque Netica es un software comercial, la compañía proporciona el acceso a una versión demo totalmente funcional que está limitada en el número de variables (López 2012). Como se puede apreciar en el panel *a* de la figura 1, un gráfico hipotético que podría ilustrar la relación entre todas esas variables podría ser aquel que especifica que la amenaza híbrida dependería de la presencia de noticias falsas y del pirateo de páginas webs. El grafo del panel *a* también representa que la debilitación de la sociedad civil dependería

de la amenaza híbrida. Este grafo, por tanto, ilustra una situación ficticia e hipotética que solo tiene sentido con fines ilustrativos, en la que la sospecha de un ataque híbrido inminente estaría condicionada por la proliferación de noticias falsas y por el ataque sistemático de webs oficiales o gubernamentales. Por su parte, el gráfico modela la situación que indicaría que la amenaza híbrida genera cierto grado de debilitación cívica en la sociedad objeto de un ataque híbrido.

Vamos a considerar cada una de las variables mencionadas, que se relacionan con la amenaza híbrida, como variables dicotómicas

Figura 1. Representación de la estructura y el funcionamiento de una red bayesiana



Leyenda: AH: amenaza híbrida, NF: noticias falsas, PW: pirateo web, DSC: debilitación de la sociedad civil, S: sí, N: no. Las probabilidades están expresadas en términos porcentuales.

Fuente: elaboración propia.

en las que serán posibles valores afirmativos (S) o negativos (N). Además, consideraremos que cada una de estas variables está definida paramétricamente por una función de probabilidad condicional en función de las variables de las que depende. De esta manera, el modelo que hemos presentado en el panel *a* de la figura 1 quedaría especificado o definido por ocho parámetros u ocho estimaciones de probabilidad.

Supondremos que las estimaciones de probabilidad (expresadas en forma porcentual) son fruto del análisis exhaustivo que se ha llevado a cabo en una agencia de inteligencia gubernamental. Según este, la probabilidad basal de ataques piratas contra webs oficiales es del 1 % y la probabilidad de difusión de noticias falsas es de un 10 %.

Estos parámetros podrían tener sentido considerando que es más fácil que se difunda un bulo falso que el asalto organizado a una web oficial o gubernamental. Las dos variables no dependen de ninguna otra (técnicamente se dice que son variables madre). No obstante, la variable que representa la amenaza híbrida sí depende de las dos anteriores. Por ello, quedaría definida por cuatro parámetros de probabilidad condicional, que se relacionarían con el resultado de combinar cartesianamente las dos variables previas. Una posible parametrización para esta variable podría ser la siguiente, expresada en notación matemática:

$$P(AH = S \mid NF = S, PW = S) = 90 \%,$$

$$P(AH = S \mid NF = N, PW = N) = 5 \%,$$

$$P(AH = S \mid NF = S, PW = N) = 56 \% \text{ y}$$

$$P(AH = S \mid NF = N, PW = S) = 70 \%.$$

Así, según lo expresado en a), diríamos que la probabilidad de que se estén produciendo amenazas híbridas dado que se han producido noticias falsas y ataques webs sería del 90 %. Por su parte, si nos fijamos en b), diríamos que la probabilidad de que se esté produciendo

una amenaza híbrida en ausencia de noticias falsas y de ataques de webs oficiales o gubernamentales sería del 5 %. Los parámetros c) y d) se interpretarían análogamente.

Los parámetros asociados con la variable DSC tendrían que estar expresados en términos de los valores de la variable AH. Supongamos que sus parámetros expresados en notación probabilística son los siguientes: $P(DSC = S \mid AH = S) = 90 \%$ y $P(DSC = S \mid AH = N) = 7 \%$. O expresado en palabras, que la probabilidad de que la sociedad civil se debilite cuando se ha producido una amenaza híbrida es del 90 %, mientras que la probabilidad de que esta misma sociedad se debilite es del 7 % cuando la amenaza híbrida no ha tenido lugar. Los valores complementarios de todas esas probabilidades se obtienen como la diferencia respecto a la unidad. Así, por ejemplo, $P(AH = N \mid NF = S, PW = S) = 1 - P(AH = S \mid NF = S, PW = S) = 10 \%$. Sobre todos estos valores de probabilidad son sobre los que el teorema de Bayes opera para hacer estimaciones del estado de cada una de las variables, teniendo en cuenta observaciones o evidencias sobre la situación evaluada.

Cuando todos los valores de probabilidad son tenidos en cuenta por la red bayesiana, se genera lo que se conoce como distribución previa del modelo. Esta aparece reflejada en el panel *b* de la figura 1. Representa las probabilidades vinculadas a cada uno de los estados de la variable cuando no se tiene información sobre la situación o cuando no se ha observado ningún dato sobre el problema. Por ejemplo, en el panel *b* se puede apreciar que, en principio, la probabilidad de ataque híbrido es relativamente pequeña, del orden del 8,5 %. Sin embargo, con este tipo de modelos podemos valorar el impacto que tendría la observación de alguno o algunos de los estados de estas

variables. De esa manera se puede evaluar el impacto que tendrían diferentes escenarios sobre la probabilidad de ocurrencia de un ataque híbrido y podrían llevarse a cabo acciones destinadas a minimizarlo. Por ejemplo, imaginemos que supiésemos que se ha perpetrado un ataque pirata a una web del gobierno. Como se aprecia en el panel *c* de la figura 1, podríamos concluir que la probabilidad (o nuestra creencia) de que se esté produciendo un ataque híbrido aumenta hasta el 72 %. Si seguimos utilizando el teorema de Bayes y nos informan que se ha observado una debilitación de la sociedad civil (panel *d* de la figura 1), nuestra estimación de probabilidad para el ataque híbrido aumentaría hasta el 97,1 %.

Obsérvese que la probabilidad de que se esté produciendo un ataque híbrido aumenta hasta el 99,1 % (panel *e* de la si, además, se detecta que se han propagado noticias falsas. Por último, tal y como se ilustra en el panel *f*, un escenario en el que se producen amenazas falsas, pero donde la sociedad civil está fortalecida, nos llevaría a pensar que la probabilidad de amenaza híbrida es tan solo del 12,2 %. Este tipo de valoración de escenarios es de vital utilidad en contextos en los que se han de llevar a cabo acciones destinadas a solventar misiones estratégicamente relevantes. Por ello, los modelos bayesianos podrían ser de utilidad para identificar y gestionar los componentes sociales de las amenazas híbridas a escala internacional (Ducaru 2016).

El ejemplo que hemos presentado es muy simple y, probablemente, poco realista, pero se ha concebido para tratar de ilustrar la utilidad de estos modelos estadísticos como aliados en la toma de decisiones estratégicas en situaciones bajo incertidumbre. Además, el modelo es estático en el tiempo y podría no reflejar las verdaderas relaciones que se establecen entre

las variables. Afortunadamente, diferentes técnicas surgidas en el seno de la Inteligencia Artificial han sido desarrolladas para identificar y encontrar modelos estadísticos con los datos de los que se dispone. Algunos autores sugieren que esa estrategia de trabajo puede ser fructífera (Anwar y Hassan 2017). Además, existen herramientas informáticas que permiten encontrar las estructuras de red bayesiana más plausibles, a partir de conjuntos de datos (por ejemplo, Heckerman 1995; Ruiz-Ruano 2015; Scutari 2010).

Conclusiones

La humanidad parece aproximarse a una situación en la que el binomio persona-computadora tiende a parecerse a lo que se nos ha presentado repetidamente en las películas o relatos de ciencia-ficción. Da la sensación de que, como sugieren algunos vaticinios quizá no extremos, llegará el momento en el que las computadoras podrán estar conectadas directamente a nuestros cerebros. Quizá esas proyecciones futuristas nunca lleguen a materializarse, pero lo que es cierto es que, cada vez más, las personas parecemos depender más de las computadoras para comunicarnos e interactuar con nuestro entorno social. Independientemente de si valoramos eso como algo positivo o negativo, hay que reconocer que existen ciertos riesgos relacionados con el inicio o desarrollo de ataques híbridos en las democracias legítimamente constituidas.

En este artículo hemos mostrado cómo podrían modelarse estadísticamente ciertos aspectos de la dimensión social de la guerra híbrida. Hemos utilizado una herramienta estadística perteneciente al ámbito de la inferencia bayesiana, las redes bayesianas, y hemos visto

cómo sus cálculos pueden ser utilizados para gestionar o enfrentar la toma de decisiones. Los modelos probabilísticos multivariados pueden servir para generar diferentes escenarios que producen distribuciones de probabilidad condicionada a diferentes observaciones. Así, este tipo de modelos bayesianos u otros que pudiesen desarrollarse serían apropiados para monitorear la amenaza híbrida en su vertiente social, dada su habilidad para racionalizar las situaciones de alta incertidumbre.

Los modelos estadísticos serán eficientes en la medida en que las definiciones de las variables estén claramente definidas. Por tanto, dado que la definición de guerra híbrida no es todavía algo universalmente aceptado, podríamos incurrir en errores si tratásemos de diseñar modelos destinados a predecirla. La propuesta que hemos utilizado en este trabajo alude a una definición de guerra híbrida caracterizada por agresiones graduadas, que incrementan en grado de hostilidad. Puede ser un buen punto de partida, pero sería necesario seguir trabajando en este campo. Como sucede en muchas áreas de estudio del ámbito social, hay que tener en cuenta que, así como la guerra híbrida es algo naturalmente dinámico y complejo, la dimensión social de los ataques híbridos no deja de ser un concepto escurridizo y difícilmente manejable desde un punto de vista científico. La agitación social siempre ha existido, existe y existirá; reconocer acciones deliberadas que se encuadren en el marco del concepto de guerra híbrida es una tarea de complejidad abismal. Las máquinas y los algoritmos informáticos que podemos utilizar para detectar fenómenos sociales como el que analizamos en este artículo tampoco están libres de error, de un tipo o de otro, y quizá no sea lo más apropiado confiar en ellas para la resolución de cierto tipo de problemas.

Bibliografía

- Alonso, Diego, y Elisabet Tubau. 2002. "Inferencias bayesianas: una revisión". *Anuario de Psicología* 33: 25-47.
- Anscombe, Francis John. 1961. "Bayesian statistics". *The American Statistician* 15: 21-24. [dx.doi.org/10.2307/2682504](https://doi.org/10.2307/2682504)
- Anwar, Amaan, y Syed Imtiaz Hassan. 2017. "Applying Artificial Intelligence Techniques to Prevent Cyber Assaults". *International Journal of Computational Intelligence Research* 13: 883-889.
- Bayes, Thomas. 1763. "An essay towards solving a problem in the doctrine of chances". *Philosophical Transactions* 53, 370-418. [dx.doi.org/10.1098/rstl.1763.0053](https://doi.org/10.1098/rstl.1763.0053)
- Berger, Peter Ludwig, y Thomas Luckmann. 1968. *La construcción social de la realidad*. Buenos Aires: Amorrortu.
- Bolstad, William. 2007. *Introduction to Bayesian Statistics*. Hoboken: Wiley.
- Butler, Declan. 2016. "A World Where Everyone Has a Robot: Why 2040 Could Blow Your Mind". *Nature* 530: 398-401. [dx.doi.org/10.1038/530398a](https://doi.org/10.1038/530398a)
- Castelvecchi, Davide. 2019. "Machine Learning Comes Up Against Unsolvable Problem". *Nature* 565: 277. [dx.doi.org/10.1038/d41586-019-00083-3](https://doi.org/10.1038/d41586-019-00083-3)
- CIA (Central Intelligence Agency). 1968. "Bayes' theorem in the Korean war". Intelligence Report No. 0605/68, Directorate of Intelligence.
- Cloud Security Alliance. 2012. "Top ten big data security and privacy challenges", https://downloads.cloudsecurityalliance.org/initiatives/bdwdg/Big_Data_Top_Ten_v1.pdf
- Colom, Guillem. 2019. "La amenaza híbrida: mitos, leyendas y realidades". *Instituto Español de Estudios Estratégicos* 24. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEE024_2019GUICOL-hibrida.pdf

- Cowell, Robert, Philip Dawid, Steffen Lauritzen, y David Spiegelhalter. 1999. *Probabilistic networks and expert systems*. Harrisonburg: Springer.
- Das, Balaram. 1999. *Representing uncertainties using bayesian networks*. Australia: Department of Defence/Defence Science and Technology Organization.
- Dixon, John. 1970. *Introducción a la probabilidad. Texto programado*. México: Limusa-Wiley.
- Ducaru, Sorin Dumitru. 2016. "The Cyber Dimension of Modern Hybrid Warfare and Its Relevance for NATO". *Europolity* 10: 7-23.
- Edwards, Ward, y Barbara Fasolo. 2001. "Decision Technology". *Annual Review of Psychology* 52: 581-606.
- Fisk, Charles. 1994. "The sino-soviet border dispute: a comparison of the conventional and Bayesian methods for intelligence warning", <https://www.cia.gov/library>
- Garbolino, Paolo, y Franco Taroni. 2002. "Evaluation of Scientific Evidence Using Bayesian Networks". *Forensic Science International* 125: 149-155.
- Glymour, Clark. 2001. *The Mind's Arrows. Bayes Nets and Graphical Causal Models in Psychology*. Cambridge: MIT Press.
- Glymour, Clark. 2003. "Learning, prediction and causal Bayes nets". *Trends in Cognitive Sciences* 7: 43-48.
- Gopnik, Alison, Glymour, Clark, Sobel, David, Schulz, Laura, Kushnir, Tamar, y Danks, David. 2004. "A Theory of Causal Learning in Children: Causal and Bayes Nets". *Psychological Review* 111: 3-32.
- Gopnik, Alison, y Laura Schulz. 2004. "Mechanisms of Theory Formation in Young Children". *Trends in Cognitive Sciences* 8: 371-377.
- Gopnik, Alison, David Sobel, Laura Schulz, y Clark Glymour. 2001. "Causal Learning Mechanisms in Very Young Children: Two, Three, and Four-Years-Olds Infer Causal Relations from Patterns of Variation and Covariation". *Developmental Psychology* 37: 620-629.
- Grinberg, Nir, Kenneth Joseph, Lisa Friedland, Briony Swire-Thompson, y David Lazer. 2019. "Fake News On Twitter During The 2016 U.S. Presidential Election". *Science* 363: 374-378. 10.1126/science.aau2706
- Heckerman, David. 1995. *A Tutorial On Learning with Bayesian*. Redmon: Microsoft Research.
- Held, Leonhard, y Manuela Ott. 2018. "On P-values and Bayes Factors". *Annual Review of Statistics and its Application* 5: 393-419. [dx.doi.org/10.1146/annurev-statistics-031017-100307](https://doi.org/10.1146/annurev-statistics-031017-100307)
- Hoffman, Frank. 2009. "Hybrid Warfare and Challenges". *Joint Force Quarterly* 52: 34-39.
- Hoijsink, Herbert, Pascal van Kooten, y Hulsker, Koenraad. 2016. "Bayes Factors Have Frequency Properties-This Should Not Be Ignored: A Rejoinder to Morey, Wagenmakers, and Rouder". *Multivariate Behavioral Research* 51: 20-22. 10.1080/00273171.2015.1071705
- Jarosz, Andrew, y Jennifer Wiley. 2014. "What Are the Odds? A Practical Guide to Computing and Reporting Bayes Factors". *Journal of Problem Solving* 7: 2-9. [dx.doi.org/10.7771/1932-6246.1167](https://doi.org/10.7771/1932-6246.1167)
- Jeffreys, Harold. 1931. *Scientific Inference*. Cambridge: Cambridge University Press.
- Jeffreys, Harold. 1948. *Theory of Probability*. Oxford: Oxford University Press.
- Jeon, Minjeong, y Paul De Boeck. 2017. "Decision Qualities of Bayes Factor and P Value-Based Hypothesis Testing". *Psychological Methods* 22: 340-360. [dx.doi.org/10.1037/met0000140](https://doi.org/10.1037/met0000140)
- Kass, Robert, y Adrian Raftery. 1995. "Bayes Factors". *Journal of the American Statistical Association* 90: 773-795. [dx.doi.org/10.1080/01621459.1995.10476572](https://doi.org/10.1080/01621459.1995.10476572)
- Lafuente, Guillermo. 2015. "The Big Data Security Challenge". *Network Security* 2015: 12-14. 10.1016/S1353-4858(15)70009-7

- Lanoszka, Alexander. 2016. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe". *International Affairs* 92: 175-195.
- Lilienfeld, Scott, Steven Jay Lynn, Laura Namy, y Nancy Woolf. 2011. *Psicología. Una introducción*. Madrid: Pearson.
- López, Jorge. 2012. "Cómo construir y validar redes bayesianas con Netica". *Revista Electrónica de Metodología Aplicada* 17: 1-17.
- Morey, Richard, y Jeffrey Rouder. 2011. "Bayes Factor Approaches for Testing Interval Null Hypothesis". *Psychological Methods* 16: 406-419. dx.doi.org/10.1037/a0024377
- Morey, Richard Donald, Eric-Jan Wagenmakers, y Jeffrey Rouder. 2016. "Calibrated Bayes Factors Should Not Be Used: A reply to Hoi-jtink, van Kooten, and Hulsker". *Multivariate Behavioral Research* 51: 11-19. dx.doi.org/10.1080/00273171.2015.1052710
- Oatley, Giles, y Brian Ewart. 2003. "Crimes Analysis Software: 'Pins in Maps', Clustering and Bayes Net Prediction". *Expert Systems with Applications* 25: 569-588.
- O'Hagan, Anthony, y Bryan Luce. 2003. *A primer on Bayesian statistics in health economics and outcome research*. Sheffield: MEDTAP International.
- Puga, Jorge, Krzywinski, Martin, y Naomi Altman. 2015. "Points of Significance: Bayesian statistics". *Nature Methods* 12: 377-378. dx.doi.org/10.1038/nmeth.3368
- Reboloso, Enrique. 1994. "Conducta colectiva y movimientos colectivos". En *Psicología social*, coordinado por José Francisco Morales, 763-800. Madrid: McGraw Hill.
- Ríos, David, Jesús Ríos, y David Banks. 2012. "Adversarial Risk Analysis". *Journal of the American Journal Association* 104: 841-854. dx.doi.org/10.1198/jasa.2009.0155
- Ruiz-Ruano, Ana María. 2015. "Aprendizaje estructural de redes bayesianas para modelar el emprendimiento académico de base sostenible y tecnológica". Tesis doctoral, Facultad de Ciencias de la Salud, Universidad Católica San Antonio de Murcia. <http://hdl.handle.net/10952/1556>
- Ruiz-Ruano, Ana María, y Jorge Puga. 2018. "Seguridad informática e inteligencia artificial en la era de la información masiva". En *Conflictos y diplomacia, desarrollo y paz, colaboración y medio ambiente*, dirigido por César Augusto Giner y Juan José Delgado, 711-724. Navarra: Aranzadi.
- Scutari, Marco. 2010. "Learning Bayesian Networks with the bnlearn R Package". *Journal of Statistical Software* 35 (3): 1-22. dx.doi.org/10.18637/jss.v035.i03
- Serrano, José. 2003. *Iniciación a la estadística bayesiana*. Madrid: Muralla/Hespérides.
- Sobel, David, Joshua Tenenbaum, y Alison Gopnik. 2004. "Children's Causal Inferences from Indirect Evidence: Backwards Blocking and Bayesian Reasoning in Pre-Schoolers". *Cognitive Science* 28: 303-333.
- Somiedo, Juan Pablo. 2018. "El análisis bayesiano como piedra angular de la inteligencia de alertas estratégicas". *Revista de Estudios en Seguridad Internacional* 4 (1): 161-176. dx.doi.org/10.18847/1.7.10
- Taddeo, Mariarosaria, Luciano y Floridi. 2018. "Regulate Artificial Intelligence to Avert Cyber Arms Race". *Nature* 556: 296-298. doi.org/10.1038/d41586-018-04602-6
- Von Solms, Rossouw, y Johan van Niekerk. 2013. "From Information Security to Cyber Security". *Computers and Security* 38: 97-102. doi.org/10.1016/j.cose.2013.04.004



Misceláneo

Narcomenudeo y control territorial en América Latina

Small Scale Drug Trafficking and Territorial Control in Latin America

Sebastián Saborío¹

Recibido: 29 de enero del 2019

Aceptado: 18 de julio de 2019

Publicado: 2 de diciembre de 2019

Resumen

El presente artículo analiza el fenómeno del control territorial llevado a cabo por parte de grupos criminales que se dedican al narcomenudeo en barrios de las ciudades latinoamericanas. Demuestra que las publicaciones sobre el tema asumen que existe una definición clara de “control territorial”, pero terminan por referirse a procesos sociales diferentes. Apoyándose en los conceptos de territorio, territorialidad y territorialización, el autor define los elementos que conforman las diferentes modalidades de control territorial que llevan a cabo las bandas del narcomenudeo. De esa manera, brinda una herramienta de análisis compuesta por diferentes indicadores: quiénes son los sujetos controlados por las bandas, cuál es la extensión, modalidad y objetivos del control territorial y de qué manera dichos grupos influyen la vida política, asociativa y otras esferas de la cotidianidad de las comunidades en las cuales están situados.

Palabras clave: control territorial; criminalidad; indicadores; narcomenudeo; territorio; violencia

Abstract

This article analyses the phenomena of territorial control that is carried on by small scale drug trafficking groups in Latin American cities. It shows that existing publications on this topic take for granted what “territorial control” is, but end up referring to different social processes. Learning in the concepts of territory, territoriality and territorialization, the author defines which elements shape the different modalities of territorial control implemented by small scale drug trafficking groups. In this way, he provides an analytical tool composed by different indicators: who are the subjects controlled by drug gangs, what is the extension, modality and objectives of territorial control and how do these groups influence political and associative life as well as other spheres of everyday life of the communities in which they are located.

Key words: criminality; indicators; small scale drug trafficking; territorial control; territory; violence

¹ Instituto de Investigaciones Sociales y Escuela de Sociología de la Universidad de Costa Rica, Costa Rica, sebastian.saborio@ucr.ac.cr,  orcid.org/0000-0002-3061-7787



Introducción

El hecho de que grupos criminales dedicados al narcomenudeo controlen partes de territorios urbanos en América Latina es indiscutible. El narcomenudeo es “el comercio de drogas ilícitas a pequeña escala” (Zamudio Angles 2013, 112), es decir, la compraventa de dosis de aprovisionamiento y consumo personal (Raffo López y Gómez Calderón 2017). Aunque existen relaciones entre este y el narcotráfico, los dos fenómenos no son la misma cosa. El segundo necesita una capacidad organizativa mucho mayor (De León Beltrán y Garzón 2014) y está compuesto por cuatro etapas: producción, distribución, comercialización y capital circulante. Este último “se tipifica en los códigos penales como lavado de activos o blanqueo de capitales” (Cortés, Gómez y García 2015, 3).

El presente artículo tiene el objetivo de analizar en profundidad el fenómeno del control territorial, comprender en qué consiste y cuáles son las modalidades a través de las cuales dichos grupos lo llevan a cabo. El concepto de territorio es de suma importancia para la comprensión del narcomenudeo, porque el factor territorial juega un papel decisivo en la creación y reproducción de grupos criminales que actúan a escala local (Raffo López y Gómez Calderón 2017). No obstante, hasta el momento son escasas las investigaciones científicas al respecto (Gutiérrez Rivera 2012). Muchos elementos que caracterizan a la relación entre control territorial y grupos criminales aún no han sido analizados en profundidad, y dichos vacíos se reflejan en los límites e imprecisiones que se pueden hablar en la literatura científica.

Por ejemplo, cuando Rodgers y Baird (2016, 34) afirman que “las pandillas pueden

construir su reputación y extender su dominio por medio de formas de control territorial”, no es claro a qué se refieren. En primer lugar, en la bibliografía consultada no se define al control territorial, ni cuáles son los aspectos que lo caracterizan. Tampoco se aclara qué definición de territorio se utiliza al momento de hablar de control territorial. De hecho, de las publicaciones consultadas sobre temas relacionados con crimen, violencia y narcomenudeo, solo Gutiérrez Rivera (2012) brinda una definición de territorio. En segundo lugar, no siempre se toman en consideración las particularidades de los diferentes contextos locales analizados y, en consecuencia, de las diferentes formas de control territorial que estos producen. Como se demostrará más adelante, el fenómeno del control territorial por parte de grupos criminales que se dedican al narcomenudeo ejerce una influencia directa en la vida política y social de gran parte de las comunidades carentes de la región latinoamericana (Arias 2017). Igualmente, la tiene en la violencia que se lleva a cabo en estas, lo cual genera un impacto directo en la seguridad ciudadana y en las políticas relacionadas con ella (Rodgers y Baird 2016).

Este artículo no pretende analizar las políticas públicas de seguridad, o de otra naturaleza, que se ejecutan en contextos de exclusión social que cuentan con la presencia de narcomenudeantes. Sin embargo, hace hincapié en el hecho de que, para garantizar la factibilidad y el éxito de dichas políticas, al momento de idearlas es indispensable comprender si los sujetos en cuestión controlan o no los territorios en los cuales están localizados. Para ello, se necesita conocer en profundidad las particularidades de cada localidad, con la finalidad de evitar soluciones estandarizadas, las cuales pueden resultar poco eficaces. Las característi-

Tabla 1. Indicadores de control territorial a escala barrial por parte de grupos que se dedican al narcotráfico

<ul style="list-style-type: none"> • PERSONAS CONTROLADAS - Población local - Sujetos externos a los barrios • Visitantes <ul style="list-style-type: none"> - Permitir o impedir el acceso • Facciones rivales • Policía <ul style="list-style-type: none"> - Patrullajes rutinarios (capacidad de ingresar en el territorio en cualquier momento) - Operativos - Incapacidad de ingresar en el barrio en cualquier momento - Falta de voluntad de ingresar en el barrio en cualquier momento - Acompañados de patrullajes rutinarios • PRESENCIA DE CRIMINALES ARMADOS - Visible <ul style="list-style-type: none"> • Al ingreso de los barrios • Cercanía de los puntos de venta de drogas • Alrededores del barrio - No visible - Cantidad - Inexistente • EXTENSIÓN DEL CONTROL TERRITORIAL - Todo el barrio - Cercanía de los puntos de venta - Parte/partes del barrio - Conjunto de barrios • OBJETIVOS DEL CONTROL TERRITORIAL - Venta de drogas ilícitas/ monopolio de la venta de drogas ilícitas <ul style="list-style-type: none"> • Protección de los miembros de grupos criminales • Protección de los compradores de drogas • Defensa del territorio contra ataques de las bandas rivales • Defensa del territorio contra la policía • Ejercer una influencia en la esfera política local • Ejercer una influencia en la esfera asociativa local • Prohibición de la violencia doméstica • Prohibición de asaltos y robos • Prohibición de riñas • Mediación de conflictos - Vigilancia del respeto del código de conducta - Acciones coercitivas, castigos para aquellos que no respetan el código de conducta 	<ul style="list-style-type: none"> • GUERRAS TERRITORIALES - Contra bandas rivales <ul style="list-style-type: none"> • Presencia de dos o más bandas en un territorio • Invasión del territorio controlado por parte de otra banda - Contra la policía <ul style="list-style-type: none"> • Operativos de la policía con objetivos específicos (arrestos, confiscación de armas y drogas) • Intento de la policía de retomar el control de territorios dominados por grupos criminales • Homicidios premeditados contra agentes de policía • Ataques contra bases policiales - Modalidades de combate <ul style="list-style-type: none"> • Combate abierto que intenta mantener su posición en caso de ataque externo • Reactivo y caracterizado por la fuga en caso de ataque externo • Con acciones dirigidas - asesinatos mirados (sicariato) - secuestros - Armas de fuego de las bandas <ul style="list-style-type: none"> • Pequeño calibre (pistolas) • Grueso calibre (armas de guerra) • IMPEDIR SERVICIOS PÚBLICOS - Ordenar el cierre de los negocios - Ordenar el cierre del transporte público • VIOLENCIA CONTRA LOS RESIDENTES <ul style="list-style-type: none"> - Homicidios - Robo de terrenos y casas - Castigos por romper los códigos de conducta • PLURALISMO JURÍDICO - Creación de normas (códigos de conducta) - Control de la violencia por parte de las bandas (monopolio interno de la violencia) <ul style="list-style-type: none"> • Prohibición de los homicidios • Prohibición de las violaciones - Amenazas <ul style="list-style-type: none"> • Actividades de protesta (permitir, prohibir o controlar) - Ocupaciones de suelo - Marchas • INSTITUCIONES PÚBLICAS - Mediación entre el Estado y la población local <ul style="list-style-type: none"> • Distribución de bienes a la población • Distribución de servicios a la población • Responsables de velar por la construcción de infraestructuras
--	---

Tabla 1. (Continuación)

<ul style="list-style-type: none"> • BENEFICIO A LA COMUNIDAD LOCAL - Venta de bienes y servicios a precios inferiores a los del mercado - Ceder bienes y servicios de forma gratuita - Ganancias económicas para los miembros del narcomenudeo - Actividades recreativas - Protección <ul style="list-style-type: none"> • Protección contra la violencia de otras bandas • Protección contra la violencia policial • Protección contra la violencia interpersonal (ver control de la violencia) • LEGITIMIDAD - Los residentes aceptan el uso y monopolio interno de la violencia por parte de las bandas - Los residentes aceptan el código de conducta de las bandas - Los residentes aceptan que se lleve a cabo la actividad de narcomenudeo - Los residentes apoyan activamente a las bandas y a la actividad de narcomenudeo <ul style="list-style-type: none"> • Informan sobre la actividad policial • Informan sobre la presencia de grupos rivales • Esconden armas • Esconden drogas • VIDA ASOCIATIVA Y CÍVICA - Control de las organizaciones comunitarias <ul style="list-style-type: none"> • Injerencia sobre actividades y decisiones • Control total de las organizaciones • Violencia contra líderes comunitarios - Homicidios 	<ul style="list-style-type: none"> - Contienda con las instituciones públicas - Relaciones con la policía <ul style="list-style-type: none"> • Antagónicas • Colaborativas <ul style="list-style-type: none"> - Venta de armas y drogas por parte de la policía - Protección brindada por la policía - Evitar operativos, patrullajes y arrestos - Ignorar la actividad de narcomenudeo - Liberar a miembros de bandas arrestados - Informar sobre operativos y otras informaciones reservadas <p>RELACIONES CON PARTIDOS POLÍTICOS</p> <ul style="list-style-type: none"> - Gestionar campañas electorales - Intimidar a los residentes para que voten por un candidato - Obligar a los partidos a postular a determinada persona como candidata - Postular a un miembro de las bandas como candidato
---	---

cas políticas, sociales, históricas, económicas y geográficas de los países, las ciudades y barrios, así como de los grupos criminales pueden generar regímenes de control local diferenciados, que requieren análisis y soluciones específicas (Arias 2017; Wolff 2015; De León Beltrán y Garzón, 2014; Salas Salazar 2015).

El artículo se basa en una revisión bibliográfica de 75 artículos científicos y capítulos de libros sobre temas relacionados con narcomenudeo, territorio, violencia y criminalidad, principalmente en el contexto latinoamericano. El análisis de la bibliografía, que se realizó a través del programa Nvivo12, permitió

elaborar 86 “nodos” temáticos con respectivos “subnodos” y construir indicadores relacionados con el control territorial ejercido por parte de grupos que se dedican al narcomenudeo. A partir de ello, se brindan elementos útiles para comprender el fenómeno del control territorial. La siguiente lista de indicadores (tabla 1) reúne los aspectos que, según cada uno de los casos, pueden conformarlo. Además, estos indicadores son una herramienta potencial para el análisis de contextos locales y la elaboración de políticas públicas.

Territorio, territorialidad y territorialización

Sack (1986) define el territorio como un “área de acceso controlado”. En él se presentan “relaciones de poder relativamente homogéneas” (Haesbaert 2011, 66). El control del acceso a un área y el establecimiento de relaciones de poder son útiles tanto para “sacar provecho de sus recursos [del territorio] como para controlar los flujos, especialmente, de personas y bienes” (Haesbaert 2011, 66). Acorde con esta definición, es importante comprender por parte de quién es controlado el territorio y qué provecho se obtiene.

En el caso del narcomenudeo, el recurso es el espacio usado para la venta de drogas. Aunque a diferentes niveles e intensidades puede existir una connivencia ciudadanía-criminalidad, en muchos casos el espacio es expropiado a la población local por parte de los miembros de los grupos criminales. En otras palabras, el narcomenudeo produce “relaciones malévolas” (Sack 1983, 58),² en las que los grupos criminales se benefician del control ejercido sobre el territorio, a expensas de la mayoría de los residentes. Para Lessing (2011, 80), a diferencia de la producción, que genera superávit, “la expropiación solo transfiere recursos existentes de una persona a otra”. Así, la imposición de la venta de drogas por los miembros de las bandas criminales puede ser considerada una forma de expropiación del espacio, lo que impide la creación de formas de producción que podrían generar ganancias a los residentes que no se involucran en la actividad de narcomenudeo. Esto sucede en mayor medida cuando el narcomenudeo pone

en práctica formas de interacción depredadoras con las comunidades (Rodgers y Baird 2016). Además, a causa de la violencia que la caracteriza, dicha actividad puede disminuir el goce del espacio por el resto de la población.

Es necesario subrayar que existen diferentes tipologías de grupos que pueden llevar a cabo formas de control territorial. Según Cunjama López y García Huitrón (2014), en la economía criminal, una de las formas a través de las cuales el espacio puede asumir la función de territorio es cuando su apropiación y defensa generan ganancias gracias a la producción o la distribución de drogas ilícitas. Este artículo se focaliza en los grupos dedicados al narcomenudeo, que ejercen formas de control territorial en barrios ubicados en zonas urbanas de América Latina.

A continuación, se tratará el narcomenudeo como un fenómeno unitario. Sin embargo, es necesario aclarar que es desarrollado por personas que realizan diferentes funciones y poseen un grado distinto en la cadena de mando. Por ejemplo, en los barrios urbano-marginalizados de Costa Rica, los grupos se dividen en personas líderes, contadoras, operacionales (encargadas de la seguridad y de los ataques contra grupos enemigos), “robots” (encargadas de la venta directa) y supervisoras (encargadas de vigilar la venta de drogas) (Saborío 2019). A estas categorías se suman los “campaneros” (como son llamados en el contexto colombiano), los cuales tienen la tarea de vigilar y advertir sobre la presencia de sujetos externos que representan una amenaza a la actividad criminal de los grupos a los cuales pertenecen (Cortés, Parra y Durán 2012; Ordóñez Valverde 2017).

El aporte teórico de Sack (1983, 1986) permite delimitar el concepto de territorio y obliga a comprender: A) la utilidad que el control de este puede tener para los grupos

² Todas las citas de textos en idiomas diferentes al español han sido traducidas literalmente por parte del autor.

criminales, B) cuáles son los recursos que generan provecho, C) quiénes son los sujetos bajo control y D) cuáles, y de qué tipo, son las relaciones de poder que se generan como consecuencia del narcomenudeo.

Las bandas criminales pueden controlar el acceso al área en la que se posicionan con guardias armadas, las cuales se desplazan también en sus alrededores, principalmente cerca de los puntos de venta de drogas (Arias 2017; Saborío 2017), manteniendo de esa manera bajo control el flujo de personas. Como se profundizará más adelante, las personas controladas por las bandas del narcomenudeo pueden ser los miembros de grupos criminales rivales y de la policía, contra los cuales se defiende el territorio en caso de invasiones; los miembros del mismo grupo criminal, contra los cuales pueden surgir conflictos internos; o los miembros de la comunidad, que pueden representar un obstáculo o un apoyo a sus actividades delictivas. La extensión de los territorios, que en América Latina se encuentran bajo control de sujetos dedicados a la venta de drogas en pequeña escala, tiene que ser medida caso por caso. Como subraya Lessing (2008), esta puede estar limitada a pequeños espacios dentro de barrios o puede comprender la totalidad de estos. Verificar la capacidad de los narcomenudeantes de controlar los accesos a determinadas áreas geográficas, su extensión y el flujo de personas en su interior (miembros de bandas rivales, policías y población local) aporta elementos fundamentales para comprender el nivel de control territorial que tales grupos efectivamente ejercen.

Sack (1983, 55) diferencia el concepto de territorio de aquel de territorialidad. Para el autor, la territorialidad humana o simplemente territorialidad, es “el intento de afectar, influenciar o controlar acciones e interaccio-

nes (de personas, cosas y relaciones) mediante la delimitación y el control sobre un área geográfica. La actividad de control y gestión del territorio que permite y facilita la “compra-venta y el consumo de estupefacientes” (Cortés y Parra 2011, 39) puede ser entendida como la territorialidad del narcomenudeo. El área geográfica controlada se vuelve territorio y recurso de este. La definición de Sack (1983) permite identificar los objetivos de los grupos criminales que realizan formas de control territorial. El control del territorio protege a los consumidores y vendedores de la represión policial y de ataques de grupos rivales (Lessing 2008), y permite que los miembros de los grupos criminales ejerzan una influencia directa en las esferas políticas y económicas de los barrios en los que se establecen (Raffo López y Gómez Calderón 2017; Arias 2017). Ambos elementos tienen la función de facilitar la finalidad última de permitir el narcomenudeo, es decir, de generar ganancias a través de la venta de drogas a escala microlocal.

El artículo analiza el control territorial que tiene como objetivo el narcomenudeo, lo que no significa que los grupos que se dedican a ello se limitan a sacar provecho del control territorial únicamente a través de este. Por ejemplo, puede suceder que se especialicen también en la extorsión a residentes y dueños de negocios, la venta de armas, la venta ilegal de servicios legales como agua, luz, gas, televisión por cable y transportes públicos y la inversión del dinero del narcomenudeo en establecimientos comerciales legales (Moncada 2016; Lessing 2008; Arias 2017; Savenije y van der Borgh 2004; Ordóñez Valverde 2017; Rodgers y Baird 2016; Berg y Carranza 2018; Cortés, Parra y Durán 2012).

De acuerdo con Sack (1986), la territorialización es la estrategia que se lleva a cabo

para controlar los recursos de una determinada área o, en otras palabras, la creación e implementación de un “sistema de control de los recursos” (Rasmussen y Lund 2018, 388) capaz de establecer nuevas formas de autoridad. En contextos de narcomenudeo, el barrio se transforma en un “territorio de la estrategia” (Ordóñez Valverde 2017, 117) en el que la contraposición entre grupos criminales, y entre estos y el Estado, puede generar nuevas autoridades a escala microlocal. Como dirían Gutiérrez Rivera (2012), la estrategia de las pandillas determina su capacidad de controlar el territorio. Rasmussen y Lund (2018, 393) recuerdan que la territorialización requiere

el establecimiento de una administración territorial, de la institución de un sistema legal y con éste la creación de sujetos de derecho y leyes de propiedad, establecer límites y mapear espacios y, de manera crucial, asegurar la capacidad de aplicar todos y cada uno de estos puntos con la fuerza, si necesario.

Según lo presentado hasta el momento, para que en el narcomenudeo exista control territorial, es necesario que exista un territorio, entendido como un espacio con recursos explotables (en este caso es un recurso inmaterial, es decir, la posibilidad de vender drogas) donde se llevaron a cabo procesos de territorialización (ideación y puesta en práctica de una estrategia capaz de generar nuevas formas de autoridad local, con el fin de vender drogas), que producen una territorialidad (la autoridad efectiva y practicada de un grupo que vende drogas). A la luz de la teorización de Sack (1983, 1986) y de su uso reciente, en las próximas secciones se desarrollarán los indicadores propuestos en la introducción. Se señala qué elementos conforman el control territo-

rial y cuáles son las prácticas que los miembros de tales grupos llevan a cabo para realizarlo. De esa manera, se brinda una base útil para futuras investigaciones sobre el tema, las cuales podrán comprobar la presencia o ausencia de cada uno de estos elementos en diferentes contextos sociales para poder determinar si (y hasta qué punto) se puede hablar de control territorial al momento de describir el dominio ejercido por las bandas del narcomenudeo.

Violencia

La violencia es un elemento intrínseco de cada proceso de territorialización, dado que su objetivo es la creación y recreación de nuevas formas de autoridad que buscan desplazar a aquellas ya existentes (Rasmussen y Lund 2018). La territorialización del narcomenudeo no es diferente. Si se considera el número de homicidios declarados y registrados, América Latina es la región con más violencia letal del mundo (Moncada 2016; Córdova 2017). El dato es importante porque la violencia en la región tiene como protagonistas a grupos criminales que se dedican a la venta de drogas (Arias 2017; Córdova 2017; Lessing 2011; Ordóñez Valverde 2017; Cunjama López y García Huitrón 2014; Vilalta Perdomo 2009; Berg y Carranza 2018). Según Valenzuela Aguilera y Ortega Breña (2013, 21), “la violencia en América Latina se ha vuelto territorial por naturaleza”. Esa es una de las razones principales que hacen necesario comprender con mayor precisión el fenómeno del control territorial.

Para De León Beltrán y Garzón (2014, 5), el narcomenudeo es “una economía criminal con un importante componente territorial”, que permite la creación de zonas urbanas dedicadas a la reproducción de esta y otras

actividades ilegales. En muchos casos, el objetivo de los grupos criminales no es la simple venta de drogas, sino el monopolio de estas (Lessing 2008). Para alcanzarlo, tienen que proteger el territorio de eventuales ataques de bandas enemigas. La territorialización es el producto de la competencia entre diferentes actores y grupos sociales, los cuales reivindican el control sobre un determinado territorio (Rasmussen y Lund 2018). La competencia entre agrupaciones rivales por el monopolio del narcomenudeo no siempre genera conflictos violentos (Berg y Carranza 2018). Las llamadas “guerras territoriales” (Rodgers y Baird 2016) se dan principalmente cuando un grupo intenta invadir el territorio donde otro ejerce el monopolio de la venta de drogas (Lessing 2008). Pueden llevarse a cabo a través del uso de armas de fuego de pequeño o gran calibre (Koonings y Veenstra 2007) y mediante “acciones dirigidas” como asesinatos mirados (sicariato) y secuestros (como sucedía hace una década en Colombia), o bajo la forma de combates abiertos, modalidad que caracteriza el caso de las guerras urbanas relacionadas con la venta de droga en pequeña escala en la ciudad brasileña de Río de Janeiro (Lessing 2011).

Los conflictos armados se pueden dar también entre las bandas del narcomenudeo y las fuerzas de policía, cuando las segundas intentan ingresar en los territorios controlados por las primeras para efectuar arrestos o confiscar armas y drogas (Arias 2017), o cuando intentan retomar el control de territorios dominados por grupos criminales (Saborío 2017). En otros casos, la violencia de los grupos criminales contra la policía no se limita a la defensa del territorio, sino que puede llegar a ser implementada como forma de ataque directo y calculado, como sucedió en São Paulo

(Brasil), donde la agrupación denominada *Primeiro Comando da Capital* (PCC) llegó al punto de realizar homicidios premeditados contra agentes y atentados explosivos contra bases policiales (Alves 2016; Willis 2015).

Los grupos criminales pueden emplear técnicas de combate de tipo reactivo contra la policía, caracterizadas por la invisibilidad y movilidad de sus miembros, o formas más orientadas a la confrontación directa, en las cuales la presencia consistente de criminales armados es más visible (Lessing 2008). El primer caso se caracteriza por el uso de armas de pequeño calibre, mientras que en el segundo las bandas pueden llegar a usar armas de guerra. En Río de Janeiro, las facciones criminales posicionadas en las favelas de la ciudad poseen en muchos casos “fusiles de asalto, ametralladoras, bazucas, [y] granadas” (Ricotta 2017, 66). El calibre de las armas que poseen los grupos del narcomenudeo puede hacer la diferencia en el caso de que se vean amenazados por rivales que cuentan con un alto potencial de fuego, como la policía, las fuerzas militares y otras facciones criminales. Esto implica que una mayor presencia, cantidad y visibilidad de criminales armados, en particular con armas de elevada capacidad de fuego, es uno de los elementos de peso mayor para el control y la defensa del territorio.

Se puede afirmar que, en contextos de narcomenudeo, la violencia “determina los espacios de control y usufructo del territorio” (Raffo López y Gómez Calderón 2017, 231). Por tanto, las bandas la usan de forma sistemática (Doyle 2016). Su presencia en un determinado territorio urbano es violenta por sí misma, en cuanto se garantiza en parte mediante el uso y la amenaza de la violencia. Sin embargo, a diferencia de lo que podría pensarse, las bandas no siempre generan may-

ores niveles de violencia. Como demuestra el caso de Brasil, no todas las facciones criminales del narcomenudeo consiguen controlar de la misma manera los lugares en los cuales están posicionadas (Wolff 2015). El control depende, en gran medida, de los recursos que estos grupos tengan a disposición para afrontar conflictos armados (Raffo López y Gómez Calderón 2017).

Ha sido demostrado que el nivel de violencia en un territorio está directamente relacionado con la capacidad de las facciones criminales de monopolizar el control de los territorios en los cuales se llevan a cabo los comercios ilícitos (Moncada 2016). Esto significa que, donde los grupos criminales alcanzan un mayor control territorial, el nivel de violencia será menor debido al hecho de que esta pasa a ser usada de manera selectiva, mirada y simbólica (Arias 2017; Wolff 2015). El caso ya mencionado del *Primer Comando da Capital* (PCC) es paradigmático al respecto. Willis (2015) mostró que el monopolio de dicho grupo en el control de los barrios carentes de São Paulo conllevó una drástica disminución de los homicidios en esas localidades. Resultados parecidos han sido registrados también fuera de América Latina. Por ejemplo, en la ciudad estadounidense de Camden, Nueva Jersey, se pudo observar que los territorios de venta de drogas que son controlados por una sola banda poseen niveles mucho menores de violencia respecto a aquellos donde se cuentan dos o más grupos (Taniguchi, Ratcliffe y Taylor 2011). Para Arias (2017), el monopolio del control territorial reduce el nivel de violencia no solo porque disminuye los conflictos entre bandas, sino también porque permite a los criminales mantener bajo control la violencia interpersonal entre los residentes, y brinda la posibilidad de tejer relaciones ilícitas con las

instituciones políticas y las fuerzas de policía, reduciendo la represión por parte del Estado. Las mismas investigaciones demuestran que, por el contrario, la multiplicidad de actores criminales en un mismo territorio genera mayores niveles de violencia, sea entre ellos mismos o entre las personas que ahí residen.

Policías y bandas rivales no son los únicos destinatarios de la violencia de los grupos criminales. En Brasil en algunos casos estos han llegado a ordenar el cierre del comercio y del transporte público fuera de los barrios que controlan, como forma de protesta contra la represión policial (Alves 2016). Según Bruneau (2014, 165), las pandillas centroamericanas son una amenaza a la seguridad de los residentes de los barrios vulnerables que controlan, los cuales se vuelven las principales víctimas de robos, extorsiones y homicidios. En la misma línea, Savenije y van der Borgh (2004) afirman que las maras salvadoreñas recurren al uso y la amenaza de la violencia contra los residentes de los barrios carentes, para asegurarse de que estos no los delaten con la policía. En general, la violencia es el medio a través del cual las bandas controlan a la población que se opone activamente a ellas, y sirve como instrumento de disuasión hacia las personas que no se posicionan ni a su favor ni en su contra para que, en otro momento, no se vuelvan una amenaza (Cortés, Parra y Durán 2012). La investigación de Arias (2017) en Colombia, Brasil y Jamaica prueba que los miembros de los grupos armados pueden llegar al punto de robar tierras y casas de los ciudadanos. La libre circulación de las personas también puede verse afectada. En Honduras, las pandillas deciden quién puede o no entrar en sus territorios (Von Santos 2016). En el Salvador algunos grupos imponen un peaje a la población local para entrar en sus

propios barrios (Savenije y van der Borgh 2004). Ordóñez Valverde (2017) afirma que, por estas razones, las calles de algunos barrios de la ciudad colombiana de Cali ya no pueden ser consideradas espacio público.

Influencia en la comunidad local

La incapacidad y falta de voluntad de los Estados latinoamericanos de incluir a la totalidad de la población en un sistema de garantías sociales y de suministro de servicios básicos genera un distanciamiento entre los barrios marginalizados y el resto de los territorios urbanos. Dicho distanciamiento es ulteriormente exacerbado por la presencia de los grupos del narcomenudeo, los cuales favorecen y potencian la creación de “fronteras invisibles” (ACAPS 2014). Estas remiten a los procesos de territorialización, en los cuales la creación de fronteras es una clara señal de la producción de nuevas autoridades y, en consecuencia, de nuevos territorios en los cuales determinados recursos son detectados y pasan a ser extraídos y comercializados (Rasmussen y Lund 2018). Dada la voluntad de extraer ganancias a través del uso del espacio para la venta de drogas, los grupos criminales no pueden emplear la violencia de forma indiscriminada contra los residentes.

En la mayor parte de los casos, ello generaría relaciones conflictuales que, potencialmente, representan un obstáculo para dichos negocios. Como señala Ordóñez Valverde (2017, 120), para las bandas del narcomenudeo, la violencia es utilitaria y responde al “régimen de la productividad”. Por lo tanto, quienes se dedican a la actividad y quieren ejercer el control en un territorio, tienen que producir formas de gobernación basadas en

un sistema legal paralelo al del Estado. Dicho de otro modo, para controlar un territorio no es suficiente enunciar su delimitación, sino también administrarlo a través de un sistema de “leyes” que se puedan hacer respetar y cumplir. De lo contrario, y según la contribución teórica de Weber (2011) sobre el Estado, el uso de la fuerza y la legitimidad, la simple intimidación e imposición de la fuerza no garantizan la adecuación de las conductas de los sujetos a las necesidades del narcomenudeo. En cambio, denotan la incapacidad de ejercer autoridad y, por ende, de controlar un territorio.

Se podría objetar que las personas ya están sometidas a las leyes del Estado, pero los gobiernos no son los únicos que poseen una autoridad efectiva sobre el manejo tanto de estas como de los recursos (Rasmussen y Lund 2018). En muchos casos, en los contextos de exclusión social en América Latina se da una superposición entre diferentes sistemas jurídicos. Algunos autores consideran que se lleva a cabo una sustitución del orden legal del Estado por el de los grupos criminales (De León Beltrán y Garzón 2014). Sin embargo, es necesario reconocer que, en realidad, la sustitución del sistema legal oficial no es total. Por ejemplo, en las localidades en cuestión los ciudadanos respetan muchas de las leyes del Estado, el cual además no está completamente ausente. Su presencia es evidente cada vez que representantes de las instituciones públicas cumplen sus funciones en esos territorios. El problema radica en que esto no sucede de la manera que debería ser; la presencia del Estado se vuelve discontinua y mucho menor respecto a las necesidades de las personas. En Río de Janeiro, el “desinterés del Estado a hacer respetar su propia legislación dentro de las favelas y a reglamentar la vida de sus resi-

dentos, permitió que dentro de éstas se desarrollara una forma jurídica diferente de la oficial” (Saborío 2014, 174). En esos contextos, primero las asociaciones de residentes y luego las facciones criminales del narcomenudeo crearon sistemas legales entendidos según la definición de derecho brindada por Boaventura de Sousa Santos (1988, 72) como un:

Conjunto de procesos reguladores y de principios normativos, considerados como justiciables por parte de un grupo, que contribuyen a la creación y a la prevención de contiendas y a una solución de estas a través de un discurso argumentativo, de amplitud variable, apoyado o no por la fuerza organizada.

Actualmente, en muchas de las favelas de Río de Janeiro se da una situación de pluralismo jurídico, es decir, coexisten dentro del mismo territorio “órdenes legales que no pertenecen al mismo sistema” (Engle Merry 1988, 871). Lo mismo sucede en otras ciudades latinoamericanas (Rodgers y Baird 2016), donde grupos criminales llevan a cabo un control social capaz de moldear los comportamientos de las personas a través de la creación de códigos de conducta (Valenzuela Aguilera y Ortega Breña 2013). Para Pérez Sáinz, Alas Velado y Montoya Hernández (2018), en las colonias de Soyapango, en el Salvador, ese código territorial está conformado por normas no escritas que son conocidas por los residentes y a las cuales se adecúan a través de estrategias que les permiten no incurrir en castigos. En algunos casos, resulta difícil comprender la utilidad de ciertos códigos de conducta impuestos por estos grupos. Por ejemplo, cuando en ciertas favelas de Río de Janeiro prohíben la utilización de prendas del color que representa a las bandas rivales (Machado da Silva 2008;

Lessing 2008). Sin embargo, en la mayoría de los casos es claro que su sistema jurídico tiene la función de permitir que en los territorios controlados se lleve a cabo la actividad de narcomenudeo de manera proficua y segura para los miembros de los grupos criminales. Eso significa también que las normas sirven para mantener la violencia interpersonal en la comunidad bajo control; para impedir que “se caliente la plaza”, es decir, que se llame la atención de las fuerzas de policía y así evitar sus operativos (Ordóñez Valverde 2017; Lessing 2008; 2011; Koonings y Veenstra 2007).

En contextos de control territorial del narcomenudeo, el Estado deja de tener lo que Max Weber considera su razón de existencia: el monopolio de la violencia legítima. En muchas de las áreas urbanas carentes de América Latina, la legitimidad del Estado y, en consecuencia, la acción coercitiva de su brazo armado, disminuyen a razón de la exclusión social que las caracteriza (Koonings y Kruijt 2004), y de la incapacidad y falta de voluntad de la policía de proteger a las personas ante la criminalidad y la violencia (Córdova 2017).

La lucha por la legitimidad es una lucha de territorialización (Rasmussen y Lund 2018). Para que el narcomenudeo compita con el Estado en ese ámbito, los habitantes de las comunidades locales no deben percibir como una mera imposición el sistema normativo de las bandas y los castigos que resultan de sus transgresiones. Por el contrario, tienen que estar convencidos de que quienes los ponen en práctica lo hacen de manera legítima, entendiendo la legitimidad como “la capacidad de un sistema político de generar y mantener la convicción de que las instituciones políticas existentes son las más apropiadas y adecuadas” (Córdova 2017, 49). La interpretación de las bandas del narcomenudeo como autoridades

“cuasipolíticas” (Berg y Carranza 2018, 2) deriva de la constatación de que, en muchos casos, no se limitan a imponer su propia voluntad y a hacerla respetar a través de la implementación de un código de normas y un aparato coercitivo. La búsqueda de legitimidad interna sirve para llevar a las comunidades locales del lado de estos grupos para que toleren y, cuando sea posible, apoyen sus actividades ilícitas (Koonings y Veenstra 2007) escondiendo en sus casas armas, drogas e individuos buscados por la policía, e informando sobre la actividad policial a las bandas (Lessing 2008).

La voluntad de las bandas de conquistar la legitimidad se refleja cuando estas conceden beneficios (económicos y de otra naturaleza) a las comunidades. En Río de Janeiro, los criminales de las favelas ofrecen a la población bienes y servicios a precios reducidos en comparación con los del mercado y, en algunos casos, los brindan de forma gratuita a los más necesitados. También llevan a cabo la mediación de conflictos entre vecinos, brindan actividades recreativas a la comunidad y suplen, a través del comercio de drogas, parte de la necesidad de los jóvenes desempleados de generar ganancias. Brindan un servicio de protección hacia los residentes, prohibiendo la violencia doméstica contra mujeres y niños, las violaciones, los robos y asaltos dentro de los territorios bajo su dominio, a través de normas y castigos que resultan claros y son acatados (Saborío 2014). Investigaciones en otras ciudades de la región latinoamericana señalan que los líderes de las bandas desarrollan formas de “asistencia social” y generan ingresos económicos para algunas personas de las comunidades en las que se sitúan (Cortés, Parra y Durán 2012). En muchos casos, los residentes de barrios carentes aceptan la violencia de las bandas porque los protege de la vio-

lencia de otros grupos criminales (Rodgers y Baird 2016; Berg y Carranza 2018), así como de la microcriminalidad causada por aquellos que tienen formas de adicción a las drogas que ellos mismos venden (Zamudio Angles 2013), y de la violencia policial (Alves 2016).

Asociacionismo, política e instituciones públicas

Arias (2017) analiza el papel que ejercen los grupos armados a escala barrial. Afirma que, contrario a lo que sostiene la mayoría de las publicaciones científicas que ven en ellos solo una fuente de desorden social, en muchos casos estos mantienen contactos con los aparatos gubernativos y cumplen una función importante en la gestión microlocal del orden en las democracias de América Latina y del Caribe. Su trabajo demuestra que los grupos armados de matriz criminal pueden llegar a influenciar, y hasta controlar totalmente, la vida asociativa y cívica de los barrios en los cuales están posicionados, limitando, direccionando o impidiendo la acción de las organizaciones comunitarias y las protestas, marchas y ocupaciones de suelo. El control de las organizaciones comunitarias raramente se lleva a cabo a través del simple convencimiento o como resultado de relaciones colaborativas entre estas y los miembros del narcomenudeo. A menudo el intento de controlar la vida asociativa de las comunidades genera fricciones y conflictos. A modo de ejemplo, entre 1992 y 2002 alrededor de 400 líderes comunitarios murieron a mano de los grupos criminales de las favelas de Río de Janeiro (Rodgers y Baird 2016).

Es probable que exista una relación entre la infiltración y usurpación que las bandas del narcomenudeo llevan a cabo en el asociativismo y el hecho de que, como demuestra Arias (2017),

los grupos armados en muchos casos asuman un papel de mediación entre la población local y el Estado. Como parte de ello, desempeñan actividades de defensa de los intereses de la ciudadanía (función que tradicionalmente corresponde a los movimientos sociales y a las organizaciones comunitarias), pueden llegar a ser los encargados de pedir la construcción de infraestructuras o distribuir bienes y servicios del Estado a la población, con el consenso de miembros de las instituciones públicas. Este fenómeno ayuda a consolidar la posición de los grupos del narcomenudeo en el territorio, aumentando a su vez su legitimidad ante las personas. Sin embargo, la situación no es generalizada; en otros casos existe una contienda entre las instituciones públicas y los agentes ilegales, para que estos últimos no asuman las funciones del Estado y, en consecuencia, no refuercen los lazos sociales con las comunidades en las cuales se sitúan (Raffo López y Gómez Calderón 2017). Cuando la contienda no se da, el riesgo efectivo es que se desarrolle una relación de corrupción entre las instituciones gubernativas y los grupos criminales, los cuales terminan ejecutando servicios públicos de manera conjunta (Valenzuela Aguilera y Ortega Breña 2013). En la relación entre instituciones y narcomenudeo, una de las formas de corrupción más analizadas es la que involucra a las fuerzas de policía. En Río de Janeiro la amplitud y normalización del fenómeno, desde la década de 1980, ha sido tal que muchos agentes de policía en las favelas no solo son conniventes con la venta de drogas, sino que llegan a formar, ellos mismos, grupos criminales dedicados a la venta de armas y drogas. Además, aceptan de forma sistemática ingentes cantidades de dinero por parte de las bandas para garantizar la protección de sus miembros y no obstaculizar sus actividades (Misse 2011).

Para Berg y Carranza (2018), la colaboración entre instituciones y grupos criminales puede, de acuerdo con cada caso, tener efectos diferentes sobre el nivel de violencia en las ciudades. En algunos casos, los grupos criminales compiten entre ellos para obtener la exclusividad de la protección y colaboración del Estado y, cuando alcanzan ese resultado, deciden limitar el uso de la violencia para mantenerla, sin llamar la atención de la ciudadanía. En otros casos fuertes de respaldo institucional, y conscientes de la impunidad que deriva, otros grupos incurren de manera más frecuente en prácticas violentas contra la población.

El contacto entre bandas criminales e instituciones puede generar relaciones clientelares, en las cuales las primeras apoyan de manera activa a candidatos durante elecciones políticas (Lessing 2008). Arias (2017) afirma que los grupos armados pueden influenciar los resultados de las elecciones de manera indirecta, gestionando la campaña electoral a escala local, o a través de injerencias mayores, como por ejemplo intimidando a los residentes de áreas carentes para que voten por un candidato, obligando a los partidos políticos a presentar a determinada persona como candidata o incluso, lanzando a uno de sus miembros como candidato.

Conclusiones

El mercado local de las drogas ilícitas no siempre se efectúa por medio de formas de control territorial, porque no todos los responsables poseen la capacidad organizativa requerida (Berg y Carranza 2018). En la Ciudad de México, en algunos casos el narcomenudeo está totalmente desvinculado del control territorial y es llevado a cabo por individuos y no por grupos criminales (Zamudio Angles 2013).

En la ciudad brasileña de Recife, las facciones no llegan a controlar más que una o dos calles en cada uno de los barrios en los que se sitúan y en estos no gestionan ningún aspecto de la vida cotidiana de la comunidad, como en cambio acontece en las favelas de Río de Janeiro (Wolff 2015). Por ello, es necesario verificar caso por caso si se puede hablar de control territorial y, en consecuencia, de territorialidad y procesos de territorialización, cuando se analiza la actividad del narcomenudeo. En otras palabras, antes de hablar de control territorial, es necesario verificar si la autoridad de los miembros del narcomenudeo en el espacio en el que se sitúan es efectiva, lo que hace que este se transforme en territorio.

Los elementos que conforman el control territorial, los cuales fueron establecidos en este artículo, podrán usarse como indicadores en futuras investigaciones que tengan el objetivo de comprender su nivel en contextos específicos. Queda pendiente elaborar un sistema de medición que tome en consideración dichos puntos y que propicie el análisis de cada caso en función de sus particularidades. Esto permitirá obtener resultados útiles para formular tipologías y modelos de control territorial por similitud y diferencia entre los distintos contextos analizados, según la ausencia, presencia e intensidad de los elementos descritos en los indicadores.

De esa manera, será posible definir si el nivel de control territorial en una localidad, por parte de los grupos del narcomenudeo, es alto, bajo o inexistente. Más específicamente, si estos grupos gozan de legitimidad interna y de qué manera la obtienen, si consiguen incidir en la vida política y asociativa local, cuán extenso es el territorio que controlan, si colaboran con la policía u otras instituciones, si cuentan con miembros armados visibles, con cuántos y

con cuáles armas, si gestionan la vida local a través de la elaboración de un código de conducta respetado por los habitantes, si imponen su autoridad sobre estos a través del uso de la violencia y si entran en conflicto con la policía y otras bandas del narcomenudeo. A partir de ello, se generarán tantas tipologías de control territorial como combinaciones haya entre sus elementos, lo que permitirá basar el análisis en las características de cada contexto, del grupo que se dedica al narcomenudeo y de las relaciones de poder que se generan en el territorio.

Bibliografía

- ACAPS. 2014. "Otras situaciones de violencia en el Triángulo del Norte Centroamericano: impacto humanitario", <http://bit.ly/2QZfB50>
- Alves, Amparo. 2016. "Blood in Reasoning: State Violence, Contested Territories and Black Criminal Agency in Urban Brazil". *Journal of Latin American Studies* 48: 61-87. doi.org/10.1017/S0022216X15000838
- Arias, Enrique Desmond. 2017. *Criminal Enterprises and Governance in Latin America and the Caribbean*. Virginia: Cambridge University Press. <https://doi.org/10.1017/9781316650073>
- Berg, Louis Alexandre, y Marlon Carranza. 2018. "Organized criminal violence and territorial control: Evidence from northern Honduras". *Journal of Peace Research* 55: 1-16. doi.org/10.1177/0022343317752796
- De Sousa Santos, Boaventura. 1988. *O discurso e o poder*. Porto Alegre: Sergio Antonio Fabris.
- Bruneau, Thomas C. 2014. "Pandillas and security in Central America". *Latin American Research Review* 49: 153-172.
- Córdova, Abby. 2017. "La incidencia de las pandillas en los barrios salvadoreños y su efecto en la legitimidad política". *América Latina Hoy* 77: 47-66.

- Cortés Vargas, Yofre Luis, Claudia Gómez Rojas, y Luis Ernesto García. 2015. *Lineamientos de política para la gestión pública contra la comercialización de estupefacientes*. Colombia: Estrategia y Decisión.
- Cortés Vargas, Yofre Luis, y Rodolfo Parra Cely. 2011. "Narcomenudeo: un neologismo para describir la venta de estupefacientes". *Criminalidad* 53: 37-71. <http://bit.ly/2XVjyta>
- Cortés Vargas, Yofre Luis, Rodolfo Parra Cely, y John Alexander Durán Martínez. 2012. *Narcomenudeo: entramado social por la institucionalización de una actividad económica criminal*. Bogotá: Dirección de Inteligencia Policial.
- Cunjama López, Emilio Daniel, y Alan García Huitrón. 2014. "Narcotráfico y territorios en conflicto en México". *Cotidiano - Revista de La Realidad Mexicana* 28: 99-111. <http://bit.ly/35IQ5F8>
- De León Beltrán, Isaac, y Juan Carlos Garzón. 2014. "Mercados urbanos de drogas y zonas de impunidad en Colombia. Los supuestos, los hechos y las respuestas detrás del narcomenudeo". *Transnationa Institute* 2: 1-16. <http://bit.ly/2XRu6t0>
- Doyle, Caroline. 2016. "Explaining Patterns of Urban Violence in Medellín, Colombia". *Laws* 5: 1-17. doi.org/10.3390/laws5010003
- Engle Merry, Sally. 1988. "Legal pluralism". *Law and Society Review* 22: 869-896.
- Gutiérrez Rivera, Lirio. 2012. "Geografías de violencia y exclusión: pandillas encarceladas en Honduras". *Latin American Research Review* 47: 167-179.
- Haesbaert, Rogério. 2011. *El mito de la desterritorialización: del "fin de los territorios" a la multiterritorialidad*. Río de Janeiro: Bertrand.
- Koonings, Kees, y Dirk Kruijt. 2004. "Armed Actors, Organized Violence and State Failure in Latin America: A Survey of Issues and Arguments". En *Armed actors. Organized violence and state failure in Latin America*, editado por Kees Koonings y Dirk Kruijt, 5-15. Nueva York: Zed Books.
- Koonings, Kees, y Sjoerd Veenstra. 2007. "Exclusión social, actores armados y violencia urbana en Río de Janeiro". *Foro Internacional* 189: 616-636.
- Lessing, Benjamin. 2008. "As facções cariocas em perspectiva comparativa". *Novos Estudos* 80 (marzo): 43-62. doi.org/10.1590/S0101-33002008000100004
- Lessing, Benjamin. 2011. "Tres mitos sobre la "guerra contra el narcotráfico"". *Perspectivas Sobre El Desarrollo: Seguridad Ciudadana y Bienestar* 9: 74-109.
- Machado da Silva, Luiz. Antonio. 2008. *Vida sob cerco: violência e rotina nas favelas do Rio de Janeiro*. Rio de Janeiro: Nova Fronteira.
- Misse, Michel. 2011. *Crime e violência no Brasil contemporâneo: estudos de sociologia do crime e da violência urbana*. Rio de Janeiro: Lumen Juris.
- Moncada, Eduardo. 2016. "Urban Violence, Political Economy, and Territorial Control: Insights from Medellín". *Latin American Research Review* 51: 225-248. doi.org/10.1353/lar.2016.0057
- Ordóñez Valverde, Jorge. 2017. "De la pandilla a la banda. Transformaciones de la violencia pandillera en barrios marginales en Cali". *Sociedad y Economía* 32: 107-126.
- Pérez Sáinz, Juan Pablo, Wendy Alas Velado, y Margarita Montoya Hernández. 2018. "Sobrevivir en la violencia. Jóvenes, vías laborales y estrategias de adaptación territorial en Soyapango, El Salvador". En *Jóvenes, exclusión laboral y violencia urbana en Centroamérica*, editado por Juan Pablo Pérez Sáinz, 81-116. San José, Costa Rica: FLACSO.
- Raffo López, Leonardo, y Diego Gómez Calderón. 2017. "Redes criminales y corrupción en la era del microtráfico y el narcomenudeo". *Revista de Economía Institucional* 19: 227-261. doi.org/10.18601/01245996.v19n37.12
- Rasmussen, Mattias Borg, y Christian Lund. 2018. "Reconfiguring Frontier Spaces: The territorialization of resource control". *World*

- Development* 101: 388-399. <https://doi.org/10.1016/j.worlddev.2017.01.018>
- Ricotta, Giuseppe. 2017. "En el territorio del enemigo: las Unidades de Policía de Pacificación (UPP) en una favela de Río de Janeiro, Brasil". *Antípoda. Revista de Antropología y Arqueología* 29: 63-79. [doi.org/https://dx.doi.org/10.7440/antipoda29.2017.03](https://doi.org/10.7440/antipoda29.2017.03)
- Rodgers, Dennis, y Adam Baird. 2016. "Entender a las pandillas de América Latina: una revisión de la literatura". *Estudios Socio-Jurídicos* 18: 13-53. doi.org/10.12804/esj18.01.2016.01
- Saborío, Sebastián. 2014. "Dalla normalizzazione al rifiuto: violenza come strumento di controllo territoriale nelle favelas pacificate". *Sociologia Del Diritto* 2: 171-196.
- Saborío, Sebastián. 2017. "Policía pacificadora, legitimidad y prácticas de ocupación territorial". *Antípoda. Revista de Antropología y Arqueología* 29: 105-122.
- Saborío, Sebastián. 2019. "Estado del arte sobre narcoviolenencia en Costa Rica". *Reflexiones* 92 (julio-diciembre): 23-38.
- Sack, Robert David. 1983. "Human Territoriality: A Theory". *Annals of the Association of American Geographers* 73 (1): 55-74.
- Sack, Robert David. 1986. *Human Territoriality: Its Theory and History*. Gran Bretaña: Cambridge University Press.
- Salas Salazar, Luis Gabriel. 2015. "Lógicas territoriales y relaciones de poder en el espacio de los actores armados: un aporte desde la geografía política al estudio de la violencia y el conflicto armado en Colombia, 1990-2012". *Cuadernos de Geografía, Revista Colombiana de Geografía* 24: 157-172.
- Savenije, Win, y Chris Van der Borgh. 2004. "Youth gangs, social exclusion and the transformation of violence in El Salvador". En *Armed actors. Organised violence and state failure in Latin America*, editado por Kees Koonings y Dirk Kruijt, 155-171. Londres/Nueva York: Zed books.
- Taniguchi, Travis, Jerry Ratcliffe y Ralph Taylor. 2011. "Gang Set Space, Drug Markets, and Crime around Drug Corners in Camden". *Journal of Research in Crime and Delinquency* 48: 327-363. doi.org/10.1177/0022427810393016
- Valenzuela Aguilera, Alfonso, y Mariana Ortega Breña. 2013. "Urban surges: power, territory, and the social control of space in Latin America". *Latin American Perspectives* 40 (marzo): 21-34. doi.org/10.1177/0094582X12466834
- Vilalta Perdomo, Carlos. J. 2009. "La geografía local del narcotráfico: patrones, procesos y recomendaciones de política urbana". *Estudios Demográficos Urbanos* 24:49-77
- Von Santos, Herard. 2016. "El Servicio Territorial como parte del sistema de control social y territorial del Estado salvadoreño durante el conflicto armado (1972-1992)". *Revista Policía y Seguridad Pública* 1: 227-294.
- Weber, Max. 2011. *La política como vocación*. Valencia: NoBooks Editorial.
- Willis, Graham Denyer. 2015. *The Killing Consensus: Police, Organized Crime, and the Regulation of Life and Death in Urban Brazil*. California: University of California Press.
- Wolff, Michael Jerome. 2015. "Policing and the Logics of Violence: A Comparative Analysis of Public Security Reform in Brazil". *Policing and Society* 27: 1-15. doi.org/10.1080/10439463.2015.1093478
- Zamudio Angles, Carlos Alberto. 2013. "Jóvenes en el narcotráfico: el caso Ciudad de México". *URVIO. Revista Latinoamericana de Seguridad Ciudadana* 13: 111-123. doi.org/10.17141/urvio.13.2013.1185

La Guardia Nacional y la militarización de la seguridad pública en México

The National Guard and the militarization of public security in Mexico

Gerardo Hernández¹ y Carlos-Alfonso Romero-Arias²

Recibido: 1 de junio de 2019

Aceptado: 13 de octubre de 2019

Publicado: 2 de diciembre de 2019

Resumen

La amenaza que representa la inseguridad pública en América Latina ha conllevado que muchos de los gobiernos asolados por ella recurran a las políticas de militarización. En el caso de México, el gobierno creó la Guardia Nacional para pacificar el país. El objetivo del artículo es responder la pregunta ¿por qué, pese a los argumentos y posturas de diferentes actores nacionales e internacionales, la Administración Federal en México (2018-2024) decidió crear una Guardia Nacional para combatir y reducir los índices de violencia? El estudio emplea un método explicativo y utiliza información del Banco Mundial, el Instituto Nacional de Estadística y Geografía (INEGI), el Fórum Brasileño de Seguridad Pública, *World Prison Brief*, el Índice de Paz Global, y el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP). La teoría de las políticas públicas en democracia permite explicar la importancia del desarrollo de esta última para comprender el diseño y los resultados de las primeras. Se toman como referencia los casos de Brasil y Colombia, países que han recurrido a estrategias de militarización (pero con resultados distintos), donde la variable ha sido el gasto militar. En ese ámbito, México está muy por debajo de los dos países aludidos.

Palabras clave: democracia; Guardia Nacional; militarización; política pública; seguridad pública

Abstract

The threat posed by public insecurity in Latin America has led many of the governments affected by this problem to resort to militarization policies. In the case of Mexico, the government created the National Guard to pacify the country. The purpose of this article is to answer the question why, despite the arguments and positions of different national and international actors, the Federal Administration in Mexico (2018-2024) decided to create a National Guard to combat and reduce the rates of violence? The study uses an explanatory method and bases on information from the World Bank, the National Institute of Statistics and Geography (INEGI), the Brazilian Public Security Forum, the World Prison Brief, the Global Peace Index, and

1 Instituto de Investigaciones Sociales, Universidad Autónoma de Baja California, México, gherandez48@uabc.edu.mx,  orcid.org/0000-0003-2803-6905

2 Universidad Autónoma de Baja California, México, carlos.romero.arias@uabc.edu.mx, orcid.  org/0000-0002-2292-3143



the Executive Secretariat of the National Public Security System (SESNP). The theory of public policies in democracy allows to explain the importance of the development of the latter to understand the design and results of the former. The cases of Brazil and Colombia, countries that have resorted to militarization strategies (but with different results), where the variable has been military spending, are taken as reference. In that area, Mexico is well below the two countries mentioned.

Key words: democracy; militarization; National Guard; public policy; public security

Introducción

El incremento de la violencia e inseguridad en los países de América Latina es uno de los grandes problemas que enfrentan los gobiernos de la región, no solo por el nivel cualitativo de violencia al que recurren los agentes criminales, sino también por la disputa abierta de estos hacia el control territorial e institucional de los Estados. En 2012, la tasa de homicidios en América Latina (21,5 por cada 100 000 habitantes) rebasaba la tasa global (siete por cada 100 000). En 2017, 17 de los 20 países con mayor tasa de homicidios en el mundo fueron latinoamericanos (Muggah y Aguirre 2018, 3-4). Lo anterior ha tenido necesariamente un impacto negativo para el desarrollo de la región. En 2014, el costo del crimen fue de 3,5% del PIB (Jaitman et al 2017, 21-32). Dentro de ese panorama destacan Honduras, El Salvador, Guatemala, Colombia, Brasil y México.

Asimismo, el grado de urgencia del incremento de los índices de criminalidad en la región ha generado que, en las agendas públicas de los gobiernos, las estrategias de seguridad estén cada vez inclinadas a implementar medidas extraordinarias como el uso de la

fuerza militar. En el caso de México, el contexto de inseguridad vivido durante las dos recientes administraciones federales (2006-2012 y 2012-2018) ha tenido como resultado el incremento generalizado de la violencia e inseguridad. En 12 años se registraron 212 016 homicidios dolosos, en gran medida por el enfrentamiento del Estado contra las organizaciones del crimen organizado (SESNP 2019). Lo anterior ha llevado a señalar que las políticas de seguridad implementadas han fallado en conseguir sus objetivos de pacificar al país. Por tal motivo, con su arribo a la presidencia de la República del Ejecutivo Federal (2018-2024), Andrés Manuel López Obrador se planteó dar un viraje a las estrategias de inseguridad, mediante la creación de una Guardia Nacional. De manera específica: “La nueva corporación será el instrumento primordial del Ejecutivo Federal en la prevención del delito, la preservación de la seguridad pública, la recuperación de la paz y el combate a la delincuencia en todo el país” (PND 2019, 24).

La medida fue rechazada desde el inicio por la Comisión Nacional de los Derechos Humanos (CNDH), la Organización de las Naciones Unidas (ONU) y más de 500 organizaciones de la sociedad civil. Dentro de los argumentos que se plantearon estuvo que la Guardia Nacional es una falsa salida a la crisis de inseguridad por la que atraviesa el país, y que se contradecía con la propuesta de campaña de desmilitarizar al país. En ese mismo sentido, los opositores propusieron construir una Policía Nacional, mejorar a las corporaciones policíacas del país y fortalecer al Sistema Nacional de Seguridad Pública (Roldán 2018). No obstante, el gobierno federal mantuvo la postura de crear una Guardia Nacional.

Considerando lo anterior, el presente estudio busca responder ¿por qué, pese a los ar-

gumentos y posturas de diferentes actores nacionales e internacionales, la Administración Federal en México (2018-2024) decidió crear una Guardia Nacional para combatir y reducir los índices de violencia? Como hipótesis se plantea que, para el Gobierno Federal, la Guardia Nacional es el último recurso en materia de seguridad pública del Estado, para centralizar y recuperar el control territorial en zonas capturadas por el crimen organizado, ante la insatisfacción con las políticas de seguridad de las dos pasadas administraciones. Esto refleja al menos dos problemas institucionales. El primero: no se fortalece la coordinación entre órdenes de gobierno, así como tampoco el desarrollo y consolidación de las policías estatales y municipales. El segundo: se evidencian los retrocesos y claroscuros de la democracia en México para brindar un adecuado estado de derecho, lo cual ha ocasionado la legitimación social de medidas extraordinarias.

El artículo tiene una estructura deductiva y se divide en cuatro apartados. En el primero, a partir de una discusión teórica sobre las políticas públicas en democracia, se explica la importancia de considerar el desarrollo de esta última para comprender el diseño y los resultados de las primeras. Esto quiere decir que, cuando existe desfase con la democracia, y ante problemas extraordinarios como la inseguridad y la violencia, se proponen estrategias de alto impacto sin considerar las consecuencias a largo plazo. En el segundo apartado se analizan los casos de Brasil, Colombia, y México, para explicar que las políticas de seguridad enfocadas en el uso de la fuerza se deben a la desafección con los resultados de la democracia. En el tercer apartado se estudia la conformación de la Guardia Nacional en México. Se hace un análisis normativo de la política y se exponen las facultades otorgadas al presidente

para hacer uso discrecional de la Guardia Nacional en todo el país. Además, se explica por qué se decidió centralizar la política de seguridad, en lugar de apostar por la corresponsabilidad entre órdenes de gobierno. En la última sección se presentan las conclusiones.

El estudio emplea un método explicativo y utiliza información del Banco Mundial, del Instituto Nacional de Estadística y Geografía (INEGI), del Fórum Brasileño de Seguridad Pública, del *World Prison Brief*, del Índice de Paz Global, y del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP).

La democracia como variable para entender el diseño y resultados de las políticas públicas

En sus aportes teóricos de las políticas públicas, Parsons plantea que estas no solo tienen lugar en los sistemas políticos nacionales, sino también en un sistema mundial. Por ejemplo, la influencia y el poder que llegan a ejercer las corporaciones transnacionales representan una restricción adicional para los formuladores de las políticas nacionales. Traen como consecuencia que el contexto en el que se instrumentan las políticas tenga las siguientes características: complejidad y diversidad; intenso patrón de interacción; permeabilidad del Estado-nación; cambios rápidos y en cascada y fragilidad del orden y la gobernanza (Parsons 2007, 263-265). La complejidad del contexto y la cantidad de agentes que intervienen en la implementación de políticas ha ocasionado que el Estado, como referente de poder político, vea minimizada su soberanía (Attili 2004, 189).

Por su parte, Beck (1997), Sassen (2007) y Barceló (2007) mencionan que ese contex-

to se debe a la globalización de los Estados-nación, caracterizada principalmente por los flujos financieros, de los bienes y servicios, sin importar las fronteras entre Estados. Si el Estado-nacional basa su poder y jerarquía en el control territorial, con la globalización ha tenido que compartir el poder con actores que tienen alcance transnacional. Por ejemplo, asociaciones internacionales, empresas, grupos financieros y organizaciones criminales, las cuales terminan actuando de mutuo acuerdo con el Estado o como poderes paralelos a este. El poder de esos nuevos actores por lo general ha determinado la agenda política de los Estados.

La complejidad aludida anteriormente se ha incrementado en el transcurso de la historia reciente, a medida que los gobiernos democráticos-liberales empezaron a requerir información para solucionar problemas públicos (Parsons 2007, 54). En este punto es pertinente señalar que no puede verse la creación e implementación de las políticas públicas por separado del contexto democrático o del tipo o calidad de la democracia del Estado donde se buscan resolver los problemas. En otras palabras, la democracia es un criterio fundamental para entender por qué se crea cierto tipo de políticas públicas y su resultado. Sobre la misma tesis, Ingram, De León y Schneider (2016, 175-196) exponen que la democracia es esencial para la gobernanza y la resolución de problemas en muchos países, pero advierten que los expertos en políticas públicas no la han considerado una variable determinante. El argumento de los autores se basa en la crítica al proceso democrático de varios países, en el cual se asume que tener un sistema bipartidista (o pluralista) competitivo, con sufragio universal y separación de poderes producirá automáticamente políticas públicas que sirvan a la democracia.

Si se partiera de lo anterior, ¿cómo explicar el hecho de que las políticas públicas generalmente no logran resolver las demandas en sociedades democráticas? Las políticas públicas son el conjunto de actividades de las instituciones de gobierno, actuando directamente o a través de agentes, dirigido a tener una influencia determinada sobre la vida de los ciudadanos. Esto significa que la participación ciudadana es importante en ese proceso, debido a que estas surgen por una demanda de la sociedad o la anticipación de las autoridades gubernamentales que, junto al gobierno, deben definir los instrumentos y las acciones de la implementación (Pérez 2005, 52; Franco 2013, 86-87; Pasquino 2011, 270). No obstante, Ingram, De León y Schneider (2016, 176-177) apuntan que los fundamentos teóricos de las políticas públicas no se están logrando en las democracias, incluso en las naciones industrializadas occidentales como Estados Unidos, donde se supone que la democracia está más profundamente arraigada.

En ese mismo sentido, y siguiendo la interrogante del párrafo anterior, la satisfacción o no con las políticas llevadas a cabo en la democracia también tiene sus consecuencias en el colectivo social. De acuerdo con lo que señala Connolly (1991, 199), cuando los resultados de las acciones de gobierno son evidentes en la sociedad, las relaciones entre la identidad personal y colectiva en una democracia proporcionan una base de ese vínculo honorable de identificación entre el individuo y el Estado. Esto quiere decir que, cuando las circunstancias son favorables, la relación del individuo con el Estado es de patriotismo, pero cuando son desfavorables, degenera en desafección con el Estado o con un nacionalismo en el que las tribulaciones de la época se atribuyen a un mal que debe ser neutralizado.

Peters (2010, 4) y Weimer y Vining (1992, 187) señalan que la complejidad que se presenta en la democracia se debe a que el gobierno central tiene que delegar autoridad a diversos actores sociales –incluidos gobiernos subnacionales, burocracia y agencias reguladoras– y redes que intervienen en las políticas públicas. No obstante, cuando los objetivos de estas se desvían, el Estado debería tener la jerarquía para retomar el control y la centralización de su implementación. Sin embargo, los autores advierten que, en los sistemas federales, el proceso de mantener la jerarquía del Estado se complejiza debido a que los gobiernos subnacionales apelan a la autonomía. En otras palabras, la descentralización del poder político que se ha presentado con la democracia ha tenido como consecuencia obstaculizar la aplicación de las políticas. Si bien la descentralización es deseable, no es una característica esencial estructural del gobierno, debido a que a veces limita la eficacia de las políticas públicas.

Asimismo, el Estado ya no emerge como un consumado agente de eficacia, aunque sigue siendo el centro oficial de la acción colectiva y la institución de último y de mayor recurso. Se ha abierto una grieta en la unidad misma del poder del Estado y, ante la complejidad aludida, los obstáculos para su eficacia se multiplican. De ahí que el Estado, cada vez más, sostenga su legitimidad e identidad a través de demostraciones teatrales de castigo y de la venganza contra aquellos elementos que amenazan con arrebatarse el control institucional y territorial. Por tal motivo es que se lanzan dramáticas cruzadas contra delincuentes de bajo nivel –o el crimen organizado–, enemigos extranjeros y terroristas (Connolly 1991, 198-222). En la actualidad, esos enemigos y amenazas se encuentran en las zonas ur-

banas, representados por la violencia homicida, las pandillas y el crimen organizado. Así se da paso a la demostración del Estado de usar la fuerza para evidenciar que tiene respuestas a la demanda social de seguridad y estado de derecho.

No obstante, ese panorama generalmente muestra contradicciones, debido a las posturas que están a favor o en contra del uso de políticas de mano dura contra la violencia y la delincuencia. En el caso de la Guardia Nacional de México, por un lado se encuentran quienes señalan que el Estado está

en una situación de emergencia, de violencia y se necesitan respuestas proporcionales por parte del Estado mexicano (...) Militarizar significa llevar las prácticas de los cuarteles a la vida cotidiana de la sociedad (...) Las policías en las democracias son organizaciones paramilitares, tienen uniforme, jerarquías, axiologías, armamento, cuarteles, doctrinas... así funcionan (Melgoza 2019).

Por otro lado están quienes plantean que una fuerza policial de corte militar o la presencia del ejército en las calles, a cargo de las funciones de seguridad pública, atentan contra los derechos humanos (Nerio 2011, 19).

Lo que no se puede dejar de lado es lo que Jaitman et al (2017, 2-10) consideran costos indirectos o intangibles del crimen y de la violencia, debido a que afectan directamente a grupos de población más vulnerable, exacerbando sus condiciones de pobreza y marginación social. Es necesaria una respuesta del Estado ante el peligro que representa el incremento de la violencia en sus diferentes manifestaciones. En ese mismo sentido, Abt. Thomas (2019) y Kleiman (2005) señalan que, ante escenarios de violencia, es necesario atacarla de manera directa. El

primero argumenta que se requiere disuasión focalizada, dirigida a grupos, mayor presencia policial en puntos estratégicos para enviar el mensaje de que el Estado posee el control territorial y, a partir de ahí, hacer partícipe a la sociedad. El segundo sostiene que mantener un alto nivel de castigo sobre ciertos delitos dentro de áreas de concentración tenderá a reducir su tasa, y dará la oportunidad de mover la estrategia a otros sitios.

Empero, desde la perspectiva teórica, la instrumentación y el éxito de una política pública también reflejan el grado de control que tiene un gobernante en el aparato estatal y en la sociedad. Para esto se debe determinar un grado de intensidad del control de los recursos externos e internos, y debe existir la coerción para hacer llegar sus políticas públicas en el aparato gubernamental y de ahí que se traspasen a la sociedad. Hay diferencias entre los procesos estructurales de las políticas públicas sólidas y regidas con formalidad y las débiles, regidas por la informalidad. Las diferencias son: el control territorial y la institucionalización del orden de cada estructura. El primero se refiere a los mecanismos por medio de los cuales el Estado resguarda la nación y al territorio. La segunda se entiende como el proceso mediante el cual los principios y valores que dan fundamento a las instituciones son conocidos, aceptados y practicados regularmente, al menos por aquellos a quienes esas mismas pautas definen como participantes o no del proceso. Ambos fundamentos del orden adquieren mayor relevancia cuando se está ante problemas de estabilidad o inestabilidad del Estado, como la violencia e inseguridad generada por el crimen organizado (Medellín 2004, 8-21). Este contexto ayuda a comprender por qué el desarrollo de la democracia en un país es fundamental para comprender

el diseño y los resultados de las políticas públicas. Sobre todo, cuando las circunstancias para los individuos no son favorables y existe un desafecto con el Estado y la democracia misma, como sistema de gobierno.

La militarización de la seguridad pública en las democracias de América Latina

De acuerdo con Latinobarómetro (2018, 3-4) en 2018 el apoyo a la democracia en la región fue de 48 %. Esto tiene que ver con lo limitado del progreso con las políticas públicas. Con excepción de Bolivia, Chile y República Dominicana, en los otros países la percepción de progreso es menos de un tercio de la población. Cabe señalar que hay países como Venezuela (6 %), Brasil (6 %) y El Salvador (9 %) donde la percepción no alcanza el 10 %.

Como consecuencia, el saldo de la trayectoria democrática en el colectivo social ha sido el incremento de la desconfianza, no solo por lo intangible de los avances, sino por lo costoso que ha resultado vivir en democracia. Tan solo en México el proceso electoral federal de 2018 tuvo un presupuesto de 28 000 022,5 millones de pesos (Integralia 2018). De ahí que solo el 16 % de los mexicanos crea en la democracia (Latinobarómetro 2018, 35). La falta de confianza y de resultados ha ocasionado que a los ciudadanos no les importe el tipo de régimen político que les resuelva sus demandas. Por ejemplo, en México—detrás de El Salvador, Honduras y Brasil— a los ciudadanos les da igual tener un régimen democrático o no democrático que les resuelva los principales problemas que afligen al país: la delincuencia, la corrupción y la compleja situación política (Latinobarómetro 2018, 7; ENSU 2018).

Las diferentes plataformas políticas que se han presentado en la región buscan rescatar, fortalecer y proteger la democracia, teniendo presente que, ante el descontento ciudadano y la necesidad de respuestas a las demandas, se requieren resultados a corto plazo y con una efectividad tangible. En México, el presidente Andrés Manuel López Obrador declaró al tomar el cargo: “El nuevo proyecto de nación buscará una auténtica democracia y no una dictadura abierta ni encubierta. Los cambios serán profundos pero con apego al orden legal” (Nájar 2018). En Brasil, al jurar el cargo, el presidente (2019-2023) Jair Bolsonaro pronunció: “Trabajaré incansablemente para que Brasil alcance su destino (...) mi promesa es fortalecer la democracia de Brasil” (Reuters 2019). En el caso de Colombia, con el arribo del presidente Iván Duque (2018-2022), uno de sus objetivos fue combatir el narcotráfico, fortalecer la seguridad y proteger la democracia (Redacción 2018; Galindo 2018).

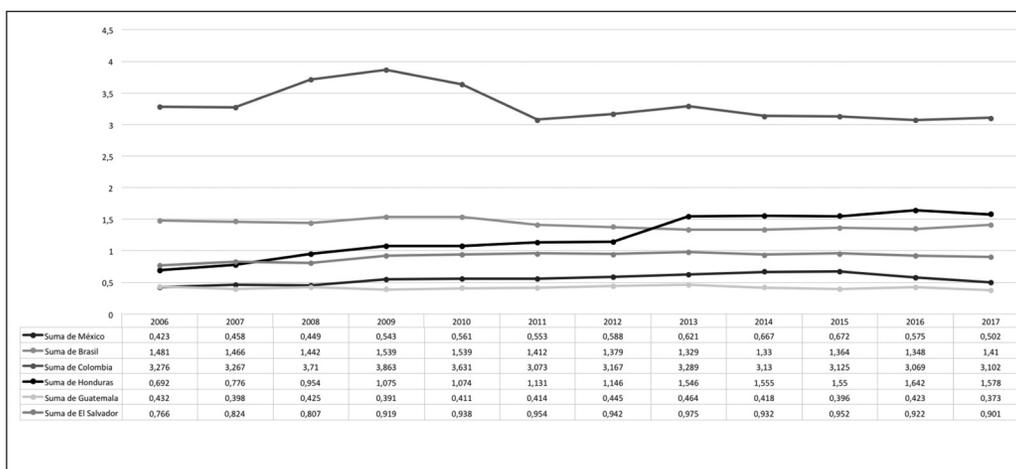
De lo anterior se desprenden dos puntos. El primero es la aceptación tácita de que existe una desafección del colectivo social con la democracia, debido a que esta no ha logrado otorgar políticas públicas que brinden progreso, pleno empleo, reduzcan la desigualdad social y sobre todo, brinden seguridad pública. Ese complejo panorama, en el cual los gobiernos centrales tienen que hacer frente a diferentes agentes criminales que no buscan apropiarse del Estado, pero sí hacer rentable las fragilidades institucionales y territoriales, es lo que ha generado en gran medida una atomización de la inseguridad. La cuantificación de la crisis se corrobora con el informe del Índice de Paz Global 2018, el cual expone que, de los 163 países y territorios independientes evaluados, los de la región de América del Sur registraron el mayor deterioro, principalmente

Brasil (lugar 106), México (lugar 140), Venezuela (lugar 143) y Colombia (lugar 145). Asimismo, en la región de Centroamérica destacan Guatemala (lugar 111) y El Salvador (lugar 116) (GPI 2018, 5-19).

El segundo punto se refiere a que, ante la demanda de respuestas y soluciones a la violencia, la inseguridad y el crimen organizado, el uso de la fuerza militar ha sido la salida de políticas públicas para los gobiernos de la región. En el caso brasileño, en 2003, cuando iniciaron los gobiernos de la izquierda encabezada por Luiz Inácio Lula Da Silva (período 2003-2011) los homicidios intencionales comenzaron una tendencia a la baja de 25,6 por cada 100 000 habitantes durante sus dos mandatos presidenciales. No obstante, cuando el modelo político empezó a mostrar signos de desgaste (sobre todo por las acusaciones probadas de corrupción), con el inicio del mandato de Dilma Rousseff (2011-2016) las cifras de homicidios se empezaron a incrementar hasta llegar a 29,5 por cada 100 000 habitantes en el año 2016 (Banco Mundial 2019). En 2018 se registraron 63 895 muertes violentas, es decir, 175 muertos por día, con una tasa de 30,8 muertos por cada 100 000 habitantes (Fórum Brasileño de Seguridad Pública 2018, 10-89).

Ante esa situación, el presidente (2016-2018) Michel Temer decretó que el ejército se hiciera cargo de la seguridad en el país: “El crimen organizado casi ha tomado control del estado de Río de Janeiro. Es una metástasis que se esparce por el país (...) juntas, la policía y las fuerzas armadas combatirán y confrontarán a aquellos que tienen secuestradas a nuestras ciudades” (Londoño y Darlington 2018). Esas medidas se radicalizaron con la victoria de Jair Bolsonaro (presidente para el período 2019-2023), quien declaró –considerando el respaldo ciudadano a la intervención

Gráfico 1. Gasto Militar (% del PIB) en México, Colombia, Brasil, Honduras, Guatemala y El Salvador: 2006-2017



Fuente: Elaboración propia con datos del Banco Mundial y el Instituto Internacional de Investigación para la Paz de Estocolmo (SIPRI 2019).

militar— un combate frontal a los criminales y las pandillas (Londoño y Andreoni 2018).

En Colombia se registraron en 1996 71,7 homicidios por cada 100 000 habitantes. La tendencia ha venido a la baja y en 2017 se registraron 24 muertes violentas por cada 100 000 habitantes (Banco Mundial 2019; Colpena 2018). Los resultados han tenido como punto de partida una política de confrontación del Estado hacia el crimen organizado y grupos paramilitares, apoyados en su momento por el Plan Colombia, durante el mandato del presidente Álvaro Uribe (2002-2010). No obstante, durante la presidencia de Juan Manuel Santos (2010-2018) se buscó un proceso de paz entre el Estado y grupos paramilitares (Alonso y Robbins 2019). Ese equilibrio se vio alterado con la llegada de Iván Duque a la presidencia del país, debido a que el nuevo mandatario declaró que no se negociarían ceses bilaterales al fuego y que las fuerzas de seguridad buscarían desarticular los Grupos Armados Organizados (GAO) —Ejército de Liberación Nacional y exparamilitares—. La

nueva política de seguridad se lograría recuperando el control institucional del territorio, lo cual inicialmente se conseguiría con la intervención de fuerzas militares y policía nacional (PDS 2018, 37).

De lo expuesto, es importante destacar los riesgos de apostar por lo rentable, lo cual ha resultado electoralmente en la retórica del uso de la militarización para pacificar sociedades asoladas por la delincuencia y el crimen organizado. Para algunos gobiernos como los mencionados es una estrategia deseable recurrir a la fuerza militar para contener la inseguridad en un primer momento —máxime si los cuerpos policiales están rebasados en sus capacidades operativas e institucionales. Sin embargo, también es cierto que ese tipo de políticas requiere mantener un presupuesto constante para lograr los objetivos de contener y controlar la violencia e inseguridad (gráfico 1).

Como se explicó en el caso de Colombia, para que los índices de homicidios intencionales descendieran a su nivel más bajo en las dos recientes décadas, el gasto militar con res-

pecto al PIB ha sido fundamental. En esto se diferencian los otros Estados representados en el gráfico 1, que no han podido salir del espiral de violencia.

El caso colombiano no puede considerarse del todo exitoso debido a que, con el cese de las negociaciones de paz entre grupos guerrilleros y el gobierno de Iván Duque, los primeros han buscado reagruparse. A ellos se suma la violencia creciente en la frontera con Venezuela. Sin embargo, el gasto para el uso de la fuerza militar es una constante en el país para mantener los niveles de estabilidad (Dalby y Carranza 2019).

En contraparte, los Estados que han apostado por la militarización de la seguridad pública, pero sin tener una inversión proporcional en gasto militar a la retórica política utilizada, se encuentran inmersos en un espiral de violencia que no solo se evidencia en los homicidios por cada 100 000 habitantes –El Salvador (51); Honduras (40) y Guatemala (23)– sino también en las violaciones a los derechos humanos y el colapso de su sistema penitenciario.³ En el caso de Brasil, con las políticas de militarización de la seguridad, la población carcelaria se ha incrementado de manera considerable, al pasar de 232 000 personas en 2000 a 726 000 en 2018 (ICPR 2019).

3 La violencia en estos tres países está relacionada con el tráfico de drogas, el crimen organizado y las pandillas. En el último caso, los gobiernos de El Salvador, Honduras y Guatemala consideran la existencia y la expansión de las maras como un serio problema de seguridad nacional. En 2003 en Honduras se promulgó una legislación “antimarera”, que facilita la formación de comandos especiales de fuerzas policíacas y militares (Operación Libertad). En 2013 las autoridades crearon la Policía Militar de Orden Público (PMOP), con la finalidad de contar con una unidad especializada en el combate frontal al crimen organizado y crimen común (DOFRH 2013, 2-6). Un plan similar se instrumentó ese mismo año en El Salvador, denominado “Plan Mano Dura”; en 2005 se modificó y se renombró “Plan Mano Súper Dura” (Alba Vega y Kruijt 2007, 492).

Los resultados en México, Brasil y Colombia muestran que, ante el panorama de violencia, inseguridad y crimen organizado, los ejecutivos federales han buscado robustecer el gobierno central dentro de sus límites territoriales, debido a que existe una complejidad muy marcada al momento de atender la violencia, la inseguridad y el crimen organizado, como se señala en el apartado teórico. Dado lo costoso y lento de la construcción y consolidación de instituciones, la doctrina militar, o en su caso la militarización de la seguridad pública, es una salida rápida en los gobiernos de la región. En el siguiente apartado se explica el caso de México y la creación de la Guardia Nacional.

La Guardia Nacional y la centralización de la seguridad pública en México

Los temas que ocuparon la agenda política durante la campaña electoral 2017-2018 fueron la inseguridad, la violencia generalizada y la poca satisfacción con la democracia en México, en específico, con el funcionamiento de las instituciones policíacas, sindicatos, senadores, presidencia, diputados y partidos políticos (Consulta Mitofsky 2018). En ese contexto de fragilidad institucional y de cuestionamiento al poder de coerción del Estado, instituciones como el ejército son las que fueron mejor evaluadas y que poseen mayor confianza por parte de la ciudadanía. Por tal motivo, una vez en el poder político presidencial, los agentes responsables de llevar a cabo la nueva estrategia de seguridad plantearon que la Guardia Nacional sería la manera en la que se pacificaría el país. Sobre todo, y de acuerdo con el *Plan Nacional de Paz y Seguri-*

dad 2018-2024 (2018, 13-15), por la crisis de inseguridad delictiva en el país y las ineficacias que han presentado las instituciones en materia de seguridad pública. Lo anterior pareció corroborarse con lo señalado por la secretaria de Gobernación, Olga Sánchez Cordero:

Se platicó mucho, se trabajaron muchas horas, el presidente electo caminó la República varias veces y en todos lados le dijeron: no nos retire a los militares porque es nuestra seguridad personal... ¿entonces cuál fue la institución que pensamos que no daría la imagen de militarización?, una Guardia Nacional, porque ahí van a estar no los militares, porque los militares van a ser para la soberanía nacional, ahí va a estar la policía que ya trae otra formación, la policía militar, policía naval, policía federal y todo esto va a ser un conjunto de Guardia Nacional, o se el término es policía, no es soldados... Hay veces en que hay que decidir entre dos situaciones, no necesariamente las mejores pero fue lo mejor que encontramos y fue de consenso (Senado de la República 2018).

Lo declarado por la secretaria de Gobernación tuvo como respaldo la crisis de seguridad que se presentó a finales de la administración federal 2012-2018 e inicios del gobierno encabezado por Andrés Manuel López Obrador. De acuerdo con el registro oficial, del 1 de diciembre de 2018 al 31 de marzo de 2019 se contabilizaron 9686 homicidios dolosos, una diferencia de 2786 homicidios dolosos más comparando con el mismo periodo de la administración federal antecesora (SESNSP 2019). De ahí que la estrategia de crear una Guardia Nacional tuviera como objetivo salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como para contribuir a la generación y preservación del orden público y la paz social. Asimismo, sería

fundamental la coordinación y colaboración con las entidades federativas y municipios (DOF 2019).

No obstante, y sumado a la postura en contra de las organizaciones de la sociedad civil en México, la Oficina en Washington para Asuntos Latinoamericanos (WOLA) y Amnistía Internacional plantearon los riesgos de llevar la estrategia de seguridad de México a través de las Fuerzas Armadas. Señalaron que la Guardia Nacional es la misma estrategia de las administraciones antecesoras, además del riesgo que representa para la protección de los derechos humanos. En ese mismo sentido, se señaló que profundiza la militarización y propicia una débil rendición de cuentas, además de no existir certeza de que resuelva los problemas de violencia, inseguridad e impunidad (Amnistía Internacional 2018, 3-7; WOLA 2019). Aun con esto, la reforma a la Constitución en materia de Guardia Nacional modificó 10 artículos. El 21 dio origen a la Guardia Nacional (tabla 1).

Puede observarse una ambigüedad en la creación de la Guardia Nacional, tanto por el carácter civil que se le buscó imprimir como por el papel secundario del fortalecimiento de los cuerpos policiacos en el país y la coordinación entre órdenes de gobierno. Sin embargo, es en los artículos transitorios donde se observa la centralización de toma de decisiones desde el poder ejecutivo federal (tabla 2).⁴

Es importante señalar que, al aprobar la creación de la Guardia Nacional, también fue necesario dar origen a cuatro leyes secundarias: la Ley Orgánica de la Guardia Nacional, la Ley Nacional sobre Uso de la Fuerza, la

⁴ El 11 de abril de 2019, el presidente Andrés López Obrador nombró comandante de la Guardia Nacional al general de brigada de estado mayor Luis Rodríguez Bucio, quien se encuentra en proceso de retiro.

Tabla 1. Reforma al artículo 21, que dio origen a la Guardia Nacional en México

Artículo	Texto acordado por los grupos parlamentarios el 20 de febrero de 2019
Artículo 21	<p>Las instituciones de seguridad pública, incluyendo la Guardia Nacional, serán de carácter civil, disciplinado y profesional.</p> <p>La Federación contará con una institución policial de carácter civil denominada Guardia Nacional, cuyos fines son los señalados en el párrafo noveno de este artículo, la coordinación y colaboración con las entidades federativas y municipios, así como la salvaguarda de los bienes y recursos de la Nación.</p> <p>El Ministerio Público y las instituciones policiales de los tres órdenes de gobierno (...) conformarán el Sistema Nacional de Seguridad Pública, que estará sujeto a las siguientes bases mínimas:</p> <p>b) El establecimiento de un sistema nacional de información en seguridad pública a cargo de la Federación al que ésta, las entidades federativas y los municipios, a través de las dependencias responsables de la seguridad pública, proporcionarán la información de que dispongan en la materia, conforme a la ley (...) Ninguna persona podrá ingresar a las instituciones de seguridad pública si no ha sido debidamente certificada y registrada en el sistema.</p> <p>La ley determinará la estructura orgánica y de dirección de la Guardia Nacional, que estará adscrita a la secretaría del ramo de seguridad Pública, que formulará la Estrategia Nacional de Seguridad Pública, los respectivos programas, políticas y acciones.</p>

Fuente: elaboración propia con datos del decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de Guardia Nacional (2019).

Ley Nacional del Registro de Detenciones, y la reforma a la Ley General del Sistema Nacional de Seguridad Pública (aprobadas el 21 de mayo de 2019). No obstante, la violencia generalizada en el país, en especial la generada por el robo de combustible, ocasionó la primera coyuntura de la agenda de seguridad del Gobierno Federal. Lo anterior, debido a que en el periodo 2016-2018 las pérdidas económicas por este delito ascendieron a 147 000 millones de pesos (Presidencia de la República 2018). Ante ello, el 21 de diciembre de 2018, el Gobierno Federal dispuso de las Fuerzas Armadas para contener el robo de hidrocarburos. Eso dio como resultado que se pasara de 81 000 barriles en promedio robados durante el mes de noviembre de 2018 a 4000 barriles

diarios robados al finalizar el mes de abril de 2019 (Gobierno de México 2019).

En la misma tesitura –y después del asesinato de un grupo de personas en Minatitlán, Veracruz– el 26 de abril de 2019, la Guardia Nacional empezó sus operaciones en los municipios de Aguadulce, Las Choapas, Coatzacoalcos y Moloacán, en el estado de Veracruz (Miranda 2019). El inicio de operaciones sin tener las leyes secundarias antes señaladas se llevó a cabo con base en el artículo segundo transitorio, el cual señala que en el periodo en el cual no estuvieran aprobadas las leyes reglamentarias, la Guardia Nacional asumiría los objetivos, atribuciones y obligaciones previstas en los artículos 2 y 8 de la Ley de la Policía Federal.

Tabla 2. Principales artículos transitorios en materia de Guardia Nacional

Segundo	<p>La Guardia Nacional se constituirá a la entrada en vigor del presente Decreto con los elementos de la Policía Federal, la Policía Naval que determine en acuerdos de carácter general el Presidente de la República.</p> <p>En tanto se expide la ley respectiva, la Guardia Nacional asumirá los objetivos, atribuciones y obligaciones previstas en los artículos 2 y 8 de la Ley de la Policía Federal (...)</p> <p>El Ejecutivo Federal dispondrá lo necesario para la incorporación de los elementos de los policías Militar y Naval a la Guardia Nacional y designará al titular del órgano de mando superior y a los integrantes de la instancia de coordinación operativa interinstitucional formada por representantes de las secretarías del ramo de Seguridad de la Defensa Nacional y de Marina.</p>
Quinto	<p>Durante los cinco años siguientes a la entrada en vigor del presente Decreto, en tanto la Guardia Nacional desarrolla su estructura, capacidades e implantación territorial, el Presidente de la República podrá disponer de la Fuerza Armada permanente en tareas de seguridad pública de manera extraordinaria, regulada, fiscalizada, subordinada y complementaria.</p>
Séptimo	<p>Los Ejecutivos de las entidades federativas presentarán ante el Consejo Nacional de Seguridad Pública, en un plazo que no podrá exceder de 180 días a partir de la entrada en vigor del presente Decreto, el diagnóstico y el programa para el fortalecimiento del estado de fuerza y las capacidades institucionales de sus respectivos cuerpos policiales estatales y municipales.</p> <p>Un año después de haberse emitido el programa referido, el Ejecutivo local enviará anualmente a la Legislatura de la entidad federativa correspondiente y al Consejo Nacional de Seguridad Pública, la evaluación integral del mismo con el informe sobre los avances en los objetivos señalados y su cumplimiento en un horizonte de seis años. Los resultados de la evaluación serán considerados para el ajuste del programa y su calendario de ejecución, por los órganos correspondientes.</p>

Fuente: elaboración propia con datos del decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de Guardia Nacional (2019).

No obstante, los artículos transitorios también reflejan la centralización y las facultades extraordinarias que tiene el presidente de la República sobre la Guardia Nacional y la política de seguridad pública del país. Esto debido a que podrá disponer de las Fuerzas Armadas de manera extraordinaria para preservar la seguridad pública en el territorio nacional. Cabe señalar que estas facultades van más allá de la coordinación y cooperación con los gobiernos subnacionales, la cual parece dejarse en segundo plano, al dar prioridad a las Fuerzas

Armadas a través de la Guardia Nacional. Esto se aprecia en la disminución del presupuesto en funciones de seguridad pública de 2019, comparado con el año anterior (tabla 3).

Todos los rubros en materia de seguridad redujeron su presupuesto y, en contraparte, la defensa nacional fue el único ramo presupuestario que tuvo una variación positiva. Los cambios presupuestales en el ramo de gobernanación (tabla 4) tuvieron dos consecuencias. La primera fue que se dejaron de integrar el Programa Nacional de Prevención del Delito.

Tabla 3. Gasto programable en las funciones de seguridad pública (2018-2019)
(millones de pesos corrientes y porcentajes)

Concepto/ramo presupuestario	PEF-2018		PEF-2019		
	Monto	Distribución%	Monto	Distribución%	Variación Porcentual real
Gasto programable neto en las funciones de seguridad pública	159 075,50	100	144 809,70	100	-12,4
Justicia	113 328,60	71,2	103 135,20	71,2	-12,4
Gobernación	18 444,70	11,6	17 955,00	12,4	-6,3
Defensa nacional	851,50	0,5	893,20	0,6	1
Asuntos de orden público y de seguridad interior	45 746,90	28,8	41 674,50	28,8	-12,3
Gobernación	35 345,80	22,2	32 464,50	22,4	-11,6
Defensa nacional	0	0	2000	1,4	n.a
Provisiones salariales y económicas	3401,10	2,1	0,00	0	-100
Aportaciones federales para entidades federativas y municipios	7000,00	4,4	7210,00	5	-0,8

Fuente: elaboración propia con datos de Senado de la República (2019).

La segunda, que se redujeran las asignaciones presupuestales a programas como subsidios en materia de seguridad pública (-22,8), administración del Sistema Federal Penitenciario (-7), así como a la implementación de las políticas, programas y acciones tendientes a garantizar la seguridad pública de la nación y sus habitantes (-23,6%) y la coordinación con las instancias que integran el Sistema Nacional de Seguridad Pública (-24,1%) (Senado de la República 2019). Este último es el más significativo políticamente debido a que es donde se sientan las bases de coordinación y competencias en materia de seguridad pública entre Federación, estados y municipios.

Si bien lo expuesto refleja la prioridad del Ejecutivo Federal de centralizar todas las funciones en materia de seguridad, otro

de los puntos a analizar es la concentración de poder político en ese ámbito, así como la formalización del uso de las Fuerzas Armadas para pacificar el país. La complejidad de implementar políticas públicas en democracia permite una explicación. Delegar responsabilidades en la toma de decisiones a otros agentes no necesariamente hace más eficiente la implementación de una política pública, sobre todo cuando se tienen problemas de fragilidad institucional y de pérdida de control territorial ante problemas como el crimen organizado.

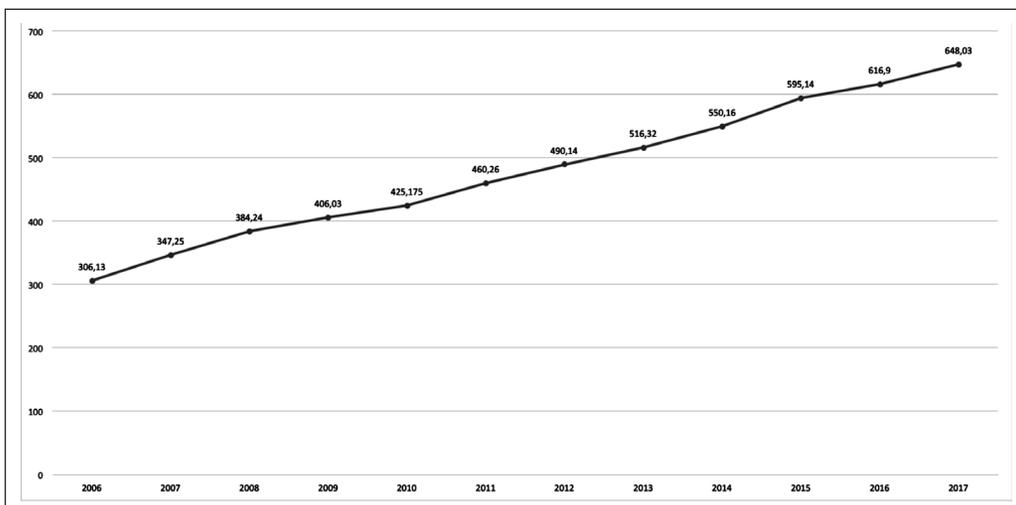
En las Administraciones Federales 2006-2012 y 2012-2018 las estrategias de seguridad tuvieron como punto de partida la coordinación entre fuerzas federales, poderes legislativos y gobiernos subnacionales (Presidencia de la República 2013). No obstante, la falta de

Tabla 4. Ramo 4: gobernación. Gasto programable por programa presupuestario (2018-2019) (millones de pesos corrientes y porcentajes)

Programa presupuestario	PEF 2018	PPEF 2019	PEF 2019	Variación		Variación		Variación	
				PPEF 2019	PEF 2018	PEF 2019	PPEF 2019	PEF 2019	PEF 2018
				Absoluta	Real%	Absoluta	Real%	Absoluta	Real%
Subsidios: sectores social y privado o entidades federativas y municipios	5300,00	4216,70	4216,70	-1083,30	-23,4	0	0	-1083,30	-23,4
Programa Nacional de Prevención del Delito	300			-300	-100			-300	-100
Subsidios en materia de seguridad pública	5000	4009,10	4009,10	-990,9	-22,8	0	0	-990,9	-22,8
Desempeño de las funciones	56 259,20	54 538,90	54 624,70	-1720,30	-6,7	85,8	0,2	-1634,50	-6,5
Servicios de inteligencia para la seguridad nacional	2888,40	2490,70	2490,70	-397,7	-17	0	0	-397,7	-17
Administración del Sistema Federal Penitenciario	17 235,30	16 641,70	16 641,70	-593,6	-7	0	0	-593,6	-7
Coordinación con las instancias que integran el Sistema Nacional de Seguridad Pública	399,5	314,9	314,9	-84,6	-24,1	0	0	-84,6	-24,1
Participación social para la reconstrucción del tejido social en México	218,2	184,8	184,8	-33,5	-18,5	0	0	-33,5	-18,5
Implementar las políticas, programas y acciones tendientes a garantizar la seguridad pública de la nación y sus habitantes	520,8	413,1	413,1	-107,7	-23,6	0	0	-107,7	-23,6
Promover la protección de los derechos humanos y prevenir la discriminación	151,6	148,9	158,6	-2,7	-5,4	9,6	6,5	7	0,7

Fuente: elaboración propia con datos de Senado de la República (2019).

Gráfico 2. Aportaciones federales del ramo general 33 (2006-2017)



Fuente: elaboración propia con datos del Instituto Nacional de Estadística y Geografía (INEGI).

resultados, de acuerdo con los responsables, se debió a las fallas en la coordinación entre agentes encargados de implementar las políticas de seguridad (Hernández 2015, 159-187). Esto, a pesar de que los recursos en el ramo 33 –mecanismo presupuestario en el que se encuentran los recursos para el fortalecimiento financiero y la seguridad pública– se incrementaron durante el periodo 2006-2017 (gráfico 2).

El incremento no significó que se hiciera un buen uso de los recursos públicos por parte de los gobernadores. Durante el periodo 2012-2018 fueron procesados al menos 11 exgobernadores⁵ por los delitos de corrupción, lavado de dinero, fraude, asociación delictuosa, delincuencia organizada, defraudación fiscal, delitos contra la salud, peculado agravado, entre otros (García 2018). Asimismo, el *Diag-*

5 César Duarte (Chihuahua), Jesús Reyna (Michoacán), Guillermo Padrés (Sonora), Andrés Granier Melo (Tabasco), Javier Duarte de Ochoa (Veracruz), Eugenio Hernández Flores (Tamaulipas), Tomás Yarrington (Tamaulipas), Roberto Borge Angulo (Quintana Roo), Luis Armando Reynoso Femat (Aguascalientes), Flavino Ríos (Veracruz), y Rodrigo Medina (Nuevo León).

nóstico Nacional sobre las Policías Preventivas de las entidades federativas mostró que el 1 de noviembre de 2018 se requerían 95 989 agentes para alcanzar el mínimo de 1,8 por cada 1000 habitantes (Muedano 2018). Ese contexto y la evidente falta de compromiso con la seguridad por parte de los gobiernos subnacionales podrían ayudar a comprender por qué el Gobierno Federal 2018-2024 apostó por la centralización de la seguridad en México.

Ante la falta de corresponsabilidad, los costos y riesgos parecen ser mayores para la democracia, debido a que es inevitable cuestionar cuánta violencia, inseguridad y crimen organizado puede soportar. Sobre todo porque la Guardia Nacional basa su estrategia en una ocupación territorial, así como en sustituir y no complementar a las policías estatales y municipales. Eso va en detrimento de la cooperación que los gobiernos estatales y municipales deberían tener con el desarrollo institucional de sus corporaciones policiacas, situación que cuestiona no solo la democracia, sino también

el federalismo en México, que queda por fuera del alcance del presente artículo. En otras palabras, la normativa de la Guardia Nacional rentabiliza el hecho de que los gobiernos subnacionales costeen presupuestalmente el uso de la Guardia Nacional en sus territorios para hacerse cargo de la seguridad pública.

Artículo 5. El objetivo de la Guardia Nacional es realizar la función de seguridad pública a cargo de la Federación y, en su caso, conforme a los convenios que para tal efecto se celebren, colaborar temporalmente en las tareas de seguridad pública que corresponden a las entidades federativas o municipios.

Artículo 16. El comandante ejercerá su autoridad a través de las Coordinaciones Territoriales, Estatales y de Unidad, sin perjuicio de ejercerla directamente. Asimismo, dispondrá de una Jefatura General de Coordinación Policial y de los organismos necesarios para el desarrollo de sus funciones.

Artículo 92. Los recursos humanos, económicos y materiales necesarios para la operación de la Guardia Nacional estarán a cargo de la Federación. Excepcionalmente, los convenios de colaboración que se suscriban entre la Secretaría y las entidades federativas o municipios contendrán las aportaciones que, en su caso deberán hacer éstos cuando la Guardia Nacional realice tareas de seguridad pública de competencia local (DOF 2019, 1-21).

Al tener una prioridad de recuperación y control territorial, la Guardia Nacional no apuesta por el fortalecimiento institucional ni mucho menos por el control o contrapeso que genere una clara rendición de cuentas. Es ambiguo asumir que el nuevo cuerpo policial, una estrategia reactiva, podrá cumplir todos los objetivos que se plantean, como la prevención del delito. Para que la política de militarización del Estado mexicano tenga la capacidad

de contener y desarticular las organizaciones criminales, y posteriormente incidir en una reconstrucción y fortalecimiento institucional, se requiere destinar mucho mayor presupuesto a la fuerza militar, panorama en el cual está muy por debajo de Colombia y Brasil.

Conclusiones

En el artículo se analizó la creación de la Guardia Nacional en México, como apuesta fundamental del gobierno encabezado por Andrés Manuel López Obrador para pacificar el país, inmerso en un espiral de violencia desde hace más de una década. El diagnóstico del cual partió la creación del nuevo cuerpo de seguridad fueron los pocos resultados de las estrategias llevadas a cabo por los expresidentes Felipe Calderón y Enrique Peña Nieto, sobre todo en lo que se refiere a conformar cuerpos policíacos estatales y municipales con capacidad de hacer frente a la violencia. A esto se le sumaron las fallas en la coordinación entre órdenes de gobierno para implementar de manera adecuada las políticas de seguridad.

En ese tenor, la discusión partió de los referentes teóricos de las políticas públicas y sus dificultades para instrumentarse en países en vías de desarrollo o que han transitado de manera reciente a la democracia. Así se explica que, ante la desafección colectiva con la democracia liberal y representativa –aquella que supone implementar un conjunto de derechos civiles, políticos y sociales– los ciudadanos han buscado soluciones inmediatas. Es entonces cuando las políticas de mano dura y de militarización han resultado rentables. Los casos de Colombia y Brasil ayudan a entender la situación de América del Sur; pero también la ola de violencia que vive Centroamérica

termina por demostrar un panorama de violencia e inseguridad en contextos democráticos. De ahí que el caso de México y su viraje hacia la Guardia Nacional indiquen que, dado el fracaso en la construcción de instituciones civiles de seguridad, el último recurso ha sido la militarización de la seguridad pública. Máxime por la pérdida de control territorial que ha tenido el Estado frente a las organizaciones criminales que sofistican sus modos de operación y de infiltración.

No obstante, las respuestas extraordinarias a problemas extraordinarios traen aparejadas consecuencias a corto y largo plazo. El diseño normativo dota de facultades extraordinarias al Ejecutivo Federal para conducir de manera discrecional durante su administración a la Guardia Nacional en el territorio nacional. No obstante, centralizar la seguridad para recuperar control territorial no significa construir y consolidar instituciones, sobre todo cuando la nueva política de seguridad no apuesta por el fortalecimiento de policías estatales y municipales. Por tal motivo, los riesgos de militarizar la seguridad pública en México son muchos. No solo se trata del respeto a los derechos humanos y la discrecionalidad en la toma de decisiones, sino también de claroscuros en cuanto a los resultados. Por un lado, delitos como el robo de hidrocarburos y los asaltos a camiones de carga pueden disminuir con la sola presencia militar, pero por otro, el número de decesos en enfrentamientos tiene una probabilidad de aumentar, debido a la letalidad de los militares que conforman la Guardia Nacional.

Por último, es imperativo señalar que la transición a la democracia en México, hace 19 años, trajo consigo una serie de cambios positivos, pero no ha resuelto grandes problemas como tener un adecuado estado de derecho

y paliar la desigualdad económica a través de políticas públicas. Asimismo, la fragmentación y la distribución del poder político hacia los gobiernos subnacionales tampoco significaron una mejor coordinación entre órdenes de gobierno. De ahí que exista descontento con el sistema político, porque los ciudadanos no se ven representados ni mucho menos aprecian resultados tangibles. Esto ha dejado espacio para las posturas que buscan solucionar de tajo problemas tan complejos como la inseguridad y el crimen organizado.

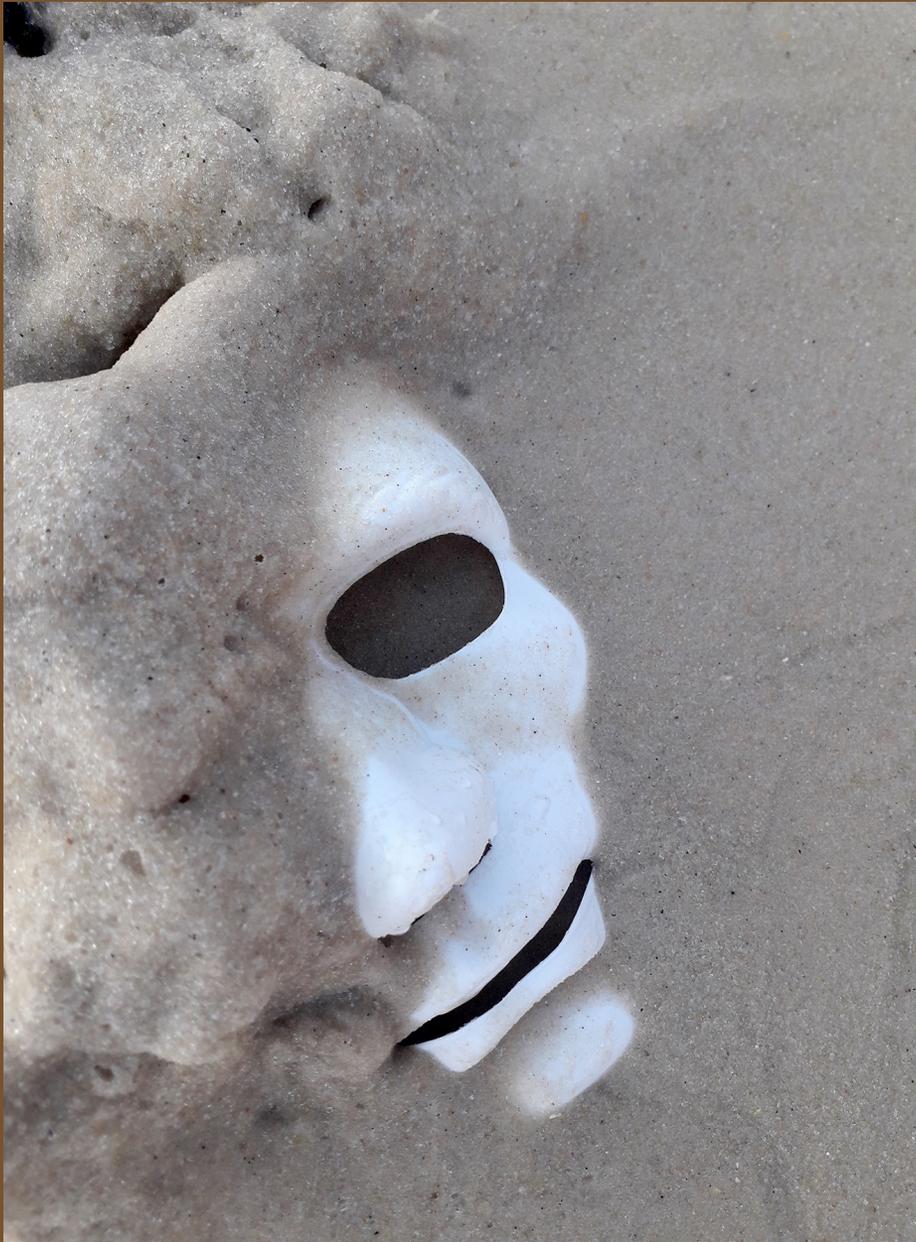
Bibliografía

- Alba Vega, Carlos, y Dirk Kruijt. 2007. "Viejos y nuevos actores violentos en América Latina: temas y problemas". *Foro Internacional* 3 (189): 485-516.
- Attili Cardamone, Antonella. 2004. "Summa potestas. Status moderno y crisis del poder político". *Polis 03 Investigación y Análisis sociopolítico y psicosocial* (2): 173-193.
- Amnistía Internacional. 2018. "La Guardia Nacional del presidente López Obrador: cinco realidades que hay que saber", <http://bit.ly/33sNZrD>
- Abt. Thomas. 2019. *Bleeding Out: The Devastating Consequences Of Urban Violence and a Bold New Plan for Peace in the Streets*. Nueva York: Hachette Book Group.
- Alonso, Laura y Robbins, Seth. 2019. "Ecos del pasado: el plan de seguridad de Duque para Colombia". *InSight Crime*, <https://es.insightcrime.org/noticias/analisis/ecos-del-pasado-el-plan-de-seguridad-de-duque-para-colombia/>
- Banco Mundial. 2019. "Homicidios intencionales (por cada 100,000 habitantes)", <http://bit.ly/34qOBPH>

- Barceló Vila, Luis Vicente. 2007. *Gobierno de globalización, del Pentágono al Hexágono*. Valencia: Editorial Universidad Politécnica de Valencia.
- Beck, Ulrich. 1997. ¿Qué es la globalización? Falacias del globalismo respuestas a la globalización. España: Paidós.
- Colprensa. 2018. “El 2017 tuvo la tasa de homicidios más baja en 42 años: Santos”. *El País*, 9 de enero. <https://www.elpais.com.co/colombia/el-2017-tuvo-la-tasa-de-homicidios-mas-baja-en-42-anos-santos.html>
- Connolly, William. 1991. *Identity/Difference: Democratic Negotiations of Political Paradox*. Londres: University of Minnesota Press.
- Consulta Mitofsky. 2018. “México: Confianza en Instituciones 2018”, <http://consulta.mx/index.php/estudios-e-investigaciones/mexico-opina/item/1084-confianza-instituciones-mx-2018>
- Dalby Chris, y Carranza Camilo. 2019. “Balance de InSight Crime sobre los homicidios en 2018”. *InSight Crime*, <https://es.insightcrime.org/noticias/analisis/ecos-del-pasado-el-plan-de-seguridad-de-duque-para-colombia/>
- DOF (Diario Oficial de la Federación). 2019. Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de Guardia Nacional (26 de marzo).
- DOFRH. 2013. 168/2013, 22 de agosto, Ley de la Policía Militar del Orden Público (22 de agosto).
- ENSU. 2018. *Encuesta nacional de seguridad urbana*. México: Instituto Nacional de Estadística y Geografía. <https://www.inegi.org.mx/programas/ensu/>
- Franco Corzo, Julio. 2013. *Diseño de políticas públicas*. México: IEXE.
- Fórum Brasileño de Seguridad Pública. 2018. “Anuário Brasileiro de Segurança Pública 2018”, <http://www.forumseguranca.org.br/atividades/anuario/>
- García, Dennis. 2018. “Borge, uno más a la lista de exgobernadores procesados”. *El Universal*, 3 de enero. <http://www.eluniversal.com.mx/nacion/seguridad/borge-uno-mas-la-lista-de-ex-gobernadores-procesados>.
- Galindo, Jorge. 2018. “El reto de Iván Duque: cuidar la democracia. El asesinato sistemático de líderes sociales supone una primera prueba para el presidente electo de Colombia”. *El País*, 8 de julio. https://elpais.com/internacional/2018/07/08/colombia/1531027199_096720.html
- Gobierno de México. 2019. “Informe de Seguridad”. Informe. <http://www.informese-guridad.cns.gob.mx/>
- PDS. 2019. *Política de Defensa y Seguridad (PDS): para la legalidad, el emprendimiento y la equidad*. Bogotá: Gobierno de Colombia Ministerio de Defensa Nacional.
- GPI (Global Peace Index). 2018. “Global Peace Index 2018: Measuring Peace in a Complex World, Sydney”, <http://vision-offhumanity.org/app/uploads/2018/06/Global-Peace-Index-2018-2.pdf>
- Hernández, Gerardo. 2015. “Análisis de la política de seguridad en México: 2006-2012”. *Política y Cultura* 44: 159-187.
- ICPR. 2019. “World Prison Brief Data/Brazil”. *World Prison Brief*, <http://www.prisonstudies.org/country/brazil>
- Integralia. 2018. “Primer reporte electoral Integralia 2018”, <https://integralia.com.mx/web/wp-content/uploads/2019/08/Cuarto-Reporte-Electoral-Integralia-2018.pdf>

- Ingram, Helen, Peter De León, y Anne Schneider. 2016. "Conclusion: Public Policy Theory and Democracy: The Elephant in the Corner". En *Contemporary Approaches to public policy: Theories, controversies and perspectives*, editado por B. Guy Peters y Philippe Zittoun, 175-200. Estados Unidos: International Series on Public Policy.
- Jaitman, Laura, Dino Capriolo, Rogelio Granguillhome Ochoa, Philip Keefer, Ted Leggett, James Andrew Lewis, José Antonio Mejía-Guerra, Heather Sutton, e Iván Torre. 2017. *Los costos del crimen y de la violencia: nueva evidencia y hallazgos en América Latina y el Caribe*. Washington: Banco Interamericano para el Desarrollo.
- Kleiman, Mark. 2005. *When Brute Force Fails: Strategic Thinking for Crime Control*. EEUU: U.S Department of Justice.
- Latinobarómetro. 2018. *Informe 2018*. Santiago de Chile: Corporación Latinobarómetro.
- Londoño, Ernesto, y Manuela Andreoni. 2018. "Cavaremos las tumbas: Brasil se alista para política de seguridad de Bolsonaro". *New York Times*, 1 de noviembre. <https://www.nytimes.com/es/2018/11/01/brasil-bolsonaro-seguridad-policia/>
- Londoño, Ernesto y Shasta Darlington. 2018. "Brasil pone al ejercito al mando de la seguridad en Río de Janeiro ante la ola de violencia". *New York Times*, 16 de febrero. <https://www.nytimes.com/es/2018/02/16/brasil-rio-janeiro-ejercito-seguridad/>
- Medellín, Pedro. 2004. "La política de las políticas públicas: propuesta teórica y metodológica para el estudio de las políticas públicas en países con frágil institucionalidad". *Serie Políticas Sociales*, julio. https://repositorio.cepal.org/bitstream/handle/11362/6082/1/S047566_es.pdf
- Miranda, Fanny. 2019. "Guardia Nacional ya opera en Minatitlán". *Milenio*. 26 de abril. <https://www.milenio.com/politica/guardia-nacional-de-amlo-ya-opera-en-minatitlan>
- Muggah, Robert, y Katherine Aguirre. 2018. "Citizen Security in Latin America: Facts and Figures". *Strategic Paper 2X*. <https://igarape.org.br/wp-content/uploads/2018/04/Citizen-Security-in-Latin-America-Facts-and-Figures.pdf>
- Muedano, Marcos. 2018. "Sexenio inicia con déficit de 96 mil policías; hay pendientes de capacitación". *Excelsior*, 12 de noviembre. <https://www.excelsior.com.mx/nacional/sexenio-inicia-con-deficit-de-96-mil-policias-hay-pendientes-en-capacitacion/1277772>
- Melgoza, Rocío. 2019. "Expertos a favor y en contra de la Guardia Nacional coinciden: el mando mixto es una mala idea". *Economía Hoy*, 16 de enero. <http://bit.ly/2rzaNZE>
- Nájar, Alberto. 2018. "López Obrador gana en México: ¿por qué es histórico el triunfo de AMLO en la elección presidencial mexicana?". *BBC News Mundo*, 2 de julio. <https://bbc.in/37RkwuI>
- Nerio Monroy, Ana Luisa. 2011. "La militarización de la seguridad pública y su impacto en los derechos humanos de la población en situación de vulnerabilidad". *Dfensor Revista de Derechos Humanos* 8: 19-22.
- WOLA. 2019. "Propuesta de Guardia Nacional concretizaría la militarización de la seguridad pública en México: el fortalecimiento del papel de las fuerzas armadas en tareas de seguridad pública pone en riesgo los derechos humanos". 10 de enero. <https://www.wola.org/wp-content/>

- uploads/2019/01/1.10.19-Guardia-Nacional-SPN.pdf
- Plan Nacional de Paz y Seguridad 2018-2024. 2018. “Plan Nacional de Paz y Seguridad 2018-2024”, https://lopezobrador.org.mx/wp-content/uploads/2018/11/Plan-Nacional-de-Paz-y-seguridad_.pdf
- Pasquino, Gianfranco. 2011. *Nuevo curso de ciencia política*. México: FCE.
- Parsons, Wayne. 2007. *Políticas públicas*. Una introducción a la teoría y la práctica del análisis de políticas públicas. México D.F.: Flacso México/ Miño y Dávila Editores.
- Pérez Sánchez, Margarita. 2005. “El estudio de las políticas públicas”. En *Análisis de políticas públicas*, editado por Margarita Pérez Sánchez, 51-75. España: Universidad de Granada.
- Peters, Guy. 2010. “Governing in the Shadows”. *SFB Governance Lecture Series 3*: 4-17.
- Presidencia de la Republica. 2018. “Conferencia de prensa matutina del Presidente Andrés Manuel López Obrador”, <https://www.youtube.com/watch?v=ul4DaFqeXqw>
- Presidencia de la República. 2013. “Discurso por el 85 Aniversario y Día del Policía Federal”, www.presidencia.gob.mx
- PND (Plan Nacional de Desarrollo). 2019. “Plan Nacional de Desarrollo 2019-2024”, https://www.dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019
- Redacción. 2018. “EE.UU. expresa admiración y saluda “sólida democracia”. *Voz de América Latina*, 18 de junio. <https://www.voanoticias.com/a/eeuu-expresa-admiraci%C3%B3n-saluda-solida-democracia-colombia/4444047.html>
- Reuters. 2019. “Nuevo presidente de Brasil llama al Congreso a combatir la corrupción y promete fortalecer la democracia”. 1 de enero. <https://www.americaeconomia.com/politica-sociedad/politica/nuevo-presidente-de-brasil-llama-al-congreso-combatir-la-corrupcion-y>
- Roldán Mariluz. 2018. “Más de 500 organizaciones manifiestan su rechazo a la Guardia Nacional”. *El Universal*, 20 de noviembre. <http://bit.ly/2qVw0Nl>
- Saskia Sassen. 2007. *Una sociología de la globalización*. Madrid: Katz Editores.
- Senado de la República. 2019. “Recursos Destinados a Seguridad Pública en el Presupuesto de Egresos de la Federación 2019”, <http://bit.ly/34Cr7Yh>
- Senado de la República. 2018. “Conferencia de la senadora Olga Sánchez Cordero”, <https://www.youtube.com/watch?v=SZbE3ouK06I>
- SESNSP (Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública). 2019. “Informe de incidencia delictiva fuero común”, <https://www.gob.mx/sesnsp>
- SIPRI. 2019. “Gasto militar (% del PIB) México, Chile, Brasil y España 2006-2017”, <https://datos.bancomundial.org/indicador/MS.MIL.XPND.GD.ZS>
- Weimer, David L., y Aidan Vining. 1992. *Policy Analysis Concepts and Practice*. Englewood Cliffs: Prentice Hall.



Estudios Globales

El tratamiento informativo de la guerra híbrida de Rusia

The Informative Treatment of the Russian Hybrid War

Javier Miguel-Gil¹

Recibido: 3 de junio de 2019

Aceptado: 2 de septiembre de 2019

Publicado: 2 de diciembre de 2019

Resumen

El artículo tiene como objetivo analizar el tratamiento informativo que los medios de comunicación han realizado de las campañas de desinformación rusa en un supuesto contexto de guerra híbrida. A partir de noticias de los principales medios de comunicación que informaron sobre el tema, el análisis se centra en el uso del concepto de guerra híbrida y lo compara con su concepción tradicional estratégica, para determinar si las actividades en cuestión pueden inscribirse en este tipo de conflictos.

Palabras clave: doctrina Gerasimov; guerra híbrida; medios de comunicación; propaganda; Rusia

Abstract

The objective of this paper is to analyze the treatment that the mass media have given to Russian disinformation campaigns in a supposed context of hybrid war. The exposition of news from the main mass media allows to focus the analysis on the concept of hybrid war, and to compare it with its traditional strategic conception, to determine if the activities in question can be classified into this kind of conflicts.

Key Words: Gerasimov Doctrine; hybrid warfare; mass media; propaganda; Russia

¹ Universidad Complutense de Madrid, España, javier.miguel.gil@ucm.es,  orcid.org/0000-0002-5141-1024



Introducción

La incorporación de las Tecnologías de la Información y Comunicación (TIC) ha comportado un cambio total en la forma en que nos relacionamos y comunicamos, pero también en la forma en que nos informamos. La expansión de lo que hoy conocemos como internet ha permitido que millones de personas en todo el mundo tengan acceso a la mayor fuente de información en la historia de la humanidad, principalmente a través de los *smartphones*, los ordenadores personales y las *tablets*.

Uno de los ámbitos en los que la propagación de internet ha tenido mayor repercusión ha sido en la comunicación, tanto en la estructura de los medios y en el alcance de su audiencia como en los propios contenidos. Los medios tradicionales han tenido que adaptar su organización a nuevos formatos y a una demanda continua de información por parte de los lectores, además de hacer frente a la aparición de nuevos medios, exclusivamente digitales. Pero esa exigencia informativa ha generado también ciertas dudas sobre la credibilidad y calidad de la información, algo realmente preocupante si tenemos en cuenta la importancia de los medios de comunicación en las sociedades democráticas. La rapidez con la que se propagan las noticias actualmente –bien sea a través de los sitios webs, de los medios de comunicación o de las redes sociales– tiene un impacto prácticamente inmediato en la opinión pública y, en muchos casos, también efímero. La necesidad de generar continuamente noticias ha comportado que estas tengan una enorme volatilidad, a la vez que ha condicionado la calidad de la información.

En ese contexto, las denuncias públicas por parte de los gobiernos occidentales sobre

unas supuestas campañas de desinformación dirigidas desde el gobierno de Vladimir Putin (Boffey 2018; Faus 2018) han centrado gran parte de la atención mediática internacional. Conceptos como ciberataques, *fake news* y amenazas híbridas se han generalizado para denunciar la propagación de noticias falsas con el objetivo de desestabilizar, en procesos internos como el *Brexit* (junio de 2016), en las elecciones presidenciales estadounidenses (noviembre de 2016) y en la crisis política y social catalana en España (con su punto álgido en octubre de 2017). Según las denuncias, los intentos de injerencia se basarían en el uso de la información entendida como un elemento militar, de carácter asimétrico, en un supuesto contexto de guerra híbrida, dirigida desde la Federación de Rusia contra las democracias occidentales, a través de la denominada “doctrina Gerasimov”.

Metodología

El presente análisis tiene como objetivo comparar el tratamiento periodístico que los medios han dado a las campañas de desinformación rusa y a las cuestiones híbridas con el concepto de lo híbrido desarrollado tradicionalmente desde un ámbito estratégico-militar, para determinar si los acontecimientos citados se inscriben en un contexto de guerra híbrida, tal y como señalan gran parte de los medios y analistas.

El artículo parte de la exposición de una serie de noticias relacionadas con las campañas de desinformación de origen ruso y del uso que hicieron del concepto de guerra híbrida. Debido a la gran cantidad de noticias publicadas sobre estas cuestiones, a partir del procedimiento sintético, se realizó una selec-

ción general de noticias de distintos medios de reconocido prestigio nacional e internacional que aportan una variedad de perspectivas como *The Guardian*, *The Washington Post*, *BBC* y *El País*. Posteriormente, y siguiendo el método descriptivo, se introduce el término guerra híbrida desde su concepción tradicional, partiendo del origen del concepto, exponiendo algunas de sus definiciones y características generales y contextualizándolo en lo que se ha popularizado como doctrina Gerasimov. Por último, a través del método comparativo, se compara el tratamiento periodístico de este tipo de conflictos con su concepción tradicional estratégica.

Contextualizando la guerra híbrida

En los últimos años, tomando como referencia temporal el referéndum que tuvo lugar en Reino Unido para abandonar la Unión Europea, en junio de 2016, y especialmente desde las elecciones presidenciales estadounidenses de noviembre de ese mismo año, los medios de comunicación han centrado gran parte de su información internacional en alertar sobre el peligro que las noticias falsas –popularizadas con el nombre de *fake news*– representan para las democracias occidentales.

En su objetivo de informar, los medios de comunicación masiva han utilizado todo tipo de conceptos, nuevos para gran parte del público, como ciberespacio, ciberataque, ciberguerra o guerra híbrida, para explicar los acontecimientos que se producían a través de lo que comúnmente denominamos internet, en los que un Estado (la Federación Rusa en este caso) utilizaría el ámbito digital para interferir en procesos internos de otro, con el objetivo de desestabilizar sus sistemas demo-

cráticos. En este novedoso y complejo contexto, ¿cómo informaron los medios de comunicación sobre los sucesos?

A pesar de que actualmente el *Brexit* se considera un ejemplo de las injerencias rusas en campaña electoral (Cohen 2018), encontramos pocas referencias en los medios que, tanto durante la campaña como en el momento posterior al referéndum, acusaron al gobierno de Vladimir Putin de querer influir en la votación del referéndum y definieron esas actividades como guerra híbrida.² En su mayoría, los análisis postelectorales se centraron en la incertidumbre que generaba la salida de Reino Unido de la Unión Europea, en las consecuencias económicas, políticas y sociales que podría tener, así como en el propio papel de la Unión a partir de ese momento (BBC 2016; Coy 2016).

En gran medida, no fue hasta las elecciones presidenciales estadounidenses, celebradas en noviembre de 2016, cuando los medios de comunicación señalaron directamente a Moscú de haber realizado ataques informáticos contra el Partido Demócrata y de haber orquestado campañas de desinformación para influir en el voto mediante la opinión pública. En este punto la atención se centró en el ciberespacio y en las vulnerabilidades que representa para las democracias occidentales. A pesar de eso, no fue hasta meses después cuando empezaron a surgir de forma continua informaciones sobre la posible injerencia del Kremlin en el referéndum británico, a través de la propagación de noticias falsas, así como el uso de las redes sociales (Adam y Booth 2017; *The Economist* 2017).

² Las escasas referencias a Rusia se centraban en cómo la incertidumbre surgida a partir del triunfo del *Brexit* era bien vista desde el Kremlin –con alusiones al todavía reciente conflicto en Ucrania–, pero sin señalar directamente al gobierno de Putin por haber promovido una campaña de desinformación o de guerra híbrida (Baunov 2016).

Los hechos marcaron un antes y un después en el papel que habría jugado una potencia extranjera para tratar de influir en un proceso electoral interno. Fueron una señal de alerta para los países europeos que meses después iban a celebrar distintos procesos electorales³ (Bransford 2017). En ese contexto, el periódico *The Guardian* afirmaba en un titular que “La UE intensifica su campaña contra la propaganda rusa” (Boffey y Rankin 2017) debido al miedo que había generado la posible injerencia rusa en las elecciones estadounidenses, y a que esta pudiera extenderse a Europa. Señalaba que la Unión iba a “aumentar sus esfuerzos para contrarrestar la campaña de guerra híbrida de Rusia tras la elección de Donald Trump”. La noticia hace referencia al *East Stratcom Task Force*, un organismo creado en 2015 por el Servicio Europeo de Acción Exterior de la UE –y, por lo tanto, anterior a los procesos aquí expuestos– para contrarrestar las campañas de desinformación rusas durante la crisis de Ucrania.

En ese contexto internacional de desinformación, noticias falsas, injerencias rusas en procesos electorales, ataques informáticos y supuesta guerra híbrida, España se encontraba inmersa en una importante crisis política y social debido a la convocatoria de un referéndum por el gobierno autonómico de la Generalitat de Catalunya, a primeros de octubre de 2017, que pretendía decidir mediante consulta sobre la posibilidad de independizarse del Estado español, sin el consentimiento del gobierno de España. Rápidamente se incorporaron estas actividades al lenguaje informativo. Titulares como “Ciberguerra entre los

gobiernos catalán y español por el cierre de la web del referéndum” (Pueyo 2017), publicado en el periódico *El País* pocos días antes de la celebración del referéndum o “The great Catalanian cyberwar of 2017” (Caryl 2017), publicado por *The Washington Post*, apenas dos semanas después de que tuviese lugar el referéndum, utilizaron el concepto de ciberguerra de forma genérica, sin tener en cuenta su posible significado e implicaciones, por el simple hecho de que determinadas actividades se realizaron a través de la red.

El concepto de ciberguerra ha sido uno de los más utilizados desde el ámbito periodístico para hacer referencia a las actividades que tienen lugar a través de internet, pero a su vez ha generado confusión. Richard A. Clarke, Excoordinador Nacional de Seguridad, Protección de Infraestructura y Contraterrorismo de EEUU y Asesor Especial del presidente en Seguridad Cibernética, define la ciberguerra como “las acciones realizadas por un Estado-nación para penetrar en los ordenadores o en las redes de otros Estados con el propósito de causar daño o alteraciones” (Clarke y Knake 2010, 6). A excepción de los ciberataques contra el Partido Demócrata, por los cuales se tuvo acceso a datos de la campaña e información de miembros del Partido, las actividades de propaganda que tuvieron lugar en el *Brexit* y en el conflicto catalán no pueden calificarse de ciberguerra, según la definición de Clarke, ya que no habrían comportado el acceso ilegítimo a los sistemas o redes de otros Estados, con el objetivo de causar daño o alteraciones, sino que más bien serían actividades de influencia y manipulación a través de la red.

En el momento álgido de los acontecimientos de Catalunya, análisis y titulares como “Rusia se apunta a la guerra híbrida” (De Pedro 2017), “La guerra híbrida amenaza

3 Países Bajos celebró elecciones generales en marzo de 2017; Francia realizó las elecciones presidenciales entre abril y mayo de 2017 y, en el mes de junio, las legislativas; en Alemania se celebraron las elecciones federales en el mes de septiembre y Chéquia celebró elecciones legislativas en octubre de 2017.

a España” (Pérez 2017) y directamente “Guerras Híbridas” (El País 2017) nos situaban en este tipo de guerras. En el último caso, el periódico afirma que la desinformación es

parte de una doctrina militar que recibe el nombre de ‘guerra híbrida’. Esta doctrina –elaborada en Rusia– busca debilitar a las democracias interfiriendo en sus procesos electorales y alimentando sus conflictos internos, sean ideológicos o territoriales, valiéndose para ello de instrumentos como las noticias falsas o la manipulación de las redes sociales (El País 2017).

Es conveniente señalar que, en algunos casos, los titulares hacen referencia a cuestiones relacionadas con informaciones o documentos gubernamentales en los que se utiliza este tipo de conceptos, como es el caso de los artículos de Pérez (2017) y el editorial de *El País* (2017), que aluden a la aprobación de la actual Estrategia de Seguridad Nacional española de 2017, la cual incluye las cuestiones de las amenazas híbridas y la desinformación.

Pero si analizamos las noticias –tanto las indicadas anteriormente como otras que tratan estas cuestiones– uno de los elementos que tienen en común es que no explican ni exponen mínimamente al lector algunos de los conceptos utilizados –entiéndase ciberataque, ciberguerra o guerra híbrida, por señalar algunos ejemplos–. En cambio, se limitan a afirmar que estamos en un conflicto (guerra híbrida) promovido por un actor estatal (Rusia), mediante la difusión de noticias falsas a través de internet y de las redes sociales, con el objetivo último de debilitar a los gobiernos democráticos occidentales. Por otro lado, gran parte de las noticias sobre estas actividades presentan la guerra híbrida como algo novedoso (El País 2017; Roig 2018), que forma

parte de una doctrina militar de origen ruso conocida como doctrina Gerasimov, aunque hay referencias anteriores a estos hechos, principalmente centrados en el contexto de la crisis de Ucrania, en 2014 (Kendall 2014; Villarejo 2014).

Si revisamos las publicaciones académicas, el origen de las denominadas guerras híbridas habría que situarlo en un contexto anterior a los hechos aquí expuestos. Algunos de trabajos, publicados a principios de 2015 –por lo tanto, anteriores al *Brexit*, a las elecciones presidenciales de EEUU y a la crisis catalana– analizaban el concepto de guerra híbrida (García y Martínez-Valera 2015) o se cuestionaban si en aquel momento era un elemento novedoso o tan solo una vieja adaptación de viejos esquemas (Baqués 2015b, 3).

Origen y características de las guerras híbridas

Hay autores que atribuyen el origen de la expresión guerra híbrida al general retirado de la Armada estadounidense Robert Walker, en 1998 (Baqués 2015b, 8; Oguz 2017, 531), quien analizó en su trabajo final de máster el modelo híbrido de las guerras –centrándose en el Cuerpo de Marines de los Estados Unidos–. Por otro lado, hay quienes señalan que el origen habría que situarlo unos años más tarde, en 2002, cuando se utilizó el término para explicar acciones tácticas de la Primera Guerra de Chechenia, que tuvo lugar entre 1994 y 1996. Sin embargo, de manera oficial no se utilizó hasta la Estrategia Nacional de Defensa estadounidense de 2005 (Colom 2019, 8). No fue hasta la publicación en 2005 del artículo *Future Warfare: The Rise of Hybrid Warfare*, del general James N. Mattis y el te-

niente coronel Frank G. Hoffman, y del trabajo *Conflict in the 21st Century. The Rise of Hybrid Wars* (Hoffman 2007) cuando el concepto adquirió contenido teórico y se popularizó (Colom 2019, 8-9).

El concepto se extendió en gran medida para intentar comprender las guerras contemporáneas entre actores estatales y no estatales, en las que un actor estatal teóricamente superior en tecnología, capacidad militar o doctrinal no era capaz de doblegar a actores irregulares. Un ejemplo de ello son las guerras que llevaron a cabo los EEUU en Afganistán (inició en 2001) e Irak (inició en 2003) y la campaña que enfrentó a Israel contra Hezboallah en el verano de 2006 (Baqués 2015b, 3).

Definiciones de guerra híbrida

Una de las primeras aproximaciones define la guerra híbrida como “la que se sitúa en los intersticios entre la guerra especial y la guerra convencional” (Walker 1998, 4-5). Por su parte, Hoffman (2007, 28) amplía y precisa su naturaleza, y considera que “mezcla la letalidad del conflicto estatal con el fervor fanático y extendido de la guerra irregular”. Puede ser promovida tanto por actores estatales como no estatales. Estos conflictos “incorporan una variedad de diferentes modos de hacer la guerra, incluyendo capacidades convencionales, tácticas y formaciones irregulares, actividades terroristas incluyendo violencia y coerción indiscriminada y desorden criminal” (Hoffman 2007, 29). En la práctica, ello supone la combinación de actividades convencionales e irregulares. En una línea similar, el coronel de Infantería del Ejército de Tierra español, José Luis Calvo Albero, define la guerra híbrida como “aquella en la que al menos uno de

los adversarios recurre a una combinación de operaciones convencionales y guerra irregular, mezclada esta última con acciones terroristas y conexiones con el crimen organizado” (Palacios 2016b, 22).

A pesar de estas aproximaciones,⁴ actualmente no hay una definición precisa del concepto, que sea ampliamente aceptada, “más allá del mínimo común denominador de la combinación de medios, procedimientos y tácticas convencionales y asimétricas” (Colom 2018, 30). Inclusive, hay quienes plantean que “no hay nada nuevo sobre el concepto de las operaciones híbridas o su utilidad en el conflicto” (Walker 1998, 5). En los conflictos de la posguerra fría, quienes se han enfrentado a Estados occidentales habrían utilizado (en distintos niveles) fuerzas convencionales, tropas irregulares, actos terroristas y crimen organizado (Baqués 2015b, 10-11).

Características de las guerras híbridas

Las noticias han presentado la guerra híbrida como un conflicto novedoso, centrándose principalmente en el elemento informativo –en la desinformación y las noticias falsas– y en su difusión por internet. Pero este tipo de conflictos supondrían, además, la combinación de otros elementos a tener en cuenta, como los actores que participan, el tipo de armamento que poseen y los escenarios en los que se desarrollan (Baqués 2015a). Algunas características de las guerras híbridas son:

⁴ El objetivo es presentar una aproximación general al concepto de guerra híbrida y sus características, pero no hay que obviar el debate en torno a la propia conceptualización, cuya discusión escapa del objetivo del presente artículo y su extensión. Para una ampliación del debate y distintas aproximaciones al concepto, ver: Johnson 2018; Schnaufer 2017; Wither 2016.

- Los actores de los conflictos: entre ellos encontramos Estados, grupos guerrilleros y terroristas, así como grupos de crimen organizado o contratistas militares privados (Colom 2012, 79). Este tipo de conflictos pueden ser planteados por actores estatales o actores no estatales (Baqués 2015b, 3-7). Como se ha señalado anteriormente, los análisis de la guerra híbrida se centraron principalmente en los enfrentamientos entre actores armados no estatales –normalmente vinculados a un Estado fallido– y los Estados occidentales, como en los casos de las guerras de Afganistán, Irak y el enfrentamiento entre Hezbollah e Israel. Los grupos insurgentes desarrollarían la guerra híbrida debido a que, *a priori*, tendrían unas capacidades inferiores a los actores estatales –en personal, doctrina, armamento y tecnología– en una eventual guerra convencional. Formados principalmente por voluntarios, el objetivo consistiría en contrarrestar la superioridad del actor estatal y explotar sus vulnerabilidades.⁵ Por otro lado, este tipo de conflictos también pueden plantearse por parte de actores estatales, en un eventual enfrentamiento convencional con otros actores estatales supuestamente superiores. Un caso novedoso sería el conflicto entre Ucrania y Rusia en 2014, en el que el Estado teóricamente más fuerte (Rusia) fue quien usó la guerra híbrida contra el más débil (Baqués 2015a). Baqués añade que esa decisión se basaría en evitar un enfrentamiento convencional y, a su vez, un posible choque con Estados Unidos y la OTAN, en el que Rusia sería precisamente la “parte débil”.
- El tipo de armamento utilizado: las fuerzas irregulares poseen armamento más propio de los ejércitos regulares, como son tecnologías de última generación y armas pesadas, por lo que es más difícil distinguir entre las formas de guerra convencional e irregular. Baqués (2015a; 2015b, 8) hace referencia a la idea de Colin Gray del *blurring* (difuminación), en el sentido de que no hay distinción clara entre las guerras convencionales y las irregulares.
- Las tácticas empleadas: desde el uso de acciones convencionales hasta actos terroristas; el empleo de *proxies*, insurgencia, operaciones informativas o ciberoperaciones (Colom 2019, 11).
- El uso de las Tecnologías de la Información y de la Comunicación (TIC): incluye desde el control de los medios tradicionales hasta internet y las redes sociales. Ello permitiría reforzar la imagen propia o contrarrestar la del adversario, con el objetivo de llegar a los “corazones y las mentes” de las personas, lo que en buena medida sería la guerra psicológica (Baqués 2015a). De esa manera, hay una creciente importancia de la denominada guerra de la información y del uso del ciberespacio (Baqués 2015b, 12).
- Los escenarios: este tipo de conflictos se consideran esencialmente urbanos, a diferencia de las guerras de guerrillas, que se desarrollarían en la selva o las montañas. Esto genera mayores dificultades para alcanzar los objetivos militares, debido a la presencia de la población civil y a las posibles consecuencias en las infraestructuras como el transporte y la energía.
- La conexión con grupos terroristas y el crimen organizado: es habitual que los

⁵ Por ejemplo, alargando el conflicto. Este hecho implicaría un desgaste del Estado occidental en cuestión, debido principalmente a la creciente presión de la opinión pública. A la vez, cuanto más se alarga el conflicto, mayores son los costes económicos. Los casos de Afganistán e Irak y su impacto económico y en la opinión pública son un ejemplo.

grupos que participan en las guerras híbridas tengan vínculos con grupos terroristas (realización de atentados terroristas) o delincuencia organizada (en el ámbito de la financiación). Esto no implica necesariamente que tengan objetivos comunes.

- La creciente importancia del elemento psicológico: hay un desprecio intencionado hacia la legalidad y el derecho internacional humanitario por parte de los actores promotores de las guerras híbridas y de los grupos criminales y terroristas vinculados. Por el contrario, las fuerzas armadas occidentales se encuentran sujetadas a reglas *–ius in bello*, las tradiciones militares o las Reglas de Enfrentamiento (ROE, por sus siglas en inglés) – (Baqués 2015b, 6). Por ello, las guerras híbridas pueden considerarse formalmente distintas a los conflictos tradicionales, en cuanto se “combatía de manera convencional y simétrica en frentes claramente definidos, con medios tecnológicamente avanzados para la época, y sometidos a los usos y costumbres de la guerra comúnmente aceptados por los contendientes” (Colom 2012, 80).
- La planificación: los promotores de este tipo de conflictos detectarían previamente los puntos débiles del adversario, en el ámbito político, ideológico, económico o demográfico, con el objetivo de alargar el conflicto, de encarecer sus costes o influir en la percepción de las sociedades y de los Estados occidentales (Baqués 2015b, 5-6).

Hay que destacar, tal y como han señalado anteriormente Hoffman (2007), Calvo Albero (Palacios 2016b, 22), Colom (2018, 30) y Baqués (2015a), que las guerras híbridas implican la combinación de elementos regulares e irregulares. Por tanto, el uso de uno de

estos elementos no implica que un conflicto pueda considerarse necesariamente “híbrido”. Las actividades rusas en los casos expuestos (*Brexit*, elecciones estadounidenses y conflicto catalán) han recibido el calificativo de híbrido en gran medida por el uso del ciberespacio y la combinación de ataques informáticos, propaganda y desinformación a través de las TIC, así como de operaciones informativas. Sin embargo, no se produjo en ningún caso un enfrentamiento armado en el que participaran actores estatales o no estatales.

La guerra híbrida en relación con las noticias

Según los medios de comunicación, Rusia está impulsando una guerra híbrida contra los Estados occidentales. No obstante, la clasificación anterior plantea un escenario distinto a los descritos. La novedad, de acuerdo con las noticias, reside en que un único Estado (Rusia) estaría impulsando este tipo de guerras prácticamente de forma simultánea contra varios Estados a la vez, entre los que se incluyen desde las principales potencias militares (Estados Unidos y Gran Bretaña) hasta países con un menor poder militar (como sería el caso de España).⁶ Esto, mediante un proceso continuo que se alarga en el tiempo, pero en el que podemos identificar momentos álgidos de presión, por ejemplo, poco antes de los procesos electorales internos. Recurriría al potencial de las TIC, sobre todo en relación con el uso del ciberespacio, para la realización de campañas de desinformación y la distribución de noticias falsas en contextos de tensión interna de los países, explotando el potencial

⁶ En relación con un hipotético enfrentamiento armado entre Rusia y otro actor estatal.

que actualmente tienen internet y las redes sociales en las sociedades occidentales. Pese al uso que Rusia ha hecho del ámbito digital, unido a las campañas de desinformación, no tiene el monopolio de estas actividades, sino que cualquier Estado –así como los actores no estatales– puede hacer uso de ellas para conseguir sus objetivos. Sin embargo, los medios de comunicación han informado que es una actividad casi exclusiva de Rusia.

Hay que tener en cuenta que una de las características fundamentales de la guerra híbrida consistiría no solo en el uso de las TIC, sino en la utilización simultánea de otros componentes señalados anteriormente (Baqués 2015a; Baqués 2015b, 12). Es decir, la combinación de los elementos regulares e irregulares a los que hacía referencia Hoffman (2007). En la supuesta guerra híbrida de Rusia contra los Estados occidentales no se produce un conflicto armado en el que participen fuerzas regulares e irregulares, se use armamento avanzado⁷ o se realicen actos terroristas, por citar algunos elementos.

Una de las características que señalaban los medios de comunicación era la supuesta novedad de este tipo de conflictos y la exclusividad que tenía Rusia en el planteamiento de las guerras híbridas. Pero según lo expuesto, algunos de los principales estudios se remontan a principios del siglo XXI, en un intento de comprender y definir los conflictos contemporáneos (Walker 1998; Hoffman 2007). Algunos expertos consideran que “estas formas de actuación difícilmente pueden calificarse como novedosas o considerarse como una respuesta específica al estilo occidentalizado de combate” (Colom 2012, 80). Tampoco sería

⁷ Baqués (2015a) considera que una de las principales características de los conflictos híbridos es el uso de armamento propio de ejércitos regulares por parte de actores irregulares.

novedad la difusión de noticias falsas, un elemento utilizado a lo largo de la historia, que se habría beneficiado de las tecnologías disponibles en cada momento histórico. Sí lo sería el alcance que tiene actualmente la difusión de noticias debido a la expansión de internet.

Por otro lado, uno de los elementos característicos de las guerras híbridas es el escenario en el que se desarrollan, principalmente los núcleos urbanos. En el caso que estamos analizando, Rusia habría utilizado el ciberespacio como el escenario principal de sus actividades, lo que supone otra diferencia. Por todo ello, aunque se hayan realizado operaciones informativas o ciberoperaciones a través de internet –no solo difusión de noticias, también ataques informáticos como los realizados contra el Partido Demócrata de Estados Unidos, que permitió el acceso a las cuentas de correo electrónico– estas actividades por sí solas no permitirían definir como guerra híbrida los sucesos expuestos en las noticias.

La doctrina Gerasimov y la guerra híbrida

Si el concepto de guerra híbrida ha centrado parte del análisis, otros conceptos han sido utilizados para contextualizar estos conflictos. Las noticias apuntaban a que la guerra híbrida formaba parte de una doctrina militar rusa que se ha popularizado como doctrina Gerasimov, la cual expondría que

ahora mismo la línea que separa a la guerra de la paz es difusa, por lo que hay que desarrollar tácticas que permitan trabajar en las sombras, condicionando procesos electorales, agitando a la población civil o hackeando objetivos en otros países (Colás 2017).

El origen del concepto se remonta a febrero de 2013, con la publicación del artículo “El valor de la ciencia en la anticipación” (Gerasimov 2013) del jefe del Estado Mayor de la Defensa, el general Valeri Gerasimov en la revista *Voyenno-Promyshlennyy Kuryer* (VPK, Correo Militar-Industrial). Para gran parte de los medios de comunicación y analistas occidentales, el artículo representa el documento fundacional de lo que en Occidente se conoce como la doctrina Gerasimov (Bartles 2016, 55; Palacios 2016a). “Se interpreta como una propuesta de una nueva manera rusa de guerra que combina la guerra convencional y la no convencional con aspectos de poder nacional” (Bartles 2016, 55), en la que se hace referencia a los “métodos indirectos y asimétricos”, que desde Occidente se han interpretado como guerra híbrida (Bartles 2016, 59). Con los sucesos de Crimea y Ucrania, se identificaron algunos de los elementos expuestos en el documento de 2013 de Gerasimov y se propagó la idea de que exponía una nueva forma de hacer la guerra⁸ (Colom 2018, 34).

Fue entonces cuando lo híbrido traspasó la frontera del debate estratégico para convertirse en vocablo de uso común y utilizarse para definir toda la gama de actividades informativas, de desestabilización y subversión que el Kremlin podía estar realizando de forma encubierta, semientucubierta o clandestina por debajo del umbral del conflicto (Colom 2019, 9).

A pesar de la aceptación generalizada del concepto y de que representa una nueva doctrina (Gamboa 2017, 31; Campos 2018, 14), algunos analistas han cuestionado que sea una

doctrina militar o que proponga una nueva manera rusa de hacer la guerra (Bartles 2016, 57,63; Palacios 2016b, 27). Estos autores precisan que Gerasimov planteaba en su artículo (dirigido principalmente a un público ruso) “su perspectiva del pasado reciente, el presente y el futuro esperado de la guerra” (Bartles 2016, 55), en gran medida a partir de lo ocurrido en la “primavera árabe” y en las “revoluciones de colores”. En ellas observa un aumento de medios no militares, como elementos políticos, económicos, humanitarios, operaciones encubiertas, así como la importancia de la información (Gerasimov 2013). Por su parte, Rusia considera que el concepto de guerra híbrida es un término occidental y, por lo tanto, distinto a su sistema doctrinal (Bartles 2016, 59; Palacios 2016b, 22-23). De hecho, los rusos hacen referencia a distintos términos relacionados con la guerra híbrida, como “guerra no lineal” (*nelinnearnaya voyna*), “guerra ambigua” (*neopredelonnaya voyna*) y “guerra de redes” (*setovaya voyna*) (Milosevich 2017, 2).

Tres años después, Gerasimov (2016) publicó un nuevo artículo en el que expuso algunas ideas sobre las guerras contemporáneas (de forma similar al documento anterior), pero en el que añadió las experiencias de los conflictos de Ucrania y Siria. Gerasimov identifica los métodos híbridos en las revoluciones de colores y afirma que estos movimientos son, de hecho, golpes de Estado promovidos por Occidente (Palacios 2016a; Gerasimov 2016). A diferencia del artículo de 2013, este documento hace referencia de forma abierta a las guerras híbridas y a los métodos híbridos, pero de forma distinta a Occidente.

8 Hasta el inicio del conflicto en Ucrania, en 2014, las referencias a los conflictos híbridos no se relacionaban de manera específica con Rusia (Palacios 2016b, 23).

9 Este término tampoco se encuentra en la Doctrina Militar 2014, pero sí lo utilizarían Gerasimov y asesores del presidente Vladimir Putin (Milosevich 2015, 5).

Como se ha señalado anteriormente, la guerra híbrida combinaría métodos convencionales e irregulares –en los que encontraríamos vínculos con el crimen organizado o grupos terroristas–, mientras que, según Palacios (2016a), Gerasimov considera que

en los conflictos contemporáneos es cada vez más frecuente que se dé prioridad a un uso conjunto de medidas de carácter no militar, políticas, económicas, informativas y de otro tipo, que se ponen en práctica con el sostén de la fuerza militar. Son los llamados métodos híbridos.

En la práctica, esto supondría una percepción más limitada de las acciones híbridas que la que tiene Occidente. A pesar de esa diferencia, el autor sostiene que la combinación de actividades tradicionales e híbridas es una característica de los conflictos armados contemporáneos, en los que señala al elemento informativo como el principal de los métodos híbridos. Esto debido a que

la falsificación de los acontecimientos, la limitación de la actividad de los medios de información, se convierten en uno de los métodos asimétricos más eficaces para la conducción de las guerras. Su efecto puede ser comparable a los resultados de un uso masivo de tropas (Palacios 2016a).

En definitiva, Gerasimov hace referencia a la guerra y los métodos híbridos porque considera que Rusia puede tener que enfrentarse a este tipo de guerras y, por ello, debe conocerlas y adaptarse a ellas (Palacios 2016b, 26-27). Además, hay que tener en cuenta que Gerasimov lo plantea en un escenario de guerra armada, mientras que las campañas de desinformación y noticias falsas desde Occidente se realizarían en un contexto de tensión y confrontación

política y social, pero en ausencia de conflicto armado. Por último –y no por ello menos importante–, Mark Galeotti (2018), el analista que acuñó el término doctrina Gerasimov, no solo ha negado la existencia de esa supuesta doctrina, sino que además señala que el artículo de Gerasimov pretendía resolver cómo luchar contra las acciones no convencionales, no promoverlas.

Conclusiones

Es habitual encontrar noticias relacionadas con las campañas de desinformación de origen ruso que afirman que estas se inscriben en un contexto de guerra híbrida contra Occidente. El principal problema de las informaciones periodísticas aquí expuestas reside en que, en su mayoría, los autores no exponen ni siquiera una breve aproximación a los conceptos utilizados, su significado e implicaciones –como pueden ser desinformación, *fake news*, ciberguerra o guerra híbrida–. En ocasiones, ello conduce a la utilización de algunos de estos conceptos como sinónimos. Posiblemente, una de las razones de la confusión es la mezcla entre el uso de conceptos recientes –en este caso, aquellos relacionados con el ciberespacio– con otros que se ubican tradicionalmente en un ámbito militar y académico, en un intento de querer informar sobre los cambios que se están produciendo en el escenario internacional. Pero también podría deberse en parte a la espiral en la que los medios de comunicación han entrado, empujados por una demanda constante de información por parte de los ciudadanos, al querer informar prácticamente al minuto sobre las últimas noticias, lo cual implica apostar por la cantidad antes que por la calidad.

Sin duda, el uso del ciberespacio y de la información por parte de Rusia han sido el eje central de las noticias relacionadas con la guerra híbrida. Pero si bien es cierto que ese país ha fomentado el uso de las operaciones de información y ha sabido aprovechar el potencial del ámbito digital a favor de sus intereses, también lo es que el desarrollo de campañas de desinformación y el uso de las TIC no pueden identificarse exclusivamente con la guerra híbrida. Una de las características de los conflictos híbridos consiste en la combinación de distintos elementos convencionales y asimétricos, pero las noticias se han centrado casi exclusivamente en el elemento digital, a través del cual se han desarrollado las campañas de desinformación, las noticias falsas y el uso masivo de las redes sociales. A pesar de que pueden formar parte de los conflictos híbridos y de que en los últimos años el elemento ciber está adquiriendo una enorme importancia en los conflictos, no podemos señalar que estas actividades sean *la* guerra híbrida.

Difícilmente un único Estado podría desarrollar de forma simultánea guerras de este tipo –si tenemos en cuenta los elementos militares y no militares– contra todos los Estados occidentales que han denunciado estas actividades, desde EEUU hasta Alemania, Francia, Reino Unido y España. Por otro lado, la guerra híbrida no es en ningún caso una estrategia exclusiva de Rusia –ni forma parte de una doctrina militar rusa– sino que puede ser desarrollada por otros actores estatales que tengan la voluntad y los recursos necesarios, así como por actores no estatales. Nada permite determinar la exclusividad rusa.

Por lo tanto, si concluimos que los acontecimientos que tuvieron lugar en el *Brexit*, en las elecciones estadounidenses y en el conflicto catalán no pueden calificarse como guerra hí-

brida, un marco de análisis para comprender las novedades que comporta el ciberespacio y su impacto en las relaciones internacionales en estos escenarios podría desarrollarse desde el concepto de la *gray zone* o zona gris. El concepto define aquellas actividades bajo el umbral del conflicto, que se realizan en tiempos de paz, a diferencia de la guerra híbrida, y que incluyen ataques informáticos o campañas de desinformación y propaganda que tendrían como característica común la dificultad de determinar su atribución. Ese concepto permitiría, por lo tanto, un análisis de las actividades que no se califican específicamente como de guerra, pero que podrían llegar a ser tan decisivas como un conflicto militar.

El análisis presentado en el artículo se ha centrado en la importancia de conceptualizar y de contextualizar los hechos de los que se informa. Es evidente que el ejercicio del periodismo difiere del ámbito académico, pero también es cierto que las noticias deben transmitir el mayor rigor posible y exponer al lector lo que sucede en su contexto concreto, intentando utilizar conceptos adecuados en cada caso. Todavía nos encontramos en una fase temprana del análisis de las capacidades que tiene el ciberespacio, y reducirlo únicamente al uso que puede hacer un único Estado para la difusión de campañas de propaganda supone no comprender su potencial en las relaciones internacionales.

Bibliografía

- Adam, Karla y William Booth. 2017. “Rising Alarm in Britain over Russian Meddling In Brexit Vote”. *The Washington Post*, 17 de noviembre. <https://wapo.st/2Ordvoz>
- Baqués, Josep. 2015a. “El papel de Rusia en el conflicto de Ucrania: ¿La guerra híbrida de

- las grandes potencias?”. *Revista de Estudios de Seguridad Internacional* 1 (1): 41-60. dx.doi.org/10.18847/1.1.3
- Baqués, Josep. 2015b. “Las guerras híbridas: un balance provisional”. *Instituto Español de Estudios Estratégicos*, Documento de Trabajo. <http://bit.ly/2XZAEFY>
- Bartles, Charles K. 2016. “Cómo comprender el artículo de Gerasimov”. *Military Review*, marzo-abril. <http://bit.ly/2OyFpTY>
- Baunov, Alexander. 2016. “A Multipolar Europe: Why Russia likes Brexit”. *Carnegie Moscow Center*, 28 de junio.
- BBC. 2016. “Brexit: What happens now?”. 29 de junio, <https://www.bbc.com/news/uk-politics-eu-referendum-36420148>
- Boffey, Daniel. 2018. “EU raises funds to fight ‘disinformation war’ with Russia”. *The Guardian*, 5 de diciembre. <http://bit.ly/33ASH6x>
- Boffey, Daniel, y Jennifer Rankin. 2017. “EU escalates its campaign against Russian propaganda.” *The Guardian*, 23 de enero. <http://bit.ly/2rzPpDA>
- Branford, Becky. 2017. “Information warfare: Is Russia really interfering in European states?”. *BBC News*, 31 de marzo. <https://www.bbc.com/news/world-europe-39401637>
- Campos, Miguel. 2018. “El arte operacional ruso: de Tikhachevsky a la actual ‘Doctrina Gerasimov’”. *Instituto Español de Estudios Estratégicos*, Documento de Opinión. <http://bit.ly/34wluuo>
- Caryl, Christian. 2017. “The great Catalan cyberwar of 2017”. *The Washington Post*, 18 de octubre. <https://www.washingtonpost.com/news/democracy-post/wp/2017/10/18/the-great-catalan-cyberwar-of-2017/>
- Clarke, Richard A., y Robert K. Knake. 2010. *Cyber War: the next threat to national security and what to do about it*. EEUU: HarperCollins Publishers.
- Cohen, Nick. “Why isn’t there greater outrage about Russia’s involvement in Brexit?”. *The Guardian*, 17 de junio. <https://www.theguardian.com/commentisfree/2018/jun/17/why-isnt-there-greater-outrage-about-russian-involvement-in-brexit>
- Colás, Xavier. 2017. “La ciberguerra, amenaza estrella en 2017”. *El Mundo*, 6 de enero. <http://bit.ly/2pZLOsW>
- Colom, Guillem. 2012. “Vigencia y limitaciones de la guerra híbrida”. *Revista Científica General José María Córdova* 1 (10), junio: 77-90. doi.org/10.21830/19006586.228
- Colom, Guillem. 2018. “La Doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo”. *Revista Ejército* 933, diciembre. <https://www.ugr.es/~gesi/Doctrina-Gerasimov.pdf>
- Colom, Guillem. 2019. “La amenaza híbrida: mitos, leyendas y realidades”. *Instituto Español de Estudios Estratégicos*, Documento de Trabajo. http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO24_2019GUICOL-hibrida.pdf
- Coy, Peter. 2016. “After Brexit, here’s what’s next for Europe”. *Bloomberg*, 30 de junio. <https://www.bloomberg.com/news/features/2016-06-30/after-brexit-here-s-what-s-next-for-europe>
- De Pedro, Nicolás. 2017. “Rusia se apunta a la guerra híbrida”. *El País*, 19 de noviembre. https://elpais.com/elpais/2017/11/18/opinion/15111025644_093966.html
- El País. 2017. “Guerras Híbridas”. 4 de diciembre. https://elpais.com/elpais/2017/12/03/opinion/1512325245_721922.html
- Faus, Joan. 2018. “Estados Unidos acusa a Rusia de tratar de interferir en la campaña de las legislativas”. *El País*, 3 de agosto. https://elpais.com/internacional/2018/08/02/estados-unidos/1533235587_731224.html
- Gamboa, Juan A. 2017. “Amenaza Híbrida, ¿un concepto doctrinal?”. *Revista Ejército* 921, diciembre: 26-43. http://www.ejercito.mde.es/Galerias/multimedia/revista-ejercito/2017/921//accesible/Revista_Ejercito_Accesible.pdf
- García, Miguel, y Gabriel Martínez-Valera. 2015. “La guerra híbrida: nociones prelimi-

- nares y su repercusión en el planeamiento de los países y organizaciones occidentales”. *Instituto Español de Estudios Estratégicos*, Documento de Trabajo. <http://bit.ly/34A06nY>
- Galeotti, Mark. 2018. “I’m sorry for creating the ‘Gerasimov Doctrine’”. *Foreign Policy*, marzo. <https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/>
- Gerasimov, Valeri. 2013. “Ценность науки в предвидении”. *VPK* 476 8, marzo. <https://vpk-news.ru/articles/14632>
- Gerasimov, Valeri. 2016. “По опыту Сирии”. *VPK* 624 9, marzo. <https://vpk-news.ru/articles/29579>
- Hoffman, Frank G. 2007. *Conflict in the 21st Century. The Rise of Hybrid Wars*. Virginia: Potomac Institute for Policy Studies. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
- Johnson, Robert. 2018. “Hybrid War and Its Countermeasures: A Critique of the Literature”. *Small Wars & Insurgencies* 1 (29): 141-163.
- Kendall, Bridget. 2014. “Qué es la nueva ‘guerra híbrida’ entre Rusia y Occidente”. *BBC Mundo*, 7 de noviembre. https://www.bbc.com/mundo/noticias/2014/11/141106_guerra_hibrida_rusia_occidente_jgc
- Milosevich, Mira. 2015. “¿Por qué Rusia es una amenaza existencial para Europa?”. *Real Instituto Elcano* 35/2015, julio. <http://bit.ly/2R0otau>
- Milosevich, Mira. 2017. “El poder de la influencia rusa: la desinformación”. *Real Instituto Elcano*, ARI 7/2017, enero. <http://bit.ly/37LSAZk>
- Palacios, José Miguel. 2016a. “La doctrina Gerasimov: segunda entrega”. *GESI*, Análisis 7/2016 (abril). <http://bit.ly/2qXviiC>
- Palacios, José Miguel. 2016b. “Rusia: guerra híbrida y conflictos asimétricos”. *Revista Ejército* 904, julio-agosto: 22-27. <http://bit.ly/2L8hmZX>
- Pérez, Paula. 2017. “La guerra híbrida amenaza a España”. *Estrella Digital*, 1 de diciembre. <http://bit.ly/34A0AdM>
- Pueyo, Jordi. 2017. “Ciberguerra entre los gobiernos catalán y español por el cierre de la web del referéndum”. *El País*, 14 de septiembre. https://elpais.com/ccaa/2017/09/14/catalunya/1505390726_024743.html
- Roig, Clara. 2018. “Las guerras de la era de la desinformación”. *La Vanguardia*, 29 de abril. <http://bit.ly/34BIVfq>
- Schnauffer, Tad A. 2017. “Redefining Hybrid Warfare: Russia’s Non-linear War against the West”. *Journal of Strategic Security* 1 (10): 17-31.
- The Economist. 2017. “Russian Twitter trolls meddled in the Brexit vote. Did they swing it?”. 23 de noviembre. <https://economics/2R0gz0Z>
- Villarejo, Esteban. 2014. “La nueva guerra híbrida”. *ABC Blogs, Por Tierra, Mar y Aire*, 29 de octubre. <https://abcblogs.abc.es/tierramar-aire/otan/nuevaguerra-hibrida.html>
- Walker, Robert G. 1998. “Spec Fi: The United States Marine Corps and Special Operations”. Tesis de maestría, Naval Postgraduate School. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a359694.pdf>
- Wither, James K. 2016. “Making Sense of Hybrid Warfare”. *Connections: The Quarterly Journal* 2 (15): 73-87.

1. Información general

URVIO, Revista Latinoamericana de Estudios de Seguridad, se edita desde 2007 y es una publicación electrónica cuatrimestral (desde 2020) de la Facultad Latinoamericana de Ciencias Sociales (Flacso), sede Ecuador, y de la Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (Relasedor). Es una publicación arbitrada que utiliza el sistema de revisión externo doble ciego, conforme a las normas de publicación del estilo Chicago, versión Chicago Deusto.

URVIO está indexada en Emerging Sources Citation Index (ESCI), ERIH PLUS (European Reference Index for the Humanities and the Social Sciences), SciELO Ecuador, Redalyc (Red de Revistas Científicas de América Latina y el Caribe, España y Portugal), EBSCO, REDIB (Red Iberoamericana de Innovación y Conocimiento Científico), DIALNET y en otras bases de datos internacionales, catálogos y repositorios del mundo.

La revista se edita en español (e-ISSN: 1390-4299; ISSN: 1390-3691), además de interfaz, títulos, resúmenes y palabras clave en inglés y portugués. Cada trabajo se identifica con un DOI (Digital Object Identifier System).

1.1 Misión

URVIO constituye un espacio de difusión del conocimiento científico en el área de las ciencias sociales y políticas. Sus principios son los pluralismos, el rigor científico, el respeto a la ética, con vistas a transmitir el pensamiento académico internacional.

1.2 Idioma

URVIO publica sus artículos en español e inglés. Si recibe un artículo escrito en español, el autor, en dependencia de su disponibilidad financiera e interés, puede traducirlo al inglés por sus medios. Si recibe un artículo escrito en inglés, se realiza su evaluación y proceso editorial en ese idioma, pero si el manuscrito es aprobado para publicación, el autor, en dependencia de su disponibilidad financiera e interés, puede remitir la misma versión en español, para que la revista publique el artículo en ambos idiomas. En la revista solo se admiten traducciones profesionales.

1.3 Frecuencia de publicación

Hasta 2019, su frecuencia era semestral. A partir de 2020, URVIO es una revista cuatrimestral, con el objetivo de aumentar el impacto, la visibilidad y la actualidad. Por esas razones, publica sus tres números al año en los meses de enero, mayo y septiembre. La periodicidad corresponde a los meses enero-abril, mayo-agosto y septiembre-diciembre.

2. Enfoque y alcance

2.1 *Temática*

Artículos científicos sobre seguridad pública, seguridad privada, seguridad internacional, ciberseguridad, defensa, crimen organizado, criminología, geopolítica, inteligencia estratégica, estudios estratégicos, riesgos y prevención de desastres naturales...

2.2 *Aportaciones*

URVIO solo edita resultados de investigación sobre la seguridad y su interdisciplinariedad, escritos en español o inglés. Los trabajos deben ser originales, no haber sido publicados en ningún medio ni estar en proceso de publicación en otra revista. En los autores recae la responsabilidad de esta norma y su cumplimiento. En caso de que un autor haya publicado un artículo en URVIO tendrá que esperar dos años para volver a presentar otro trabajo.

La revista tiene tres secciones:

- Tema Central: 5.000/8.000 palabras de texto, incluyendo título, resúmenes, descriptores, tablas y referencias (en versión inglesa, máximo 7.000).
- Misceláneo: 5.000/8.000 palabras de texto, incluyendo título, resúmenes, descriptores, tablas y referencias.
- Estudios Globales: 5.000/8.000 palabras de texto, incluyendo título, resúmenes, descriptores, tablas y referencias.

URVIO, desde 2020, publica tres veces al año (21 artículos por año) y cuenta por número con cuatro trabajos en Tema Central (sección monográfica planificada, con llamada pública de envío de artículos a través de convocatorias, que coordinan especialistas en la temática; dos trabajos en Misceláneo (aportaciones variadas dentro de la temática general de la publicación, con un perfil latinoamericano); y un trabajo en Estudios Globales (aportaciones variadas dentro de la temática general de la publicación, generalmente con un perfil mundial). El Consejo Editorial asigna los manuscritos a la sección más pertinente. La revista inicia el proceso editorial de cada número seis meses antes de su publicación.

3. Proceso editorial

Las normativas para autores están disponibles en el sitio web de la revista. Incluyen las normas completas de publicación, la estructura requerida de los manuscritos y la carta de presentación, que debe contener nombre completo, nacionalidad, dirección de correo electrónico, títulos académicos, afiliación institucional actual, líneas de investigación y publicaciones recientes en libros y/o revistas. La revista acusa recepción automática de los trabajos enviados por los autores e informa por correo electrónico y en la plataforma del proceso de estimación/desestimación para siguiente fase de revisión doble ciego (período máximo de 30 días después de finalizar la convocatoria).

En caso de que el manuscrito presente deficiencias formales o no se incluya en el interés temático de URVIO, el Consejo Editorial desestimará formal o temáticamente el trabajo sin opción de vuelta.

No se mantendrá correspondencia posterior con autores de artículos desestimados.

Los manuscritos serán arbitrados de forma anónima por académicos con experiencia en la disciplina. Cada artículo será arbitrado mínimo por dos especialistas en la temática. En caso de que un artículo tenga una evaluación positiva (sí/publicable con modificaciones) y otra negativa (reevaluable con modificaciones/no), se recurrirá a un tercer evaluador para que ofrezca un desempate. Incluso, ante situaciones puntuales, se puede recurrir a un cuarto y hasta un quinto revisor. Aunque la revista respeta el contenido del manuscrito original, cuando sean requeridas, puede solicitar modificaciones moderadas o profundas, en cuanto a su extensión, estructura o estilo.

El plazo de revisión doble ciego, superada la etapa previa de recepción por parte del Consejo Editorial, es de tres meses (12 semanas) como máximo. El tiempo promedio es de mes y medio (6 semanas). Una vez recibido el dictamen de los revisores, los autores recibirán los informes de arbitraje de forma anónima. Los trabajos que sean propuestos para publicación, que requieran modificaciones (tanto menores como mayores), se devolverán en un plazo de 15 días como máximo.

Los autores de artículos aceptados, antes de la fase de diseño y maquetación, recibirán la última versión del documento en formato Word, ya con la corrección de estilo que ofrece URVIO, para su chequeo y corrección por correo electrónico. Únicamente se aceptarán correcciones mínimas sobre el contenido del manuscrito original ya evaluado. En esta etapa, el plazo máximo de entrega por parte del autor será de tres días naturales.

Una vez recibido el manuscrito en español, los autores tienen la oportunidad de presentar el artículo en lengua inglesa (según la posibilidad e interés de cada autor). Publicar el manuscrito en ambos idiomas garantizan mayor impacto y difusión internacional. El texto traducido de manera obligatoria tiene que tener calidad profesional.

En general, una vez vistas las revisiones científicas externas, los criterios que justifican la decisión sobre la publicación o no de los trabajos por parte del Consejo Editorial se basan en los siguientes puntos:

- a) Conocimiento actual y estratégico.
- b) Originalidad.
- c) Fiabilidad y validez científica: calidad metodológica contrastada.
- d) Organización y presentación formal.
- e) Grado de internacionalización de la propuesta y del equipo.
- f) Buena redacción.

4. Presentación y estructura de originales

Los manuscritos deben ser enviados exclusivamente por la plataforma OJS de la revista. Los autores tienen que crearse una cuenta, con sus créditos, en la plataforma OJS, aunque uno solo será el responsable de correspondencia. Ningún autor podrá tener en revisión dos manuscritos de forma simultánea.

Los trabajos se presentarán en tipo de letra *times new roman* 12, interlineado 1,5 y justificado. Las notas al pie van con un tamaño de letra 10. Si el trabajo contiene una cita textual de más de 40 palabras, se quitan las comillas, se coloca tamaño de letras 11, interlineado sencillo y sangría a la derecha. Los trabajos se presentan en formato Word para PC. El archivo debe ser anónimo en Propiedades de archivo del documento Word, de forma que no aparezca la identificación de los autores.

4.1 Estructura

Deben subirse a la página OJS de la revista, de manera simultánea, dos archivos: 1) Carta de presentación; y el 2) Manuscrito, conforme a las normas detalladas.

A. Carta de presentación

Nombre completo, nacionalidad, dirección de correo electrónico, número de Orcid, títulos académicos, afiliación institucional actual, líneas de investigación y publicaciones recientes en libros y/o revistas.

B. Manuscrito

- Introducción (propósitos del estudio, revisión de literatura previa que funcione como estado del arte, objetivos/hipótesis y descripción de la estructura que tendrá el manuscrito).
- Metodología y soporte teórico
- Discusión y resultados
- Conclusiones
- Bibliografía

Otras orientaciones:

Título: no podrán ser mayores a 15 palabras, y deberán estar traducidos al inglés y al portugués.

Resumen: en español, traducidos al inglés y al portugués, no mayor a 200 palabras, con la siguiente estructura: 1ra y 2da oración (Introducción/objetivo), 3ra oración (Metodología/teoría) y 4ta oración (Conclusiones del manuscrito).

Palabras clave: de cinco a siete, separadas por punto y coma (;) y en orden alfabético. Recomendamos que los autores se apoyen en el Tesoro de la Unesco.

Notas al pie: solo las imprescindibles.

Recursos de apoyo (tablas, gráficos, figuras, imágenes, mapas): no más seis en todo el manuscrito. Tienen que estar presentados en el texto.

Bibliografía: No debe incluirse referencias no citadas en el artículo. Su número ha de ser suficiente y necesario para contextualizar el marco teórico, la metodología usada y los resultados de investigación en un espacio de investigación internacional. Las citas deberán extraerse de los documentos originales, preferentemente, revistas y libros.

Siglas: la primera vez que aparezcan deberá escribirse su significado completo y su sigla entre paréntesis, luego solamente, la sigla.

4.2 Normas para las referencias

Estructura Básica de una cita en el cuerpo del texto

En el sistema autor-año de Chicago Deusto, 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 debe 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)

Orden cronológico para los nombres repetidos en una lista de referencias

Las entradas se disponen cronológicamente por año de publicación en orden ascendente, no alfabétizadas 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.
Segura Munguía, Santiago. 2007. Diccionario por raíces del latín y de las voces derivadas. Bilbao: Universidad de Deusto.

Segura Munguía, Santiago. sf. Nuevo diccionario etimológico latín –español y de las voces derivadas. Bilbao: Universidad de Deusto.

Entradas de la lista de referencias con el mismo autor o autores y el mismo año

Las obras de un mismo autor 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

Chaume Varela, Frederic. 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)

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 Ascencio, 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)

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 completo 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 magazines en la lista de referencias

Ejemplo:

Lafuente, Javier. 2015. "Venezuela da la espalda al chavismo". El País, 7 de diciembre. http://internacional.elpais.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. <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 empezando por el año, separado del número por una barra, 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.

Ejemplos:

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).

(Manuela Ambas, 2 septiembre 2010)

5. Promoción y difusión del artículo

Los autores se comprometen a participar en la máxima difusión de su artículo una vez publicado, así como de toda la revista, a través de su lista de contactos, vía correo electrónico o redes sociales genéricas y académicas. En la promoción de los textos se utilizará el enlace de la página de **URVIO** (<https://revistas.flacsoandes.edu.ec/urvio/index>), y el respectivo DOI, para de esta manera aumentar la difusión del artículo en la comunidad científica.

6. Política de acceso abierto, tasas y archivos

URVIO es una revista científica de acceso abierto, gratuita para autores y lectores. No cobra tarifa alguna por el envío o el procesamiento de contribuciones académicas a autores interesados en publicar en esta revista.

6.1 Archivos

Esta revista utiliza el sistema LOCKSS para crear un sistema de almacenamiento distribuido entre las bibliotecas participantes y permite la creación de archivos permanentes en la revista con fines de conservación y restauración.

6.2 Derechos de autor

- Urvio opera bajo la licencia Creative Commons Reconocimiento-Sin Obra Derivada 3.0 Unported (CC BY-ND 3.0). Los autores/as que publiquen en Urvio aceptan estos términos:
- Usted es libre de compartir — copiar y redistribuir el material en cualquier medio o formato para cualquier finalidad, incluso comercial. Por tanto, autores conservan los derechos de autor y ceden a la revista el derecho de la primera publicación (CC BY-ND 3.0), que permite a terceros la redistribución, comercial o no comercial, de lo publicado siempre y cuando el artículo circule sin cambios.

Existen las siguientes condiciones para los autores:

- Reconocimiento — Debe reconocer la autoría, proporcionar un enlace a la licencia e indicar si se han realizado cambios. Puede hacerlo de cualquier manera razonable, pero no de una manera que sugiera que tiene el apoyo del licenciador o lo recibe por el uso que hace.
- Sin Obra Derivada — Si remezcla, transforma o crea a partir del material, no puede difundir el material modificado.

Para más detalles, visitar la página de Creative Commons (CC).

6.3 Declaración de privacidad

Los nombres y las direcciones de correo electrónico introducidos en esta revista se usarán exclusivamente para los fines establecidos en ella y no se proporcionarán a terceros o para su uso con otros fines.

Política frente al plagio académico

URVIO utiliza el programa informático Turnitin, como sistema antiplagio. El proceso de análisis se desarrolla a nivel cuantitativo y cualitativo. El porcentaje de similitud para nuestra revista será el siguiente:

- 1 a 7% Coincidencias menores. El trabajo pasa a evaluación.
- 7 a 15% Se sugiere verificación cualitativa. El artículo es devuelto al autor para cambios.
- 16% a 25% Se analiza el reporte por miembros del Consejo Científico Internacional. En caso de errores tipográficos, se devuelve al autor para que realice los cambios.
- 26% o + Se rechaza el artículo.

Código de ética

URVIO, como miembro de la Facultad Latinoamericana de Ciencias Sociales (Flacso), se compromete a promover una conducta ética como publicación científica (<https://www.flacso.edu.ec/portal/pnTemp/PageMaster/lu0e5rhzxcgogy044rl8ku4x711brc.pdf>), y además, toma como referencia también los principios publicados por el *Committee on Publication Ethics* (COPE) en el *Code of Conduct and Best Practice Guidelines for Journal Editors* (<https://publicationethics.org/resources/code-conduct>).

Instructions for publication of URVIO. Latin American Journal of Security Studies

1. General Information

URVIO, Latin American Journal of Security Studies is edited since 2007, and it is a four-monthly (since 2020) electronic publication of the Latin American Faculty of Social Sciences (FLACSO-Ecuador), and the Latin American Network for the Analysis of Security and Organized Crime (RE-LASEDOR). Is an arbitrated publication that uses the external revision system peer-blind review, according to the publication norms of Chicago style, and specifically its Chicago Deusto version.

URVIO its indexed in Emerging Sources Citation Index (ESCI), ERIH PLUS (European Reference Index for the Humanities and the Social Sciences), SciELO Ecuador, Redalyc (Scientific Journals Network of Latin America and the Caribbean, Spain and Portugal), EBSCO, REDIB (Iberoamerican Network of Innovation and Scientific Knowledge), DIALNET and in others international databases, catalogs and repositories around the world.

The journal is edited in Spanish (e-ISSN: 1390-4299; ISSN: 1390-3691) and at the same time interface, titles, abstracts, and keywords in English and Portuguese. Each work its identified with a DOI (Digital Object Identifier System).

1.1 Mision

URVIO constitute a space of diffusion of scientific knowledge in different areas of Social Science and politics. Its guidelines are the pluralism of points of view, scientific rigor, and ethical respect, in order to transmit academic thinking in an international perspective.

1.2 Language

URVIO publishes its articles in Spanish and English. If receives an article in Spanish, the author, according to his o her financial availability and interest, could translate it to English for his or her own means. If receives an article in English, the journal makes an evaluation and an editorial process in that language; but if the manuscript is approved for its publication, the author, according to his o her financial availability and interest, could send the same version in Spanish, in order to the journal publishes the article in both languages. The journal only accepts professional translations.

1.3 Publishing frequency

Until 2019, its frequency was semestral. Since 2020, URVIO is a quarterly publication, with the objective of increasing impact, visibility, and current situations. For these reasons, publish its three volumes per year in January, May, and September.

2. Focus and Scope

2.1 Topics

Scientific papers about public security, private security, international security, cybersecurity, Defense, organized crime, criminology, geopolitics, strategic intelligence, strategic studies, risks, and natural disasters prevention.

2.2 Contributions

URVIO only publish research results about security and its interdisciplinary fields, wrote in Spanish or English. The contributions have to be originals, not been published in any other media or keep in the publishing process in another journal. The authors have the responsibility to fulfill this norm. In case that an author has been published an article in URVIO, he or she needs to wait two years to present another paper.

The journal has three sections:

- Main topic: 5.000/8.000 text words, including title, abstracts, keywords, boards and references (in the English version, 7.000 words max.)
- Miscellaneous: 5.000/8.000 text words, including title, abstracts, keywords, boards and references.
- Global Studies: 5.000/8.000 text words, including title, abstracts, keywords, boards and references.

URVIO, since 2020, published three times per year (21 articles per year) and has per volume four articles in Main Topic (monographic section planned with a public and open call for papers, coordinated by an academic specialist in the main topic); two papers at Miscellaneous (multiple contributions according to the main lines of the journal, with a Latin American perspective); and one paper at Global Studies (multiple contributions according to the main lines of the journal, with a worldwide perspective). The Editorial Board select the manuscripts to the most pertinent section. The journal begins the editorial process of each volume six months before its publication.

3. Editorial process

The instructions for authors are available in the journal's web site. They describe the required structure of the manuscripts and the cover letter. The latter must include full name, nationality, email address, academic titles, current institutional affiliation, research lines and recent publications (books and/or articles). The journal sends an automatic acknowledgment of receipt to the authors and informs them by email and on the platform about the estimation/rejection process for the next phase of double-blind evaluation (maximum period of 30 days after the end of the call).

In the event that the manuscript has formal deficiencies or is not included in the thematic interest of URVIO, the Editorial Board will reject the work without an option to resend it. No further correspondence will be maintained with authors of rejected articles.

The manuscripts will be arbitrated anonymously by scholars with experience in the discipline. Each article will be reviewed by at least two specialists in the subject. In case an article receives a positive review (yes / publishable with modifications) and a negative one (re-evaluable with modifications / no), a third reviewer will provide the final decision. In specific situations, a fourth and even a fifth review may be required. Although the journal respects the content of the original manuscript, when it is required, editors may request moderate or profound changes, in terms of its extension, structure or style.

The double-blind review period, after the previous stage of reception by the Editorial Board, is three months (12 weeks) maximum. The average time is one and a half months (6 weeks). Once the reviews are received anonymous reports will be sent to the authors. Articles proposed for publication that requires modifications (both minor and major), will be returned by the authors within a maximum period of 15 days.

To authors that have been his or her articles accepted, will receive by email the latest version of the text in Word format, after style correction provided by URVIO, for its checking and correction before the design phase. Only minimal corrections to the manuscript will be accepted. In this phase, the author will have a maximum of three calendar days to return the manuscript to the editors of the journal.

Once the final version of the manuscript in Spanish have been received, the authors have the opportunity to provide a version in English (depending on the economic resources and interest of each author). Professional quality of the translation is mandatory. Publishing the manuscript in both languages ensures greater impact and international dissemination.

In general, after the external scientific reviews are examined, justification criteria for the decision on the publication or rejection of the article by Editorial Board is based on the following points:

- a) Current and strategic knowledge
- b) Originality.
- c) Reliability and scientific validity: proved methodological quality.
- d) Organization and formal presentation.
- e) The geographical location of the paper and the authors.
- f) Good writing.

4.1 Structure

They must be uploaded to the OJS page of the magazine, simultaneously, two files: 1) Letter of presentation; 2) and the manuscript, according to detailed norms.

A. Letter of presentation

Full name, nationality, email address, Orcid number, academic titles, current institutional affiliation, research lines of the authors, and recent publications in books and/or journals.

B. Manuscript

- Introduction (proposal of the study, previous review of the literature, objectives, hypotheses, and a description of the structure of the paper).
- Methodology and theoretical perspective
- Discussion and results
- Conclusions
- Bibliography

Another orientations:

Title: Couldn't be more than 15 words, and should be translated to English and Portuguese.

Abstract: in Spanish, translated to English and Portuguese, no more than 200 words, as the following instructions: 1st and 2nd sentence (introduction/objective) 3rd sentence (methodology/theory), and 4th sentence (conclusions of the paper).

Keywords: since five to seven, separated with a semicolon (;) and in alphabetical order. We suggest to authors finds support in the Thesaurus index from Unesco.

Footnotes: Only the essential commentaries.

Support resources (boards, graphics, figures, images, maps): no more than six in the whole manuscript. The support resources have to be presented in the text.

Bibliography: references not quoted, should not be included in the article. The number of the references should be enough to context the theoretical framework, used methodology and the results of the investigation, in international context research. Quotes should be extracted from original documents, primarily books and journals.

Acronym: the first time that they appear, it should be written its full meaning and its acronym in brackets; then, only the acronym.

4.2 Norms for references

Basic structure of a quote in the body of the text

In the system year-author of Chicago Deusto, reference in the text usually appear in brackets and have just the two first elements mentioned in the reference list: author and the year of publication, without punctuation between them. Further, it needs to add the page number or another element of reference after a coma. In no case use op. cit., ibid, ibidem.

Example:

(Cox 2010)
(Cox 2010, 91)

Chronological order to the repeated names in the reference list

References are placed chronologically according to the year of publication, in ascending order, not literate by title. References without date (branded as s.f.) or in the press, are placed after references dated.

Example:

Segura Munguía, Santiago. 2005. Los jardines en la Antigüedad. Bilbao: Universidad de Deusto.
Segura Munguía, Santiago. 2007. Diccionario por raíces del latín y de las voces derivadas. Bilbao: Universidad de Deusto.
Segura Munguía, Santiago. sf. Nuevo diccionario etimológico latín –español y de las voces derivadas. Bilbao: Universidad de Deusto.

References in the list with the same author(s) and the same year of publication

References of the same author and the same year should be diferenced with the edition as a, b, c, etc., and they are placed chronologically by title. Quotations in the text consign the author and the year with the letter.

Example:

Chaume Varela, Frederic. 2004a. Cine y traducción. Cátedra: Madrid
Chaume Varela, Frederic. 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)

Book by one author or editor

Example:

Duch, Lluís. 1998. Mito, interpretación y cultura. Barcelona: Harder
(Duch 1998, 99-100)

Book by two or three authors

In the case of books by two authors, in the list of references just put differently the first name.

Example:

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)

Book by three authors

Example:

Borrego Nieto, Julio, José J. Gómez Ascencio, y Emilio Prieto de los Mozos. 1986. El subjuntivo. Valores y usos. Madrid: SGEL.
(Borrego Nieto, Gómez Ascencio y Prieto de los Mozos 1986)

More than four authors

If the book has four or more authors, it includes all of them at the beginning of the references (bibliography). The order and punctuation are the same in the case of books by two or three authors. In the text, nevertheless, it needs to indicate the last name of the author that appears in the first place, followed of et al.

Example:

(Lago et al. 2008, 118-19)

Book chapter

Example:

Gómez Mendoza, Josefina. 2009. "Ecología urbana y paisaje en la ciudad". En La ciudad del futuro, edited by Antonio Bonet Correa, 177-217. Madrid: Instituto de España.

Articles from a scientific journal

The element that should be considered in the reference are as the following: complete name of the author(s), year of publication, title and subtitle of the article, name of periodical publication, information about volume, number, date; page indication when its necessary, and the URL or DOI references when are available.

Example:

Bernárdez, Enrique. 2000. "Estrategias constructivistas de la descripción oral". Revista Española de Lingüística 30 (2): 331-356.

Articles in newspapers and magazines in the list of references

Example:

Lafuente, Javier. 2015. "Venezuela da la espalda al chavismo". El País, December 7th. http://internacional.elpais.com/internacional/2015712/077america/1449454340_373673.html

Article without signature taken from newspapers or magazines from internet

Example:

Mundo Diner. 2014. “Japón, una nación que combina la modernidad con tradiciones y costumbres ancestrales”. December 29th. <http://www.revista-mundodiners.com/?p=4509>

Electronic documents in a web page

Example:

Senescyt. 2011. “Becas docentes universitarios”, <http://programasbecas.educacionsuperior.gob.ec/becas-para-docentes-universitarios/>

Presentation made in a congress, conference, and others

Example:

Castro Gómez, Santiago. 2013. “El Dasein como Design: sobre el concepto de antropotécnica en Peter Sloterdijk”. Presentation made at the colloquium Poder, vida y subjetivación, Universidad Nacional, Bogotá, April 14th.

Thesis

Example:

Black, John. 1999. “The making of an Indigenous Movement”. Master’s Thesis, Universidad de Nuevo México.

Legal rules

Norms the field of law are quoted indicating the following elements: kind of norm, number, and date, beginning with the year, separated from the number by a dash, without interspaces, day and month between coma, the full name of the norm as the original publication; place and date of the publication.

Examples:

Organic Law 8/ 1980, from September 22th, about Financing of the Autonomous Communities (BOE núm.236 of October 1st, 1980), LOFCA since now.

Ley 14/2007, de 26 de noviembre, del Patrimonio Histórico de Andalucía (BOJA núm. 248 de 19 de diciembre de 2007).

Unpublished interviews and personal communications

Example:

Real name or fictitious (any identifying element relevant to the context of the interview: example position / occupation / residence), day, month and year. The interview does not have to be in the bibliography. With its reference in the text is enough.

(Manuela Ambas, Miraflores Neighborhood, Perú, September 2nd, 2010).

(Manuela Ambas, September 2nd, 2010)

5. Promotion and dissemination of the article

The authors agree to participate in the dissemination of their published articles, as well as the entire journal, through their contact list, via email or generic and academic social networks. In order to promote each text, the link to the URVIO page (<https://revistas.flacsoandes.edu.ec/urvio/index>) will be used, as well as the respective DOI of the article, to increase its dissemination in the scientific community.

6. Open access policy, rates and files

URVIO is a scientific open access journal, free for authors and readers. The journal does not charge any fee for the sending or processing of academic contributions to authors interested in publishing in it.

6.1 Files

This journal uses the LOCKSS system to create a distributed storage system among participating libraries and allows the creation of permanent archives in the journal for conservation and restoration purposes.

6.2 Copyright

URVIO operates under the Creative Commons Attribution-No Derivatives 3.0 Unported license (CC BY-ND 3.0). The authors that publish in URVIO accept these terms:

You are free to share - copy and redistribute the material in any medium or format for any purpose, including commercial ones. Therefore, authors retain the copyright and assign to the journal the right of the first publication (CC BY-ND 3.0), which allows third parties redistribution, commercial or non-commercial, of the published as long as the article circulates without changes and respects the following conditions:

- Recognition – the article must recognize authorship, provide a link to the license and indicate if changes have been made. You can do it in any reasonable way, but not in a way that suggests that you have the support of the licensor or receive it for the use you make.

- No Derivative Work - If you remix, transform or create from the published material, you cannot disseminate the modified material.

For more details, visit the Creative Commons (CC) page.

6.3 Privacy statement

The names and email addresses entered in this journal will be used exclusively for the purposes established in it and will not be provided to third parties or for their use or for other purposes.

7. Policy against academic plagiarism

URVIO uses Turnitin software as an anti-plagiarism system. The process of analysis is both quantitative and qualitative. We handle percentages of similarity in the following way:

- 1 to 7%: Minor matches. The article goes to the evaluation phase.
- 7 to 15%: Qualitative verification is suggested. The article is returned to the author for changes.
- 16% to 25%: The Turnitin report is analyzed by members of the International Scientific Board. In case of typographical errors, the article is returned to the author for changes.
- 26% or +: The article is rejected.

8. Ethical Code

URVIO, as a member of the Latin American Faculty of Social Sciences (FLACSO), is committed to promoting ethical behavior as a scientific publication (<https://www.flacso.edu.ec/portal/pnTemp/PageMaster/lu0e5rhzxxgogy044rl8ku4x711brc.pdf>). It also takes as reference the principles published by the *Committee on Publication Ethics* (COPE) in the *Code of Conduct and Best Practice Guidelines for Journal Editors* (<https://publicationethics.org/resources/code-conduct>).

The Editorial Board and the International Advisory Board of URVIO, Latin American Journal of Security Studies, will ensure that editors, peer reviewers, and authors respect ethical principles during all phases of the entire editorial process. In this perspective, we detail our norms to the entire academic community.

