Aproximación al panorama actual de la Protección de Infraestructuras Críticas en Colombia[1]

1

https://doi.org/10.21830/9789585380226.01

Julio César González Rodríguez[2]
Universidad Militar Nueva Granada
Christian Acevedo Navas[3]
Escuela Militar de Cadetes "General José María Córdova"

Resumen. En este capítulo se analiza el estado actual de la Protección de Infraestructuras Críticas en Colombia. El diseño metodológico es mixto: primero cualitativo, mediante análisis de contenido de la literatura conceptual y normativa a una muestra de trece países destacados, la Unión Europea y Colombia. Segundo, cuantitativo, en el cual se analizan estadísticamente las cifras sobre atentados a la Infraestructura Crítica colombiana. Los hallazgos muestran que si bien no hay un consenso conceptual ni sobre los sectores críticos que cada país prioriza, sí hay unos sectores comunes que se destacan. Los análisis muestran que Colombia está rezagada frente al mundo en cuanto a la legislación sobre este tema, aunque muestra avances en ciberseguridad e intentos legislativos previos que no se han logrado concretar. Finalmente, se concluye que a Colombia le conviene definir los sectores críticos, su nivel de criticidad y sus nodos y enlaces para formular una Política Nacional de Protección de la Infraestructura Crítica, aún no resuelta.

Palabras clave: carretera; defensa; hidrocarburo; infraestructura energética; infraestructura vial; política energética; Protección de Infraestructuras Críticas.

---

1 Este capítulo se deriva parcialmente del desarrollo de una tesis doctoral, a cargo de uno de los autores. No recibe financiación externa diferente del propio pecunio del autor. Los puntos de vista que se presentan en este capítulo pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

2 Estudiante del Doctorado en Gestión de la Universidad Ean. Magíster en Ciencias de la Seguridad y Criminología de la Universidad Católica de San Antonio. Administrador marítimo de la Escuela Naval de Cadetes "Almirante Padilla". Docente investigador de la Universidad Militar Nueva Granada (Umng), Bogotá, D. C., Colombia. Orcid: https://orcid.org/0000-0003-1280-2230 - Contacto: julio.gonzalezr@unimilitar.edu.co

3 Doctor en Ciencias Sociales. Coordinador de Investigaciones de la Facultad de Administración de la Escuela Militar de Cadetes "General José María Córdova" (Esmic), Bogotá, D. C., Colombia. Orcid: https://orcid.org/0000-0003-4880-3024 - Contacto: christian.acevedo@esmic.edu.co

Introducción

Particularmente a partir de los atentados terroristas del 9/11 en Estados Unidos, gran parte del mundo comenzó a tomar conciencia de la importancia y la vulnerabilidad de ciertos tipos de infraestructuras que son claves para el funcionamiento normal de la sociedad. También, con el aumento de la informática como un ámbito de importancia transversal a diversos sectores y la necesidad de protegerlo, se ha ido consolidando un cuerpo teórico, conceptual y normativo de lo que se denominan Infraestructuras Críticas (Ic) y Protección de Infraestructuras Críticas (Pic). El propósito de este trabajo es analizar el estado actual de esta temática en Colombia, para lo cual se revisa el panorama conceptual y normativo de la Pic en el mundo y en Colombia, y luego se analizan las principales cifras disponibles sobre atentados terroristas (At) a la Ic en Colombia.

Métodos

Se planteó un diseño metodológico mixto, de alcance descriptivo, mediante la consulta de fuentes secundarias. En primer lugar, se desarrolló una metodología cualitativa mediante análisis de contenido de la literatura sobre Pic, tanto desde los conceptos como desde las normas. Posteriormente, se aplicó una metodología cuantitativa para hacer el análisis estadístico de las cifras sobre At a la Ic colombiana.

Por cuanto no existe un observatorio o reporte sobre Ic mundial, se previó una muestra de países sobre los cuales hacer la indagación. Este muestreo se basó en tres criterios: primero, que los países estén incluidos en el estudio de Ritter y Weber (2004); segundo, que sean parte de la Otan, y, tercero, que estén incluidos en el *Global Firepower Ranking 2019.* De esta manera, la muestra quedó conformada por 13 países, más la Unión Europea (Ue), por su rol de eslabón normativo.

Respecto a Colombia, se revisaron diversos documentos relacionados con la Pic en los ámbitos jurídico y conceptual, además se recurrió a cifras del Ministerio de Defensa para hacer el análisis de los atentados a la Ic. Así,

teniendo en cuenta las limitaciones de información disponible sobre esta temática, se seleccionaron países, documentos conceptuales, normativos y cifras de atentados contra la Ic, con los cuales se configuró una muestra no probabilística por conveniencia.

Resultados y discusión

En esta sección se presentan los principales hallazgos, análisis y discusión relacionados con el panorama conceptual y normativo de la protección de infraestructuras críticas en el mundo y en Colombia, así como los atentados terroristas contra la infraestructura crítica colombiana.

Panorama conceptual y normativo de la Protección de Infraestructuras Críticas en el mundo

Cada nación es independiente en su postura frente a las Ic. Si bien la Pic ha resurgido globalmente a partir de los atentados del 9/11 en los Estados Unidos, su planteamiento se remonta a la Guerra Fría (Gheorghe *et al.*, 2018). Así, por ejemplo, Alemania define su Pic después del 9/11 y la inundación por el río Elba (2002). El gobierno alemán asumió las Ic como estructuras organizacionales o físicas de tal importancia para la sociedad y la economía, que cualquier fallo resultaría en afectación al suministro, la seguridad pública y otras consecuencias, e incluyó sectores como energía, Tic, transporte, agua y aguas residuales, salud pública, alimentación, emergencia y rescate, parlamento, gobierno, administración pública, finanzas, aseguramiento de negocios y cultura. Australia, también impulsado por el 9/11, creó con Nueva Zelanda el Comité Contra Terrorismo Anzctc (Australia-New Zealand Counter-Terrorism Committee) (Rothery, 2005) y definió la Ic como instalaciones físicas, cadenas de abastecimiento, tecnologías de información (Ti) y redes de comunicación, que si fueran afectadas podría impactar el bienestar social y económico de la nación. De esta manera, incluyeron sectores como energía, agua, alimentos, salud, transporte, finanzas y banca, y comunicaciones.

Canadá, que asumió conceptos de Pic desde la Guerra Fría, define la Ic como procesos, sistemas, instalaciones, tecnologías, redes, activos y servicios esenciales para la salud, la seguridad, el bienestar y la seguridad económica de los canadienses y el funcionamiento del gobierno (Gouvernement du Canada, 2009). Entre estos sectores se incluyen: salud, comida, finanzas, agua, Tic, seguridad, energía, manufactura, gobierno y transporte. En China, el presidente Xi Jinping mencionó que los sectores que requieren protección informática son: finanzas, energía, telecomunicaciones, transporte y gobierno (Lu, 2018). Además, la Administración China del Ciberespacio evaluaría la seguridad de la información en los sectores: gobierno, energía, finanzas, transporte, agua, salud, educación, seguridad social, medio ambiente, computación en la nube, defensa nacional, manufactura, industria química, alimentación y medicamentos (Davis Wright Tremaine [Dwt], 2017).

España aprobó el primer catálogo nacional de Ic en el 2007 (Caro, 2011) y luego creó el Centro Nacional de Coordinación Antiterrorista (Enamorado, 2005). Este país define las Ic como infraestructuras cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación tendría grave impacto sobre servicios esenciales. Se incluyen sectores como administración, espacio, investigación, industria nuclear y química, agua, energía, salud, Tic, transporte, alimentación, finanzas e impuestos (Ley 8 de 2011). Estados Unidos puso la Pic en cabeza del Department of Homeland Security, y define la Ic como activos y sistemas que son tan importantes, que su incapacidad o destrucción podría tener un impacto debilitante en seguridad, economía y/o salud pública (Department of Homeland Security [Dhs], 2003). Incluyen estos sectores: química, comercio, comunicaciones, manufactura crítica, represas, defensa, emergencias, energía, finanzas, comida, agricultura, gobierno, salud, Tic, energía nuclear, transporte, agua y alcantarillado.

Francia define las Ic como aquellas instituciones, estructuras e instalaciones que proveen los bienes y servicios esenciales de la sociedad francesa (General Secretariat for Defence and National Security [Sgdsn], 2011). Se incluyen sectores como comida, agua, salud, actividades civiles, legales y militares, energía, finanzas, transporte, comunicación, tecnologías y radiodifusión, industria, espacio e investigación. Las Ic informáticas están en la Estrategia

Nacional Francesa para la Seguridad del Ámbito Digital, con un estatus de asunto de interés nacional (República Francesa, 2015).

India define la Ic como medios computacionales cuya incapacitación tendría un impacto en seguridad, economía, salud y seguridad pública (Indian Ministry of Law, 2009). El Centro Nacional de Pic informática incluye los siguientes sectores: transporte, energía, banca, finanzas y seguros, telecomunicaciones, empresas públicas y gobierno. Singh *et al*. (2014) proponen: agricultura y comida, telecomunicaciones, banca y finanzas, manufactura crítica, defensa, emergencias, energía, salud, Ti, monumentos, servicio postal, transporte y agua.

Italia define la Ic como cualquier infraestructura pública o privada cuya operación es esencial para la seguridad y el funcionamiento del país. Incluye sectores como energía, redes de Ti, transporte, defensa, banca y finanzas, salud nacional, agua, transporte, redes de información pública, agricultura y alimentos y gobierno (Istituto Superiore delle Comunicazioni e Tecnologie dell'Informazione [Iscom], 2005). Aunque en este país hay una ausencia parcial de legislación sobre Pic, con excepción de las Ic cibernéticas, se encuentra que la Pic en general forma parte de la estrategia de seguridad nacional (Di Camillo & Marta, 2009).

Japón formuló el Plan de Seguridad en la Información en el 2005 (Brunner & Suter, 2008) y define las Ic como aquellas entidades del gobierno que proveen servicios esenciales para garantizar la vida social y las actividades económicas de las personas, las cuales serían afectadas en caso de que estos sectores fueran destruidos: telecomunicaciones, gobierno y administración, finanzas, aviación, ferrovías, logística, electricidad, gas, servicios médicos y agua.

Noruega identificó estos sectores en 1997: energía eléctrica, telecomunicaciones, transporte e información (Nystuen & Hagen, 2003). En el 2000 agregaron los siguientes: amenazas naturales, ataques humanos y sabotaje. Luego, Husdal y Brathen (2010) identificaron estos sectores: administración y gobierno, energía, combustibles fósiles, agua, telecomunicaciones, banca y finanzas, transporte, construcción e ingeniería, industria y negocios, salud, comida, bomberos y rescate, policía y orden público.

El Reino Unido define las Ic como instalaciones, sistemas, sitios, información, personas, redes y procesos necesarios para el funcionamiento de la nación y de los cuales depende la vida diaria y algunas actividades no tan vitales, pero que se vean en riesgo (Cabinet Office, 2019). Se incluyen sectores como industria química y nuclear civil, comunicaciones, defensa, emergencias, energía, finanzas, gobierno, alimentación, salud, espacio, transporte y agua. La agencia encargada de la Pic es el Centre for the Protection of National Infrastructure.

Rusia define la Ic como aquella que, en caso de daño, podría afectar la infraestructura, economía, salud y seguridad de las personas (Sneps-Sneppe *et al.*, 2016), incluyendo los siguientes sectores: organismos estatales, empresas con sistemas de información, redes de información y telecomunicaciones, sistemas de control automatizado, ciencia, transporte, comunicaciones, energía, banca y finanzas, combustibles, defensa, espacio, minería, metalurgia, química y empresas que proporcionan esta interacción (Federación Rusa, 2017).

Finalmente, en la Ue la Pic data del Tratado de Ámsterdam de 1997 (Burgess, 2007), pero los atentados del 9/11-Nueva York y 04/2004-Madrid detonaron el tema. El Programa Europeo para la Protección de Infraestructuras Críticas (Pepic) y la Directiva 2008/114 definen la Ic como el sistema o elemento situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, salud, integridad física, seguridad y bienestar socioeconómico, cuya perturbación afectaría gravemente al Estado. Los sectores incluidos fueron energía, Tic, transporte, finanzas, salud, alimentación, agua, producción y gobierno.

Panorama conceptual y normativo de la Protección de Infraestructuras Críticas en Colombia

En Colombia, la Pic es incipiente y, al igual que otros países, pareciera comenzar a partir de la informática. Si bien se creó el Grupo de Emergencias Cibernéticas Colcert y el Conpes 3854, Política Nacional de Seguridad Digital, aún no se ha legislado sobre otros sectores críticos. En el 2019 se propuso un proyecto de ley para definir el marco estratégico, jurídico y operativo de la Pic colombiana, en el cual se definieron las Ic como

> aquellas instalaciones, redes, servicios esenciales y equipos físicos y de tecnología de la información en los sectores públicos y privados, cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado en todos sus niveles de administración pública. (Proyecto de Ley 245 de 2019, p. 1)

Se proponían estos sectores: defensa y seguridad, salud, agua potable y saneamiento básico, transporte, energía, Tic, industria química y nuclear, financiero y tributario, espectro electromagnético y órbita geoestacionaria, monumentos y patrimonio, alimentación y entidades administrativas. Este proyecto no fue aprobado y el vacío legislativo permanece.

Atentados terroristas contra la Infraestructura Crítica en Colombia

La discusión sobre el concepto de *terrorismo* en Colombia es sensible, dado su conflicto interno. En la literatura se establecen cinco ondas de terrorismo: (1) de derecha, (2) etno-nacional, (3) de izquierda, (4) de crimen organizado y (5) de semi-Estados terroristas (Honig & Yahel, 2019; Rapoport, 2001). Los carteles de droga colombianos que tuvieron su apogeo en los años 80 encajan en la categoría de terrorismo de crimen organizado, mientras que la guerrilla parece encajar en la tercera onda, debido a su origen marxista-leninista. Post *et al*. (2002) catalogan a las Farc y al Eln como organizaciones de terrorismo social revolucionario, que buscan, mediante la violencia, cambiar el orden socioeconómico en Colombia. Autores como Dishman (2001) y Schmid (2011) plantean que las guerrillas colombianas no deberían ser consideradas grupos terroristas, ya que el componente político de sus actos es difuso y sus actuaciones parecen más criminales que terroristas. Ahora bien, más allá de la denominación como terroristas, criminales o insurgentes, lo cierto es que cometen actos para provocar terror. Así, para efectos de esta investigación, estos se asumen como ataques, actos o atentados terroristas (At) desarrollados por grupos armados ilegales mediante el uso de explosivos.

El Eln cometió su primer At en 1965, contra la infraestructura petrolera de Texaco en Barrancabermeja. Las Farc y el Epl también iniciaron con esta

táctica. En el periodo 1996-2005, en Colombia se presentaron 1.029 secuestros, 1.615 masacres, 1.235 desapariciones y 423 At (Feldmann & Hinojosa, 2009). Hoy hay disidencias y grupos más dispersos, que evitan la confrontación directa con las Fuerzas Militares y se han concentrado en afectar la infraestructura eléctrica, de hidrocarburos, urbana y a la población (Alzate, 2004) (tablas 1 a 3 y figura 1).

Tabla 1. Atentados Terroristas perpetrados por disidencias de las Farc (febrero 2018-abril 2020)

Dpto.	Municipios	Afectación	Tipo	Cant.
Antioquia	Yarumal	Población civil	Atentados, asesinatos	2
Arauca	Arauquita, Panamá, Saravena	Población civil, escolta	Bloqueo de vías, secuestros	3
Cauca	Buenos Aires, Caloto, Naya, Corinto, El Tambo, Popayán, Guachené, Puerto Tejada, Santander de Quilichao, Suárez, Tacueyó, Toribío	Población civil e indígena, Fuerza Pública, casco urbano, Fiscalía, guardias del Inpec, Defensoría, candidato político	Atentados; asesinatos; carros, motocicletas y cilindros bomba; ataques armados; masacres	18
Córdoba	Tierralta	Fuerza Pública y población civil	Siembra de minas antipersona	1
C/marca	Alto de las Rosas, Sumapaz	Población civil	Quema de buses	2
Ecuador	Mataje	Población civil extranjera	Secuestro y asesinato	1
Guaviare	San José del Guaviare, Calamar	Población civil, Ic energética	Casa bomba, atentado	2
Meta	Macarena	Fuerza Pública	Ataques armados	2
Norte de Santander	Catatumbo	Población civil, candidato político	Camión bomba, asesinato	2
Nariño	Tumaco	Ic energética	Atentado	2
Valle del Cauca	Florida, Jamundí	Oficina municipal, ingenio azucarero, población civil	Motocicleta bomba, asesinato, robo de armas, masacres	5

Fuente: Elaboración propia.

Tabla 2. Atentados Terroristas contra el oleoducto Caño Limón-Coveñas atribuidos por el periodismo al Eln

Vereda/municipio	Fecha(s)
Arauca	
Granada	05.02.18
Mata Oscura La Osa	28.06.18
Consuelo	11.08.18
Colorada	10.02.19
Saravena	07.06.19
Pava	25.06.19
Pajuila	04.03.19
Acacías	14.03.19
Boyacá	
Cañaguata	10.01, 08.11, 22.11.18
Granada	10.01.18
Miramar	10.01.18
Blanquita	24.10.18
Norte de Santander	
Cubugón	15.02.18
Llana Baja	05.09.18, 12.02.19
Cecilia	15.03.19
Quebrada seca	10.12.18

Fuente: Elaboración propia.

Tabla 3. Atentados Terroristas contra el oleoducto Trasandino atribuidos por el periodismo al Eln

Vereda/municipio	Fecha(s)
Nariño	
Ricaurte	13.01.18, 23.03.19
Tumaco	21.04.18
Pupiales	16.05.18
Mallama	19.01.19
Barbacoas	12.04, 18.08.19
Nariño	
Casas Frías	26.04.19
El Corzo	06.07.19
Putumayo	
El Porvenir	19.10.18

Fuente: Elaboración propia.

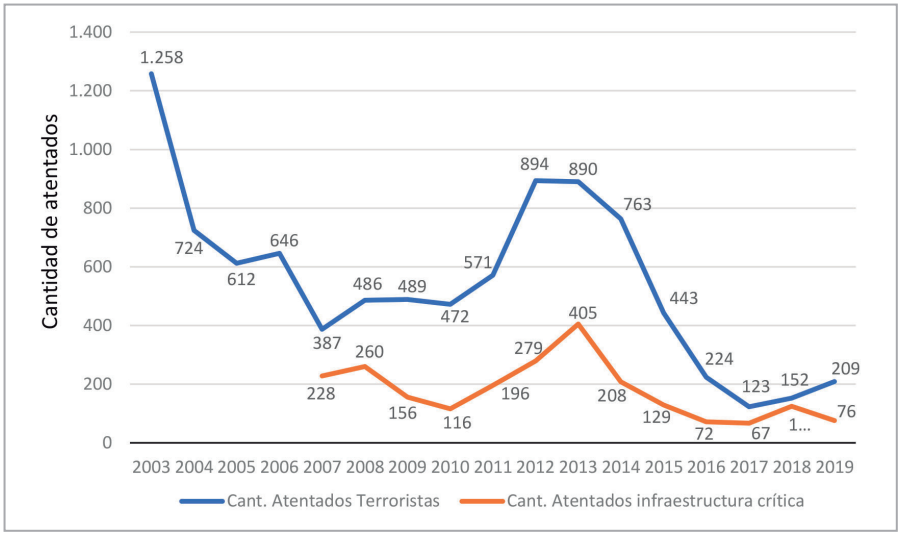

Figura 1. Atentados Terroristas contra las Infraestructuras Críticas colombianas (2003-2019). Fuente: Elaboración propia.

Como se observa en la figura 1, los atentados sobre las Ic tuvieron su peor momento durante el 2013, con 405 At. Sin embargo, estos actos representan el 45 % de los At totales. En el 2018, pese a una reducción del 70 % con 125 At respecto al 2013, representó el 82 % del total de At. En el 2019, estos atentados representaron el 36 % del total. Estas cifras arrojan una Correlación de Pearson, con una significancia bilateral de 0,00 (tabla 4). Esto indica que a mayor cantidad de At, mayor afectación de las Ic, de lo cual se infiere que la

Tabla 4. Correlación de Pearson entre Atentados Terroristas totales y Atentados Terroristas a las Infraestructuras Críticas

		Att	Atic
Atentados Terroristas Totales (Att)	Correlación de Pearson	1	0,832 *
	Significancia (bilateral)		0,000
	N	13	13
Atentados Terroristas a la Ic (Atic)	Correlación de Pearson	0,832 *	1
	Significancia (bilateral)	0,000	
	N	13	13
	* La correlación es significativa en el nivel 0,01 (bilateral).		

Fuente: Elaboración propia.

reducción de los atentados sobre las Ic no se ha logrado en virtud de la capacidad de protección, sino como consecuencia proporcional de la reducción de atentados en general.

También se evidencia que los atentados a la Ic de hidrocarburos se concentran en los oleoductos, más que en refinerías y campos petroleros. Los atentados a la Ic energética se concentran en las torres, más que en subestaciones, mientras que en la Ic vial se da una afectación semejante en vías y puentes (tabla 5).

Tabla 5. Atentados Terroristas a las Infraestructuras Críticas de hidrocarburos, vial y energética

	Ic de hidrocarburos		**Ic energética**		**Ic vial**	
Año	Oleoductos	Campos	Torres	Subestaciones	Vías	Puentes
2018	107	5	9	3	3	3
2019	71	3	0	0	5	0

Fuente: Elaboración propia.

Esto implica dos conceptos importantes sobre la Ic que ameritan ser discutidos para el contexto colombiano. Se trata de las Ic nodales y las Ic tipo enlace. *Grosso modo*, los nodos son centros vitales de procesamiento o distribución, mientras que los enlaces son líneas de comunicación o conexión entre nodos (Bouwmans *et al.*, 2006). La vulnerabilidad de un nodo se materializa cuando un evento afecta su capacidad de transferir a los enlaces, mientras que, por su parte, un enlace es crítico o está siendo vulnerado si se degrada su acceso a la red o al nodo (Murray & Grubesic, 2007). Así, para el caso de los tres sectores aquí revisados, la tabla 6 muestra una clasificación sugerida de nodos y enlaces a partir de la literatura consultada (Bullock *et al.*, 2011; Jenelius *et al.*, 2006).

Tabla 6. Clasificación sugerida de nodos y enlaces de Infraestructuras Críticas

Tipo	Ic hidrocarburos	Ic energética	Ic vial
Nodos	Campos petroleros, refinerías, zonas de almacenamiento	Hidroeléctricas, represas, parques solares, termoeléctricas, parques eólicos, subestaciones	Puertos y terminales marítimos, terrestres y aéreos
Enlaces	Oleoductos	Torres energéticas de alta, media y baja tensión, sistemas de cableado aéreo y terrestre	Canales de acceso a puertos marítimos, avenidas nacionales, carreteras departamentales e intermunicipales, puentes

Fuente: Elaboración propia.

A pesar de que los puentes se consideran enlaces, merecen un tratamiento especial, dada su alta sensibilidad y tiempos de rehabilitación en caso de que sean afectados. También son delicados los canales de acceso a los puertos marítimos, ya que, en caso de afectación, dejarían aislados los terminales. Así, por ejemplo, un At que dejase un buque obstaculizando un canal en Cartagena o Buenaventura produciría afectaciones económicas y reputacionales importantes.

Referencias

Alzate, C. (2004). Terrorismo, narcotráfico y conflicto en el caso colombiano: la cooperación internacional. *Cuadernos de Estrategia*, (126), 49-69.

Bouwmans, I., Weijnen, M., & Gheorghe, A. (2006). Infrastructures at risk. En A. Gheorghe, M. Masera, M. Weijnen, & J. De Vries (Eds.), *Critical infrastructures at risk* (pp. 19-36). Springer.

Brunner, E., & Suter, M. (2008). *International CIIP handbook 2008/2009.* Center for Security Studies ETH.

Bullock, J., Haddow, G., & Coppola, D. (2011). *Introduction to homeland security: Principles of all-hazards risk management*. Butterworth-Heinemann.

Burgess, J. (2007). Social values and material threat: The European Programme for CIP. *International Journal of Critical Infrastructures*, *3*(3-4), 471-487.

Cabinet Office. (2019). *Public summary of sector security and resilience plans 2018.* Civil Contingencies Secretariat.

Caro, M. (2011). *La protección de las infraestructuras críticas*. Documento 021/2011, Instituto Español de Estudios Estratégicos.

CONPES 3854. (2016). Política de Seguridad Digital. Departamento Nacional de Planeación.

Davis Wright Tremaine [DWT]. (2017). The Chinese Government issues draft cybersecurity regulations to protect critical information infrastructure. https://www.dwt.com/insights/2017/07/the-chinese-government-issues-draft-cybersecurity

Department of Homeland Security [DHS]. (2003). Vulnerability assessment methodologies report: Phase I final report. https://www.ojp.gov/pdffiles1/206046.pdf

Di Camillo, F., & Marta, L. (2009). *National security strategies: The Italian case* [Working Paper 39/2009]. Real Instituto Elcano.

Dishman, C. (2001). Terrorism, crime, and transformation. *Studies in Conflict and Terrorism*, *24*(1), 43-58.

Enamorado, J. (2005). Servicios de inteligencia y lucha antiterrorista. *Arbor*, *180*(709), 227-246.

Federación Rusa. (2017). *Ley sobre la seguridad de las infraestructuras críticas informáticas N 187-FZ.* Moscú. FSTEC.

Feldmann, A., & Hinojosa, V. (2009). Terrorism in Colombia: Logic and sources of a multidimensional and ubiquitous phenomenon. *Terrorism and Political Violence*, *21*(1), 42-61.

General Secretariat for Defence and National Security [SGDSN]. (2011). *The critical infrastructure protection in France.* http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf

Gheorghe, A., Vamanu, D., Katina, P., & Pulfer, R. (2018). *Critical infrastructures, key resources, and key assets.* Springer.

Global Firepower Ranking. (2019). 2019 military strength ranking. https://www.globalfirepower.com/global-ranks-previous.php

Gouvernement du Canada. (2009). National strategy for critical infrastructure. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

Hokstad, P., Utne, I., & Vatn, J. (Eds.). (2012). *Risk and interdependencies in critical infrastructures.* Springer.

Honig, O., & Yahel, I. (2019). A fifth wave of terrorism? The emergence of terrorist semi-states. *Terrorism and Political Violence*, *31*(6), 1210-1228.

Husdal, J., & Brathen, S. (2010). *Bad locations, bad logistics? How Norwegian freight carriers handle transportation disruptions.* WCTR.

Indian Ministry of Law. (2009). The information technology act, 2008. DL-N04/0007/2003-09. *The Gazette of India.*

Istituto Superiore delle Comunicazioni e Tecnologie dell'Informazione [ISCOM]. (2005). *Network security in critical infrastructures*. ISCOM.

Jenelius, E., Petersen, T., & Mattsson, L. (2006). Importance and exposure in road network vulnerability analysis. *Transportation Research Part A*, *40*(7), 537-560.

Ley 8. (2011). Por la que se establecen medidas para la protección de las infraestructuras críticas. Jefatura del Estado. BOE-A-2011-7630, España.

Lu, X. (2018). Scoping critical information infrastructure in China. *The Diplomat.*

Murray, A., & Grubesic, T. (Eds.). (2007). *Critical infrastructure: Reliability and vulnerability*. Springer.

Nystuen, K., & Hagen, J. (2003). *Critical information infrastructure protection in Norway.* Goethe-Universität Frankfurt.

Post, J., Ruby, K., & Shaw, E. (2002). The radical group in context: 2. Identification of critical elements in the analysis of risk for terrorism by radical group type. *Studies in Conflict and Terrorism*, *25*(2), 101-126.

Proyecto de Ley 245. (2019). Por el cual se crea el Sistema Nacional de Protección de Infraestructuras Críticas. Congreso de la República.

Rapoport, D. (2001). The fourth wave: September 11 in the history of terrorism. *Current History*, *100*(650), 419.

República Francesa. (2015). *Estrategia nacional francesa para la seguridad del ámbito digital.* Primer Ministro.

Ritter, S., & Weber, J. (2004). *Critical infrastructure protection: Survey of world-wide activities.* Bundesamt für Sicherheit in der Informationstechnik.

Rothery, M. (2005). Critical infrastructure protection and the role of emergency services. *Australian Journal of Emergency Management*, *20*(2), 45-50.

Schmid, A. (2011). *The Routledge handbook of terrorism research.* Taylor & Francis.

Singh, A., Gupta, M., & Ohja, A. (2014). Identifying critical infrastructure sectors and their dependencies: An Indian scenario. *International Journal of Critical Infrastructure Protection*, *7*(2), 71-85.

Sneps-Sneppe, M., Seleznev, S., Namiot, D., & Kupriyanovsky, V. (2016). About the status of cybersecurity of critical infrastructure of the state. *International Journal of Open Information Technologies*, *4*(7), 22-31.