# El entorno global amenazante. Relaciones internacionales y crisis del sistema[1]

# 1

https://doi.org/10.21830/9789585287860.01

*Vicente Torrijos*[2]
Escuela Superior de Guerra "General Rafael Reyes Prieto"
*Daniel Jiménez Salcedo*[3]
Organización de los Estados Americanos

## Resumen

El surgimiento de nuevos actores amenazantes en el sistema internacional, así como el desarrollo de nuevas tecnologías han hecho que los gobiernos tengan que replantear sus estrategias de seguridad y defensa para poder afrontar estos nuevos factores. Este trabajo analiza un entorno global amenazante en el que los nuevos actores que han surgido en el sistema internacional plantean distintas amenazas no tradicionales a la seguridad nacional de los Estados. La Estrategia de Defensa y Seguridad Nacional de los Estados es un documento que recopila las principales amenazas que cada gobierno se propone combatir. En ese sentido, se analizan y comparan estos textos para vislumbrar las nuevas amenazas y temas que surgen en la agenda de seguridad internacional. Los resultados de este trabajo evidencian que los Estados no son los únicos actores que generan amenazas, sino que también hay organizaciones que producen una inestabilidad en el entorno global. Esto ha llevado a que en la actualidad se hable de conflictos multimodales, que se presentan de modos distintos y no pueden clasificarse como internacionales o internos. Se concluye que han surgido nuevas amenazas como producto del desarrollo tecnológico, lo cual ha complejizado las agendas de seguridad de los Estados. Además, ahora se puede hablar de un *sharp power* utilizado por los países que tienen un régimen autoritario con el fin de cumplir con sus intereses nacionales.

**Palabras clave:** amenazas; defensa; estrategia; seguridad nacional; poder agudo; terrorismo.

---

1 Este capítulo forma parte de los resultados del proyecto de investigación "La legitimidad de las Fuerzas Militares en la geopolítica nacional e internacional de Colombia" del grupo de investigación de Ciencias Militares de la Escuela Militar de Cadetes "General José María Córdova", categorizado en B por Minciencias y con código de registro COL0082556. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

2 Profesor investigador de la Escuela Superior de Guerra y profesor adjunto de la Universidad Nacional de la Defensa, Centro William Perry, Washington, D. C. Investigador de la Escuela Militar de Cadetes "General José María Córdova", Bogotá, D. C., Colombia, grupo de investigación en Ciencias Militares. **ORCID:** https://orcid.org/0000-0003-3837-6196. **Contacto:** vicente.torrijos@esdegue.edu.co

3 Consultor en la Organización de Estados Americanos - Departamento de Relaciones Externas e Institucionales. Candidato a magíster en Política Internacional de Sciences Po Bordeaux. Egresado de la Universidad del Rosario en Relaciones Internacionales y Ciencia Política. **ORCID:** https://orcid.org/0000-0001-6443-157X.

## Introducción

Los temas sobre seguridad y defensa deben ser ejes centrales en la articulación de la política del Estado. Si bien pueden existir problemáticas que varíen de un periodo de gobierno a otro, la política de seguridad y defensa debería ser formulada, en todo caso, como una política de Estado. A la hora de hacer la proyección sobre estos temas, es necesario reflexionar sobre cuáles son las principales amenazas que se deben afrontar. Por esto, es importante tener en cuenta que las amenazas no son estáticas, sino que cambian a través del tiempo, exigen nuevas dinámicas y se presentan en nuevos fenómenos que muchas veces no responden a la concepción tradicional de lo que significa una amenaza para un Estado.

En cuanto al ámbito conceptual, se debe mencionar que la sociología, la ciencia política, el derecho y otras áreas de las ciencias sociales han hecho una aproximación al estudio y comprensión de la fenomenología de la seguridad y la defensa. Entendiendo la fenomenología como la teoría de los fenómenos o de lo que está apareciendo (RAE, 2018, *s. v. fenomenología*), han surgido así nuevas tendencias de estudio en el análisis estratégico.

En ese afán por descifrar lo que vendrá en el futuro, los sociólogos Anthony Giddens y Ulrich Beck han descrito a la sociedad moderna como una sociedad del riesgo. Por lo tanto, para ellos vivir en el mundo de hoy no es más riesgoso que en el pasado, pero pensar en términos de riesgo es parte de nuestra cotidianidad, lo cual genera mayor incertidumbre (Giddens, 2016). Además, Giddens desarrolla el concepto de "conciencia de riesgo", en el cual se deben tener en cuenta tres elementos fundamentales, que son el peligro, la amenaza y el riesgo, pues cada uno de ellos se puede presentar con una taxonomía que permite caracterizarlos y clasificarlos. Por un lado, es necesario determinar si esas amenazas son antrópicas o naturales. Esto, teniendo en cuenta si surgen como producto de la intencionalidad de un actor por generar la amenaza o si se presentan de forma no intencional. Por otro, es necesario identificar si dicha amenaza es inminente, latente y/o persistente, lo cual permite determinar si sus posibles consecuencias serán catastróficas, agobiantes y/o tolerables.

Lo anterior lleva a una reflexión sobre la manera como el Estado debe afrontar las amenazas, lo cual implica estudiar la forma como se entienden, cómo se lograrían superar y cómo se podrían transformar. En ese sentido, es fundamental que el estudio de la fenomenología actual de la seguridad y la defensa se haga con un pensamiento crítico que permita una anticipación estratégica, de modo que se logre prevenir efectivamente las amenazas del entorno global moderno. Sobre todo, en

un contexto en el que la interconectividad y el desarrollo de las tecnologías se han convertido en un nuevo factor determinante en la definición y ejecución de la estrategia de seguridad de un Estado.

## Ciberataques

No se puede negar que posiblemente se está viviendo el momento de mayor interconexión en la historia de la humanidad. A pesar de las ventajas que esto representa, también puede servir como una herramienta usada para generar daño. Así lo plantea Susan Brenner (2002) en el artículo "Cyberterrorism: how real is the threat?" cuando argumenta que el espacio cibernético es el más peligroso porque no existen fronteras entre los Estados. El ciberespacio les permite a los atacantes realizar varias agresiones en distintos lugares al mismo tiempo; y esos ataques, a pesar de ser dirigidos en el mundo virtual, afectan lo real.

En ese sentido, las ciberamenazas se han convertido, sin lugar a duda, en uno de los principales temas en la agenda de seguridad de todo el mundo. Incluso para las grandes potencias, como Estados Unidos, mantenerse seguro en la era cibernética se ha convertido en otro de los propósitos que se ha planteado con el fin de defender sus intereses nacionales. Esto ocurre porque el ciberespacio les permite tanto a los Estados como a los actores no estatales la posibilidad de afectar la actividad económica, política y de seguridad de una nación. Por ello, la prevención de cualquier ciberataque se convierte en una prioridad en la agenda internacional.

Ahora bien, es importante tener en cuenta que los ciberataques no son conducidos únicamente por actores individuales, sino también por Estados. Tal es la situación que identifica el documento de la Estrategia de Defensa Nacional de los Estados Unidos, respecto a Ucrania y Arabia Saudita (White House, 2017). Para el gobierno estadounidense, los principales perpetradores estatales de ataques cibernéticos contra Estados Unidos en el año 2018 serían Rusia, China, Irán y Corea del Norte (Mattis, 2018). Los ataques de estos últimos pueden obedecer a actividades de espionaje, robo de información, entre otros. Asimismo, los terroristas también continuarán usando internet para reclutar y radicalizar personas, dirigir operaciones, coordinar y ordenar segmentos de las organizaciones y realizar propaganda.

Dentro de los ataques cibernéticos se pueden distinguir dos modalidades, según explica Dorothy Denning (2000): se puede hablar de la ciberguerra y ciberterrorismo. La ciberguerra se presenta cuando los Estados actúan mediante el uso del ciberespacio para afectar otro Estado. En ese sentido, la ciberguerra es un conflicto

informático o de red que involucra ataques de motivación política de un Estado-nación en otro Estado-nación. En este tipo de ataques, los actores del Estado-nación intentan interrumpir las actividades de las organizaciones o Estados-nación, especialmente con fines estratégicos o militares y ciberespionaje (Chivis & Dion, 2017). El uso de ciberataques como una herramienta de política exterior había sido esporádico a principios de siglo. Sin embargo, Rusia, Irán y Corea del Norte están provocando ataques más agresivos en contra de Estados Unidos (Coats, 2018).

Es por esto que el espacio cibernético se ha convertido en un elemento crítico del cual no solo dependen los sectores económicos y productivos, sino que el Estado mismo debe tener en consideración. Las operaciones bancarias y financieras, tanto nacionales como internacionales, la infraestructura, los medios de transporte, el sector energético y el sanitario dependen en gran medida de nuevas tecnologías relacionadas con el uso de internet. Debido al alto grado de dependencia que estos sectores presentan del espacio cibernético y de las tecnologías de la información y de la comunicación, un fallo en la red o una incidencia sobre esta podría suponer una vulnerabilidad y/o amenaza en materia de seguridad en cualquiera de estos sectores.

Todo esto evidencia la necesidad de realizar acciones que doten a esta nueva realidad de una estrategia de ciberseguridad (Machín & Gazapo, 2016). Ataques cibernéticos se han producido cada vez con mayor frecuencia e impacto. Ya en el 2007 se había dado un ataque a la infraestructura financiera y comercial en Estonia. De igual forma, en el 2010 ocurrió el sabotaje a las instalaciones nucleares de Irán por medio del gusano informático *Stuxnet*. En este caso, el virus informático tomó el control de mil máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse. Esta fue la primera vez que un ataque cibernético logró dañar la infraestructura nuclear de un Estado, con lo cual marcó un hito en el campo de la ciberseguridad. Más recientemente, es importante señalar los casos de ciberataques en Arabia Saudita y Ucrania, los cuales deben activar las alertas del mundo puesto que la capacidad que tienen estos ataques para irrumpir en la cotidianidad de una nación y generar caos en distintos ámbitos de la sociedad significa una amenaza que en cualquier momento podría sufrir indistintamente un Estado.

Asimismo, está la amenaza del ciberterrorismo, la cual se puede definir como un ataque premeditado, motivado políticamente en contra de información, sistemas y programas informáticos que resultan en violencia en contra de objetivos no combatientes por parte de agentes no nacionales (Chivis & Dion, 2017). En ese sentido, esta táctica es utilizada por los grupos terroristas con el fin de perpetrar un

ataque y dar lugar a la violencia contra personas o propiedades, o al menos causar suficiente daño para generar miedo (Denning, 2000).

El uso del internet se convierte así en una herramienta fundamental pues les permite a los miembros de la organización comunicarse y coordinar eventos, pero también es el medio con el cual pueden irrumpir en la cotidianidad de las personas y generar grandes impactos. Es importante señalar que en 1998 el Departamento de Estado de Estados Unidos apenas registraba en la web a 12 de 30 organizaciones terroristas, mientras que en la actualidad todas ellas tienen actividad en la web. Esto ha provocado que el ciberespacio esté constantemente bajo asalto. Ciberespías, ladrones y saboteadores irrumpen en los sistemas informáticos para robar datos personales y secretos comerciales, vandalizar los sitios web, interrumpir servicios, sabotear datos y sistemas, lanzar virus y gusanos informáticos, realizar fraude en transacciones, y hostigar a individuos y compañías. Estos ataques son facilitados con herramientas de software cada vez más potentes y fáciles de usar, que están disponibles de forma gratuita desde miles de sitios web en internet.

Por todo esto se puede decir que el ciberterrorismo ocurre en el ciberespacio, pero tiene repercusiones en el mundo real. Esa afectación del mundo real se suele dar sobre la infraestructura crítica, la cual se refiere a los sistemas de energía, las comunicaciones, la banca, el transporte, el sistema de agua, los servicios de emergencia y los servicios de gobierno. No obstante, esto ha sido motivo de debate puesto que hay quienes argumentan que es posible que exista una mayor probabilidad de que los grupos terroristas se especialicen en este tipo de ataque, mientras hay quienes son más escépticos frente a dicha posibilidad (Rubin, 2017). Esto considerando la capacidad técnica y tecnológica que puedan llegar a tener las distintas organizaciones terroristas para tener la suficiente incidencia e impacto en el ciberespacio. Por esto vale la pena recordar que el fin último de este tipo de ataques es generar repercusiones políticas.

## Poder agudo

Otra de las nuevas amenazas dentro del actual entorno global que tiene que ver con las relaciones y actividades que llevan a cabo los Estados se refiere a lo que Joseph Nye ha denominado *sharp power* (también conocido como *poder punzante* o *poder agudo*). El denominado *sharp power* se refiere a aquellos esfuerzos de influencia autoritaria bajo los lentes del *soft power* (Cardenal et al., 2017). Estas prácticas las han implementado Estados cuyos regímenes políticos distan de ser democráticos

y por ello han desarrollado la capacidad de incidir en las democracias liberales más vulnerables. Principalmente aquellos Estados que hacen uso del *sharp power* son China y Rusia. Lo más interesante sobre estos dos Estados es que en un contexto de máxima globalización han logrado crear barreras a la influencia política y cultural que les pueda llegar de afuera.

En el caso específico de Rusia, el gobierno se ha encargado de crear una imagen positiva del régimen autocrático que los gobierna, y a su vez ha generado una imagen negativa del modelo democrático. En el caso de China ocurre un fenómeno similar, puesto que el gobierno se ha encargado de suprimir cualquier tipo de crítica internacional al Partido Comunista Chino (Cardenal et al., 2017). Su estrategia se ha basado en el manejo de los medios de comunicación, la academia y la comunidad política, de manera que sus intereses no se vean afectados por estos otros.

En ese sentido, el modelo político que ambos Estados han adoptado es fundamental para analizar la aproximación que han hecho al problema, dado que ese carácter autoritario que determina sus acciones políticas privilegia el poder estatal sobre las libertades individuales. Esto lleva a pensar que, aunque el proceso de globalización y la democracia se han expandido ampliamente por el mundo entero, la idea de regímenes autoritarios poderosos sigue en pie y ha adquirido recientemente un carácter global.

Por eso se puede decir que las ambiciones de los regímenes autoritarios han adquirido un carácter global y han afectado aquellas regiones del mundo donde las democracias son aún muy débiles y vulnerables. Específicamente, América Latina y Europa Central son dos escenarios donde la consolidación de los regímenes democráticos aún está en proceso y por ende son más vulnerables a una eventual intervención de China o Rusia. Asimismo, estas dos regiones tienen una relevancia geopolítica y estratégica para los poderes autoritarios dado que son zonas muy cercanas a las principales democracias consolidadas en el mundo (Norteamérica y Europa Occidental). Al respecto, el estudio de Cardenal et al. (2017) analiza cómo el ejercicio del *sharp power* por parte de Rusia y China se evidencia en ciertos escenarios específicos como Eslovaquia, Polonia, Argentina y Perú.

Ahora bien, vale la pena recordar que el *hard power* es definido por Joseph Nye (2018) como aquel ejercicio del poder basado en la dominación, como las acciones militares o las presiones económicas que emplean algunos Estados para alcanzar sus fines políticos. En contraste con esto, Nye (2018) define el *soft power* como la capacidad de un actor político, por ejemplo un Estado, para incidir en las acciones

o intereses de otros actores valiéndose de medios culturales e ideológicos, con el complemento de medios diplomáticos.

La diferenciación entre una acción de *soft power* y *sharp power* ha sido motivo de una gran controversia porque la línea divisoria entre uno y otro pareciera ser muy difusa e indistinguible. Sin embargo, Cardenal et al. (2017) señalan que la influencia que adquiere un Estado sobre distintas esferas, como los medios de comunicación, la academia y la cultura no se basa en la atracción o persuasión (*soft power*), sino en la manipulación y la distracción (*sharp power*) (Cardenal et al., 2017). En ese sentido, el objetivo del gobierno ruso y chino es manipular las percepciones, sentimientos y opiniones que se tiene en el exterior sobre el Estado. Esto ha sido posible gracias a los desarrollos tecnológicos que Rusia y China han logrado durante las últimas décadas.

Vale la pena, entonces, revisar un poco el contexto interno de cada uno de estos países. Por un lado, tanto el gobierno chino como el ruso se han encargado de suprimir la oposición interna al régimen, puesto que han silenciado a los opositores políticos por medio de acciones coercitivas. De igual forma, se han encargado de adquirir los medios de comunicación y, por medio de ellos, difundir propaganda a favor del gobierno, con lo cual han restringido la libertad de prensa y de expresión, que es tan valorada en los Estados democráticos. En el caso puntual de China, el gobierno ha logrado desarrollar un sofisticado sistema de control y monitoreo de la información que manejan los distintos departamentos gubernamentales, así como las compañías privadas. De esta manera, han logrado suprimir cualquier riesgo de discernimiento político que pueda afectar la estabilidad del Estado. En últimas, el pluralismo de ideas que tanto se dice respetar en sociedades abiertas y democráticas es completamente suprimido en los regímenes autoritarios. Sin embargo, es importante aclarar que, según Cardenal et al. (2017), a pesar de la existencia de estas restricciones, tanto Rusia como China han logrado mantener una buena reputación en términos internacionales, de manera que ningún gobierno se ha pronunciado enfáticamente sobre este respecto.

En parte, han logrado mantener esta imagen gracias a que una de sus tácticas es generar desorden y confusión en el sistema internacional. Se podría decir que han logrado con éxito cumplir este objetivo, pues la estrategia de defensa nacional de los Estados Unidos inicia reconociendo el desorden que actualmente se presenta en el sistema. De acuerdo con el secretario de Defensa estadounidense James Mattis, Estados Unidos está resurgiendo de un periodo de "atrofia estratégica" en el que la competitividad de su ejército ha disminuido y el desorden en el mundo ha aumen-

tado (Mattis, 2018). En todo caso, este desorden les ha permitido llevar a cabo sus estrategias de *sharp power* sin que otros Estados lo denuncien.

Ahora bien, vale la pena detenerse un poco sobre el término mismo y analizar el significado de *sharp power*. El termino *sharp* se utiliza con el sentido de penetrar en las instituciones de quien se quiere afectar, para lo cual se consigue información que sea beneficiosa para el interés de quien la intercepta (Cardenal et al., 2017). De esta manera, el objetivo de utilizar el *sharp power* es manipular la percepción de la población en favor del Estado que actúa. Así, el Estado podrá tener el control, no solo de la economía y la política, sino también el total control de la opinión pública nacional e internacional.

En el caso específico de la manipulación de los medios de comunicación, Cardenal et al. (2017) determinaron que China utiliza un triple enfoque, el cual consiste en lo siguiente: primero se debe desarrollar presencia local de los medios de comunicación chinos, por ejemplo, en América Latina. Luego se deben crear alianzas comerciales entre los medios de comunicación chinos y los medios de comunicación locales que permitan una mayor cooperación. En tercer lugar, se debe ofrecer oportunidades de intercambio de los periodistas en China con la excusa de hacer entrenamiento profesional, pero en realidad tiene como propósito que dichos periodistas transmitan información favorable de China en sus países.

En resumen, se puede decir que estas iniciativas se llevan a cabo en las esferas de los medios de comunicación, la cultura, los centros de pensamiento y la academia, y que se centran en la distracción y la manipulación. Además, se trata de acciones de carácter autoritario que bajo el escudo del *soft power* penetran la política y la información de un Estado en específico. Los Estados que aplican el *sharp power* han suprimido el pluralismo político y la libre expresión. En ese sentido, buscan expandir esta situación en el escenario internacional de manera que puedan satisfacer sus propios intereses. Estados en América Latina y de Europa Central han sido blanco del poder punzante ejercido por China y Rusia, dado que son países próximos geográficamente a Estados Unidos y a Europa Occidental. De igual forma, los Estados ubicados en estas zonas tienen democracias más susceptibles de ser afectadas por el poder punzante.

Según el estudio realizado por Cardenal et al. (2017), en todos los Estados donde estudiaron la influencia del *sharp power*, es decir, en Estados de América Latina y Europa Central, existía un desconocimiento generalizado en términos mediáticos y académicos sobre China y Rusia. Esto se produce como resultado del poco interés que el público en estas regiones del mundo tiene sobre dichos Estados, su sistema de gobierno, su sistema económico, etc. En ese sentido, cuando

el gobierno chino o el gobierno ruso hacen alianzas con instituciones educativas en estos países, como universidades públicas o privadas, pueden generar un mayor impacto porque no se conoce mucho sobre ellos con anterioridad.

En el caso de China, el Instituto Confuciano se ha convertido en una de las principales organizaciones que en el ámbito internacional ha logrado penetrar en el sistema educativo de muchos Estados (Cardenal et al., 2017). Además, se dice que este instituto trabaja en colaboración con el gobierno chino, de manera que las personas que ingresan al instituto en Latinoamérica o Europa Central adquirirán la visión de China que el gobierno aprobó. La cultura china se ha convertido en otro factor determinante en la utilización que hace ese Estado del *sharp power*, dado que el mundo en general tiene una visión de la cultura china que no presenta ningún riesgo, y que en muchos casos genera curiosidad. Ante la gran acogida internacional que ha tenido la cultura china en los grandes eventos culturales donde se expone alrededor del mundo, el gobierno, además, ha influido de manera que también se muestre una visión positiva del régimen.

El caso de Rusia es ligeramente distinto por cuanto la relación de Rusia con muchos Estados ha estado envuelta en tensiones históricas, particularmente durante el periodo de la Guerra Fría. Por eso la estrategia rusa se ha basado sobre todo en la expansión de los medios de comunicación estatales como RT. Por ejemplo, Cardenal y Kucharczy (2017) mencionan que en el caso de Polonia el principal objetivo de Rusia es promover una visión negativa de la Unión Europea. De igual forma ocurre en Eslovaquia, donde además la prensa rusa dice que las dos naciones comparten valores mutuos que son propios del pueblo eslavo, al cual ambos Estados pertenecen. Esto en contraste con los valores occidentales que profesan Estados Unidos y los países de Europa occidental.

Todo este surgimiento del *sharp power* ha logrado afectar todo tipo de Estados, desde las democracias más débiles hasta las más fuertes. Sin embargo, China y Rusia han centrado su atención en aquellos Estados donde el régimen democrático es aún muy débil. Por este motivo Cardenal y Kucharczy (2017) proponen que los Estados con democracias débiles y que están siendo víctimas del *sharp power* de países autoritarios sigan ciertos pasos que les permitirían construir un sistema de defensa. El primer elemento fundamental es reconocer a China y Rusia como los actores específicos que están influyendo la información, además de hacer un estudio profundo sobre las verdaderas intenciones de los Estados autoritarios en esta región y analizar cómo han logrado penetrar en el país en cuestión. En segundo lugar, es necesario que la sociedad los estudie y los ponga en el centro de atención, de tal manera que se devele su influencia autoritaria porque normalmente se camuflan entre las élites

gobernantes para pasar inadvertidos. Una vez los han descubierto, estos Estados deben armar mecanismos de protección contra la amenaza del poder punzante y recalcar la importancia de los valores democráticos que los definen como nación. En tercer lugar, cada Estado que sufra del *soft power* debe fortalecer los valores democráticos dentro de la sociedad, de manera que a las personas no les llame la atención la opción autoritaria gracias a que son capaces de entender las restricciones a las libertades individuales que implican estos modelos.

Finalmente, se debe seguir haciendo un análisis sobre la diferenciación entre las acciones de *soft power* y *sharp power*, ya que dentro de la confusión y el desorden que se suele crear es muy probable que los Estados no se den cuenta de la forma en que Rusia y China han logrado penetrar e influir hasta las más altas instancias de su administración pública. Tal es el caso de Argentina, Perú, Eslovaquia y Polonia, donde exitosamente Rusia y China han logrado adentrarse en los escenarios de los medios de comunicación, la academia, los centros de pensamiento y la política, de manera que han influido y sacado provecho para beneficiar sus propios intereses nacionales.

## Terrorismo

Dentro del discurso político moderno siempre han estado presentes dos conceptos que por su naturaleza son difíciles de definir y muchas veces cuesta diferenciarlos: el terrorismo y la insurgencia, que si bien han existido desde la fundación del Estado mismo, hoy en día tienen un papel fundamental en el estudio de la seguridad.

En este sentido, es necesario definir el término *insurgencia*. Para O'Neill (2005), la insurgencia (o guerra interna) es un concepto global general que se refiere a un conflicto entre un gobierno y un grupo o adversario que utiliza recursos políticos y violencia para cambiar, reformular o mantener la legitimidad de uno o más de los aspectos clave de la política. Dentro de esos aspectos de la política que se busca reformular está la integridad de las fronteras y la composición del Estado-nación, el sistema político, las autoridades en el poder y las políticas que determinan quién obtiene qué en las sociedades (O'Neill, 2005).

De acuerdo con este punto de vista, la actividad insurgente es una forma de movimiento, un esfuerzo político con un objetivo específico, ya que son actores por fuera de la regularidad que buscan generar un cambio. Por ello, la insurgencia se puede entender también como un levantamiento sistemático, progresivo y violento

en contra de la autoridad para revertir el orden establecido. Esa insurgencia puede adoptar muchas formas tácticas, entre ellas la guerra de guerrillas o el terrorismo como método de guerra para una insurgencia.

De esta manera se introduce el segundo concepto clave en esta discusión, el *terrorismo*. De acuerdo con Young y Gray (2011), el terrorismo es una táctica, un método de guerra que no puede ser considerado como un fenómeno aparte. De alguna manera, es la táctica del débil porque no tiene la fuerza suficiente para afrontar directamente a su enemigo. Ahora bien, Hoffman (2006) menciona unos elementos fundamentales desde la concepción más clásica que tiene el terrorismo. Entre estos está que tiene ineludiblemente un carácter político, recurre a la violencia o a la amenaza del uso de la violencia, genera un impacto psicológico en la población, es conducido por una organización con una estructura de mando determinada y es realizado por un actor subnacional.

Como se mencionó anteriormente, las insurgencias pueden adoptar múltiples tácticas. Una de ellas es el terrorismo, pero otra es la guerrilla, que surgió en 1809-1812 tras la invasión de Napoleón a España. Es una forma de las tácticas irregulares de la guerra —también conocida como "la guerra pequeña"—, una forma de guerra irregular en la que no se confrontan ejércitos de Estado contra Estado pues no existe un enfrentamiento frontal. La guerra de guerrillas adopta tácticas como atacar y esconderse o atacar suministros esenciales. Específicamente, desde la teoría de la guerra de Mao se puede hablar de tres elementos: en primer lugar, la debilidad estratégica, la cual busca desgastar al enemigo; en segundo lugar, alcanzar el equilibrio mediante la conquista de la gente, y, en tercer lugar, la ofensiva estratégica, en la cual el grupo insurgente logra atacar a su enemigo y eventualmente vencerlo.

Sobre estas características se puede profundizar en los siguientes aspectos: por un lado, la respuesta del gobierno, puesto que muchas veces su ausencia es lo que propicia el surgimiento de las insurgencias, ya sea por causas colectivas, individuales o morales. En cuanto a las colectivas, se puede ver la pobreza, la opresión, la identidad y la política, pues para Young y Gray (2011), un liderazgo centralizado con la capacidad de efectuar cambios es primordial en minimizar o disipar la violencia insurgente. Muchos de los agravios transmitidos por los insurgentes y las organizaciones guerrilleras giran en torno a la incapacidad del régimen político para hacer negocios en una manera exenta de dominación. De acuerdo con los autores, también sería necesario aumentar las capacidades económicas de forma que se pueda incluir la gestión de recursos por parte de grupos indígenas y grupos minoritarios, en lugar de que estos sean controlados únicamente por las corpora-

ciones internacionales, lo cual sería una medida adicional para derrotar el trasfondo de una insurgencia.

Por otro lado, el uso de las organizaciones internacionales para combatir las insurgencias tiene un papel en la política de contrainsurgencia. Las acciones militares, económicas y políticas de las coaliciones internacionales tienen la capacidad de luchar contra las estrategias insurgentes, pero su presencia a menudo aumenta la condición y la propaganda para una mayor resistencia. De igual forma, a través del aumento regional de acuerdos cooperativos, países como Estados Unidos han podido reducir sus actividades militares en Estados en vía de desarrollo, al tiempo que asisten a grupos como la Asociación de Naciones del Sudeste Asiático (ASEAN), el Mercado Común del Sur (MERCOSUR), la Liga Árabe y la Organización para la Unidad Africana (OUA). Todo esto para implementar y actuar sobre el cambio cultural e ideológico pertinente a su región y campo de especialización.

Finalmente, la internacionalización de los grupos insurgentes se ha llevado a cabo no solo mediante su inclusión en la agenda política y de seguridad internacional, sino también gracias a los medios de comunicación. Al reunir a las masas mediante los medios de comunicación, la utilización de la propaganda para difundir los mensajes de los grupos insurgentes se ha convertido en un avance indispensable para el terrorismo moderno. Esto conduce a un conflicto, puesto que el aumento de la tecnología y la popularidad de los medios de comunicación les han permitido a los grupos insurgentes realizar ataques con mayor impacto mundial. Así, con el aumento del terrorismo, los grupos insurgentes han usado la acción de intervención humanitaria internacional como herramienta para aumentar la propaganda y la formación de la opinión pública internacional. Esta nueva herramienta, trabajando en conjunto con los medios de comunicación modernos, ha fomentado un nuevo medio para utilizar el terrorismo.

Ahora bien, es importante señalar que el terrorismo ha adquirido muchos centros y núcleos, lo cual permitiría introducir la idea del *terrorismo policéntrico*. En la actualidad, las organizaciones terroristas operan bajo una modalidad que remite a la teoría de redes, en la cual se entiende que la forma natural de un sistema es una red (Gueller, 2011). En ese sentido, estas organizaciones crean una serie de conexiones entre distintos actores en diferentes sitios para crear lo que se conoce como *nodos* (elementos que se van a conectar) y *hubs* (nodo con mayor número de conexiones). Así, la organización va adquiriendo la morfología de una red. No obstante, esta puede variar, pues hay organizaciones que mantienen el modelo jerárquico tradicional de árbol, así como hay otras que tienen una red de estrella, lineal o de múltiples canales (Zanini & Edwards, s. f.).

Todo esto lleva a repensar la manera como se deben afrontar las organizaciones terroristas. Como se evidenció en la lucha contra Isis por parte de Estados Unidos, en noviembre de 2015 la estrategia en Siria e Irak consistía en recuperar el territorio, interrumpir el financiamiento y desmantelar la cúpula de los yihadistas. Esto denota la complejidad que implica la lucha contra estas organizaciones terroristas, que al estar organizadas en red hacen mucho más difícil su identificación y ataque. De hecho, tras la experiencia crítica de los ataques del 13 de noviembre de 2015 en París se produjo la Declaración Antiterrorista del G-20, la cual se enfoca en luchar contra la financiación del terrorismo, el control de fronteras, la propaganda y el reclutamiento. De igual forma, en la Comunicación de la Comisión al Parlamento Europeo sobre la aplicación de la agenda europea de seguridad para luchar contra el terrorismo y allanar el camino hacia una Unión de la Seguridad genuina y efectiva, se hace alusión a la nueva dinámica con la cual operan las organizaciones terroristas y la cual significa una importante amenaza para la seguridad de los países que conforman la Unión Europea.

## Crimen transnacional organizado

Desde el final de la Guerra Fría las actividades delictivas criminales organizadas se han convertido en una de las principales fuentes de ingresos para grupos terroristas en todo el mundo. Teniendo en cuenta el precedente establecido por el narcoterrorismo, tal como surgió en América Latina en la década de 1980, el uso del crimen se ha convertido en un factor importante en la evolución del terrorismo. Como tal, el decenio de 1990 puede ser descrito como la década en la que se consolidó el nexo crimen-terrorismo. En ese sentido, hoy en día se puede hablar del crimen por parte de grupos terroristas como su principal fuente de financiación, lo cual incluye actividades delictivas como gravar el tráfico de drogas o participar en fraudes con tarjetas de crédito.

De igual manera, se ha construido un nexo entre las organizaciones criminales y los grupos terroristas. Tamara Makarenko (2004), en su texto *The crime-terror continuum: tracing the interplay between transnational organised crime and terrorism*, caracteriza la relación que existe en la actualidad entre el crimen organizado y el terrorismo. Para ello se tienen en cuenta las alianzas que pueden establecer estos dos tipos de organizaciones, las motivaciones operacionales de cada una y la convergencia que eventualmente se puede dar entre ellas. En ese orden de ideas, vale la pena aclarar que para Makarenko (2004), un grupo delincuencial puede pasar por

todo un continuo entre ser un grupo criminal organizado a ser un grupo terrorista. En ese sentido, una organización no se podría categorizar como estrictamente terrorista o criminal. Asimismo, Makarenko (2004) señala que se puede encontrar un punto de convergencia, es decir, el punto central donde se presentan en igual medida las características de un grupo criminal y las de un grupo terrorista.

Ahora bien, el primer nivel de relación que existe entre el crimen organizado y el terrorismo son las alianzas que se pueden construir entre ellos. Las alianzas existen en ambos extremos del continuo: grupos delictivos que forman alianzas con organizaciones y grupos terroristas que buscan alianzas con organizaciones criminales, ya sean de corta o larga duración. La cooperación con los terroristas puede tener importantes beneficios para los delincuentes organizados porque desestabilizan la estructura política y socavan la aplicación de la ley, así como limitan las posibilidades de cooperación internacional. Un claro ejemplo de ello ha sido la alianza que han tenido grupos terroristas con carteles del narcotráfico con el fin de ganar beneficios para los dos tipos de grupos.

Esto indica que la formación de alianzas responde al interés tanto de los grupos criminales, como al de los grupos terroristas, de tal forma que se logre satisfacer las necesidades de ambos. La inestabilidad política es entonces favorable para los terroristas porque disminuye la legitimidad de los gobiernos a los ojos de la población, de quien buscan obtener apoyo. Para los grupos criminales, la inestabilidad permite maximizar sus operaciones, sobre todo para los grupos dedicados al contrabando a gran escala de productos lícitos o ilícitos.

Los grupos criminales y los grupos terroristas han tratado de evitar los problemas inherentes a todas las alianzas: diferencias sobre prioridades y estrategias, desconfianza, deserciones y la amenaza de que las alianzas puedan crear competidores. Para evitar todo esto, los grupos criminales han desarrollado sus propias capacidades para poder perpetrar ataques terroristas. De igual forma, los grupos terroristas ahora están en la capacidad de poder realizar actividades criminales. Por ejemplo, desde la década de 1970 grupos como las FARC, ETA, el Partido de los Trabajadores del Kurdistán (PKK) y Sendero Luminoso han sido vinculados al tráfico de drogas. Como resultado de esto, se puede ver que los grupos criminales se han involucrado cada vez más en la actividad política en un esfuerzo por manipular las condiciones operacionales presentes en el creciente número de Estados débiles. Asimismo, los grupos terroristas se han enfocado cada vez más en actividades delictivas para reemplazar el apoyo financiero perdido de los patrocinadores estatales y como un medio mucho más efectivo de financiamiento.

Ahora bien, es necesario señalar que las organizaciones criminales usan la violencia selectiva para destruir a sus competidores o amenazar a las autoridades antinarcóticos. Un ataque violento dirigido por una organización criminal transnacional está destinado a un objetivo específico, más que a una audiencia nacional o internacional, y en ese sentido no está ligada a la retórica política.

De igual forma, se puede hablar de la tesis de la convergencia propuesta por Makarenko (2004), la cual establece que las organizaciones criminales y terroristas pueden converger en una misma entidad que tenga simultáneamente las características de ambos grupos. En ese sentido, se puede hablar de dos componentes fundamentales en la tesis de la convergencia: por un lado, puede haber grupos criminales con motivaciones políticas y, por el otro, están los grupos terroristas interesados en las ganancias económicas que produce la criminalidad. Todo esto evidencia que cuando estos grupos ganan control sobre las instituciones económicas, pueden a su vez conseguir ventajas políticas.

Otro fenómeno relacionado con esto es el de los "hoyos negros", los cuales son escenarios donde no hay ningún tipo de legalidad y por ende allí se desarrollan libremente las actividades criminales y terroristas. Un claro ejemplo de ello es la triple frontera entre Brasil, Argentina y Uruguay, donde no hay presencia de ningún Estado, razón por la cual las organizaciones criminales han aprovechado para llevar a cabo en este territorio todo tipo de actividades criminales y terroristas.

En conclusión, se puede ver que el crimen organizado transnacional está estrechamente vinculado con el terrorismo, puesto que ambas actividades han visto en la otra un medio de apoyo a su causa. En ese sentido, si bien se han formado alianzas entre grupos criminales y terroristas, también cada uno de esos grupos ha logrado desarrollar las capacidades suficientes para llevar a cabo las actividades del otro. Todo esto reafirma la teoría de Makarenko (2004) de que existe un proceso continuo entre el terrorismo y la criminalidad, de manera que en el centro existe un punto de convergencia donde un mismo grupo u organización puede realizar ambas actividades.

## Organizaciones antisistémicas violentas

A lo largo de este texto se han estudiado desde las amenazas que pueden generar otros Estados hasta aquellas que pueden producir actores no estatales como las insurgencias, los grupos terroristas y los grupos criminales. No obstante, se han excluido las denominadas *organizaciones antisistémicas violentas*, que se podrían

definir como grupos armados no estatales (aunque puedan gozar de apoyos estatales) que recurren a la violencia organizada como herramienta para lograr sus objetivos (Mulaj, 2010). La consecución de esos objetivos se produce como resultado de su longevidad y su letalidad. Su longevidad en cuanto es perdurable y sostenible a través del tiempo. Su letalidad en cuanto a su capacidad destructiva.

Ante este panorama es indispensable plantear posibles soluciones para combatir a este tipo de actores que amenazan el sistema. En primer lugar, proteger y servir al ciudadano debe ser una prioridad que se logra mediante el robustecimiento institucional. En segundo lugar, se debe controlar el territorio y recuperar la autoridad local, para lo cual se deben eliminar las áreas grises o los vacíos de poder, fortalecer las identidades locales y fomentar la transparencia y la rendición de cuentas en todo nivel. En tercer lugar, es fundamental empoderar al ciudadano expandiendo la cultura de Derechos Humanos y generando que la población se apropie de la política de seguridad, de forma que rechace a las organizaciones antisistémicas violentas. De esta manera se lograría mantener una unidad entre las élites y los ciudadanos que contribuye a conservar la política de seguridad.

En cuarto lugar, es necesario doblegar la voluntad de lucha del adversario, se debe tener la capacidad de paralizarlo, aislarlo y atraerlo. Paralizarlo, en cuanto que no pueda utilizar los recursos con los que cuente; aislarlo de manera que no pueda sustituir al Estado, y atraerlo en cuanto deserte, se reconvierta y pase a colaborar con el Estado. En quinto lugar, se debe lograr la conjunción estratégica y la innovación constante, es decir, que las Fuerzas Armadas deben funcionar conjuntamente asegurando la alta movilidad, la anticipación y la prevención. De igual forma, esto permitiría identificar los verdaderos centros de gravedad propios y ajenos.

Otra de las tácticas contempladas para combatir las organizaciones antisistémicas violentas sería convertir la asimetría en una ventaja estratégica para dar golpes contundentes al adversario. En ese sentido, se deben asimilar, adecuar y reinventar los modos de operar. De igual forma, se debe buscar anular la resiliencia de dichas organizaciones, de manera que se logre tener una victoria contundente sobre ellas. Esto implica que se debe ganar la guerra de la narrativa y del discurso ideológico sobre estas organizaciones, pues se debe desenmascarar su estructura simbólica del poder, como los estereotipos, las plataformas, el uso del diálogo como medio revolucionario, etc. Finalmente, se debe asegurar la gobernabilidad democrática y repensar permanentemente las amenazas, ya sean emergentes, recicladas o persistentes. Así se lograría evaluar cuidadosamente la madurez de los conflictos y si se ha alcanzado el punto culminante de la victoria antes de iniciar un eventual proceso de negociación.

## Conclusión

Tras hacer un rastreo del entorno global actual, se puede determinar que han surgido nuevas amenazas como producto del desarrollo tecnológico, lo cual ha complejizado las agendas de seguridad de los Estados. Además, ahora se puede hablar de un *sharp power* utilizado por los países que tienen un régimen autoritario con el fin de cumplir con sus intereses nacionales. Como lo describe Joseph Nye (2018), "mientras el poder blando utiliza el atractivo de la cultura y los valores para aumentar la fortaleza de un país, el poder punzante es una herramienta de regímenes autoritarios para forzar conductas en el país de origen y manipular la opinión en el extranjero" (Nye, 2018, p. 2). Ese carácter autoritario con el que opera el *sharp power*, junto con las repercusiones que tiene su utilización, lleva a que Nye (2018) concluya que este tipo de poder, más que tener cierta similitud con el *soft power*, podría llegar a considerarse como más parecido al *hard power*.

Ahora bien, las amenazas no solo provienen de los Estados, sino que también existen organizaciones que provocan inestabilidad en el entorno global. Esto ha llevado a que en la actualidad se pueda hablar de conflictos multimodales y que no sea posible clasificarlos simplemente como internacionales o internos. Las nuevas dinámicas con las que operan las distintas organizaciones terroristas y criminales hacen que la manera de combatirlas no sea solamente desde la lógica de un conflicto interno, sino que muchas veces se tiene que recurrir a la idea de un conflicto internacional.

De hecho, esta incertidumbre en la inseguridad ha conducido a que se incremente el fenómeno de las áreas grises, es decir, territorios que no son controlados por los Estados a escala rural o en ambientes urbanos. De esta forma, han surgido regiones en las que pululan no solo fenómenos como la minería ilegal o el contrabando, sino que ahora se puede decir que la minería ilegal es mucho más lucrativa que el narcotráfico porque no solo involucra la explotación de metales, sino el control de extensas zonas por parte de grupos armados ilegales. Por todo esto, dentro de este entorno global amenazante es indispensable que cada Estado busque afianzar una diplomacia de paz y defensa, en la que se gesten alianzas y coaliciones esenciales contra la lucha de las amenazas. Así, el estudio de las amenazas en la sociedad de riesgo en la que vivimos debe ser constante, de tal manera que logre orientar la formulación de las políticas de seguridad y defensa de los Estados.

## Conflicto de intereses

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con este capítulo.

## Financiación

Los autores no declaran fuente de financiamiento para la realización de este artículo.

## Referencias

Brenner, S. (2002). Cyberterrorism: how real is the threat? *Media Asia*, *9*, 149-154. https://doi.org/10.1080/01296612.2002.11726680

Cardenal, J. P., Kucharczyk, J., Mesežnikov, G., & Pleschová, G. (2017). *Sharp power rising authoritarian influence* [documento en línea]. Recuperado de https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf

Chivis, C., & Dion, C. (30 de marzo de 2017). Why it's so hard to stop a cyberattack and even harder to fight back [nota de blog]. Recuperado de https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html.

Coats, D. (2018). Worldwide Threat assesement of the US Intelligence Community. National Intelligence.

Denning, D. (2000). Cyberterrorism [documento en línea]. Recuperado de http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf

Giddens, A. (2016). Fate risk and security. En J. F. Cosgrabe (Ed.), *The sociology of risk and gambling reader* (pp. 29-45). Routledge.

Gueller, A. (2011). The use of complexity-based models in international relations. *Cambridge Review of International Affairs*, *24*, 63-80. https://doi.org/10.1080/09557571.2011.559191

Hoffman, B. (2006). *Inside terrorism* (2a. Ed.). Columbia University Press.

Machín, N., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista* UNISCI, *42*, 47-68. https://revistas.ucm.es/index.php/RUNI/article/view/53786

Makarenko, T. (2004). The crime-terror continuum: tracing the interplay between transnational organized crime and terrorism. *Global Crime*, *6*, 129-145. https://www.iracm.com/wp-content/uploads/2013/01/makarenko-global-crime-5399.pdf

Mattis, J. (2018). Summary of the National Defense Strategy [documento en línea]. Recuperado de https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Mulaj, K. (2010). Violent non-state actors in world politics. Londres: C. Hurst & Co. Publishers Ltd.

Nye, J. (4 de enero de 2018). China: poder blando y poder punzante [información en página web]. Recuperado de https://www.project-syndicate.org/commentary/china-soft-and-sharp-power-by-joseph-s--nye-2018-01/spanish

O'Neill, B. (2005). Insurgency and terrorism: from revolution to apocalypse. En D. Galula, *Counterinsurgency warfare: theory and practice*. St. Petersburg, FL: Hailer Publishing.

Real Academia Española de la Lengua [RAE]. (2018). Fenomenología. Recuperado de https://dle.rae.es/fenomenolog%C3%ADa?m=form

Rubin, M. (2017). The age of hyper-terrorism and 'low cost' terrorism. Recuperado de http://www.aei.org/publication/the-age-of-hyper-terrorism-and-low-cost-terrorism/

Young, A., & Gray, D. (2011). Insurgency, guerilla warfare and terrorism: conflict and its applications for the future. *Global Security Studies*, *2*(2), 60-71. http://globalsecuritystudies.com/Insurgency.pdf

Zanini, M., & Edwards, S. (s. f.). The networking of terror in the information age. En *Networks and netwars: the future of terror, crime, and militancy* (pp. 29-60). Recuperado de https://www.rand.org/pubs/monograph_reports/MR1382.html