Seguridad, terrorismo y conflictos no convencionales

PID_00248468

Francisco Beltrán Adell

Tiempo mínimo de dedicación recomendado: 1 hora

Universitat Oberta de Catalunya

Índice

Introducción

Este módulo intenta explicar en qué consiste la cambiante naturaleza de las amenazas en materia de seguridad que afectan a los Estados. En primer lugar, se estudiará cuál es el impacto de la globalización y de las nuevas tecnologías en la definición de las guerras y en las circunstancias en que se libran los conflictos bélicos. En segundo lugar, veremos cómo afectan, de nuevo, la globalización y la tecnología a la definición de terrorismo y a su transformación de fenómeno local a otro de alcance global. Y, en tercer lugar, abordaremos los conflictos no convencionales y, en concreto, las amenazas que aparecen en la escena internacional y que están estrechamente ligadas al uso de internet, como la llamada ciberguerra. Como los anteriores, el módulo se cierra con una lista comentada de referencias de consulta obligatoria.

1. Amenazas globales: la globalización y la guerra

La globalización implica no solo el movimiento beneficioso de bienes, ideas, capitales y personas, sino también la distribución planetaria de productos que tienen efectos perniciosos y la agudización de problemas que anteriormente estaban más o menos sujetos a las fronteras nacionales. Algunos autores han calificado estas amenazas globales como «flujos globales negativos» (Ritzer, 2010). Ejemplos de estos flujos negativos que ahora traspasan las fronteras son las importaciones peligrosas para la salud por emplear sustancias químicas nocivas, los productos adulterados o las enfermedades infecciosas que se extienden a medida que sus portadores viajan por el mundo. En este módulo, no obstante, nos vamos a centrar en otras de estas amenazas globales: las guerras, el terrorismo y los nuevos riesgos digitales.

Como afirma Ritzer (2010), «es cada vez más difícil encontrar ejemplos de guerras que no se hayan visto afectadas por los procesos de globalización». Una cuestión importante respecto a la relación entre la guerra y la globalización reside en conocer si esta última hace que los conflictos armados sean más o menos probables. Están los que afirman que, dados los lazos crecientes entre las economías del mundo, asistimos a una disminución de la recurrencia de las guerras, porque las pérdidas en que incurrirían los países aumentan el coste de aquellas. Otros autores afirman, sin embargo, que las ganancias de las guerras han aumentado tanto que las naciones estarían ahora más dispuestas a entrar en conflicto unas con otras, aun a riesgo de deteriorar los lazos económicos. Entre los factores que favorecerían esta última situación, estarían:

- Unos flujos de comercio mundial de armamento en expansión; armamento cuyo precio relativo ha disminuido en las últimas décadas, lo que ha hecho más fácil su adquisición por parte de un mayor número de actores estatales y no estatales.

- La compresión del espacio y del tiempo gracias a la globalización (los ejércitos pueden ser movilizados con mayor rapidez y desplazados con mayor facilidad a través de largas distancias).

- Las nuevas tecnologías, que permiten ahora librar guerras sin la necesidad de estar físicamente presente en el lugar en el que se producen.

Un ejemplo del cambio en el papel jugado por el tiempo y el espacio, a la hora de iniciar un conflicto armado, lo tenemos en la invasión de Afganistán por parte de una coalición militar internacional tras los atentados en Nueva York en 2001. La coalición liderada por Estados Unidos tardó únicamente unos meses en reunir uno de los ejércitos multinacionales más poderosos de la historia reciente y en desplazarlo hasta Afganistán para combatir a las milicias taliba-

nes que gobernaban el país junto a Al Qaeda, responsable de los atentados. Otro ejemplo, relacionado con la necesidad de la presencia física de tropas a la hora de librar una guerra reside en la creciente utilización de drones y aparatos no tripulados, de sistemas de imagen a distancia, de cámaras de precisión montadas en estas aeronaves automáticas, de sistemas de guía basados en satélites y de misiles que pueden ser lanzados desde instalaciones terrestres o barcos militares situados a miles de kilómetros de sus objetivos.

Otro aspecto importante de la transformación del concepto contemporáneo de la guerra es el paso de la llamada «guerra industrial» a la «guerra de información». La guerra «industrial» solía implicar al Estado-nación, los sentimientos patrióticos, la lucha por el territorio, la movilización de una gran parte de la población, bajas a gran escala, las posiciones casi simétricas de dos ejércitos masivos enfrentados uno a otro, y el alineamiento y fervor de unos medios de comunicación que, por otra parte, no poseían una información muy detallada de lo que ocurría en el campo de batalla (Ritzer, 2010).

Por todo ello, podemos afirmar que la globalización tiene un efecto cuando menos incierto a la hora de incrementar o disminuir la probabilidad de las guerras, pero que su impacto en la transformación de las mismas es indudable (Ritzer, 2010).

2. Terrorismo global

El terrorismo puede ser definido como aquellas «acciones que causan muertes, heridas graves y serios daños a la propiedad pública o privada, lugares, instalaciones u otros sistemas, y que tienen por finalidad amedrentar a ciudadanos, gobiernos u organizaciones internacionales» (Ritzer, 2010). Si bien el terrorismo no es un fenómeno nuevo, su manifestación actual tiene algo de novedoso. El poder de los medios de comunicación y de las redes sociales permite que sus acciones tengan una repercusión planetaria. En cierta manera, parece que el principal fin de los ataques y asesinatos cometidos sea aterrorizar a personas y poblaciones muy alejadas del lugar en que tienen lugar los hechos, pero también –en particular cuando nos referimos a los atentados de Al Qaeda o del Estado Islámico (ISIS)– reclutar a potenciales miembros entre aquellos más susceptibles de ser receptivos a su mensaje.

Los grupos terroristas anteriores solían verse obligados a operar en su propio territorio, pero los actuales pueden atentar muy lejos de él, y de hecho lo hacen, buscando maximizar la atención de los medios de información en todo el mundo. En este sentido, los lugares elegidos suelen ser ciudades globales como Nueva York (atentados del 11 de septiembre de 2001), Londres (atentado en el metro en 2005), Boston (atentado en el maratón de 2013), París (varios atentados recientes, por ejemplo en 2015, simultáneamente en la sala de conciertos Bataclan y en otros lugares de la ciudad) o Barcelona (atentado en Las Ramblas en 2017).

Por otra parte, y dados los medios a su disposición, los terroristas pueden hacer llegar sus mensajes de forma inmediata a todo el planeta, controlando además un contenido que anteriormente dependía de la orientación que quisieran darle los medios de comunicación. En la actualidad, son los propios terroristas los encargados de difundir directamente su particular relato a través de internet, por medio de la utilización de blogs, de videos alojados en canales de YouTube y de herramientas de mensajería instantánea como Telegram, una aplicación que encripta la información y hace muy difícil descifrarla para los servicios de inteligencia.

Existen otras características que podemos asociar a este nuevo terrorismo global y que están directamente relacionadas con las transformaciones derivadas de la globalización (Ritzer, 2010):

- El desarrollo de los sistemas globales de transporte facilita que los terroristas se desplacen por el mundo para llevar a cabo sus acciones.

- Las fronteras nacionales son mucho más porosas, los Estados poseen crecientes dificultades para controlarlas, lo que provoca que los terroristas puedan moverse de un país a otro con facilidad.

- La globalización ha provocado una reacción adversa en varias regiones del mundo –Oriente Medio y el norte de África, por ejemplo–, que culpan a los países occidentales de causar o agravar sus problemas sociales y hace receptivos al mensaje de los radicales a muchos grupos entre sus poblaciones. Los terroristas suelen explotar las quejas de estos grupos desfavorecidos y señalar a los países desarrollados de Europa y Norteamérica como los culpables de la supuesta explotación que sufren, encontrando así una justificación para sus acciones violentas.

- Si bien con anterioridad los grupos terroristas basaban sus acciones en una u otra ideología política, los grupos actuales apelan a una idea amplia de identidad étnica y a las quejas contra la globalización.

Difícil control de fronteras

Los obstáculos jurídicos e institucionales a los que se enfrentan los Estados a la hora de controlar las fronteras nacionales se evidenciaron con ocasión de los atentados en París en 2015, y en Bruselas y Berlín, ambos en 2016. En todos estos casos, los terroristas fueron capaces de dejar rápidamente el país en el que habían cometido los atentados y escapar a otro país europeo. En el caso del terrorista del mercado de Navidad en Berlín, el atacante pudo huir hasta Italia sin ser detectado por la policía de ninguno de los países que cruzó en su escapada. Mientras los individuos tienen libertad de movimientos por todo el continente, los cuerpos de seguridad solo pueden actuar dentro de sus respectivos territorios.

La sofisticación de los atentados terroristas actuales es mucho mayor que la de las acciones anteriores y, al mismo tiempo, mucho más básica. Ejemplos de ambos extremos serían, por un lado, el secuestro y utilización de aviones comerciales en el atentado contra el World Trade Center de Nueva York en 2001 y, por el otro, los atentados de los llamados «lobos solitarios», individuos radicalizados e informalmente vinculados al Estado Islámico que emplean coches o camiones para arrollar al máximo número de peatones posible.

Una de las mayores preocupaciones de la comunidad internacional respecto al terrorismo global reside en la posibilidad de que estos grupos se hagan con armas químicas, biológicas o nucleares. En internet, está disponible actualmente una vasta cantidad de información que permitiría a individuos o grupos la fabricación de este tipo de armamento. No obstante, gran parte de esta información no es sistemática ni fiable. La efectividad de artefactos construidos a partir de la información disponible en las redes va a ser muy limitada si las personas implicadas no poseen una formación especializada en ingeniería o química, o si no tienen entrenamiento militar. Estos conocimientos especializados son mucho más importantes que la información de fuentes desconocidas a la hora de organizar atentados a gran escala (Larabee, 2015).

Respecto a sus métodos de organización, grupos como Al Qaeda se dividen en células en muchas ocasiones independientes entre sí y cuentan con el equivalente al sistema de franquicias de las empresas multinacionales: constantemente reciben la adhesión de grupos terroristas locales –en particular en África, Asia y Oriente Medio– que dicen compartir sus motivaciones y objetivos. Este sistema de franquicias es también el empleado por el Estado Islámico, pero llevado al extremo de que en ocasiones sus células consisten en un reducido número de personas –o incluso una persona sola– que no han tenido un contacto formal con el grupo y cuya radicalización y captación se ha producido vía internet. El Estado Islámico también se diferencia de Al Qaeda por sus conquistas territoriales. Hasta sus derrotas militares del año 2017, el ISIS controlaba gran parte del territorio de Irak y de Siria, donde estableció su llamado «califato».

3. Amenazas en la red y conflictos no convencionales

La llamada ciberguerra constituye quizá la dimensión de los conflictos bélicos en la que el impacto de las nuevas tecnologías resulta más evidente. Los episodios de ciberguerra son inéditos en la historia de la humanidad y están estrechamente asociados al desarrollo de internet.

El riesgo de una ciberguerra es directamente proporcional al desarrollo de internet. En la actualidad, existen cientos de millones de páginas web y billones de usuarios de internet. Dado que ningún sistema ni software ha logrado demostrar su invulnerabilidad, esta enorme interconexión de usuarios y servicios ofrece múltiples posibilidades para un ataque por parte de *hackers* (Chng, 2013).

Cuando hablamos de ciberguerra, podemos estar refiriéndonos a alguna de estas tres dimensiones (Orend, 2014):

- Espionaje. La utilización de internet para reunir información que un país considera –y protege– como clasificada, confidencial o secreta por razones de seguridad nacional.

- La difusión de información falsa mediante el empleo de internet para dañar la seguridad de un país o los intereses vitales del mismo.

- Sabotaje. El empleo de internet para destruir, dañar o interferir en el funcionamiento de sistemas cuyo funcionamiento es esencial para una comunidad política, como suministros básicos o telecomunicaciones.

La posibilidad de que *hackers* al servicio de gobiernos o grupos no estatales desaten una guerra entre Estados en un contexto de seguridad globalizada como el actual es perfectamente real. El ciberespacio se ha convertido cada vez más en un espacio de conflicto en el que los gobiernos son vulnerables al sabotaje, la manipulación o la destrucción de información, la interrupción de las comunicaciones y de las transacciones económicas y el robo de información clasificada (Mansbach, 2013). Las telecomunicaciones, las finanzas, las redes de suministro y almacenamiento energético y el control de las centrales de producción de energía, los transportes, el suministro de agua, los servicios públicos y la defensa…, todos estos sectores son susceptibles de ser atacados por *hackers* que trabajen para un gobierno extranjero o por individuos y grupos independientes.

Los casos de Estonia y Georgia

Estonia sufrió en 2007 un ataque que tenía su origen en Rusia. Estonia es un país especialmente vulnerable a los ciberataques por su dependencia de las conexiones por internet. La mayor parte de los estonios emplean internet y telefonía móvil para sus gestiones diarias, desde gestiones administrativas hasta operaciones bancarias. Los *hackers* rusos lograron paralizar las operaciones financieras y los servicios de telefonía en Estonia. Asimismo, en 2008, durante su breve guerra con Rusia, Georgia fue víctima de un ciberataque procedente de ese país.

Los casos más destacados de intervención fraudulenta en las redes con intención de desestabilizar un sistema político –o difusión de información falsa, en palabras de B. Orend– son aquellos en que los *hackers* –generalmente rusos–

han tratado de influir en los resultados de unas elecciones en un país occidental sembrando las redes sociales de noticias falsas sobre los candidatos. El ejemplo más conocido es el de las elecciones presidenciales en Estados Unidos en 2016, pero también se constataron intentos rusos de influir en las elecciones presidenciales francesas y en las legislativas en Alemania en 2017. En el transcurso de la investigación en el Senado estadounidense de las interferencias rusas en las elecciones, se descubrió que Rusia intentó asimismo influir en el resultado de la consulta sobre la independencia de Cataluña de octubre de 2017.

Para combatir la amenaza de las campañas de desinformación se han sugerido, entre otras, las siguientes medidas (Hwang, 2017):

- Contar con mejores **instrumentos de comprobación de la veracidad de los datos** (*fact-checking*) que permitan establecer la autenticidad de la información que circula por las redes.

- **Educar a los usuarios en la utilización de las redes sociales**, en particular a la hora de evaluar la calidad de la información consultada.

- Estudiar la efectividad de **etiquetas que nos avisen de la veracidad de las informaciones** contenidas en determinados sitios web, etiquetas que puedan ser interpretadas por los sistemas informáticos e incluidas en los algoritmos empleados por páginas como Google o Facebook a la hora de mostrarnos resultados de búsqueda.

- Apoyar el **periodismo de calidad** y promover iniciativas públicas y privadas que permitan el mantenimiento del periodismo de investigación.

- Establecer **sistemas de alerta pública** por medio de legislación que obligue a las plataformas en línea a aportar información al público acerca de campañas de desinformación de una cierta relevancia, lo que permitiría a investigadores, periodistas y usuarios estar alerta y evaluar la autenticidad de la información existente.

4. Lecturas obligatorias

Hough, P. (2004). *Understanding Global Security* (cap. 1: «Security and securitization»). Londres: Routledge.

El capítulo de Hough se presenta como un glosario sobre los conceptos de seguridad y «securitización», y explica las diferentes teorías relativas a los diversos aspectos incluidos en estos conceptos. También estudia el papel de la seguridad para realistas, pluralistas y otras teorías de las relaciones internacionales, los actores relevantes y los procesos de securitización.

Navari, C. (2006). «Globalization and security: much ado about nothing?». En: W. Bain (ed.). *The Empire of Security and the Safety of the People*. Abingdon, Oxon: Routledge.

El texto de Cornelia Navari analiza el potencial impacto de la globalización en las ideas tradicionales de seguridad, abordando distintas dimensiones. ¿Puede la globalización agudizar el conflicto étnico? ¿Qué consecuencias puede tener para el medio ambiente? ¿Supone un retroceso del Estado? ¿Cuál es el impacto de la globalización en las políticas de desarrollo y cooperación internacional? Y, por último, ¿qué papel juega la geopolítica de la seguridad?

Orend, B. (2014). «Fog in the fifth dimension: The ethics of cyber war». En: L. Floridi; M. Taddeo (eds.). *The Ethics of Information Warfare*. Berlín, Heidelberg: Springer.

Brian Orend intenta definir en su capítulo el concepto de ciberguerra, en qué formas puede encarnarse, y cuáles son las actitudes o posiciones respecto al concepto en relación con las teorías convencionales sobre la guerra –realismo, teorías sobre la guerra justa, pacifismo, etc.–, y en relación con sus procedimientos y sus consecuencias. Se trata de un análisis ético sobre la guerra, pero aplicado en este caso a la que se libra en un espacio digital.

Bibliografía

Chng, G. (2013). «Cyber War: One Strike, and you're Out». En: R. Mansbach; E. Rhodes (eds.). *Introducing Globalization. Analysis and Readings*. Thousand Oaks, CA: Sage-CQ Press.

Hwang, T. (2017). «Digital Disinformation: A Primer». Konrad Adenauer Stiftung / Atlantic Council - Eurasia Center.

Mansbach, R. (2013). «Cyber War and Institutional Vulnerability». En: R. Mansbach; E. Rhodes (eds.). *Introducing Globalization. Analysis and Readings*. Thousand Oaks, CA: Sage-CQ Press.

Larabee, A. (2015). «Terrorism and Technology». En: R. D. Law. *The Routledge History of Terrorism*. Londres: Routledge.

Orend, B. (2014). «Fog in the fifth dimension: The ethics of cyber war». En: L. Floridi; M. Taddeo (eds.). *The Ethics of Information Warfare*. Berlín, Heidelberg: Springer.

Ritzer, G. (2010). *Globalization. A Basic Text*. West Sussex: Wiley-Blackwell.