Crisis de Ucrania y Rusia: terrorismo y ciberataques

Institute for Economics and Peace

He aquí un análisis de la frecuencia de los atentados terroristas cometidos en Rusia, Ucrania y Georgia en el pasado, así como de los ciberataques contra Kiev en los últimos 10 años y los preparativos de la guerra actual.

El terrorismo ha ido aumentando a medida que se intensificaba el conflicto. Tanto la guerra de Georgia en 2008 como la de Ucrania en 2014 provocaron un enorme incremento de la actividad terrorista, y, a medida que se intensifique la actual guerra, es previsible que crezca también.

Por otro lado, los ciberataques contra Ucrania han aumentado significativamente en el último decenio, sobre todo en los meses y semanas inmediatamente anteriores a que comenzaran los enfrentamientos. Además, los ciberataques pueden extenderse de manera involuntaria a otros países debido a la conectividad global, cuyos efectos hemos visto en numerosas ocasiones. Como este tipo de acciones son un fenómeno reciente, y dado lo difícil que es atribuírselos, el límite entre ciberataque, guerra cibernética y ciberterrorismo no está claro.

Terrorismo en Rusia, Ucrania y Georgia

El terrorismo en Ucrania y Georgia estuvo vinculado sobre todo a los conflictos con Rusia, en 2008 y 2014, respectivamente. Aparte de esos dos periodos, las acciones terroristas han sido escasos en ambos países. Si nos guiamos por las tendencias pasadas, es de suponer que este tipo de actividad aumentará considerablemente ahora con la guerra. En general, el nivel de terrorismo es proporcional a la intensidad del conflicto. Por otra parte, los atentados son una táctica muy utilizada en la guerra asimétrica y suelen tener como objetivo las infraestructuras militares, policiales y gubernamentales. Si Rusia se hace con el control y nombra un gobierno títere, lo más probable es que encuentre una fuerte resistencia y se enfrente a una insurgencia continua. Myanmar es un ejemplo: en 2021, un golpe militar derrocó el Ejecutivo elegido democráticamente y, a partir de ese momento, el terrorismo se multiplicó por 23, con el resultado de 521 muertos.

En los últimos seis años, el terrorismo en la región de Rusia y Eurasia ha disminuido. El 93% de los atentados cometidos en la zona desde 2007 se produjeron antes de 2016, lo que deja bien claro lo pronunciado que ha sido este descenso. El terrorismo alcanzó su apogeo en la región en 2010, tras la guerra entre Rusia y Georgia, con 339 atentados y 318 muertes registradas en ese año.

Desde 2007, el grupo terrorista más activo en la zona es Shariat Jamaat, que, con sus afiliados, provocó 315 atentados y 257 muertes, la mayoría de ellas en Rusia. A ellos les sigue el Emirato del Cáucaso, al que se atribuyen 39 atentados y 134 muertes.

Aunque fundamentalmente es un grupo *yihadista*, Shariat Jamaat, también conocido como Vilayat Dagestan, está estrechamente relacionado con los conflictos separatistas de las repúblicas rusas de Chechenia e Ingusetia. Shariat Jamaat también mantenía vínculos con el Emirato del Cáucaso. El grupo dejó de actuar tras la muerte de sucesivos jefes a manos de las fuerzas especiales rusas. El autoproclamado Estado Islámico también ha actuado en la región durante las dos últimas décadas, con 36 atentados y 102 muertes registradas desde 2007.

La mayoría de los atentados no fueron reivindicados por ningún grupo terrorista reconocido. Hay 1.122 atentados y 846 muertes, el 73 % de ellos, de autoría desconocida.

Rusia es el país que, casi de forma sistemática, ha sufrido el mayor número de ataques y muertes por terrorismo de la región, con 1.312 atentados y 1.179 muertes registradas desde 2007. En la última década han experimentado un descenso constante, hasta el punto de que en 2021 no hubo más que uno que se saldó con dos muertes.

De los últimos veinte años, el periodo transcurrido entre la guerra con Georgia y la anexión de Crimea fue en el que más atentados hubo en Rusia, con un 87% de ataques y víctimas mortales entre 2008 y 2014. En Georgia, la actividad terrorista refleja la tendencia rusa, ya que el 90% de los atentados terroristas registrados se produjeron durante ese mismo periodo. Ucrania es el segundo país con mayor número de ellos en la región desde 2007, con un total de 108 y 17 muertos. Los atentados y las muertes alcanzaron su máximo, 58 atentados y 10 muertes, en 2015, lo que se corresponde con el conflicto con Rusia. Desde entonces ha habido un descenso bastante continuo, puesto que no hubo acciones de este tipo en Ucrania en 2021 y solo uno en 2020.

Desde 2007 no ha habido más que un atentado reivindicado por un grupo, Odessa Underground; los 107 atentados restantes no fueron reivindicados por ninguna organización conocida.

El aumento de las manifestaciones violentas coincide con la tendencia mundial, según la cual éstas aumentaron un 10% anual entre 2010 y 2020.

A pesar de haber disminuido el 9% en 2021, Rusia sigue siendo el país de la región en el que más protestas y disturbios violentos se producen, con 1.337 incidentes. Le sigue Ucrania, con 1.052 incidentes en 2021, un descenso del 23% respecto al año anterior.

Rusia, Ucrania y Bielorrusia fueron los únicos países de zona en los que hubo más de 1.000 manifestaciones violentas en 2021.

Asimismo, en el este de Ucrania han actuado grupos insurgentes separatistas. Desde 2014, los conflictos relacionados con la República Popular de Donetsk (RPD) y la República Popular de Luhansk (RPL) han causado más de 4.000 muertes en combate. El pico se produjo en 2014, año en el que hubo casi 3.000 muertes en combate.

Ciberterrorismo, la guerra de Ucrania y los ciberataques rusos

La dependencia cada vez mayor de las comunicaciones y la tecnología de la información ha hecho que Internet haya adquirido un gran interés para los actores perversos y hayan aparecido términos como “ciberataques”, “ciberguerra” y “ciberterrorismo”. Pero clasificar un incidente informático dentro de una de estas tres categorías es complicado. Muchas veces, es difícil clasificar un incidente porque resulta difícil rastrear el origen del ataque, de modo que no están claros el autor, los motivos ni el objetivo previsto. Sin esos datos, es difícil delimitar qué constituye una guerra (acciones llevadas a cabo por Estados) y qué terrorismo (acciones de origen no estatal). Esta confusión es la base de la guerra híbrida, en la que, para desestabilizar, se utilizan herramientas civiles y militares y operaciones a la luz del día y encubiertas.

El mundo cibernético está convirtiéndose en uno de los campos de batalla cruciales de la guerra híbrida. En la Cumbre de Varsovia de 2016, la OTAN reconoció el ciberespacio como el quinto ámbito de batalla y declaró que un ciberataque es un posible caso de aplicación del Artículo 5, que estipula que un ataque contra un miembro es una agresión contra todos. En la actualidad, este artículo se refiere a un ataque armado físico y carece de una definición cibernética compatible. Por tanto, son los 30 Estados miembros de la OTAN los que tendrán que definir qué es una ciberguerra tras un ciberataque de suficiente entidad.

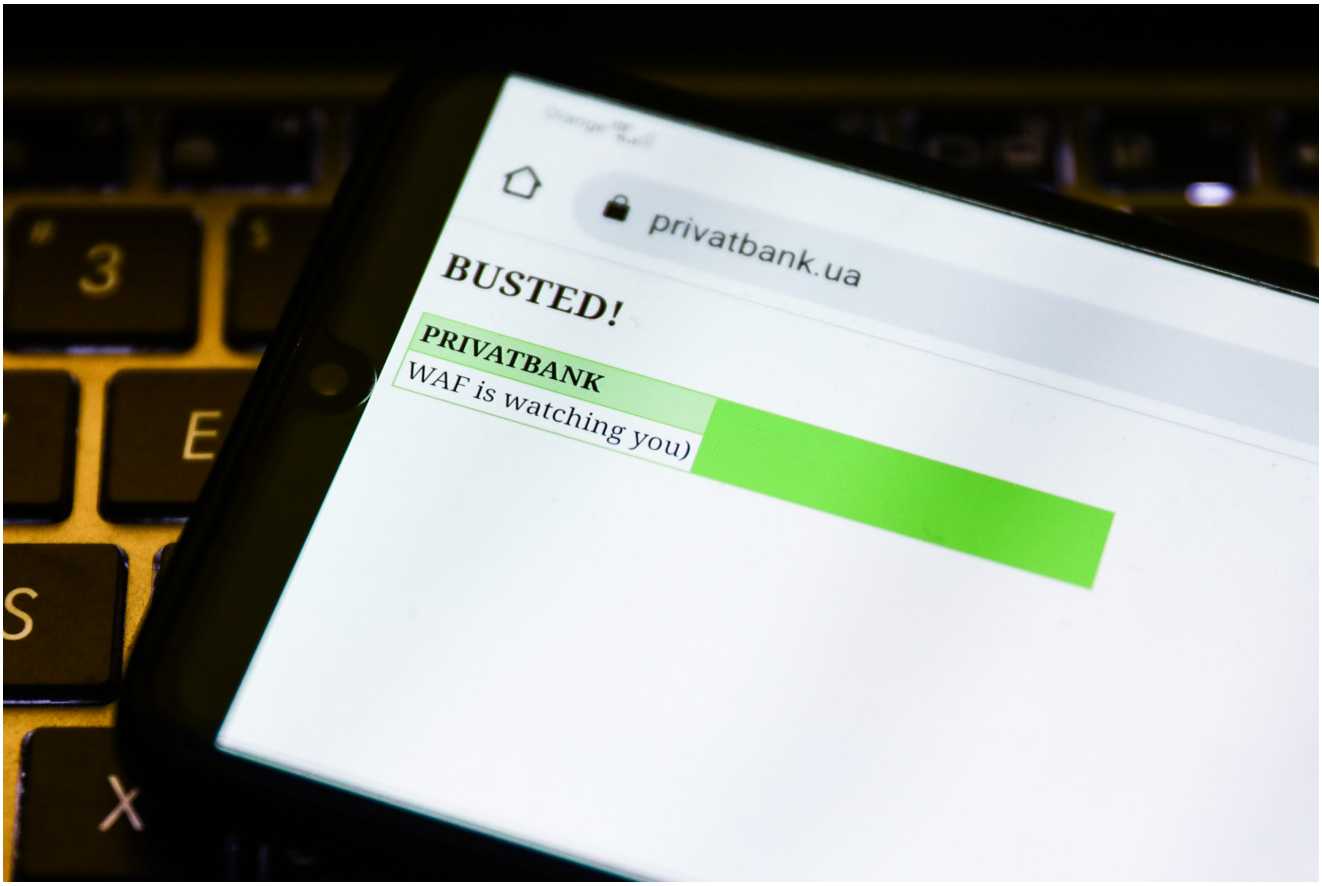
Por otra parte, un acto terrorista convencional se considera terrorismo cuando la acción es obra de un agente no estatal y su objetivo es utilizar la violencia o amenazar con ella para transmitir un mensaje a un público más amplio, no solo los directamente afectados por la violencia. Por tanto, los ataques de Rusia contra el Gobierno, las infraestructuras y las empresas de Ucrania no son un acto de ciberterrorismo. Fuera de una situación de guerra, tampoco está clara la clasificación de los ciberataques emprendidos por los gobiernos como ciberataques o ciberguerra.

El uso creciente de los ciberataques hace que para la comunidad mundial sea necesario refinar

las definiciones de ciberguerra, ciberterrorismo y ciberataque. La decisión tendrá consecuencias de peso, porque de ello dependerá saber si un grupo pertenece al ámbito de la legislación terrorista o si se ha declarado un acto de guerra. Hoy no está claro, por ejemplo, en qué circunstancias un ciberataque contra un miembro de la OTAN constituiría un acto de ciberguerra.

Ciberataques en Ucrania

La crisis actual en Ucrania ha obligado a prestar más atención a los ciberataques. A escala mundial, el número de ellos ha aumentado de forma considerable en el último decenio. No sabemos aún en qué medida se utilizarán en la guerra actual. En las semanas anteriores al conflicto, varios sitios web sufrieron ataques de denegación de servicios (DDoS). En estos momentos, el Gobierno ucraniano está creando un ejército informático internacional, formado por *hackers* voluntarios. Anonymous ha declarado la ciberguerra al Ejecutivo ruso. En las primeras 24 horas, el grupo reivindicó la inutilización varios sitios web del Gobierno.



En los últimos años, Ucrania ha sufrido ciberataques constantes, muchos de los cuales se atribuyen a Rusia. En 2020 sufrió 397.000 ataques y en los primeros 10 meses de 20201

alrededor de 280.000. Las acciones de este tipo fueron tan amplias que la UE envió un Equipo de Respuesta Informática Rápida para ayudar.

Desde que Vladímir Putin es presidente, se han atribuido a Rusia numerosos ataques informáticos en todo el mundo. Dichas acciones pueden emprenderse con gran rapidez, de forma independiente o en coordinación con otras operaciones físicas. Además dependen menos del tiempo y la distancia y son relativamente baratos de llevar a cabo. Y, lo que es más importante, es excepcionalmente difícil defenderse frente a ellos, porque se presentan en formas muy variadas. Además, la interconectividad de la Red hace que los programas maliciosos pueda transferirse fácilmente y sin querer a terceros contra los que no estaban destinados.

El uso de ciberataques por parte de Rusia comenzó tras la retirada rusa de Georgia en 2008.

El uso creciente de estas ciberagresiones puede ser un indicador de que se está planeando algo perverso. Por ejemplo, en enero de 2022, al tiempo que se intensificaban los esfuerzos diplomáticos, Ucrania sufrió un ciberataque generalizado contra varios departamentos gubernamentales. La acción consistió en un mensaje que decía: “¡Ucranianos! … Se ha hecho pública toda la información sobre vosotros. Tened miedo y esperad lo peor. Es vuestro pasado, presente y futuro”. El mensaje incluía una reproducción de la bandera de Ucrania y un mapa tachado con una referencia a la “tierra histórica”. Hay que subrayar que, poco después de esto, el Ministerio de Defensa sufrió un ataque de denegación de servicios, igual que PrivatBank y Oschadbank, aunque en estos dos casos la acción consistió más bien en una manipulación informativa, porque se trató de mensajes que decían que los cajeros automáticos no funcionaban. Quizá la intención era causar más pánico.

Las operaciones de ciberataque, en su mayoría, corren a cargo de la Dirección Principal de Inteligencia rusa (GRU) y otras entidades que no están oficialmente afiliadas al Estado ruso, lo que permite que el Moscú niegue toda relación con ellas.

Uno de los primeros ejemplos de ciberataques lanzados por Rusia se produjo en diciembre de 2015, cuando las redes de los sistemas de control industrial de Ucrania fueron objeto de un programa malicioso que provocó cortes de electricidad en la región occidental de Ivano-Frankivsk; alrededor de 700.000 hogares se quedaron sin luz durante varias horas.

Un año después, la red eléctrica ucraniana sufrió el ataque de un programa malicioso, denominado CrushOverride, que apagó parte de la capacidad energética de Kiev durante una hora. El ataque comenzó con la intromisión en una subestación de 330 kilovatios de una serie de elementos externos que permanecieron dentro del sistema informático, inadvertidos, durante

seis meses, y en ese tiempo adquirieron más conocimientos sobre el sistema. Parece que los responsables del ataque fueron unos *hackers* que querían probar un nuevo programa malicioso diseñado para atacar redes de energía eléctrica y se cree que el programa podría adaptarse para atacar otras infraestructuras críticas. Rusia siguió promoviendo ciberataques como los de NotPetya, programas cuyo fin era inutilizar los datos contenidos en un sistema.

El programa se propagaba a través de los programas que utilizan las empresas y los particulares para presentar la declaración de impuestos en Ucrania. Con su código, aunque los usuarios pagaran, nunca podrían recuperar sus datos, así que no era estrictamente *ransomware* (que secuestra datos y pide un rescate), puesto que su objetivo era destruirlos. El programa malicioso se extendió a otros países, incluido Estados Unidos. El Departamento de Justicia estadounidense acusó a seis oficiales del GRU de desplegar el programa NotPetya, que afectó a hospitales y centros médicos de todo el mundo. El coste económico, solo para EE UU, fue de aproximadamente 1.000 millones de dólares.

Otro ejemplo fue la operación Exchange Marauder, consistente en que unos piratas informáticos rusos encontraron supuestamente una puerta trasera en Microsoft Exchange que les permitió acceder a cuentas de correo electrónico y redes asociadas de todo el mundo, en países como Australia, Estados Unidos y Ucrania.

La amenaza de contagio

Cada vez preocupa más la posibilidad de que los ciberataques se extiendan más allá de Ucrania. Jeremy Fleming, director de la Sede de Comunicaciones del Gobierno (GCHQ) de Gran Bretaña, ha pedido a los responsables de proveer y mantener las infraestructuras críticas que estén más atentos. La preocupación por la posibilidad de contagio es doble. En primer lugar, no está claro hasta dónde puede llegar un ciberataque debido a la interconectividad entre personas y entidades, como se vio con NotPetya o WannaCry.

En segundo lugar, si la guerra no avanza como esperaba y Putin considera que el suministro de armas por parte de los países europeos a Ucrania es un acto hostil, quizá ordene a los *hackers* rusos que amplíen sus maniobras y traten de paralizar a quienes se opongan a la campaña rusa.

Varios países bálticos han sufrido ciberataques de origen ruso. Un ejemplo de uno de ellos, el denominado “Ghostwriter”, infectó al menos a siete miembros del *Bundestag* alemán y a 31 parlamentarios de las cámaras estatales. Comenzó en Lituania, Letonia y Polonia con la

difusión de desinformaciones para incitar a oponerse a la OTAN y después se trasladó a Alemania.

Es evidente que Rusia comprende la importancia de la informática para alcanzar objetivos políticos globales, recurriendo a entidades afiliadas y no afiliadas.

El ciberterrorismo puede ser una herramienta eficaz para quienes desean alcanzar unos objetivos políticos concretos y carecen de los recursos necesarios para llevar a cabo ataques convencionales selectivos contra edificios, instituciones u organismos gubernamentales.

Además, cuando un gobierno emprende un ataque físico, existe el riesgo de que se desencadene una guerra, mientras que no está tan claro cuándo un ciberataque es suficientemente importante para declarar la guerra.

Debido a la interconexión global, estas acciones pueden llegar a perjudicar a la sociedad en general y causar destrucción y pánico en todas partes, sobre todo si el atacante ha conseguido introducirse en el sistema y tiene el programa malicioso preparado para hacer el máximo daño.

El peligro del ciberterrorismo y los ataques informáticos, cada vez más generalizados, es que, como sucede con la violencia, las sociedades pueden acostumbrarse y considerarlos parte del

precio que hay que pagar por vivir. Pero eso nos lleva a una perspectiva inquietante: si no se toman las medidas necesarias contra los autores de este tipo de acciones y, por consiguiente, se normalizan, crece la probabilidad de que vuelva a haber ataques de ese tipo y de que todas las partes de un conflicto estén más dispuestas a desencadenarlos contra sus adversarios.

Traducción de María Luisa Rodríguez Tapia.

Fecha de creación
16 marzo, 2022