El ciberterrorismo es la nueva frontera

Serge Stroobants

Frente a este nuevo desafío sigue faltando que los Estados recuperen la iniciativa en la batalla contra el ciberterrorismo, pasando de estrategias defensivas a otras de carácter más ofensivo.

Europa se ha visto arrojada al epicentro de la reciente evolución del terrorismo, y Francia, que ocupa el puesto número 30 en el Índice de terrorismo global 2017, lo refleja con su exposición a los atentados de nuevo cuño en los últimos años. Este país es uno de los que ocupan puestos más altos en el Índice sin estar envueltos en un conflicto armado, que suele ser el principal impulsor de la actividad terrorista. Su puntuación es tan elevada porque en años recientes ha sufrido muchos atentados cometidos por primera vez: tácticas guerrilleras, guerrilla urbana, atentados suicidas en París y un atentado con un camión en Niza ponen en evidencia una sociedad y unos servicios de seguridad desacostumbrados a las nuevas amenazas terroristas y mal adaptados para subsanar las vulnerabilidades derivadas de ellas. A eso hay que añadir la combinación de terrorismo y mundo informático, que convierte en arma la propaganda y la

ideología, difunde convicciones extremistas, facilita el reclutamiento y la radicalización e incluso galvaniza e impulsa directamente atentados terroristas.

Eso es lo que ocurrió con la decapitación de un sacerdote francés en Normandía, en julio de 2016, cuyos autores no solo se habían radicalizado en Internet sino que recibían sus directrices y sus órdenes a través de las redes de telefonía móvil. Se trata de una tendencia más amplia, de la que ya advirtió la Financial Action Task Force (Grupo de acción financiera contra el blanqueo de dinero) en 2015: la Red es la herramienta más utilizada para reclutar y para apoyar a las organizaciones terroristas.

Aunque los servicios de seguridad internos han reaccionado frente a estos atentados con la ayuda de unidades militares y de los servicios de inteligencia, las organizaciones terroristas han encontrado una vulnerabilidad que está a caballo entre la seguridad interna y la seguridad externa. En esta zona gris entre el terrorismo y la insurgencia, entre técnicas y objetivos convencionales y no convencionales, entre el mundo real y el mundo virtual, es muy difícil dar con las medidas de prevención y respuesta apropiadas.

Siria ha sido una prueba de fuego para la aparición *del mando y control remoto*. Muchos atentados terroristas cometidos en Europa no solo se planificaron en Siria sino que estuvieron organizados en directo desde allí, a través de Internet y plataformas de comunicación encriptadas. Pese a la derrota sobre el terreno de grupos como Daesh, que ya no tienen capacidad de planear y ejecutar atentados contra objetivos europeos, sigue existiendo la amenaza de los terroristas locales, sobre todo en la medida que esos grupos han pasado de fomentar el traslado para librar la *yihad* en Oriente Medio a recomendar a sus seguidores que ataquen en sus propios países.

A la hora de cometer sus crímenes, este terrorismo local o de *lobos solitarios* puede estar inspirado y controlado por grupos terroristas y agentes externos, y los Estados no reaccionan contra este nuevo tipo de atentados hasta después de que se haya producido el primero. Ante los ataques de ciberterrorismo y con el fin de recuperar la seguridad, especialmente en Europa, los Estados deben dar el primer paso y tomar medidas preventivas, para lo cual tienen que informarse más sobre las estrategias, herramientas y técnicas del terrorismo informático. No se puede luchar en guerras nuevas con las estrategias de las anteriores: el ciberterrorismo es la nueva frontera.

La seguridad informática es un problema nuevo y que preocupa mucho a diversos Estados y organizaciones, en paralelo a una conciencia cada vez mayor de las vulnerabilidades de la Red y de cómo se aprovechan, con ataques de denegación de servicio y *software* malicioso. Con la importancia fundamental del ciberespacio en la vida diaria, los ataques informáticos son cada

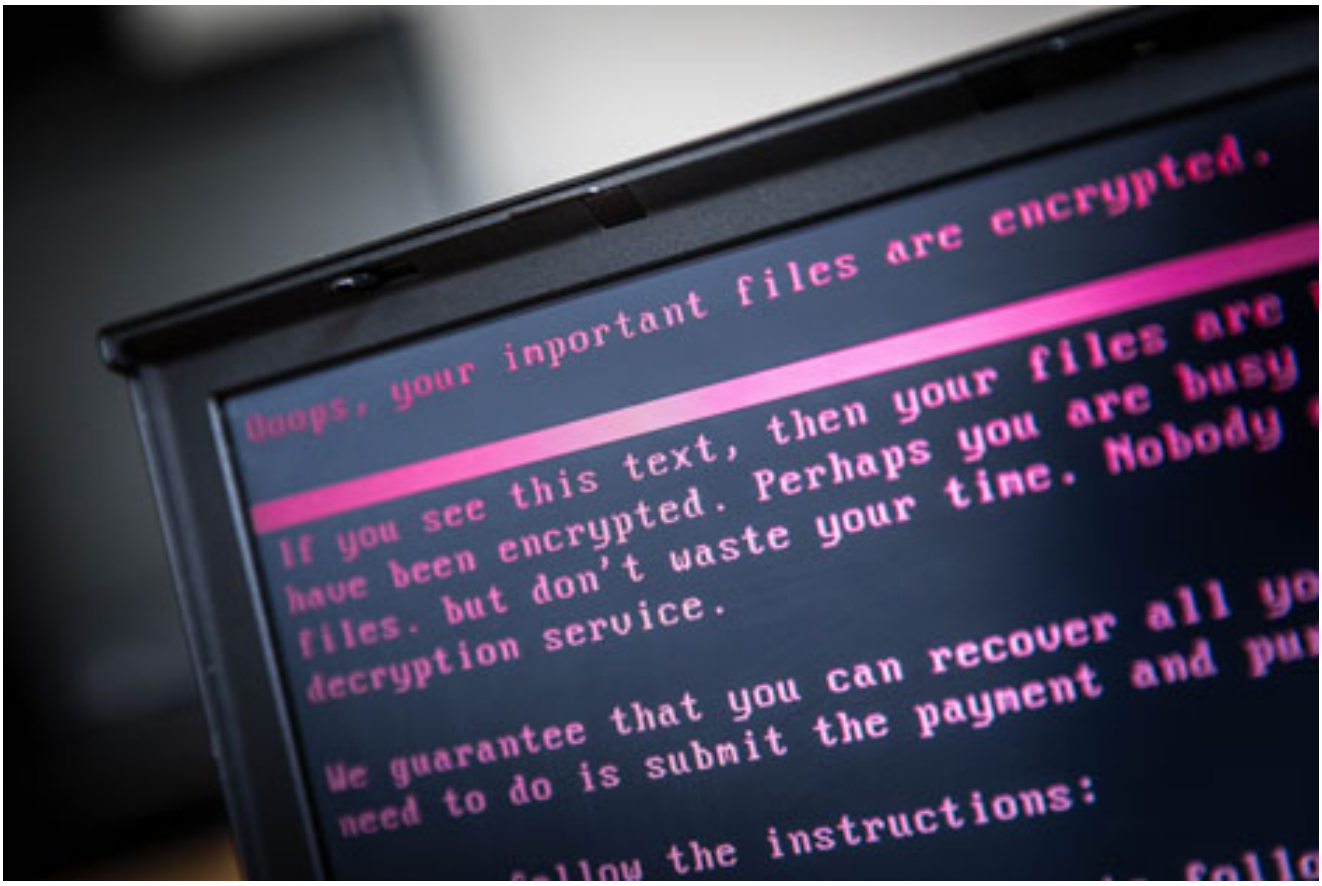
vez más peligrosos, disruptivos y frecuentes.

En los últimos años ha habido ataques contra servicios civiles como el acceso a Internet, los sistemas hospitalarios y las redes de suministro eléctrico, cometidos tanto por Estados como por agentes no gubernamentales. Entre los mayores ataques no gubernamentales contra estructuras críticas estuvo el apagón del Sistema Nacional de Salud británico durante el ataque llamado de *Wannacry* en 2017. Estas agresiones socavan la seguridad nacional e internacional, pueden dañar infraestructuras críticas y, por tanto, pueden afectar a la seguridad de los ciudadanos; de ahí la idea de ciberterrorismo. Este es una agresión contra infraestructuras electrónicas por motivos políticos o con el fin de causar e inspirar miedo en la población general por medios electrónicos.

El ciberterrorismo es una estrategia conocida desde que el líder de la filial de Al Qaeda Jemaat Islamiyah dedicó un capítulo de sus textos extremistas a criticar las redes informáticas de Estados Unidos por su vulnerabilidad al blanqueo de dinero y el fraude con tarjetas de crédito. Lo acompañó de una especie de hoja de ruta que mostraba conexiones con mentores piratas y páginas web en las que se explicaba cómo llevar a cabo un ataque informático y cómo ocultar la identidad. Es bien sabido que Daesh ha utilizado la relativa anarquía del ciberespacio para perpetuar su forma de terrorismo, movilizando a células con mensajes encriptados para planear, reclutar y cometer sus atentados y con especial atención al *terrorismo local.* Es una estrategia diferente a la anterior, de animar a los partidarios a que viajaran a las zonas de conflicto. Además, Daesh ha recurrido a la piratería informática: entró en las bases de datos del Departamento de Defensa de EE UU y robó los datos del personal militar, que luego publicó en la Red para convertirlos en objetivos, junto a manuales detallados de instrucciones para fabricar explosivos caseros y peticiones de dinero.

Las organizaciones terroristas como Daesh no pueden existir sin financiación, y aquí también interviene el ciberterrorismo. Un destacado agente de Al Qaeda, encargado de publicar vídeos extremistas y de radicalización en Internet, robó más de 30.000 números de tarjetas de crédito, blanqueó el dinero robado a través de portales de apuestas en la Red y después transfirió el dinero blanqueado a cuentas bancarias con las que se compraban armas y se financiaba a la organización en general. Este sistema de fraude con tarjetas de crédito en Internet se utilizó para financiar en parte los atentados del metro de Londres en 2005, lo cual demuestra las posibilidades de la conexión ciberterrorista. Por ejemplo, el agente de Al Qaeda pudo disponer de una serie de herramientas —VPN, *proxies* y *software* para ocultar la dirección IP— que le permitieron ocultar su identidad, e incluso utilizó empresas con sede en Estados Unidos para albergar su propaganda terrorista.

Los ciberataques no necesitan ser tan físicos para causar daños, ni tan letales para provocar el miedo. En su mayoría, estos ataques comienzan de forma inocua, con una mera suplantación de identidad mediante un archivo adjunto a un correo e infectado con un virus. La víctima abre el archivo adjunto, que descarga el código malicioso en la red de forma que se contagia a otros ordenadores. Se sospecha que esta fue la táctica empleada cuando el cibercalifato de Daesh se apoderó del perfil de Twitter del Mando Central estadounidense y filtró estrategias y nombres de militares. La suplantación de identidad da al pirata acceso a los mismos datos al alcance del usuario legítimo: información financiera, informaciones clasificadas o delicadas, el comportamiento de un sistema crítico e incluso el acceso a las redes de suministro o electricidad.



Las instituciones financieras son blanco del terrorismo desde hace mucho tiempo, y en la Red ocurre lo mismo. En el caso del asalto a un banco de Bangladesh en 2016, se instaló en el sistema informático del banco un *software* malicioso, probablemente enviado en un correo electrónico. El programa recogió contraseñas y nombres de usuarios y después borró las huellas de su presencia, es decir, se volvió prácticamente invisible. Las credenciales robadas se utilizaron para acceder a SWIFT, el sistema de transferencias internacionales de dinero más seguro del mundo. En cuatro transacciones se perdieron 81 millones de dólares. Con el mismo método, un agente de Hizbut Tahrir al Islami defraudó a varios bancos a escala mucho menor a

base de transacciones falsas o dobles transacciones que llevaba a cabo desde su café de Rusia y después utilizó el dinero robado para financiar su grupo terrorista.

Los ataques de denegación de servicio distribuido (DDoS en sus siglas en inglés) también son métodos populares, fáciles y baratos de trastocar la vida ciudadana. Consisten en inundar el sistema de una institución con mensajes y solicitudes constantes hasta rebasar el ancho de banda y forzar a esa entidad a desconectarse por haber sobrepasado la capacidad de la línea de datos. Esta sobrecarga deja el servicio o la red inutilizable o inaccesible a los usuarios. El cibercalifato de Daesh empleó este tipo de ataques contra páginas web de los gobiernos de Yemen e Irak en enero de 2017 y obligó a cerrarlas durante dos meses, hasta que pudieron volver a abrirse en servidores nuevos que incluían protección contra los DDoS.

Otros métodos muy utilizados son los ataques con *ransomware*, es decir, los secuestros de datos, que combinan la denegación de servicios con la posibilidad de beneficiarse económicamente. Consisten en apoderarse de la infraestructura informática de una institución y mantenerla secuestrada, de modo que la entidad afectada tiene que pagar un rescate para recuperar el control y el acceso a sus propios sistemas. Europa sufrió un secuestro de datos generalizado en mayo de 2017, con el ataque de *Wannacry*. Esta acción surtió especial efecto en Reino Unido, donde los hospitales se quedaron sin poder acceder a los historiales médicos y tuvieron que cancelar citas y operaciones, y 16 de ellos se vieron obligados a cerrar. En Estados Unidos, en la ciudad de Atlanta, los servicios de emergencias no pudieron usar sus bases de datos, y los servicios ciudadanos quedaron desconectados cuando unos piratas no identificados desplegaron su *software* malicioso y exigieron 51.000 dólares en bitcoins para devolver el control a la ciudad.

El terrorismo se ha afianzado en el ciberespacio como respuesta natural a las medidas militares y de seguridad tradicionales. Las organizaciones internacionales han reconocido que se tratade una zona de guerra nueva: en la cumbre de Varsovia de 2016, la OTAN declaró que el ciberespacio era un nuevo campo de batalla y una justificación para invocar la defensacolectiva. Sin embargo, los Estados suelen desarrollar sus propias políticas individualmente, yla cooperación internacional en este campo sigue siendo escasa. Aunque la Comisión Europea, recientemente, indicó que la UE debe dirigirse hacia un mercado único de la seguridad informática, con comunicaciones abiertas entre los Estados, criterios normalizados para certificar las conexiones seguras de Internet y un intercambio cada vez mayor de información sobre el ciberterrorismo, todavía no existe una estrategia mundial homogénea para abordareste reto. Si bien Estados Unidos y Gran Bretaña cuentan con instituciones sólidas y biendotadas para hacer frente al ciberterrorismo, otros Estados no están tan bien preparados yestán tratando de afrontar las amenazas en la Red completamente por su cuenta.

La estrategia antiterrorista aprobada por la UE en 2005 se centra en cuatro pilares: prevención, protección, persecución y reacción. El objetivo de la prevención es abordar las causas de la radicalización y el reclutamiento de terroristas. La protección hace hincapié en la defensa de los ciudadanos y las infraestructuras y en reducir la vulnerabilidad a los atentados. Incluye asegurar las fronteras externas, mejorar la seguridad del transporte, proteger objetivos estratégicos y disminuir la vulnerabilidad de las infraestructuras críticas. La persecución trata de entorpecer la capacidad terrorista de planear y organizar atentados y de llevar a los autores ante la justicia. La reacción incluye la preparación, gestión y minimización de las consecuencias de un atentado, la coordinación de las medidas de respuesta y la atención a las necesidades de las víctimas. Este pilar es el de dimensión más internacional y el que más requiere la solidaridad de toda la UE, con acuerdos de coordinación en caso de crisis, la revisión de los mecanismos de protección civil, la integración de las respuestas a las crisis y el intercambio de experiencias en materia de ayuda a las víctimas del terrorismo.

Entre los principales métodos para abordar el ciberterrorismo están las colaboraciones con entidades empresariales y líderes destacados del campo del ciberespacio, con el fin de crear de campos de entrenamiento para la formación ofensiva y defensiva de los militares encargados de la seguridad informática. Otros métodos se centran en la gobernanza mundial y en que los países, además de compartir más sus respectivas informaciones, refuercen sus intentos de crear un protocolo común de respuesta a los incidentes de ciberterrorismo, con elementos como la formación de una base de datos de imágenes extremistas conocidas para compartirlas con los proveedores de protocolos de Internet, con el fin de que, cuando aparecen esas imágenes en la Red, se eliminen automáticamente.

Otro problema es la popularización de la tecnología *blockchain* (cadena de bloques), un protocolo de intercambio entre iguales normalmente asociado a las transacciones informáticas de criptomonedas que se hacen en abierto, sin supervisión ni restricciones, con maniobrabilidad mundial y casi anónimas. Ese es el motivo de que el bitcoin y otras monedas virtuales e imposibles de rastrear se hayan vuelto métodos favoritos y anónimos de financiar el terrorismo y sus actividades. Las transacciones pueden hacerse en forma de intercambios, minado de criptomonedas y donaciones. La naturaleza de la cadena de bloques permite la estratificación de fondos, mediante compras y transferencias electrónicas, de las cuentas en divisas virtuales, con lo que se les otorga una capa de legitimidad y se enturbia aún más una pista ya difícil de seguir en primer lugar. La formación de empresas tapaderas para comprar criptomonedas en los mercados más regulados puede lograr que no se disparen los mecanismos de denuncia y hacer aún más confusa la combinación de ingresos legales e ilegales. Algunos de los grandes centros financieros han puesto en marcha leyes sobre los procedimientos apropiados en relación con la clientela de las criptomonedas y procedimientos de verificación de identidad y notificación obligatoria de las transacciones sospechosas, pero los países que lo han hecho son minoría.

Los Estados deben recuperar la iniciativa en la lucha contra el ciberterrorismo para conservar su ventaja sobre las organizaciones y los individuos que están combinando los atentados físicos con las posibilidades que ofrece Internet. En vez de esperar a que la amenaza se materialice y entonces reaccionar ante la fuerza física del ataque, deben intentar evitar las sorpresas para proteger a los ciudadanos y sus intereses. En la confrontación entre Estados y terroristas debe tener la iniciativa el Estado, que debe contar con un plan de acción decisivo y enérgico que prevenga posibles atentados y sirva como disuasorio. Unas normas más estrictas para las empresas que operan en el ciberespacio y una colaboración más estrecha con ellas contribuirían a identificar y neutralizar a los posibles terroristas, como también lo haría disponer de personal mejor formado y especializado en la seguridad y las amenazas informáticas. Si los Estados toman estas medidas, podrán cambiar las estrategias defensivas por otras ofensivas y, de esa forma, dejarán claro de lo que son capaces y garantizarán más paz para sus países en general.

Traducción de María Luisa Rodríguez Tapia

Fecha de creación
5 diciembre, 2018