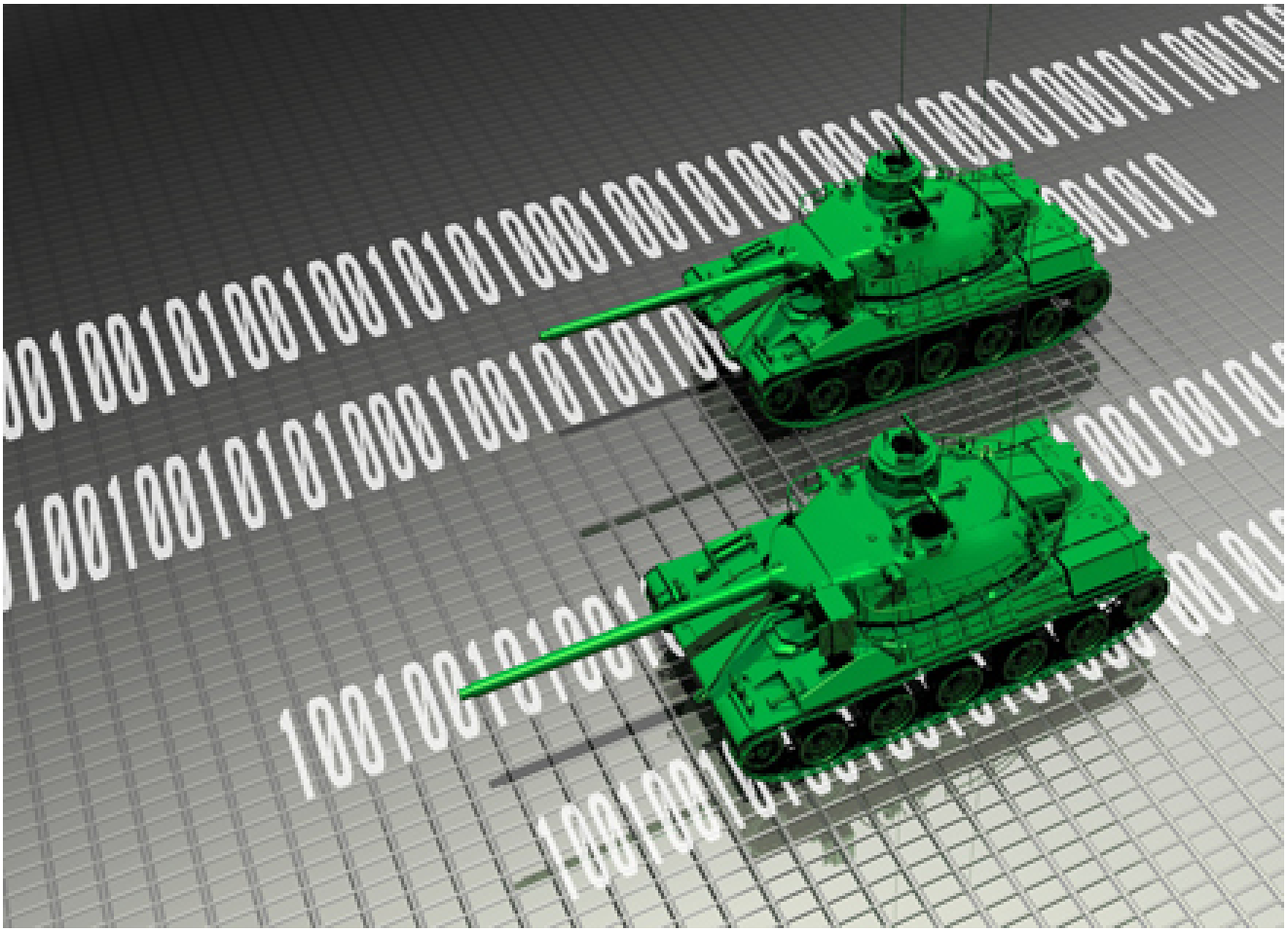
Seis ciberejércitos canallas

Iván Giménez Chueca

¿Cuáles son los Estados más agresivos en la Red?



El reciente caso del ciberataque de Corea del Norte contra Sony ha puesto sobre la mesa las capacidades ofensivas de los Estados para operar en la Red. La inversión para tener un ciberejército con alta capacidad es una opción más económica que desarrollar un arsenal convencional, y permite a regímenes como el de Pyongyang o Teherán medirse con las grandes potencias en este terreno.

La propia naturaleza de la ciberguerra donde es muy difícil demostrar la autoridad de un ataque propicia este tipo de acciones subversivas contra los potenciales enemigos. En ocasiones, estos Estados actúan a través de grupos de *hackers* que, junto a su dominio de la tecnología para dificultar el rastreo, hace que sea muy difícil atribuir una acción a un país.

En esta lista encontramos candidatos habituales en la calificación de Estados canallas como

Corea del Norte, Siria o Irán. Pero también grandes potencias como China o Rusia. Asimismo hay un actor que ha alimentado todo tipo de especulaciones como Estado Islámico (EI), cuyas posibilidades ofensivas en el ciberespacio son objeto de debate.

Corea del Norte, una fuerza en la Red en un país sin Internet

Las capacidades para la ciberguerra de Pyongyang saltaron a las portadas de la prensa internacional cuando Estados Unidos le acusó a finales de 2014 de estar detrás del ataque a Sony por la película *The Interview*. Pero no era la primera vez que los norcoreanos hacían un ataque de gran entidad en la Red.

Corea del Sur lleva años advirtiendo de las capacidades de su vecino. Según el Ministerio de Defensa, el régimen estalinista habría lanzado seis grandes ciberataques desde 2007. Uno de los más destacados fue en 2012 cuando causaron graves interferencias en las señales GPS de Corea del Sur que afectaron a 553 vuelos, aunque no hubo ningún accidente. Otra acción de la que se ha responsabilizado a Pyongyang fue de una serie de ataques contra entidades financieras surcoreanas y estadounidenses en 2009.

El Ministerio de Defensa de Corea del Sur ha cifrado al ciberejército norcoreano en 6.000 efectivos. Además destaca la Unidad 121, que sería la élite de las tropas de Kim Jong-un que actúan Internet, y que habrían estado detrás del ataque contra Sony. Esta agrupación dependería de la Oficina General de Reconocimiento, una agencia de espionaje que depende del Ejército.

El Ejército Electrónico Sirio, los 'cibermatones' de Al Assad

Paralelamente al inicio de la revuelta en Siria y cuando comenzaron a proliferar las noticias sobre atrocidades cometidas contra los manifestantes, apareció este grupo que aseguraba que quería contar la verdad de lo que estaba sucediendo en el país.

El Ejército Electrónico Sirio (conocido por sus siglas inglesas, SEA) atrajo la atención internacional cuando lanzaron ataques de denegación de servicio (DDoS, en sus siglas en inglés) contra algunos de los principales medios de comunicación del planeta como CNN, *New York Times, Time* o *Washington Post.* Su acción más destacada fue el *hackeo* de la cuenta de Twitter de Associated Press que anunció la falsa explosión de una bomba en la Casa Blanca que hirió al presidente Barack Obama, lo que provocó una caída del Dow Jones de un

1% en 90 segundos.

Entre sus otras acciones también están hostigar a las cuentas en redes sociales de los grupos opositores al régimen de Damasco. Tanto para evitar que difundan noticias incómodas de lo que sucede en la guerra civil, como para intentar identificar a posibles opositores. También atacan a empresas vinculadas a países que apoyan a la oposición, como sería el caso de Qatar.

Como suele pasar con estos ciberejércitos canallas, el Gobierno del país niega cualquier vinculación y asegura que son un grupo de *hackers.* Pero uno de los primeros dominios que utilizó el SEA (www.sea.sy) estaba registrado por la Syrian Computer Society, un organismo que depende del régimen de Bashar al Assad. Para Helmi Noman, investigador del Citizen Lab de la Universidad de Toronto (centro de referencia para el estudio del ciberactivismo), Siria se había convertido en el primer país árabe en tener un Ejército en la Red.

La Unidad 61398 del Ejército Popular de Liberación, los maestros que no existen

China está considerada junto a Rusia y Estados Unidos como una de las principales potencias del planeta en ciberguerra. En 2013, el Pentágono publicó un informe que acusaba a Pekín de estar detrás de una serie de ciberataques, que según la propia prensa estadounidense habrían comprometido seriamente informaciones clasificadas de las Fuerzas Armadas del país.

El Gobierno chino niega rotundamente estas acusaciones, y sólo reconoce que dispone de unas pocas decenas de expertos para defenderse, el llamado Ejército Azul, y que se desplegó oficialmente en 2011.

Pero los analistas coinciden que el Ejército Popular de Liberación cuenta con varios contingentes especializados en ciberguerra. La más célebre de ellas sería la Unidad 61398 con base en un edificio de doce plantas en Shanghai. Estos *hackers* habrían atacado docenas de compañías desde 2006, según apunta un informe de la compañía estadounidense Mandiant, especializada en seguridad informática.

Según el informe de Mandiant, estos ataques consistirían en la implantación de *malware* (*software* malicioso) o de ataques de *spear phising* para robar información sensible. Los principales objetivos fueron empresas estadounidenses de sectores estratégicos como la energía nuclear, renovables o la tecnología, y con nombres tan conocidos como IBM, Intel o Cisco.

Irán, la potencia en auge

Se puede decir que en la presente década uno de los actores internacionales que ha desarrollado más rápidamente sus capacidades para la ciberguerra ha sido Irán. En buena medida, fue consecuencia del ataque del virus Stuxnet contra los ordenadores de sus instalaciones nucleares (como Bushehr o Natanz), y que diversas fuentes responsabilizaron a Israel y Estados Unidos.

En un primer momento, parecía que la República islámica no podría desplegar una capacidad que no fuera más allá de perseguir a la disidencia interna en la Red. Pero tal y como apunta el gobierno de EE UU, Irán habría apoyado en 2012 una serie de ataques contra compañías y bancos estadounidenses en lo que sería una acción de respuesta por las sanciones impuestas a Teherán por su programa nuclear.

Esta información se habría obtenido a través de unas conversaciones interceptadas por la NSA. Según otras fuentes, Washington contemplaría a día de hoy a Teherán como un rival muy peligroso en el ciberespacio. Mientras que Rusia y China se ocuparían más en acciones de propaganda o en robar secretos, los iraníes se estarían dotando de una capacidad de ataque para dañar las infraestructuras del enemigo.

Otra vez encontramos la tónica de que las autoridades iraníes niegan cualquier responsabilidad. Algunos ataques los reivindica el grupo de *hackers* Ajax Security Team. La República Islámica reconoce que sus capacidades son defensivas, coordinadas por el Consejo Supremo del Ciberespacio y serían unidades encuadradas dentro de los Cuerpos de la Guardia Revolucionaria Islámica, y contarían con unos 2.400 efectivos.

Rusia, los pioneros en el ciberataque

Moscú fue un actor pionero en el mundo de la ciberguerra. En 2007 se le acusó de estar tras una serie de ataques contra entidades bancarias y gubernamentales de Estonia, tras una crisis diplomática por la retirada de una estatua que homenajeaba a los soldados soviéticos que lucharon en la Segunda Guerra Mundial.

El conflicto con Georgia en 2008 también tuvo su frente en la Red donde se realizaron ataques contra sistemas de comunicación gubernamentales, e incluso se llegó a sabotear un tramo del oleoducto Baku-Tblisi-Ceyhan.

Como no podía ser de otra manera, el Kremlin siempre ha negado estas acusaciones, y ha dicho que han sido obra de *hackers* rusos independientes con un sentimiento patriótico algo exaltado. Entre estos destaca el grupo Russian Business Network, en teoría una organización cibercriminal, pero a los que organismos como Open Democracy han vinculado con el Gobierno ruso; y no sólo para luchar contra enemigos exteriores, sino también para hostigar a la oposición como fue el caso de las elecciones de 2012.

Las acciones de los *hackers* rusos también se han hecho presentes en el conflicto con Ucrania. Comenzaron con ataques a sitios de noticias, en lo que parecía una campaña de propaganda, pero pronto se intensificaron, dejando fuera de combate a los ordenadores del Consejo de Defensa y Seguridad de Ucrania, o bloqueando las comunicaciones en Ucrania para facilitar el despliegue de los *hombres verdes*, tal y como señalaba esta publicación del Massachussets Institute of Technology (MIT).

Estado Islámico, ¿ciberamenaza real o exagerada?

Este grupo ha demostrado que sabe utilizar las redes sociales como herramienta de propaganda para atraer reclutas y difundir sus acciones. Esta comodidad para moverse por Internet ha hecho que muchos comiencen a especular si EI tiene capacidad para la ciberguerra, y en especial tras la irrupción del misterioso grupo autodenominado Ciber Califato.

David DeWalt, responsable de la empresa de seguridad informática FireEye, advirtió en Financial Times de que el grupo *yihadista* podría intentar adquirir *malware* en el mercado negro que se utilizaría para un ciberataque contra alguna estructura sensible, seguramente en Estados Unidos.

Pero también han surgido voces críticas con las capacidades de EI para la ciberguerra. Jim Lewis, investigador sobre ciberguerra del Center for Strategic and International Studies, cree que los islamistas no tienen entre sus filas a gente con los conocimientos informáticos adecuados para este tipo de operaciones.

De momento, no se ha probado que tengan una capacidad real de ataque, y las acciones que se les han atribuido han tenido un foco propagandístico. Un ejemplo sería los mencionados ciberataques del Ciber Califato contra las cuentas en redes sociales del Mando Central de las

Fuerzas Armadas de EE UU (responsable de las operaciones en Oriente Medio y Afganistán). Muchas voces alertaron contra la supuesta vulnerabilidad, pero otros pusieron de manifiesto que el daño fue muy limitado, y que los presuntos documentos confidenciales que se filtraron no tenían ningún valor.

Curiosamente, quien más preocupado se ha mostrado por hostigar a Daesh en el ciberespacio ha sido el grupo ciberactivista Anonymous, que ha lanzado la Operación ISIS para desenmascarar cuentas en redes sociales que apoyan a los *yihadistas.*

Fecha de creación
26 marzo, 2015