¿Hay una ciberguerra entre Irán y Arabia Saudí?

Iván Giménez Chueca

Teherán y Riad también podrían estar enfrentandose en el ciberespacio, como una muestra más de la lucha que libran por la hegemonía en Oriente Medio.

Siria, Yemen, Irak… la sombra de la rivalidad entre Arabia Saudí e Irán se percibe en los conflictos que vive Oriente Medio estos años. Teherán y Riad también habrían llevado esta hostilidad a la Red. Ambos países están desplegando sus capacidades de ciberguerra en acciones de inteligencia y de propaganda.

La empresa estadounidense Recorded Future, especializada en el análisis de amenazas de seguridad en Internet, publicó a finales de 2015 un informe que señalaba el enfrentamiento que habían llevado a cabo en el ciberespacio saudíes e iraníes. Concretamente se fijaba en los hechos que habían sido consecuencia de la intervención en la guerra de Yemen de la coalición liderada por Riad.

Como suele suceder cuando se analiza la conflictividad en el ciberespacio, es difícil encontrar pruebas concluyentes sobre la autoría de estas operaciones. Pero lo cierto es que la República Islámica ha desarrollado unas capacidades considerables desde que sus instalaciones

nucleares fueron víctimas del virus Stuxnet. Mientras que el reino saudí ha tenido un perfil más discreto, pero no hay que perder de vista que Riad es uno de los principales inversores de armamento en el mundo, y la defensa en la Red no iba a ser un frente sin cubrir.

Irán, ¿la mejor defensa es un buen ciberataque?

El *régimen de los ayatolás* comenzó a demostrar una voluntad por controlar lo que sucedía en el ciberespacio pensando en la disidencia interna. En 2005, creó los primeros organismos de control de Internet, bajo supervisión del Cuerpo de Guardianes de la Revolución Islámica. Cuatro años después, con las protestas de la Revolución Verde, el control de Intenet se extendió aún más, incluyendo las principales redes sociales (Facebook, Twitter, YouTube…) y medios de comunicación digitales de Occidente.

Pero estos mecanismos demostraron poca utilidad para hacer frente a amenazas exteriores de importancia. En 2010, la Operación Olympic Games, llevada a cabo por Estados Unidos e Israel, deshabilitó 1.000 centrifugadoras para el enriquecimiento de uranio en la central de Natanz a través del virus informático Stuxnet.

Irán pasó a la acción lanzando varias campañas de ciberataques contra grandes empresas estadounidenses, israelíes y europeas. Aunque mucho de estos ataques, son reivindicados por el Iranian Cyber Army, una organización de *hackers,* pero no se ha podido probar un vínculo claro con el gobierno de Teherán.

Enrique Fojón, subdirector de THIBER (El primer *think tank* español dedicado específicamente a la ciberprotección), ha señalado por qué Irán debe ser tomado en serio con este tipo de operaciones en Internet, “Al contrario de lo que ocurre con Corea del Norte, donde se exageran sus cibercapacidades propias, Teherán dispone de un arsenal cibernético que le permite ser considerado como una amenaza real”. Es decir, desde 2010 las capacidades de Teherán para lanzar una ofensiva en el ciberespacio podrían haber aumentado considerablemente.

Estados Unidos acusó a Irán de estar detrás de uno de los ciberataques más devastadores registrados hasta ahora, el que sufrió la petrolera Saudi Aramco, responsable de la producción del 10% del crudo mundial) en agosto de 2015. Un nuevo virus, identificado como Shamoon, ocasionó el borrado de datos en el 75% de los ordenadores de la empresa, y durante meses tuvieron que trabajar sin apenas apoyo informático en muchos departamentos. Washington también responsabilizó a Teherán del ataque que sufrió la gasística qatarí RasGas.

Arabia Saudí: potencia en ciberdefensa

Por su parte, los saudíes han mantenido una perfil bajo a la hora de exhibir sus cibercapacidades. “Arabia Saudí esta más centrado en cibercapacidades defensivas y de explotación que en ofensivas”, señala Fojón. Además, tal y como señala Recorded Future, este país y Estados Unidos son los objetivos predilectos de los *hackers* iraníes (trabajen o no para el gobierno de Teherán).

Pero mientras que Irán ha sido acusado de realizar ciberataques, ya sean directamente ordenados por el régimen o por obra de grupos de *hackers* nacionalistas, “a Arabia Saudí no se le ha responsabilizado de ningún ataque”, recuerda Vicente Díaz, analista de la compañía de seguridad informática Kaspersky.

Además, Díaz considera que “es posible que externalice estas capacidades de combatir en el ciberespacio; o tal vez confíe en aliados”. Es decir, siguiendo la tradición de Riad de contar con extranjeros (ya sean compañías o contingentes de países extranjeros subcontratados) para sus operaciones de defensa.

Sobre la discreción de los saudíes en el ciberespacio, Díaz recuerda que “atribuir una actuación de este tipo tiene una dificultad grande, pero que no hayamos visto ciberataques saudíes no quiere decir que no existan”.

Tal y como sucede en el terreno del armamento convencional, Arabia Saudí también realiza importantes inversiones en sus capacidades para la ciberdefensa. Según datos del SIPRI, la inversión en ciberseguridad de este país superó los 6.000 millones de dólares en 2013.

Dentro de esta vocación defensiva que resalta el subdirector de THIBER, tanto los sectores privado y público saudíes se han fijado en la defensa del sector energético, clave para la economía y el peso político del país. En el caso del ciberataque contra Aramco, la compañía pudo mantener al margen su red informática destinada a la extracción de crudo, hecho que evitó males mayores.

Yemen y la guerra de la desinformación

La escalada de tensión entre Teherán y Riad que ha supuesto la intervención saudí en Yemen también ha tenido su réplica en el ciberespacio. Desde el punto de vista del informe de Recorded Future, Irán estaría apostando por una estrategia de guerra híbrida.

El informe también habla de una intercambio de ataques sobre páginas web y cuentas de redes sociales protagonizados por *hackers* de ambos países, como por ejemplo, una acción de los saudíes contra la agencia de noticia Fars (próxima al régimen de Teherán) a final de marzo de 2015, o el pirateo de las cuentas de Twitter y YouTube de la televisión estatal iraní (pero que emite en árabe), Al Alam.

“Parece evidente que existe un ciberconflicto entre ambas naciones, caracterizado principalmente por operaciones de propaganda y desinformación y ataques de perfil bajo”, apunta Enrique Fojón.

Por su parte, Irán también habría respondido. Principalmente, a través de grupos aparentemente independientes pero que están vinculados al *régimen de los ayatolás.* Recorded Future señala al grupo Yemen Cyber Army (YCA) como responsable de los ataques a webs de medios saudíes como el diario *Al Hayat*. El periódico *Washington Post* señaló que la acción más importante de estos *hackers* fue el robo de información del Ministerio de Asuntos Exteriores de Arabia Saudí.

En junio de 2015, Wikileaks publicó una serie de documentos de la diplomacia saudí. La organización no quiso desvelar la procedencia de esta información, y tampoco sacaron a la luz datos sensibles, pero sí que mostraban a las autoridades de este país árabe verdaderamente obsesionadas con las actividades de la inteligencia iraní.

Arabia Saudí ha acusado al YCA de estar controlados por Teherán. Recorded Furute resalta que este grupo ha utilizado la expresión “We Are Cutting Sword of Justice” en sus mensajes reivindicando en su ataque contra el Ministerio de Asuntos Exteriores saudí. Esta misma frase se utilizó para reivindicar la acción contra Aramco, asegurando que era una manera de protestar contra las políticas del régimen de Riad.

Recorded Future también señala que el YCA no tiene presencia en las principales redes sociales como sí sucede con otros grupos de ciberactivistas (como por ejemplo, Anonymous), que las utilizan para dar eco a sus operaciones y recabar apoyos. Esta organización prefiere recurrir a la agencia Fars para publicitar sus acciones, lo que para esta firma de seguridad, es un indicio de la vinculación entre estos *hackers* e Irán, pero no puede aportar una prueba más firme.

Otros grupos de perfil parecido al YCA, como el Syrian Electronic Army (ciberactivistas sirios que han actuado contra la oposición al régimen de Bachar Al Assad pero que han negado cualquier vinculación con Damasco), ha sido acusado de actuar a las órdenes de Teherán, tal y como señalaba el diario *The New York Times*, citando fuentes de la inteligencia estadounidense. Pero nuevamente, no se ha podido encontrar un vínculo claro.

En cualquier caso, la ciberguerra y las acciones de *hackeo* son una opción interesante para ambos países. “En un escenario de rivalidad clara como el saudí-iraní no es descartable que el cibersabotaje remoto se utilice para evitar una escalada de violencia abierta”, explica Vicente Díaz, de Kaspersky. Aunque también apunta que hay riesgos de que una tercera nación utilice las hostilidades para enmascarar una operación propia o haya peligro de daño colateral.

Fecha de creación
20 mayo, 2016