Rusia, el Ciberespacio y las Elecciones estadounidenses

Manuel Gazapo
UNISCI
30 enero 2017

La sociedad internacional, durante los últimos meses, ha sido testigo de un tenso y polémico enfrentamiento entre los Estados Unidos de América (EEUU) y Rusia. La razón del conflicto se halla en que este último fue, según afirma el Gobierno Americano, el responsable de torpedear la campaña presidencial de Hillary Clinton mediante el uso de diversos y complejos ciberataques. Eso acabó produciendo que el cuadragésimo quinto presidente de los EEUU fuese Donald J. Trump, en lugar de la sexagésima séptima secretaria de Estado.

Estos acontecimientos ponen de relieve la importancia del ciberespacio en lo que a las cuestiones de geopolítica y geoestrategia se refiere. El ciberespacio, entendido como la quinta dimensión del conflicto tras la tierra, el mar, el aire y el espacio, cobra cada vez más protagonismo. Las referencias a los beneficios que nos aporta su uso suelen ser equivalentes a las críticas que recibe por los riesgos que su uso lleva implícito. El problema se haya en que esos riesgos se hacen progresivamente más numerosos, más dañinos y más sonoros. El último ejemplo de ello, lo encontramos en las citadas injerencias cibernéticas realizadas por Rusia en las elecciones presidenciales de EEUU.

Este tipo de actuaciones no son nuevas. En 2008 y 2012 las campañas de McCain, Romney y Obama también fueron objetivo de ataques virtuales. El uso de ciberataques por parte de Estados para presionar, chantajear o incluso dañar físicamente a otros gobiernos no es algo alejado de la realidad. Todo lo contrario, es algo mucho más corriente de lo que se suele pensar.

Vayamos punto por punto, caso por caso, para comprender el enorme poder e influencia que un Estado puede llegar a acumular y ejercer si maneja adecuadamente sus capacidades virtuales.

El primer caso con verdadera repercusión internacional fue el ataque cibernético que sufrió Estonia el año 2007. Ese año, Estonia fue objeto de ciberataques que iban desde ataques de denegación de servicios, ataques que provocaban la desconfiguración de sitios web, ataques a servidores hasta correos basura y hacktivismo. Todo ello provocó que numerosos sectores del gobierno, entidades bancarias, medios de comunicación y demás infraestructuras críticas quedaran bloqueadas parcial o totalmente. Estonia estuvo durante varias horas aislada del mundo. A pesar de que no hubo pruebas suficientes para demostrar la acusación, las autoridades del país declararon a Rusia como responsable del ataque, ya que la investigación forense realizada indicaba que el ciberataque masivo procedía de terminales rusos.

El segundo caso lo encontramos en el conflicto armado que enfrentó a Georgia y Rusia durante el año 2008. Tras desestabilizar Estonia y Lituania, Rusia tomó la decisión de dar un paso más y combinar las operaciones armadas con las operaciones cibernéticas. Durante dicho enfrentamiento, Georgia recibió ataques de denegación de servicios procedentes de Rusia, lo cual provocó que los principales sitios web del gobierno, de los bancos y de los principales medios de comunicación quedasen bloqueados.

A pesar de que las pruebas y el contexto apuntaban directamente a Rusia, en esta ocasión tampoco fue posible probar que esas operaciones cibernéticas extremadamente ofensivas fueran diseñadas, ordenadas o lanzadas por el gobierno ruso. Ahora bien, lo que si estaba claro es que

un actor estatal estaba detrás de los ciberataques ya que semejante sofisticación solo podía alcanzarse con la inversión y los recursos pertenecientes a un Estado.

El tercer ejemplo de ataques cibernéticos de un Estado contra otro Estado lo encontramos en Ucrania en el año 2015. El 23 de diciembre de ese año, según denunciaron las autoridades ucranianas, varias centrales eléctricas sufrieron un ciberataque que dejó sin electricidad a más de 103 ciudades y 230.000 personas. Concretamente, en la región de Ivano-Frankivsk se produjeron tres apagones simultáneos en tres centros de distribución de energía. Ucrania solicitó ayuda internacional para llevar a cabo una investigación forense que pudiera dilucidar quién era el responsable de los ciberataques, los cuales, prácticamente no tenían precedentes, en tanto, habían sido capaces de penetrar en las infraestructuras críticas de producción y distribución de energía eléctrica sin demasiada dificultad.

Tras finalizar las investigaciones, Ucrania atribuyó los ataques a Rusia y acusó a su gobierno de haber diseñado el malware "BlackEnergy". Sin embargo, las autoridades americanas, que participaron intensamente en las investigaciones forenses, advirtieron que no había evidencias suficientes para atribuir el ataque al gobierno ruso. Ahora bien, en lo que sí coincidían los americanos y los ucranianos era en que sus infraestructuras críticas eran ampliamente vulnerables a los ataques cibernéticos. Las investigaciones realizadas demostraron que las infraestructuras críticas ucranianas estaban mucho mejor protegidas que las americanas en lo que al ámbito digital se refiere, por lo que fue una importante señal de advertencia que debería de haber incitado a Estados Unidos a mejorar su ciberseguridad. A pesar de ello, como veremos más adelante, esas mejoras no se implementaron adecuadamente.

El cuarto ejemplo de una injerencia cibernética no autorizada de un país en el espacio virtual de otro Estado, es el propio objeto de estudio de este comentario: los ciberataques elaborados por el gobierno ruso para influir en los resultados de las elecciones presidenciales americanas de 2016.

INJERENCIA EN LAS ELECCIONES PRESIDENCIALES

Tras varias arremetidas, la alarma saltó definitivamente en junio de 2016. En ese momento, el FBI alertó a los ciudadanos y a las autoridades de que el sistema electoral de Illinois y Arizona se había visto comprometido por hackers rusos. A pesar de que en un principio el FBI no especificó si el gobierno ruso estaba detrás de estos ataques, la ansiedad se extendió rápidamente.

Ante semejante escenario, Tom Hicks, director de la Comisión de Asistencia Electoral, se mostró confiado y expuso que el sistema de voto electrónico de los Estados Unidos tenía suficientes cortafuegos como para garantizar que ninguno de sus datos se vieran manipulados. El vicepresidente Joe Biden respaldó las palabras de Hicks al afirmar que Estados Unidos estaba preparado para responder al intento ruso de condicionar las elecciones.

Desgraciadamente, la realidad demostró que Hicks y Biden estaban equivocados. James R. Clapper, Director de la Inteligencia Nacional Americana, acertó al advertir que la manipulación de datos y votos a través del ciberespacio era la nueva y principal amenaza que se cernía sobre los Estados Unidos. El Departamento de Seguridad Nacional (DHS) alertó de que el voto online practicado a gran escala podría ser alterado. Desde ese momento, las agencias de seguridad e inteligencia de los EEUU empezaron a apuntar con el dedo a Rusia debido a

que las metodologías de ataque y los patrones de actuación eran bastante similares a aquellas situaciones en las que los rusos parecían haber actuado previamente. En definitiva, las "huellas dactilares" de los ciberataques contra el sistema electoral y contra el Partido Demócrata coincidían en gran medida con las huellas encontradas en Estonia, Georgia o Ucrania.

ACUSACIÓN Y REACCIÓN

El 7 de octubre de 2016 Estados Unidos acusó oficialmente a Rusia de intentar interferir en el proceso electoral de noviembre de 2016. El ataque cibernético contra el Partido Demócrata y Hillary Clinton no sólo dañó sus posibilidades de alcanzar la presidencia, sino que también sacó a luz los trapos sucios del partido y mostró que la candidata y su presidente de campaña, John Podesta, no jugaron limpio durante las primarias.

Posteriormente, el 29 de diciembre de 2016, la Casa Blanca publicó un Joint Analysis Report (JAR) elaborado conjuntamente por el DHS y el FBI. El documento tiene una importancia fundamental para comprender cómo se llevó a cabo la injerencia rusa y poder prevenir futuros ataques. El JAR, titulado como "Grizzly Steppe", permitió a la comunidad de inteligencia americana atribuir la autoría de los ataques cibernéticos a la *Russian civilian and military Intelligence Service* (RIS). En el texto se apunta que la inteligencia rusa no sólo había atacado al Partido Demócrata, sino que también había atacado a otras infraestructuras críticas, empresas, think tanks, universidades y otros actores de la sociedad. El FBI y el DHS añaden que la inteligencia rusa intentó enmascarar los ataques para torpedear las investigaciones forenses destinadas a identificar la autoría de los ataques cibernéticos. Asimismo, en el JAR se puede encontrar un análisis detallado de los dos principales ataques cibernéticos de origen ruso: la amenaza de ataque persistente o APT 29 y el APT 28.

Como respuesta a estas injerencias, Barack Obama ordenó la expulsión de 35 diplomáticos rusos y el cierre inmediato de dos agencias de inteligencia rusas en suelo americano, entre otras acciones. Obama advirtió que iría contra todos aquellos que hubiesen tenido relación con las interferencias cibernéticas.

Paul Ryan, portavoz de la Cámara de representantes, y el senador republicano John McCain lamentaron y criticaron efusivamente que las represalias de Obama llegasen tan tarde y tuvieran tampoco recorrido. Denunciaron que, si el gobierno tenía evidencias claras de que los ciberataques fueron dirigidos desde las más altas instancias del gobierno ruso, las respuestas debían de haberse implementado mucho antes y con mucho mayor impacto.

DOBLE VARA DE MEDIR

Cuando EEUU no es víctima de un ataque cibernético no es posible determinar el origen de este. Tan solo hay que estudiar los casos ya retratados de Estonia, Georgia y Ucrania. Sin embargo, cuando ocurre al contrario, sí es posible identificar rápidamente al autor de los ciberataques. James R. Clapper señaló que atribuir ciberoperaciones es difícil, pero no imposible y que EEUU contaba con fuentes y pruebas de alta calidad que sustentaban la acusación. Y es en base a este comentario donde surge la siguiente cuestión: ¿acaso existe, por parte de EEUU, una doble vara de medir a la hora de atribuir la autoría de los ciberataques?

Desde la perspectiva de reputados expertos en seguridad cibernética como Graham Cluley, sí existe una doble vara de medir principalmente porque los ciberataques son ya la nueva forma

de plantear la geopolítica y la geoestrategia. No hace falta más que recordar que en el año 2013, Rusia anunció al mundo que el ciberespacio iba ser el escenario de conflicto al que iba a dedicar más atención y esfuerzo. El General Valery Gerasimov afirmó que Rusia, a partir de ese momento, buscaría gestionar sus intereses, sus relaciones internacionales y sus conflictos utilizando cada vez más las capacidades cibernéticas a su disposición.

Las intenciones de Rusia, a pesar de sus discursos oficiales, siempre han ido encaminadas a recuperar cotas de poder y crear un contexto internacional favorable a sus intereses personales. En consecuencia, no se entiende por qué las autoridades americanas han negado una y otra vez la participación de hackers rusos en altercados previos a las injerencias en sus elecciones, cuando existían evidencias claras.

Tal y como apuntan fuentes del Partido Demócrata, la Administración Obama ha eludido apoyar las acusaciones contra Rusia en los casos de Estonia, Georgia o Ucrania para evitar la creación de una guerra cibernética. Es fundamental comprender que lo ocurrido durante los últimos años está teniendo lugar en una de las épocas más tensas desde el final de la Guerra Fría. Los ataques cibernéticos contra Estados aliados, el ciberataque chino contra Sony o los enfrentamientos con Rusia en los conflictos de Siria y Ucrania, crean un contexto donde cualquier acción no calculada quirúrgicamente puede desatar consecuencias fatales.

Sin embargo, el que EEUU haya actuado estos años con una extrema prudencia o incluso relativizando la importancia de actos que podían afectar a la seguridad de sus aliados con el fin de mantener la calma, no ha impedido que Rusia haya jugado sus cartas de forma mucho más directa, agresiva y decidida. La forma de actuar de EEUU ha acabado siendo contraproducente para su seguridad nacional, en tanto que su archienemigo por excelencia ha tenido acceso a los servidores de ambos partidos y ha utilizado la información para “encaminar” el resultado de las elecciones y construir un panorama geopolítico mucho más beneficioso para sus intereses.

VULNERABILIDAD CIBERNÉTICA

Lo ocurrido revelaba que Estados Unidos es digitalmente vulnerable. La idea de que hackers rusos, con el apoyo o no del gobierno, pudieran socavar la confianza en el sistema de voto demuestra que Estados Unidos ya no sólo no es una potencia intocable en el plano físico, como demostró el 11-S, sino que tampoco lo es en el plano virtual.

El aumento la dependencia del ciberespacio por parte del gobierno y de grandes compañías americanas ha provocado que su vulnerabilidad y su fragilidad aumente considerablemente. Como advertíamos al principio de este comentario, las amenazas y riesgos en la dimensión digital avanzan y evolucionan a una velocidad mucho mayor que los mecanismos de defensa. Estados Unidos es ahora consciente de que los virus informáticos ya no se utilizan únicamente de manera táctica, sino también de forma estratégica, es decir, que se diseñan e implementan de manera orquestada e inteligente con el fin de provocar el mayor daño posible.

CONCLUSIONES

Los ciberataques al Partido Demócrata y al Partido Republicano durante las elecciones de 2016 marcan un punto de inflexión a nivel internacional en temas de seguridad: los conflictos del mundo físico de los que habíamos sido testigos hasta nuestros días, tienen su continuación en el mundo virtual del ciberespacio. De estos hechos, se extrae la primera conclusión: en el siglo

XXI, la competencia de un Estado ya no es sólo su territorio, su espacio aéreo y marítimo, sino también su infraestructura electrónica o ciberespacio.

Cada vez más actores pasan a operar en el ciberespacio y sus cibercapacidades se disparan. Mientras que Rusia está a la cabeza, Estados Unidos se desmorona al no haber implementado las reformas y las respuestas cibernéticas esperadas. Quizás, la Administración Obama no hizo nada porque no deseaba revelar sus capacidades ocultas o, por el contrario, porque carecía de ellas. En cualquier caso, lo que queda claro es que en este nuevo campo de batalla dominan aquellos que se mueven con más rapidez, con más sigilo y con menos escrúpulos. Moscú celebra hoy la victoria de Trump.

La segunda conclusión es el hecho irrefutable de que EEUU es vulnerable virtualmente. La guerra en el ciberespacio ha sido uno de los principales elementos que han quitado el sueño a Obama durante sus ocho años mandato. Por lo tanto, es probable que también se lo quite a Trump a pesar de su acercamiento a Putin.

La tercera conclusión es que Rusia es el hegemon en cuanto a capacidades cibernéticas se refiere. Por un lado, disuadió al gobierno ucraniano de nacionalizar las compañías privadas de energía -propiedad de un oligarca ruso cercano a Putin- mediante un brutal ataque cibernético sobre sus infraestructuras críticas. Por otro lado, crispado con la administración demócrata, consiguió influir lo suficiente en las elecciones americanas como para servir de apoyo en el descrédito de Hillary Clinton y allanar el camino de Donald J. Trump hacia la presidencia.

Estos acontecimientos demuestran que Rusia no solo tiene *hard power* y *soft power*, sino también la fusión de ambos, el *cyberpower*, lo cual, representa un riesgo para el actual equilibrio de poder global: Si Rusia ha sido capaz de interferir en las elecciones presidenciales americanas, nada impedirá que vuelva hacerlo en las próximas elecciones que han de acontecer en 2017 en Alemania, Francia y Holanda.

La geopolítica y geoestrategia actuales cada vez dependen más de un uso ágil del ciberespacio. El problema es que éste es una inmensa llanura siberiana donde prácticamente todos estamos al descubierto y sumidos en la niebla. Es ahí, donde se juegan las nuevas partidas del poder global. Ante semejante situación, no cabe más que reaccionar de forma urgente y prepararse para un futuro incierto mediante la mejora de los sistemas de alerta temprana, el perfeccionamiento de los cortafuegos, la creación de ciberejércitos, la expansión de una cultura de ciberseguridad, el aumento de la resiliencia en las infraestructuras críticas y la sincronización de los servicios de inteligencia. Solo así, podremos garantizar un mínimo de seguridad frente al oso ruso y otros depredadores que existen en esta nueva dimensión del conflicto que es el ciberespacio.