Valentín Katasonov

La quinta esfera de la guerra

Los ciberataques estadounidenses contra Rusia pueden expandirse dramáticamente este otoño.

Estados Unidos ha estado librando una guerra cibernética contra Rusia durante al menos diez años. Como dice Richard A. Clarke, asesor de seguridad de la administración presidencial de los Estados Unidos durante el gobierno de Bush Jr., en *Cyber ??War* (HarperCollins, 2010): «la guerra cibernética son las acciones de un Estado nacional para infiltrarse en las computadoras o redes de otro estado nacional con el fin de lograr el objetivo de causar daños o destrucción».

Hace diez años, la revista británica *The Economist* llamó al ciberespacio «la quinta esfera de la guerra, después de la tierra, el mar, el aire y el espacio exterior» **[1]**. Se puede suponer que una guerra cibernética a gran escala contra Rusia comenzó en 2009, cuando se creó el Comando Cibernético de Estados Unidos (USCYBERCOM). Desde el principio, Rusia se encontró en la corta lista de los países objetivo para las operaciones planificadas por el Comando Cibernético de EE.UU.

La guerra cibernética tiene dos áreas principales: 1) la inteligencia cibernética (ciberespionaje); 2) los ciberataques.

El ciberespionaje contra Rusia se llevó a cabo incluso antes de la creación del Comando Cibernético de EE.UU. a través de la NSA, la CIA, la inteligencia militar y otros servicios especiales. Todo esto fue bien descrito por Edward Snowden. Pero los ciberataques comenzaron a llevarse a cabo desde principios de esta década; su frecuencia y escala aumentan cada año. Las principales áreas de operaciones activas en el marco de la ciberguerra son: 1) destrucción y daño a la información electrónica del enemigo; 2) propaganda: colocar materiales de propaganda en el espacio de información del enemigo; 3) bloqueo de servicios (interrupción del funcionamiento de sitios o sistemas informáticos); 4) interferencia en el funcionamiento de los equipos, su apagado o avería (ataques a las computadoras que sirven al funcionamiento de dichos equipos).

Pueden ocurrir daños a gran escala como resultado de ataques a computadoras que sustentan la vida de las ciudades, su infraestructura (sistemas de comunicación, sistemas de suministro de agua, redes eléctricas, brigadas de bomberos, transporte urbano, etc.). Existe la posibilidad de bloquear el trabajo de grandes empresas industriales, instituciones bancarias, empresas de transporte, centrales eléctricas, etc. Finalmente, el objeto de los ciberataques pueden ser sistemas de gobierno, fuerzas armadas, sistemas de armas complejas. En 2010, dejaron claro al mundo que Estados Unidos podía bloquear el funcionamiento de instalaciones estratégicamente importantes con la ayuda de «armas digitales». Luego, los servicios de inteligencia estadounidenses, junto con los servicios de inteligencia israelíes, lograron infligir graves daños a las centrifugadoras de una instalación nuclear iraní Natanz utilizando el virus informático Stuxnet.

Durante mucho tiempo, Washington ocultó cuidadosamente el hecho de la guerra cibernética contra Rusia. Las actividades del Comando Cibernético de los Estados Unidos y las organizaciones bajo su mando que realizan operaciones de guerra cibernética se clasificaron de

manera confiable. Al mismo tiempo, incluso durante la época del presidente Barack Obama, Washington acusó a Moscú de librar una guerra cibernética contra Estados Unidos. Cualquier ataque de piratas informáticos que se llevara a cabo en Estados Unidos contra agencias gubernamentales, bancos, instalaciones de infraestructura, etc., Washington casi siempre las calificaba como «intrigas de Moscú». Dicen que los ataques los llevan a cabo personas detrás de las cuales se encuentra el Kremlin y que trabajan bajo las órdenes del Kremlin.

Bajo el presidente Obama, se recurrió a operaciones cibernéticas activas contra Rusia y otros países, pero con cautela. La inteligencia cibernética prevaleció. Los ciberataques seguían siendo raros, temían el «efecto bumerang». Por ejemplo, bajo Obama, funcionarios del Departamento del Tesoro de Estados Unidos propusieron abstenerse de ataques cibernéticos contra bancos extranjeros, creyendo que tales acciones podrían socavar el sistema financiero global.

Las acusaciones de que Moscú está librando una guerra cibernética contra Estados Unidos han aumentado drásticamente desde la llegada de Donald Trump a la Casa Blanca. Moscú fue acusada de interferir en las elecciones presidenciales de 2016 con la ayuda de «tecnologías digitales». Dicen que hubo una influencia activa de Moscú en el contenido de Internet y las redes sociales a favor de Trump y en contra de los demócratas.

El Comité de Inteligencia del Senado de EE.UU. publicó este año la quinta parte de un informe de investigación secreto sobre la «injerencia rusa en las elecciones de 2016» (informe del 6 de enero de 2017). Aquí hay un extracto de ese evento: «El gobierno ruso, en una actitud agresiva y multidimensional, influyó o trató de influir en el resultado de las elecciones, y el presidente ruso Vladimir Putin dirigió personalmente los esfuerzos para piratear redes informáticas y cuentas asociadas con el Partido Demócrata de Estados Unidos». ¡Personalmente!

Han pasado cuatro años desde esa campaña electoral, pero no se ha presentado ninguna evidencia concreta de la interferencia cibernética de Moscú en el proceso electoral estadounidense. En marzo de 2020, un tribunal estadounidense cerró el caso contra la empresa rusa Concord Management and Consulting, de la que se sospechaba que «interfería» en las elecciones estadounidenses. También hubo otros intentos de procedimientos legales contra personas físicas y jurídicas rusas, pero todos terminaron en un fiasco. Además, se han registrado casos de falso testimonio contra esas personas por parte de algunos ciudadanos estadounidenses. El fiscal especial Robert Mueller, que investigaba la supuesta colusión entre Rusia y el equipo de Trump, se vio obligado a dimitir.

Pero no hay duda de que Washington está librando una guerra cibernética contra Rusia. El reconocimiento de este hecho vino de labios del presidente de los Estados Unidos. Donald Trump, durante una entrevista con el columnista del Washington Post, Mark Thyssen, en la Oficina Oval en julio de 2020, admitió que en 2018 autorizó un ciberataque encubierto contra la Agencia de Investigación de Internet de Rusia, con sede en San Petersburgo **[2]**. Algunos medios de comunicación estadounidenses lo llamaron una «fábrica de trolls».

¡Y cuántas operaciones de este tipo contra Rusia hubo! Nos enteramos de que algunas de ellas son obra de los servicios de inteligencia estadounidenses de exfuncionarios del gobierno estadounidense. The New York Times (NYT) publicó un artículo en junio de 2019 sobre un aumento en el número de ataques cibernéticos estadounidenses a las redes eléctricas rusas. En estos artículos, los expertos se refirieron a fuentes no identificadas entre ex funcionarios del

gobierno que brindaron esta información relevante durante la entrevista **[3]**. Se señaló que las redes eléctricas rusas durante la primavera de 2019 fueron objeto de ataques cibernéticos masivos por parte de Estados Unidos. El propósito de los ataques era inyectar códigos maliciosos en el sistema cibernético que pudieran paralizar el funcionamiento de las redes eléctricas. La información filtrada sobre esta operación especial ha enfurecido a Trump.

En septiembre de 2018, John Bolton, entonces asesor de seguridad nacional de Donald Trump, anunció que el presidente había ampliado las capacidades de las agencias de inteligencia y el ejército para realizar operaciones ofensivas en el ciberespacio. Los detalles aparecieron dos años después. Yahoo News ha publicado revelaciones de exfuncionarios de la administración Trump sobre un decreto presidencial de Estados Unidos de hace dos años. El decreto de 2018 fue clasificado **[4]**; le dio a la CIA mayores poderes y herramientas para llevar a cabo ciberataques. Este decreto liberó a la CIA de la necesidad de justificar la elección del objetivo del ataque (estructuras empresariales, medios de comunicación, ONG) mediante una conexión con un Estado «hostil». Uno de los exfuncionarios de la administración presidencial de Estados Unidos dijo bajo condición de anonimato: «Anteriormente, era necesario durante años recolectar evidencias (en decenas de páginas) de que esta organización en particular está directamente relacionada con las autoridades referidas. Ahora, si se puede demostrar de manera aproximada que ella está actuando en interés del gobierno referido, se le puede dar luz verde».

Además, un decreto secreto de 2018 otorgó a la CIA autoridad adicional para realizar operaciones activas destinadas a desactivar las instalaciones económicas y de infraestructura. Finalmente, la CIA recibió carta blanca para un uso más amplio de una herramienta de guerra cibernética como la publicación de pruebas comprometedoras sobre personas y entidades legales que están en la lista negra de Washington. Lo que, por supuesto, requiere una ciberinteligencia más activa en relación con esas personas.

Según Yahoo News, la CIA, a la que se le han otorgado poderes adicionales, ha realizado más de una docena de operaciones activas durante los últimos dos años. Se menciona un ciberataque contra tres bancos iraníes presuntamente vinculados al Cuerpo de la Guardia Revolucionaria Islámica. Esto terminó con el hecho de que los datos personales de millones de depositantes de estas instituciones de crédito llegaron a Internet. También se mencionó a la empresa rusa SyTech, cuyo servidor fue pirateado en julio de 2019. Los atacantes obtuvieron acceso a 7,5 TB de información. Los documentos de la empresa se publicaron en la red, de lo que se desprende que era un contratista del FSB y otros servicios especiales rusos. Los piratas informáticos estadounidenses de la CIA enviaron información sobre veinte proyectos no públicos de SyTech a los principales medios de comunicación. Los piratas informáticos de Tsereushnye compartieron la información obtenida con el grupo Digital Revolution, que un año antes pirateó el servidor del Instituto de Investigación «Kvant», que estaba bajo el control del FSB.

En octubre de 2019, el secretario del Consejo de Seguridad de la Federación de Rusia, Nikolai Patrushev, informó que se habían llevado a cabo varios millones de ciberataques en la red de organismos estatales en varios distritos federales de Rusia. Casi todos fueron rechazados con éxito. Añadió que los servicios de inteligencia estadounidenses y extranjeros están buscando «puntos débiles» en la infraestructura de información de Rusia para la posterior realización de ciberataques a gran escala. Por lo tanto, la tarea de mantener y fortalecer la seguridad de la información y digital de Rusia es cada vez más urgente.

A fines del año pasado, los medios estadounidenses informaron que la CIA y otros servicios especiales, bajo el liderazgo general del Comando Cibernético de Estados Unidos, estaban desarrollando tácticas para las elecciones presidenciales en Estados Unidos en 2020 (se llevarán a cabo el 3 de noviembre). En particular, están considerando un escenario en el que Moscú interfiere en estas elecciones, y en el que luego Washington responderá con una serie de ciberrespuestas a Moscú. Si, en vísperas de las elecciones, los servicios especiales sienten el «aliento» de Moscú, comenzarán a filtrar información clasificada sobre ciudadanos rusos sospechosos de interferencia en el espacio de la información (la dirección del FSB, el Ministerio de Defensa, otros departamentos y, posiblemente, algunos oligarcas; con la excepción del Presidente de la Federación de Rusia).

Los expertos señalan que en 2016 el Consejo de Seguridad Nacional de EE.UU. desarrolló tácticas para una guerra de información con Rusia durante la campaña presidencial y las propias elecciones, pero las reacciones cibernéticas de Washington fueron extremadamente lentas. Esta vez, la CIA y otras agencias de inteligencia estadounidenses prometen que las respuestas a Moscú serán muy duras. Como señala el Washington Post el 18 de diciembre del año pasado, las medidas desarrolladas por el Comando Cibernético de Estados Unidos para las actuales elecciones son tan distintas a las propuestas en 2016 «como lo son el día y la noche».

No hay duda de que, cualquiera que sea el resultado de las elecciones estadounidenses, Moscú será acusado de «interferencia» y es probable que siga una serie de ciberataques graves contra Rusia. Entonces tenemos que prepararnos.

PD: Ya se han realizado las primeras acciones en el marco de las tácticas desarrolladas por el Ciber-Comando de Estados Unidos. En agosto de 2020 el Departamento de Estado de EE.UU. comenzó a enviar mensajes SMS a los rusos sobre una recompensa de $10 millones por datos sobre interferencia en las elecciones estadounidenses. Las presentaciones son parte del programa Rewards for Justice. El 5 de agosto de 2020, el secretario de Estado de Estados Unidos, Mike Pompeo, anunció el inicio de este programa **[5]**.

Notas:

[1] https://www.economist.com/leaders/2010/07/01/cyberwar?story_id=16481504&source=features_box1

[2] https://www.washingtonpost.com/people/marc-a-thiessen/

[3] https://www.bbc.com/news/technology-48675203

[4] https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html

[5] https://www.buzzfeednews.com/article/christopherm51/state-department-reward-russia-election-interference-spam

Traducido del ruso por Juan Gabriel Caro Rivera

?

[Fuente: Fondsk.ru]

?