Artyom Ignatiev

En noviembre, el Ministerio de Defensa de Ucrania clasificó por completo la información sobre la formación de sus tropas cibernéticas. Quizás una de las razones de este secreto radica en el hecho de que, **según** los involucrados, *"las tropas cibernéticas son a veces más terribles que las armas nucleares, porque pueden usar estas armas nucleares pirateando recursos de información"* .

En muchos países existen unidades especiales de ciberseguridad. El número de piratas informáticos en la administración pública está creciendo rápidamente. Según la empresa rusa *Z ecurion*
, los cinco estados principales con el mayor gasto en tropas de TI son
Estados Unidos, China, Reino Unido, Corea del Sur
y
Rusia
. Sin embargo, no solo estos países crean y desarrollan sus ejércitos cibernéticos y combaten unidades de TI. Ésta es una tendencia mundial.

A principios de marzo de 2020, seis países de la Unión Europea crearon tropas cibernéticas para actuar contra Rusia. Lituania, Estonia, Croacia, Polonia, los Países Bajos y Rumanía han firmado el memorando por el que se establece **la Fuerza Cibernética de Reacción Rápida de la UE** . Según el ministro de Defensa de Lituania, Raimundas Karoblis, este acuerdo aseguró un mecanismo permanente para *"la presencia de un país en el ciberespacio soberano de otro país"*
. Los poderes cibernéticos de la UE pueden operar tanto en los países de la UE que firmaron el acuerdo como en los países observadores; este estatus se otorgó a Francia, Bélgica, Grecia, España, Italia, Eslovenia y Finlandia. Las potencias clave de la OTAN en el Viejo Mundo, Alemania y Gran Bretaña, todavía están tratando de mantener un perfil bajo y, al mismo tiempo, están mejorando activamente sus tropas cibernéticas nacionales.

Alemania se acerca muy a fondo a la creación de un ejército cibernético. "Junto con las fuerzas aéreas, navales y terrestres, la Bundeswehr está adquiriendo ahora un cuarto tipo de tropas": así lo expresó el corresponsal francés de ***Le Figaro*** en Berlín, quien señaló en 2017 el hecho del establecimiento oficial de la primera Formación cibernética del ejército alemán. El núcleo de la unidad son 260 expertos militares en TI.
"Los ciberataques requieren pocos recursos humanos, pero mucha competencia"
, dijo la secretaria de Estado del Ministerio de Defensa de Alemania, Katrin Zuder.
Representantes del Servicio Federal de Inteligencia de Alemania (BND)
explicaron
con franqueza alemana: "Rusia está bajo sospecha".

Al salir de la UE, Gran Bretaña se inclinó en el ámbito militar hacia el componente de TI. Según el general de división Tony Raper de la *Agencia de Servicios de Comunicaciones de Defensa (DCSA)* del Departamento de Defensa del Reino Unido, *"las fuerzas armadas con tecnología de la información representan una nueva categoría de tropas con tácticas especiales de guerra. Acciones, estructura organizativa y de personal, el nivel de entrenamiento de personal y armas que satisfagan plenamente los requisitos de la guerra moderna"*
.

Hace pocos años, **Japón** ha anunciado su intención de crear "fuerzas de seguridad cibernética", como parte de las fuerzas armadas y de manera significativa ampliar el alcance de los servicios que los sistemas informáticos proteger de la piratería. El Consejo de Seguridad de la Información es responsable de la implementación de esta decisión. El pretexto para el surgimiento del tipo más nuevo de tropas en el país realmente ocupado por los estadounidenses después de 1945 fue elegido como puramente económico. Digamos que Japón y sus empresas se han convertido en repetidas ocasiones en víctimas de ataques masivos de piratas informáticos desconocidos. El hecho de que los piratas informáticos tomaran el control, por ejemplo, de las redes de información de la corporación de ingeniería pesada *Mitsubishi Heavy Industries* comprometido en el lanzamiento de tecnología militar y espacial, aunque no particularmente sobresaliente.

China ha estado construyendo su ejército cibernético durante una década, cuando el Ejército de Liberación Popular de la República Popular de China formó un grupo de treinta especialistas, llamado "Equipo Azul Cibernético", estacionado en la región militar de Guangdong en el sur del país. Los profesionales chinos de *TI* se centran inicialmente en "no tomar en cantidad, sino en calidad". Qué tan efectivo puede ser juzgado por el informe del Consejo Científico del Departamento de Defensa de los Estados Unidos, según

el cual, en la primavera de 2013, alrededor de 40 programas de armas del Pentágono y alrededor de 30 otras tecnologías de defensa estaban en manos de expertos cibernéticos, algunos de ellos, según los medios occidentales, están directamente relacionados con el gobierno y los departamentos militares de la República Popular China. Estados Unidos está convencido de que China es el enemigo más peligroso y hace planes para derrotar a Estados Unidos.

Estados Unidos, según el Ministerio de Defensa de la República Popular China, ya ha gastado miles de millones de dólares en la creación de más de cuarenta "equipos de agentes virtuales" que, bajo el pretexto de luchar contra los piratas informáticos, están activos en todo el mundo. También luchan contra la libertad de expresión. Uno de los muchos ejemplos es una unidad especial *"para el uso de la fuerza para neutralizar los medios de comunicación extranjeros al interrumpir el funcionamiento de su infraestructura técnica",* cuya creación fue anunciada al mundo por la empresa de televisión estadounidense NBC. William M. Arkin, columnista de *The Washington Post* y autor de varios libros sobre temas militares, afirma que esta unidad especial " *tiene la tarea de utilizar e interrumpir las comunicaciones y los sistemas informáticos de los medios de comunicación de todo el mundo* ". También señala que la estructura principal del Comando Estratégico para neutralizar los medios de comunicación extranjeros es la sede de los ataques a la red de apoyo *(Network Attack Support Staff)* en la base de "Fort Meade", Maryland, el mismo lugar donde se ubica la NSA, responsable del espionaje electrónico y control del espacio virtual.

Irán anunció la creación de tropas cibernéticas especializadas a principios de 2012. Se ha creado en el país una sede especial para contrarrestar las ciberamenazas. La tarea consiste en prevenir la piratería de redes de objetos estratégicos y el robo de datos sensibles. De vez en cuando, en las fuentes de noticias de las agencias mundiales, hay informes de que Teherán está utilizando el cuartel general clandestino de las fuerzas de seguridad de Hezbollah en el sur de Beirut (Líbano) como base para sus ciber centros militares. De acuerdo a los expertos del *Instituto Washington para la Política del Cercano Oriente* , Irán está listo para llevar a cabo operaciones cibernéticas para bloquear los sistemas de control de instalaciones militares críticos, la infraestructura y la logística de los Estados Unidos.

Israel también está desarrollando y mejorando activamente sus tropas cibernéticas. Los medios extranjeros no descartan que Israel, que ha creado poderosas unidades anti-piratas informáticos con la ayuda de piratas informáticos locales, esté librando no solo guerras defensivas sino también ofensivas en el ciberespacio virtual. Los israelíes, en particular, son

sospechosos de crear virus informáticos que atacaron las instalaciones nucleares iraníes hace varios años. Los servicios de inteligencia israelíes y el *departamento de sistemas informáticos y comunicaciones del* Estado Mayor de las Fuerzas Armadas de Israel son responsables de la planificación y ejecución de operaciones cibernéticas destinadas a distorsionar los componentes de la infraestructura de información y telecomunicaciones en otros países.

Turquía y sus ciberespecialistas, desde el comienzo de la guerra en Siria, han estado realizando operaciones militares contra Rusia en el espacio virtual. Un ejemplo ilustrativo: piratería informática a principios de 2016 por parte de hackers turcos, jefe de *Instagram* del Ministerio de Comunicaciones de la Federación de Rusia, Nikolai Nikiforov. Como resultado del hackeo, las banderas de Turquía, una foto de Ataturk, así como las fotos de un bombardero ruso Su-24 cayendo, derribado por la *Fuerza Aérea* Turca el 24 de noviembre de 2015, en la frontera turco-siria, fueron publicado en la página del Ministro de Comunicaciones de Rusia. Según *RBC*, la cuenta del Ministro de Comunicaciones de la Federación de Rusia fue pirateada por el grupo de piratas informáticos turco *Börteçine Siber Tim*, que casi simultáneamente pirateó el sitio web de la Embajada de Rusia en Israel.

India comenzó a construir sus fuerzas cibernéticas mediante la creación de una unidad dedicada a las escuchas telefónicas e Internet después de un insolente ataque terrorista sin precedentes en Mumbai en noviembre de 2008 que mató a 166 personas. Se formó una Agencia Nacional de Investigación para centralizar la lucha contra el terrorismo en todo el país. En las cuatro ciudades más grandes de la India - Mumbai, Chennai, Kolkata e Hyderabad - se abrieron las bases de la unidad de élite de la Guardia de Seguridad Nacional, comenzó la creación de estructuras de *TI* enfocadas en la confrontación en el espacio virtual.

Se están produciendo cambios importantes en los asuntos militares. Las principales potencias, desde Alemania hasta la India, por el mismo hecho de la formación de ciberejércitos declaran el desarrollo de nuevas estrategias y un cambio en los métodos de guerra. Y estamos hablando no solo de la informatización del equipo militar y el equipamiento de los militares, sino también de cambiar los fundamentos y tareas de las operaciones militares. El objetivo de la guerra ya no es la derrota final del enemigo, la toma de su territorio y recursos, sino su control cibernético.