Este artículo es copia fiel del publicado en la revista Nueva Sociedad Nº 269,
mayo-junio de 2017, ISSN: 0251-3552, <www.nuso.org>.

# Cómo Rusia reclutó y formó a «batallones» de *hackers*

En los últimos años, la defensa del ciberespacio se ha convertido en una de las principales preocupaciones del Kremlin. En 2013, el Ejército ruso lanzó una operación destinada a reclutar a especialistas en seguridad de la información, tal como lo revelaron el diario digital *Meduza* y *The New York Times*.

**Agathe Duparc**

Fue en plena celebración de la Navidad rusa cuando los servicios secretos de Estados Unidos decidieron lanzar sus acusaciones contra Vladímir Putin. El presidente ruso asistía en ese momento a misa, en el monasterio de San Jorge (Yuriev), cerca de Nóvgorod, y, hasta la fecha, no ha considerado necesario pronunciarse al respecto personalmente. Sí lo hizo Dmitri Peskov, su portavoz, quien calificó de «sandez» el informe estadounidense. «Cada día, decenas de miles de *hackers* atacan la web de Putin. Y la mayoría de los ataques se producen desde EEUU, pero cada vez que eso sucede no acusamos a la Casa Blanca o a Langley», replicó.

Si bien todavía no se han dado a conocer las «pruebas» técnicas de la implicación de los dirigentes rusos en el ataque a los servidores del Partido Demócrata, nadie duda de que, en estos últimos años, el control del ciberespacio ha pasado a ser una de las prioridades de Rusia, uno de los elementos estratégicos del país a la hora de reafirmar su poder. Frente al mastodonte norteamericano y a su Agencia Nacional de Seguridad (NSA, por sus siglas en inglés) capaz de vigilar al planeta entero, los responsables rusos se han lanzado sin disimulo a reclutar especialistas en ciberseguridad.

---

**Agathe Duparc:** es periodista y fue corresponsal en Moscú de varios medios. Es coautora de *Des mots pour comprendre la Russie* (con Alexandre Adler y Nathalie Amargier, Plume, París, 1994).
**Palabras claves:** *hackers*, internet, servicios secretos, Vladímir Putin, Rusia.
**Nota:** la versión original de este artículo se publicó en *Mediapart*, 10/1/2017. Agradecemos la autorización para reproducirla. Traducción de Mariola Moreno.

En julio de 2013, Serguéi Shoigú, ministro de Defensa desde noviembre de 2012, fue el encargado de dar la señal de largada. En presencia de los rectores de las universidades técnicas rusas, anunció que se abría «la caza de programadores» –«en el buen sentido de la palabra», precisó–, para dar con ello respuesta en los años posteriores a las necesidades del Ejército en materia de nuevos softwares. El ministro lanzó también la idea de crear «batallones científicos» integrados por los mejores estudiantes que, sin dejar la universidad, se pondrían al servicio del Ejército con el fin de, por ejemplo, ayudar a enfrentar ciberataques –cada vez más comparables con las armas de destrucción masiva, dijo– y a velar por la «seguridad de la información de las infraestructuras del Estado».

En la primavera boreal de 2014, la agencia de noticias ITAR-TASS, citando a una fuente anónima, anunciaba la creación, en el seno de las Fuerzas Armadas, de la división encargada de las «operaciones vinculadas a la información», capaces por ejemplo «de atacar las redes de un enemigo potencial», a partir del modelo del Cyber Command (Uscybercom), existente en EEUU desde 2010[1].

Una investigación publicada el pasado mes de noviembre en el diario digital *Meduza* revelaba que se había reclutado de forma precipitada a programadores, especialistas en encriptado, matemáticos e ingenieros[2]. A finales de diciembre, *The New York Times* completaba esa información en un artículo titulado: «Cómo Rusia ha reclutado a la elite de los *hackers* para llevar a cabo su guerra cibernética»[3].

En todo el país, las unidades militares se dotaban así de las famosas «brigadas científicas». Se ha contratado a los estudiantes más brillantes, en colaboración con las universidades, como en Novosibirsk, de donde se han enviado jóvenes al Instituto de Investigación Científica de Sérguiev Posad (cerca de Moscú), dependiente del Ministerio de Defensa. El objetivo era desarrollar nuevas tecnologías aplicadas a «superordenadores». En septiembre de 2015, se abrió una escuela de cadetes especializada en internet y en nuevas tecnologías y tres meses después se diplomaban en la Academia Militar de Comunicaciones los primeros «*spetsnazy*[4] en seguridad de la información».

---

1. «В России созданы кибервойска» en *Besti.ru*, 12/5/2014.
2. «Российские вооруженные киберсилы Как государство создает военные отряды хакеров. Репортаж Даниила Туровского» en *Meduza*, 7/11/2016.
3. Andrew E. Kramer: «How Russia Recruited Elite Hackers for Its Cyberwar» en *The New York Times*, 29/12/2016.
4. Nombre utilizado para las fuerzas especiales.

También se difundieron en las redes sociales videos ultrapatrióticos, de inspiración soviética. Uno de ellos fue publicado en Vkontakte (el Facebook ruso) en verano de 2015 por el Centro de las Fuerzas Armadas Radioeléctricas (REB, por sus siglas en ruso) en Tambov. En él se ve a un soldado con un fusil Kalashnikov que poco a poco va dando paso a las manos anónimas de un *hacker* que teclea: «Si acabas de terminar con éxito la universidad, si eres especialista en ciencias técnicas, si quieres aplicar tu saber, te damos la posibilidad», se puede leer en la pantalla. A los candidatos –aquellos en edad de hacer el servicio militar– se les ofrecen mejores condiciones de vida y la posibilidad de trabajar en «sistemas informáticos muy potentes» (lo que no se corresponde con las fotos presentadas en el video).

Una parte del grafismo utilizado –las manos de los *hackers*– también aparece en otro video, en este caso anónimo y mucho más agresivo, sobre el «ocupante ruso» expulsado de diferentes países (naciones bálticas, Ucrania, Asia central, etc.) después de haber hecho el bien y ahora dispuesto a luchar contra la «democracia en estado de descomposición» y «los valores occidentales»[5]. «Cortésmente les advierto por última vez: ¡no se metan conmigo! Construyo la paz, amo la paz, pero lucho mejor que cualquier otra persona en este mundo», anuncia en ruso una voz viril.

Según *Meduza*, algunos cibercriminales –ex-*hackers* rusos independientes que hace diez años eran considerados los mejores del mundo– habrían sido invitados a trabajar por la patria a cambio de ver reducidas sus condenas. Para apoyar esta tesis, *The New York Times* cita al general Oleg Ostapenko, viceministro de Defensa, quien en 2013 declaraba en *Rossiyskaya Gazeta* que «*hackers* con un pasado criminal» podían ser de utilidad y que la cuestión era objeto de debate.

Dmitri Alperovitch, confundador de la compañía estadounidense CrowdStrike, la empresa de seguridad informática que redactó el primer informe sobre la posible participación del grupo de *hackers* rusos Fancy Bear en el ataque a los servidores del Partido Demócrata, afirma que «se ha detenido a piratas informáticos rusos, pero nunca han terminado en la cárcel». En su investigación, *Meduza* detalla también que el Instituto de Estudios Científicos Kvant, especializado en sistemas de protección de la información, y vinculado desde 2007 al Servicio Federal de Seguridad (FSB, por sus siglas en ruso), el

5. «Я Русский Оккупант | I'm a Russian Occupant» en YouTube, 27/2/2015, <www.youtube.com/watch?v=T65SwzHAbes> (con subtítulos en español).

antiguo KGB, ha adquirido en el extranjero material informático. Según documentos publicados por WikiLeaks, en la primavera de 2011 Georgey Babakin, entonces director del Kvant, fue contactado por la empresa italiana Hacking Team y su director Marco Bettini, quienes querían vender un software espía denominado «Remote Control System» (un troyano al servicio de los gobiernos entonces de venta libre), que permite infiltrarse en computadoras y *smartphones*[6]. En varios e-mails hechos públicos por WikiLeaks, el italiano dice haber viajado a Moscú en septiembre de 2012 para presentar el producto por el que los rusos habían mostrado interés. Asegura que se entrevistó con miembros del FSB. Entre 2012 y 2014, la sociedad Infotechs, que representaba al instituto Kvant, pagó 451.000 euros a Hacking Team por la compra del Remote Control System.

*Meduza* y *The New York Times* también se hacen eco de la historia de Alexandre Vyarya, especialista ruso en seguridad informática, quien tuvo que exiliarse en Finlandia. Empleado por la empresa moscovita Qrator Labs, que trabajaba para varios medios de la oposición, y también para el sitio del bloguero Alekséi Navalny, Vyarya asegura haber sido contactado por Rostec –holding ruso creado en 2007 para «alentar al desarrollo, la fabricación y la exportación de la producción de fabricación de alta tecnología» de uso civil y militar–, que le propuso colaborar. Y que rechazó. Tras sentirse amenazado, finalmente huyó en agosto de 2015 a Helsinki, donde pidió asilo político.

Meses antes, Vyarya había sido testigo en Bulgaria de un extraño encuentro. En un viaje a Sofía, adonde había sido invitado por uno de los responsables de Rostec, participó en una reunión durante la cual una empresa local presentó un nuevo software capaz de lanzar potentes ataques de denegación de servicio (DDOS, por sus siglas en inglés) contra páginas de internet (a las que se puede tumbar y quedan neutralizadas mediante un tráfico artificial). Para demostrarlo, se atacó la web del Ministerio de Defensa ucraniano y la del periódico digital ruso *Slon.ru*, que ese día se vio paralizado durante unos minutos, como confirmó su director a *The New York Times*. Según Vyarya, el responsable de Rostec le propuso después trabajar para él y le preguntó si era posible mejorar el *software* malicioso que esperaba comprar por un millón de dólares.

6. Pueden encontrarse los documentos en <https://wikileaks.org/hackingteam/emails/?q=Russia+Bettini&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult>.