Documento
Opinión

31/2023 23 de marzo de 2023

Francisco Marín Gutiérrez *

Hacktivismo al servicio del Estado: ciberproxies en Ucrania

Hacktivismo al servicio del Estado: ciberproxies en Ucrania

Resumen:

Las implicaciones internacionales que tiene realizar determinadas acciones hostiles determinan que algunos Estados utilicen personas u organizaciones que ejecuten por delegación las acciones deseadas sin que estos puedan ser considerados directamente responsables. El uso de estos intermediarios, doctrinalmente definidos como *adversarios por delegación*, aunque resulte más conocido el término *proxy*, es habitual en el mundo real y aún más en el ciberespacio.

Se pretende exponer aquí como los Estados, en los enfrentamientos desarrollados en el ámbito del ciberespacio, usan ciberproxies en apoyo de sus fines, en particular, a los denominados grupos hacktivistas.

En definitiva, la utilización de proxies encuentra en el ciberespacio un nuevo y valioso campo de actuación y con este trabajo se quiere prestar especial atención a cómo organizaciones del colectivo hacktivista son empleadas a modo de *adversarios por delegación* para efectuar acciones ofensivas en el ámbito cibernético en beneficio de un Estado, centrándonos en el actual conflicto Rusia-Ucrania, por ser el mejor ejemplo de dicha tendencia.

Palabras clave: Hacktivismo, ciberguerra, guerra por delegación, proxies, Rusia, Ucrania.

Hacktivism at the service of the State: cyber proxies in Ukraine

Abstract:

The international implications of executing certain hostile actions mean that some States use individuals or organisations to carry out the desired actions by delegation without being held directly responsible. The use of such intermediaries, doctrinally defined as surrogates (although the term proxy is better known), is a common practice in the real world and even more in cyberspace.

The purpose of this work is to show how States confronted in cyberspace, use cyber-proxies to support their aims, in particular hacktivist - a term derived from the words "hacker" and "activist" - groups.

To sum up, the use of proxies has found a new and valuable field of action in cyberspace, and this paper aims to pay special attention to how hacktivist organisations are used as adversaries by proxy to carry out offensive actions in the cybernetic domain for the benefit of a State, focusing on the current Russia-Ukraine conflict as the best example of this trend.

Keywords:

Hacktivism, cyberwar, proxy war, proxies, Russia, Ukraine.

Cómo citar este documento:

MARÍN GUTIÉRREZ, Francisco. *Hacktivismo al servicio del Estado: ciberproxies en Ucrania*. Documento de Opinión IEEE 31/2023. https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO31_2023_FRAMAR_Ucrania.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción

Durante los últimos años se ha consolidado la tendencia según la cual los Estados llevan a cabo operaciones encubiertas en el ámbito ciberespacial —que abarcan desde el espionaje a las acciones de sabotaje— mediante la utilización de elementos interpuestos o sustitutos (*proxies*). En este sentido, los Estados nación han utilizado cada vez más a los grupos patrióticos o activistas que actúan y se manifiestan en el ciberespacio, y que configuran lo que se conoce como *hacktivismo*. El término fue acuñado en 1994 por Cult of the Dead Cow[1] —grupo de hackers formado en 1984 en Lubbock, Texas—, a partir de las palabras *hacker* y *activismo*, y se define como la realización de ciberataques para promover los objetivos del activismo político o social.

En los últimos doce meses, la guerra entre Rusia y Ucrania ha reconfigurado el panorama de las ciberamenazas, confirmando las tendencias que comenzaron a manifestarse en 2014 durante las primeras fases del conflicto. Entre los cambios más relevantes están la ejecución por parte de uno de los bandos, Rusia, de operaciones ofensivas en el ciberespacio en estrecha coordinación con acciones militares convencionales y, por otro, el significativo incremento de la actividad hacktivista, apoyando ambas partes del conflicto. En este sentido, y para hacernos una idea del nivel de actividad, diremos que se estima en 201 el número de este tipo de grupos activos durante 2022; 117 de los cuales habían apoyado al bando ucraniano, 74 al ruso y 10 estaban sin definir[2]. La guerra en Ucrania se ha convertido así en el mejor y más actual ejemplo de la utilización del hacktivismo por parte de dos Estados en conflicto.

Algunos conceptos: *guerra de sustitutos* y *proxies* en el ciberespacio

Desde hace tiempo es objeto de debate la denominada *guerra de sustitutos* (*surrogate warfare)*, entendida como aquellos casos en los que un Estado utiliza a agentes no identificables con sus fuerzas armadas tradicionales para llevar a cabo acciones bélicas defendiendo sus intereses nacionales en un conflicto. Según estudiosos del tema, en un esfuerzo por minimizar la exposición de las tropas propias a los riesgos operativos de la guerra y limitar así los riesgos para los responsables políticos, los Estados comparten y

[1] The Cult of the Dead Cow. Disponible en: https://cultdeadcow.com/about.html [consulta: 28/2/2023].
[2] @CyberKnow. Publicación en Twitter de 19 de diciembre de 2022. Disponible en: https://twitter.com/Cyberknow20/status/1604805201885417472?cxt=HHwWgMCigYP1tMUsAAAA [consulta: 28/2/2023].

delegan cada vez más estos riesgos con apoderados, auxiliares y plataformas tecnológicas[3]. Por otro lado, el empleo de estos actores también puede incrementar la capacidad de actuar unilateralmente cuando sea necesario, preservando el capital político y los recursos nacionales[4].

A lo largo de la historia, los *sustitutos* —también denominados *proxies*— han sido elementos de muy distinta naturaleza, desde auxiliares mercenarios a grupos insurgentes, pasando por organizaciones terroristas y empresas comerciales. Más recientemente, los Estados también han externalizado la carga que supone la guerra a plataformas tecnológicas como la aviación no tripulada, la robótica o las armas cibernéticas, siendo estas últimas exclusivas de las operaciones en el ámbito ciberespacial que, recordemos, se compone de tres capas: física, lógica y humana.

Existe cierta controversia respecto a las diferencias entre los términos anglosajones *surrogate* (*sustituto*) y *proxy* (*apoderado*), no existiendo un acuerdo en relación con las capacidades o autonomía otorgadas a cada uno. Una excelente definición de la *guerra de proxies* la caracteriza como el patrocinio directo o indirecto de terceras fuerzas convencionales o irregulares ajenas al orden constitucional de los Estados involucrados en un conflicto armado[5]. Pero para la finalidad de este trabajo basta con afirmar que en el ámbito de los conflictos bélicos el concepto de *proxy warfare* puede considerarse una variante de la *guerra de sustitutos*, en la que la tecnología se ha convertido por derecho propio en ese importante *apoderado* o *sustituto*.

La doctrina de las Fuerzas Armadas españolas también contempla el concepto de *adversarios por delegación* o *proxies*, definidos como «los actores no estatales o Estados débiles empleados de forma encubierta por un tercer Estado adversario con la finalidad de alcanzar sus propios objetivos. De esta forma, el tercer Estado y su proxi forman en cierta manera un solo conjunto»[6].

---

[3] KRIEG, Andreas y RICKLI, Jean-Marc. *Surrogate Warfare. The Transformation of War in the Twenty-First Century*. Georgetown University Press, Washington D. C., 2019.

[4] SMITH, Kelly H. *Surrogate Warfare for the 21st Century*. Monografía Army Command and General Staff Coll. Fort Leavenworth Ks School of Advanced Military Studies, 25 de mayo de 2008. Disponible en: https://apps.dtic.mil/sti/citations/ADA451060 [consulta: 28/2/2023].

[5] RONDEAUX, Candace y STERMAN, David. *Twenty-First Century Proxy Warfare. Confronting Strategic Innovation in a Multipolar World Since the 2011 NATO Intervention*. New America, Washington, febrero 2019. Disponible en: https://d1y8sb8igg2f8e.cloudfront.net/documents/Twenty-First_Century_Proxy_Warfare_Final.pdf [consulta: 28/2/2023].

[6] *PDC-01(A) Glosario de Terminología de uso Conjunto*. Estado Mayor de la Defensa, Ministerio de Defensa, Madrid, julio de 2021. Disponible en: PDC-00_Glosario_de_Terminologia_de_uso_Conjunto_xJUL21x.pdf (defensa.gob.es) [consulta: 28/2/2023].

Y ya para centrar este trabajo, un *ciberproxy* puede definirse como un intermediario que lleva a cabo o contribuye directamente a una acción ofensiva en el ciberespacio que es permitida a sabiendas, bien activa o pasivamente, por un beneficiario[7].

Ciberproxies en un conflicto

La menor capacidad cibernética interna y el deseo de ahorrar costes puede explicar el porqué los Estados optan por utilizar *proxies* en el ámbito digital. Entre estos últimos se incluyen distintas entidades, que van desde grupos de ciberpatriotas a organizaciones asociadas con actividades criminales en el ciberespacio o a los PSOA (Private Sector Offensive Actors, es decir, actores ofensivos del sector privado), empresas privadas que fabrican, venden e incluso operan ciberarmas en paquetes de *hacking - como - servicio* a agencias gubernamentales de todo el mundo.

La utilización de *ciberproxies* obedece también a otras importantes razones: se elude la aplicación del derecho internacional tradicional; resulta más flexible que el empleo de funcionarios civiles o militares; impide la asociación de las actividades ejecutadas con el Gobierno que las motiva, dificultando su atribución, y posibilita participar en un conflicto en circunstancias en las que el apetito público por las operaciones militares tradicionales ha disminuido. En este sentido Michael S. Rogers —exdirector de la NSA y del US Cyber Command— afirmaba al hablar de *ciberproxies* en Rusia que «el Gobierno ruso está tratando de generar mayor capacidad y que tales grupos resultan atractivos porque les ofrecen una medida de negación plausible»[8].

Las relaciones entre un Estado y dichos grupos son diversas y existen estudios que abordan las diferentes posibilidades. La siguiente clasificación recoge los distintos grados de responsabilidad, de menor a mayor intervención estatal[9]:

[7] MAURER, Tim. *Cyber Mercenaries: the state, hackers, and power*. Cambridge University Press, Cambridge, 2018.
[8] MCMILLAN, Robert y VOLZ, Dustin. «Google Sees Russia Coordinating with Hackers in Cyberattacks Tied to Ukraine War», *The Wall Street Journal*. 26 de septiembre de 2022. Disponible en: https://www.wsj.com/articles/google-sees-russia-coordinating-with-hackers-in-cyberattacks-tied-to-ukraine-war-11663930801 [consulta: 28/2/2023].
[9] HEALEY, Jason y GRINBERG, Olivia. «Patriotic Hacking' Is No Exception», *Lawfare*. 27 de septiembre de 2022, 'Patriotic Hacking' Is No Exception - Lawfare (lawfareblog.com) [consulta: 28/2/2023].

Espectro de la responsabilidad del Estado	
Prohibido por el Estado	El gobierno nacional ayudará a detener un ataque de terceros.
Prohibición estatal pero inadecuada	El gobierno nacional coopera, pero es incapaz de detener el ataque de terceros.
Ignorado por el Estado	El Gobierno nacional conoce los ataques de terceros, pero no está dispuesto a tomar ninguna medida oficial.
Fomentado por el Estado	Terceros controlan y dirigen el ataque, pero el gobierno nacional los fomenta como una cuestión política.
Conformado por el Estado	Terceros controlan y dirigen el ataque, y el Estado proporciona cierto apoyo.
Coordinado por el Estado	El gobierno nacional coordina el ataque de terceros, por ejemplo, *sugiriendo* detalles operativos.
Ordenado por el Estado	El gobierno nacional ordena a terceros que lleven a cabo el ataque en su nombre.
Dirigido pero no reconocido por el Estado	Elementos fuera de control de las fuerzas cibernéticas del gobierno nacional llevan a cabo el ataque ordenado.
Ejecutado por el Estado	El gobierno nacional lleva a cabo el ataque utilizando fuerzas cibernéticas bajo su control directo.
Integrado en el Estado	El gobierno nacional ataca utilizando proxies integrados y fuerzas cibernéticas gubernamentales.

Tabla 1. Espectro de la responsabilidad del Estado en relación con los proxies.

'Patriotic Hacking' Is No Exception – *Lawfare* (lawfareblog.com)

En relación con este amplio espectro, naciones occidentales como los Estados Unidos mantienen a sus proxies —normalmente contratistas— relativamente cerca, lo que permite una estrecha dirección y supervisión de sus actividades en términos de selección

de objetivos y técnicas utilizadas[10]. Otros, como Siria, parecen haber puesto más distancia con sus apoderados, proporcionando tan solo apoyo material e ideológico a cambio de su cooperación para atacar a adversarios políticos específicos.

En cuanto a Rusia, como veremos a continuación, el apoyo se caracteriza fundamentalmente porque el Estado elude voluntariamente ver las actividades posiblemente delictivas del proxy a cambio de que este alcance los objetivos que se le marcan.

Por último, China ha utilizado una combinación de estos enfoques, pues ha ido centralizando sus operaciones cibernéticas ofensivas, aplicando un programa sistemático de incorporación de hackers privados a sus agencias de inteligencia, a la vez que desplazaba las responsabilidades de las operaciones cibernéticas del Ejército Popular de Liberación a unidades especializadas del Ministerio de Seguridad del Estado.

Posibilidades de empleo de hacktivistas como ciberproxies

Los grupos hacktivistas son empleados normalmente para llevar a cabo acciones ofensivas limitadas, en especial ataques tipo DDoS (denegación de servicio distribuido, que bloquean la página objetivo o su infraestructura con una avalancha de tráfico) contra páginas web institucionales o de empresas del adversario, o bien desfigurando esas mismas páginas inyectando contendidos propios o publicando información sensible previamente robada. También pueden utilizarse como vector de difusión de desinformación y así, al iniciarse el conflicto en Ucrania, algunos grupos prorrusos centraron su apoyo en la difusión de información tergiversada sobre el conflicto, caso del grupo *Zatoichi*, cuya cuenta de Twitter no tardó en suspenderse[11].

Posteriormente, campañas, como las llevadas a cabo en diciembre de 2022 por grupos prorrusos como *NoName057(16)* contra páginas de ministerios de Defensa occidentales[12] o como las de *KillMilk, KillNet* o *Anonymous Sudan* a finales de enero de 2023 contra instalaciones sanitarias europeas y norteamericanas, evidencian cómo dichos grupos se emplean para propagar información triunfalista, muy distante de la

[10] AKOTO, William. «Hackers for hire: proxy warfare in the cyber realm», *Modern War Institute at West Point*. 31 de enero de 2022**.** Disponible en: https://mwi.usma.edu/hackers-for-hire-proxy-warfare-in-the-cyber-realm/ [consulta: 9/2/2023].
[11] *#Zatoichi*. Disponible en: https://twitter.com/ZATOICHIJR/status/1498671579798065157 [consulta: 28/2/2023].
[12] *NoName057(16),* publicación en Telegram del 9 de diciembre de 2022. Disponible en: https://t.me/s/noname05716eng [consulta: 28/2/2023].

realidad, según la cual las listas de objetivos que proponen son atacados y supuestamente puestos fuera de servicio en cuestión de horas[13], sin que las defensas cibernéticas occidentales sean capaces de detenerlos. En este sentido, también se utilizan para lanzar mensajes que intentan sembrar sensación de impotencia entre las audiencias de las naciones cuyas instalaciones son atacadas, generando falta de confianza en sus propias autoridades, sin importar que sus ataques a páginas web tengan muy limitado impacto operativo. Ejemplo de esto último es la siguiente publicación de *KillMilk* en febrero de 2023 tras un ataque a instalaciones hospitalarias:

> «Da las gracias porque hoy no hemos tocado la red corporativa de los médicos y hoy no ha muerto nadie en las clínicas. Pero mañana mi mente puede cambiar rápidamente y te mataré con un ciberataque»[14].

Respecto a esta parte del espectro de actividades, empresas de ciberseguridad reiteran que grupos de habla rusa autodenominados *hacktivistas*, como *Killnet* y *Xaknet*, están participando activamente en operaciones de información contra organizaciones y entidades occidentales, facilitadas por medios de comunicación rusos posiblemente patrocinados por el Estado, con el objetivo probable de instigar el miedo o disminuir el apoyo a Ucrania[15].

A la pregunta de si continuará esta tendencia a corto plazo la respuesta es que sí, y para algunos autores no solo continuará, sino que se acelerará porque las tecnologías emergentes convergen y se refuerzan mutuamente[16]. Sin embargo, esta supuesta panacea para que el Estado pueda participar en los conflictos posmodernos no está exenta de consecuencias negativas. La mayoría de ellas están relacionadas con la pérdida de control, dando lugar a que los sustitutos rindan menos de lo esperado, sin alcanzar los resultados previstos, prolongando los conflictos o abusando del apoyo del patrocinador para conseguir agendas alternativas interesadas[17].

---

[13] *KILLMILK*, publicación en Telegram del 28 de enero de 2023. Disponible en: https://t.me/s/killmilk_rus/492 [consulta: 28/2/2023].
[14] *KILLMILK*, publicación en Telegram del 30 de enero de 2023. Disponible en: https://t.me/s/killmilk_rus/492 [consulta: 28/2/2023].
[15] INSIKT GROUP. «Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine», *Recorded Future*. 31 de enero de 2023. Disponible en: https://go.recordedfuture.com/hubfs/reports/cta-2023-0131.pdf [consulta: 28/2/2023].
[16] RICKLI, Jean-Marc. «Surrogate warfare and the transformation of war in the 2020s», *Observer Research Foundation*, entrada blog del 30 diciembre 2020. Disponible en: https://www.orfonline.org/expert-speak/surrogate-warfare-transformation-war-2020s/ [consulta 28/2/2023].
[17] KRIEG, Andreas y RICKLI, Jean-Marc. «Surrogate warfare: the art of war in the 21st century?», *Defence Studies*, Volume 18, issue 2. Routledge, Londres, 2018.

Por otro lado, aparecen problemas respecto al estatus legal de los *proxies*. El pasado 17 de febrero, durante la Munich Cyber Security Conference 2023, un asesor tecnológico del Comité Internacional de la Cruz Roja (ICRC) afirmó que «los civiles que acudan al ciberespacio para participar en las hostilidades entre Rusia y Ucrania podrían verse expuestos legalmente a acciones militares como respuesta»[18]. Añadió que fomentar la participación de civiles en actividades cibernéticas durante los conflictos armados podría socavar la protección de los civiles, que deben estar a salvo de los efectos de los conflictos armados, y que, por ello, «el ICRC recomienda encarecidamente a los Estados que inviertan la tendencia a la civilización del campo de batalla digital».

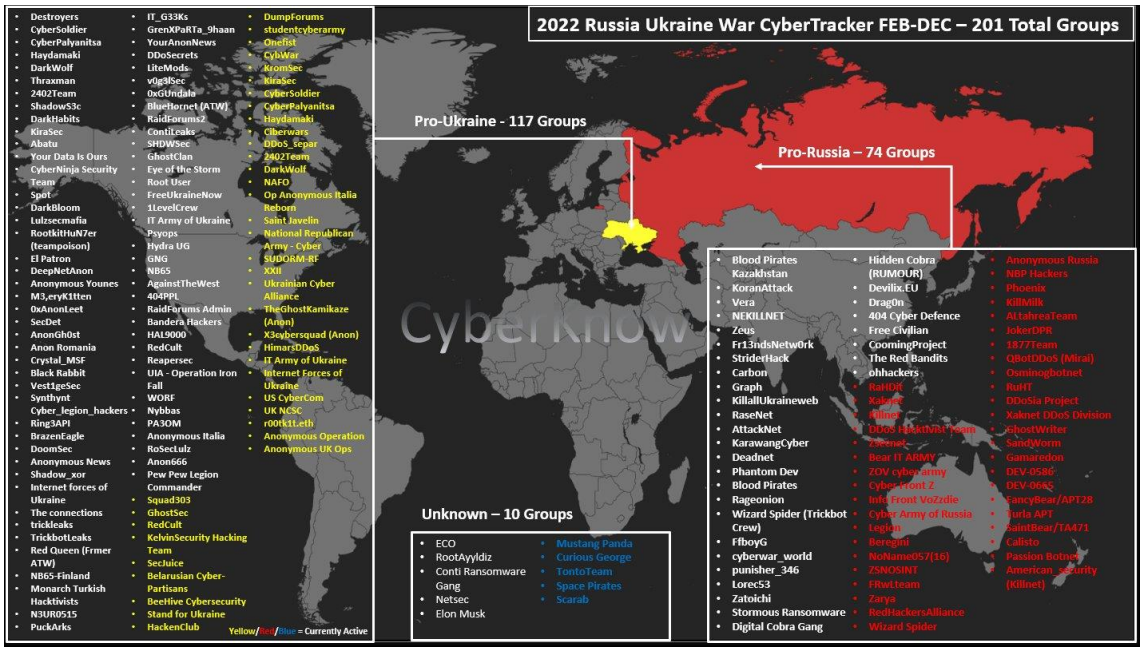

Imagen 1. Listado de grupos hacktivistas activos durante el conflicto en Ucrania en 2022. https://twitter.com/Cyberknow20/status/1604805201885417472?cxt=HHwWgMCigYP1tMUsAAAA

El caso especial de los hackers patrióticos

Los grupos hacktivistas suelen constituirse de acuerdo con principios ideológicos —destacando el patriotismo y el nacionalismo— y como reacción ante acontecimientos clave que les sirven de catalizador. Uno de los primeros antecedentes fueron los disturbios antichinos en Indonesia en 1998, que desencadenaron el primer gran ataque

[18] MARTI, Alexander. «Civilian hackers could become military targets, Red Cross warns», *Recorded Future News*. 17 de febrero de 2023. Disponible en: https://therecord.media/civilian-hackers-could-become-military-targets-red-cross-warns/ [consulta: 1/3/2023].

de grupos de hackers patrióticos de China como *Green Army*, *China Eagle Union* o *Hongke*. Estos utilizaron chats de Internet para coordinar campañas de envíos masivos de correo electrónico, ataques tipo DDoS y acciones de desfiguración contra páginas web indonesias. Los mismos grupos llevaron a cabo, en 2001, acciones similares contra la página web de la Casa Blanca e industrias norteamericanas tras el choque entre un avión de reconocimiento electrónico *EP-3* de esta nacionalidad y un caza chino sobre la isla de Hainan[19].

La táctica fue posteriormente imitada por otros Estados, como Siria o Rusia. Recordemos a la organización *Nashi* (que se podría traducir como *Movimiento Juvenil Democrático Antifascista «Los nuestros»*), grupo juvenil fundado por el Gobierno ruso para defender valores tradicionales del comunismo y de Rusia, y cuyos componentes contribuyeron a la realización de ciberataques contra entidades gubernamentales de Estonia en 2007 y de Georgia en 2008[20]. Así lo reconoció Konstantin Goloskokov —uno de los *comisarios* de *Nashi*, además de ayudante de un parlamentario pro-Kremlin— en una entrevista al *Financial Times*[21]. Goloskokov afirmó haber creado una red de simpatizantes que bombardearon con peticiones de acceso varias páginas web de Estonia hasta bloquearlas, y en una entrevista telefónica manifestó que «lo que yo hice y lo que hicieron mis amigos no fue ningún tipo de ataque, fue un acto de desobediencia civil, absolutamente legal»[22]. Muchos de aquellos ataques contra Estonia fueron operaciones coordinadas de mucha mayor complejidad y dirigidas contra centros gubernamentales, bancos, nodos de telecomunicaciones y proveedores de servicios de Internet, todo para influir psicológicamente en la población, produciendo una sensación de miedo, así como de incapacidad y desconfianza en sus propias autoridades.

Al año siguiente, 2008, durante el breve conflicto entre Rusia y Georgia, se realizaron múltiples ataques informáticos contra las infraestructuras críticas georgianas, en esta ocasión con cierta coordinación con acciones militares convencionales. El análisis de la campaña demostró que las *botnets* —redes de equipos infectados por un atacante

[19] HANG, Ryan. «Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism», *The Yale Review of International Studies*. Octubre de 2014. Disponible en: Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism – The Yale Review of International Studies (yira.org) [consulta: 28/2/2023].
[20] CARR, Jeffrey. «Rival hackers fighting proxy war over Crimea», *CNN*. 25 de marzo de 2014. Disponible en: https://edition.cnn.com/2014/03/25/opinion/crimea-cyber-war/ [consulta: 28/2/2023].
[21] CLOVER, Charles. «Kremlin-backed Group behind Estonia Cyber Blitz», *Financial Times*. 12 de marzo de 2009. Disponible en: https://www.ft.com/content/57536d5a-0ddc-11de-8ea3-0000779fd2ac [consulta: 28/2/2023].
[22] LOWE, Christian. «Kremlin loyalist says launched Estonia cyber-attack», *Reuters*. Disponible en: https://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313 [consulta: 28/2/2023].

remoto— utilizadas en los ataques pertenecían, o habían sido utilizadas anteriormente, por la Russian Business Network (RBN)[23], organización cibercriminal que ganó notoriedad en 2007 y 2008. La RBN también proporcionó alojamiento en servidores seguros a foros de Internet como *StopGeorgia.ru* que resultaban esenciales para la coordinación y control de los ataques cibernéticos, proporcionando un servicio que garantizaba el anonimato de los atacantes frente a los investigadores de los equipos de respuesta a emergencias (CERT) extranjeros. El foro *StopGeorgia.ru* se creó 24 horas después de iniciarse el ataque a Georgia, y proporcionaba a hackers atacantes listados de objetivos, enlaces a *malware* para atacar las páginas web del Gobierno georgiano, así como consejos prácticos para hackers con menor experiencia. Y, curiosamente, la RBN cesó sus actividades poco después de finalizar dicho conflicto en Georgia.

En cuanto a la utilización de grupos patrióticos por otras naciones, destaca el caso de Siria. En abril de 2011, pocos días después de que se incrementaran las protestas antigubernamentales en el país, se creó en aquella nación el *Syrian Electronic Army* (SEA). El grupo alegaba ser un equipo de jóvenes entusiastas sirios que no querían permanecer pasivos ante la fabricación de hechos sobre los acontecimientos en Siria, si bien disponía de conexión directa con la Syrian Computer Society, dirigida en la década de 1990 por Bashar al-Assad, antes de convertirse en presidente de dicha nación[24]. El SEA realizaba, fundamentalmente, acciones de desfiguración de sitios web de la oposición siria y de páginas de noticias occidentales consideradas hostiles. No está probado si mantiene o no una afiliación directa con las fuerzas de seguridad sirias pero el propio presidente al-Assad manifestaba su apoyo al afirmar en una entrevista en referencia al SEA que «el Ejército está formado por los hermanos de cada ciudadano sirio, y el ejército siempre defiende el honor y la dignidad. Los jóvenes tienen un papel importante que desempeñar en esta etapa, porque han demostrado ser un poder activo. Existe el ejército electrónico que ha sido un ejército real en realidad virtual»[25].

[23] CORBIN, Kenneth. «Lessons From the Russia-Georgia Cyberwar», *Internet News*. 12 de marzo de 2009. Disponible en: https://www.Internetnews.com/security/lessons-from-the-russia-georgia-cyberwar/ [consulta: 28/2/2023].
[24] NOMAN, Helmi. «The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army», *OpenNet Initiative*. Disponible en: https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army [consulta: 28/2/2023].
[25] O´BRIEN, Danny. «Syria's Assad gives tacit OK to online attacks on press», *Committee to Protect Journalists*. 24 junio de 2011. Disponible en: http://www.cpj.org/internet/2011/06/syrias-assad-gives-tacit-ok-to-online-attacks-on-p.php [consulta: 28/2/2023].

No obstante, ninguna de las operaciones anteriores tuvo la escala ni vínculos gubernamentales tan fuertes y prolongados, como los demostrados en Ucrania desde 2022.

2022: los hackers patrióticos ucranianos se organizan

En la invasión rusa de Crimea en 2014 se pudo ver una intensa utilización de ataques en el ciberespacio, que en el bando prorruso se materializaban en las acciones llevadas a cabo por grupos como *CyberBerkut* y *Anonymous Ukraine*. A su vez, estos últimos se enfrentaban a grupos favorables al gobierno ucraniano como *Cyber Ukrainian Army*, *Cyber Hundred* y *Null Sector*[26]. Como es lógico, no se puede establecer con claridad el grado de apoyo oficial, pero sí la coincidencia de las acciones en tiempo y contenido con los intereses de los respectivos Gobiernos. En cualquier caso, Ucrania no tuvo la visión para coordinar las acciones de los grupos hacktivistas partidarios de su causa.

La invasión de Ucrania en febrero de 2022 ha provocado un resurgimiento del movimiento hacktivistas y de algunos de sus representantes históricos. Su respuesta se materializó a partir del primer trimestre de 2022 en forma de ciberataques sobre sistemas informáticos conectados a Internet de empresas e instituciones rusas. Bajo las etiquetas *#OpRussia* u *#OpRedScare* han actuado diversos actores que pueden clasificarse según su relación con grupos preexistentes:

1. Entidades hacktivistas con afiliación previa conocida al movimiento Anonymous. El grupo original publicó el 24 de febrero de 2022 en su canal de Twitter que «el colectivo Anonymous está oficialmente en ciberguerra contra el Gobierno ruso»[27]. Otros grupos se incorporaron después —*Powerful Greek Army* o *LiteMods*— y todos han realizado acciones de denegación de servicio y de desfiguración de sitios web en Rusia, si bien no participaron en las grandes exfiltraciones de datos que han sido mediáticas durante el conflicto.

[26] MAURER, Tim. «Cyber proxies and the crisis in Ukraine», *Cyber War in Perspective: Russian Aggression against Ukraine*. NATO Cooperative Cyber Defence Centre of Excellence Publications, Tallinn, 2015. https://ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf [consulta: 28/2/2023].

[27] Anonymous @YourAnonOne, 24 de febrero de 2022. Disponible en: https://twitter.com/YourAnonOne/status/1496965766435926039?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496965766435926039%7Ctwgr%5E0a41595a459096dbe4ff05efe7e151f2f0df536a%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Ftherecord.media%2Frussia-or-ukraine-hacking-groups-take-sides%2F [consulta: 28/2/2023].

2. Actores que, hasta iniciarse el conflicto —*Kelvin Security* o *Against The West*—, se dedicaban a la compraventa de credenciales e información sensible en foros especializados, puesta en marcha la invasión, reivindican acciones de obtención y divulgación en el dominio público de información sensible rusa.

3. Actores no identificados que se autodefinen como «próximos a *Anonymous*». Llevan a cabo filtraciones de datos, supuestamente sensibles y procedentes de sistemas informáticos de empresas o instituciones rusas. Reivindican sus acciones y publican la información en canales de propaganda hacktivista (*YourAnonTV'* o *'YourAnonNews*) con iconografía de Anonymous.

4. Nuevos grupos hacktivistas creados tras el inicio del conflicto. Realizan filtraciones de información y ataques de denegación de servicio contra entidades rusas o bielorrusas. Entre ellos encontramos a *Belarusian CyberPartisans*, *Pwn-Bär International Hack Team*, *The Black Rabbit World* y, por supuesto, el *IT Army of Ukraine* del que se hablará con más detalle.

Los grupos contemplados en los párrafos 3 y 4 son los mejores candidatos a ser la herramienta de un Estado y resulta significativa la capacidad de anticipación de algunos de ellos. Así, días antes de iniciarse la invasión, en el canal de Twitter *Anonymous TV*, el grupo homónimo anunciaba que «si las tensiones continúan empeorando en Ucrania, entonces podemos tomar rehenes… sistemas de control industrial»[28]. Al día siguiente añadieron que «la única de las partes que se culpará si llegamos a esa escalada será la misma que la empezó con la concentración de tropas, amenazas infantiles y oleadas de irrazonables ultimátums»[29].

En lo que a grupos puramente ucranianos se refiere desde el comienzo del ataque ruso, se optó por centralizar esfuerzos y así, el 26 de febrero de 2022, el viceprimer ministro y ministro de Transformación Digital ucraniano, Mykhailo Fedorov, anunció la formación del *IT Army of Ukraine*, publicando el siguiente mensaje en sus cuentas oficiales de Facebook y Telegram:

[28] ANONYMOUS TV. Publicación en Twitter de 15 de febrero de 2022. Disponible en: https://twitter.com/youranontv/status/1493718462207832065 [consulta: 28/2/2023].
[29] ANONYMOUS TV. Publicación en Twitter de 16 de febrero de 2022. Disponible en: https://twitter.com/YourAnonTV/status/1493721942955741189 [consulta: 28/2/2023].

«Tenemos muchos ucranianos con talento en el ámbito digital: desarrolladores, ciberespecialistas, diseñadores, redactores, especialistas en marketing, especialistas en *targeting*, etc. Estamos creando un ejército informático. Todas las tareas operativas se presentarán en el canal de Telegram: https://t.me/itarmyofucraine. Habrá tareas para todos»[30].

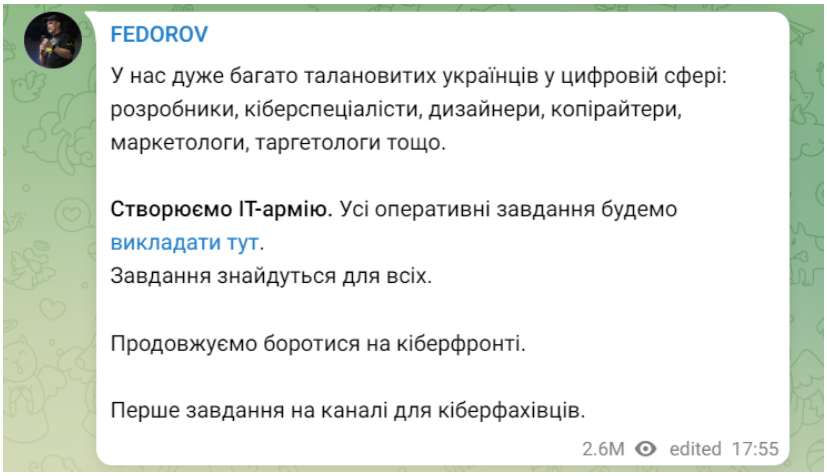

Imagen 2. Anuncio formación *IT Army of Ukraine* (FEDOROV – Telegram)

El mismo día 26, el recién creado *IT Army*, estrenó su perfil de Telegram con la publicación de un listado de páginas web de empresas, bancos y organismos gubernamentales rusos añadiendo que «te animamos a que utilices cualquier vector cíber y ataques DDoS contra estos recursos»[31]. Al día siguiente hicieron lo propio con un listado de canales de noticias en YouTube y medios de comunicación rusos que, según ellos, mentían sobre lo que sucedía en Ucrania; el 1 de marzo hicieron lo propio con las páginas de empresas rusas dedicadas a proveer servicios de firma digital y desde entonces no ha cesado su actividad de señalamiento de objetivos y reivindicación de ataques.

El apoyo público a la causa se incrementó de forma explosiva y el canal de Telegram del *IT Army* ganó 120.000 miembros en un solo día. No existen evidencias de que miembros

[30] Publicación del 26 de febrero de 2022. Disponible en: FEDOROV – Telegram [consulta: el 28/1/2023].
[31] Publicación en Telegram de 26 de febrero de 2022. Disponible en: https://t.me/s/itarmyofukraine2022 [consulta: 28/2/2023].

del gobierno ucraniano dirijan oficialmente los ataques realizados bajo esta iniciativa, si bien la publicidad y apoyo proporcionado por medios oficiales ha sido constante. Así, el 28 de febrero, el Ministerio de Transformación Digital de Ucrania publicó en su perfil de Facebook los siguientes mensajes: «Tres días desde el lanzamiento del IT Army. Primeras victorias sobre el enemigo. En muy poco tiempo, nuestro canal de Telegram ha reunido a muchos profesionales digitales de todo el mundo»[32]. Incluía también algunos objetivos atacados añadiendo que «y esto solo es el principio». La cuenta personal de Telegram de Fedorov ha ido divulgando anuncios del *IT Army*, y la cuenta oficial de su ministerio en la misma red ha seguido publicando actualizaciones sobre el número de objetivos alcanzados mediante ataques tipo DDoS, anunciando que el grupo había paralizado más de 2.400 recursos en línea entre el 29 de agosto y el 11 de septiembre.

Resulta de interés conocer el punto de vista ruso acerca de tales grupos y para ello acudimos a una entrevista concedida por el representante especial del presidente de la Federación Rusa para la Cooperación Internacional en el Ámbito de la Seguridad de la Información, quien afirmó que «en mayo de 2022 más de 65.000 “hackers de sofá” de Estados Unidos, Turquía, Georgia y países de la UE participaban regularmente en ataques DDoS coordinados contra las infraestructuras de información críticas de nuestro país, incluido el sitio de alojamiento de vídeos Rutube»[33]. Añadió a continuación que «un total de 22 grupos de hackers participan en operaciones ilegales contra Rusia, siendo los más activos IT-army of Ukraine (Ucrania), GhostClan (Estados Unidos), GNG (Georgia) y Squad303 (Polonia)». Para finalizar, afirmó que «la militarización del espacio de la información por parte de Occidente y los intentos de convertirlo en un escenario de confrontación interestatal ha multiplicado la amenaza de un choque militar directo de consecuencias imprevisibles». Tales declaraciones no dejan de sorprendernos al provenir del representante de una nación que parece haber realizado un uso intensivo de grupos similares desde hace unos 15 años.

[32] Publicación en Facebook el 28 de febrero de 2023. Disponible en: https://www.facebook.com/photo/?fbid=322693079900015&set=a.292461882923135 [consulta: 29/1/2023].

[33] Respuesta de A. V. Krutskikh, representante especial del presidente de la Federación Rusa para la Cooperación Internacional en el Ámbito de la Seguridad de la Información, director del Departamento de Seguridad de la Información Internacional del Ministerio de Asuntos Exteriores de Rusia, a una pregunta de los medios de comunicación sobre los ataques a instalaciones de infraestructuras críticas rusas. Ministerio de Asuntos Exteriores de la Federación de Rusia, entrevista del 9 de junio de 2022. Disponible en: https://archive.ph/8U6CN [consulta: 28/2/2023].

Pero ¿han resultado efectivos los ataques contra objetivos rusos? Según un informe de Rostelecom[34] —uno de los mayores proveedores de servicios de telecomunicaciones de Rusia— sobre ataques a empresas rusas en 2022, el mayor número (30 %) de tales acciones se han dirigido contra el sector público, que se atacó una media de 3 veces, y en algunos lugares hasta 12 veces más, que el año anterior. Indica también que, al principio del conflicto, los ataques DDoS contra Rusia eran masivos y poco sofisticados, pero que en el tercer trimestre del año se registró un descenso de los ataques masivos y una reorientación de los agresores hacia ataques selectivos más sofisticados. En resumen, Rostelecom, y sus expertos identificaron en este periodo 21,5 millones de incidentes con un alto grado de criticidad.

El *IT Army* ucraniano representa uno de los mejores ejemplos de la nueva herramienta que representan los grupos hacktivistas, y su estatus resulta complejo. En uno de los más completos estudios sobre el grupo se define su estructura como «una construcción híbrida que no es ni civil ni militar, ni pública ni privada, ni local ni internacional, ni legal ni ilegal»[35].

La cuestión de si naciones occidentales han utilizado el hacktivismo como herramienta encubierta de apoyo a Ucrania es un tema que también se ha planteado. En este sentido, fuentes autorizadas ven en el renacimiento de clásicos del hacktivismo como Anonymous —tradicionalmente gran aglutinador de causas activistas, pero hasta no hace mucho con una presencia testimonial limitada a su simbología— como un fenómeno que podría haber sido iniciado por algún Estado, si bien al movimiento se han sumado posteriormente numerosos individuos o grupos que sí se adscriben claramente a las causas hacktivistas. Así, organizaciones como el Centro Criptológico Nacional han advertido de la existencia de una nueva tendencia a la «instrumentación del hacktivismo y de 'Anonymous' como banderas de conveniencia en conflictos híbridos o en

[34] Отчет об атаках на онлайн-ресурсы российских компаний за 2022 год (Informe sobre los ataques a los recursos en línea de las empresas rusas en 2022), *Rostelecom-Solar*. Enero 2023. Disponible en: https://rt-solar.ru/upload/iblock/02e/nns12uwyw3k2olfwq13o52aabrjrun2z/Otchet-ob-atakakh-na-onlayn_resursy-rossiyskikh-kompaniy.pdf [consulta: 29/1/2023].

[35] SOESANTOM, Stefan. «The IT Army of Ukraine Structure, Tasking, and Ecosystem», *Center for Security Studies (CSS)*. ETH Zürich, junio de 2022. Disponible en: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf [consulta: 28/2/2023].

ciberataques donde confluyen varios intereses de parte por actores que pretenden una ganancia, ya sea geopolítica, militar, económica o de otra naturaleza»[36].

Como resumen, podemos concluir que, si bien durante las primeras fases del conflicto —en 2014— el gobierno ucraniano no supo coordinar el potencial de las capacidades proporcionadas por voluntarios, en esta segunda fase, iniciada en 2022, Ucrania ha demostrado disponer del conocimiento y la voluntad para organizar y aglutinar dichas capacidades en una única entidad, el *IT Army*, que, de una manera o de otra, ha sido apoyado por las autoridades y orientado para alcanzar objetivos de interés nacional.

2022: grupos prorrusos, el oso se desata

Desde el inicio de la invasión de Ucrania en 2022 los atacantes supuestamente respaldados por el gobierno ruso persiguen agresivamente una ventaja bélica en el ciberespacio[37]. Los ciberataques se han diseñado para aumentar el caos de una invasión convencional, reducir la gobernabilidad del país y dañar las infraestructuras críticas. No obstante, el objetivo principal de los hackers rusos ha cambiado desde el comienzo de la guerra. Antes de la invasión, y durante el primer mes del conflicto, los ciberataques se dirigieron contra las infraestructuras de comunicaciones gubernamentales, indicando que su objetivo era limitar la funcionalidad del ejército y el Gobierno de Ucrania. Sin embargo, tras la primera derrota en el frente, Rusia se centró en infligir daño a la población civil, siendo el mejor ejemplo la coordinación entre ciberataques y ataques cinéticos contra las infraestructuras energéticas[38].

El ecosistema del hacktivismo prorruso es muy variable y tan pronto aparecen grupos nuevos como surgen alianzas entre otros. No aceptan restricciones y no reconocen fronteras internacionales, realizando ataques contra entidades que, dentro y fuera de Ucrania, son consideradas una amenaza para Rusia. La mayoría se comunican y coordinan sus ataques a través de la plataforma de mensajería Telegram y su

[36] *CCN-CERT IA-03/22 Informe anual hacktivismo y ciberyihadismo 2021*. Centro Criptológico Nacional, Madrid, mayo de 2022. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6594-ccn-cert-ia-03-22-informe-anual-2021-hacktivismo-y-ciberyihadismo-1/file.html [consulta: 28/2/2023].

[37] GOOGLE THREAT ANALYSIS GROUP (TAG). «Fog of War How the Ukraine Conflict Transformed the Cyber Threat Landscape», *Google*. Febrero de 2023. Disponible en: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf [consulta: 28/2/2023].

[38] KHMELOVA, Ilona. *Cyber, Artillery, Propaganda. General Overview of the Dimensions of Russian Aggression*. The Economic Security Council of Ukraine / State Service of Special Communications and Information Protection of Ukraine, 2022. Disponible en: https://cip.gov.ua/en/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi [consulta: 28/2/2023].

coordinación se efectúa en gran medida mediante el anuncio público previo de listas de objetivos que pueden ser objeto de ataques. Estos son predominantemente ataques tipo DDoS, si bien otros actores incluyen la desfiguración de sitios web, vulneración de redes y publicación de los documentos exfiltrados (*hack-and-leak*), así como la ejecución de acciones de *doxing*, consistentes en hacer pública la información personal de individuos u organizaciones. Los grupos han reaccionado a los acontecimientos casi en tiempo real y así, en julio de 2022, hacktivistas prorrusos atacaron páginas web del Gobierno y entidades financieras lituanas tan pronto aquella nación decidió bloquear el transporte de mercancías y suministros a Kaliningrado, el enclave ruso situado entre Lituania y Polonia.

Desde el inicio de la guerra han destacado por su actividad dos grupos hacktivistas prorrusos autoproclamados patrióticos, *Killnet* y *Xaknet*. *Killnet* apareció en escena al registrar dominios de Internet y crear cuentas en diversas redes sociales a finales de enero de 2022, esto es, cerca de un mes antes de iniciarse la ofensiva militar[39]. Comenzó sus actividades alrededor del 4 de marzo de 2022, y originalmente anunció ataques a través de *Cyber Army of Russia* y su canal de desinformación en la red Telegram. Posteriormente, *KillNet* ha alcanzado cierta notoriedad gracias a medios rusos, por ejemplo con un discurso en vídeo difundido por el canal de noticias estatal Russia Today (RT)[40]. Posteriormente ha concedido entrevistas a medios estales como *Gazeta.ru* anunciando su alianza con Phoenix, grupo supuestamente localizado en Ucrania[41], y a *RT*, afirmando respecto a sus ataques contra páginas web de la OTAN del pasado 12 de febrero que «el ataque DDoS a los sitios web de la OTAN de este domingo fue una distracción y que hacer chillar a Stoltenberg sale caro, lo que significa que hemos dado en el clavo»[42].

Existen evidencias técnicas que constatan cómo grupos hacktivistas prorrusos como *XakNet Team*, *Infoccentr* y *CyberArmyofRussia_Reborn* coordinan sus operaciones con el agente de la amenaza APT28, asociado a la Unidad 26165 de la Dirección Principal

[39] INSIKT GROUP. «Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine», *Recorded Future*. 31 de enero de 2023. Disponible en: https://go.recordedfuture.com/hubfs/reports/cta-2023-0131.pdf [consulta: 28/2/2023].
[40] Página ya no accesible, referencia en https://twitter.com/cyberknow20/status/1528736348437303301?lang=es [consulta: 5/2/2023].
[41] KILDYUSHKIN, Roman. «KillNet: украинские хакеры начали поддерживать Россию (KillNet: los hackers ucranianos empiezan a apoyar a Rusia)», *Gazeta.ru*. 5 de febrero de 2023. Disponible en: https://www.gazeta.ru/tech/news/2023/02/05/19667983.shtml [consulta: 5/2/2023].
[42] WE ARE KILLNET, publicación Telegram 14 de febrero de 2023. Disponible en: https://t.me/s/killnet_reservs/5127 [consulta: 28/2/2023].

de Inteligencia del Ejército ruso (GRU). Esta evaluación se basa principalmente en las observaciones realizadas acerca del despliegue de programas maliciosos exclusivos de APT28 para robo de datos en las redes de múltiples organizaciones ucranianas y en el procedimiento seguido por los grupos hacktivistas, que publican en sus canales de Telegram los datos robados 24 horas después de que estas hayan sido atacadas con *wipers* —*malware* destinado a borrar el disco duro del ordenador que infecta, eliminando maliciosamente información y programas— y dichos datos borrados en los objetivos ucranianos. Empresas de ciberseguridad han identificado al menos 16 filtraciones de datos de estos grupos, cuatro de las cuales coincidieron con ataques de *wipers* de APT28[43].

Imagen 3. Reivindicación de *Noname057(16)* de ataques DDoS contra ministerios de defensa occidentales. https://t.me/s/noname05716eng

[43] «GRU: Rise of the (Telegram) MinIOns», *Mandiant Intelligence*. 23 de septiembre de 2022. Disponible en: https://www.mandiant.com/resources/blog/gru-rise-telegram-minions [consulta: 28/2/2023].

Los beneficios económicos no desempeñan un papel primordial en el hacktivismo pero algún grupo ha incentivado la actividad de sus miembros mediante recompensas. Por ejemplo, a partir de agosto de 2022, el grupo *Noname057(16)* premió con bonificaciones económicas a final de mes a los tres atacantes más activos a la hora de realizar acciones ofensivas tipo DDoS. Por otro lado, el grupo hacktivista *KillNet* aprovechó su creciente reputación y popularidad en los círculos prorrusos para vender artículos de marca como pendientes, camisetas y anillos con el logotipo del grupo[44]. Hay que destacar también que *KillNet* mantiene un canal en Telegram específico para recibir donaciones, donde afirma: «No somos una estructura estatal, nuestras actividades no las paga el presidente de la Federación Rusa»[45].

Ya se ha dicho que algunos de estos grupos son utilizados secundariamente para la difusión de desinformación, si bien para estos menesteres se han creado otras organizaciones de supuestos jóvenes patrióticos. El principal exponente es *Cyber Front Z*, que en su canal de Telegram, inaugurado el 11 de marzo de 2022, se autodenomina movimiento popular afirmando trabajar para combatir la avalancha de noticias falsas y desinformación procedentes de Ucrania, Estados Unidos y Europa Occidental sobre la «operación especial» y alertando de que «cuanto más éxito tengan nuestros guerreros en la lucha contra la plaga en Ucrania, más falsificaciones y ataques informativos aparecerán»[46]. No obstante, el grupo parece ser una nueva versión de la desaparecida Internet Research Agency —la famosa granja de *trolls* activa entre 2013 y 2018— según demuestran periodistas de un medio ruso infiltrados en la organización[47], y desde el mismo se impulsan muchas de las teorías y narrativas conspirativas infundadas que el Kremlin ha apoyado a lo largo de esta guerra.

Resulta también muy probable que grupos cibercriminales trabajen con el Estado ruso para coordinar o amplificar las operaciones cibernéticas y de información ofensivas[48]. En

[44] INTEL 471. «Pro-Russian Hacktivism and Its Role in the War in Ukraine», *INTEL 471 Blog*. 19 de octubre de 2022. Disponible en: https://intel471.com/blog/pro-russian-hacktivism-and-its-role-in-the-war-in-ukraine [consulta: 28/2/2023].
[45] @donate_killnet. Publicación en Telegram del 23 de mayo de 2022. Disponible en: https://t.me/s/donate_killnet [consulta: 28/2/2023].
[46] Canal Telegram @Cyber front Z. Disponible en: https://t.me/s/cyber_frontZ [consulta: 28/2/2023].
[47] KLOCHKOVA, Ksenia. «Вы ведь не верите, что это настоящие отзывы?» Как «Фонтанка» заглянула на передовую информационных фронтов Z (No creerás que son críticas reales, ¿verdad? Cómo Fontanka se asomó a la primera línea de los frentes informativos Z. *Fontanka.ru*. 21 de marzo de 2022. Disponible en: https://www.fontanka.ru/2022/03/21/70522490/ [consulta: 28/2/2023].
[48] INSIKT GROUP. «Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine», *Recorded Future*. 31 de enero de 2023. Disponible en: https://go.recordedfuture.com/hubfs/reports/cta-2023-0131.pdf [consulta: 28/2/2023].

este sentido, en una declaración conjunta publicada por la Cybersecurity & Infrastructure Security Agency (CISA), las autoridades de ciberdefensa estadounidenses, australianas, canadienses, neozelandesas y británicas consideran que varios grupos de ciberdelincuentes de aquella nación suponen una amenaza para las organizaciones de infraestructuras críticas[49].

Se considera que en un futuro próximo la actividad de todas estas entidades se mantendrá e incluso puede evolucionar en sus procedimientos, llegando incluso a llevar a cabo acciones ofensivas más sofisticadas, tal y como apunta la declaración de la CISA. El continuado uso por parte de Rusia a lo largo del conflicto de proxies como el Grupo Wagner y los ciberdelincuentes prorrusos, los hacktivistas y los actores de influencia, ha evidenciado el control estatal sobre estos grupos, al tiempo que ha puesto de manifiesto el deseo de Rusia de tener una negación plausible de sus acciones[50].

Y para finalizar este apartado, un punto de vista ruso muy actual. El pasado 10 de febrero Alexander Khinshtein, jefe del Comité de la Duma Estatal sobre Política de Información, expresó a los periodistas tras una reunión que debatía sobre la ciberseguridad de Rusia que «los llamados piratas informáticos que actúan en interés de Rusia en su territorio y en el extranjero deben estar exentos de responsabilidad». El parlamentario también afirmó que «creo firmemente que es necesario utilizar cualquier recurso para luchar eficazmente contra el enemigo»[51]. No deja de ser una opinión personal pero de gran relevancia, no solo por la posición de quien opina sino, sobre todo, porque puede tratarse de la manera de hacer llegar el mensaje a otras naciones.

Conclusiones

La utilización de *adversarios por delegación* es un principio aplicado desde los primeros conflictos bélicos y, con la aparición del ciberespacio como ámbito de operaciones, recurrir a *ciberproxies* se ha convertido en práctica habitual para que algunas naciones

[49] «Alert AA22-110A Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure», *Cybersecurity & Infrastructure Security Agency* (CISA). 9 de mayo 2022. Disponible en: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a [consulta: 28/2/2023].
[50] INSIKT GROUP. TA-2023-0209 «Themes and Failures of Russia's War Against Ukraine», *Recorded Future*. 9 de febrero de 2023. Disponible en: https://go.recordedfuture.com/hubfs/reports/ta-2023-0209.pdf [consulta: 28/2/2023].
[51] TASS. 10 de febrero de 2023. Хинштейн заявил, что действующих в интересах РФ хакеров надо освободить от ответственности (Hinshtein dice que los hackers que actúan para Rusia deben ser exonerados). Disponible en: https://tass.ru/obschestvo/17021313 [consulta: 28/2/2023].

realicen actividades que oficialmente no pueden llevar a cabo, bien por razones legales, o bien por no resultar aceptables de cara a la opinión pública propia.

Esta estrategia resulta especialmente útil a algunos Estados pues posibilita ocultar la atribución de sus acciones y mantener la opción de la negación plausible.

Por otro lado, el empleo de *ciberproxies* también permite a los Estados no revelar sus verdaderas capacidades, una ventaja importante para quienes deseen mantener discreción en áreas de importancia estratégica como las capacidades ofensivas en el ciberespacio.

Entre las distintas opciones de ciberactores no estatales, los grupos hacktivistas se han convertido en el medio preferido de actuación para algunos Estados en el ciberespacio. Utilizar tales grupos como *ciberproxies* constituye una excusa excelente por tratarse de un conjunto heterogéneo de individuos o entidades, que no se ajustan a los comportamientos socialmente establecidos y que cuentan con una pseudolegitimación moral o ideológica. El mejor y más reciente ejemplo lo constituye el actual conflicto entre Rusia y Ucrania.

Si bien durante las primeras fases del conflicto —en 2014— el Gobierno ucraniano no supo coordinar el potencial de las capacidades ciberofensivas proporcionadas por voluntarios, en esta segunda fase iniciada en 2022 Ucrania ha demostrado disponer del conocimiento y la voluntad para organizar y aglutinar dichas capacidades en una única entidad, el *IT Army*, que de una manera o de otra se ha orientado para alcanzar objetivos de interés nacional.

Por su parte, Rusia ha sabido usar desde hace años como *proxies* a grupos hacktivistas y entidades que operan en foros de ciberdelincuentes, y comenzó a experimentar con su empleo en la campaña de Georgia en 2008. En el actual conflicto contra Ucrania estos grupos han coordinado y realizado ataques contra entidades, dentro y fuera del país, consideradas una amenaza para Rusia.

Secundariamente, estos grupos pueden emplearse también como vector de difusión de desinformación, y las campañas que desarrollan utilizadas para propagar información tergiversada y triunfalista, generando en las audiencias de las naciones atacadas una falta de confianza en sus propias autoridades. De la misma manera se utilizan para reforzar la moral de las audiencias propias.

Se considera que en un futuro próximo la utilización de *proxies* continuará siendo —incluso en mayor medida— uno de los principales recursos empleados por las naciones en los futuros conflictos, independientemente de la fase en que estos se encuentren.

El creciente uso de *proxies* cibernéticos no resulta especialmente tranquilizador pues incrementa la probabilidad de sufrir ciberataques. Además, existe el riesgo añadido de que los Estados pierdan el control sobre los objetivos y los medios de actuación de la operación al delegar en *proxies*.

Todo lo anterior evidencia la importancia fundamental de mantener unas adecuadas capacidades de ciberdefensa que puedan hacer frente a unos agentes amenazantes, cada vez más preparados y dispuestos a llevar ataques de un alto nivel de complejidad e impacto.

*Francisco Marín Gutiérrez***

Teniente coronel del Ejército de Tierra
Mando Conjunto del Ciberespacio (MCCE)