ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

94/2023 6 de noviembre de 2023

Josué Expósito Guisado *

«Ciberproxies»: las APT como factor de riesgo futuro

«Ciberproxies»: las APT como factor de riesgo futuro

Resumen:

Una vez extraídas las lecciones que la guerra de Ucrania dejará, un futuro próximo podría venir marcado por la revitalización de las zonas grises de los conflictos. Esta situación intermedia entre la paz y la guerra supone el caldo de cultivo perfecto para que el ciberespacio se configure como el escenario ideal de confrontación entre grandes potencias que pueden ver en la utilización de *ciberproxies* un recurso idóneo para escalar la tensión geopolítica.

Los *ciberproxies* se convertirán en un factor de riesgo para las democracias occidentales y en un reto para la seguridad internacional.

Palabras clave:

Ciberproxy, APT, ciberguerra, ciberdominio.

Cyberproxies: APT's as a future risk factor

Abstract:

The near future could be marked by a revitalization of the gray areas of conflict, drawing on the lessons that the war in Ukraine will leave behind. Precisely, this intermediate scenario between peace and war is the perfect breeding ground for cyberspace to be configured as the ideal scenario for confrontation between great powers. The great powers may see the use of cyberproxies as the perfect resource to increase the escalation of geopolitical tension. Cyberproxies will become a risk factor for Western democracies, and a challenge for international security

Keywords:

Cyberproxy, APT, cyber warfare, ciber domain

Cómo citar este documento:

EXPÓSITO GUISADO, Josué. *Ciberproxies: Las APT como factor de riesgo futuro*. Documento de Opinión IEEE 94/2023.
https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO94_2023_JOSEXP_Ciber.pdf
y/o enlace bie[3] (consultado día/mes/año)

Introducción

El nacimiento y popularización de nuevas tecnologías suele venir acompañado de un cambio en las doctrinas militares, producto de nuevas ventanas de oportunidad y de nuevos riesgos para la seguridad[1].

El surgimiento de internet y de la tecnología generada a partir de la piedra angular de la conectividad (el internet de las cosas) ha supuesto un cambio en las sociedades contemporáneas tan gigantesco como el experimentado por nuestros abuelos en febrero de 1946 con el nacimiento del Electronic Numerical Integrator and Computer (ENIAC), el primer ordenador calculador e integrador numérico electrónico.

La conectividad que caracteriza a nuestras sociedades ha avanzado hasta el punto de la práctica interconexión entre el plano intangible de la informática y el espacio físico. El nacimiento de un nuevo dominio, el cibernético —también conocido en Occidente como ciberespacio—[2], ha condicionado en los últimos años la visión que las potencias geopolíticas tienen de los principales desafíos a la seguridad mundial.

Antes de la invasión rusa de Ucrania, la inmensa mayoría de los analistas en Occidente descartaba un conflicto de características convencionales como el que está ocurriendo. En su lugar, abogaban por un protagonismo especialmente destacado de la zona gris del conflicto, donde el papel de las operaciones de desinformación y las operaciones cibernéticas fuese especialmente activo.

Lamentablemente, el escenario ruso-ucraniano superó esta suerte de calma tensa a medio camino entre la paz *(bona fides)* y la guerra *(open warfare)*[3]. Los mismos académicos que antes descartaban la posibilidad de un conflicto de esta magnitud en Europa coinciden hoy en resaltar el papel marginal que el ciberespacio está jugando en él, sin tener en cuenta la idoneidad de su utilización en un contexto de guerra abierta o

[1] TORRES SORIANO, Manuel. «Ciberguerra», en Jordán, Javier (coord.), *Manual de estudios estratégicos y seguridad internacional*. Plaza y Valdés, Madrid, 2013, pp. 329-348.
[2] El ciberespacio ha de ser entendido como «un dominio global perteneciente al entorno de la información, compuesto por una infraestructura de redes de tecnologías de la información interdependientes, que incluye internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores» (NMSCO. National Military Strategy for Cyberspace Operations by the Joint Chiefs of Staff of the Armed Forces of the United States of America. 2006).
[3] BAQUÉS, Josep. «Hacia una definición del concepto *gray zone* (GZ)». *Revista del Instituto Español de Estudios Estratégicos,* n.º 6. 2017, pp. 1045-1076.

las doctrinas militares que explican la concepción distinta que tienen los rusos de la utilización del componente cibernético.

En un conflicto de tintes convencionales como el ruso-ucraniano, donde la artillería está jugando un papel central, el uso de medios cibernéticos ciertamente es marginal, pues estos no pueden competir con los medios convencionales en términos de potencialidad destructiva y eficiencia. La competencia entre potencias en el ciberdominio no está orientada hacia escenarios de guerra abierta, al menos no por parte de Rusia.

El papel que juegan las operaciones cibernéticas se limita a proporcionar una ventaja inicial mediante ciberataques tempranos, ya que, una vez estalla la tensión en la zona gris, las funcionalidades cibernéticas convergen hacia la inteligencia y el despliegue de operaciones de influencia en el dominio de la información, y no tanto hacia el potencial destructivo de estas herramientas.

Realizando un ejercicio de prospectiva, todo parece indicar que un alto el fuego no supondría el fin de la confrontación cibernética. Cuando intereses estratégicos, consideraciones políticas y emociones se combinan y confrontan es poco probable que la fricción desaparezca. Al contrario, tanto el conflicto ruso-ucraniano como el existente entre China y Taiwán evolucionarán hacia unas futuras zonas grises donde la utilización de medios cibernéticos será especialmente atractiva.

La determinación de las partes en conflicto se orientará al mantenimiento de la influencia sociopolítica y el despliegue de operaciones de información en el dominio cibernético.

En una futura disputa en la zona gris entre Rusia y Ucrania, ambas partes pueden tratar de promover operaciones cibernéticas de falsa bandera con el objetivo de culpar al enemigo de deteriorar la estabilidad y, bajo este pretexto, descongelar una posible situación encallada tras un futuro alto el fuego[4].

Precisamente, una de las funciones principales del dominio cibernético en la guerra de Ucrania está siendo albergar operaciones de hostigamiento y perturbación cibernética realizadas por hacktivistas vinculados con el Kremlin, que utilizan de forma reiterada

[4] LEVITÉ, Ariel E. «Integrating Cyber into Warfighting: Some early takeaways from the Ukraine conflict. Cyber Conflict in the Russia-Ukraine War». Carnegie Endowment for International Peace, 18 de abril de 2023. Disponible en: https://carnegieendowment.org/2023/04/18/integrating-cyber-into-warfighting-some-early-takeaways-from-ukraine-conflict-pub-89544 [consulta: 28/8/2023].

ataques DDoS (denegación de servicio distribuido)[5] con el objetivo de crear un clima de tensión y acoso persistente entre los enemigos occidentales.

Este objetivo se alinea con los estudios doctrinales y estratégicos rusos que enuncian la «confrontación de información» o «guerra de información» *(informatsionnoe protivoborstvo).* Esta perspectiva concibe el ciberespacio desde una gama de operaciones amplia que abarca varios subconjuntos en el entorno de la información con el fin de alcanzar un impacto tanto psicológico como tecnológico[6,7].

En el escenario prospectivo de paz imperfecta descrito parece evidente que no solo resurgirá el debate sobre las implicaciones de los ciberataques y sobre si estos podrían llegar a considerarse actos de guerra, sino que también se potenciará el recurso a uno de los actores más controvertidos del ciberdomino, dada la facilidad que otorga a los Estados para ocultar su identidad: los *ciberproxies*.

Ciberproxies: **un riesgo presente y futuro**

Hasta el momento, los *ciberproxies* han venido «personificándose» a través de distintas entidades vinculadas al mundo de la ciberdelincuencia y el ciberespionaje. Sin embargo, el término es mucho más amplio, pues engloba desde grupos criminales hasta empresas privadas cuyo modelo de negocio son las ciberarmas —actores ofensivos del sector privado, en inglés *private sector offensive actor* (PSOA)—, pasando por grupos terroristas, insurgentes o activistas, entre los cuales encontraríamos a los denominados «ciberpatriotas».

[5] Ataques orientados a bloquear la distribución del servicio o la infraestructura en red de un objetivo mediante la sobresaturación producida por una avalancha de tráfico de red concentrada en un tramo horario.

[6] Como seres humanos, las percepciones y concepciones que tenemos del mundo no son universales, sino que estas se encuentran sesgadas por una infinidad de factores. Estos factores permiten que conceptos similares sean entendidos de formas distintas. Así, mientras que en las naciones occidentales, y en Estados Unidos en particular, las actividades de control político que permite el ciberespacio se definen de forma estricta como la negación al adversario de la capacidad de proyectar su influencia en el terreno doméstico y hacia el resto de los Estados, para Rusia o China este no es más que un objetivo secundario. Quizás, obviar las diferencias entre el ciberespacio entendido desde Occidente y la concepción de dominio de la información rusa sea uno de los factores que llevó a múltiples analistas occidentales a esperar una ciberguerra en Ucrania.

[7] BO POULSEN, Niels y STAUN, Jørgen. *Russia's Military Might – A Portrait of its Armed Forces.* Djøf Forlag, Copenhague, 2021.

En términos generales, podemos decir que los *ciberproxies* son intermediarios que llevan a cabo acciones ofensivas en el ciberespacio en beneficio de un actor principal[8]. El término engloba a un gran número de entidades organizadas que de forma directa o indirecta actúan en el ciberespacio, y que en la actualidad suponen un factor de riesgo para las principales empresas y gobiernos occidentales, por lo que se las ha calificado como amenazas persistentes avanzadas (APT).

A este respecto, Rondeaux y Sterman realizan una excelente definición de la guerra de *proxies,* que se distingue por el patrocinio directo o indirecto de terceros actores convencionales o irregulares, ajenos a la estructura de seguridad de los Estados involucrados en un conflicto armado[9].

Dejando a un lado las cuestiones puramente teóricas, lo cierto es que el recurso de la guerra por delegación ha sido ampliamente utilizado a lo largo de la historia, especialmente en el contexto estratégico de la Guerra Fría, donde los riesgos inherentes a una posible escalada nuclear hicieron de este tipo de enfrentamientos la herramienta predilecta para debilitar la posición del adversario sin correr riesgos excesivos.

La posibilidad de impulsar intereses estratégicos a bajo coste también ha sido un poderoso incentivo tras el fin de las hostilidades entre bloques. Asimismo, destaca su utilización tras la irrupción del ciberespacio, un dominio cuyo carácter ambiguo favoreció intensamente el enfrentamiento indirecto entre Estados.

APT: definición y catalogación

Con lo visto hasta el momento, podemos resaltar dos aspectos fundamentales de la delegación: los actores apoderados y la relación que estos establecen con las estructuras de poder estatales.

[8] MAURER, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, 2018.
[9] RONDEAUX, Candance y STERMAN, David. (2019). «Twenty-First Century Proxy Warfare. Confronting Strategic Innovation in a Multipolar World Since the 2011 NATO Intervention». New America, Washington, 20 de febrero de 2019. Disponible e https://www.newamerica.org/future-security/reports/twenty-first-century-proxy-warfare-confronting-strategic-innovation-multipolar-world/ [consulta: 25/8/2023].

Conviene, por tanto, definir qué entendemos por APT y cuáles son sus principales características, pues a través de ellas cobra sentido este acrónimo[10].

En primer lugar, una ATP se define como un grupo de personas que actúa en pro de un fin concreto, cuya consecución va en detrimento de la seguridad del objetivo atacado, para el cual supone una amenaza.

En segundo lugar, a diferencia de los ciberdelincuentes comunes, este tipo de grupos no se centra únicamente en obtener un lucro económico inmediato[11]. Normalmente desarrollan una actividad continuada a través de la monitorización del sistema infectado. Para ello, instalan *softwares* específicos destinados a la recopilación de información y persisten en su ataque creando nuevas formas de entrada al sistema, que les permiten acceder a él durante un tiempo prolongado.

Por último, cabe destacar que estos grupos emplean una amplia diversidad de medios para acceder a los ordenadores, redes y sistemas objetivo (*malware*, *spyware*, ingeniería humana, robo de identidad, medios de infección, etc.), lo que *de facto* los convierte en una amenaza con un potencial técnico avanzado.

En términos generales, estos grupos son empleados para llevar a cabo dos tipos de acciones. Las acciones ofensivas limitadas son las más comunes: ataques DDoS contra páginas web institucionales o de empresas vinculadas a sectores críticos para el adversario (transporte, energía, financieros) y la desconfiguración de esas mismas páginas inyectándoles contenidos maliciosos o utilizándolas para publicar información sensible exfiltrada. Por otro lado, estos grupos pueden emplearse como vectores de difusión de desinformación en campañas de guerra informativa para propagar información tergiversada y triunfalista que refuerce la moral de las audiencias internas y genere un clima de desafección hacia los gobernantes e instituciones entre la opinión pública del enemigo: estas son las dos caras de este tipo de campañas.

[10] DAMBALLA. *Advanced Persistent Threats.* Atlanta, 2010.

[11] Las APT implican una gama de recompensas diversas, que van desde el prestigio personal atribuido a sus miembros en la red hasta la defensa de ideales políticos. Si bien los beneficios económicos no desempeñan un papel primordial para este tipo de actores, existen grupos hacktivistas vinculados con distintas APT que han incentivado la actividad de sus miembros mediante distintas recompensas. Por ejemplo, desde agosto de 2022, Noname057 premia con bonificaciones económicas mensuales a sus atacantes más activos.

En la guerra de Ucrania se ha podido comprobar que el papel fundamental de este tipo de actores es la realización de ataques DDoS regulares contra infraestructuras críticas. Decenas de grupos y miles de individuos han participado en las operaciones mencionadas. En el bando ucraniano destacan grupos como IT-Army of Ukraine (Ucrania), GhostClan (Estados Unidos), GNG (Georgia) y Squad303 (Polonia); en el bando ruso sobresalen NoName057, Killnet, Turla APT y FancyBear (APT-28).

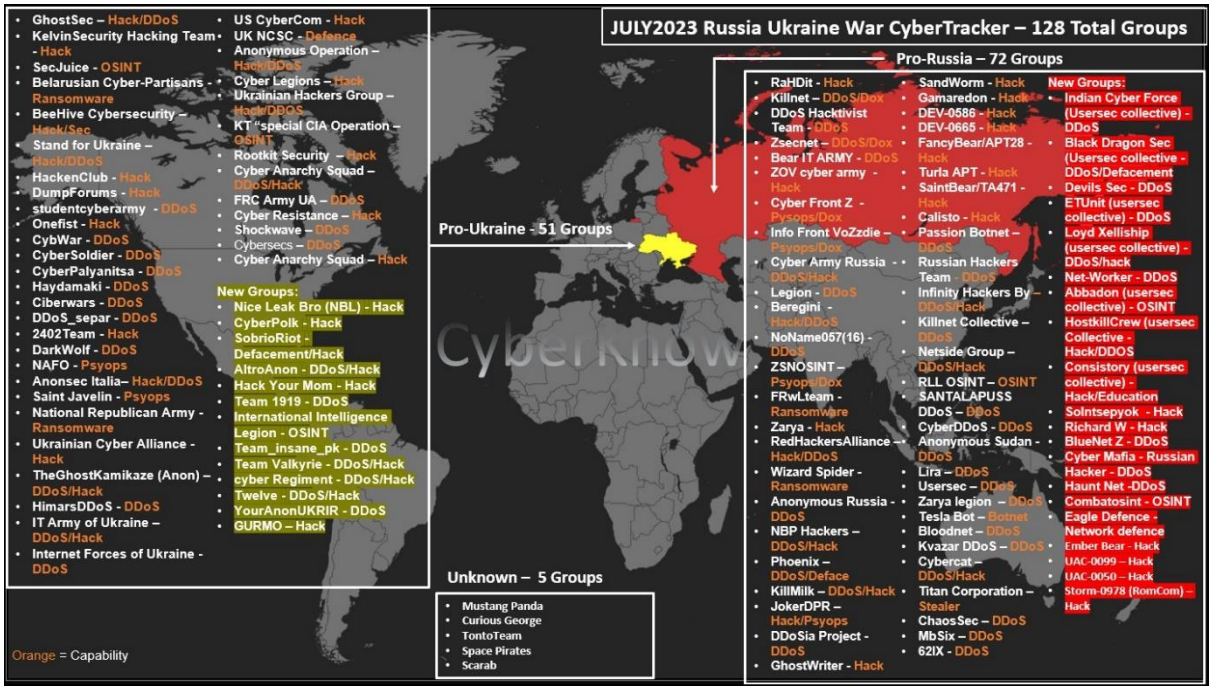

Figura 1. Principales grupos *proxies* involucrados en el conflicto ruso-ucraniano
Fuente: CYBERKNOW (@CyberKnow20). «Cybertracker Russia-Ukraine War». Twitter, 20 de julio de 2023 (actualizado el 24 de julio de 2023). Disponible en: https://twitter.com/Cyberknow20/status/1682006183299923968 [consulta: 3/9/2023].

Las características intrínsecas del ciberespacio —principalmente la dificultad que entraña atribuir la autoría de un ciberataque, la diversidad de adversarios y la falta de regulación internacional— propician que estas amenazas se ajusten a la perfección a la etiqueta de «acción no convencional»[12].

Estas acciones no convencionales suelen implementarse en contextos de guerra híbrida, pero no únicamente, pues resultan especialmente útiles en la llamada «zona gris» *(gray*

[12] ARTEAGA, Félix. (2019). «Capacidades ofensivas, disuasión y ciberdefensa». Real Instituto Elcano, 10 de septiembre de 2019. Disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari92-2019-arteaga-capacidades-ofensivas-disuasion-y-ciberdefensa [consulta: 4/9/2023].

zone), el escenario intermedio entre las situaciones pacíficas *(bona fides)* y la guerra propiamente dicha *(open warfare).*

La utilización de APT y grupos vinculados en procesos de guerra *proxy* se ha convertido en la actualidad en una práctica habitual para algunos Estados, ya que permite ocultar la autoría de las acciones y posibilita que estas sean negadas de forma plausible ante posibles casos de escalada y errores de medición de impacto.

Una de los rasgos más interesantes de este tipo de actores es el carácter «voluntario» que podríamos llegar a atribuir a sus acciones, lo que además impide determinar con certeza si están dirigidas por entidades estatales. A lo expuesto, se suma la dificultad técnica que entraña establecer la autoría de un ataque.

Sin embargo, la imposibilidad técnica de establecer el origen de un ataque no es más que un mito. El rastro que las operaciones cibernéticas generan y los objetivos que persiguen aportan pruebas suficientes para pensar que, si bien no existe una conexión directa entre organismos estatales y las distintas APT, sí que puede demostrarse que estas últimas siguen en cierta forma las directrices de las principales agencias de seguridad.

Dicho de otro modo, el hecho de que sus acciones coincidan en tiempo y contenido con los intereses de los actores patrocinadores evidencia que determinar la autoría de un ciberataque, aunque técnicamente resulta complejo, no es una tarea imposible[13].

De hecho, el aspecto forense no es determinante ni principal —no estamos ante un proceso judicial constituido sobre la necesidad de pruebas legales—, es la propia lógica política la que dificulta que pueda ocultarse la autoría de un ataque al existir una rivalidad previa que condiciona la interacción entre las partes[14].

[13] GUITTON, Clement y KORZAK, Elaine. «The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks», *The RUSI Journal,* vol. 158, n.º 4. 2013, pp. 62-68.
[14] AXELROD, Robert. «A Repertory of Cyber Analogies», en GOLDMAN, Emily O. y ARQUILLA, John (eds.), *Cyber Analogies.* Department of Defense Information Operations, Center for Research, Monterey, 2014.

Así, es lógico que cuando Corea del Sur es atacada en el ciberespacio mire hacia Corea del Norte[15]; que cuando Israel sufre este tipo de agresiones sospeche de Irán o que cuando Georgia o Ucrania son el objetivo atribuyan la responsabilidad a Rusia[16].

En este último caso, existen además evidencias técnicas que constatan que distintos grupos 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 de Inteligencia del Ejército ruso (GRU)[17].

El otro aspecto fundamental, las relaciones características que las distintas APT establecen con las estructuras de poder estatales, puede estudiarse a través de las diferencias enunciadas en la siguiente tipología, que las cataloga en cuatro grupos[18].

Proxies *cautivos*

En primer lugar, encontraríamos los denominados *proxies* cautivos, que adolecen de una sólida dependencia (económica, legal o política) respecto de la entidad estatal que actúa como actor principal, capaz de imponer su poder para orientar las acciones del *proxy* (activas o pasivas) contra un objetivo determinado. El ejemplo paradigmático de estos actores son las empresas privadas vinculadas al sector IT *(information and technology)* —más conocido en el mundo hispanohablante como TIC (tecnologías de la información y la comunicación)—, que terminan actuando como *proxies* por «omisión», es decir, plegándose a los dictámenes estatales.

En los últimos años, y especialmente a raíz de la guerra de Ucrania, las tecnológicas estadounidenses han resultado clave a la hora de analizar las acciones ofensivas rusas. Empresas como Mandiant, Apple o Microsoft han tenido que enfrentar el dilema ético y político que supone determinar si debe prevalecer la lealtad a sus clientes o la impuesta por los intereses nacionales de los Estados donde tienen sede.

[15] RID, Thomas y BUCHANAN, Ben. «Attributing Cyber Attacks», *Journal of Strategic Studies,* vol. 38, n.º 1-2. 2015, pp. 4-37.
[16] INKSTER, Nigel. «Cyber Attacks in La-La Land», *Survival: Global Politics and Strategy,* vol. 57, n.º 1. 2015, pp. 105-116.
[17] MANDIANT INTELLIGENCE. «Hacktivists Collaborate with GRU-sponsored APT28». 23 de septiembre de 2022. Disponible en: https://www.mandiant.com/resources/blog/gru-rise-telegram-minions [consulta: 3/9/2023].
[18] TORRES SORIANO, Manuel. «Guerras por delegación en el ciberespacio», *Revista del Instituto Español de Estudios Estratégicos*, n.º 9. 2017, pp. 15-36.

Proxies *dependientes*

En segundo lugar, los *proxies* dependientes son aquellos que carecen de autonomía con respecto al Estado que los crea e instrumentaliza, sin que exista ningún interés por aparentar que estos tengan alguna suerte de independencia. Es el caso, por ejemplo, de la relación que se estableció entre el régimen de Bashar al-Assad y el llamado Syrian Electronic Army (SEA) o del IT-Army, un ciberactor creado *ad hoc* por el Gobierno ucraniano, que cuenta con una estructura definida como «una construcción híbrida que no es ni civil ni militar, ni pública ni privada, ni local ni internacional, ni legal ni ilegal»[19].

En esta misma categoría incluiríamos también a aquellos *proxies* que manifiestan una vinculación orgánica evidente con su Estado patrocinador, como el Iranian Cyber Army (IRGC), creado por la Guardia Revolucionaria y utilizado reiteradamente contra Israel[20].

Proxies *tácitos*

En tercer lugar, los *proxies* tácitos serían aquellos actores cuya supervivencia depende de la voluntad de un Estado que les cobija y les permite seguir actuando en su territorio mediante un acuerdo tácito de no agresión[21]. Un ejemplo clásico lo encontraríamos en los grupos vinculados al cibercrimen, especialmente activos en Rusia (donde antes y durante la guerra se ha demostrado que existe una interacción fluida entre cibercriminales y actores estatales).

El patrocinio de este tipo de grupos suele llevarse a cabo de manera implícita, sin necesidad de una coordinación directa, ya que el actor *proxy* entiende que la tolerancia del gobierno respecto a su actuación se mantendrá mientras que sus acciones ofensivas perjudiquen o erosionen política o económicamente a sus adversarios y se abstenga de realizar actividades ilícitas en el territorio que lo acoge.

[19] SOESANTO, 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: 27/8/2023].

[20] ADELKHAH, Nima. (2016). «Iran and Its Cyber-Terrorism Strategies», *Terrorism Monitor,* vol. 14, n.º 10. The Jamestown Foundation, 16 de mayo de 2016. Disponible en: http://www.jamestown.org/single/?tx_ttnews[tt_news]=45435&tx_ttnews[backPid]=7&cHash=fa0da141d63052f600aa6a7bffa1f625 [consulta: 20/8/2023].

[21] BORGHARD, Erica.D. y LONERGAN, Shawn W. «Can States Calculate the Risks of Using Cyber Proxies?», *Orbis,* vol. 60, n.º 3. 2016, pp. 395-416.

Proxies *autónomos*

Por último, en cuarto lugar estarían los *proxies* autónomos, actores con una identidad y una agenda propia, que no tiene por qué alinearse en la totalidad con los objetivos de los Estados patrocinadores.

Este tipo de actores *proxy* suele ser el menos común en el ciberespacio, pues su control e instrumentalización por parte del Estado resulta volátil al existir enfoques diferentes en los cursos de evolución de la consecución de objetivos.

En cualquier caso, esta tipología de ciberactores no escapa a la lógica del espectro de responsabilidad del Estado respecto de su actor *proxy*. En la siguiente tabla se observan las distintas formas en que puede implementarse la relación entre el actor patrocinador (el Estado) y el APT que actúa como *proxy*.

Tabla 1. Espectro de la responsabilidad del Estado

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

Fuente: HEALEY, Jason. «Beyond Attribution: Seeking National Responsibility for Cyber Attacks», *IssueBrief-Cyber Statecraft Initiative.* Atlantic Council, 2012. Disponible en: https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF [consulta: 1/9/2023].

Beneficios y riesgos de utilizar grupos APT como actores proxies *en el ciberespacio*

Con base en lo expuesto hasta el momento, resulta innegable la existencia de una conexión —en mayor o menor medida estrecha— entre los Estados y las APT, pero ¿cuáles son los beneficios reales que aporta a los Estados la utilización de estos grupos como *ciberproxies*?

En primer lugar, la utilización de actores *proxies* por parte de las estructuras de poder estatales reduce el riesgo de escalada de los conflictos. La dificultad para atribuir a un Estado concreto la responsabilidad de un ciberataque o de una operación de información realizada por un tercer actor es compleja. A veces el hecho de que la acción sea implementada por uno de estos actores incluso consigue engañar a las defensas del enemigo, que entiende la agresión como de menor entidad.

Recurrir a un *proxy* para llevar a cabo actividades de reconocimiento en las redes del adversario es una opción muy atractiva, pues, en caso de ser descubierta la intrusión, el Estado objetivo puede creer que carece de importancia estratégica y catalogarla como un cibercrimen más, con lo que esta se cubre con un manto de ambigüedad capaz de salvaguardar el *statu quo*.

En este sentido, los *ciberproxies* podrían llegar a configurarse como una de las herramientas predilectas en las guerras híbridas[22], en tanto que su objetivo principal de es evitar un enfrentamiento armado directo entre grandes potencias. Los *ciberproxies* no solamente permitirían alargar la situación de tensión en el conflicto, sino también desgastar a nivel social, político y económico al adversario.

En segundo lugar, esta forma de actuar de manera encubierta es precisamente otro de los beneficios de operar a través de *proxies*, ya que su utilización permite a los Estados actuar al margen de las regulaciones internas y de la crítica de sectores gubernamentales contrarios —o incluso de la propia opinión pública en las democracias—.

Un ejemplo de ello podemos encontrarlo en la compra o contratación de cibercapacidades de carácter ofensivo, ofrecidas en el mercado negro o por empresas

[22] Entendidas estas como una situación conflictiva de carácter «simultáneo y adaptativo […], una mezcla fusionada de armas convencionales, tácticas irregulares, terrorismo y comportamiento delictivo en el espacio de batalla» (HOFFMAN, Frank. *Future Hybrid Threats: An Update.* Center for Strategic Research, Washington D. C. 2012, p. 3).

privadas que plantean una serie de problemas fácilmente evitables si se actúa de forma encubierta.

Casos como los de Hacking Team o Pegasus, donde gobiernos democráticos tuvieron que lidiar con la oposición política y la opinión pública al descubrirse la compra de *softwares* para la monitorización ofensiva de comunicaciones a empresas relacionadas con regímenes dictatoriales y figuras vinculadas al crimen organizado, son ejemplos de estas problemáticas[23].

En tercer lugar, la utilización de *ciberproxies* aporta a los Estados rapidez y flexibilidad a la hora de responder a las acciones ofensivas de sus adversarios. Si un Estado es atacado y desea responder, necesitará reunir evidencias técnicas y de inteligencia que permitan una atribución sólida de la responsabilidad de cara a la legitimación interna y externa de la necesidad de una respuesta ofensiva.

Sin embargo, tal y como hemos explicado, este proceso resulta difícil y, por ende, lento. Por ello, para una mayor agilidad a la hora de articular una respuesta, los Estados pueden instrumentalizar *ciberproxies* afines para que estos respondan con celeridad contra los responsables o patrocinadores de las agresiones sufridas.

Por último, el cuarto de los beneficios se traduce en la capacidad de disuasión que los Estados pueden desplegar mediante la utilización de este tipo de grupos. Al diluirse la responsabilidad y adquirirse fuentes de negación plausibles, los Estados pueden aumentar su poder coactivo, ya que los adversarios son susceptibles de ser amenazados con sufrir actos delictivos, al no estar sujetos los *ciberproxies* a limitaciones morales o legales[24].

Además de aportar estos cuatro beneficios principales, la utilización de *ciberproxies* permite a los Estados eludir la aplicación del derecho internacional tradicional, utilizar personal experto sin necesidad de ofrecer contratación legal y participar en conflictos

[23] GARCÍA ROSADO, Silas. «Pegasus como caso de estudio: el ciberespionaje como amenaza y oportunidad», *Ejércitos.* 26 de mayo de 2022. Disponible en: https://www.revistaejercitos.com/2022/05/26/pegasus-como-caso-de-estudio/ [consulta: 2/9/2023].
[24] TORRES SORIANO, Manuel. «Guerras por delegación en el ciberespacio», *Revista del Instituto Español de Estudios Estratégicos*, n.º 9. 2017, pp. 15-36.

internacionales que en otras circunstancias resultarían económica y políticamente inabarcables[25].

No obstante, la consecución de estos beneficios no está exenta de problemáticas para los Estados. De hecho, el principal atractivo de recurrir a un *proxy,* que no es otro que obtener una negación plausible de una agresión, es también su principal debilidad.

La falta de un apoyo estatal a la agresión diluye la capacidad coactiva y disuasiva del patrocinador, ya que, de acuerdo con las teorías de Clausewitz, resulta obvio que, para que un Estado modifique su conducta según la voluntad de otro, es preciso que este sepa la procedencia del acto de coacción sufrido. Dicho de otra forma, el anonimato y la clandestinidad son un importante reductor de la potencialidad estratégica de las operaciones cibernéticas.

Por ejemplo, un ataque amparado en un anonimato absoluto que dañe los sectores críticos de un Estado o que afecte a la vida de sus ciudadanos carece de utilidad coercitiva, pues el actor atacado no conoce el origen ni la razón y, por tanto, no puede modificar su conducta en función de los intereses del agresor.

Los *ciberproxies* son útiles cuando se emplean en contextos operacionales donde existe la necesidad o el interés de mantener el control de la escalada por parte del Estado agresor. Es decir, en la zona gris de los conflictos, donde el objetivo principal es la búsqueda de logros relativos y limitados, sin cruzar la línea que provocaría un conflicto armado de carácter convencional.

Otro de los problemas de la utilización de *ciberproxies* surge de su selección y control por parte del Estado que los instrumentaliza. La existencia de intereses no compartidos entre ambas partes puede traducirse en deslealtad del *proxy* y en un daño económico o político para el actor que los emplea. Al fin y al cabo, los *ciberproxies* actúan generalmente en esferas donde el Estado no puede o no desea entrar, cuestión que dificulta la monitorización de sus acciones.

[25] MARÍN GUTIÉRREZ, Francisco. «Hacktivismo al servicio del Estado: ciberproxies en Ucrania» (Documento de Opinión IEEE, 31/2023). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO31_2023_FRAMAR_Ucrania.pdf [consulta: 18/8/2023].

El valor de los *proxies* radica en su capacidad de operar en la clandestinidad, pero esta opacidad también juega en contra del Estado patrocinador, que se ve limitado a la hora de comprobar sus antecedentes y fiabilidad.

La literatura académica coincide en señalar que, además, el control sobre los *proxies* se ve dificultado si el Estado carece de una capacidad efectiva para castigar su deslealtad o si existen estructuras descentralizadas donde no se garantice un correcto cumplimiento de las órdenes jerárquicas[26].

Valoración

Dados los beneficios enunciados y el interés de las potencias geopolíticas por no escalar conflictos tras una futura paz en Ucrania, los *proxies* podrían llegar a ser uno de los principales recursos empleados por los Estados en futuras disputas.

El creciente uso de *proxies* cibernéticos no resulta especialmente tranquilizador de cara a la seguridad mundial: de una parte, se incrementa la probabilidad de sufrir ciberataques y, de otra, los Estados pueden ejercer un frágil control sobre los integrantes del *proxy* y los medios empleados por estos[27].

En un futuro próximo podría producirse una revitalización de las zonas grises y las guerras híbridas, una vez extraídas las lecciones que la guerra de Ucrania dejará a las principales potencias mundiales y visto el desgaste económico y militar que supone una guerra convencional en pleno siglo XXI.

Sería lógico pensar en un futuro marcado por una tensión geopolítica cada vez más acuciante, sin que se llegue a superar nuevamente el umbral de la guerra abierta. Este es precisamente el escenario predilecto para que el empleo de *ciberproxies* aumente hasta convertirse en un factor de riesgo para las democracias occidentales y en un reto para la seguridad internacional, tal y como vienen prediciendo múltiples autoridades

[26] POPOVIC, Milos. (2015). «Fragile proxies: Explaining rebel defection against their state sponsors», *Terrorism and Political Violence,* vol. 29, n.º 5. 2015, pp. 922-942. DOI:10.1080/09546553.2015.1092437.
[27] MARÍN GUTIÉRREZ, Francisco. *Op. cit.*

gubernamentales a través de la Cybersecurity and Infrastructure Security Agency (CISA)[28].

*Josué Expósito Guisado**
Guardia Civil
@JosueExposito

[28] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA). «Alert AA22-110A Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure». 9 de mayo de 2022. Disponible en: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a [consulta: 27/8/2023].