REVISTA DEL INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (IEEE)

Manuel R. Torres Soriano
Profesor titular de Ciencia Política en la Universidad Pablo de Olavide de Sevilla

Correo: mrtorsor@upo.es

GUERRAS POR DELEGACIÓN EN EL CIBERESPACIO

PROXY WARS IN CYBERSPACE

Resumen

El propósito de este artículo es profundizar en las dinámicas específicas que posee el ciberespacio como escenario en el cual proyectar las llamadas guerras por delegación. Se parte de la tesis de que la principal ventaja que aporta esta estrategia (bajo riesgo de padecer la represalia por parte del actor atacado) es también su principal debilidad, ya que la participación indirecta en un ciberconflicto, resta eficacia a un Estado para que este pueda alcanzar objetivos tácticos, y tiene un valor reducido para avanzar en la consecución de objetivos estratégicos. A lo largo del trabajo se analizan las ventajas y limitaciones del uso de esta estrategia, y se propone una tipología de los diferentes ciberproxies en función de su relación con el Estado que los instrumentaliza.

Palabras Clave

Ciberespacio, conflictos, espionaje, disuasión, hacktivismo.

Abstract

The purpose of this article is to examine the specific dynamics that cyberspace has as scenario in which use proxy wars. This work support the thesis that the main advantage offered by this strategy (low risk of retaliation by the attacked actor) is also its main weakness. The indirect participation in a cyber conflict undermines the effectiveness of a State to achieve tactical objectives and strategic goals. The article analyses the advantages and limitations of using this strategy, and proposes a typology of the different cyber proxies based on their relationship to the State sponsor.

Keywords

Cyberspace, conflict, espionage, deterrence, hacktivism.

Guerras por delegación en el ciberespacio

GUERRAS POR DELEGACIÓN EN EL CIBERESPACIO

INTRODUCCIÓN

La posibilidad de impulsar los intereses estratégicos a un bajo coste, ha sido un poderoso incentivo para que, a lo largo de la historia, numerosos Estados hayan apostado por las llamadas guerras por delegación, guerras subsidiarias o *proxy wars* (del inglés). Estas han sido entendidas tradicionalmente como conflictos en los cuales una tercera parte interviene indirectamente para influenciar su resultado a favor de aquella facción, cuya victoria mejora la posición relativa de poder de su patrocinador. Esta estrategia es una opción atractiva para los países que tratan de eludir los elevados costes en términos humanos y económicos que implica la participación directa en un enfrentamiento armado.

El recurso a la guerra por delegación ha sido especialmente prevalente dentro del contexto estratégico de la Guerra Fría, donde los riesgos de una escalada nuclear convirtieron a esta opción en el recurso menos arriesgado para debilitar la posición del adversario. El fin de la hostilidad entre Bloques, no restó atractivo al enfrentamiento indirecto. El profesor británico Andrew Mumford señala[1] cuatro factores que habrían otorgado un renovado interés hacia las guerras por delegación:

a) La reticencia de la opinión pública a la hora de apoyar el uso de la guerra como instrumento para favorecer los intereses nacionales.
b) El incremento de la importancia y las capacidades de las compañías militares privadas (PMC's por sus siglas en inglés), lo que las convierte en un actor en el cual apoyarse para proyectar indirectamente los recursos de fuerza de un Estado.
c) El ascenso de China como potencia, y la necesidad de contener su influencia sin una confrontación directa y sin perjudicar la interdependencia económica existente.
d) La disponibilidad del ciberespacio como plataforma donde participar indirectamente en un conflicto.

El propósito de este artículo es profundizar en las dinámicas específicas que posee el ciberespacio como escenario en el cual proyectar las llamadas guerras por delegación. La acumulación de ciberincidentes de diferente origen y naturaleza a lo largo de la última década permite gozar de un corpus de evidencias a partir del cual trazar las primeras generalizaciones sobre las dinámicas de actuación de los actores

1 MUMFORD, Andrew. «Proxy Warfare and the Future of Conflict», *The RUSI Journal*, vol. 158, núm. 2 (2013), pp. 40-46.

que patrocinan, o participan activamente en este tipo de conflictos. Se parte de la tesis de que la principal ventaja que aporta esta estrategia (bajo riesgo de padecer la represalia por parte del actor atacado) es también su principal debilidad ya que, la participación indirecta en un ciberconflicto, resta eficacia a un Estado para que este pueda alcanzar objetivos tácticos, y tiene un valor reducido para avanzar en la consecución de objetivos estratégicos.

EXPECTATIVAS DESPROPORCIONADAS

El ciberespacio como escenario para el conflicto aparenta ser la sublimación de aquellas características que han convertido a las guerras por delegación en la opción predilecta para los actores que quieren promover sus intereses asumiendo un bajo riesgo. Por un lado, se parte de la idea de que este nuevo entorno tecnológico crea un poderoso incentivo para que las partes diriman sus disputas de manera conflictiva. Por otro lado, se presupone que el anonimato y la dificultad de atribuir responsabilidades ante un ciberataque permiten un elevado nivel de «denegación plausible». Es habitual asumir que existe una baja barrera de acceso en el ciberconflicto, debido al escaso coste económico que supondría el desarrollo de cibercapacidades. De igual modo, la ubicuidad y democratización del acceso a las nuevas tecnologías de la información habría generado un amplísimo número de actores sobre los cuales apoyarse para erosionar la posición del adversario.

A pesar de que estas visiones sobre la naturaleza del ciberespacio se encuentran sólidamente arraigadas en la opinión pública y los medios de comunicación, es preciso realizar una serie de matizaciones.

En primer lugar, cuando se habla de ciberataques, se hace un uso abusivo del término, ya que se alude de manera indistinta a acciones tan diferentes en cuanto a su viabilidad técnica e impacto, como son el espionaje, el robo de propiedad intelectual, el acoso, o provocar daños físicos contra personas o infraestructuras a través del ciberespacio.

Si bien es cierto, que el anonimato y la clandestinidad son requisitos básicos para las labores de ciberespionaje, para otro tipo de acciones puede tener un reducido o nulo valor estratégico[2]. Que un Estado padezca un ataque que dañe su economía, sus infraestructuras, o la vida de sus ciudadanos, sin que se conozca el origen del mismo, ni la razón por la cual se ha llevado a cabo, tiene una escasa utilidad coercitiva. Un anonimato absoluto, en el cual ni siquiera es posible establecer una atribución especulativa por motivaciones, puede ser más bien un problema para el atacante, que para el defensor. La tecnología no ha transformado la naturaleza política de la guerra que en su momento formuló Clausewitz: un acto de coacción dirigido hacia

2 BETZ, David. «Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed», *Journal of Strategic Studies*, vol. 35, núm. 5 (2012), pp. 689-711.

un enemigo (con independencia de con qué instrumento se proyecte) sigue siendo una acción destinada a que otro actor modifique su conducta según la voluntad de otro. El mero empleo de la violencia (física o simbólica), si no va acompañado de un significado sobre por qué se ha empleado, y cuáles son las condiciones para dejar de hacerlo, difícilmente puede contribuir a los objetivos del que lo emplea. Aunque puede argumentarse que una posible ventaja de la «violencia anónima» a través del ciberespacio, es la de degradar la economía y poder de un adversario[3], sin tener que asumir el coste de una represalia; lo cierto es que en plena globalización, el elevado grado de interrelación económica, comercial y financiera origina que el intento de alterar la balanza de poder, degradando la riqueza, conectividad o el grado de confianza con el que usa los servicios digitales un competidor, termina generando también consecuencias negativas para los intereses del atacante. En este sentido, los cibersabotajes económicos provocan un escenario de suma-negativa en el que todos los actores que participan en la economía global resultan perjudicados, y donde la única diferencia es quien soporta un perjuicio mayor.

En cuanto al aumento de la conflictividad debido a la disponibilidad de estos nuevos recursos, la evidencia empírica[4] nos muestra como los contendientes están dispuestos a tolerar la existencia de ciberagresiones aisladas, siempre y cuando no rebasen el límite de lo que se considera un acto explícito de guerra. En los numerosos conflictos interestatales ocurridos en las dos últimas décadas puede constatarse como la actitud predominante entre los actores que poseían estas capacidades, ha sido la de recurrir únicamente a operaciones de muy baja entidad, o renunciar a su uso, incluso en situaciones de guerra abierta. El riesgo de sentar un precedente[5] que anime a otros competidores a seguir esa misma vía, junto al miedo a los daños colaterales, o la pérdida de control sobre sus efectos, han seguido condicionando la estrategia de enfrentamiento. Esta es la razón, por ejemplo, por la que Estados Unidos, a pesar de contemplar su uso, renunció a emplearlas contra el sistema bancario iraquí en 2003, o contra la infraestructura de comunicaciones del régimen del coronel Gadafi en 2011[6].

3 Esta es una visión popular entre muchos analistas que consideran que actores como China se encuentran inmersos en una estrategia contra Estados Unidos que denominan «muerte por mil cortes», donde el riesgo para el país norteamericano no es un gran ataque al «estilo Pearl Harbor», sino la acción continua y silenciosa de robo de propiedad intelectual de sus empresas, lo que estaría drenando la riqueza e innovación del país hacia su competidor chino. Véase: LINDSAY, JON R. y CHEUNG, Tai Ming. «From Exploitation to Innovation. Acquisition, Absorption, and Application» en LINDSAY, JON R. China and Cybersecurity. Espionage, Strategy, and Politics the Digital Domain, Oxford: Oxford University Press, 2015.

4 VALERIANO, Brandon G. y MANESS, Ryan. «The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011», *Journal of Peace Research,* vol. 51, núm. 3 (May 2014), pp. 347-360.

5 LITWAK, Robert y KING, Meg. «Arms Control in Cyberspace?» *Wilson Briefs*, (October 2015). https://www.wilsoncenter.org/publication/arms-control-cyberspace

6 KAPLAN, Fred. Dark Territory. The secret History of Cyber War, New York: Simon & Schuster, 2016.

Esta actitud de contención también se encuentra motivada por la naturaleza operativa de las llamadas «ciberarmas», muchas de las cuales son instrumentos de un solo uso, basados en la explotación de una o varias vulnerabilidades (tanto de *software*, como en el *hardware*), que permanecen inéditas salvo para el actor que las ha descubierto, y ha sabido instrumentalizarlas. A diferencia de la mayoría de las armas convencionales, en el «ámbito ciber» no se aplica el llamado «efecto demostración», el cual lleva a un Estado a forzar el empleo de sus nuevas adquisiciones en un conflicto armado, o a mostrar su posesión en eventos públicos, para fortalecer así su carácter disuasorio ante potenciales enemigos. Por el contrario, el empleo de una ciberarma desvela la ventaja que posee el actor que la emplea, lo que provoca que las potenciales víctimas corrijan esas vulnerabilidades y tomen medidas activas para evitar un ciberataque idéntico. Esto lleva a los contendientes a dosificar el empleo de sus ciberarsenales, haciendo solamente uso en contextos donde no existe una alternativa viable, o incluso renunciando en el presente, para disponer de estas armas en un potencial conflicto de mayor calado.

Esta contención puede apreciarse incluso en actores con una mayor predisposición al uso de la fuerza. Resulta muy significativo que en el conflicto entre Rusia y Ucrania, apenas se haya producido ningún ciberataque de consideración más allá de los habituales ataques de denegación de servicio y sabotajes de páginas webs por parte de cibermilicias patrióticas y grupos de hacktivismo[7]. La anexión rusa de parte del territorio ucraniano y su intento de desestabilizar el régimen de Kiev, han sido interpretados como un ejemplo nítido de la llamada «guerra híbrida», donde el atacante hace un uso intensivo de aquellos recursos de fuerza que le permiten difuminar su responsabilidad en el desarrollo del conflicto. A pesar de que el recurso al ciberespacio encaja perfectamente en esta estrategia de ocultación, en el caso ruso ha pesado más el temor a los efectos no deseados, que las ventajas que podrían aportar su uso[8]. En palabras de un miembro de la inteligencia estadounidense, el problema de usar una ciberarma es que «una vez que ha sido desvelada, es igual que usar un avión invisible por primera vez, has hecho sonar la campana, y no puedes pretender que el avión ya no existe. La cuestión es: ¿para qué batalla aérea realmente quieres utilizar tu avión invisible?[9]».

Uno de los mitos más asentados sobre los ciberconflictos es la supuesta imposibilidad técnica de establecer el origen de un ataque, lo que habría espoleado la agresividad de un amplio número de actores amparados en el anonimato que proporciona el ciberespacio. La realidad es que aunque técnicamente resulta complejo determinar la

7 LIBICKI, Martin «The Cyber War that Wasn't», en GEERS, Kenneth (ed.) Cyber War in Perspective: Russian Aggression against Ukraine, Tallin: NATO CCD COE Publications, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf.

8 VALERIANO, Brandon G. y MANESS, Ryan. Cyberwars versus Cyber Realities. Cyber Conflict in the International System, Oxford: Oxford University Press, 2015.

9 KETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Random House, New York, 2014.

autoría de un ciberataque, no es una tarea imposible[10]. De hecho, el aspecto forense no es un elemento determinante, en ocasiones, ni siquiera el principal. La reacción contra el atacante, obedece a una lógica política[11], y por tanto, hace muy difícil que el agresor quede impune porque no ha podido demostrarse su culpabilidad de manera fehaciente, como sucedería, por ejemplo, en un proceso judicial. Es muy difícil que pueda ocultarse la autoría cuando se actúa en el marco de una rivalidad pre-existente[12]. Así, por ejemplo, cuando Corea del Sur resulta ciberatacada, es lógico que mire a su vecino del norte[13], o que cuando Georgia y Ucrania sufren un cibersabotaje sospechen de Rusia. Por tanto, es muy matizable que el uso de la ciberguerra es una actividad exenta de costes para el que la utiliza, debido a la imposibilidad de atribuir responsabilidades[14].

En cuanto al supuesto bajo coste económico de los ciberataques, se trata de una percepción errónea cuyo origen se sitúa en extender al uso bélico del ciberespacio, el *modus operandi* del cibercrimen, el cual se basa mayoritariamente, en el uso de herramientas automatizadas, baratas y fácilmente asequibles para llevar a cabo cientos de miles de ataques contra ordenadores y dispositivos con una baja o deficiente seguridad. Estos son ataques «escalables» donde el coste de la operación no se incrementa linealmente con el número de objetivos atacados, lo que permite emplear de manera indiscriminada *software* malicioso para capturar datos de las víctimas, tomar el control sobre su equipo, o simplemente plantearle una estafa. Sin embargo, en el caso del ataque contra objetivos individualizados que cuentan con una buena protección, o unas características singulares; hablamos de ataques no escalables, los cuales exigen un esfuerzo suplementario por cada unidad adicional, así como contar con recursos de inteligencia que aporten un conocimiento profundo sobre el objetivo, y la capacidad de testar el vector de ataque antes de su utilización[15].

Aunque el coste económico de la ciberguerra es muy inferior al que debería acometer un Estado para dotarse de un sistema de armas complejo; su coste no es despreciable. En un ejercicio llevado a cabo por Estados Unidos en 2002 estimó que

10 GUITTON, Clement y KORZAK, Elaine. «The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks», *The RUSI Journal*, vol. 158, núm. 4 (2013), pp. 62-68.

11 GOMPERT, David C. y LIBICKI, Martin. Waging Cyber War the American Way, *Survival: Global Politics and Strategy,* vol. 57, núm. 4 (*August–September* 2015), pp. 7-28.

12 AXELROD, Robert. «A Repertory of Cyber Analogies», en GOLDMAN, Emily O. y ARQUILLA, John (eds.) Cyber Analogies, Monterey, CA: Departament of Defense Information Operations Center for Research, 2014.

13 INKSTER, Nigel. «Cyber Attacks in La-La Land», *Survival: Global Politics and Strategy,* vol. 57, núm. 1 (February–March 2015), pp. 105-116.

14 RID, Thomas y BUCHANAN, Ben. «Attributing Cyber Attacks», *Journal of Strategic Studies*, vol. 38, núm. 1-2 (2015), pp. 4-37.

15 LINDSAY, Jon R. «Proxy Wars: Control Problems in Irregular Warfare and Cyber Operations», International Studies Association anual meeting, San Francisco, (April 2013). http://www.jonrlindsay.com/papers.

la realización de un ciberataque de gran magnitud requería de un presupuesto de 200 millones de dólares, así como un plazo de cinco años para poder implementarse[16]. A pesar de la imaginería popular, la posibilidad de tomar el control y provocar daños o un comportamiento anómalo sobre una infraestructura crítica (como pueda ser una central nuclear), empleando únicamente un ordenador conectado a Internet, es un escenario irreal. La verdadera barrera de entrada se encuentra en la capacidad de movilizar recursos de reconocimiento de objetivos, inteligencia humana y de señales, el uso de operativos sobre el terreno, equipos multidisciplinares de técnicos y expertos que cuenten con un bagaje adecuado, y poder evaluar la eficacia de la ciberarma en un entorno real, antes de proceder a su empleo. Se trata, por tanto, de requisitos que van más allá de la mera disponibilidad de recursos económicos y que desbordan las capacidades de muchos de los potenciales candidatos a ser utilizados como proxies en un ciberconflicto.

QUÉ APORTAN LOS CIBERPROXIES

A pesar de que las expectativas sobre las capacidades de los ciberproxies pueden estar sobredimensionadas, su contribución a un conflicto no es despreciable. Un actor que trate de hacer prevalecer sus intereses por esta vía, obtendrá cuatro beneficios principales:

a) *Reduce el riesgo de escalada*. Un ciberataque complejo requiere de una actividad previa de reconocimiento de las redes y servicios sobre las cuales va a actuarse. Las actividades preparatorias, son indistinguibles en un contexto operacional, de aquellas otras que tienen como único propósito el espionaje[17], lo que puede provocar una interpretación errónea de las intenciones del responsable de un acceso ilegítimo. Esta ambivalencia es peligrosa en un entorno de elevada tensión, ya que las actividades habituales de inteligencia pueden ser interpretadas como el indicador de un ataque inminente, dando lugar a respuestas desproporcionadas. El recurso a un proxy para llevar a cabo estas tareas es una opción atractiva, ya que en caso de resultar detectado, aparenta ser una intrusión menos grave, que si sus autores están vinculados orgánicamente al entramado institucional de un Estado.

b) *Incrementa la capacidad de disuasión*. Una de las cuestiones más debatidas en torno a las implicaciones estratégicas de la ciberguerra es la dificultad de

16 PURCHASE, Eric y CALDWELL, French, «Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack» en GHOSH, Sumit, MALEK, Manu y STOHR, Edward A. (coord.) Guarding Your Business: A Management Approach to Security, Nueva Yok: Springer, 2004.

17 LIN, Herbert. «Operational Considerations in Cyber Attack and Cyber Exploitation», en REVERON, Derek S. Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Washington D.C.: Georgetown University Press, 2012.

implementar la teoría clásica de la disuasión militar[18]. Aparecen interrogantes sobre cómo interpretar el requisito de proporcionalidad en la respuesta, cuando no existen ciberobjetivos similares que puedan ser represaliados, o cuando responder de manera simétrica plantea un conflicto de valores. La disponibilidad de un proxy permite al Estado ampliar el abanico de instrumentos de represalia, abarcando también aquellas acciones que no podría acometer directamente por limitaciones morales o legales. Su poder coactivo resulta reforzado cuando la instrumentalización de un proxy le permite amenazar de manera tácita con actos que se mueven en el terreno delictivo: *doxing* sobre individuos clave, exfiltración de la propiedad intelectual de las empresas de su competidor, estafas, etc.

Un ejemplo ilustrativo del papel que pueden ejercer los proxies como agentes de coacción lo podemos hallar en el ciberataque sufrido por los casinos de Sheldon Adelson[19]. Este millonario estadounidense posee una dilatada historia como defensor de las políticas del Estado de Israel. En una conferencia en una universidad neoyorkina fue preguntado por su opinión sobre el acuerdo nuclear de Estados Unidos con Irán, a lo que Anderson respondió: «*Lo que yo diría es: Escucha. ¿Ves ese desierto de ahí? Quiero mostrarte algo*». Adelson afirmó que tiraría una bomba nuclear en ese momento. «*La explosión no haría daño a nadie*» —continuó—, «*tal vez un par de serpientes de cascabel, a un escorpión o lo que sea*». Pero sí establecería una advertencia: «¿Quieren ser eliminados? Eso es lo que les diría a los mulás». El video se convirtió en un fenómeno viral en Youtube. Dos semanas después el Ayatolá Ali Khamenei, líder supremo de Irán, declaró que Estados Unidos debería «*dar un bofetón a esos charlatanes, y aplastarles la boca*». Un día después de esta declaración, las página web de la red de casinos Las Vegas Sands fue hackeada por un colectivo que se hacía llamar «**Anti WMD Team**», para que mostrase el siguiente mensaje: «Incentivar el uso de Armas de Destrucción Masiva bajo cualquier condición es un crimen». De manera paralela a este *defacement*[20] se produjo un ciberataque que destruyó veinte mil ordenadores de la red del casino, con un coste estimado de 40 millones de dólares. Los autores del ataque también enviaron a un medio de comunicación un video que mostraba contraseñas de acceso a la red de los casinos, e información sensible sobre la empresa.

18 LINDSAY, Jon R. «Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack», *Journal of Cybersecurity*, vol. 1, núm. 1 (2015), pp. 53-67. http://cybersecurity.oxfordjournals.org/content/cybers/1/1/53.full.pdf.

19 KAPLAN, Fred. Dark Territory. The secret History of Cyber War, New York: Simon & Schuster, 2016.

20 *Defacement* es una palabra inglesa traducible por «desfiguración». Dicho término se emplea en el ámbito de la informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que ha conseguido acceder de manera ilegítima a la gestión de la misma.

En el ámbito de regímenes dictatoriales, estos actores, sobre todo, si están recubiertos de la apariencia de una «milicia patriótica», también pueden emplearse para ejercer la coacción interna contra disidentes políticos y otros grupos contra los cuales se prefiere no actuar explícitamente por los perjuicios que eso puede suponer para la imagen exterior de esos gobiernos.

c) *Proporciona rapidez y flexibilidad*. La velocidad con la que un Estado responde a una ciberagresión que no afecta a los pilares básicos de su seguridad, está condicionada por la capacidad de construir «un caso» contra el responsable del ataque. Para ello, no solo deberá reunir evidencias técnicas y de inteligencia para realizar una atribución sólida de responsabilidad, sino también concienciar a la opinión pública sobre la necesidad de la respuesta. Este proceso se ve dificultado si el agresor se ha esforzado en diluir su responsabilidad utilizando, por ejemplo, un proxy para disfrutar de una negación plausible.

   Para gozar de una mayor agilidad a la hora de articular una respuesta, los Estados pueden espolear de manera activa o tácita que el espectro de ciberproxies que le son afines, tomen represalias contra los responsables o patrocinadores de las agresiones. En esa misma línea, la insistencia en los últimos años en la llamada «defensa activa» o «ciberretorsión»[21] no deja de ser un eufemismo para externalizar en empresas y otros actores privados las actividades de represalia contra los proxies utilizados por otros actores.

d) *Permite operar de manera encubierta*. Se puede recurrir a un proxy para sortear las barreras que dificultan que un Estado actúe de manera explícita en determinados ámbitos del ciberespacio. Uno de los ejemplos más significativos es el de los mercados negros de *exploits*. La cibercapacidades de un actor están directamente vinculadas a su habilidad para construir un arsenal en forma de vulnerabilidades de *software* y *hardware* que pueden ser integradas en sus operaciones en el ciberespacio. Aunque los actores más avanzados son capaces de detectar y operativizar por sus propios medios estas brechas de seguridad, lo habitual es que también recurran a los mercados no regulados de compra-venta de *exploits* para incrementar sus recursos[22]. La intervención directa de una agencia estatal sobre estos mercados no regulados o de carácter delictivo, plantea una serie de problemas que en parte pueden ser evitados si esta intervención se produce de manera encubierta. Así, por ejemplo, se plantea un dilema legal en el momento en que el Estado ha adquirido (habitualmente mediante fondos opacos[23]) una vulnerabilidad que no solo compromete la seguridad y el secreto de

21 VALLEJO, Ángel. «El avance de la ciber-retorsión», Ciber Elcano, núm. 3 (mayo 2015), pp.7-13. http://www.realinstitutoelcano.org/wps/wcm/connect/68979900485661a5a4b6b77939ebc85f/Ciber_Elcano_Num3.pdf?MOD=AJPERES&CACHEID=1431364739259.

22 HARRIS, Shane. @WAR: The Rise of the Military-Internet Complex, Boston: Mariner Books, 2015.

23 DEIBERT, Ronald J. Black Code: Inside the Battle for Cyberspace, Toronto: Signal/McClelland & Stewart, 2013.

las comunicaciones de sus adversarios, sino también de los propios ciudadanos. A pesar de ello, decide no hacer pública esta vulnerabilidad para evitar que sea «parcheada», y poder explotar en su beneficio esta ignorancia. Utilizar a un proxy como actor interpuesto, ofrece no solo capacidad de negación, sino que también ofrece ventajas adicionales como evitar una crisis de imagen cuando la existencia de las interacciones con actores de dudosa reputación queda al descubierto[24], o dificultar que los adversarios puedan elaborar una imagen veraz de las cibercapacidades que tiene a su disposición un Estado.

UNA TIPOLOGÍA DE LOS CIBERPROXIES

La naturaleza del vínculo que se establece entre un Estado y aquellos grupos que utiliza como proxies en un ciberconflicto, es esencial para entender sus dinámicas de actuación y capacidades. De ahí que a continuación se propongan la siguiente tipología:

a) *Proxies cautivos*. Se trata de aquellos actores que padecen una sólida dependencia económica o legal hacia uno o varios Estados, lo que confiere a estos últimos un claro poder para orientar sus acciones contra determinados objetivos, o para que se inhiban a la hora de actuar hacia otros. El ejemplo paradigmático de estos actores son las empresas de ciberseguridad. La militarización del ciberespacio ha forzado una transformación del entorno en el cual estas compañías prestan sus servicios. En poco tiempo, se ha pasado de un modelo de negocio donde el objetivo casi exclusivo era ofrecer soluciones de seguridad a los usuarios particulares, empresas y gobiernos frente al *software* malicioso desarrollado por individuos y grupos motivados por el lucro criminal, a un nuevo contexto donde los actores estatales son los más importantes creadores y usuarios de este tipo de código. Un responsable de ciberseguridad de la compañía estadounidense Adobe declaraba en 2011 que los adversarios que realmente le preocupan eran los «tipo portaviones»: aquellos que tenían el suficiente dinero para adquirir los *exploits* importantes hallados en sus programas y tenían los conocimientos necesarios para saber utilizarlos[25].

24 Esta es la situación que se produjo para muchos gobiernos cuando la polémica empresa italiana Hacking Team dedicada a la venta de *software* para la monitorización ofensiva de comunicaciones sufrió un hackeo que dio como resultado la publicación en internet de 400 giga-bytes de datos procedentes de la compañía, incluyendo su relación de clientes y contratos. Muchos gobiernos democráticos tuvieron que lidiar ante su opinión pública con la incómoda realidad de haber hecho negocios con una empresa que también tenían entre su lista de compradores a algunos de regímenes dictatoriales que utilizaban sus servicios para reprimir a la oposición y vulnerar los derechos humanos. Véase: KOPSTEIN, Joshua. «Meet the Companies that Helped Hacking Team Sell Tools to Repressive Governments», *Mother Board*, (July 9, 2015). https://motherboard.vice.com/read/meet-the-companies-that-helped-hacking-team-sell-tools-to-repressive-governments.

25 ZETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York: Crown, 2014.

En los últimos años, las empresas de ciberseguridad han sido clave a la hora de desvelar la existencia y supuesta autoría de algunas de las principales acciones ofensivas en el ciberespacio. Al hacerlo, estas empresas se han tenido que enfrentar al dilema ético y político de qué lealtad debe prevalecer: a sus potenciales clientes, o a los intereses nacionales de los países que las cobijan.

Estas empresas se pueden convertir en proxies por «omisión», donde la demanda por parte del Estado es que se inhiban a la hora de investigar o publicitar la autoría de determinadas operaciones que podrían en riesgo la viabilidad y éxito de estas ciberoperaciones.

Estos actores privados pueden desempeñar un papel más activo cuando deben desarrollar sus actividades en contextos donde se practica un «capitalismo de Estado», o donde resulta imposible operar sin el beneplácito de sus gobernantes (ej. China, Rusia e Irán). Los Estados pueden rentabilizar la credibilidad asociada a determinadas marcas, incentivando su acción hacia determinados objetivos, transfiriendo conocimiento, asistiéndolas técnicamente, o proporcionándoles recursos de inteligencia para que resulten exitosas a la hora de boicotear activamente las operaciones de inteligencia de sus adversarios, o debilitar su imagen internacional.

La aparente libertad de estas empresas se convierte en la pantalla que permite implementar una estrategia proactiva. Así, por ejemplo, la empresa rusa Kaspersky ha sido percibida «no solamente como una empresa de antivirus, sino como la líder en desvelar el ciberespionaje»[26], debido a su protagonismo a la hora de airear la existencia de dos de las más importantes ciberoperaciones de Estados Unidos hasta la fecha: Stuxnet y Flame. Para algunos observadores, el historial como miembro del servicio de inteligencia de la URSS de su fundador, Eugeny Kaspersky, y la interferencia permanente del Estado ruso sobre los distintos agentes económicos, lejos de ser datos irrelevantes, suponen evidencias sobre la instrumentalización geoestratégica que padecen algunas de las principales empresas del sector.

La presión que ejercen los gobiernos sobre el sector empresarial puede llevarse a cabo también por medios más sutiles, especialmente cuando se encuentran limitados por el Estado de Derecho y el refrendo democrático. Los actores estatales explotan en su beneficio la presión competitiva que existe entre las empresas del sector, así como su necesidad de añadir un elemento diferencial a sus servicios. El valor de estas empresas, en demasiadas ocasiones, guarda más relación con la alarma existente entre sus potenciales clientes y su habilidad para elaborar informes vistosos, que sobre la calidad de sus productos y su capacidad de aportar soluciones a problemas específicos. En los últimos años,

26 SHACHTMAN, Noah. «Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals», *Wired*, (June 23, 2012). http://www.wired.com/dangerroom/2012/07/ff_kaspersky/.

se ha producido una feroz competencia por desvelar nuevos casos de APT'S[27] (en la industria se bromea con la expresión: «Advanced Persistent Marketing»). Lo que les lleva a precipitar sus conclusiones basándose únicamente en indicios circunstanciales. Estas empresas suelen mostrar sus principales fortalezas en el análisis forense del *malware* detectado. Sin embargo, basar la identificación de una APT recurriendo exclusivamente a este tipo de información constituye una enorme limitación, ya que dichos indicios pueden ser ambiguos o deliberadamente engañosos.

Buena parte de los informes elaborados por estas empresas buscan un amplio impacto mediático utilizando títulos que se inspiran en la imaginería popular sobre el funcionamiento de un servicio de inteligencia. Para ello imitan supuestos códigos en clave para designar las nuevas operaciones que creen haber descubierto. Sin embargo, no es descartable que varios de estos productos estén aludiendo a los mismos responsables pero con diferentes nombres[28], que estos actores no existan como organización con identidad propia, o que sus componentes hayan fluctuado de grupo en grupo sin que conozcamos esa información.

La forma adecuada de abordar dicho sesgo es confrontar y complementar dichas conclusiones con los datos procedentes de otras fuentes de inteligencia (especialmente humanas). Sin embargo, es en esta otra dimensión del análisis donde dichas empresas muestran sus principales carencias[29]. Los Estados pueden aprovechar esta necesidad para orientar a través de las filtraciones o colaboraciones informales, el trabajo de esas empresas hacia aquellos objetivos sobre los que se desea actuar. Estos cauces informales pueden ser fundamentales para generar progresivamente un clima de opinión que fortalezca la posición del país frente a sus adversarios.

b) *Proxies dependientes*. Carecen de autonomía con respecto al Estado que los crea e instrumentaliza. Es el caso, por ejemplo, de la relación que se establece entre el régimen de Bashar al-Assad y el llamado Syrian Electronic Army (SEA), el cual se ha atribuido un amplio número de acciones de cibersabotaje hacia medios de comunicación internacionales y grupos de oposición que se manifiestan hostiles al dictador sirio.

27 Se entiende por amenaza persistente avanzada (o APT por sus siglas en inglés) a una operación compleja de infiltración cibernética dirigida contra objetivos específicos a lo largo del tiempo, y que a diferencia de las acciones automatizadas, tiene un importante componente humano, tanto en el diseño, como en la implementación de la acción.

28 SCOTT, James y SPANIEL, Drew. «Know Your Enemies 2.0», *ICIT Report* (February 2016). http://icitech.org/wp-content/uploads/2016/02/ICIT-Brief-Know-Your-Enemies-2.0.pdf.

29 LEE, Robert M. y RID, Thomas. «OMG Cyber!» *The RUSI Journal*, vol. 159, núm 5 (October-November 2014), pp. 4-12. http://www.tandfonline.com/doi/pdf/10.1080/03071847.2014.969932.

En ocasiones estos proxies no solo son creaciones *ad hoc*, sino que además el Estado manifiesta un escaso interés en aparentar que tienen una entidad propia que vaya más allá de la operación para la que fueron concebidos. Es el caso del grupo autodenominado «Espada cortante de la justicia», el cual se definía asimismo como «un grupo de hackers antiopresión», que se atribuyó en el verano de 2012 el ciberataque contra la red informática de la empresa petrolera saudí Aramco, produciendo daños en más de 30.000 ordenadores de la compañía. Este supuesto grupo carecía de una trayectoria previa o un perfil público. Su única manifestación se limitó a un escueto comunicado escrito en el portal de publicaciones anónimas Pastebin donde justifica sus acciones como una respuesta a los «crímenes y atrocidades que tienen lugar en diversos países de todo el mundo, especialmente en los países vecinos como Siria, Bahrein, Yemen, Líbano, Egipto...», los cuales eran esponsorizados, según el comunicado, con los recursos petroleros de los musulmanes[30]. Las especulaciones sobre el origen del ataque pronto se dirigieron hacia Irán[31], algo que este país, probablemente deseaba teniendo en cuenta su desidia a la hora de dotar a «Espada Cortante» de continuidad en el tiempo. Irán ya había sufrido por parte de Estados Unidos e Israel el principal ciberataque conocido hasta el momento (Stuxnet), y deseaba hacer un alarde público de sus nuevas capacidades de ciberguerra dirigiendo una acción contra su principal rival regional, y aliado de su enemigo estadounidense. A través de una acción puntual, atribuida a un proxy aparentemente independiente, y orientado el ataque hacia una empresa (y no una institución política o instalación militar), el país persa reforzaba de manera indirecta su capacidad de ciberdisuasión, evitando el riesgo de una respuesta bélica por parte del reino saudí.

En esta misma categoría también se incluyen aquellos proxies que manifiestan una vinculación orgánica más evidente con respecto a su patrocinador. Es el caso del llamado *Iranian Cyber Army*, una creación de la Guardia Revolucionaria Iraní (IRGC por sus siglas en inglés)[32], el cual se utiliza contra objetivos contra los que no existe una elevada necesidad de difuminar la responsabilidad, bien porque existe una hostilidad explícita y activa por otras vías (como es el caso de Israel), o bien porque no se teme la adopción de represalias adicionales por parte de la víctima (como es el caso de las ciberoperaciones contra el grupo terrorista Estado Islámico).

30 MCKIE, Gladys. «Cutting Sword of Justice», Cyber Threat Research (sin fecha). https://cyberthreatresearch.wordpress.com/hacktivist-groups/cutting-sword-of-justice/.

31 BRONK, Christopher y TIKK-RINGAS, Eneken. «The Cyber Attack on Saudi Aramco», *Survival*, vol. 55, núm. 2 (April 2013), pp. 81-96.

32 ADELKHAH, Nima. «Iran and Its Cyber-Terrorism Strategies», *Terrorism Monitor,* vol. 14, núm. 10 (May 16, 2016). http://www.jamestown.org/single/?tx_ttnews[tt_news]=45435&tx_ttnews[backPid]=7&cHash=fa0da141d63052f600aa6a7bffa1f625.

c) *Proxies tácitos.* Engloban a aquellos actores cuya supervivencia depende de un acuerdo tácito de no agresión por parte del Estado, en cuyo territorio se ubican sus miembros[33]. Es el caso de las organizaciones dedicadas al cibercrimen. La existencia de un vibrante sector de ciberdelincuencia transnacional puede ser un potenciador de fuerza a la hora de subcontratar ciberoperaciones. En el caso de Rusia, por ejemplo, existe una interacción fluida con estos actores, que se ve favorecida por los nexos criminales que se aprecian en los máximos niveles gubernamentales[34].

   Este tipo de patrocinio puede llevarse a cabo también de manera implícita, sin necesidad de que se produzcan canales de coordinación directos. Son supuestos donde existe un entendimiento mutuo, según el cual, el actor que actúa como proxy asume que sus acciones cuentan con la tolerancia del Estado desde el cual opera el grupo, siempre y cuando sus objetivos se limiten a perjudicar o erosionar la posición económica de sus adversarios, y se abstenga de extender sus actividades ilícitas al ámbito doméstico. Se produce una relación simbiótica entre el grupo que se enriquece a través de actividades como el fraude bancario, las estafas online, la piratería sobre la propiedad intelectual, etc., y el Estado que tolera la actividad delincuencial porque degrada la fortaleza económica de sus adversarios, al tiempo que drena su riqueza a favor de su economía doméstica, la cual se ve estimulada por la circulación del dinero obtenido de manera fraudulenta en otros países. Se trataría de una reedición 2.0 de las patentes de corso del siglo XVIII-XIX, con la diferencia de que el Estado, lejos de reconocer esa colaboración con los piratas virtuales, manifestará de manera pública su voluntad de luchar contra la ciberdelincuencia allí donde esta tenga lugar.

d) *Proxies autónomos*. Engloba a aquellos actores que tienen una identidad propia asentada y una agenda que no coincide exactamente con los intereses de los potenciales estados patrocinadores. Habitualmente son grupos cuya existencia no se limita al ámbito cibernético, sino que este es solo una más de las manifestaciones del activismo del grupo, el cual puede incluir el uso de la violencia física. Un ejemplo de esta categoría es la organización libanesa Hezbollah, la cual posee unas considerables capacidades ofensivas en el ámbito cibernético, en gran medida adquiridas por la proliferación que ha llevado a cabo Irán, para que esta milicia hostigue a Israel y a los enemigos de su aliado sirio[35]. Este tipo de actores son los que plantean más problemas para el Estado

33 BORGHARD, Erica D. y LONERGAN, Shawn W. «Can States Calculate the Risks of Using Cyber Proxies?», *Orbis*, vol. 60, núm. 3 (2016), pp. 395-416.

34 SMITH, David. «Russian Cyber Operations», *Potomac Institute for Policy Studies* (2012). http://www.potomacinstitute.org/80-potomac-institute-cyber-center/piccpublications/670-new-picc-paper-russian-cyber-operations.

35 JONES, Sam. «Cyber warfare: Iran opens a new front», *Financial Times* (April 26, 2016). http://www.ft.com/cms/s/0/15e1acf0-0a47-11e6-b0f1-61f222853ff3.html.

que trata de instrumentalizarlos, ya que la existencia de una agenda propia provoca que las relaciones con su benefactor vayan evolucionando a lo largo del conflicto, especialmente cuando el proxy es celoso de su autonomía y tiene un enfoque diferente sobre cómo debe avanzar hacia sus objetivos.

LOS PROBLEMAS DE LA DELEGACIÓN

Aunque la delegación en otros actores permite al Estado patrocinador eludir parte de las represalias, también resta efectividad a la acción de los proxies, ya que su capacidad de coacción no se puede beneficiar de la implicación directa y explícita de su benefactor. Los ciberconflictos no dejan de ser otro tipo de manifestación del ejercicio del poder estatal[36], donde se mantiene el objetivo político de forzar a otro actor a que haga, o deje de hacer algo en la línea de los propios intereses. Los ciberataques mantienen esa naturaleza política, y por tanto, la finalidad última es coaccionar tanto al adversario, como a potenciales contendientes. Sin embargo, cuanto más se presuponga la desconexión (real o simulada) de un proxy con respecto a un Estado, menor es su poder coactivo, ya que los únicos instrumentos con los que cuenta para doblegar la voluntad del atacado, son los que ha demostrado con su ciberataque, sin que pueda emplear la amenaza de una escalada empleando los recursos con los que cuenta su patrocinador.

Es el caso del llamado «Comodo Hack», donde un «hacker patriótico iraní» aseguró haberse hecho con los certificados digitales gestionados por la autoridad de certificaciones Comodo, los cuales se utilizan para autentificar servicios de correo electrónico tan populares como Google Gmail, Yahoo Mail, o Microsoft Hotmail. Esta apropiación le habría dado supuestamente la capacidad de espiar dentro de estos correos «al igual que hace Estados Unidos e Israel». El autor de este ataque se encargó a través de un comunicado de evidenciar la naturaleza política de esta acción, acusando a los gobiernos y empresas occidentales de conspirar para espiar y ciberatacar a su país. En referencia al llamado Movimiento Verde y al grupo terrorista Organización de los Muyahidines del Pueblo de Irán (MKO, por sus siglas en inglés) afirmaba que: «No voy a dejar que nadie dentro de Irán, haga daño a la gente de Irán, dañe a los científicos nucleares de mi país, dañe a mi líder (…) para esta gente, no hay privacidad en Internet, no tienen seguridad en el mundo digital»[37]. Sin embargo, dentro de ese mismo comunicado hacía hincapié en el carácter individual de esta acción, afirmando que se trataba de un «programador de 21 años» que carecía de vinculación con ningún grupo. Su énfasis, en el carácter individual de este ataque restó contundencia a

36 BETZ, David y STEVENS, Tim. «Power and cyberspace», *Adelphi Series*, Vol. 51, núm. 424 (2011), pp. 9-34.

37 BRIGHT, Peter. «Independent Iranian Hacker Claims Responsibility for Comodo Hack», *Wired* (March 28, 2011). http://www.wired.com/threatlevel/2011/03/comodo_hack/.

sus amenazas, como demuestra el hecho de que dicha acción no produjo ninguna modificación en el comportamiento de sus destinatarios.

Incluso cuando un ciberataque se utiliza como herramienta de presión para conseguir objetivos muy específicos, y la presunción de respaldo estatal es elevada, tampoco se garantiza el éxito. Es el caso del incidente sufrido por la productora cinematográfica Sony en las navidades de 2014, cuando fue víctima de un chantaje para evitar la distribución pública de la comedia «The Interview». La cinta, en la cual se parodia al presidente de Corea del Norte, había sido definida por el portavoz de Exteriores de este país como «un actor de terrorismo», anunciando «represalias sin compasión»[38] si la película era proyectada.

Unas semanas antes de su pase en cines, Sony padeció un ciberataque consistente en el robo del contenido de los correos electrónicos de todos sus empleados, así como de la apropiación de la copia de cinco películas inéditas o recién estrenadas. Toda esa información fue filtrada a Internet, ocasionando un daño económico a la empresa por la distribución ilegal de las cintas valorado en 17 millones de dólares[39], así como a la reputación de la empresa, por el contenido de algunos de esos correos que mostraban expresiones denigrantes contra actores y otros miembros de la industria audiovisual americana.

El robo de datos fue reivindicado por un grupo que se hacía llamar «Guardianes de la Paz», el cual trasladó sus amenazas más allá del ámbito cibernético, anunciando atentados contra las salas de cine que proyectasen la película. La *premier* de la película fue cancelada por la empresa, lo que provocó un notorio malestar, no solo entre actores que denunciaron el mal ejemplo que Sony estaba dando ante el chantaje, sino incluso la involucración del presidente Obama que lamentó que se atendiese las demandas de los atacantes. La empresa reconsideró su decisión inicial, y decidió proyectar la película en un número menor de salas de cine «seleccionadas», así como su distribución simultánea a través de Internet.

Como resultado final de este episodio, la película no solo se hizo pública, sino que posiblemente alcanzó una difusión mayor a la prevista originalmente debido al elevado interés público generado por esta polémica producción, la cual había sido capaz de provocar la furia del dictador. Corea del Norte, no tuvo mayor interés en disociarse de esta acción, sin embargo, todo el mundo asumió que Corea del Norte no materializaría en última instancia las amenazas lanzadas por los «Guardianes», ya que eso supondría forzar un acto de guerra contra Estados Unidos.

38 BBC. «The Interview: A guide to the cyber attack on Hollywood», *BBC News* (December 29, 2014). http://www.bbc.com/news/entertainment-arts-30512032.

39 RUSHE, Dominic. «The Interview revenge hack cost Sony just $15m», *The Guardian* (February 4, 2015), http://www.theguardian.com/film/2015/feb/04/guardians-peace-revenge-hack-sony-finances-unscathed.

Otro de los problemas de los ciberconflictos por delegación, son los riesgos asociados a la selección y control de los proxies. Las preferencias de estos pueden variar notablemente con respecto al patrocinador. Algunos de ellos son desleales con el paso del tiempo, y otros lo son desde el principio. La literatura académica[40] señala, por ejemplo, que el control sobre estos actores se ve enormemente dificultado si el Estado carece de capacidad efectiva para castigar las transgresiones de sus socios, o si estos poseen una estructura descentralizada que no garantiza el correcto cumplimiento de las órdenes que emanan de sus líderes.

En el ámbito ciber, encontramos además otras particularidades. Estos actores actúan en ocasiones en áreas que el patrocinador no puede, o no desea alcanzar, lo que plantea el problema de cómo monitorizar sus acciones en un entorno que permanecen opaco al control estatal. La correcta selección de estos activos se ve dificultada por las limitaciones existentes a la hora de poder chequear sus antecedentes, y fiabilidad, debido a que una de las características que los convierten en útiles, es precisamente su capacidad de operar en la clandestinidad.

El riesgo de una mala elección también reside en la incapacidad de verificar si el proxy tiene la destreza necesaria para culminar con éxito la misión que se la ha encomendado. Un «socio» incompetente puede comprometer la coartada de su patrocinador, sobre todo si la viabilidad de la operación depende del factor sorpresa, o de la capacidad de implementarla sin dejar tras de sí un rastro incriminatorio. Esta mala praxis, puede incluso encontrarse en el ámbito institucional, donde es esperable un mayor nivel de profesionalidad. Así, por ejemplo, la empresa de ciberseguridad Madiant[41] fue capaz de atribuir a la llamada Unidad 61398 del ejército chino, la responsabilidad en el ciberespionaje sobre 141 organizaciones de todo el mundo, basándose en las deficientes prácticas de seguridad operativa que emplearon los hacker chinos. En la preparación e implementación de la operación emplearon no solo servidores de prueba ubicados en su país, direcciones IP, números de teléfono y teclados chinos, sino que también se comunicaron entre ellos empleando expresiones coloquiales chinas, y reutilizaron sus pseudónimos personales, los cuales habían sido empleados en el pasado para participar en foros de Internet, páginas de empleo, etc. donde se aportaban fotografías y datos identificativos de sus propietarios.

Otro error habitual de un ciberproxy incompetente consiste en emplear código desarrollado de manera prematura, el cual suele presentar errores que lo hacen fracasar cuando se emplea en un contexto real, o que generan efectos no deseados, o contraproducentes. También existe el riesgo de causar «bajas colaterales», extendiendo el conflicto hacia otros actores, o perjudicando la imagen del patrocinador.

40 POPOVIC, Milos (2015). «Fragile proxies: Explaining rebel defection against their state sponsors», *Terrorism and Political Violence*, (2015) DOI: 10.1080/09546553.2015.1092437.

41 MADIANT. «APT1: Exposing One of China's Cyber Espionage Units», Mandiant Intelligence Center (2013). http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

CONCLUSIONES

Un simple repaso por los diferentes episodios de conflictos por delegación en el ciberespacio nos muestra la reducida eficacia de esta estrategia para alcanzar objetivos de carácter estratégico. El principal atractivo de recurrir a un proxy (obtener una negación plausible cuando se agrede a un enemigo), es también su principal debilidad. La falta de respaldo estatal diluye gran parte del poder coactivo que podría tener este tipo de acciones.

Los ciberproxies muestran claramente su utilidad cuando se emplean en contextos operacionales donde existe una clara necesidad de obscurecer la autoría estatal, como por ejemplo, los actos de naturaleza eminentemente delincuencial o de espionaje.

A pesar de que las acciones de este tipo de actores se han movido técnicamente en las capas más superficiales de la llamada ciberguerra, es precipitado dictaminar que los proxies están llamados a desempeñar un papel marginal en los ciberconflictos venideros. Aunque en la última década se ha producido un crecimiento exponencial del número de ciberincidentes relacionados con rivalidades estatales, aún nos encontramos en un contexto experimental donde los Estados todavía no han madurado sus doctrinas de actuación en este nuevo escenario tecnológico. Muchos de estos incidentes tienen el carácter de indagaciones, donde a través de un proceso de ensayo-error los Estados aprenden sobre los efectos del empleo de estos recursos, la respuesta de sus adversarios, así como su potencial integración en ofensivas que vayan más allá del ámbito virtual.

De la misma manera, tampoco puede descartarse que mucha de esta conflictividad de baja intensidad tenga como objeto crear un bagaje operativo y una credibilidad contrastada para los mismos proxies que hasta el momento han sido poco eficaces por no contar con estos avales. Que estos grupos mantengan un nivel de actividad, aparentemente desconectada de los intereses de ningún país, contribuye a reforzar la coartada con la que cuenta el Estado en el momento en que decida alinearlos a su favor. En un entorno de gran incertidumbre, estos actores permiten que algunos estados puedan adentrarse en el ámbito de los ciberconflictos para otear sus posibilidades sin un excesivo riesgo. En este sentido, los proxies pueden asumir la función de iniciar y sostener en una baja intensidad ciberconflictos que serán asumidos y potenciados en el futuro por las propias capacidades del Estado en un contexto que le resulte más favorable.

BIBLIOGRAFÍA

ADELKHAH, Nima. «Iran and Its Cyber-Terrorism Strategies», *Terrorism Monitor,* vol. 14, núm. 10 (May 16, 2016), http://www.jamestown.org/single/?tx_ttnews[tt_news]=45435&tx_ttnews[backPid]=7&cHash=fa0da141d63052f600aa6a7bffa1f625.

BBC. «The Interview: A guide to the cyber attack on Hollywood», *BBC News* (December 29, 2014). http://www.bbc.com/news/entertainment-arts-30512032.

BETZ, David y STEVENS, Tim. «Power and cyberspace», *Adelphi Series*, Vol. 51, núm. 424 (2011), pp. 9-34.

BETZ, David. «Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed», *Journal of Strategic Studies*, vol. 35, núm. 5 (2012), pp. 689-711.

BORGHARD, Erica D. y LONERGAN, Shawn W. «Can States Calculate the Risks of Using Cyber Proxies?», *Orbis*, vol. 60, núm, 3 (2016), pp. 395-416.

BRIGHT, Peter. «Independent Iranian Hacker Claims Responsibility for Comodo Hack», *Wired* (March 28, 2011). http://www.wired.com/threatlevel/2011/03/comodo_hack/.

BRONK, Christopher y TIKK-RINGAS, Eneken. «The Cyber Attack on Saudi Aramco», *Survival*, vol. 55, núm. 2 (April 2013), pp. 81-96.

DEIBERT, Ronald J. Black Code: Inside the Battle for Cyberspace, Toronto: Signal/McClelland & Stewart, 2013.

GEERS, Kenneth (ed.) Cyber War in Perspective: Russian Aggression against Ukraine, Tallin*:* NATO CCD COE Publications, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf.

GHOSH, Sumit, MALEK, Manu y STOHR, Edward A. (coord.) Guarding Your Business: A Management Approach to Security, Nueva Yok: Springer, 2004.

GOLDMAN, Emily O. y ARQUILLA, John (eds.) Cyber Analogies, Monterey, CA: Departament of Defense Information Operations Center for Research, 2014.

GOMPERT, David C. y LIBICKI, Martin. Waging Cyber War the American Way, *Survival: Global Politics and Strategy, vol. 57, núm. 4 (*August-September *2015), pp. 7-28.*

GUITTON, Clement y KORZAK, Elaine. «The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks», *The RUSI Journal*, vol. 158, núm. 4 (2013), pp. 62-68.

HARRIS, Shane. @WAR: The Rise of the Military-Internet Complex, Boston: Mariner Books, 2015.

INKSTER, Nigel. «Cyber Attacks in La-La Land», *Survival: Global Politics and Strategy, vol. 57, núm. 1 (*February-March 2015), pp. 105-116.

JONES, Sam. «Cyber warfare: Iran opens a new front», *Financial Times* (April 26, 2016). http://www.ft.com/cms/s/0/15e1acf0-0a47-11e6-b0f1-61f222853ff3.html.

KAPLAN, Fred. Dark Territory. The secret History of Cyber War, New York: Simon & Schuster, 2016.

KETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Random House, New York, 2014.

KOPSTEIN, Joshua. «Meet the Companies that Helped Hacking Team Sell Tools to Repressive Governments», *Mother Board*, (July 9, 2015), https://motherboard.vice.com/read/meet-the-companies-that-helped-hacking-team-sell-tools-to-repressive-governments.

LEE, Robert M. y RID, Thomas. «OMG Cyber!» *The RUSI Journal*, vol. 159, núm 5 (October-November 2014), pp. 4-12. http://www.tandfonline.com/doi/pdf/10.1080/03071847.2014.969932.

LINDSAY, Jon R. «Proxy Wars: Control Problems in Irregular Warfare and Cyber Operations», International Studies Association anual meeting, San Francisco, (April 2013). http://www.jonrlindsay.com/papers.

LINDSAY, Jon R. «Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack», *Journal of Cybersecurity*, vol. 1, núm. 1 (2015), pp. 53-67. http://cybersecurity.oxfordjournals.org/content/cybers/1/1/53.full.pdf.

LINDSAY, JON R. China and Cybersecurity. Espionage, Strategy, and Politics the Digital Domain, Oxford: Oxford University Press, 2015.

LITWAK, Robert y KING, Meg. «Arms Control in Cyberspace?» *Wilson Briefs*, (October 2015). https://www.wilsoncenter.org/publication/arms-control-cyberspace.

MANDIANT. «APT1: Exposing One of China's Cyber Espionage Units», Mandiant Intelligence Center (2013). http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

MCKIE, Gladys. «Cutting Sword of Justice», Cyber Threat Research (sin fecha). https://cyberthreatresearch.wordpress.com/hacktivist-groups/cutting-sword-of-justice/

MUMFORD, Andrew. «Proxy Warfare and the Future of Conflict», *The RUSI Journal*, vol. 158, núm. 2 (2013), pp. 40-46.

REVERON, Derek S. Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Washington D.C.: Georgetown University Press, 2012.

RID, Thomas y BUCHANAN, Ben. «Attributing Cyber Attacks», *Journal of Strategic Studies*, vol. 38, núm. 1-2 (2015), pp. 4-37.

RUSHE, Dominic. «The Interview revenge hack cost Sony just $15m», *The Guardian* (February 4, 2015) http://www.theguardian.com/film/2015/feb/04/guardians-peace-revenge-hack-sony-finances-unscathed.

SCOTT, James y SPANIEL, Drew. «Know Your Enemies 2.0», *ICIT Report* (February 2016). http://icitech.org/wp-content/uploads/2016/02/ICIT-Brief-Know-Your-Enemies-2.0.pdf.

SHACHTMAN, Noah. «Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals», *Wired*, (June 23, 2012). http://www.wired.com/dangerroom/2012/07/ff_kaspersky/.

SMITH, David. «Russian Cyber Operations», *Potomac Institute for Policy Studies* (2012). http://www.potomacinstitute.org/80-potomac-institute-cyber-center/piccpublications/670-new-picc-paper-russian-cyber-operations.

VALERIANO, Brandon G. y MANESS, Ryan. «The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011», *Journal of Peace Research,* vol. 51, núm. 3 (May 2014), pp. 347-360.

VALERIANO, Brandon G. y MANESS, Ryan. Cyberwars versus Cyber Realities. Cyber Conflict in the International System, Oxford: Oxford University Press, 2015.

VALLEJO, Ángel. «Elavancedelaciber-retorsión», CiberElcano, núm. 3 (mayo 2015), pp. 7-13. http://www.realinstitutoelcano.org/wps/wcm/connect/68979900485661a5a4b6b77939ebc85f/Ciber_Elcano_Num3.pdf?MOD=AJPERES&CACHEID=1431364739259.

ZETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York: Crown, 2014.

Artículo recibido: 5 de septiembre de 2016.
Artículo aceptado: 19 de diciembre de 2016.