Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Artículo de Investigación

HACKTIVISMO: DE LA PROTESTA SOCIAL A LA INSTRUMENTALIZACIÓN ESTATAL

Josué Expósito Guisado
Sargento de la Guardia Civil
Doctorando en la Universidad Pablo de Olavide
Máster en Paz, Seguridad y Defensa por el
Instituto Universitario Gutiérrez Mellado (UNED)
jexpgui@gmail.com
ORCID: 0009-0003-4977-3899

Recibido 18/03/2025
Aceptado 05/05/2025
Publicado 27/06/2025

Cita recomendada: Expósito, J. (2025). Hacktivismo: de la protesta social a la instrumentalización estatal. *Revista Logos Guardia Civil*, 3(2), pp. 101-122.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

ORCID: 0009-0003-4977-3899

HACKTIVISMO: DE LA PROTESTA SOCIAL A LA INSTRUMENTALIZACIÓN ESTATAL

Resumen: El hacktivismo ha evolucionado desde una forma inicial de protesta digital hasta convertirse en una herramienta clave en los conflictos geopolíticos contemporáneos. Lo que comenzó como un movimiento descentralizado en defensa de la libertad de expresión y la justicia social, ha sido progresivamente instrumentalizado por los Estados para ejecutar ciberataques, manipular la opinión pública y desplegar operaciones de desinformación. Un fenómeno que se ha visto especialmente acentuado en el marco de la guerra de Ucrania, donde la convergencia entre grupos de Amenaza Persistente Avanzada (APT) y hacktivistas patrióticos ha permitido la ejecución de operaciones cibernéticas coordinadas con los intereses estatales. Paralelamente, la internacionalización del hacktivismo ha llevado a la formación de alianzas entre grupos de distintas regiones, ampliando su impacto más allá del conflicto ruso-ucraniano. El ciberespacio se ha consolidado como un escenario idóneo para la confrontación entre Estados en un entorno controlado. Sin embargo, la creciente sofisticación de los ataques y la selección de objetivos cada vez más estratégicos plantean serios desafíos a la estabilidad internacional y la seguridad de los Estados occidentales.

Abstract: Hacktivism has evolved from an initial form of digital protest into a key tool in contemporary geopolitical conflicts. What began as a decentralized movement advocating for freedom of expression and social justice has been progressively instrumentalized by states to conduct cyberattacks, manipulate public opinion, and deploy disinformation operations. This phenomenon has been particularly pronounced in the context of the war in Ukraine, where the convergence between Advanced Persistent Threat (APT) groups and patriotic hacktivists has enabled the execution of cyber operations aligned with state interests. At the same time, the internationalization of hacktivism has led to the formation of alliances between groups from different regions, expanding its impact beyond the Russia-Ukraine conflict. Cyberspace has become an ideal battleground for controlled confrontation between states. However, the increasing sophistication of attacks and the selection of increasingly strategic targets pose serious challenges to international stability and the security of Western states.

Palabras clave: Hacktivismo, APT, ciberproxies, ciberconflicto, ciberataques.

Keywords: *Hacktivism*, APT, *cyberproxies*, *cyberconflict*, *cyberattacks*.

ABREVIATURAS

APT: Amenaza Persistente Avanzada. (*Advanced Persistent Threat*).

DDoS: Ataque de Denegación de Servicio Distribuido. (*Distributed Denial of Service*).

DOJ: Departamento de Justicia de EE.UU. (*Department of Justice*).

FBI: Buró Federal de Investigaciones. (*Federal Bureau of Investigation*).

GRU: Dirección Principal de Inteligencia de Rusia. (*Glavnoe Razvedyvatel'noe Upravlenie*).

ICS: Sistemas de Control Industrial. (*Industrial Control Systems*).

IRGC: Cuerpo de la Guardia Revolucionaria Islámica de Irán. (*Islamic Revolutionary Guard Corps*).

IT Army of Ukraine: Ejército Informático de Ucrania.

NSA: Agencia de Seguridad Nacional de EE.UU. (*National Security Agency*).

PMC: Empresa Militar Privada. (*Private Military Company*).

PSOA: Actor Ofensivo del Sector Privado. (*Private Sector Offensive Actor*)

SCADA: Control Supervisor y Adquisición de Datos (*Supervisory Control And Data Acquisition*).

Stuxnet: Nombre del *malware* usado en la operación "Olympic Games".

1. INTRODUCCIÓN

La guerra de Ucrania ha supuesto para el mundo occidental enfrentar nuevamente el impacto del realismo político. Antes de la invasión de 2022, la inmensa mayoría de analistas occidentales eran incapaces de vislumbrar en el panorama internacional un conflicto convencional como el que sigue ocurriendo a las puertas de Europa. Cegados por unas doctrinas centradas en el poder blando y siguiendo los paradigmas liberales de la teoría de la paz capitalista o paz comercial, los dirigentes europeos obviaron voluntariamente que, en algunas zonas del mundo, el realismo político sigue imperando.

En un mundo cada vez más digitalizado, donde prácticamente existe una interconexión entre el plano intangible de la informática y el propio espacio físico, no es de extrañar que el actual enemigo de Europa suponga un desafío para la seguridad. A medida que los Estados han aumentado su dependencia de las tecnologías de la información, también han crecido las oportunidades para que actores hostiles (estatales y no estatales) puedan influir en el entorno político y geopolítico mediante el despliegue de acciones en el ciberespacio.

La guerra de Ucrania ha supuesto, no solamente el inicio de una operación de hostigamiento y perturbación cibernética por parte de ciberamenazas vinculadas al Kremlin, sino que también ha provocado un cambio en el panorama hacktivista mundial: lo que hasta hace no tantos años fue el baluarte de la defensa de la libertad de expresión, la privacidad, la justicia social y los derechos humanos, hoy es un instrumento con implicaciones estratégicas y, en muchos casos, vinculado directa o indirectamente con gobiernos y servicios de inteligencia.

El activismo digital con fines ideológicos y de protesta que representaba Anonymous se encuentra en un proceso de evolución hacia un fenómeno conformado por un sinfín de grupos nacionalistas que utilizan de forma reiterada ataques de denegación de servicio distribuido (DDoS) con el objetivo de crear un clima de tensión y de acoso persistente en los enemigos occidentales.

El hacktivismo se ha convertido en una herramienta de doble filo. Por un lado, representa una forma de expresión y lucha por la justicia social, la transparencia y los derechos humanos. Por otro, se ha transformado en un arma utilizada por los Estados para desplegar campañas de desestabilización política y de desinformación.

El empleo de ciberataques con fines geopolíticos ha puesto de manifiesto la delgada línea que existe entre el activismo y el cibercrimen patrocinado por Estados. Este artículo busca analizar la evolución del hacktivismo y su relación con los gobiernos, así como el papel de los grupos de Amenaza Persistente Avanzada (APT) en el uso del ciberespacio con fines políticos y militares[1].

[1] Grupos de ciberatacantes frecuentemente asociados a Estados-nación o grandes organizaciones criminales, altamente sofisticados y persistentes que infiltran redes durante largos períodos para espionaje o sabotaje y que cuentan con recursos abundantes (técnicos, económicos) para atacar objetivos de alto valor (gobiernos, grandes empresas) con premeditación y sigilo.

A través de una revisión de casos concretos, se explorará la colaboración (o instrumentalización) de los hacktivistas por parte de los Estados, las implicaciones de esta práctica y su impacto en la geopolítica actual. Finalmente, se ofrecerá una reflexión sobre el futuro del hacktivismo en un mundo cada vez más interconectado, donde la inteligencia artificial y otras tecnologías emergentes podrían redefinir el papel de estos actores en el ciberespacio.

El hacktivismo ya no es solo un fenómeno marginal de protesta digital, sino un riesgo potencial para la seguridad de los Estados. Comprender su evolución y sus implicaciones resulta fundamental para analizar el futuro de la ciberseguridad española.

2. DE LA PROTESTA SOCIAL A LA CIBERGUERRA

El hacktivismo ha experimentado una notable transformación desde sus orígenes, pasando de ser una forma de protesta social a una herramienta utilizada por los gobiernos para sustentar una agenda política. Si lo pensamos detenidamente, esta transformación traiciona los orígenes y la esencia misma del activismo, por ello, antes de analizar el papel que juega el hacktivismo como herramienta al servicio del Estado, creemos necesario observar el recorrido que ha tenido este fenómeno desde sus orígenes.

En ciertos enfoques contemporáneos, particularmente aquellos orientados a la sistematización terminológica, se tiende a establecer una relación jerárquica entre el ciberactivismo y el hacktivismo, entendiendo al primero como un fenómeno más amplio y que necesariamente abarca al segundo como una manifestación específica o una variante radicalizada. Esta lectura, presente tanto en literatura divulgativa como en algunos marcos analíticos normativos, considera que el ciberactivismo representa la utilización de las tecnologías digitales para la promoción de causas sociales, políticas o culturales mediante campañas de sensibilización, peticiones en línea o protestas virtuales. Por su parte, el hacktivismo se caracterizaría por el uso de herramientas propias del hacking —como los ataques distribuidos de denegación de servicio (DDoS), las filtraciones de datos o la alteración de sitios web— con fines similares, aunque por medios más disruptivos o incluso ilícitos.

Sin embargo, esta interpretación, aunque extendida, resulta problemáticamente reduccionista y no resiste un escrutinio más profundo desde la historia ni desde la teoría crítica de los movimientos digitales. En primer lugar, la suposición de una evolución lineal y progresiva —del ciberactivismo “moderado” al hacktivismo “radical”— ignora las trayectorias históricas diferenciadas de ambos conceptos. El hacktivismo, lejos de ser una derivación tardía del ciberactivismo, emerge de forma simultánea e incluso anterior en determinados contextos, enraizado en la cultura hacker de las décadas de 1980 y 1990, y articulado en torno a principios como la libertad de información, el acceso abierto al conocimiento y la desobediencia civil en el ciberespacio (Jordan & Taylor, 2004; Coleman, 2014).

De hecho, el término "hacktivismo" surge de la combinación etimológica de "hacker" y "activismo", describiendo el uso de habilidades informáticas para promover causas políticas o sociales; y sus raíces se remontan a mediados de la década de 1990, cuando grupos como “*Cult of the Dead Cow*” (La Secta de la Vaca Muerta, en referencia al matadero texano donde el grupo realiza sus reuniones) defendían el acceso universal a

la información en línea como un derecho humano fundamental y la lucha contra los gobiernos opresivos[2].

"Cult of the Dead Cow", considerado uno de los fundadores del hacktivismo moderno, no solo difundía manifiestos críticos sobre el control estatal y corporativo de Internet, sino que también desarrolló herramientas con una clara vocación disruptiva. Entre ellas destaca *Back Orifice* (1998), un software diseñado para exponer las vulnerabilidades del sistema operativo Windows y denunciar las deficiencias en la privacidad de los usuarios[3]. Un año más tarde, en 1999, varios miembros de sus miembros impulsaron el proyecto *Hacktivismo*, una rama explícitamente orientada a la lucha contra la censura digital que dio lugar al desarrollo de herramientas como *Six/Four* o *Peekabooty*, diseñadas para sortear los filtros impuestos por regímenes autoritarios y facilitar el acceso libre a la información.

En el ideario de *Cult of the Dead Cow*, el acceso a la información en línea no solo constituía un derecho fundamental, sino también un campo de disputa política que exigía formas innovadoras de intervención técnica y simbólica. Sin embargo, estas acciones, si bien no eran violentas en términos físicos, implicaban una confrontación directa con las legislaciones restrictivas sobre uso de redes y propiedad intelectual; o, dicho de otra forma, revelaban el carácter ambiguo del hacktivismo.

Por otra parte, conceptualizar el hacktivismo como una simple intensificación táctica del ciberactivismo nos hace perder de vista las divergencias ideológicas y epistemológicas entre ambos. Mientras que el ciberactivismo suele enmarcarse en lógicas de participación ciudadana, incidencia institucional y utilización estratégica de los medios sociales, el hacktivismo opera muchas veces desde el antagonismo directo, la resistencia a las estructuras de poder y el cuestionamiento de los marcos legales vigentes.

Si bien pensar que el hacktivismo constituye una subcategoría del ciberactivismo puede ser útil desde ciertas aproximaciones descriptivas, resulta epistemológicamente insuficiente y empíricamente cuestionable cuando se aborda la genealogía, el marco normativo y las implicaciones ético-políticas de ambas formas de activismo digital. En el presente artículo nos centraremos únicamente en la evolución del hacktivismo, entendido como fenómeno propio, y dejando al margen la formulación de una revisión crítica de esta clasificación.

En los primeros estadios del hacktivismo, el objetivo principal era la realización de ataques contra entidades gubernamentales y corporativas como forma de protesta frente a la censura y las injusticias sociales. Unos mensajes que se fueron recrudeciendo conforme el movimiento antiglobalización de mediados de los noventa emergía en el panorama social (Auty, 2004).

Un hito clave en la consolidación del hacktivismo como herramienta de confrontación política fue la guerra de Kosovo en la década de 1990 (a menudo descrita como la primera guerra librada en línea), donde los contendientes no solo compartían

---

[2] La web de "The Cult of the Dead Cow" a día de hoy aún puede ser consultada en: https://cultdeadcow.com/about.html

[3] Si bien inicialmente fue concebida como una herramienta de auditoría de seguridad, su creación generó cierta controversia y se percibió como una amenaza por la industria tecnológica.

información y testimonios sobre la guerra a través de la red, sino que también difundían propaganda y desinformación. E incluso, surgieron *hackers* que intervinieron activamente en el conflicto desfigurando sitios web gubernamentales y ejecutando ataques de denegación de servicio contra infraestructuras en línea del bando contrario (Denning, 2001).

Académica y socialmente, los movimientos hacktivistas se percibían como la expresión natural de un activismo político preexistente que había sabido encontrar en una nueva herramienta (Internet) la posibilidad de emplear a un tipo de activista con perfil técnico en la expansión de sus mensajes de una forma más mediática (Jordan, 2002).

Sin embargo, el desprecio manifiesto hacia las normas establecidas, los nombres escogidos por los grupos (*The Legion of Doom, Bad Ass Mother Fuckers, Toxic Shock*, etc.) y el contexto de inseguridad social que abrió los atentados del 11-S, hicieron que un fenómeno que inicialmente se percibía positivamente comenzara a suscitar cierta desconfianza. (Torres Soriano, 2018).

La figura del *hacker* comenzó a identificarse con la del criminal, y por extensión, en un contexto geopolítico marcado por la lucha contra el Terror, con la del ciberterrorista. Y las acciones hacktivistas comenzaron a identificarse básicamente como una nueva forma de participación política ilegítima, que empleaba los ciberataques para realizar sabotajes y ciberespionaje (Vegh, 2005).

A nivel académico, la identificación del hacktivismo con lo ilegal o lo criminalizable, frecuente en ciertos discursos, reduce el hacktivismo a una "forma radical de ciberactivismo", y con ello empobrece el análisis y la capacidad explicativa de las ciencias sociales ante la complejidad de las prácticas políticas digitales contemporáneas.

Los inicios de esta década reflejan un hacktivismo marcado por el deseo de sus miembros de transgredir las convenciones sociales por pura diversión. De hecho, las raíces del grupo hacktivista más conocido (Anonymous) se remontan al foro japonés *2chan*, donde la comunidad virtual se dedicaba a compartir todo tipo de contenidos aberrantes relacionados con el anime, el porno y las bromas pesadas (Bartlett, 2015).

Sin embargo, en torno al año 2003, se originan las primeras tensiones internas en una comunidad virtual que había encontrado en el foro *4chan* un espacio ideal para divertirse sin importar las consecuencias. Precisamente, en este foro, algunos usuarios (conocidos como *moralfags*) proponen enfocar sus actividades hacia causas más trascendentales como la lucha contra la censura en Internet, para lavar la imagen del hacktivismo y representar la defensa de la libertad de expresión, la transparencia y otros derechos civiles.

Bajo el lema "*We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us*." y la máscara de Guy Fawkes, surge un colectivo descentralizado de activistas que combinaban la exfiltración de información y los ataques DDoS para reivindicar la lucha contra la corrupción, la censura y los abusos de poder.

Desde el poder, rápidamente Anonymous fue interpretado como una premonición del riesgo que suponía una nueva generación de actores virtuales motivados, con una estructura sin liderazgo y un funcionamiento basado en la voluntariedad y la

espontaneidad (Olson, 2012). Sin embargo, no fue hasta que el colectivo comenzó a apoyar las acciones de WikiLeaks, cuando el grupo fue percibido como una ciberamenaza de primer nivel.

En poco tiempo, Anonymous pasó de ser un pequeño grupo de *hackers* con inquietudes políticas a convertirse en un movimiento global con miles de seguidores distribuidos por todo el mundo. No obstante, su atractivo no radicaba en una ideología estructurada o en un programa de acción definido. Más allá de su postura antisistema, que los llevó a denunciar la manipulación y el control ejercido por gobiernos y corporaciones, su filosofía carecía de una orientación clara sobre cómo debían organizarse la política, la sociedad o la economía. Esto convirtió a Anonymous en un fenómeno difícil de encasillar, ya que su identidad se basaba más en la acción y la protesta que en una agenda concreta de cambio (Torres Soriano, 2018).

Bajo la máscara de Guy Fawkes se congregaron individuos que ciertamente creían que apoyaban un cambio social positivo, pero también otros: aquellos cuya inspiración era la destrucción nihilista del mundo tal y como lo conocemos y quienes buscaban ocultarse bajo la bandera de Anonymous para obtener un beneficio político o económico.

Del principal legado de Anonymous (el convertir al hacktivismo en una práctica popular que trascendió el ámbito *hacker*) surge una nueva era de hacktivistas que operan en un panorama de fragmentación y complejidad, donde conviven múltiples actores con motivaciones diversas.

Actualmente, si bien grupos como Anonymous continúan operando de forma descentralizada, su impacto ha disminuido en comparación con el auge que llegaron a alcanzar a principios de la década de 2010. En paralelo, han surgido nuevas generaciones de hacktivistas, que, aunque cuentan con un menor nivel de experiencia técnica, lo compensan con el uso de herramientas de automatización y con un dominio del impacto mediático y de la movilización social.

En la actualidad, el hacktivismo es utilizado tanto por colectivos independientes que denuncian injusticias, como por grupos patrocinados por Estados que instrumentalizan estas tácticas con fines geopolíticos. El conflicto entre Rusia y Ucrania ha evidenciado la existencia de una guerra cibernética, en la que hacktivistas pro-ucranianos y pro-rusos llevan a cabo ataques coordinados en beneficio de sus respectivos bandos.

La frontera entre activismo digital legítimo, ciberdelincuencia y operaciones de inteligencia encubiertas es cada vez más difusa. Sin embargo, podríamos considerar que actualmente existen tres tipos de hacktivistas: ciberterroristas, *hackers* cívicos y *hackers* patrióticos (Dahan, 2013; Denning, 2001; Johnson y Robinson, 2014; Sauter, 2013).

El ciberterrorismo comprendería todas aquellas acciones hostiles en el ciberespacio encaminadas a perpetrar actos de violencia contra personas o propiedades, con el objetivo de intimidar o coaccionar a gobiernos o sociedades para alcanzar unos fines políticos, religiosos o ideológicos determinados. Principalmente, sus acciones se concretan en la propagación de virus y *malware*, el vandalismo contra *webs* y la realización de ataques de denegación de servicio (DDoS) o de *botnets* ((Denning, 2001; Jordan y Taylor, 2004; Goode, 2015).

En la categoría de *hackers* cívicos encontraríamos a todos aquellos grupos organizados que realizan acciones contra sistemas informáticos con el objetivo de aportar algún bien a la comunidad, bordeando generalmente la alegalidad. (Hunsinger y Schrock, 2016; Schrock, 2016).

Por último, los *hackers* patrióticos son aquellos individuos o grupos, cuyos esfuerzos se alinean con la ideología nacionalista y se consideran una "milicia cibernética" en pos de la defensa de unos intereses determinados (Dahan, 2013; Green, 2016). Aunque desde el exterior estos *hackers* parezcan no estar directamente patrocinados por ningún Estado, lo cierto es que, actualmente sí que podemos inferir su instrumentalización como parte de un entramado de fuerzas estatales mayor.

El *hackeo* patriótico se originó en China en la década de 1990 como respuesta a los disturbios antichinos en Indonesia, y desde, entonces viene utilizándose como táctica por parte de China, Rusia, Siria y otros Estados como medio para dañar a sus enemigos en el dominio cibernético. No obstante, ninguna de las operaciones anteriores a la guerra de Ucrania había alcanzado la magnitud, el impacto ni unos lazos gubernamentales tan sólidos y prolongados, ni transgredió de manera tan evidente las normas internacionales, como el hacktivismo contemporáneo (Healey & Grinberg, 2022).

3. EL NEXO DE UNIÓN ENTRE EL HACKTIVISMO Y LAS APT

A lo largo de la historia, los Estados han recurrido a actores interpuestos para llevar a cabo sus estrategias de conflicto sin comprometer directamente a sus Fuerzas Armadas. Unidades auxiliares, grupos mercenarios, insurgencias, organizaciones terroristas o empresas militares privadas (PMC) son solamente algunas de las formas que han adoptado terceros actores para actuar como sustitutos en la acción estratégica de los Estados.

Por ello, hoy no resulta sorprendente que, a la luz de una sociedad cada vez más digitalizada, la acción de los Estados haya encontrado en los grupos hacktivistas un nuevo actor para personificar la externalización de la autoría, y en el ciberespacio, el entorno idóneo para proyectar influencia geopolítica.

El concepto de guerra de sustitutos (*surrogate warfare*) ha sido objeto de un debate extenso en la comunidad académica y de seguridad, especialmente por la dificultad que existe para diferenciarlo de la guerra de *proxies*, dada la naturaleza estrechamente entrelazada de ambos conceptos.

En ambos términos, los objetivos del actor principal (el Estado) y el agente apoderado coinciden. Sin embargo, mientras que, en las *proxy warfare* existen dos o más actores relacionados jerárquicamente (el actor principal trabaja por, con y a través del agente apoderado para lograr un objetivo común); en las *surrogate warfare* éstos actores solo se alinean únicamente si el actor principal es capaz de movilizar el apoyo adecuado que exige el agente apoderado (Fox 2019). Dicho de otra forma, los conceptos s*urrogate warfare* y *proxy warfare* difieren en función de la relación existente entre los actores y sus motivaciones.

Dado que los grupos hacktivistas apenas tienen independencia para ejercer resistencia al control del Estado que les patrocina (o al menos, que los influencia o tolera), en nuestro caso de estudio hablaremos en términos de actores *proxies*.

Más concretamente, para referirnos a ellos utilizaremos la definición de Rondeaux y Sterman (2019) de "actores *proxies*", quienes los definen como "*sujetos ajenos a la estructura de seguridad de los Estados involucrados en un conflicto que actúan bajo patrocinio directo o indirecto de un actor convencional (un Estado)*"; y en la definición de Maurer (2018) de *ciberproxies*, como "*intermediarios que llevan a cabo acciones ofensivas en el ciberespacio en beneficio de un actor principal*".

Históricamente, los *ciberproxies* se han personificado a través de distintas entidades vinculadas al mundo de la ciberdelincuencia y el ciberespionaje. No obstante, el término engloba un gran número de entidades organizadas que, de forma directa o indirecta, suponen un factor de riesgo para empresas y Estados. De hecho, la lista de actores es realmente amplia: grupos criminales, empresas privadas de ciberarmas (actores ofensivos del sector privado, en inglés *Private Sector Offensive Actor*, PSOA), grupos terroristas, insurgentes, hacktivistas, actores estales o APT son solamente algunos de ellos.

Las razones detrás de su utilización son variadas: (1) la utilización de actores *proxies* por parte de los gobiernos reduce el riesgo de escalada en los conflictos, dado que la dificultad de atribuir la responsabilidad de un ciberataque es compleja; (2) existe una posibilidad de negación plausible que desvía la responsabilidad de un ataque hacia un actor fuera de control gubernamental; (3) favorece a los Estados alargar la situación de tensión en los conflictos, desgastando a su adversario a un nivel social, político y económico; (4) 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; (5) aporta a los Estados rapidez y flexibilidad en la respuesta a las acciones ofensivas de sus adversarios, al no exigir evidencias técnicas ni legitimación pública; (6) ofrece a los Estados una herramienta más de disuasión; (7) permite a los Estados eludir la aplicación del derecho internacional; (8) facilita la utilización de personal experto sin necesidad de ofrecer una contratación legal; (9) posibilita participar en conflictos internacionales que en otras circunstancias resultarían económica y políticamente inabarcables (Torres Soriano, 2017; Expósito Guisado, 2024; Marín Gutiérrez, 2023).

No obstante, la consecución de estos beneficios no está exenta de problemáticas. De hecho, el principal atractivo de recurrir a un *proxy* (que no es otro que obtener una negación plausible de una agresión), resulta también su principal debilidad, pues el anonimato y la clandestinidad diluyen la capacidad coactiva y disuasiva del Estado patrocinador –al fin y al cabo, no podemos obviar las teorías Clausewitz que sugieren que para que un Estado modifique su conducta en base a la voluntad de otro es preciso que éste sepa la procedencia del acto de coacción sufrido.

Otro inconveniente del uso de *ciberproxies* radica en cómo el Estado los selecciona y controla cuando los instrumentaliza. La existencia de intereses divergentes entre ambas partes puede llevar a la deslealtad del *proxy*, ocasionando perjuicios económicos o políticos para el propio actor que los emplea –un hecho agravado si

tenemos en cuenta que estos *proxies* operan generalmente en ámbitos donde el Estado ni puede ni quiere intervenir.

El beneficio de los *proxies* está en su capacidad para actuar de forma encubierta, aunque esa misma falta de transparencia es lo que limita al Estado patrocinador a la hora de verificar sus antecedentes y confiabilidad. La literatura académica destaca que el control sobre los *proxies* se complica aún más si el Estado no cuenta con mecanismos efectivos para sancionar la deslealtad, o si existen estructuras descentralizadas que impidan un correcto cumplimiento de las órdenes jerárquicas (Popovic, 2015).

En el presente documento nos centraremos únicamente en dos actores que representan los dos polos distintos (activismo abierto y espionaje silencioso) de un mismo fenómeno, pero que no son tan diferentes si nos basamos en los fines que persiguen y en la instrumentalización que de ellos realizan los Estados.

En términos generales, el hacktivismo y las APT difieren en motivación, métodos y grado de respaldo estatal. Así, mientras que, el hacktivismo es movido por un contexto político-social (protesta, activismo, causas morales), las APT se centran en el espionaje estratégico y la obtención de una ventaja económico-militar.

Operacionalmente, las APT actúan a través del sigilo y la persistencia, empleando *malwares* personalizados, puertas traseras y movimientos laterales; a diferencia de las acciones hacktivistas que suelen buscar la atención pública y que se centran generalmente en el ataque mediante DDosS a corto plazo.

Sin embargo, no es extraño observar como las APT actúan temporalmente como hacktivistas (cuando divulgan públicamente los datos que exfiltran para provocar un impacto político) y como las hacktivistas son instrumentalizadas por los Estados para lograr sus fines estratégicos.

A nivel organización, hacktivistas y APT también presentan divergencias: los hacktivistas generalmente actúan de forma descentralizada, espontánea, incluso anónima, y sin mando unificado. Por su parte, las APT suelen ser equipos estructurados, muchas veces integrados en una organización mayor (un ejército, agencia de inteligencia o grupo criminal), con una jerarquía definida y una financiación considerablemente más potente (CyberZaintza, 2021).

Precisamente, la diferencia de recursos y de capacitación técnica sugiere un vínculo más estrecho de las APT con los Estados que los grupos hacktivistas. Pese a todo, las líneas que separan ambos conceptos se vienen difuminado recientemente en vistas a la constatación de que algunos grupos hacktivistas prorrusos vienen recibiendo el apoyo encubierto del Estado, o actúan alineados con la agenda estatal, borrando así la hasta ahora distinción clara entre "*hackers* activistas" y "operativos estatales" (Muncaster, 2024).

De hecho, no es descartable que, ciertos grupos hacktivistas en realidad estén formados o respaldados por APT's o, directamente, por actores estatales. Un ejemplo, lo encontraríamos en "XakNet Team", "Infoccentr" y "CyberArmyofRussia_Reborn", grupos hacktivistas prorrusos que según Mandiant se constituyen como actores de

ciberamenazas patrocinados por la Dirección Principal de Inteligencia de Rusia (GRU) a través de la APT44 (Mandiant, 2022).

A lo largo de la última década se han documentado múltiples casos en que los Estados han recurrido tanto a grupos APT propios como a colectivos hacktivistas (o sus identidades) para llevar a cabo operaciones de ciberespionaje, sabotaje en conflictos y manipulación política.

Un ejemplo paradigmático que ilustra la interdependencia de ambos conceptos, lo encontramos en las elecciones de EE.UU. de 2016, cuando "*DCLeaks*" y "*Guccifer 2.0*", dos identidades vinculadas a la Dirección Principal de Inteligencia de Rusia (*Glavnoe Razvedyvatel'noe Upravlenie*, GRU), robaron los correos del Partido Demócrata y los difundieron haciéndose pasar por "hacktivistas estadounidenses patriotas" (DOJ, 2018).

A raíz de la guerra de Ucrania, no es extraño encontrar la interdependencia entre hacktivistas y APT rusas, grupos como *Killnet, NoName057(16), Anonymous Sudan* que han atacado sitios web gubernamentales y empresas occidentales en apoyo a la narrativa del Kremlin muestran que, si bien estos grupos se autodenominan "activistas espontáneos", lo cierto es que, sospechosamente actúan de forma coordinada con la acción estatal rusa (Van Der Walt, 2025).

Sin embargo, Rusia no es el único actor estatal que emplea APT y hacktivistas para desplegar su poder. Otros Estados como China, Corea del Norte o Irán también han sido acusados durante años de conducir de esta forma sus actividades ofensivas en el ciberespacio.

Concretamente, China ha sido acusada durante años de patrocinar vastas campañas de espionaje cibernético a través de unidades militares y *hackers* a sueldo, como los del grupo APT1, considerados por Mandiant en 2013, como la Unidad 61398 del Ejército Popular de Liberación chino.

Las operaciones de APT chinas suelen centrarse en objetivos estratégicos (industrias aeroespaciales, energéticas, telecomunicaciones, defensa, etc.) y se consideran parte de la inteligencia estatal china, pero a diferencia de Rusia, en las estrategias chinas, el uso del hacktivismo no es tan prominente.

El gobierno ha tolerado e incluso inspirado a "*hackers* patrióticos" chinos en algunos conflictos, siendo un ejemplo de ello la "*Red de Hackers Honker*", una comunidad de *hackers* fuera de control gubernamental –según fuentes chinas— que ha atacado a actores adversarios de China durante disputas territoriales o incidentes diplomáticos.

Irán por su parte, sí ha mostrado una tendencia a instrumentalizar grupos de *hackers* supuestamente activistas para realizar operaciones de represalia contra sus adversarios, a la vez que desarrolla sus propias APT. Un ejemplo significativo de ello fueron los ataques DDoS contra bancos estadounidenses en 2012-2013, en represalia por las sanciones occidentales: una entidad que se presentaba como hacktivistas religiosa y autodenominada "*Cyber Fighters of Izz ad-Din al-Qassam*" se atribuyó la ofensiva alegando un sentimiento de indignación por un video antislámico (CFR, 2012).

Las agencias de inteligencia estadounidenses concluyeron posteriormente que se trató de una operación orquestada por Irán (probablemente su Guardia Revolucionaria) como respuesta a las medidas adoptadas contra su programa nuclear. De hecho, en 2016 el Departamento de Justicia de EE.UU. imputó a siete iraníes vinculados al Cuerpo de la Guardia Revolucionaria Islámica (IRGC) por estos ataques.

Otro ejemplo lo encontraríamos en el ataque "*Shamoonj*" de 2012 del grupo "*Cutting Sword of Justice*", un supuesto grupo hacktivista que borró los datos de 30.000 ordenadores de la petrolera saudí Aramco, pero que posteriormente los analistas atribuyeron a una operación del Estado iraní en respuesta a la ofensiva de *Stuxnet* y las tensiones regionales.

Corea del Norte, pese a su aislamiento, también ha logrado construir una de las amenazas cibernéticas más activas, principalmente para recaudar fondos y generar desestabilización en sus adversarios geopolíticos. Su grupo APT más notable, *Lazarus Group* (vinculado al APT38) ha robado cientos de millones mediante ataques a entidades bancarias.

Otro caso que ilustra la instrumentalización de las campañas activistas por parte de los Estados lo encontramos también en una de sus actuaciones, el *hackeo* a Sony Pictures en 2014, cuando un grupo denominado "*Guardians of Peace*" exfiltró datos confidenciales y destruyó sistemas de Sony en aparente represalia por la película satírica sobre el líder norcoreano "*The Interview*". (FBI, 2014).

Corea del Norte muestra el paradigma de la instrumentalización directa, sus *hackers* son agentes del Estado que en ocasiones asumen nombres de grupos ficticios para difundir sus mensajes o justificar sus ataques, pero a diferencia de otros Estados, los norcoreanos suprimen absolutamente la distinción entre APT y aparato estatal, manteniendo la cobertura únicamente en la narrativa pública de cara al exterior.

Por su parte, en las potencias occidentales obviamente también se emplean capacidades cibernéticas ofensivas para atacar otros Estados. Quizás el caso más relevante sea la operación "Olympic Games" atribuida a las agencias NSA y la unidad 8200 (no oficialmente reconocida), en la cual Estados Unidos e Israel desarrollaron el malware *Stuxnet* para sabotear las centrifugadoras nucleares de Irán alrededor del año 2010 (The Guardian, 2017).

Sin embargo, en Occidente, si bien existen entidades APT sustentadas por los Estados para actuar ofensivamente en campañas de espionaje, la instrumentalización de grupos hacktivistas para ocultar sus acciones es prácticamente inexistente. De hecho, únicamente podemos encontrar un caso donde un grupo hacktivista occidental vincula su actividad a la capacidad ciberofensiva de un Estado: el "*IT Army of Ukraine*".

Este caso es especialmente controvertido, pues el apoyo estatal público por parte del gobierno ucraniano viola abiertamente las normas recientemente acordadas sobre la conducta de los Estados en el ciberespacio, así como las posiciones de política exterior de los miembros de la OTAN (Healey y Grinberg, 2022).

Si utilizamos la tabla "Espectro de la responsabilidad" de Healey y Grinberg (2022), donde correlacionan la actividad de los grupos en función del grado de

responsabilidad del Estado para con su *ciberproxy*, podemos ver como el apoyo del Gobierno ucraniano al *IT Army of Ukraine* comenzó al menos como "coordinado por el Estado (nivel 6)", (cuando el Ministro ucraniano de Transformación Digital, Mijailo Fedorov llamó abiertamente a voluntarios hacktivistas de todo el mundo para que apoyaran a Ucrania en el frente digital) hasta llegar incluso a "alentado por el Estado (nivel 4)".

Tabla 1: *Espectro de la responsabilidad del Estado.*

Posición estatal	Relación Estado-*proxy*
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 el ataque, 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.

(Healey, 2022).

Especialmente, en los conflictos geopolíticos es donde vemos una convergencia más acelerada entre el hacktivismo y las operaciones estatales. En el caso de la guerra de Ucrania, tres años después del inicio del conflicto y, pese a que el número de actores hacktivistas ha disminuido considerablemente (de más de 130 grupos en 2024 a sólo unos 80 grupos en 2025), podemos seguir observando como ambos bandos mantienen un cruce de ciberataques destructivos, coordinados con su campaña militar y apoyados en sus actuaciones por "hackers patrióticos" (Cyberknow, 2025).

En el bando ucraniano, el *IT Army of Ukraine* sigue vigente como la fuerza hacktivista más importante de Ucrania, movilizando aún a voluntarios dentro y fuera del país para atacar las infraestructuras rusas, efectuar contrapropaganda y apoyar misiones de inteligencia. En el periodo 2023-2024, se le atribuye, por ejemplo, la caída temporal

de servicios de Internet en zonas ocupadas por Rusia y el continuo despliegue de campañas de DDoS contra entidades rusas de alto perfil (Optiv, 2023).

Del lado prorruso, el grupo más prominente en la actualidad es *NoName057(16)*, un grupo vinculado al GRU, que actúa en coordinación con la agenda del Kremlin, al seleccionar objetivos en sintonía con los intereses estratégicos rusos y que se considera a sí mismo una suerte de "brazo ciberespontáneo" permanente del Ejército ruso.

Tabla 2: *Casos cronológicos de instrumentalización estatal del hacktivismo.*

Año	***Estado***	***Grupo hacktivista***	***Característica***	***Nivel de vinculación estatal (Healey & Grinberg).***
1998-1999	Kosovo	Hackers patrióticos	Primer conflicto con intervención hacktivista notable.	Ignorado / Espontáneo
1999	China	Red Honker	Hackers patrióticos activos en conflictos territoriales. Campañas de espionaje industrial y ciberataques a infraestructuras críticas.	Fomentado / Conformado
2012-2013	Irán	Cyber Fighters of Izz ad-Din al-Qassam	Ataques DDoS a bancos de EE.UU. como represalia por sanciones. Operación Shamoon contra Aramco con borrado masivo.	Coordinado / Ordenado
2014	Corea del Norte	Lazarus Group	Ciberataques para financiación estatal. Ataque a Sony Pictures (2014) como represalia simbólica	Ejecutado / Integrado
2022-presente	Rusia	Killnet/ Cyber Army of Russian Reborn/ NoName057(16)	Grupos hacktivistas coordinados con la estrategia rusa en la guerra de Ucrania. Ataques DDoS.	Coordinado / Fomentado
2022-presente	Ucrania	IT Army of Ukraine	Convocatoria pública del gobierno para hacktivismo contra Rusia. DDoS, sabotaje y propaganda pro-Ucrania.	Coordinado / Fomentado

4. EL FUTURO DE LOS GRUPOS HACKTIVISTAS.

La supervivencia de los grupos hacktivistas indica que el hacktivismo integrado en la guerra ha llegado para quedarse, al menos mientras dure el conflicto subyacente y los Estados en conflicto encuentren útil esa capa de acción descentralizada. Es más, el panorama hacktivistas actual nos lleva a observar como el hacktivismo está traspasando la frontera del DDoS y adentrándose en ataques más sofisticados propios de las APT, como son los ataques a sistemas SCADA y de control industrial (ICS) de infraestructuras críticas[4].

El hecho de que grupos pertenecientes al ecosistema hacktivista prorruso, como *Z-Pentest Alliance* o *Sector 16,* vengan realizando activamente intrusiones a plantas energéticas, instalaciones de agua potable e industrias en general, refleja no solamente una maduración y estatalización del fenómeno hacktivista, sino también la existencia de unos riesgos cada vez más físicos de sus acciones (Antoniuk, 2024).

La reducción del número de grupos hacktivistas del entorno prorruso sugiere que la efervescencia inicial ha dado paso a una selección natural donde sobreviven los colectivos con mejor apoyo, organización y protección. Un fenómeno que se traduce en operaciones más eficaces y coordinadas, aunque también más predecibles al estar alineadas con la agenda estatal rusa.

Al mismo tiempo, la persistencia de ataques diarios indica que la guerra cibernética de baja intensidad se ha vuelto rutinaria. Los DDoS constantes mantienen una presión psicológica y propagandística sobre las poblaciones objetivo (recordando diariamente la presencia del conflicto), mientras que, la adopción de *ransomware* y los ataques a las industrias eleva el potencial de daño real a infraestructuras críticas, desdibujando la línea entre el hacktivismo y ciberterrorismo –un hecho que puede terminar por derivar en respuestas más contundentes por parte de los Estados víctimas y posibilidades de escalada en los conflictos.

Otro hecho de relevancia es el desarrollo notable en las alianzas emergentes entre causas hacktivistas que transciende el teatro de operaciones más allá de Ucrania e implica a terceros países. Un ejemplo, es la reciente alianza entre hacktivistas prorrusos y propalestinos, que une causas geopolíticas aparentemente distintas bajo una narrativa de ataque común hacia Occidente.

Las tensiones globales de 2024 (incluida la guerra de Gaza) crearon un extraño frente unido de hacktivista. Los grupos rusos (especialmente *NoName057(16)*) comenzaron a coordinar operaciones con colectivos vinculados a Oriente Medio (como *Mr. Hamza* o *Anonymous Guys*), y sincronizaron sus ataques bajo la bandera de la unión "*Holy League*" contra países que percibían como adversarios compartidos, como es el ejemplo de Francia.

Este tipo de alianzas son conocidas en España, y particularmente, por la Guardia Civil, ya que, en julio de 2024, la Institución fue objetivo directo de una de campaña de ciberataques conjuntos, "*#FuckGuardiaCivil*", que respondía a una iniciativa promovida

[4] Sistema centralizado que permite supervisar, controlar y recopilar datos de procesos y dispositivos en tiempo real.

por el grupo *NoName057(16),* para "vengarse de las autoridades españolas" que habían detenido a tres personas en Manacor (Mallorca), Huelva y Sevilla, sospechosas de participar en ciberataques contra entidades públicas y empresas estratégicas de España y otros países de la OTAN.

De hecho, en abril de 2025, ya se registró una nueva alianza conformada, entre otros, por los grupos *Keymous+, Mr Hamza, ¡Alixsec y NoName057(16)* para atacar a Polonia, Alemania, Francia, Italia y España bajo el lema "*Operation Hack For Humanity V2!*".

Tan solo en el caso español, el primer día de la campaña "Operation Hack For Humanity V2!" se registraron más de 30 ataques a empresas y sitios web gubernamentales, siendo los grupos más activos en el ataque *Mr Hamza*, *NoName057(16)*, *TwoNet* y *Keymous+*.

La frecuencia con la que se viene produciendo esta convergencia en los últimos meses demuestra que, el fenómeno cada día es más internacional y está más interconectado. Las alianzas entre grupos hacktivistas se han solidarizado entre sí, trascendiendo las fronteras del conflicto ruso-ucraniano con un único objetivo: ampliar sus acciones hacia el enemigo común occidental.

El hecho de que países de la OTAN, como Francia, Italia o la propia España, puedan convertirse en objetivos de los *hackers* patrióticos rusos podría llegar a producir una escalada en el conflicto, especialmente si uno de sus ataques lograse dañar severamente una infraestructura crítica, la guerra cibernética de baja intensidad podría obtener una respuesta más firme de lo usual.

5. CONCLUSIONES

El análisis del hacktivismo y su relación con los Estados demuestra que, este fenómeno ha evolucionado desde la protesta digital hacia una instrumentalización estatal con implicaciones geopolíticas y estratégicas. La frontera entre activismo, cibercriminalidad y operaciones estatales es cada vez más difusa, especialmente en conflictos como la guerra de Ucrania, donde se ha observado una creciente instrumentalización de los grupos hacktivistas por parte de las fuerzas gubernamentales en la defensa de sus intereses nacionales.

Ciertamente, el conflicto entre Rusia y Ucrania ha marcado un punto de inflexión en el uso del ciberespacio como campo de batalla, donde tanto actores estatales como no estatales han participado activamente en ataques de denegación de servicio (DDoS), ciberespionaje y sabotaje de infraestructuras críticas.

El presente estudio, desarrollado a través del estudio de los casos más destacados en el escenario internacional, ha permitido establecer una distinción entre los *hackers* cívicos y los *hackers* patrióticos. Mientras que, los primeros abrazan causas nihilistas o socialmente conflictivas, los segundos son utilizados por los Estados como una herramienta encubierta en conflictos internacionales, lo cual supone una externalización de las capacidades cibernéticas gubernamentales y ofrece una serie de ventajas

estratégicas: negación plausible de responsabilidad, prolongación de situaciones de tensión o la reducción de costes políticos y económicos.

En síntesis, podríamos decir que, los Estados han aprendido a aprovechar el hacktivismo como un arma adicional, ya sea fingiéndose hacktivistas para desinformar o exfiltrando datos o animando a sus simpatizantes a lanzar ciberataques en masa contra su enemigo.

Esta instrumentalización plantea, sin embargo, serios desafíos a nivel estratégico. La progresiva sofisticación de unos ataques que han pasado del vandalismo digital a operaciones más avanzadas contra infraestructuras críticas no hace sino incrementar seriamente las posibilidades de represalias por parte de los Estados afectados y aumentar el riesgo potencial de escalada en los conflictos asimétricos.

Además, la convergencia entre las APT y los hacktivistas pone en cuestión las normativas internacionales vigentes, ya que, los ataques perpetrados por actores *proxies* difuminan la responsabilidad estatal y dificultan la aplicación de medidas de disuasión o represalias directas. Especialmente, cuando los colectivos hacktivistas parecen evolucionar hacia un nuevo panorama de alianzas capaz de aglutinar a grupos hacktivistas con agendas geopolíticas diversas para atacar a los países occidentales.

La seguridad cibernética de los Estados debe adaptarse a una nueva realidad en la que los grupos hacktivistas juegan un papel clave en la proyección del poder estatal. Las democracias occidentales, tradicionalmente más reacias a utilizar este tipo de tácticas, se deben enfrentar al dilema de cómo responder de manera efectiva sin comprometer sus valores.

La tendencia actual no solamente muestra una clara evolución del hacktivismo hacia una vinculación cada vez mayor con los intereses estatales del Gobierno que les sustenta, sino que también refuerza la idea de que el ciberespacio continuará adquiriendo una mayor importancia en los conflictos del futuro. Casos como el de Rusia, donde grupos como *Killnet* o *NoName057(16)* han reivindicado operaciones cibernéticas coincidentes con los intereses geopolíticos del Kremlin —especialmente durante la guerra en Ucrania—, o el de Irán, con colectivos como *Tapandegan*, cuya retórica oposicionista no impide sospechas de coordinación indirecta con agendas estatales, ejemplifican esta deriva, evidencian un progresivo desdibujamiento entre actores no estatales y estatales en el ámbito digital, donde el hacktivismo deja de ser exclusivamente una forma de disidencia ciudadana para convertirse, en ciertos contextos, en una herramienta informal de proyección del poder estatal.

6. REFERENCIAS BIBLIOGRÁFICAS

Antoniuk, D. (2024). *Cybervolk: Hacktivists from India and Russia collaborate on ransomware attacks*. The Record. https://therecord.media/cybervolk-india-hacktivists-russia-ransomware

Antoniuk, D. (2024). *Cybervolk: Hacktivists from India and Russia collaborate on ransomware attacks*. The Record. https://therecord.media/cybervolk-india-hacktivists-russia-ransomware

Auty, C. (2004). Political hacktivism: Tool of the underdog or scourge of cyberspace? *Aslib Proceedings, 56*(4), 212-221.

Bartlett, J. (2015). *The dark net: Inside the digital underworld*. Melville House.

CFR (2012). *Denial of service attacks against U.S. banks in 2012–2013*. Council on Foreign Relations (CFR). https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso Books.

Cyberknow (2025). *Russia-Ukraine war: Hacktivist update*. https://cyberknow.substack.com/p/russia-ukraine-war-hacktivist-update

CyberZaintza (2021). *Grupo APT*. https://www.ciberseguridad.eus/ciberglosario/grupo-apt

Dahan, M. (2013). Hacking for the homeland: Patriotic hackers versus hacktivists. *International Conference on Information Warfare and Security*, 51–VII. Academic Conferences International Limited. https://search.proquest.com/docview/1549245919

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. En J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239-288). RAND Corporation.

DOJ (2018). *Grand jury indicts 12 Russian intelligence officers for hacking offenses related to the 2016 election*. U.S. Department of Justice. https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

Expósito Guisado, J. (2023). *Ciberproxies: las APT como factor de riesgo futuro*. Instituto Español de Estudios Estratégicos (IEEE). *Boletín IEEE*, (32), 815-831.

FBI (2014). *Update on Sony Investigation*. Federal Bureau of Investigation (FBI), Washington, D.C. https://www.fbi.gov/news/press-releases/update-on-sony-investigation

Fox, A. C. (2019). *Conflict and the need for a theory of proxy warfare*. *Journal of Strategic Security, 12*(1), 44–71. JSTOR. www.jstor.org/stable/26623077

Goode, L. (2015). Anonymous and the political ethos of hacktivism. *Popular Communication, 13*(1), 74–86. https://doi.org/10.1080/15405702.2014.978000

Green, K. (2016). People's war in cyberspace: Using China's civilian economy in the information domain. *Military Cyber Affairs, 2*(1). https://doi.org/10.5038/2378-0789.2.1.1022

Healey, J., & Grinberg, A. (2022). *Patriotic hacking: No exception*. Lawfare. https://www.lawfaremedia.org/article/patriotic-hacking-no-exception

Hern, A. (2017). NSA contractor leaked US hacking tools by mistake, Kaspersky says. *The Guardian*. https://www.theguardian.com/technology/2017/oct/26/kaspersky-russia-nsa-contractor-leaked-us-hacking-tools-by-mistake-pirating-microsoft-office

Hunsinger, J., & Schrock, A. (2016). The democratization of hacking and making. *New Media & Society, 18*(4), 535–538. https://doi.org/10.1177/1461444816629466

Johnson, P., & Robinson, P. (2014). Civic hackathons: Innovation, procurement, or civic engagement? *Review of Policy Research, 31*(4), 349–357. https://doi.org/10.1111/ropr.12074

Jordan, T. (2002). *Activism! Direct action, hacktivism and the future of society*. Reaktion Books.

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and cyberwars: Rebels with a cause?* Psychology Press.

Mandiant (2022). *GRU's rise: Telegram minions*. https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions

Marín, F. (2023). *Hacktivismo al servicio del Estado: ciberproxies en Ucrania*. Documento de Opinión. Instituto Español de Estudios Estratégicos (IEEE).

Maurer, T. (2018). *Cyber Mercenaries: The state, hackers, and power*. Cambridge University Press.

Muncaster, P. (2024). *El hacktivismo: Evolucionando amenazas para las organizaciones*. WeLiveSecurity. https://www.welivesecurity.com/es/cibercrimen/el-hacktivismo-evolucionando-amenazas-organizaciones

Olson, P. (2012). *5 things every organization can learn from Anonymous*. Forbes. http://www.forbes.com/sites/parmyolson/2012/06/05/5-things-every-organization-can-learn-from-anonymous/

OPTIV (2023). *Russia/Ukraine Update - December 2023*. https://www.optiv.com/insights/discover/blog/russiaukraine-update-december-2023

Popovic, M. (2015). Fragile proxies: Explaining rebel defection against their state sponsors. *Terrorism and Political Violence*. https://doi.org/10.1080/09546553.2015.1092437

Rondeaux, C., & Sterman, D. (2019). *Twenty-first century proxy warfare: Confronting strategic innovation in a multipolar world since the 2011 NATO intervention*. New America. https://d1y8sb8igg2f8e.cloudfront.net/documents/Twenty-First_Century_Proxy_Warfare_Final.pdf

Sauter, M. (2013). "LOIC will tear us apart": The impact of tool design and media portrayals in the success of activist DDOS attacks. *American Behavioral Scientist, 57*(7), 983–1007. https://doi.org/10.1177/000276

Schrock, A. R. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *New Media & Society, 18*(4), 581–599. https://doi.org/10.1177/1461444816629469

Torres Soriano, M. (2017). Guerras por delegación en el ciberespacio. *Revista del Instituto Español de Estudios Estratégicos, (9)*, 15-36.

(2018). El hacktivismo como estrategia de comunicación de Anonymous al cibercalifato. *Cuadernos de Estrategia, (197)*, 197-224.

Van Der Walt (2025). *Reflecting on three years of cyber warfare in Ukraine*. *ComputerWeekly*. https://www.computerweekly.com/opinion/Reflecting-on-three-years-of-cyber-warfare-in-Ukraine

Vegh, S. (2005). *The media's portrayal of hacking, hackers, and hacktivism before and after September 11*. *First Monday*. http://uncommonculture.org/ojs/index.php/fm/article/view/1206/1126