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

Artigo de investigação

HACKTIVISMO: DO PROTESTO SOCIAL À INSTRUMENTALIZAÇÃO DO ESTADO

Tradução para o português com ajuda de IA (DeepL)

Josué Expósito Guisado
Sargento da Guardia Civil
Estudante de doutoramento na Universidade Pablo de Olavide
Mestrado em Paz, Segurança e Defesa pelo
Instituto Universitário Gutiérrez Mellado (UNED)
jexpgui@gmail.com
ORCID: 0009-0003-4977-3899

Recebido em 18/03/2025
Aceite em 05/05/2025
Publicado em 27/06/2025

Citação recomendada: Expósito, J. (2025). Hacktivismo: do protesto social à instrumentalização do Estado. *Revista Logos Guardia Civil*, 3(2), pp. 101-122.

Depósito legal: M-3619-2023
NIPO em linha: 126-23-019-8
ISSN em linha: 2952-394X

ORCID: 0009-0003-4977-3899

HACKTIVISMO: DO PROTESTO SOCIAL À INSTRUMENTALIZAÇÃO DO ESTADO

Resumo: INTRODUÇÃO. 2. DO PROTESTO SOCIAL À GUERRA CIBERNÉTICA. 3. 3.A LIGAÇÃO ENTRE HACKTIVISMO E APT. 4. O FUTURO DOS GRUPOS HACKTIVISTAS. 5. CONCLUSÕES. 6. REFERÊNCIAS BIBLIOGRÁFICAS.

Resumo: O hacktivismo evoluiu de uma forma inicial de protesto digital para se tornar um instrumento fundamental nos conflitos geopolíticos contemporâneos. O que começou por ser um movimento descentralizado em defesa da liberdade de expressão e da justiça social tem sido progressivamente instrumentalizado pelos Estados para executar ciberataques, manipular a opinião pública e lançar operações de desinformação. Este fenómeno foi particularmente acentuado no contexto da guerra na Ucrânia, onde a convergência entre grupos de Ameaças Persistentes Avançadas (APT) e hacktivistas patrióticos permitiu a execução de ciberoperações coordenadas com os interesses do Estado. Paralelamente, a internacionalização do hacktivismo levou à formação de alianças entre grupos de diferentes regiões, alargando o seu impacto para além do conflito russo-ucraniano. O ciberespaço estabeleceu-se como uma arena ideal para o confronto entre Estados num ambiente controlado. No entanto, a crescente sofisticação dos ataques e o facto de visarem alvos cada vez mais estratégicos colocam sérios desafios à estabilidade internacional e à segurança dos Estados ocidentais.

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.

Palavras-chave: Hacktivismo, APTs, ciberproxies, ciberconflito, ciberataques.

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

ABREVIATURAS

APT: *Ameaça Persistente Avançada*.

DDoS: Ataque *de negação de serviço distribuído*.

DOJ: *Departamento de Justiça* dos EUA.

FBI: *Federal Bureau of Investigation*.

GRU: Direção Principal de Informações da Rússia (*Glavnoe Razvedyvatel'noe Upravlenie*).

ICS: *Sistemas de Controlo Industrial*.

IRGC: *Corpo de Guardas da Revolução Islâmica* do Irão.

Exército informático da Ucrânia: Exército informático da Ucrânia.

NSA: *Agência de Segurança* Nacional dos EUA.

PMC: *Empresa Militar Privada*.

PSOA: *Private Setor Offensive Ator*.

SCADA: *Controlo de Supervisão e Aquisição de Dados*.

Stuxnet: Nome do *malware* utilizado na operação "Jogos Olímpicos".

1. INTRODUÇÃO

A guerra na Ucrânia fez com que o mundo ocidental fosse mais uma vez confrontado com o impacto do realismo político. Antes da invasão de 2022, a grande maioria dos analistas ocidentais era incapaz de imaginar um conflito convencional na cena internacional como o que continua a ocorrer às portas da Europa. Cegos pelas doutrinas do soft power e seguindo os paradigmas liberais da paz capitalista ou da teoria da paz comercial, os líderes europeus ignoraram deliberadamente o facto de que, em algumas partes do mundo, o realismo político ainda prevalece.

Num mundo cada vez mais digitalizado, onde existe uma interconexão virtual entre o plano intangível da tecnologia da informação e o próprio espaço físico, não é surpreendente que o atual inimigo da Europa represente um desafio de segurança. À medida que os Estados se tornaram cada vez mais dependentes das tecnologias da informação, também aumentaram as oportunidades para os actores hostis (estatais e não estatais) influenciarem o ambiente político e geopolítico através de acções no ciberespaço.

A guerra na Ucrânia não só marcou o início de uma operação de assédio e de perturbação cibernética por parte de ciberameaças ligadas ao Kremlin, como também provocou uma mudança no panorama hacktivista mundial: o que até há não muitos anos era o bastião da defesa da liberdade de expressão, da privacidade, da justiça social e dos direitos humanos, é agora uma ferramenta com implicações estratégicas e, em muitos casos, ligada direta ou indiretamente a governos e serviços secretos.

O ativismo digital ideológico e orientado para o protesto que os Anonymous outrora representaram está a evoluir para um fenómeno constituído por uma miríade de grupos nacionalistas que recorrem repetidamente a ataques distribuídos de negação de serviço (DDoS) para criar um clima de tensão e perseguição persistente dos inimigos ocidentais.

O hacktivismo tornou-se uma ferramenta de dois gumes. Por um lado, representa uma forma de expressão e de luta pela justiça social, pela transparência e pelos direitos humanos. Por outro lado, tornou-se uma arma utilizada pelos Estados para desenvolver campanhas de desestabilização política e de desinformação.

A utilização de ciberataques para fins geopolíticos pôs em evidência a linha ténue entre o ativismo e a cibercriminalidade patrocinada pelo Estado. Este artigo procura analisar a evolução do hacktivismo e a sua relação com os governos, bem como o papel dos grupos de Ameaças Persistentes Avançadas (APT) na utilização do ciberespaço para fins políticos e militares . [1]

Através de uma análise de casos concretos, será explorada a colaboração (ou instrumentalização) dos hacktivistas pelos Estados, as implicações desta prática e o seu

[1] Grupos de ciberatacantes frequentemente associados a Estados-nação ou a grandes organizações criminosas, altamente sofisticados e persistentes, que se infiltram nas redes durante longos períodos de tempo para espionagem ou sabotagem e que dispõem de recursos abundantes (técnicos, económicos) para atacar alvos de elevado valor (governos, grandes empresas) com premeditação e furtividade.

impacto na geopolítica atual. Por fim, será feita uma reflexão sobre o futuro do hacktivismo num mundo cada vez mais interligado, onde a inteligência artificial e outras tecnologias emergentes poderão redefinir o papel destes actores no ciberespaço.

O hacktivismo já não é apenas um fenómeno marginal de protesto digital, mas um potencial risco de segurança para os Estados. Compreender a sua evolução e implicações é fundamental para analisar o futuro da cibersegurança espanhola.

2. DO PROTESTO SOCIAL À GUERRA CIBERNÉTICA

O hacktivismo sofreu uma transformação notável desde as suas origens, passando de uma forma de protesto social a uma ferramenta utilizada pelos governos para apoiar uma agenda política. Se pensarmos bem, esta transformação trai as origens e a própria essência do ativismo, e é por isso que, antes de analisarmos o papel desempenhado pelo hacktivismo como uma ferramenta ao serviço do Estado, acreditamos que é necessário olhar para a forma como este fenómeno evoluiu desde as suas origens.

Em certas abordagens contemporâneas, nomeadamente as orientadas para a sistematização terminológica, existe uma tendência para estabelecer uma relação hierárquica entre ciberactivismo e hacktivismo, entendendo o primeiro como um fenómeno mais amplo e englobando necessariamente o segundo como uma manifestação específica ou variante radicalizada. Esta leitura, presente tanto na literatura popular como em alguns quadros analíticos normativos, considera que o ciberactivismo representa a utilização das tecnologias digitais para a promoção de causas sociais, políticas ou culturais através de campanhas de sensibilização, petições em linha ou protestos virtuais. O hacktivismo, por outro lado, caraterizar-se-ia pela utilização de ferramentas de hacking - como ataques distribuídos de negação de serviço (DDoS), violações de dados ou alteração de sítios Web - para fins semelhantes, embora por meios mais perturbadores ou mesmo ilícitos.

No entanto, esta interpretação, embora generalizada, é problematicamente reducionista e não resiste a um exame mais atento da teoria histórica e crítica dos movimentos digitais. Em primeiro lugar, o pressuposto de uma evolução linear e progressiva - do ciberactivismo "moderado" ao hacktivismo "radical" - ignora as trajectórias históricas distintas dos dois conceitos. O hacktivismo, longe de ser uma derivação tardia do ciberactivismo, surge simultaneamente e até mais cedo em certos contextos, com raízes na cultura hacker das décadas de 1980 e 1990, e articulado em torno de princípios como a liberdade de informação, o acesso aberto ao conhecimento e a desobediência civil no ciberespaço (Jordan & Taylor, 2004; Coleman, 2014).

De facto, o termo "hacktivismo" surge da combinação etimológica de "hacker" e "ativismo", descrevendo a utilização de conhecimentos informáticos para promover causas políticas ou sociais; e as suas raízes remontam a meados da década de 1990, quando grupos como o "*Culto da Vaca Morta*" (uma referência ao matadouro do Texas onde o grupo realiza as suas reuniões) defendiam o acesso universal à informação em linha como um direito humano fundamental e a luta contra governos opressivos .[2]

[2] O sítio Web de "O Culto da Vaca Morta" pode ainda ser consultado em: https://cultdeadcow.com/about.html

"Cult of the Dead Cow", considerado um dos fundadores do hacktivismo moderno, não só divulgou manifestos críticos do controlo estatal e empresarial da Internet, como também desenvolveu ferramentas com uma clara vocação disruptiva. Entre elas está o *Back Orifice* (1998), um software concebido para expor vulnerabilidades no sistema operativo Windows e denunciar deficiências na privacidade dos utilizadores[3] . Um ano mais tarde, em 1999, vários dos seus membros promoveram o projeto *Hacktivismo,* um ramo explicitamente orientado para a luta contra a censura digital que deu origem ao desenvolvimento de ferramentas como o *Six/Four* ou *o Peekabooty*, concebidas para contornar os filtros impostos por regimes autoritários e facilitar o livre acesso à informação.

Na ideologia *do Culto da Vaca Morta*, o acesso à informação online não era apenas um direito fundamental, mas também um campo de contestação política que exigia formas inovadoras de intervenção técnica e simbólica. No entanto, estas acções, embora não violentas em termos físicos, implicavam um confronto direto com a legislação restritiva sobre a utilização da rede e a propriedade intelectual; por outras palavras, revelavam o carácter ambíguo do hacktivismo.

Por outro lado, concetualizar o hacktivismo como uma simples intensificação tática do ciberactivismo faz-nos perder de vista as divergências ideológicas e epistemológicas entre ambos. Enquanto o ciberactivismo tende a enquadrar-se na lógica da participação dos cidadãos, da advocacia institucional e da utilização estratégica das redes sociais, o hacktivismo opera frequentemente através do antagonismo direto, da resistência às estruturas de poder e do questionamento dos quadros legais existentes.

Embora possa ser útil pensar o hacktivismo como uma subcategoria do ciberactivismo a partir de certas abordagens descritivas, é epistemologicamente insuficiente e empiricamente questionável quando se aborda a genealogia, o enquadramento normativo e as implicações ético-políticas de ambas as formas de ativismo digital. Neste artigo, centrar-nos-emos apenas na evolução do hacktivismo, entendido como um fenómeno em si mesmo, deixando de lado a formulação de uma revisão crítica desta classificação.

Nas fases iniciais do hacktivismo, o principal objetivo era levar a cabo ataques contra entidades governamentais e empresariais como forma de protesto contra a censura e as injustiças sociais. Estas mensagens tornaram-se mais intensas à medida que o movimento anti-globalização de meados da década de 1990 emergiu na cena social (Auty, 2004).

Um marco fundamental na consolidação do hacktivismo como ferramenta de confronto político foi a guerra do Kosovo, na década de 1990 (frequentemente descrita como a primeira guerra travada em linha), em que os contendores não só partilharam informações e testemunhos sobre a guerra em linha, como também difundiram propaganda e desinformação. *Os hackers* chegaram mesmo a intervir ativamente no conflito, desfigurando sítios Web do governo e executando ataques de negação de serviço contra as infra-estruturas em linha do lado oposto (Denning, 2001).

[3] Embora inicialmente concebida como uma ferramenta de auditoria de segurança, a sua criação gerou alguma controvérsia e foi vista como uma ameaça pela indústria tecnológica.

Académica e socialmente, os movimentos hacktivistas eram vistos como a expressão natural de um ativismo político pré-existente que tinha encontrado numa nova ferramenta (a Internet) a possibilidade de empregar um tipo de ativista com um perfil técnico para difundir as suas mensagens de uma forma mais mediática (Jordan, 2002).

No entanto, o manifesto desrespeito pelas normas estabelecidas, as designações escolhidas pelos grupos (*The Legion of Doom*, *Bad Ass Mother Fuckers*, *Toxic Shock*, etc.) e o contexto de insegurança social aberto pelos atentados de 11 de setembro, fizeram com que um fenómeno que inicialmente era visto de forma positiva começasse a suscitar alguma desconfiança. (Torres Soriano, 2018).

A figura do *hacker* começou a ser identificada com a do criminoso e, por extensão, num contexto geopolítico marcado pela luta contra o Terror, com a do ciberterrorista. E as acções hacktivistas passaram a ser identificadas fundamentalmente como uma nova forma de participação política ilegítima, recorrendo a ciberataques para levar a cabo sabotagem e ciberespionagem (Vegh, 2005).

No plano académico, a identificação do hacktivismo com o ilegal ou criminalizável, frequente em certos discursos, reduz o hacktivismo a uma "forma radical de ciberactivismo", empobrecendo assim a capacidade de análise e explicação das ciências sociais face à complexidade das práticas políticas digitais contemporâneas.

O início desta década reflecte um hacktivismo marcado pelo desejo dos seus membros de transgredir as convenções sociais por prazer. De facto, as raízes do grupo hacktivista mais conhecido (Anonymous) remontam ao fórum japonês *2chan*, onde a comunidade virtual se dedicava a partilhar todo o tipo de conteúdos aberrantes relacionados com anime, pornografia e piadas práticas (Bartlett, 2015).

No entanto, por volta de 2003, surgiram as primeiras tensões internas numa comunidade virtual que tinha encontrado no fórum *4chan* o local ideal para se divertir sem se importar com as consequências. Precisamente neste fórum, alguns utilizadores (conhecidos como *moralfags*) propuseram concentrar as suas actividades em causas mais transcendentais, como a luta contra a censura na Internet, para limpar a imagem do hacktivismo e representar a defesa da liberdade de expressão, da transparência e de outros direitos civis.

Sob o lema "*Somos Anónimos. Somos a Legião. Nós não perdoamos. Nós não esquecemos. Esperem por nós*" e a máscara de Guy Fawkes, surgiu um coletivo descentralizado de activistas que combinou a exfiltração de informação e os ataques DDoS para reivindicar a luta contra a corrupção, a censura e os abusos de poder.

Por parte do poder, o Anonymous foi rapidamente interpretado como uma premonição do risco representado por uma nova geração de actores virtuais motivados, com uma estrutura sem líderes e uma operação baseada no voluntarismo e na espontaneidade (Olson, 2012). No entanto, só quando o coletivo começou a apoiar as acções da WikiLeaks é que o grupo passou a ser visto como uma ameaça cibernética de alto nível.

Em pouco tempo, os Anonymous passaram de um pequeno grupo de *hackers* com ideias políticas para um movimento global com milhares de seguidores em todo o mundo.

No entanto, a sua atração não residia numa ideologia estruturada ou num programa de ação definido. Para além da sua posição anti-establishment, que os levou a denunciar a manipulação e o controlo exercidos pelos governos e pelas empresas, a sua filosofia carecia de uma orientação clara sobre a forma como a política, a sociedade ou a economia deveriam ser organizadas. Isto fez do Anonymous um fenómeno difícil de classificar, uma vez que a sua identidade se baseava mais na ação e no protesto do que numa agenda concreta para a mudança (Torres Soriano, 2018).

Sob a máscara de Guy Fawkes reuniram-se indivíduos que certamente acreditavam apoiar uma mudança social positiva, mas também outros: aqueles cuja inspiração era a destruição niilista do mundo tal como o conhecemos e aqueles que procuravam esconder-se sob a bandeira do Anonymous para obter ganhos políticos ou económicos.

Do principal legado dos Anonymous - transformar o hacktivismo numa prática popular que transcendeu a esfera *dos hackers* - surge uma nova era de hacktivistas que operam numa paisagem de fragmentação e complexidade, onde coexistem múltiplos actores com motivações diversas.

Atualmente, embora grupos como os Anonymous continuem a operar de forma descentralizada, o seu impacto diminuiu em comparação com o boom que atingiram no início da década de 2010. Ao mesmo tempo, surgiram novas gerações de hacktivistas que, embora tenham um nível inferior de conhecimentos técnicos, compensam com a utilização de ferramentas de automatização e um domínio do impacto mediático e da mobilização social.

Atualmente, o hacktivismo é utilizado tanto por colectivos independentes que denunciam a injustiça como por grupos patrocinados pelo Estado que instrumentalizam estas tácticas para fins geopolíticos. O conflito entre a Rússia e a Ucrânia pôs em evidência a existência de uma guerra cibernética, com hacktivistas pró-ucranianos e pró-russos a levarem a cabo ataques coordenados em benefício dos respectivos lados.

A fronteira entre o ativismo digital legítimo, o cibercrime e as operações secretas dos serviços secretos é cada vez mais ténue. No entanto, podemos considerar que existem atualmente três tipos de hacktivistas: os ciberterroristas, *os hackers* cívicos e *os hackers* patrióticos (Dahan, 2013; Denning, 2001; Johnson e Robinson, 2014; Sauter, 2013).

O ciberterrorismo incluiria todas as acções hostis no ciberespaço destinadas a perpetrar actos de violência contra pessoas ou bens, com o objetivo de intimidar ou coagir governos ou sociedades a atingir fins políticos, religiosos ou ideológicos específicos. As suas acções envolvem principalmente a propagação de vírus e *malware*, a vandalização de *sítios Web* e a realização de ataques de negação de serviço (DDoS) ou *botnet* (Denning, 2001; Jordan e Taylor, 2004; Goode, 2015).

Na categoria de *hackers* cívicos encontraríamos todos os grupos organizados que realizam acções contra sistemas informáticos com o objetivo de contribuir com algum bem para a comunidade, geralmente na fronteira da legalidade (Hunsinger e Schrock, 2016; Schrock, 2016).

Por último, *os hackers* patrióticos são os indivíduos ou grupos cujos esforços estão alinhados com a ideologia nacionalista e são considerados uma "milícia cibernética" em busca de interesses específicos (Dahan, 2013; Green, 2016). Embora de fora estes *hackers* possam não parecer diretamente patrocinados por qualquer Estado, podemos agora inferir que são instrumentalizados como parte de uma rede mais vasta de forças estatais.

O hacktivismo patriótico teve origem na China, na década de 1990, em resposta a motins anti-chineses na Indonésia e, desde então, tem sido utilizado como tática pela China, Rússia, Síria e outros Estados como forma de prejudicar os seus inimigos no domínio cibernético. No entanto, nenhuma das operações anteriores à guerra da Ucrânia atingiu a escala, o impacto e os laços governamentais tão robustos e prolongados, nem transgrediu de forma tão flagrante as normas internacionais, como o hacktivismo contemporâneo (Healey & Grinberg, 2022).

3. O NEXO ENTRE O HACKTIVISMO E A APT

Ao longo da história, os Estados têm recorrido a actores por procuração para levar a cabo as suas estratégias de conflito sem envolver diretamente as suas forças armadas. Unidades auxiliares, grupos mercenários, insurreições, organizações terroristas ou empresas militares privadas (PMC) são apenas algumas das formas que os terceiros actores assumiram para substituir a ação estratégica dos Estados.

Por isso, não é de estranhar que hoje, perante uma sociedade cada vez mais digitalizada, a ação do Estado tenha encontrado nos grupos hacktivistas um novo ator para personificar a exteriorização da autoria e no ciberespaço o ambiente ideal para projetar influência geopolítica.

O conceito de *guerra de substituição* tem sido objeto de um amplo debate na comunidade académica e de segurança, sobretudo devido à dificuldade de o diferenciar da guerra *por procuração*, dada a natureza intimamente ligada dos dois conceitos.

Em ambos os casos, os objectivos do ator principal (o Estado) e do agente substituto coincidem. No entanto, enquanto na *guerra por procuração* existem dois ou mais atores hierarquicamente relacionados (o ator principal trabalha para, com e através do ator por procuração para atingir um objetivo comum), na *guerra de substituição* estes atores só estão alinhados se o ator principal conseguir mobilizar o apoio adequado exigido pelo ator por procuração (Fox 2019). Por outras palavras, os conceitos de *guerra de substituição* e *de guerra por procuração* diferem consoante a relação entre os atores e as suas motivações.

Uma vez que os grupos hacktivistas têm pouca independência para resistir ao controlo do Estado que os patrocina (ou que, pelo menos, os influencia ou tolera), no nosso estudo de caso falaremos em termos de actores *por procuração*.

Mais especificamente, para nos referirmos a eles, utilizaremos a definição de "*proxy* actors" de Rondeaux e Sterman (2019), que os definem como "*sujeitos fora da estrutura de segurança dos Estados envolvidos num conflito que agem sob o patrocínio direto ou indireto de um ator convencional (um Estado)*"; e a definição de Maurer (2018) de *cyber proxies* como "*intermediários que realizam acções ofensivas no ciberespaço em benefício de um ator principal*".

Historicamente, *os ciberproxies* têm sido personificados através de várias entidades ligadas ao mundo da cibercriminalidade e da ciberespionagem. No entanto, o termo engloba um grande número de entidades organizadas que, direta ou indiretamente, constituem um fator de risco para as empresas e os Estados. De facto, a lista de actores é muito extensa: grupos criminosos, *actores ofensivos do sector* privado (PSOA), grupos terroristas, insurrectos, insurgentes, hacktivistas, actores estatais ou APTs são apenas alguns deles.

As razões subjacentes à sua utilização são variadas: (1) a utilização de actores *por procuração* pelos governos reduz o risco de escalada dos conflitos, uma vez que a dificuldade de atribuir a responsabilidade por um ciberataque é complexa; (2) existe a possibilidade de uma negação plausível que desvia a responsabilidade de um ataque para um ator fora do controlo do governo; (3) ajuda os Estados a prolongar a situação de tensão nos conflitos, desgastando o adversário a nível social, político e económico; (4) permite que os Estados actuem à margem das regulamentações internas e das críticas de sectores governamentais adversários - ou mesmo da própria opinião pública nas democracias; (5) dá aos Estados rapidez e flexibilidade na resposta às acções ofensivas dos seus adversários, uma vez que não requer provas técnicas ou legitimação pública; (6) oferece aos Estados um instrumento adicional de dissuasão; (7) permite aos Estados contornar a aplicação do direito internacional; (8) facilita a utilização de pessoal especializado sem a necessidade de oferecer recrutamento legal; (9) possibilita a participação em conflitos internacionais que, de outra forma, seriam económica e politicamente incontroláveis (Torres Soriano, 2017; Expósito Guisado, 2024; Marín Gutiérrez, 2023).

No entanto, a obtenção destes benefícios não é isenta de problemas. De facto, o principal atrativo da utilização de um *proxy* (que não é outro senão a obtenção de uma negação plausível de uma agressão) é também a sua principal fraqueza, uma vez que o anonimato e a clandestinidade diluem a capacidade coerciva e dissuasora do Estado patrocinador - afinal, não podemos ignorar as teorias de Clausewitz que sugerem que para um Estado modificar a sua conduta com base na vontade de outro, este último tem de conhecer a origem do ato de coerção a que foi submetido.

Outro inconveniente da utilização de *ciberproxies* reside na forma como o Estado os seleciona e controla quando são utilizados. A existência de interesses divergentes entre as duas partes pode levar à deslealdade do *proxy*, causando prejuízos económicos ou políticos ao ator que o utiliza - facto que é agravado se tivermos em conta que estes *proxies* operam geralmente em áreas onde o Estado não pode nem quer intervir.

A vantagem dos *mandatários* reside na sua capacidade de atuar de forma dissimulada, embora seja precisamente esta falta de transparência que limita o patrocinador estatal na verificação dos seus antecedentes e fiabilidade. A literatura académica salienta que o controlo sobre os *mandatários* é ainda mais complicado se o Estado não dispuser de mecanismos eficazes para sancionar a deslealdade, ou se existirem estruturas descentralizadas que impeçam a aplicação adequada de ordens hierárquicas (Popovic 2015).

Neste artigo, vamos concentrar-nos apenas em dois actores que representam os dois pólos diferentes (ativismo aberto e espionagem silenciosa) do mesmo fenómeno, mas que não são assim tão diferentes em termos dos fins que perseguem e da sua instrumentalização pelos Estados.

Em termos gerais, o hacktivismo e as APT diferem em termos de motivação, métodos e grau de apoio estatal. Assim, enquanto o hacktivismo é motivado por um contexto político-social (protesto, ativismo, causas morais), as APT centram-se na espionagem estratégica e na obtenção de uma vantagem económico-militar.

Operacionalmente, as APT actuam de forma furtiva e persistente, recorrendo a *malware* personalizado, backdoors e movimentos laterais, ao contrário das acções de hacktivismo, que normalmente procuram chamar a atenção do público e se concentram em ataques DDosS de curta duração.

No entanto, não é raro observar como as APT actuam temporariamente como hacktivistas (quando divulgam publicamente os dados que exfiltram para provocar um impacto político) e como os hacktivistas são instrumentalizados pelos Estados para atingir os seus objectivos estratégicos.

A nível organizacional, os hacktivistas e as APT também diferem: os hacktivistas agem geralmente de forma descentralizada, espontânea, mesmo anónima, e sem um comando unificado. As APT, por outro lado, são geralmente equipas estruturadas, muitas vezes integradas numa organização maior (um exército, uma agência de informações ou um grupo criminoso), com uma hierarquia definida e um financiamento consideravelmente mais poderoso (CyberZaintza, 2021).

De facto, a diferença de recursos e de formação técnica sugere uma ligação mais estreita entre as APT e os Estados do que entre os grupos de hacktivistas. No entanto, as linhas que separam os dois conceitos foram recentemente esbatidas pela constatação de que alguns grupos de hacktivistas pró-russos têm recebido apoio estatal encoberto ou actuam de acordo com a agenda do Estado, esbatendo a distinção até agora clara entre "*hackers* activistas" e "agentes do Estado" (Muncaster, 2024).

De facto, não se pode excluir que certos grupos de hacktivistas sejam realmente formados ou apoiados por APT ou diretamente por actores estatais. Um exemplo é o "XakNet Team", o "Infoccentr" e o "CyberArmyofRussia_Reborn", grupos hacktivistas pró-russos que, segundo a Mandiant, são agentes de ciberameaças patrocinados pela Direção Principal dos Serviços Secretos russos (GRU) através da APT44 (Mandiant, 2022).

Na última década, foram documentados vários casos em que os Estados utilizaram os seus próprios grupos APT e colectivos de hacktivistas (ou as suas identidades) para levar a cabo ciberespionagem, sabotagem de conflitos e manipulação política.

Um exemplo paradigmático que ilustra a interdependência de ambos os conceitos pode ser encontrado nas eleições de 2016 nos EUA, quando "*DCLeaks*" e "*Guccifer 2.0*", duas identidades ligadas à Direção Principal de Inteligência da Rússia (*Glavnoe Razvedyvatel'noe Upravlenie*, GRU), roubaram e-mails do Partido Democrata e os divulgaram fazendo-se passar por "hacktivistas patrióticos americanos" (DOJ, 2018).

No rescaldo da guerra na Ucrânia, não é raro encontrar interdependência entre hacktivistas russos e APT, grupos como *Killnet, NoName057(16), Anonymous Sudan* que atacaram sítios Web governamentais e empresas ocidentais em apoio da narrativa do Kremlin mostram que, embora estes grupos se autodenominem "activistas espontâneos",

agem de forma suspeita em coordenação com a ação do Estado russo (Van Der Walt, 2025).

No entanto, a Rússia não é o único ator estatal que recorre às APT e aos hacktivistas para fazer valer o seu poder. Há anos que outros Estados, como a China, a Coreia do Norte ou o Irão, são acusados de conduzir desta forma as suas actividades ofensivas no ciberespaço.

Concretamente, a China é acusada há anos de patrocinar vastas campanhas de ciberespionagem através de unidades militares e *hackers* pagos, como os do grupo APT1, considerado pela Mandiant em 2013 como a Unidade 61398 do Exército Popular de Libertação da China.

As operações APT chinesas tendem a centrar-se em alvos estratégicos (aeroespacial, energia, telecomunicações, defesa, etc.) e são consideradas parte dos serviços secretos do Estado chinês, mas, ao contrário da Rússia, o recurso ao hacktivismo não é tão proeminente nas estratégias chinesas.

O governo tolerou e até inspirou "*hackers* patrióticos" chineses em alguns conflitos, sendo um exemplo a "*Honker Hacker Network*", uma comunidade de *hackers* fora do controlo do governo - de acordo com fontes chinesas - que atacou actores adversários da China durante disputas territoriais ou incidentes diplomáticos.

O Irão, por outro lado, tem mostrado uma tendência para instrumentalizar grupos *de hackers* supostamente activistas para levar a cabo operações de retaliação contra os seus adversários, ao mesmo tempo que desenvolve as suas próprias APT. Um exemplo significativo deste facto foram os ataques DDoS contra bancos norte-americanos em 2012-2013, em retaliação contra as sanções ocidentais: uma entidade que se dizia hacktivista religiosa e se intitulava "*Cyber Fighters of Izz ad-Din al-Qassam*" reivindicou a autoria da ofensiva, invocando a indignação contra um vídeo anti-islâmico (CFR, 2012).

Os serviços secretos americanos concluíram posteriormente que se tratava de uma operação orquestrada pelo Irão (provavelmente a sua Guarda Revolucionária) em resposta às medidas tomadas contra o seu programa nuclear. De facto, em 2016, o Departamento de Justiça dos EUA indiciou sete iranianos ligados à Guarda Revolucionária Islâmica (IRGC) por estes ataques.

Outro exemplo é o ataque "*Shamoonj*" de 2012 do "*Cutting Sword of Justice*", um alegado grupo hacktivista que apagou dados de 30 000 computadores da empresa petrolífera saudita Aramco, mas que os analistas atribuíram mais tarde a uma operação estatal iraniana em resposta à ofensiva *Stuxnet* e às tensões regionais.

A Coreia do Norte, apesar do seu isolamento, também conseguiu criar uma das ciberameaças mais activas, principalmente para angariar fundos e desestabilizar os seus adversários geopolíticos. O seu grupo APT mais notável, o *Lazarus Group* (ligado ao APT38), roubou centenas de milhões através de ataques a bancos.

Outro caso que ilustra a instrumentalização de campanhas activistas pelos Estados pode também ser encontrado numa das suas acções, a *pirataria* informática da Sony Pictures em 2014, quando um grupo chamado "*Guardians of Peace*" exfiltrou dados

confidenciais e destruiu sistemas da Sony em aparente retaliação pelo filme satírico sobre o líder norte-coreano "*The Interview*". (FBI, 2014).

A Coreia do Norte é o paradigma da instrumentalização direta, *os* seus *hackers* são agentes do Estado que, por vezes, assumem os nomes de grupos fictícios para disseminar as suas mensagens ou justificar os seus ataques, mas, ao contrário de outros Estados, os norte-coreanos eliminam completamente a distinção entre APT e aparelho de Estado, mantendo a cobertura apenas na narrativa pública para o mundo exterior.

Por seu lado, as potências ocidentais também empregam, obviamente, capacidades cibernéticas ofensivas para atacar outros Estados. Talvez o caso mais relevante seja a operação "Jogos Olímpicos" atribuída às agências NSA e à unidade 8200 (não oficialmente reconhecida), na qual os EUA e Israel desenvolveram o malware *Stuxnet* para sabotar as centrifugadoras nucleares do Irão por volta de 2010 (The Guardian, 2017).

No entanto, no Ocidente, embora existam entidades APT apoiadas por Estados para atuar ofensivamente em campanhas de espionagem, a instrumentalização de grupos hacktivistas para esconder as suas acções é praticamente inexistente. De facto, só encontramos um caso em que um grupo hacktivista ocidental associa a sua atividade à capacidade ciber-ofensiva de um Estado: o "*IT Army of Ukraine*".

Este caso é particularmente controverso, uma vez que o apoio público do governo ucraniano viola abertamente as normas recentemente acordadas sobre a conduta dos Estados no ciberespaço, bem como as posições de política externa dos membros da NATO (Healey e Grinberg, 2022).

Se utilizarmos a tabela "Spectrum of Responsibility" de Healey e Grinberg (2022), que correlaciona a atividade dos grupos de acordo com o grau de responsabilidade do Estado pela sua *representação cibernética*, podemos ver como o apoio do governo ucraniano ao *IT Army of Ukraine* começou pelo menos como "coordenado pelo Estado (nível 6)", (quando o Ministro ucraniano da Transformação Digital, Mikhail Fedorov, apelou abertamente a voluntários hacktivistas de todo o mundo para apoiarem a Ucrânia na frente digital) e até "encorajado pelo Estado (nível 4)".

Quadro 1: *Espectro da responsabilidade do Estado.*

Posição do Estado	Relação *Estado-Procurador*
1. Proibido pelo Estado.	O governo nacional ajudará a travar uma ataque de terceiros.
2. Proibição estatal mas inadequada.	O governo nacional coopera, mas é incapaz de impedir o ataque de terceiros.
3. Ignorado pelo Estado.	O governo nacional está ciente dos ataques de terceiros, mas não está disposto a tomar nenhuma ação oficial.
4. Patrocinado pelo Estado.	Terceiros controlam e dirigem o ataque, mas o governo nacional promove-os como um questão política.
5. Moldado pelo Estado.	Terceiros controlam e dirigem o ataque, e o O Estado presta algum apoio.
6. Coordenado pelo Estado.	O governo nacional coordena o ataque através de terceiros, por exemplo, sugerindo pormenores operacional.
7. Obrigatório pelo Estado.	O governo nacional ordena a terceiros que realizar o ataque em seu nome.
8. Gerido, mas não reconhecido pelo Estado.	Elementos fora do controlo das forças ataques cibernéticos do governo nacional levam a ataque ordenado.
9. Implementado pelo Estado.	O governo nacional efectua o ataque utilizando forças cibernéticas sob a sua controlo direto.
10. Integrado no Estado.	Ataques do governo nacional utilizando proxies e forças cibernéticas incorporadas governamental.

(Healey, 2022).

É sobretudo nos conflitos geopolíticos que vemos a convergência mais acelerada entre o hacktivismo e as operações estatais. No caso da guerra ucraniana, três anos após o início do conflito e apesar de o número de actores hacktivistas ter diminuído consideravelmente (de mais de 130 grupos em 2024 para apenas cerca de 80 grupos em 2025), podemos ainda observar como ambos os lados mantêm um cruzamento de ciberataques destrutivos, coordenados com a sua campanha militar e apoiados nas suas acções por "hackers patrióticos" (Cyberknow, 2025).

Do lado ucraniano, o *IT Army of Ukraine* continua a ser a força hacktivista mais importante da Ucrânia, continuando a mobilizar voluntários dentro e fora do país para atacar infra-estruturas russas, realizar contra-propaganda e apoiar missões de informação. No período de 2023-2024, é-lhe atribuída, por exemplo, a tarefa de derrubar temporariamente os serviços de Internet nas zonas ocupadas pela Rússia e de lançar continuamente campanhas de DDoS contra entidades russas de alto nível (Optiv, 2023).

Do lado pró-russo, o grupo mais proeminente neste momento é o *NoName057(16)*, um grupo ligado ao GRU, que actua em coordenação com a agenda do Kremlin,

selecionando alvos de acordo com os interesses estratégicos russos e considera-se uma espécie de "braço ciberespontâneo" permanente dos militares russos.

Quadro 2: *Casos cronológicos de instrumentalização do hacktivismo pelo Estado.*

Ano	***Estado***	***Grupo hacktivista***	***Caraterística***	***Nível de ligação ao Estado (Healey & Grinberg).***
1998-1999	Kosovo	Hackers patriotas	Primeiro conflito com uma intervenção notável de hacktivistas.	Ignorado / Espontâneo
1999	China	Buzina vermelha	Hackers patrióticos activos em conflitos territoriais. Campanhas de espionagem industrial e ciberataques a infra-estruturas críticas.	Incentivado / Moldado
2012-2013	Irão	Combatentes cibernéticos do Izz ad-Din al-Qassam	Ataques DDoS contra bancos americanos em retaliação às sanções. Operação Shamoon contra a Aramco com eliminação em massa.	Coordenado / Ordenado
2014	Coreia do Norte	Grupo Lazarus	Ciberataques para obter financiamento estatal. Ataque à Sony Pictures (2014) como retaliação simbólica.	Implementado / Integrado
2022-presente	Rússia	Killnet/ Cyber Army of Russian Reborn/ NoName057(16)	Os grupos hacktivistas coordenaram-se com a estratégia russa na guerra da Ucrânia. Ataques DDoS.	Coordenado / Incentivado
2022-presente	Ucrânia	Exército informático da Ucrânia	Apelo público do Governo ao hacktivismo contra a Rússia. DDoS, sabotagem e propaganda pró-ucraniana.	Coordenado / Incentivado

4. O FUTURO DOS GRUPOS HACKTIVISTAS.

A sobrevivência dos grupos de hacktivistas indica que o hacktivismo integrado na guerra veio para ficar, pelo menos enquanto durar o conflito subjacente e os Estados em conflito

considerarem útil esta camada de ação descentralizada. Além disso, o panorama atual dos hacktivistas leva-nos a observar que o hacktivismo está a ir além do DDoS e a entrar em ataques APT mais sofisticados, como os ataques a infra-estruturas críticas SCADA e a sistemas de controlo industrial (ICS) . [4]

O facto de grupos pertencentes ao ecossistema hacktivista pró-russo, como a *Z-Pentest Alliance* ou o *Setor 16,* terem vindo a intrometer-se ativamente em centrais eléctricas, instalações de água potável e indústrias em geral, reflecte não só uma maturação e uma estadualização do fenómeno hacktivista, mas também a existência de riscos físicos crescentes das suas acções (Antoniuk, 2024).

A redução do número de grupos hacktivistas no ambiente pró-russo sugere que a efervescência inicial deu lugar a um processo de seleção natural em que sobrevivem os grupos com melhor apoio, organização e proteção. Um fenómeno que se traduz em operações mais eficazes e coordenadas, mas também mais previsíveis, uma vez que estão alinhadas com a agenda do Estado russo.

Ao mesmo tempo, a persistência de ataques diários indica que a guerra cibernética de baixa intensidade se tornou uma rotina. O DDoS constante mantém a pressão psicológica e de propaganda sobre as populações-alvo (lembretes diários da presença do conflito), enquanto a adoção de *ransomware* e os ataques a indústrias aumentam o potencial de danos reais a infra-estruturas críticas, esbatendo a linha entre o hacktivismo e o ciberterrorismo - um facto que pode, em última análise, levar a respostas mais enérgicas por parte dos Estados vítimas e a uma potencial escalada do conflito.

Outro desenvolvimento relevante é o desenvolvimento notável de alianças emergentes entre causas hacktivistas que transcendem o teatro de operações para além da Ucrânia e envolvem países terceiros. Um exemplo é a recente aliança entre hacktivistas pró-russos e pró-palestinianos, que une causas geopolíticas aparentemente distintas sob uma narrativa comum de ataque ao Ocidente.

As tensões globais de 2024 (incluindo a guerra de Gaza) criaram uma estranha frente unida de hacktivistas. Grupos russos (especialmente *NoName057(16)*) começaram a coordenar operações com colectivos ligados ao Médio Oriente (como *Mr. Hamza* ou *Anonymous Guys*) e sincronizaram os seus ataques sob a bandeira da união da "*Santa Liga*" contra países que consideravam adversários comuns, como a França.

Este tipo de aliança é bem conhecido em Espanha, e particularmente pela Guardia Civil, uma vez que, em julho de 2024, a instituição foi o alvo direto de uma campanha conjunta de ciberataques, "*#FuckGuardiaCivil*", que respondeu a uma iniciativa promovida pelo grupo *NoName057(16),* para "se vingar das autoridades espanholas" que tinham detido três pessoas em Manacor (Maiorca), Huelva e Sevilha por suspeita de participação em ciberataques contra entidades públicas e empresas estratégicas em Espanha e noutros países da NATO.

[4] Sistema centralizado para monitorizar, controlar e recolher dados de processos e dispositivos em tempo real.

De facto, em abril de 2025, já estava registada uma nova aliança, incluindo os grupos *Keymous+, Mr Hamza, Alixsec e NoName057(16),* para atacar a Polónia, a Alemanha, a França, a Itália e a Espanha sob o lema "*Operação Hack For Humanity V2!*

Só em Espanha, no primeiro dia da campanha "Operação Hack For Humanity V2!", foram registados mais de 30 ataques a empresas e sítios Web governamentais, sendo *o Sr. Hamza*, o *NoName057(16)*, o *TwoNet* e *o Keymous+* os grupos mais activos no ataque.

A frequência com que esta convergência tem vindo a ocorrer nos últimos meses mostra que o fenómeno está a tornar-se cada vez mais internacional e interligado. As alianças entre grupos hacktivistas tornaram-se solidárias, transcendendo as fronteiras do conflito russo-ucraniano com um único objetivo: expandir as suas acções para o inimigo comum ocidental.

O facto de países da NATO como a França, a Itália ou a própria Espanha se poderem tornar alvos de *piratas* informáticos patriotas russos pode levar a uma escalada do conflito, especialmente se um dos seus ataques danificar gravemente infra-estruturas críticas, a guerra cibernética de baixa intensidade pode atrair uma resposta mais forte do que o habitual.

5. CONCLUSÕES

A análise do hacktivismo e da sua relação com os Estados mostra que este fenómeno evoluiu do protesto digital para uma instrumentalização estatal com implicações geopolíticas e estratégicas. A fronteira entre ativismo, cibercrime e operações estatais é cada vez mais ténue, especialmente em conflitos como a guerra na Ucrânia, onde se tem observado uma crescente instrumentalização de grupos hacktivistas por forças governamentais na defesa dos seus interesses nacionais.

Com efeito, o conflito entre a Rússia e a Ucrânia marcou um ponto de viragem na utilização do ciberespaço como campo de batalha, em que tanto os intervenientes estatais como não estatais se envolveram ativamente em ataques de negação de serviço (DDoS), ciberespionagem e sabotagem de infra-estruturas críticas.

Este estudo, desenvolvido através do estudo dos casos mais proeminentes na cena internacional, permitiu-nos estabelecer uma distinção entre *hackers* cívicos e *hackers* patrióticos. Enquanto os primeiros abraçam causas niilistas ou socialmente conflituosas, os segundos são utilizados pelos Estados como um instrumento encoberto nos conflitos internacionais, o que implica uma externalização das cibercapacidades governamentais e oferece uma série de vantagens estratégicas: negação plausível de responsabilidades, prolongamento de situações de tensão ou redução de custos políticos e económicos.

Em suma, poderíamos dizer que os Estados aprenderam a explorar o hacktivismo como uma arma adicional, quer fingindo ser hacktivistas para desinformar ou exfiltrar dados, quer encorajando os seus simpatizantes a lançar ciberataques em massa contra o seu inimigo.

No entanto, esta instrumentalização coloca sérios desafios a nível estratégico. A sofisticação progressiva dos ataques, que passaram do vandalismo digital para operações mais avançadas contra infra-estruturas críticas, só aumenta seriamente as possibilidades de retaliação por parte dos Estados afectados e aumenta o risco potencial de escalada em conflitos assimétricos.

Além disso, a convergência entre as APT e os hacktivistas põe em causa as normas internacionais existentes, uma vez que os ataques perpetrados por agentes *por procuração* esbatem a responsabilidade do Estado e dificultam a aplicação de medidas de dissuasão ou de retaliação direta. Tanto mais que os colectivos de hacktivistas parecem estar a evoluir para uma nova paisagem de alianças capazes de reunir grupos de hacktivistas com agendas geopolíticas diversas para atacar países ocidentais.

A cibersegurança do Estado tem de se adaptar a uma nova realidade em que os grupos hacktivistas desempenham um papel fundamental na projeção do poder do Estado. As democracias ocidentais, tradicionalmente mais relutantes em utilizar tais tácticas, enfrentam o dilema de como responder eficazmente sem comprometer os seus valores.

A tendência atual não só mostra uma clara evolução do hacktivismo no sentido de uma ligação cada vez maior aos interesses estatais do governo que o apoia, como também reforça a ideia de que o ciberespaço continuará a ser mais importante em conflitos futuros. Casos como o da Rússia, onde grupos como o *Killnet* ou o *NoName057(16)* reivindicaram operações cibernéticas coincidentes com os interesses geopolíticos do Kremlin - sobretudo durante a guerra na Ucrânia -, ou o do Irão, com grupos como o *Tapandegan*, cuja retórica oposicionista não impede suspeitas de coordenação indireta com agendas estatais, exemplificam esta deriva e demonstram um progressivo esbatimento entre actores não-estatais e estatais na esfera digital, onde o hacktivismo deixa de ser exclusivamente uma forma de dissidência cidadã para se tornar, em certos contextos, uma ferramenta informal de projeção do poder estatal.

6. REFERÊNCIAS BIBLIOGRÁFICAS

Antoniuk, D. (2024). *Cybervolk: Hacktivistas da Índia e da Rússia colaboram em ataques de ransomware*. The Record. https://therecord.media/cybervolk-india-hacktivists-russia-ransomware

Antoniuk, D. (2024). *Cybervolk: Hacktivistas da Índia e da Rússia colaboram em ataques de ransomware*. 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). *Ataques de negação de serviço contra bancos dos EUA em 2012-2013*. Conselho de Relações Exteriores (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). *Guerra Rússia-Ucrânia: Atualização dos hacktivistas*. 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. *Conferência Internacional sobre Guerra e Segurança da Informação*, 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. Em J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239-288). RAND Corporation.

DOJ (2018). *Grande júri acusa 12 oficiais dos serviços secretos russos por crimes de pirataria informática relacionados com as eleições de 2016*. Departamento de Justiça dos EUA. https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

Expósito Guisado, J. (2023). *Ciberproxies: APTs como um fator de risco futuro*. Instituto Espanhol de Estudos Estratégicos (IEEE). *Boletim IEEE*, (32), 815-831.

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

Fox, A. C. (2019). *Conflito e a necessidade de uma teoria da guerra por procuração. Journal of Strategic Security, 12*(1), 44-71. JSTOR. www.jstor.org/stable/26623077

Goode, L. (2015). Anonymous e o ethos político do hacktivismo. *Comunicação Popular, 13*(1), 74-86. https://doi.org/10.1080/15405702.2014.978000

Green, K. (2016). A guerra do povo no ciberespaço: Utilização da economia civil da China no domínio da informação. *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). O contratante da NSA divulgou ferramentas de hacking dos EUA por engano, diz Kaspersky. *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). A democratização do hacking e da criação. *New Media & Society, 18*(4), 535-538. https://doi.org/10.1177/1461444816629466

Johnson, P., & Robinson, P. (2014). Civic hackathons: Inovação, aquisição ou envolvimento cívico? *Review of Policy Research, 31*(4), 349-357. https://doi.org/10.1111/ropr.12074

Jordan, T. (2002). *Ativismo! Ação direta, hacktivismo e o futuro da sociedade*. Reaktion Books.

Jordan, T., & Taylor, P. A. (2004). *Hacktivismo e guerras cibernéticas: rebeldes com uma causa?* Psychology Press.

Mandiant (2022). *A ascensão do GRU: os lacaios do Telegram*. https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions

Marín, F. (2023). *Hacktivismo ao serviço do Estado: ciberproxies na Ucrânia*. Documento de opinião. Instituto Espanhol de Estudos Estratégicos (IEEE).

Maurer, T. (2018). *Cyber Mercenaries: The state, hackers, and power [Mercenários cibernéticos: o estado, os hackers e o poder*]. Cambridge University Press.

Muncaster, P. (2024). *Hacktivismo: A evolução das ameaças às organizações*. WeLiveSecurity. https://www.welivesecurity.com/es/cibercrimen/el-hacktivismo-evolucionando-amenazas-organizaciones

Olson, P. (2012). *5 coisas que todas as organizações podem aprender com o Anonymous.* Forbes. http://www.forbes.com/sites/parmyolson/2012/06/05/5-things-every-organization-can-learn-from-anonymous/

OPTIV (2023). *Atualização Rússia/Ucrânia - dezembro de 2023.* https://www.optiv.com/insights/discover/blog/russiaukraine-update-december-2023

Popovic, M. (2015). Fragile proxies: Explaining rebelde defection against their state sponsors. *Terrorismo e Violência Política.* 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 procuração no ciberespaço. *Revista do Instituto Español de Estudios Estratégicos, (9),* 15-36.

(2018). O hacktivismo como estratégia de comunicação do Anonymous ao cibercalifado. *Cuadernos de Estrategia, (197),* 197-224.

Van Der Walt (2025). *Reflexão sobre três anos de guerra cibernética na Ucrânia. 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