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

Article de recherche

HACKTIVISME : DE LA PROTESTATION SOCIALE À L'INSTRUMENTALISATION DE L'ÉTAT

Traduction en français à l'aide de l'IA (DeepL)

Josué Expósito Guisado
Sergent de la Guardia Civil
Doctorant à l'Université Pablo de Olavide
Maîtrise en paix, sécurité et défense par l'Institut de recherche sur la paix, la sécurité et la défense.
Institut universitaire Gutiérrez Mellado (UNED)
jexpgui@gmail.com
ORCID : 0009-0003-4977-3899

Reçu le 18/03/2025
Accepté le 05/05/2025
Publié le 27/06/2025

Citation recommandée : Expósito, J. (2025). Hacktivisme : de la protestation sociale à l'instrumentalisation de l'État. *Logos Guardia Civil Magazine*, 3(2), pp. 101-122.

Dépôt légal : M-3619-2023
NIPO en ligne : 126-23-019-8
ISSN en ligne : 2952-394X

ORCID : 0009-0003-4977-3899

HACKTIVISME : DE LA PROTESTATION SOCIALE À L'INSTRUMENTALISATION DE L'ÉTAT

Résumé: INTRODUCTION. 2. DE LA PROTESTATION SOCIALE À LA CYBERGUERRE. 3. 3. LE LIEN ENTRE HACKTIVISME ET APT. 4. L'AVENIR DES GROUPES HACKTIVISTES. 5. CONCLUSIONS. 6. RÉFÉRENCES BIBLIOGRAPHIQUES.

Résumé : L'hacktivisme est passé d'une forme initiale de protestation numérique à un outil clé dans les conflits géopolitiques contemporains. Ce qui a commencé comme un mouvement décentralisé de défense de la liberté d'expression et de la justice sociale a été progressivement instrumentalisé par les Etats pour exécuter des cyber-attaques, manipuler l'opinion publique et déployer des opérations de désinformation. Ce phénomène s'est particulièrement accentué dans le contexte de la guerre en Ukraine, où la convergence entre les groupes APT (Advanced Persistent Threat) et les hacktivistes patriotes a permis l'exécution d'opérations cybernétiques coordonnées avec les intérêts de l'État. Parallèlement, l'internationalisation de l'hacktivisme a conduit à la formation d'alliances entre des groupes de différentes régions, élargissant ainsi son impact au-delà du conflit russo-ukrainien. Le cyberespace s'est imposé comme une arène idéale pour la confrontation entre États dans un environnement contrôlé. Toutefois, la sophistication croissante des attaques et le ciblage de plus en plus stratégique posent de sérieux défis à la stabilité internationale et à la sécurité des États occidentaux.

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.

Mots-clés : Hacktivisme, APT, cyberproxies, cyberconflits, cyberattaques.

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

ORCID : 0009-0003-4977-3899

ABBREVIATIONS

APT : *Advanced Persistent Threat (menace persistante avancée).*

DDoS : attaque par *déni de service distribué.*

DOJ : *Département de la justice des* États-Unis.

FBI : *Federal Bureau of Investigation (Bureau fédéral d'enquête).*

GRU : Direction principale du renseignement de la Russie (*Glavnoe Razvedyvatel'noe Upravlenie*).

ICS : *Industrial Control Systems (systèmes de contrôle industriel).*

IRGC : *Corps des gardiens de la révolution islamique d*'Iran.

IT Army of Ukraine : IT Army of Ukraine.

NSA : *Agence* nationale *de sécurité des* États-Unis.

PMC : *Private Military Company (société militaire privée).*

PSOA : *Private Sector Offensive Actor (acteur offensif du secteur privé).*

SCADA : *Supervisory Control And Data Acquisition (contrôle de surveillance et acquisition de données).*

Stuxnet : nom du *logiciel malveillant* utilisé dans l'opération "Jeux olympiques".

1. INTRODUCTION

Avec la guerre en Ukraine, le monde occidental est à nouveau confronté à l'impact du réalisme politique. Avant l'invasion de 2022, la grande majorité des analystes occidentaux étaient incapables d'envisager un conflit conventionnel sur la scène internationale tel que celui qui continue de se produire aux portes de l'Europe. Aveuglés par les doctrines de soft power et suivant les paradigmes libéraux de la paix capitaliste ou de la théorie de la paix commerciale, les dirigeants européens ont volontairement ignoré le fait que dans certaines parties du monde, le réalisme politique règne toujours en maître.

Dans un monde de plus en plus numérisé, où il existe une interconnexion virtuelle entre le plan intangible des technologies de l'information et l'espace physique lui-même, il n'est pas surprenant que l'ennemi actuel de l'Europe pose un problème de sécurité. Les États étant de plus en plus dépendants des technologies de l'information, les acteurs hostiles (étatiques et non étatiques) ont de plus en plus de possibilités d'influencer l'environnement politique et géopolitique en déployant des actions dans le cyberespace.

La guerre en Ukraine a non seulement marqué le début d'une opération de harcèlement et de cyberperturbation par des cybermenaces liées au Kremlin, mais elle a également entraîné un changement dans le paysage mondial de l'hacktivisme : ce qui, il n'y a pas si longtemps encore, était le bastion de la défense de la liberté d'expression, de la vie privée, de la justice sociale et des droits de l'homme, est aujourd'hui un outil aux implications stratégiques et, dans de nombreux cas, lié directement ou indirectement à des gouvernements et à des services de renseignement.

L'activisme numérique idéologique et protestataire que représentait autrefois Anonymous évolue vers un phénomène composé d'une myriade de groupes nationalistes qui utilisent de manière répétée les attaques par déni de service distribué (DDoS) pour créer un climat de tension et un harcèlement persistant des ennemis occidentaux.

L'hacktivisme est devenu un outil à double tranchant. D'une part, il représente une forme d'expression et de lutte pour la justice sociale, la transparence et les droits de l'homme. D'autre part, il est devenu une arme utilisée par les États pour déployer des campagnes de déstabilisation politique et de désinformation.

L'utilisation de cyberattaques à des fins géopolitiques a mis en évidence la frontière ténue entre l'activisme et la cybercriminalité parrainée par l'État. Cet article vise à analyser l'évolution de l'hacktivisme et ses relations avec les gouvernements, ainsi que le rôle des groupes de menaces persistantes avancées (APT) dans l'utilisation du cyberespace à des fins politiques et militaires . [1]

À travers l'examen de cas concrets, il explorera la collaboration (ou l'instrumentalisation) des hacktivistes par les États, les implications de cette pratique et son impact sur la géopolitique actuelle. Enfin, une réflexion sera proposée sur l'avenir de

[1] Groupes de cyber-attaquants souvent associés à des États-nations ou à de grandes organisations criminelles, très sophistiqués et persistants, qui infiltrent des réseaux pendant de longues périodes à des fins d'espionnage ou de sabotage et qui disposent d'abondantes ressources (techniques, économiques) pour attaquer des cibles de grande valeur (gouvernements, grandes entreprises) avec préméditation et furtivité.

l'hacktivisme dans un monde de plus en plus interconnecté, où l'intelligence artificielle et d'autres technologies émergentes pourraient redéfinir le rôle de ces acteurs dans le cyberespace.

L'hacktivisme n'est plus seulement un phénomène marginal de protestation numérique, mais un risque potentiel pour la sécurité des États. Il est essentiel de comprendre son évolution et ses implications pour analyser l'avenir de la cybersécurité espagnole.

2. DE LA PROTESTATION SOCIALE À LA CYBERGUERRE

L'hacktivisme a subi une transformation remarquable depuis ses origines, passant d'une forme de protestation sociale à un outil utilisé par les gouvernements pour soutenir un agenda politique. Si l'on y réfléchit bien, cette transformation trahit les origines et l'essence même de l'activisme. C'est pourquoi, avant d'analyser le rôle joué par l'hacktivisme en tant qu'outil au service de l'État, nous pensons qu'il est nécessaire d'examiner l'évolution de ce phénomène depuis ses origines.

Dans certaines approches contemporaines, en particulier celles qui sont axées sur la systématisation terminologique, il existe une tendance à établir une relation hiérarchique entre le cyberactivisme et l'hacktivisme, en considérant le premier comme un phénomène plus large et en englobant nécessairement le second comme une manifestation spécifique ou une variante radicalisée. Cette lecture, présente à la fois dans la littérature populaire et dans certains cadres analytiques normatifs, considère que le cyberactivisme représente l'utilisation des technologies numériques pour la promotion de causes sociales, politiques ou culturelles par le biais de campagnes de sensibilisation, de pétitions en ligne ou de protestations virtuelles. Le hacktivisme, quant à lui, se caractérise par l'utilisation d'outils de piratage informatique - tels que les attaques par déni de service distribué (DDoS), les violations de données ou la modification de sites web - à des fins similaires, mais par des moyens plus perturbateurs, voire illicites.

Cependant, cette interprétation, bien que largement répandue, est problématiquement réductrice et ne résiste pas à un examen plus approfondi de la théorie historique et critique des mouvements numériques. Premièrement, l'hypothèse d'une évolution linéaire et progressive - du cyberactivisme "modéré" à l'hacktivisme "radical" - ignore les trajectoires historiques distinctes des deux concepts. L'hacktivisme, loin d'être une dérivation tardive du cyberactivisme, émerge simultanément et même plus tôt dans certains contextes, enraciné dans la culture hacker des années 1980 et 1990, et articulé autour de principes tels que la liberté d'information, le libre accès à la connaissance et la désobéissance civile dans le cyberespace (Jordan & Taylor, 2004 ; Coleman, 2014).

En fait, le terme "hacktivisme" provient de la combinaison étymologique de "hacker" et "activism", décrivant l'utilisation de compétences informatiques pour promouvoir des causes politiques ou sociales ; ses racines remontent au milieu des années 1990, lorsque des groupes tels que le "*Cult of the Dead Cow*" (une référence à l'abattoir texan où le groupe tient ses réunions) ont défendu l'accès universel à l'information en

ligne comme un droit humain fondamental et la lutte contre les gouvernements oppressifs.[2] .

"Cult of the Dead Cow, considéré comme l'un des fondateurs de l'hacktivisme moderne, a non seulement diffusé des manifestes critiquant le contrôle de l'Internet par l'État et les entreprises, mais a également mis au point des outils à vocation clairement perturbatrice. Parmi eux, *Back Orifice* (1998), un logiciel conçu pour exposer les vulnérabilités du système d'exploitation Windows et dénoncer les lacunes des utilisateurs en matière de protection de la vie privée[3] . Un an plus tard, en 1999, plusieurs de ses membres ont promu le projet *Hacktivismo*, une branche explicitement orientée vers la lutte contre la censure numérique qui a donné lieu au développement d'outils tels que *Six/Four* ou *Peekabooty*, conçus pour contourner les filtres imposés par les régimes autoritaires et faciliter le libre accès à l'information.

Dans l'idéologie du *Culte de la Vache Morte*, l'accès à l'information en ligne n'est pas seulement un droit fondamental, mais aussi un champ de contestation politique qui exige des formes innovantes d'intervention technique et symbolique. Cependant, ces actions, bien que non violentes sur le plan physique, impliquent une confrontation directe avec la législation restrictive sur l'utilisation des réseaux et la propriété intellectuelle ; en d'autres termes, elles révèlent le caractère ambigu de l'hacktivisme.

D'autre part, conceptualiser l'hacktivisme comme une simple intensification tactique du cyberactivisme nous fait perdre de vue les divergences idéologiques et épistémologiques entre les deux. Alors que le cyberactivisme tend à s'inscrire dans une logique de participation citoyenne, de plaidoyer institutionnel et d'utilisation stratégique des médias sociaux, l'hacktivisme opère souvent sur la base d'un antagonisme direct, d'une résistance aux structures de pouvoir et d'une remise en question des cadres juridiques existants.

S'il peut être utile de considérer l'hacktivisme comme une sous-catégorie du cyberactivisme selon certaines approches descriptives, cette approche est épistémologiquement insuffisante et empiriquement discutable lorsqu'il s'agit d'aborder la généalogie, le cadre normatif et les implications éthico-politiques de ces deux formes d'activisme numérique. Dans cet article, nous nous concentrerons uniquement sur l'évolution de l'hacktivisme, compris comme un phénomène à part entière, en laissant de côté la formulation d'un examen critique de cette classification.

Dans les premiers temps de l'hacktivisme, l'objectif principal était de mener des attaques contre les gouvernements et les entreprises pour protester contre la censure et les injustices sociales. Ces messages se sont intensifiés lorsque le mouvement anti-mondialisation du milieu des années 1990 est apparu sur la scène sociale (Auty, 2004).

La guerre du Kosovo dans les années 1990 (souvent décrite comme la première guerre menée en ligne) a constitué une étape clé dans la consolidation de l'hacktivisme en tant qu'outil d'affrontement politique : les belligérants ont non seulement partagé des

---

[2] Le site web de "The Cult of the Dead Cow" peut toujours être consulté à l'adresse suivante : **https://cultdeadcow.com/about.html**

[3] Bien que conçu à l'origine comme un outil d'audit de sécurité, sa création a suscité une certaine controverse et a été perçue comme une menace par l'industrie technologique.

informations et des témoignages sur la guerre en ligne, mais ils ont également diffusé de la propagande et de la désinformation. *Des pirates informatiques* sont même apparus et sont intervenus activement dans le conflit en défigurant des sites web gouvernementaux et en exécutant des attaques par déni de service contre les infrastructures en ligne de la partie adverse (Denning, 2001).

Sur le plan académique et social, les mouvements hacktivistes ont été perçus comme l'expression naturelle d'un activisme politique préexistant qui avait trouvé dans un nouvel outil (Internet) la possibilité d'employer un type d'activiste au profil technique pour diffuser ses messages d'une manière plus médiatique (Jordan, 2002).

Cependant, le mépris manifeste des normes établies, les noms choisis par les groupes (*The Legion of Doom, Bad Ass Mother Fuckers, Toxic Shock,* etc.) et le contexte d'insécurité sociale ouvert par les attentats du 11 septembre 2001 ont fait qu'un phénomène initialement perçu positivement a commencé à susciter une certaine méfiance (Torres Soriano, 2018).

La figure du *hacker* a commencé à être identifiée à celle du criminel et, par extension, dans un contexte géopolitique marqué par la lutte contre la Terreur, à celle du cyberterroriste. Et les actions hacktivistes ont commencé à être identifiées fondamentalement comme une nouvelle forme de participation politique illégitime, utilisant les cyber-attaques pour effectuer du sabotage et du cyber-espionnage (Vegh, 2005).

Au niveau académique, l'identification de l'hacktivisme à l'illégal ou au criminalisable, fréquente dans certains discours, réduit l'hacktivisme à une "forme radicale de cyberactivisme", et appauvrit ainsi la capacité d'analyse et d'explication des sciences sociales face à la complexité des pratiques politiques numériques contemporaines.

Les débuts de cette décennie reflètent un hacktivisme marqué par la volonté de ses membres de transgresser les conventions sociales pour le plaisir. En effet, les racines du groupe hacktiviste le plus connu (Anonymous) remontent au forum japonais *2chan*, où la communauté virtuelle était dédiée au partage de toutes sortes de contenus aberrants liés à l'anime, au porno et aux blagues (Bartlett, 2015).

Cependant, vers 2003, les premières tensions internes sont apparues au sein d'une communauté virtuelle qui avait trouvé dans le forum *4chan* un endroit idéal pour s'amuser sans se soucier des conséquences. C'est précisément dans ce forum que certains utilisateurs (connus sous le nom de *moralfags*) ont proposé de concentrer leurs activités sur des causes plus transcendantes telles que la lutte contre la censure sur Internet, afin d'assainir l'image de l'hacktivisme et de représenter la défense de la liberté d'expression, de la transparence et d'autres droits civils.

Sous le slogan "*Nous sommes anonymes. Nous sommes la Légion. Nous ne pardonnons pas, nous n'oublions pas. Attendez-vous à nous*" et le masque de Guy Fawkes, un collectif décentralisé d'activistes a vu le jour, combinant l'exfiltration d'informations et les attaques DDoS pour justifier la lutte contre la corruption, la censure et les abus de pouvoir.

Du côté du pouvoir en place, Anonymous a rapidement été interprété comme une prémonition du risque posé par une nouvelle génération d'acteurs virtuels motivés, avec une structure sans leader et un fonctionnement basé sur le volontarisme et la spontanéité (Olson, 2012). Cependant, ce n'est que lorsque le collectif a commencé à soutenir les actions de WikiLeaks que le groupe a été perçu comme une cybermenace de premier plan.

En peu de temps, les Anonymous sont passés d'un petit groupe de *hackers* à l'esprit politique à un mouvement mondial comptant des milliers d'adeptes dans le monde entier. Cependant, leur attrait ne réside pas dans une idéologie structurée ou un programme d'action défini. Au-delà de leur position anti-establishment, qui les a amenés à dénoncer la manipulation et le contrôle exercés par les gouvernements et les entreprises, leur philosophie manquait d'une orientation claire sur la manière dont la politique, la société ou l'économie devraient être organisées. Cela a fait des Anonymous un phénomène difficile à cerner, car leur identité reposait davantage sur l'action et la protestation que sur un programme concret de changement (Torres Soriano, 2018).

Sous le masque de Guy Fawkes se sont rassemblés des individus qui croyaient certainement soutenir un changement social positif, mais aussi d'autres : ceux dont l'inspiration était la destruction nihiliste du monde tel que nous le connaissons et ceux qui cherchaient à se cacher sous la bannière d'Anonymous pour en tirer un profit politique ou économique.

Le principal héritage d'Anonymous, qui a fait de l'hacktivisme une pratique populaire transcendant la sphère des *hackers*, a donné naissance à une nouvelle ère d'hacktivistes opérant dans un paysage fragmenté et complexe, où coexistent de multiples acteurs aux motivations diverses.

Aujourd'hui, si des groupes comme Anonymous continuent d'opérer de manière décentralisée, leur impact a diminué par rapport à l'essor qu'ils ont connu au début des années 2010. Dans le même temps, de nouvelles générations d'hacktivistes sont apparues, qui, bien qu'ayant un niveau d'expertise technique inférieur, compensent par l'utilisation d'outils d'automatisation et une maîtrise de l'impact médiatique et de la mobilisation sociale.

Aujourd'hui, l'hacktivisme est utilisé à la fois par des collectifs indépendants dénonçant l'injustice et par des groupes parrainés par l'État qui instrumentalisent ces tactiques à des fins géopolitiques. Le conflit entre la Russie et l'Ukraine a mis en évidence l'existence d'une cyberguerre, les hacktivistes pro-ukrainiens et pro-russes menant des attaques coordonnées au profit de leur camp respectif.

La frontière entre l'activisme numérique légitime, la cybercriminalité et les opérations secrètes de renseignement est de plus en plus floue. Cependant, nous pouvons considérer qu'il existe actuellement trois types d'hacktivistes : les cyberterroristes, les *hackers* civiques et les *hackers* patriotiques (Dahan, 2013 ; Denning, 2001 ; Johnson et Robinson, 2014 ; Sauter, 2013).

Le cyberterrorisme comprendrait toutes les actions hostiles dans le cyberespace visant à perpétrer des actes de violence contre des personnes ou des biens, dans le but d'intimider ou de contraindre des gouvernements ou des sociétés à atteindre des objectifs politiques, religieux ou idéologiques spécifiques. Ces actions consistent principalement à

diffuser des virus et des *logiciels malveillants*, à vandaliser des *sites web* et à mener des attaques par déni de service (DDoS) ou par *botnet* (Denning, 2001 ; Jordan et Taylor, 2004 ; Goode, 2015).

Dans la catégorie des *hackers* civiques, on trouve tous les groupes organisés qui mènent des actions contre des systèmes informatiques dans le but d'apporter une contribution à la communauté, généralement à la limite de la légalité (Hunsinger et Schrock, 2016 ; Schrock, 2016).

Enfin, les *hackers* patriotiques sont des individus ou des groupes dont les efforts sont alignés sur l'idéologie nationaliste et qui sont considérés comme une "cyber-milice" à la poursuite d'intérêts spécifiques (Dahan, 2013 ; Green, 2016). Même si, de l'extérieur, ces *hackers* ne semblent pas être directement parrainés par un État, nous pouvons désormais en déduire qu'ils sont instrumentalisés dans le cadre d'un réseau plus large de forces étatiques.

Le piratage informatique patriotique a vu le jour en Chine dans les années 1990 en réponse aux émeutes anti-chinoises en Indonésie, et a depuis été utilisé comme tactique par la Chine, la Russie, la Syrie et d'autres États pour nuire à leurs ennemis dans le domaine cybernétique. Toutefois, aucune des opérations antérieures à la guerre d'Ukraine n'a eu l'ampleur, l'impact et les liens gouvernementaux aussi solides et prolongés, ni n'a transgressé les normes internationales de manière aussi flagrante que l'hacktivisme contemporain (Healey & Grinberg, 2022).

3. LE LIEN ENTRE L'HACKTIVISME ET L'APT

Tout au long de l'histoire, les États ont eu recours à des acteurs de substitution pour mener à bien leurs stratégies de conflit sans engager directement leurs forces armées. Unités auxiliaires, groupes mercenaires, insurrections, organisations terroristes ou sociétés militaires privées (SMP) ne sont que quelques-unes des formes que les acteurs tiers ont prises pour se substituer à l'action stratégique des États.

Il n'est donc pas surprenant qu'aujourd'hui, dans une société de plus en plus numérisée, l'État ait trouvé dans les groupes hacktivistes un nouvel acteur pour personnifier l'externalisation de la paternité, et dans le cyberespace, l'environnement idéal pour projeter une influence géopolitique.

Le concept de *guerre de substitution* a fait l'objet d'un débat approfondi au sein de la communauté universitaire et de la communauté de la sécurité, notamment en raison de la difficulté à le différencier de la guerre *par procuration*, étant donné la nature étroitement liée des deux concepts.

Dans les deux cas, les objectifs de l'acteur principal (l'État) et de l'agent mandataire coïncident. Cependant, alors que dans la *guerre par procuration* il y a deux ou plusieurs acteurs hiérarchiquement liés (l'acteur principal travaille pour, avec et par l'intermédiaire de l'acteur mandataire pour atteindre un objectif commun), dans la *guerre de substitution* ces acteurs ne sont alignés que si l'acteur principal est en mesure de mobiliser le soutien adéquat requis par l'acteur mandataire (Fox 2019). En d'autres termes, les concepts de *guerre de substitution* et de *guerre par procuration* diffèrent en fonction de la relation entre les acteurs et de leurs motivations.

Étant donné que les groupes hacktivistes ont peu d'indépendance pour résister au contrôle de l'État qui les sponsorise (ou du moins les influence ou les tolère), nous parlerons dans notre étude de cas d'acteurs *par procuration.*

Plus précisément, pour les désigner, nous utiliserons la définition des " *proxy* actors " de Rondeaux et Sterman (2019), qui les définissent comme des " *sujets extérieurs à la structure de sécurité des États impliqués dans un conflit qui agissent sous le parrainage direct ou indirect d'un acteur conventionnel (un État)* " ; et la définition des *cyberproxies* de Maurer (2018) comme des " *intermédiaires qui mènent des actions offensives dans le cyberespace au profit d'un acteur principal* ".

Historiquement, *les cyberproxies* ont été personnifiées par diverses entités liées au monde de la cybercriminalité et du cyberespionnage. Cependant, le terme englobe un grand nombre d'entités organisées qui, directement ou indirectement, représentent un facteur de risque pour les entreprises et les États. En fait, la liste des acteurs est très longue : groupes criminels, *acteurs offensifs du secteur* privé (PSOA), groupes terroristes, insurgés, hacktivistes, acteurs étatiques ou APT n'en sont que quelques-uns.

Les raisons de leur utilisation sont diverses : (1) l'utilisation d'acteurs *mandataires* par les gouvernements réduit le risque d'escalade des conflits, car il est difficile d'attribuer la responsabilité d'une cyber-attaque ; (2) il existe une possibilité de déni plausible qui détourne la responsabilité d'une attaque vers un acteur échappant au contrôle du gouvernement ; (3) elle aide les États à prolonger la situation de tension dans les conflits en épuisant leur adversaire sur le plan social, politique et économique ; (4) elle permet aux États d'agir en dehors des réglementations nationales et des critiques des secteurs gouvernementaux opposés - voire de l'opinion publique elle-même dans les démocraties ; (5) elle permet aux États de réagir rapidement et avec souplesse aux actions offensives de leurs adversaires, car elle ne nécessite pas de preuves techniques ni de légitimation publique ; (6) elle offre aux États un outil de dissuasion supplémentaire ; (7) elle permet aux États de contourner l'application du droit international ; (8) elle facilite l'utilisation de personnel expert sans qu'il soit nécessaire de proposer un recrutement légal ; (9) elle permet de participer à des conflits internationaux qui seraient autrement économiquement et politiquement ingérables (Torres Soriano, 2017 ; Expósito Guisado, 2024 ; Marín Gutiérrez, 2023).

Cependant, l'obtention de ces avantages n'est pas sans poser de problèmes. En effet, le principal attrait de l'utilisation d'un *proxy* (qui n'est autre que l'obtention d'un déni plausible d'une agression) est aussi sa principale faiblesse, car l'anonymat et la clandestinité diluent la capacité coercitive et dissuasive de l'État commanditaire - après tout, nous ne pouvons ignorer les théories de Clausewitz qui suggèrent que pour qu'un État modifie sa conduite en fonction de la volonté d'un autre, ce dernier doit connaître l'origine de l'acte de coercition subi.

Un autre inconvénient de l'utilisation des *cyberprocurations* réside dans la manière dont l'État les sélectionne et les contrôle lorsqu'elles sont utilisées. L'existence d'intérêts divergents entre les deux parties peut conduire à la déloyauté du *proxy*, causant des dommages économiques ou politiques à l'acteur qui les utilise - un fait qui est aggravé si l'on tient compte du fait que ces *proxys* opèrent généralement dans des zones où l'État ne peut ni ne veut intervenir.

L'avantage des *mandataires* réside dans leur capacité à agir secrètement, mais c'est justement ce manque de transparence qui empêche l'État commanditaire de vérifier leurs antécédents et leur fiabilité. La littérature académique souligne que le contrôle des *mandataires* est encore plus compliqué si l'État ne dispose pas de mécanismes efficaces pour sanctionner la déloyauté, ou s'il existe des structures décentralisées qui empêchent l'application correcte des ordres hiérarchiques (Popovic 2015).

Dans cet article, nous nous concentrerons uniquement sur deux acteurs qui représentent les deux pôles différents (activisme ouvert et espionnage silencieux) d'un même phénomène, mais qui ne sont pas si différents en termes d'objectifs qu'ils poursuivent et d'instrumentalisation de ces derniers par les États.

D'une manière générale, l'hacktivisme et les APT se distinguent par leurs motivations, leurs méthodes et le degré de soutien de l'État. Ainsi, alors que l'hacktivisme est motivé par un contexte socio-politique (protestation, activisme, causes morales), les APT se concentrent sur l'espionnage stratégique et l'obtention d'un avantage économique et militaire.

Sur le plan opérationnel, les APT agissent de manière furtive et persistante, en utilisant des *logiciels malveillants* personnalisés, des portes dérobées et des mouvements latéraux, contrairement aux actions des hacktivistes qui cherchent généralement à attirer l'attention du public et se concentrent généralement sur des attaques DDosS à court terme.

Cependant, il n'est pas rare d'observer comment les APT agissent temporairement comme des hacktivistes (lorsqu'ils divulguent publiquement les données qu'ils exfiltrent pour provoquer un impact politique) et comment les hacktivistes sont instrumentalisés par les États pour atteindre leurs objectifs stratégiques.

Au niveau organisationnel, les hacktivistes et les APT diffèrent également : les hacktivistes agissent généralement de manière décentralisée, spontanée, voire anonyme, et sans commandement unifié. Les APT, en revanche, sont généralement des équipes structurées, souvent intégrées dans une organisation plus vaste (une armée, une agence de renseignement ou un groupe criminel), avec une hiérarchie définie et un financement nettement plus puissant (CyberZaintza, 2021).

En effet, la différence de ressources et de formation technique suggère un lien plus étroit entre les APT et les États qu'avec les groupes hacktivistes. Toutefois, la frontière entre les deux concepts a récemment été brouillée par la prise de conscience que certains groupes hacktivistes pro-russes recevaient un soutien secret de l'État ou agissaient conformément à l'agenda de l'État, brouillant ainsi la distinction jusqu'alors claire entre les "*hackers* activistes" et les "agents de l'État" (Muncaster, 2024).

En fait, il n'est pas exclu que certains groupes d'hacktivistes soient formés ou soutenus par des APT ou directement par des acteurs étatiques. C'est le cas par exemple de "XakNet Team", "Infoccentr" et "CyberArmyofRussia_Reborn", des groupes hacktivistes pro-russes qui, selon Mandiant, sont des acteurs de la cybermenace parrainés par la Direction principale du renseignement russe (GRU) par l'intermédiaire de l'APT44 (Mandiant, 2022).

Au cours de la dernière décennie, de nombreux cas ont été documentés dans lesquels des États ont utilisé à la fois leurs propres groupes APT et des collectifs d'hacktivistes (ou leurs identités) pour mener des opérations de cyberespionnage, de sabotage de conflits et de manipulation politique.

Un exemple paradigmatique illustrant l'interdépendance de ces deux concepts se trouve dans les élections américaines de 2016, lorsque "*DCLeaks*" et "*Guccifer 2.0*", deux identités liées à la Direction principale du renseignement de la Russie (*Glavnoe Razvedyvatel'noe Upravlenie*, GRU), ont volé des courriels du Parti démocrate et les ont diffusés en se faisant passer pour des "hacktivistes américains patriotiques" (DOJ, 2018).

Dans le sillage de la guerre en Ukraine, il n'est pas rare de constater une interdépendance entre les hacktivistes russes et les APT, des groupes tels que *Killnet, NoName057(16), Anonymous Sudan* qui ont attaqué des sites web gouvernementaux et des entreprises occidentales pour soutenir le discours du Kremlin montrent que, bien que ces groupes se qualifient d'"activistes spontanés", ils agissent de manière suspecte en coordination avec l'action de l'État russe (Van Der Walt, 2025).

Cependant, la Russie n'est pas le seul acteur étatique à employer des APT et des hacktivistes pour déployer sa puissance. D'autres États comme la Chine, la Corée du Nord ou l'Iran sont également accusés depuis des années de mener leurs activités offensives dans le cyberespace de cette manière.

Plus précisément, la Chine est accusée depuis des années de parrainer de vastes campagnes de cyberespionnage par l'intermédiaire d'unités militaires et de *pirates informatiques* rémunérés, tels que ceux du groupe APT1, considéré par Mandiant en 2013 comme l'unité 61398 de l'Armée populaire de libération de la Chine.

Les opérations APT chinoises ont tendance à se concentrer sur des cibles stratégiques (aérospatiale, énergie, télécommunications, défense, etc.) et sont considérées comme faisant partie des services de renseignement de l'État chinois, mais contrairement à la Russie, l'utilisation de l'hacktivisme n'est pas aussi importante dans les stratégies chinoises.

Le gouvernement a toléré et même inspiré des "*hackers* patriotiques" chinois dans certains conflits, par exemple le "*Honker Hacker Network*", une communauté de *hackers* échappant au contrôle du gouvernement - selon des sources chinoises - qui a attaqué des acteurs adverses de la Chine lors de différends territoriaux ou d'incidents diplomatiques.

L'Iran, quant à lui, a montré une tendance à instrumentaliser des groupes de *hackers* prétendument activistes pour mener des opérations de représailles contre ses adversaires, tout en développant ses propres APT. Les attaques DDoS contre des banques américaines en 2012-2013, en représailles aux sanctions occidentales, en sont un exemple significatif : une entité se réclamant de l'hacktivisme religieux et s'appelant les "*Cyber Fighters of Izz ad-Din al-Qassam*" a revendiqué l'offensive, invoquant l'indignation suscitée par une vidéo anti-islamique (CFR, 2012).

Les agences de renseignement américaines ont ensuite conclu qu'il s'agissait d'une opération orchestrée par l'Iran (probablement ses gardiens de la révolution) en réponse aux mesures prises à l'encontre de son programme nucléaire. En fait, en 2016, le ministère

américain de la justice a inculpé sept Iraniens liés au Corps des gardiens de la révolution islamique (CGRI) pour ces attaques.

Un autre exemple est l'attaque "*Shamoonj*" menée en 2012 par le "*Cutting Sword of Justice*", un groupe hacktiviste présumé qui a effacé les données de 30 000 ordinateurs de la compagnie pétrolière saoudienne Aramco, mais que les analystes ont ensuite attribuée à une opération de l'État iranien en réponse à l'offensive *Stuxnet* et aux tensions régionales.

Malgré son isolement, la Corée du Nord a également réussi à créer l'une des cybermenaces les plus actives, principalement pour collecter des fonds et déstabiliser ses adversaires géopolitiques. Son groupe APT le plus connu, *Lazarus Group* (lié à APT38), a volé des centaines de millions en attaquant des banques.

Un autre cas illustrant l'instrumentalisation des campagnes militantes par les États peut également être trouvé dans l'une de leurs actions, le *piratage* de Sony Pictures en 2014, lorsqu'un groupe appelé "*Guardians of Peace*" a exfiltré des données confidentielles et détruit les systèmes de Sony en représailles apparentes au film satirique sur le dirigeant nord-coréen "*The Interview*". (FBI, 2014).

La Corée du Nord est le paradigme de l'instrumentalisation directe : ses *pirates informatiques* sont des agents de l'État qui prennent parfois le nom de groupes fictifs pour diffuser leurs messages ou justifier leurs attaques, mais contrairement à d'autres États, les Nord-Coréens ne font pas de distinction entre les APT et l'appareil d'État, ne gardant la couverture que dans le discours public destiné au monde extérieur.

Pour leur part, les puissances occidentales emploient manifestement aussi des capacités cybernétiques offensives pour attaquer d'autres États. Le cas le plus pertinent est sans doute l'opération "Jeux olympiques" attribuée aux agences de la NSA et à l'unité 8200 (officieusement reconnue), dans le cadre de laquelle les États-Unis et Israël ont développé le logiciel malveillant *Stuxnet* pour saboter les centrifugeuses nucléaires iraniennes vers 2010 (The Guardian, 2017).

En revanche, en Occident, s'il existe des entités APT soutenues par des Etats pour agir de manière offensive dans des campagnes d'espionnage, l'instrumentalisation de groupes hacktivistes pour masquer leurs actions est quasiment inexistante. En fait, on ne trouve qu'un seul cas où un groupe hacktiviste occidental lie son activité à la capacité cyber-offensive d'un État : l'"*Armée informatique de l'Ukraine*".

Ce cas est particulièrement controversé, car le soutien public du gouvernement ukrainien viole ouvertement les normes récemment adoptées sur la conduite des États dans le cyberespace, ainsi que les positions de politique étrangère des membres de l'OTAN (Healey et Grinberg, 2022).

Si nous utilisons le tableau "Spectre de responsabilité" de Healey et Grinberg (2022), qui établit une corrélation entre l'activité des groupes et le degré de responsabilité de l'État dans leur *cyberprocuration*, nous pouvons voir que le soutien du gouvernement ukrainien à l'*Armée de l'informatique de l'Ukraine* a commencé au moins comme "coordonné par l'État (niveau 6)", (lorsque le ministre ukrainien de la transformation numérique, Mikhail Fedorov, a ouvertement appelé les hacktivistes volontaires du monde

entier à soutenir l'Ukraine sur le front numérique) et même "encouragé par l'État (niveau 4)".

Tableau 1 : *Spectre de la responsabilité de l'État.*

Position de l'État	Relation entre *l'État et le mandataire*
1. Interdit par l'État.	Le gouvernement national contribuera à mettre fin à une l'attaque d'un tiers.
2. Interdiction de l'État, mais insuffisante.	Le gouvernement national coopère, mais il est incapables d'arrêter l'attaque des tiers.
3. Ignorée par l'État.	Le gouvernement national est conscient des attaques des des tiers, mais n'est pas disposé à prendre aucune action officielle.
4. parrainé par l'État.	Des tiers contrôlent et dirigent l'attaque, mais le gouvernement national les promeut en tant que politique.
5. Façonné par l'État.	Des tiers contrôlent et dirigent l'attaque, et les L'État apporte un certain soutien.
6. Coordonné par l'État.	Le gouvernement national coordonne l'attaque en des tiers, par exemple en suggérant des détails opérationnel.
7. Obligation de l'État.	Le gouvernement national ordonne à des tiers de mener l'attaque en leur nom.
8. Géré, mais non reconnu par l'État.	Éléments échappant au contrôle des forces les attaques cybernétiques du gouvernement national conduisent à attaque ordonnée.
9. Mise en œuvre par l'État.	Le gouvernement national mène l'attaque en utilisant des forces cybernétiques sous leur le contrôle direct.
10. Intégrée à l'État.	Attaques des gouvernements nationaux à l'aide de mandataires intégrés et de cyberforces gouvernemental.

(Healey, 2022).

C'est surtout dans les conflits géopolitiques que l'on observe la convergence la plus accélérée entre l'hacktivisme et les opérations étatiques. Dans le cas de la guerre en Ukraine, trois ans après le début du conflit et malgré le fait que le nombre d'acteurs hacktivistes ait considérablement diminué (de plus de 130 groupes en 2024 à seulement environ 80 groupes en 2025), nous pouvons toujours observer comment les deux parties maintiennent un croisement de cyberattaques destructrices, coordonnées avec leur campagne militaire et soutenues dans leurs actions par des "hackers patriotiques" (Cyberknow, 2025).

Du côté ukrainien, l'*IT Army of Ukraine* reste la plus importante force hacktiviste d'Ukraine, mobilisant toujours des volontaires à l'intérieur et à l'extérieur du pays pour attaquer l'infrastructure russe, mener des actions de contre-propagande et soutenir des missions de renseignement. Au cours de la période 2023-2024, on lui attribue, par

exemple, la coupure temporaire des services Internet dans les zones occupées par la Russie et le déploiement continu de campagnes DDoS contre des entités russes de premier plan (Optiv, 2023).

Du côté pro-russe, le groupe le plus en vue actuellement est *NoName057(16)*, un groupe lié au GRU, qui agit en coordination avec l'agenda du Kremlin en sélectionnant des cibles en accord avec les intérêts stratégiques russes et se considère comme une sorte de "bras cyber-spontané" permanent de l'armée russe.

Tableau 2 : *Chronologie des cas d'instrumentalisation de l'hacktivisme par l'État.*

Année	***État***	***Groupe hacktiviste***	***Fonctionnalité***	***Niveau de lien avec l'État (Healey & Grinberg).***
1998-1999	Kosovo	Pirates informatiques patriotes	Premier conflit avec une intervention hacktiviste notable.	Ignoré / Spontané
1999	Chine	Red Honker	Les pirates informatiques patriotiques actifs dans les conflits territoriaux. Campagnes d'espionnage industriel et cyber-attaques contre des infrastructures critiques.	Encouragé / Formé
2012-2013	L'Iran	Cybercombattants d'Izz ad-Din al-Qassam	Attaques DDoS contre des banques américaines en représailles aux sanctions. Opération Shamoon contre Aramco avec effacement massif.	Coordonné / ordonné
2014	Corée du Nord	Groupe Lazarus	Cyber-attaques pour le financement de l'État. Attaque contre Sony Pictures (2014) à titre de représailles symboliques.	Mis en œuvre / Intégré
2022-aujourd'hui	Russie	Killnet/ Cyber Army of Russian Reborn/ NoName057(16)	Les groupes hacktivistes se sont coordonnés avec la stratégie russe dans la guerre en Ukraine. Attaques DDoS.	Coordonné / Encouragé

2022-aujourd'hui	Ukraine	Armée informatique de l'Ukraine	Appel public du gouvernement à l'hacktivisme contre la Russie. DDoS, sabotage et propagande pro-ukrainienne.	Coordonné / Encouragé

4. L'AVENIR DES GROUPES HACKTIVISTES.

La survie des groupes hacktivistes indique que l'hacktivisme intégré à la guerre est là pour durer, du moins tant que le conflit sous-jacent perdure et que les États en conflit trouvent ce niveau d'action décentralisée utile. En outre, le paysage actuel de l'hacktivisme nous amène à constater que l'hacktivisme va au-delà des DDoS et s'oriente vers des attaques APT plus sophistiquées, telles que les attaques contre les infrastructures critiques SCADA et les systèmes de contrôle industriel (ICS)[4] .

Le fait que des groupes appartenant à l'écosystème hacktiviste pro-russe, tels que *Z-Pentest Alliance* ou *Sector 16*, se soient activement introduits dans des centrales électriques, des installations d'eau potable et des industries en général, reflète non seulement une maturation et une étatisation du phénomène hacktiviste, mais aussi l'existence de risques physiques croissants de leurs actions (Antoniuk, 2024).

La réduction du nombre de groupes hacktivistes dans l'environnement pro-russe suggère que l'effervescence initiale a cédé la place à un processus de sélection naturelle dans lequel les groupes bénéficiant d'un meilleur soutien, d'une meilleure organisation et d'une meilleure protection survivent. Ce phénomène se traduit par des opérations plus efficaces et mieux coordonnées, mais aussi plus prévisibles car alignées sur l'agenda de l'État russe.

Dans le même temps, la persistance des attaques quotidiennes indique que la cyberguerre de basse intensité est devenue une routine. Les DDoS constants maintiennent une pression psychologique et de propagande sur les populations cibles (rappel quotidien de la présence d'un conflit), tandis que l'adoption de *ransomwares* et d'attaques contre les industries augmente le potentiel de dommages réels aux infrastructures critiques, brouillant la frontière entre l'hacktivisme et le cyberterrorisme - un fait qui peut finalement conduire à des réponses plus énergiques de la part des États victimes et au potentiel d'escalade du conflit.

Une autre évolution pertinente est le développement remarquable d'alliances émergentes entre les causes hacktivistes qui transcendent le théâtre des opérations au-delà de l'Ukraine et impliquent des pays tiers. Un exemple est la récente alliance entre les hacktivistes pro-russes et pro-palestiniens, qui réunit des causes géopolitiques apparemment distinctes sous un récit commun d'attaque de l'Occident.

[4] Système centralisé permettant de surveiller, de contrôler et de collecter des données en temps réel à partir de processus et d'appareils.

Les tensions mondiales de 2024 (y compris la guerre de Gaza) ont créé un étrange front uni d'hacktivistes. Des groupes russes (en particulier *NoName057(16)*) ont commencé à coordonner leurs opérations avec des collectifs liés au Moyen-Orient (tels que *Mr. Hamza* ou *Anonymous Guys*), et ont synchronisé leurs attaques sous la bannière de l'union de la "*Sainte Ligue*" contre des pays qu'ils percevaient comme des adversaires communs, tels que la France.

Ce type d'alliance est bien connu en Espagne, et notamment par la Guardia Civil, puisqu'en juillet 2024, l'institution a été la cible directe d'une campagne de cyberattaque conjointe, " *#FuckGuardiaCivil* ", qui répondait à une initiative promue par le groupe *NoName057(16),* pour "se venger des autorités espagnoles" qui avaient arrêté trois personnes à Manacor (Majorque), Huelva et Séville, soupçonnées d'avoir participé à des cyberattaques contre des entités publiques et des entreprises stratégiques en Espagne et dans d'autres pays de l'OTAN.

En effet, en avril 2025, une nouvelle alliance était déjà enregistrée, comprenant les groupes *Keymous+, Mr Hamza, Alixsec et NoName057(16),* pour attaquer la Pologne, l'Allemagne, la France, l'Italie et l'Espagne sous le slogan "*Operation Hack For Humanity V2 !*

Rien qu'en Espagne, le premier jour de la campagne "Operation Hack For Humanity V2 !", plus de 30 attaques contre des sites web d'entreprises et de gouvernements ont été enregistrées, *M. Hamza, NoName057(16), TwoNet* et *Keymous+* étant les groupes les plus actifs dans l'attaque.

La fréquence à laquelle cette convergence s'est produite ces derniers mois montre que le phénomène devient de plus en plus international et interconnecté. Les alliances entre groupes hacktivistes se renforcent mutuellement, dépassant les frontières du conflit russo-ukrainien dans un seul but : étendre leurs actions à l'ennemi commun occidental.

Le fait que des pays de l'OTAN tels que la France, l'Italie et l'Espagne puissent devenir la cible de *pirates informatiques* patriotes russes pourrait conduire à une escalade du conflit, en particulier si l'une de leurs attaques devait gravement endommager des infrastructures critiques, la cyberguerre de basse intensité pourrait susciter une réponse plus forte que d'habitude.

5. CONCLUSIONS

L'analyse de l'hacktivisme et de ses relations avec les États montre que ce phénomène a évolué de la protestation numérique à l'instrumentalisation étatique avec des implications géopolitiques et stratégiques. La frontière entre l'activisme, la cybercriminalité et les opérations étatiques est de plus en plus floue, en particulier dans les conflits tels que la guerre en Ukraine, où nous avons observé une instrumentalisation croissante des groupes hacktivistes par les forces gouvernementales dans la défense de leurs intérêts nationaux.

En effet, le conflit entre la Russie et l'Ukraine a marqué un tournant dans l'utilisation du cyberespace comme champ de bataille, où des acteurs étatiques et non étatiques se sont activement engagés dans des attaques par déni de service (DDoS), le cyberespionnage et le sabotage d'infrastructures critiques.

Cette étude, développée à travers l'étude des cas les plus importants sur la scène internationale, nous a permis d'établir une distinction entre les *hackers* civiques et les *hackers* patriotiques. Alors que les premiers embrassent des causes nihilistes ou socialement conflictuelles, les seconds sont utilisés par les États comme un outil clandestin dans les conflits internationaux, ce qui entraîne une externalisation des capacités cybernétiques gouvernementales et offre une série d'avantages stratégiques : déni plausible de responsabilité, prolongation des situations de tension ou réduction des coûts politiques et économiques.

En résumé, nous pourrions dire que les États ont appris à exploiter l'hacktivisme comme une arme supplémentaire, soit en se faisant passer pour des hacktivistes afin de désinformer ou d'exfiltrer des données, soit en encourageant leurs sympathisants à lancer des cyberattaques de masse contre leur ennemi.

Toutefois, cette instrumentalisation pose de sérieux problèmes au niveau stratégique. La sophistication progressive des attaques, qui sont passées du vandalisme numérique à des opérations plus avancées contre des infrastructures critiques, ne fait qu'accroître sérieusement les possibilités de représailles de la part des États touchés et le risque potentiel d'escalade dans les conflits asymétriques.

En outre, la convergence entre les APT et les hacktivistes remet en question les normes internationales existantes, car les attaques perpétrées par des acteurs *mandataires* brouillent la responsabilité des États et rendent difficile la mise en œuvre de la dissuasion ou de représailles directes. D'autant plus que les collectifs d'hacktivistes semblent évoluer vers un nouveau paysage d'alliances capables de rassembler des groupes d'hacktivistes aux agendas géopolitiques divers pour attaquer les pays occidentaux.

La cybersécurité des États doit s'adapter à une nouvelle réalité dans laquelle les groupes hacktivistes jouent un rôle clé dans la projection du pouvoir de l'État. Les démocraties occidentales, traditionnellement plus réticentes à utiliser de telles tactiques, sont confrontées à un dilemme : comment réagir efficacement sans compromettre leurs valeurs ?

La tendance actuelle montre non seulement une évolution claire de l'hacktivisme vers un lien croissant avec les intérêts du gouvernement qui le soutient, mais renforce également l'idée que le cyberespace continuera à prendre de l'importance dans les conflits futurs. Des cas tels que la Russie, où des groupes comme *Killnet* ou *NoName057(16)* ont revendiqué des cyber-opérations coïncidant avec les intérêts géopolitiques du Kremlin - en particulier pendant la guerre en Ukraine -, ou l'Iran, avec des groupes comme *Tapandegan*, dont la rhétorique oppositionnelle n'empêche pas les soupçons de coordination indirecte avec les agendas de l'État, illustrent cette dérive et renforcent l'idée que le cyberespace continuera à prendre de l'importance dans les conflits à venir, illustrent cette dérive, et démontrent un brouillage progressif entre acteurs non étatiques et étatiques dans la sphère numérique, où l'hacktivisme n'est plus exclusivement une forme de dissidence citoyenne mais est devenu, dans certains contextes, un outil informel de projection du pouvoir étatique.

6. RÉFÉRENCES BIBLIOGRAPHIQUES

Antoniuk, D. (2024). *Cybervolk : Hacktivists from India and Russia collaborate on ransomware attacks (Cybervolk : des hacktivistes indiens et russes collaborent à des attaques par ransomware)*. The Record. https://therecord.media/cybervolk-india-hacktivists-russia-ransomware

Antoniuk, D. (2024). *Cybervolk : Hacktivists from India and Russia collaborate on ransomware attacks (Cybervolk : des hacktivistes indiens et russes collaborent à des attaques par ransomware)*. The Record. https://therecord.media/cybervolk-india-hacktivists-russia-ransomware

Auty, C. (2004). L'hacktivisme politique : outil de l'opprimé ou fléau du cyberespace ? *Aslib Proceedings, 56*(4), 212-221.

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

CFR (2012). *Attaques par déni de service contre les banques américaines en 2012-2013*. Conseil des relations étrangères (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). *Guerre entre la Russie et l'Ukraine : le point sur les hacktivistes.* https://cyberknow.substack.com/p/russia-ukraine-war-hacktivist-update

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

Dahan, M. (2013). Hacking for the homeland : Patriotic hackers versus hacktivists. *Conférence internationale sur la guerre de l'information et la sécurité*, 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. Dans J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars : The future of terror, crime, and militancy* (pp. 239-288). RAND Corporation.

DOJ (2018). *Un grand jury inculpe 12 officiers de renseignement russes pour des délits de piratage liés à l'élection de 2016.* Département de la justice des États-Unis. https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

Expósito Guisado, J. (2023). *Cyberproxies : APTs as a future risk factor (Les cyberproxies : les APTs comme facteur de risque futur)*. Institut espagnol d'études stratégiques (IEEE). *IEEE Bulletin*, (32), 815-831.

FBI (2014). *Mise à jour de l'enquête sur Sony*. 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 (Le conflit et la nécessité d'une théorie de la guerre par procuration)*. *Journal of Strategic Security, 12*(1), 44-71, JSTOR. www.jstor.org/stable/26623077

Goode, L. (2015). Anonymous et l'éthique politique de l'hacktivisme. *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. et Grinberg, A. (2022). *Patriotic hacking : No exception*. Lawfare. https://www.lawfaremedia.org/article/patriotic-hacking-no-exception

Hern, A. (2017). Un contractant de la NSA a divulgué des outils de piratage américains par erreur, selon 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. et Schrock, A. (2016). La démocratisation du piratage et de la fabrication. *New Media & Society, 18*(4), 535-538. https://doi.org/10.1177/1461444816629466

Johnson, P. et 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). *Activisme ! Action directe, hacktivisme et avenir de la société*. Reaktion Books.

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

Mandiant (2022). *L'ascension du GRU : les sous-fifres de Telegram*. https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions

Marín, F. (2023). *L'hacktivisme au service de l'État : les cyberproxies en Ukraine*. Opinion Paper. Institut espagnol d'études stratégiques (IEEE).

Maurer, T. (2018). *Cyber Mercenaires : l'État, les hackers et le pouvoir*. Cambridge University Press.

Muncaster, P. (2024). *Hacktivisme : évolution des menaces pour les organisations*. WeLiveSecurity. https://www.welivesecurity.com/es/cibercrimen/el-hacktivismo-evolucionando-amenazas-organizaciones

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

OPTIV (2023). *Mise à jour Russie/Ukraine - décembre 2023*. https://www.optiv.com/insights/discover/blog/russiaukraine-update-december-2023

Popovic, M. (2015). Fragile proxies : Explaining rebel defection against their state sponsors. *Terrorisme et violence politique*. https://doi.org/10.1080/09546553.2015.1092437

Rondeaux, C. et 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" : l'impact de la conception des outils et des représentations médiatiques sur le succès des attaques DDOS des activistes. *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). Proxy wars in cyberspace (Guerres par procuration dans le cyberespace). *Revista del Instituto Español de Estudios Estratégicos, (9)*, 15-36.

(2018). L'hacktivisme comme stratégie de communication, des Anonymous au cybercalifat. *Cuadernos de Estrategia, (197)*, 197-224.

Van Der Walt (2025). *Réflexion sur trois années de cyberguerre en 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