Gawel, Hanna

Article

Hacktivism

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Gawel, Hanna (2024) : Hacktivism, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 13, Iss. 2, pp. 1-12, https://doi.org/10.14763/2024.2.1751

This Version is available at:
https://hdl.handle.net/10419/296498

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 13 **Issue** 2

GLOSSARY ENTRY

OPEN ACCESS

PEER REVIEWED

Hacktivism

Hanna Gawel *Jagiellonian University*

DOI: https://doi.org/10.14763/2024.2.1751

Published: 4 April 2024
Received: 10 July 2023 **Accepted:** 12 October 2023

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Gawel, H. (2024). Hacktivism. *Internet Policy Review*, *13*(2). https://doi.org/10.14763/2024.2.1751

Keywords: Hacktivism, Hacking, Hacker, Political activism

Abstract: Hacktivism represents a dynamic intersection of technology and activism, where individuals or groups leverage digital tools to advance social or political causes. This text explores the multifaceted nature of hacktivism, encompassing a spectrum of activities from online protests and information dissemination to more disruptive forms of digital direct action.

This article belongs to the **Glossary of decentralised technosocial systems**, a special section of *Internet Policy Review*.

Definition

Hacktivism is the term used to describe computer hacking. It is a combination of the terms “hacking” and “activism”, and it refers to online activist tactics and strategies that are largely derived from the history of individuals engaged in direct action, resistance, and anti-globalisation campaigns (Delmas, 2018; Huschle, 2002). It is a digital activity carried out for political or social purposes, such as drawing attention to a conflict or promoting certain ideas. Hacktivists, unlike cybercriminals, are not motivated by financial or personal gain (Ireland, 2022; Jordan & Taylor, 2004; Krapp, 2005). The most inclusive definition of hacktivism would be *a non-violent action in the digital space, using legal or illegal solutions to achieve a stated goal of civic dissent, raising civic awareness or disseminating socially relevant information for hacktivists* (George & Leidner, 2019; Romagna, 2020).

Origin of the term

The term hacktivism was coined from a combination of two words: hacking and activism. The term 'hack' was popularised in the 1960s at the Massachusetts Institute of Technology and meant paid pranks that had to be characterised by particular ingenuity and style and not cause harm to anyone (Coleman, 2020; Erickson, 2008; Nowviskie, 2016). The term ‘hack’ or ‘hacking’ or even ‘hacker’ (as a person capable of hacking) often occurs in a derogatory context. These terms can be equated with something illegal or questionable in terms of established legal norms, and this is because *hacking in media coverage has come to be associated with illegal computer hacking* (Gunkel, 2005; Hampson, 2012). It is crucial to first distinguish between hackers and crackers. Those who hack computers with malicious intent are known as crackers. Hackers are distinct, despite the media’s frequent confusion of these two terms. The term ‘hacker’ was first used to denote someone with extensive knowledge of computer networks and systems. Hackers create, alter, or improve these systems using their talents and skills; they frequently utilise computer creativity to accomplish an objective for which the system was not designed.

The term hacktivism is thus debatable. Some claim that the term was specifically created to explain how combining critical thinking and programming abilities in electronic direct action could lead to societal transformation. Some interpret it as

practically equivalent to malevolent, destructive deeds that compromise the security of the internet as a platform for technology, commerce, and politics (Hearn et al., 2009; Huschle, 2002). Others, however, link it to information ethics, human rights, and free expression. Hacktivism emphasises the hacker attitude of hacking as exploring, testing, and creating solutions to technical limitations; hacktivism, on the other hand, might be the preferred spelling if one is concerned about radicalised activism (Dahlberg & Siapera, 2007; Neumayer & Svensson, 2016).

The advent of the internet altered the way that politics was conducted worldwide, enabling anti-government organisations to form alliances that would not have been possible without this cutting-edge form of communication (York & Zuckerman, 2019). It dawned on activists that the internet was the best medium for spreading messages to a larger audience. The internet was thus facilitating the democratisation of the media, because it was comparatively inexpensive to post messages to a public forum or website, as opposed to the significant expenses of running a radio or television station (Conti et al., 2011; Dean, 2012; Deseriis, 2017).

Hacktivism, thus, cannot be equated with conventional actions in physical space (activism) or cyberspace (cyber activism). The concept of activism has been redefined to consider public relations, issue management, politics and sociology. Comparing two terms together, based on Illia's seven factors of redefinition comparison (2003, p. 328), both terms are based on different societal experiences.

The term hacktivism was first used by the group 'Cult of the Dead Cow' in 1996, although the first politically motivated cyber attacks occurred earlier, as early as the late 1980s and early 1990s (Joque, 2018; Menn, 2019). The creators of the Cult of the Dead Cow group used it to describe individuals or groups using their computer skills to publicise specific political demands connected to legal regulations and unacceptable behaviour of politicians (Menn, 2019, pp. 87–103). The establishment of the website 4chan.org in 2003 was crucial to the growth of hacktivism. Because of the way the service operated (any content, even contentious, could be published by anonymous users), hackers with similar political views placed around underground anarchistic radicalism could "gather" there. The acts were first dismissed as a kind of amusement and a bunch of jokes (Dery, 2017), but eventually, they developed into a coordinated struggle (Hypponen, 2017; Hyppönen, 2022). This portal served as the birthplace of the well-known hacktivist collective Anonymous.

Anonymous

Anonymous is undoubtedly based on a decentralised structure — it is a grassroots initiative, directly linked to information technologies, leaderless and able to operate in any configuration (Dibbell, 2011; Greenberg, 2020). Its actions are *ad hoc*, based on a specific demand and aimed at a selected target. Anonymous is a secretive and widespread organisation, difficult to define nowadays, and the methods of training and mobilisation are, as with terrorist organisations and many grassroots initiatives, unofficial. What connects Anonymous to terrorist organisations, but no longer to 'grassroots globalisation' organisations, may be *the systematic blurring of the boundaries between times and spaces of war and peace* (Appadurai, 2000, p. 33). Project "Chanology", in which Anonymous took on the Church of Scientology, which was preparing to go to court to defend itself against those who criticised the sect, was one of the group's most astute uses of media. The hacktivists claimed that the Church of Scientology was attempting to censor free speech in this way. At that point, Anonymous released its first self-referential video online, using a Guy Fawkes mask as its trademark. Its strategies were hailed as part of a larger movement — the Internet Freedom Movement, which included groups such as the Electronic Frontier Foundation, the Richard Stallman-founded Free Software Foundation, Public Knowledge or La Quadrature du Net, and whose aim was to oppose the work on ACTA (AntiCounterfeiting Trade Agreement). The protest concerned both the secrecy surrounding the drafting of the law and its content, mainly regarding increased penalties for copyright infringement and the creation of mechanisms that would allow internet providers to track user activity.

Hacktivism and cyber security

For hacktivists, breaking computer security and using their skills in this area was intended to promote certain attitudes or values in the public sphere. The group has raised awareness about a wide range of issues, from government wiretapping and internet monitoring to free speech violations. The primary targets of hacktivists are entities such as states, quasi-state actors, and multinational corporations that support the limitations of freedom, including freedom on the internet. Hacktivists use contemporary technology, viewing it as a weapon as well as a place of conflict (Dinniss, 2013; Guo, 2016; Maxigas, 2017). We can identify the following tactics in the arsenal of activists pursuing political objectives via cyberspace: defacing, distributed denial-of-service (DDoS) attacks, ping storms, e-mail bombing, malicious code attacks, and redirects. Defacing, also known as website defacement, is the act of making changes to a website's content.

In November 2012, a hacker from the Teamr00t group altered the content of a Syrian government website as a reaction to the country's lack of internet access. This is one instance of defacement. In a message to the government, the hacktivist blamed President Bashar al-Assad for the current state of affairs. The Teamr00t member urged that the rights of citizens to free speech, a normal life, and internet access be respected. By doing this, he assured Syrians that the Teamr00to group was aware of them and would work to restore their freedom (König, 2014).

The phrase "disrupting a network by flooding it with simultaneous requests for data from thousands of computers" (Munivara Prasad et al., 2012, p. 13) describes DDoS assaults. The attack that took over Estonia's network in April and May 2007 is a noteworthy example (Lesk, 2007; Mansfield-Devine, 2012; Ottis, 2008). Internet users experienced a temporary loss of access to e-mail, electronic banking, and other services as a result of the attacks. It should be clarified that a DDoS attack is a more advanced type of DoS attack, which involves blocking services (Sauter, 2015). The goal of service blocking is to hinder or stop a website's regular operations.

Forms of hacktivism

Hacktivism refers to several types of electronic malice, including page swapping, misdirection, information theft, information theft and dissemination, page parody, virtual sabotage, and software development. Hacker culture places importance on humour, much like the art-activist scene from which many hacktivists originate; not unexpectedly, many hacktivists use humour to convey their points, or 'for the lulz' (Coleman, 2013; Steinmetz, 2016). Hacktivists usually take pride in their tech skills — their ability to implement hacktivism successfully or inventively (Coleman, 2017; Goerzen & Coleman, 2022; Postill, 2018).

Nevertheless, there are also significant differences between the various forms of hacktivism (Karagiannopoulos, 2021). Varying forms of hacktivism relate to diverse political cultures, represent different political orientations and lend themselves to different types of political statements. These differences mean that hacktivists' tactical choices about which forms of hacktivism to engage in represent larger differences like varied types of hacktivism (de Certeau, 1984; Postill, 2014). The issues targeted by hacktivism are as varied as their forms. One can distinguish between cyberwar participation, anti-corporate activism, actions aimed at defending national sovereignty, information-sharing activities and anti-globalisation hacktivism. This division is based on the observed activities of activists online to date, directed at their various chosen targets. This distinguishes hacktivist activities and

emphasises the multiplicity of hacktivism's forms, which are evolving as rapidly as global societal developments.

Issues associated with the term

Hacktivism is a blend of socio-political activism with hacking, which poses difficulty in identifying the movement. On the one hand, it is regarded as a manifestation of online mobilisation; on the other, the phrase depicts illegal acts in virtual space (Coleman, 2020). What characterises and at the same time distinguishes the actions of hacktivism from those of online activists is the directness in movement and activities of a contentious nature, due to their greater effectiveness than the passive forms of civic participation accepted by social activists through, for example, signing a digital list in support of a particular cause. The dilemma presented is in comprehending hacktivism as a form of civil disobedience (Delmas, 2018; Himma, 2005). Hacktivism is assumed to fulfil the tenets of the four pillars of the concept of civil disobedience because it is conducted openly, non-violently, conscientiously, and usually adheres to norms of accountability (Shantz, 2020).

Huschle implies a more rigorous definition of civil disobedience and argues that hacktivism often underperforms because it is not public enough and does not sufficiently respect the law (Huschle, 2002). The broad conception of civil disobedience and thus the fluidity of the definition of hacktivism in academic works may result in hacktivism being treated in media coverage and by governments as a form of digital terrorism (Ireland, 2022; Vegh, 2005).

The term 'cyber-terrorism' was first used by Barry Collin, a senior research fellow at the Security and Intelligence Institute in California, in 1980 (Mazanec, 2015). A popular definition present in the literature defines cyber-terrorism as an illicit attack or threat of attack on computers, networks and information. It is carried out through computers, in pursuit of political objectives by intimidating and attempting to coerce state power or citizens to behave in certain ways. Denning's definition presents cyber-terrorism as *politically motivated hacking activities with the intention of causing serious damage, such as loss of life or damage to an economic area* (Denning, 2001). Thus, one of the constitutive features of the definition of cyberterrorism is the ability to commit specific terrorist actions using a computer and to achieve disproportionate effects of failure, paralysis and disruption of institutions and public facilities. The second aspect of the consequences of cyber-attacks is to increase panic and escalate negative emotions in society by influencing, distorting or controlling the information process, which consequently increases the effect and efficiency of the overall terrorist action. The result is that numerous computer

and information security experts or information warfare theory researchers in their work describe cyber protesters as perpetrators and hacktivism as a moderate form of cyberterrorism, as the methods of the intrusion and interference are similar, although they differ significantly in motivation, scale and outcome. To summarise the points raised thus far, it should be mentioned that there are more human activities carried out in virtual spaces than just the hacktivism-related events shown above. This is the result of social life's intricacy and its digital environment (Gawel, 2021).

Usage of the term 'hacktivism'

The term *hacktivism* has been consistently used over the years to describe a spectrum of digital activities aimed at advancing political or social causes. More recently, the term has echoed through media reports covering actions by groups like Anonymous, whose activities ranged from online protests against perceived injustices to interventions during significant global events such as the Arab Spring. WikiLeaks, with its mission to expose classified information, has also been integral to the narrative of hacktivism. The evolving nature of the term is evident in discussions surrounding nation-state cyber operations, as seen with the Stuxnet malware targeting Iran's nuclear facilities (Poroshyn, 2019; Stevens, 2020). In contemporary contexts, news reports continue to use "hacktivism" to describe a variety of digital actions, reflecting an ongoing intersection of technology, politics, and activism in the digital age.

The term *hacktivism* has evolved into a complex meaning in popular culture and among netizens as a result of a convergence of technology breakthroughs, sociopolitical events, and media portrayals. Commonly understood as the amalgamation of hacking techniques with activism, hacktivism has become synonymous with digital protest and dissent in the collective consciousness. Netizens, representing a diverse and digitally connected global community, frequently employ *hacktivism* to describe online activities that challenge established power structures, demand transparency, or seek to address perceived injustices. The term has thus evolved beyond its initial association with cyber disruptions to encompass a broader range of digitally mediated political expressions. In this contemporary context, hacktivism serves as a linguistic bridge between technology and activism, encapsulating the digital *zeitgeist* of an era where the internet plays a pivotal role in shaping socio-political narratives.

Conclusion

Based on the above analysis, it is clear that hacktivism has various guises. Undoubtedly, due to its nuanced complexity and heterogeneity, it has many supporters and opponents. Research on hacktivism involves scholars and researchers from various disciplines, including computer science, sociology, political science, and cyber security.

The study of hacktivism within the field of alternative media studies has evolved over the years, and scholars like Stefania Milan and Arne Hintz have made significant contributions to this intellectual history. Their works have shed light on the intersection of technology, activism, and media, providing insights into the role of hacktivism in shaping contemporary political landscapes (Hintz & Milan, 2009). Milan's work often focuses on the intersection of social movements, digital technology, and activism. In her book "Social Movements and Their Technologies: Wiring Social Change" (2013), Milan explores how social movements adopt and adapt digital technologies, including hacktivism, to advance their causes. She emphasises the importance of understanding the socio-technical practices of activists engaged in hacktivism. Milan's research also delves into the dynamics of global activism networks, providing insights into the transnational nature of hacktivist campaigns and their impact on political discourse.

In the context of hacktivism, Arne Hintz has contributed to understanding the broader implications of digital activism. His work often explores how hacktivism intersects with issues of surveillance, privacy, and freedom of expression (2009). Also Beaufort has co-edited and edited volumes that address the changing landscape of media activism and hacktivism (Seethaler et al., 2023; Seethaler & Beaufort, 2017). For example, the book "Digital Media, Political Polarization and Challenges to Democracy" (Beaufort, 2020) examines how digital technologies, including hacktivism, impact democratic processes.

References

Appadurai, A. (2000). Grassroots globalization and the research imagination. *Public Culture*, *12*(1), 1–19. https://doi.org/10.1215/08992363-12-1-1

Beaufort, M. (Ed.). (2020). *Digital media, political polarization and challenges to democracy*. Routledge.

Coleman, E. G. (2012). Phreaks, hackers, and trolls: The politics of transgression and spectacle. In M. Mandiberg (Ed.), *The social media reader* (pp. 99–119). New York University Press. https://doi.org/10.18574/nyu/9780814763025.003.0012

Coleman, G. (2013). Anonymous and the politics of leaking. In B. Brevini, A. Hintz, & P. McCurdy (Eds.), *Beyond WikiLeaks* (pp. 209–228). Palgrave Macmillan. https://doi.org/10.1057/9781137275745_13

Coleman, G. (2017). From internet farming to weapons of the geek. *Current Anthropology*, *58*(S15), S91–S102. https://doi.org/10.1086/688697

Conti, G., & Raymond, D. (2011, July 11). Leadership of cyber warriors: Enduring principles and new directions. *Small Wars Journal*. https://apps.dtic.mil/sti/citations/ADA545300

Dahlberg, L., & Siapera, E. (Eds.). (2007). *Radical democracy and the internet: Interrogating theory and practice*. Palgrave Macmillan. https://doi.org/10.1057/9780230592469

de Certeau, M. (1984). *The practice of everyday life*. University of California Press.

Dean, J. (2012). *The communist horizon*. Verso Books. https://play.google.com/store/books/details?id=kBghOq42S3YC

Delmas, C. (2018). Is hacktivism the new civil disobedience?: *Raisons Politiques*, *69*(1), 63–81. https://doi.org/10.3917/rai.069.0063

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239–288). RAND Corporation. https://www.jstor.org/stable/10.7249/mr1382osd.13

Dery, M. (2017). Culture jamming: Hacking, slashing, and sniping in the empire of signs. In M. DeLaure & M. Fink (Eds.), *Culture jamming: Activism and the art of cultural resistance* (pp. 39–61). NYU Press. https://www.jstor.org/stable/j.ctt1bj4rx2.6

Deseriis, M. (2017). Hacktivism: On the use of botnets in cyberattacks. *Theory, Culture & Society*, *34*(4), 131–152. https://doi.org/10.1177/0263276416667198

Dibbell, J. (2011, May 16). Is Anonymous less anonymous now? *MIT Technology Review*. https://www.technologyreview.com/2011/05/16/194661/is-anonymous-less-anonymous-now/

Dinniss, H. H. (2013). Participants in conflict—Cyber warriors, patriotic hackers and the laws of war. In D. Saxon (Ed.), *International humanitarian law and the changing technology of war* (Vol. 41, pp. 251–278). Martinus Nijhoff Publishers. https://doi.org/10.1163/9789004229495_013

Erickson, J. (2008). *Hacking: The art of exploitation* (2nd ed.). No Starch Press. https://play.google.com/store/books/details?id=0FW3DMNhl1EC

George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, *29*(3), Article 100249. https://doi.org/10.1016/j.infoandorg.2019.04.001

Goerzen, M., & Coleman, G. (2022). *Wearing many hats: The rise of the professional security hacker* [Report]. Data & Society. https://datasociety.net/library/wearing-many-hats-the-rise-of-the-professional-security-hacker/

Greenberg, A. (2020, June 22). Hack brief: Anonymous stole and leaked a megatrove of police documents. *Wired*. https://www.wired.com/story/blueleaks-anonymous-law-enforcement-hack/

Gunkel, D. J. (2005). Editorial: Introduction to hacking and hacktivism. *New Media & Society*, *7*(5), 595–597. https://doi.org/10.1177/1461444805056007

Guo, B. (2016). Why hackers become crackers—An analysis of conflicts faced by hackers. *Public Administration Research*, *5*(1), 29–36. https://doi.org/10.5539/par.v5n1p29

Hampson, N. C. N. (2012). Hacktivism: A new breed of protest in a networked world. *Boston College International and Comparative Law Review*, *35*(1), 511–544. https://ssrn.com/abstract=1927505

Hearn, K., Mahncke, Rachel. J., & Williams, Patricia. A. (2009, December 1). *Culture jamming: From activism to hactivism* [PDF]. 10th Australian Information Warfare and Security Conference, Perth, Western Australia. https://doi.org/10.4225/75/57A7F10A9F480

Hintz, A. (2009). *Civil society media and global governance: Intervening into the World Summit on the Information Society*. LIT Verlag.

Hintz, A., & Milan, S. (2009). At the margins of Internet governance: Grassroots tech groups and communication policy. *International Journal of Media & Cultural Politics*, *5*(1–2), 23–38. https://doi.org/10.1386/macp.5.1-2.23_1

Huschle, B. J. & Philosophy Documentation Center. (2002). Cyber disobedience: When is hacktivism civil disobedience? *International Journal of Applied Philosophy*, *16*(1), 69–83. https://doi.org/10.5840/ijap20021613

Hypponen, M. (2017). Silicon plagues. In J. L. Heeney & S. Friedemann (Eds.), *Plagues* (pp. 168–183). Cambridge University Press. doi.org/10.1017/9781108147910.009

Hyppönen, M. (2022). *If it's smart, it's vulnerable*. John Wiley & Sons.

Illia, L. (2003). Passage to cyberactivism: How dynamics of activism change. *Journal of Public Affairs*, *3*(4), 326–337. https://doi.org/10.1002/pa.161

Ireland, L. (2022). We are all (not) Anonymous: Individual- and country-level correlates of support for and opposition to hacktivism. *New Media & Society*. https://doi.org/10.1177/14614448221122252

Joque, J. (2018). *Deconstruction machines: Writing in the age of cyberwar*. University of Minnesota Press. https://doi.org/10.5749/j.ctt20vxpw5

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

König, T. (2014). Revolutionaries' tech support: Hacktivism and anonymous in the Egyptian Uprising. In A. Hamed (Ed.), *Revolution as a process: The case of the Egyptian Uprising*. Wiener Verlag für Sozialforschung.

Krapp, P. (2005). Terror and play, or what was hacktivism? *Grey Room*, *21*, 70–93. https://doi.org/10.1162/152638105774539770

Lesk, M. (2007). The new front line: Estonia under cyberassault. *IEEE Security & Privacy Magazine*, *5*(4), 76–79. https://doi.org/10.1109/MSP.2007.98

Mansfield-Devine, S. (2012). Estonia: What doesn't kill you makes you stronger. *Network Security*, *2012*(7), 12–20. https://doi.org/10.1016/S1353-4858(12)70065-X

Maxigas, P. (2017). Hackers against technology: Critique and recuperation in technological cycles. *Social Studies of Science*, *47*(6), 841–860. https://doi.org/10.1177/0306312717736387

Mazanec, B. M. (2015). *The evolution of cyber war: International norms for emerging-technology weapons*. University of Nebraska Press, Potomac Books. https://doi.org/10.2307/j.ctt1d989jr

Menn, J. (2019). *Cult of the Dead Cow: How the original hacking supergroup might just save the world*. Public Affairs.

Milan, S. (2013). *Social movements and their technologies: Wiring social change*. Palgrave Macmillan. https://doi.org/10.1057/9781137313546

Munivara Prasad, K., Rama Mohan Reddy, A., & Jyothsan, V. (2012). IP traceback for flooding attacks on internet threat monitors (ITM) using honeypots. *International Journal of Network Security & Its Applications*, *4*(1), 13–27. https://doi.org/10.5121/ijnsa.2012.4102

Neumayer, C., & Svensson, J. (2016). Activism and radical politics in the digital age: Towards a typology. *Convergence: The International Journal of Research into New Media Technologies*, *22*(2), 131–146. https://doi.org/10.1177/1354856514553395

Nowviskie, B. (2016). On the origin of "hack" and "yack". In M. K. Gold & L. F. Klein (Eds.), *Debates in the digital humanities 2016* (pp. 66–70). University of Minnesota Press. https://doi.org/10.5749/j.ctt1cn6thb

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In D. Remenyi (Ed.), *Proceedings of the 7th European Conference on Information Warfare and Security* (pp. 163–168). Academic Publishing Limited. https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/

Poroshyn, R. (2019). *Stuxnet: The revenge of malware: How the discovery of malware from the Stuxnet family led to the U. S. Government ban of Kaspersky Lab anti-virus software*. Independently published. https://play.google.com/store/books/details?id=FIQzzAEACAAJ

Postill, J. (2014). Freedom technologists and the new protest movements: A theory of protest formulas. *Convergence: The International Journal of Research into New Media Technologies*, *20*(4), 402–418. https://doi.org/10.1177/1354856514541350

Postill, J. (2018). *The rise of nerd politics: Digital activism and political change*. Pluto Press. https://doi.org/10.2307/j.ctv4ncp67

Romagna, M. (2020). Hacktivism: Conceptualization, techniques, and historical view. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 743–769). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_34

Sauter, M. (2015). Show me on the map where they hacked you: Cyberwar and the geospatial internet doctrine. *Case Western Reserve Journal of International Law*, *47*, 63. https://scholarlycommons.law.case.edu/jil/vol47/iss1/9

Seethaler, J., & Beaufort, M. (2017). Community media and broadcast journalism in Austria: Legal and funding provisions as indicators for the perception of the media's societal roles. *Radio Journal: International Studies in Broadcast & Audio Media*, *15*(2), 173–194. https://doi.org/10.1386/rjao.15.2.173_1

Seethaler, J., Beaufort, M., & Schulz-Tomančok, A. (2023). *Monitoring media pluralism in the digital era: Application of the media pluralism monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2022. Country report: Austria* [Research project report]. EUI Centre for Media Pluralism and Media Freedom (CMPF). doi.org/10.2870/329744

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime* (Vol. 2). NYU Press. https://doi.org/10.2307/j.ctt1bj4rth

Stevens, C. (2020). Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*, *41*(1), 129–152. https://doi.org/10.1080/13523260.2019.1675258

York, J. C., Zuckerman, E., & Jørgensen, R. F. (2019). Moderating the public sphere. In *Human rights in the age of platforms* (Vol. 137, pp. 137–162). The MIT Press. https://doi.org/10.7551/mitpress/11304.003.0012

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

cnrs centre internet et societe

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies