1
Phreaks and Geeks

By david_shankbone, CC BY 2.0, via Wikipedia.

A protestor wearing the signature Guy Fawkes mask associated with Anonymous at an Occupy Wall Street event.

Political Action in the Digital Age

The portmanteau "hacktivism" combines the term "activism," which means to campaign for political or social change or reform, with the term "hack," which is a Digital Era term generally meaning to gain unauthorized access to a computer system or to data contained within a computer system. Hacktivism is therefore defined as the use of digital tools, like "hacking" into computer systems, as a form of civil disobedience or as a political demonstration. Hacktivism typically involves violating legal guidelines and so opinions on the issue vary considerably, with some considering hacktivism a type of cybercrime while others have argued that hacktivism, like other kinds of activism, constitutes an important form of political discourse in the digital age.

Dawning of the Cyber Age

Hacking, which involves gaining unauthorized access to a computer system, has a long and storied history and the first "hack" predated the digital era by decades. In the early 1970s, there were nearly 40,000 computer systems being used in the United States, most of which were manufactured by International Business Machines (IBM) and used by corporations to manage menial and repetitive operations. The telephone network of the era was essentially operated via computer system as well, and this system became the target for the first generation of "protohackers," known as "telephone phreakers." Phreakers were individuals who used experimental means to get around telephone security systems in order to make free telephone calls, in an era in which long-distance calling was still expensive and complicated. Some of the phreakers were simply imaginative and creative small-time criminals, but many of them were engineers and electronics experts who used this extra-legal recreational activity to experiment with digital networks and systems.

At the time, phone networks like AT&T used a series of tones to manage access to various lines. Phreakers discovered that a plastic toy whistle contained in boxes of the children's cereal "Cap'n Crunch" emitted a tone at the frequency 2600Hz, which was the perfect tone to fool the AT&T system into giving a user access to certain long-distance lines. Though he did not discover this fact, proto-hacker John Draper, known by the alias "Cap'n Crunch" make this exploit famous by incorporating this tone and other useful tones into devices called "blue boxes" that could essentially be used to bypass AT&T security and to gain unauthorized access to various phone lines. Draper claimed in interviews that he was actually able to place a call directly to President Richard Nixon using a hijacked phone line.

Draper knew that his phreaking activities were illegal, but considered himself an experimenter, violating security systems primarily to show what could be done

with human ingenuity in the growing world of digital communication and security. Draper therefore never tried to hide his activities, and he was brought up on charges for violating AT&T's system, serving several years on probation for violating the laws. Nonetheless, Draper's pioneering experiments with violating digital security systems inspired many others, including Steve Wozniak and Steve Jobs who became associates of Draper's and had a side business selling their own "blue boxes" before founding what would become one of the world's largest and most powerful companies; Apple Computers.[1]

Draper's experiments were occurring just about the time that the first email system was being developed, by the US-military linked research organization Defense Advanced Research Projects Agency (DARPA), resulting in "Arpanet," a precursor of the modern internet. It was during the military development phase that engineers began to discover ways that computer programs and digital tools could be used by outsiders to gain access to computer systems. The first computer "virus," a program that can move from computer to computer in a linked network and can cause infected computers to perform unwanted actions, was invented by engineers working on network security and trying to discover what kinds of computer programs could be used to again unauthorized access to networks and individual systems.[2]

As computer networks spread and computer usership became more common, more and more inventive tech experts, engineers, and lay computer aficionados experimented with computer security systems, figuring out how to violate security protocols and how to obtain and introduce information to computer systems. For a number of years, there was a largely unknown arms race between computer security professionals and individuals seeking to violate computer security for entertainment or profit. The public knew little about the subculture of hackers or about this early digital arms race until the 1983 film *WarGames*, which tells the story of a teenage hacker who hacks into the North American Aerospace Defense Command (NORAD) system, which was used at the time to control the nation's nuclear arsenal. For a generation of early hackers, *WarGames* was a hacker fantasy, telling the story of a nobody "nerd" who, thorough ingenuity and experimentation, manages to bypass the most secure computer network in the world, and then must use these same skills to save the world from annihilation. However unrealistic the story might have been in 1983, many nascent hackers were inspired by the story and the number of Americans involved in computer and network engineering exploded in the wake of the film's release. This also brought hacking and "hacker groups" to the mainstream, introducing Americans to this shadowy world of engineering misbehavior.[3]

One of the hackers inspired by *WarGames* was Loyd Blankenship, better known in hacking circles as "The Mentor," who was a member of the influential early hacking group known as the Legion of Doom (LOD). Blankenship was arrested in 1986 for violating computer security systems and, upon his release, Blankenship wrote an essay entitled "The Conscience of a Hacker," which is better known as "The Hacker Manifesto," which was published in the underground magazine *Phrack*. In his essay, Blankenship reflected on the existence of hacking as a subculture, making

the argument that hacking served a more significant purpose than simply allowing hackers to harm other people, companies, or networks, but was a statement about capitalism and freedom of information. In his manifesto, Blankenship explains:

> We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore…and you call us criminals. We seek after knowledge…and you call us criminals. We exist without skin color, without nationality, without religious bias…and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, lie to use and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.[4]

The Evolution of Hacktivism

While some might find Blankenship's screed self-serving, self-aggrandizing, or childish, many have taken inspiration from Blankenship's manifesto, and more generally, have also embraced the idea that the digital networks of the world constitute a capitalistic, corporate barrier to knowledge, free expression, and freedom of information. The idea of using hacking to make a broader political and social statement about the nature of the world and ownership of collective information, is the key behind the emergence of "hacktivism," which can be defined as the use of digital tools and manipulation techniques specifically to make a political statement.[5]

Over the years, hacking evolved in many different ways simultaneously. By far the most common use of hacking is as an avenue for profit. Legal hackers investigate security flaws in systems as a profession and provide information that is used by companies to protect their systems from attacks. Meanwhile, the birth of hacking also led to the birth of cybercrime, in which criminals use hacking and other digital tools to steal information from individuals or companies that can be used to generate profit. The most familiar activity in this realm is known as "identity theft," in which individuals use hacking or other methods to obtain an individual's personal information and then use that information to make fraudulent purchases or to gain access to credit. This is one of the earliest forms of cybercrime and has remained a core tool that cybercriminal use for profit. In the 2020s, security professionals noted that cybercriminals are increasingly using hacking to steal information on young students and children, who lack credit history and so make excellent templates for forging fake identities.

Alongside the evolution of cybercrime, hacking and other digital tools were also incorporated into governmental and military systems. The shift to the digital realm meant, on one hand, that countries needed to protect their data from external incursions, but also that military and intelligence organizations can use hacking and other tools to attack enemy states or groups. This new approach to national security and military action, called "cyberwarfare" has dramatically altered the security landscape of the world, forcing governments and security experts to adapt to an

expanding variety of threats and potential attacks. Most famously, China has been linked to attacks involving the theft of information from American corporations, while Russia used cyberwarfare tactics in an effort to influence the US political system by promoting the disruptive political career of Donald Trump.

Cyberactivism, or "hacktivism," also had its origins in the 1980s, and grew alongside the use of hacking for more nefarious purposes. Notable hacktivist incidents in the 1980s included the 1989 "Worms Against Nuclear Killers (WANK)" attack, in which a computer virus or "worm" was used to spread protest methods through the networks of National Aeronautics and Space Administration (NASA) and the US Department of Energy, protesting the launch of a shuttle carrying radioactive materials into space. One of the most common types of attacks that have been used by hacktivists involves redirecting traffic from government websites or corporate sites and replacing the landing page with protest messages. For instance, in 1996, a hacker group broke into the US Department of Justice website and replaced the photo of then Attorney General Janet Reno with an image of Adolph Hitler, while replacing the agency's name with "Department of Injustice."[6] These early examples of protest-oriented cyberhacks gave rise to more and more sophisticated methods over the years. In addition to hacking pranks, hacktivist groups have infiltrated protected data systems and leaked classified information revealing controversial government and corporate activities and have turned their attention to many different arenas of perceived injustice or misconduct, including the prison system, police and other security departments, military, and government organizations and groups.

By the twenty-first century, hacktivism was a familiar part of cyberculture, straddling the line between cybercrime and social activism, while hacking groups like "Anonymous" had become globally famous for their attention-getting activities. The techniques commonly used by hacktivist groups, like the employment of computer worms or viruses, or Distributed Denial of Service (DDoS) attacks, in which computer systems are paralyzed by a flood of misdirected traffic, have also become common in the realm of cyberwarfare and profit-driven cybercrime. Hacktivism came to the forefront of the public debate in 2022–23 as hacking groups targeted the Russian government in protest over Russia's unlawful invasion of the Ukraine. Meanwhile, state-sponsored hacking groups in Russia have targeted the Ukrainian military and allied nations supporting the Ukrainian defense against Russia.

The Ukrainian hacker war was also only one of many prominent examples of hacktivism and cyberwarfare in the period. While hacktivists battled it out to make statements about Ukrainian safety, security, and sovereignty, other hacktivist groups continue to conduct attacks to protest capitalistic exploitation, wage and income inequality, and the destruction of natural resources. The integration of digital technology into so many different aspects of public life and economics has meant that cyberactivity can use digital demonstrations to call attention to many of the different perceived ills or challenges of the world. The Ukraine cyberwar marked the first time in history that hacktivist groups were positioned as enemy combatants in a global conflict, and this demonstrated, for many analysts, the potential importance of cyberactivism in terms of national and international security, while also renewing

the debate over the perceived value and ethics of cyberactivism and hacking culture in general.

Hacking the Ethical System

Is hacktivism a type of cybercrime, or is it an important form of political expression that should be protected or, at least, considered separately from the more common types of cybercrimes used to gain profit or cyberattacks used by military organizations against enemy or competing nations or groups? Hacktivism has come a long way from the cyberprotests of the 1990s, but opinions on this kind of cyberactivism vary widely. Some believe that cyberactivists don't have the right to interfere with the jobs and work of others, infiltrating privately-owned and government-owned networks and systems to get their message across, but others see hacktivism as the inevitable next stage in the evolution of political activism, applying the tools, language, and now familiar communication formats of the Digital Age to the venerable tradition of social/political activism. Lawmakers and corporate security professionals have adapted to hacking culture in many ways, and in many regions law enforcement will decline to prosecute hackers who infiltrate systems with the goal of legitimately finding security failings and informing companies and/or organizations about the existence of these faults and vulnerabilities. Should law enforcement likewise take a different approach towards individuals and groups violating security systems to send a political message? If so, what kinds of messages should be protected and where does one draw the line between political statement and cyberterrorism? What is clear from the history of cyberactivism is that this new form of political discourse is evolving and that the full significance of hacktivism in American society is only just beginning to be understood.

Works Used

"A Brief History of Computer Viruses & What the Future Holds." *Kapersky Labs*. 2023. usa.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds.

"The Conscience of a Hacker." *Phrack*. 8 Jan. 1986. phrack.org/issues/7/3.html.

Denning, Dorothy. "The Rise of Hacktivism." *Georgetown Journal of International Affairs*. people.computing.clemson.edu/~jmarty/courses/commonCourseContent/AdvancedModule-SecurityConceptsAndApplicationToLinux/The%20Rise%20of%20Hacktivism%20_%20Georgetown%20Journal%20of%20International%20Affairs.pdf.

Ewbank, Anne. "Early Hackers Used Whistles from Cap'n Crunch Cereal Boxes." *Atlas Obscura*. 18 May 2018. www.atlasobscura.com/articles/capn-crunch-whistle.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. Simon & Schuster, 2016.

Tillett, L. Scott. "Report on Web Site Hack: This Is What Not to Do." *FCW*. 31 Aug. 1997. fcw.com/1997/08/report-on-web-site-hack-this-is-what-not-to-do/239838/.

Notes

1. Ewbank, "Early Hackers Used Whistles from Cap'n Crunch Cereal Boxes."
2. "A Brief History of Computer Viruses & What the Future Holds," *Kapersky Labs*.
3. Kaplan, *Dark Territory: The Secret History of Cyber War*.
4. "The Conscience of a Hacker," *Phrack*.
5. Denning, "The Rise of Hacktivism."
6. Tillett, "Report on Web Site Hack: This Is What Not to Do."

The Hacker Group Anonymous Has Waged a Cyber War Against Russia: How Effective Could They Actually Be?

By Jennifer Medbury and Paul Haskell-Dowland
The Conversation, February 28, 2022

A spate of cyber attacks has affected Ukraine's digital systems since Russia's invasion began. It soon became clear Russia's "boots on the ground" approach would be supplemented by a parallel cyber offensive.

Last week Ukraine called on its citizens to take to their keyboards and defend the country against Russia's cyber threat. At the same time, a campaign was underway among the hacktivist collective Anonymous, calling on its global army of cyber warriors to target Russia.

Who Is Anonymous?

Anonymous is a global activist community that has been operating since at least 2008. It brings a potential for significant cyber disruption in the context of Russia's invasion of Ukraine.

The group has previously claimed responsibility for acts of hacktivism against a wide range of targets, including against big businesses and governments. Anonymous's activities are often aligned to major events, and the group claims to have an "anti-oppression" agenda.

The collective has no defined structure or leadership. Acts are simply undertaken under the banner "Anonymous", with some reports of limited rules of engagement being used to guide actions (although these are likely fluid).

As Anonymous is a movement, with no formal legal status or assets, responsibility for actions shifts to individuals. But there remains a fundamental issue of attribution in cyber security incidents, wherein it's difficult to determine a specific source for any attack.

What Are They Threatening to Do?

On February 16, Anonymous TV posted a video message with a series of recommendations and threats. Leaning on the stereotypical "hacker" image, the masked speaker issues a serious warning to Russia:

> If tensions continue to worsen in Ukraine, then we can take hostage […] industrial control systems. Sole party to be blamed if we escalate on that will be the same one who started it in the very first place with troop buildups, childish threats and waves of unreasonable ultimatums.

Several Russian government websites and media outlets have since been targeted, with Anonymous taking credit on its Twitter channel.

The attacks have leveraged the same distributed denial of service techniques used in many previous cyber attacks, including attacks on Ukrainian banking and government websites. In such attacks, the attacker knocks targeted websites offline by flooding them with bot traffic.

Further incidents have included the theft and publication of Russian Department of Defence data, which may contain sensitive information useful to fighters in Ukraine. Emails from Belarusian weapons manufacturer Tetraedr and data from the Russian Nuclear Institute have also reportedly been accessed.

It's too early to determine how useful these data may be. Most of the stolen information will be in Russian, which means translators will be needed to help examine it.

Russian TV channels were also attacked and made to play Ukrainian music and display uncensored news of the conflict from news sources outside Russia.

It's hard to be certain that Anonymous did carry out the cyber attacks for which it has claimed responsibility. The movement is founded on anonymity, and there are no viable means of verification. But the tactics, targets and theatrics on show are consistent with previous attacks claimed by the group.

Also, even if some attacks are not a direct consequence of Anonymous's actions, one could argue this doesn't really matter. Anonymous is all about being perceived as having an impact.

Will It Make a Difference?

It's unlikely the cyber attacks claimed by Anonymous will have a significant impact on Russia's intent or military tactics. That said, these actions could provide key intelligence about specific tactics Russia is using, which would be valuable to the Ukrainians and their allies.

A further benefit is that the impact of the invasion on Ukrainian people is getting more publicity—especially within Russia, where news is significantly censored. This could help counter Russia's domestic propaganda machine, and present a more balanced view of events.

Cyber attacks will likely continue to escalate on both sides, involving both state and non-state actors. Russia's National Computer Incident Response and Coordination Center has raised its threat level to "critical", indicating concerns about Russian infrastructure being targeted through cyber attacks.

Citizen Hackers

Alongside Anonymous, large numbers of Ukrainian cyber professionals have volunteered to assist with Ukraine's cyber defence. The volunteers are being organised through Telegram channels and other encrypted apps.

Russian TV channels were also attacked and made to play Ukrainian music and display uncensored news of the conflict from news sources outside Russia.

Their goals include defending Ukraine's critical infrastructure, helping the government with cyber espionage, taking down Russian disinformation from the web, and targeting Russian infrastructure, banks and government websites.

But despite reports of some 175,000 joining the cyber army's Telegram channel, its impact so far remains unclear.

Print Citations

CMS: Medbury, Jennifer, and Paul Haskell-Dowland. "The Hacker Group Anonymous Has Waged a Cyber War Against Russia: How Effective Could They Actually Be?" In *The Reference Shelf: Hacktivism,* edited by Micah L. Issitt, 31–33. Amenia, NY: Grey House Publishing, 2023.

MLA: Medbury, Jennifer, and Paul Haskell-Dowland. "The Hacker Group Anonymous Has Waged a Cyber War Against Russia: How Effective Could They Actually Be?" *The Reference Shelf: Hacktivism,* edited by Micah L. Issitt, Grey House Publishing, 2023, pp. 31–33.

APA: Medbury, J., & Haskell-Dowland, P. (2023). The hacker group Anonymous has waged a cyber war against Russia: How effective could they actually be? In M. L. Issitt (Ed.), *The Reference Shelf: Hacktivism* (pp. 31–33). Grey House Publishing. (Original work published 2022)