ANTHROPOLOGY OF AN IDEA
HACKTIVISM

COMPUTER HACKERS AREN'T an especially earnest bunch. After all, lulz (a corruption of the phrase "laugh out loud" and a reference to hackers' penchant for tomfoolery) was the primary objective of the hacker collective Anonymous before it graduated to more serious cyberoperations in the latter half of the 2000s. But if the hacking community likes to flaunt its glib side, it also has a rich history of political activism—or "hacktivism"—that has come to define it in the era of WikiLeaks. If there's one thing that unites hacktivists across multiple generations, it's dedication to the idea that information on the Internet should be free—a first principle that has not infrequently put them at odds with corporations and governments the world over.

—Ty McCormick

1950s-1980s A culture of "hacking" springs up at the Massachusetts Institute of Technology, where the term is coined by members of the Tech Model Railroad Club as they play around with track circuitry. The original "hacks" are mostly harmless pranks and practical jokes perpetrated by students in early artificial intelligence labs. Hackers soon discover that toy whistles produce the right frequency for them to "phreak" Ma Bell's telephone system, allowing them to place long-distance calls for free.

Among those who make names for themselves as "phone phreaks" are Steve Wozniak and Steve Jobs, the future founders of Apple.

OCTOBER 1989 Computers at NASA and the U.S. Energy Department are penetrated by an anti-nuclear "wank" worm, which alters computers' log-in screens to "WORMS AGAINST NUCLEAR KILLERS ... Your System Has Been Officially WANKed." The malware, believed to have originated in Australia, is the second major worm deployed in history, but the first with an explicitly political aim. (The genesis worm was released a year earlier by Robert Morris, a 23-year-old Cornell University graduate student, who said he wanted to approximate the size of the Internet but ended up running afoul of the U.S. Computer Fraud and Abuse Act.)

NOVEMBER 1994 A mostly British activist group known as the Zippies launches an "email bomb" and distributed denial-of-service (DDOS) attack against British government websites to protest Prime Minister John Major's Criminal Justice and Public Order Act, which outlawed outdoor raves featuring music with "a succession of repetitive beats." The attack, known as the "Intervasion of the UK," knocks out a number of government websites for more than a week. It is the first known use of DDOS—which takes down a targeted website by overwhelming it with communication requests—for political purposes.

1996 "Omega," a member of the Texas-based computer-hacking group Cult of the Dead Cow (cDc), coins the word "hacktivism" in an email to the cDc listserv. Although somewhat tongue-in-cheek, the term aptly characterizes the group's increasingly political ethos. Founded in 1984 for the whimsical goal of "global domination through media saturation," cDc is by the mid-1990s an explicitly political organization, one that leverages technology to advance human rights and protect the free flow of information. In subsequent years, cDc members team up with a group of dissidents calling themselves the Hong Kong Blondes to hack the computer networks of Chinese government agencies and companies with poor human rights records in China.

> "State-sponsored censorship of the Internet is a serious form of organized and systematic violence against citizens."
>
> *—Hacktivismo Declaration, July 4, 2001*

JULY 2001 Hacktivismo, an offshoot of cDc, issues a code of conduct for online civil disobedience that draws on the United Nations' Universal Declaration of Human Rights and its International Covenant on Civil and Political Rights. This "Hacktivismo Declaration" affirms the right to "freedom of opinion and expression" and declares the hacker community's intent to develop technologies to challenge "state-sponsored censorship of the Internet." The declaration, which can be read as a disavowal of hacking techniques like DDosing that interfere with free speech, largely falls by the wayside as the next generation of hacktivists increasingly seeks to take government and corporate websites offline.

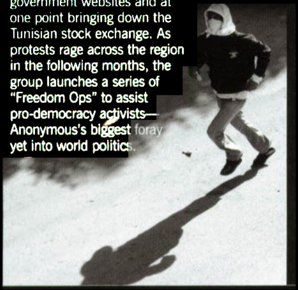
TOM MUNNECKE/HULTON ARCHIVE/GETTY IMAGES

2003 Christopher Poole, 15, sets up the website 4chan.org from his suburban New York bedroom. The site garners attention primarily for its proliferation of humorous feline memes (LolCats) and gag hyperlinks (Rickrolls) to Rick Astley's insufferable 1987 hit "Never Gonna Give You Up," but over time it attracts a global army of anonymous hackers, many of them politically minded, who exchange coding tips and eventually plot cyberops. What begins as a series of pranks carried out for idle amusement gradually evolves into systematized cyberwarfare or, as one Anonymous member puts it, "ultra-coordinated motherfuckery." Anonymous is born here.

APRIL 2007 Estonia removes a Soviet war memorial from its capital, provoking a series of cyberhits—mostly DDOS attacks—originating on Russian servers. Details about who is responsible for the attacks, which disable various Estonian government websites and substantially disrupt commerce for several hours, remain murky, but the pro-Kremlin youth group Nashi eventually claims responsibility, though it denies having carried out direct orders from the Russian government. Whether state-sponsored or an especially virulent example of nationalist hacktivism, the cyberassault against Estonia amounts to one of the largest DDOS attacks in history.

JANUARY 2008 Anonymous releases a YouTube video announcing Project Chanology, a deliberate campaign to destroy the Church of Scientology due to its "campaigns of misinformation" and "suppression of dissent." "We are Anonymous. We are legion. We do not forgive. We do not forget. Expect us," the group declares in an ominous, automated voice. Less than a month later, Anons hold their first physical protest (also against Scientology) simultaneously at various locations around the world, with many demonstrators wearing the signature Guy Fawkes masks that will later become iconic symbols of the movement.

NOVEMBER 2010 Tunisian dictator Zine el-Abidine Ben Ali blocks access to WikiLeaked U.S. State Department cables noting massive corruption in his government. In response, Anonymous hackers launch "#OpTunisia," attacking Tunisian government websites and at one point bringing down the Tunisian stock exchange. As protests rage across the region in the following months, the group launches a series of "Freedom Ops" to assist pro-democracy activists—Anonymous's biggest foray yet into world politics.



DECEMBER 2010 Anonymous launches Operation Avenge Assange after MasterCard and Visa block payments to the whistle-blowing website WikiLeaks. Anons knock out the websites of the credit card giants and briefly slow web traffic to PayPal using an application called Low Orbit Ion Cannon, which directs massive amounts of traffic to specified websites.

DECEMBER 2011 AntiSec, an offshoot of Anonymous that takes particular issue with the cybersecurity industry, hacks the Texas-based private intelligence firm Stratfor, knocking its website offline and lifting 200GB of data, mostly emails, which it hands over to WikiLeaks. It is the largest public "d0xing"—the posting of private information online—attack that Anonymous has carried out to date.

JANUARY 2012 A group of pro-Palestinian hacktivists calling themselves "Nightmare" knocks out the websites of the Tel Aviv Stock Exchange and El Al airlines. In an online post taking credit for the attacks, the group says it is joining Saudi hacker OxOmar, who previously released tens of thousands of Israelis' credit card numbers on the Internet, in a "movement" of "Islamic hackers against Israel." The next day, Israeli hackers going by the name IDF-Team retaliate by knocking the Saudi Stock Exchange and the Abu Dhabi Securities Exchange offline.

FEBRUARY 14, 2012 On the one-year anniversary of Bahraini armed forces' violent dispersal of rallies in the capital, Manama, during the Arab uprisings, Anons carry out a series of hacks against the Bahraini government and its backers, notably the Pennsylvania-based tear gas manufacturer Combined Systems. The kingdom is eventually moved, in February 2013, to ban the import of Guy Fawkes masks to its still-roiling territory.

FEBRUARY 29, 2012 Interpol arrests 25 suspected Anonymous hackers from around the world following an FBI sting operation that flipped an Anonymous ringleader, Hector Monsegur, known online as "Sabu." The information he provides leads to a wave of hacktivist arrests—for taking part in everything from the Stratfor hack to illegal eavesdropping on an FBI conference call—dealing Anonymous a major blow.

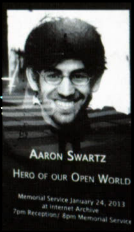
MARCH 2012 Frustrated with the way WikiLeaks handled the Stratfor data dump—it was an unqualified media flop—Anonymous launches its own WikiLeaks clone: Par:Anoia (Potentially Alarming Research: Anonymous Intelligence Agency). The website relies on purloined "submissions" provided by the Anonymous community and publishes everything from hacked emails from the Syrian Foreign Ministry to New York City Police Department video footage of the 2011 eviction of Occupy protesters from Zuccotti Park.

> **"We will lay waste to your servers, spread the truth about your illegitimate government, show solidarity with our brothers and sisters in Bahrain, and expose your crimes against humanity."**
>
> *—Anonymous message to Bahrain, March 9, 2012*

APRIL 2012 Anonymous turns its guns on China, knocking out a number of corporate and local government websites and tagging them with the message: "Dear Chinese government, you are not infallible, today websites are hacked, tomorrow it will be your vile regime that will fall."

OCTOBER 2012 WikiLeaks puts millions of its documents behind a pay wall, prompting a vicious rebuke from the freedom-obsessed web underground. The main Anonymous Twitter account tweets @wikileaks: "die in a fire." The Anonymous-WikiLeaks breakup is complete.

JANUARY 2013 Computer whiz kid and Internet activist Aaron Swartz hangs himself in his New York City apartment after federal prosecutors indict him for hacking into JSTOR's digital library, presumably to free millions of academic articles from behind its pay wall. His death in many ways symbolizes the battered state of the hacktivist movement and the futility of its utopian vision—after all, Swartz stole mostly obscure journal articles—but hardly sounds its death knell. Within weeks of Swartz's death, sympathetic Anons hack into the website of the government agency responsible for the sentencing policies of federal courts, at one point turning its home page into a version of the computer game Asteroids.


AARON SWARTZ
HERO OF OUR OPEN WORLD
Memorial Service January 24, 2013
at Internet Archive
7pm Reception/ 8pm Memorial Service

REID BEELS/FLICKR; STR/AFP/GETTY IMAGES; EPA/OLIVER WEIKEN; YOUTUBE; STEVE RHODES/FLICKR