White Paper

Hacktivism

Cyberspace has become the new medium for political voices

By François Paget, McAfee Labs™

Table of Contents

What is hacktivism? It combines politics, the Internet, and other elements. Let's start with the political. Activism, a political movement emphasising direct action, is the inspiration for hacktivism. Think of Greenpeace activists who go to sea to disrupt whaling campaigns. Think of the thousands of activists who responded to the Adbusters call in July 2011 to peacefully occupy a New York City park as part of Occupy Wall Street.

Adding the online activity of hacking (with both good and bad connotations) to political activism gives us hacktivism. One source claims this term was first used in an article on the filmmaker Shu Lea Cheang; the article was written by Jason Sack and published in *InfoNation* in 1995. In 1996, the term appeared in an online article written by a member of the American group Cult of the Dead Cow.[1] In 2000, Oxblood Ruffin, another member of CDC, wrote that hacktivists use technology to defend human rights.[2] At times citing libertarian ideals (a desire to preserve free enterprise, individual freedoms, freedom of speech, and freedom to circulate information), many activists also argue that the Internet should be free. The Anonymous movement is the epitome of hacktivism. Focusing initially on actions to uphold their notion of the Internet, they have expanded their activities from web actions to struggles that are also happening in the streets.

Hacktivism is not a new phenomenon. Three years ago events in the former Soviet republics of Estonia (in 2007) and Georgia (in 2008) brought hacktivism to the world's attention. These two cyberattacks, which seemed more like the beginnings of a cyberwar than what we now call hacktivism, are quite unlike the attacks that targeted the opponents of WikiLeaks and companies such as Monsanto.

Key Dates in the Origins of Hacktivism

Date	Comment
September 12, 1981	The Chaos Computer Club forms in Berlin.[3]
1984	The book *Hackers: Heroes of the Computer Revolution*, by Steven Levy, is published.
January 8, 1986	*The Hacker Manifesto*, by Loyd Blankenship (a.k.a. The Mentor), is first published.
October 16, 1989	Using the DECNET protocol, a worm spreads through a NASA computer network in Maryland. Named WANK (Worms Against Nuclear Killers), one of its objectives is to broadcast a message denouncing the evils of nuclear tests.[4]
November 5, 1994 (Guy Fawkes Day)	The Zippies, a group in San Francisco, launches a distributed denial of service (DDoS) and mail bombing campaign against British government servers to protest a law prohibiting outdoor music concerts with a repetitive beat.[5]
December 21, 1995	In Italy, the Strano Network decides to block French websites to protest against nuclear testing in Mururoa.[6]
February 9, 1996	John Perry Barlow publishes *A Declaration of the Independence of Cyberspace*.
June 30, 1997	The Portuguese hacker group UrBan Ka0s attacks around 30 Indonesian government sites to draw attention to the oppression of the people of Timor.[7]
January 29, 1998	In support of Zapatista guerrillas, a virtual demonstration is held in response to a massacre committed by paramilitary forces in a village in Chiapas, Mexico.[8]
November 1999	Toywar: an act of resistance against the toy distributor eToys Inc., which had sued a group of artists under the pretext that its domain name was too close to theirs.[9]
December 3, 1999, 4pm GMT	The Electrohippies Collective organizes a virtual sit-in, asking all of its supporters to visit World Trade Organization web pages to block the final communiqué of the Seattle, Washington, conference from being issued.[10]
June 20, 2001	To protest against the use of Lufthansa airplanes to deport undocumented migrants out of Germany, two German humanitarian networks organize a virtual protest to block the airline's website by bombarding it with emails.[11]

Today, hacktivism combines three major groups:

1. **Anonymous**, the most publicized component of the movement. Its members are known for supporting a free Internet and for opposing anyone they accuse of impeding information flow. Their methods often involve hacking, including DDoS attacks, and stealing and distributing personal and/or confidential information. Often favoring jokes in bad taste, they sometimes seem to be moving away from political acts. A large portion of this paper is devoted to them.
2. **Cyberoccupiers**, the real activists. They primarily use the Internet and social networks to build relationships and to spread propaganda and information. They include **cyberdissidents** who, like their counterparts in real life, no longer recognize the legitimacy of the political power they are expected to obey. By attempting high-profile actions on the Internet, they hope to bolster democracy and fight corruption in their countries.
3. **Cyberwarriors**, patriots who group together as "cyberarmies" that thrive in many countries with totalitarian tendencies. Whether or not it is true, these groups claim to act on behalf of their governments by supporting national and extremist movements. Their main weapon is to deface websites. Also using DDoS tools, they do everything they can to silence dissidents.

The Anonymous Movement

Origins

The origins of Anonymous can be found in the image forums on 4chan. Created in 2003 and initially devoted to manga culture, the website is currently one of the most frequently visited on the Net, with about 9.5 million unique visitors per month.[12]

Anonymous is an offshoot of its most active section, "/b/." According to its creator, Christopher "moot" Poole, the /b/ imageboard received 150,000 to 200,000 messages a day in 2008.[13] Absolute freedom of speech and anonymity are two of its major tenets. On this site, laughing out loud (lol) rubs shoulders with "lulz," its evil counterpart.[14] Hard-core pornography and scatological, racist, or anti-Semitic images appear alongside schoolboy photographic montages containing "lolcats," highly visited photos of cats shown in the most unlikely circumstances. Unless they are noticed or reintroduced, the large number of submissions nearly all pass into oblivion. There is no sign-up system on the site. Anyone can write on it, and most people post without a username, which gives them the default name—anonymous.

At that time, Anonymous members also frequented the Encyclopedia Dramatica (created by Sherrod De Grippo in December 2004).[15] A double of Wikipedia, it satirically—and even shockingly—documented anything in the news.

In 2006 Anonymous achieved its first great coup, known as the Habbo raid. By coordinating on 4chan and using avatars depicting black Americans all wearing gray suits, the group blocked adolescent avatars from accessing the pool in the virtual world of Habbo Hotel. Even then, their motivations were ambiguous. For some, it was simply for fun; but for others, it was a way to highlight the lack of black characters in social networking.

Another early target for Anonymous was pedophiles. In 2007, Anonymous identified a Canadian pedophile who was later arrested thanks to their research.[16] Again, however, the motivation was unclear. Pedophilia-related images and jokes are frequently circulated on 4chan, which features an icon called Pedobear. Frédéric Bardeau and Nicolas Danet, authors of the book *Anonymous*, write "in 4chan culture, people denounce paedophiles while at the same time mocking people who publish, not always happy, pictures of their children on the Internet."[17]

Anonymous really became known to the public in 2008 through the Chanology project.[18] This project is still going on today, and its goals have not changed. The project protests the founding myths of Scientology in a nonviolent way, along with its obscurity and the dangers it brings upon its members by isolating them from the outside world.

On February 10, 2008, Anonymous hit the streets. To avoid being identified by the Scientologists, they wore the masks of Guy Fawkes, the comic book hero featured in the film *V for Vendetta*.

Poster for the film *V for Vendetta*

Guy Fawkes (1570-1606) was an English Catholic who planned to assassinate King James I on November 5, 1605, in response to his policy on religion, which he felt lacked tolerance.

The 1980s comic book series V for Vendetta, written by Alan Moore and drawn by David Lloyd, later adapted to film in 2006 by the Wachowski siblings, deals with a completely different story. The action takes place in London around 2040, in a dictatorial society where a freedom fighter named "V" is trying to establish political and social change, carrying out a violent personal vendetta against the powerful. He wears a mask with the face of Guy Fawkes, whom he wants to imitate by inciting the people to break free of their lethargy. After being reworked for the film, the mask was adopted by Anonymous members to forge an identity.

We will not detail all of the actions Anonymous carried out between 2006 and the start of the WikiLeaks Cablegate operation. However, the following table provides a summary.

Key Dates in the History of Anonymous

Date	Comment
July 12, 2006	Great Habbo Raid. First raid on the Habbo Hotel social network for adolescents. Highlights the lack of black characters.
December 2006	Attack on the website of American nationalist Hal Turner.
August 2007	Support for Burmese monks during the Saffron Revolution.
December 5, 2007	Arrest of the pedophile Chris Forcand in Canada. "Cybervigilante" members of 4chan seem to have helped the police.[19]
January 14, 2008	Chanology Project. Uploads propaganda video on YouTube that was meant to be internal to Scientology. Although it was quickly removed, posting the video was the springboard for 4chan's fight against Scientology.
March 28, 2008	Info or intox. Anonymous members are accused of inserting JavaScript animations and messages on the Epilepsy Foundation's forum to cause migraines and seizures in people with epilepsy.

Date	Comment
June 2008	Hip-hop music sites SOHH and AllHipHop are attacked after publishing insults about 4chan supporters.
January 2009	A young California man is harassed for having created a website to protest swearing (No Cussing Club).
April 2009	Operation MarbleCake. Manipulates a Time magazine poll to name the most influential person in the world.[20]
April 2009	Operation Baylout. Controversy surrounds the Telecom Reforms Package (a set of EU directives targeting illegal downloads). Attacks the IFPI (an international union representing the recording industry).
May 20, 2009	YouPorn Day. Seemingly harmless videos distributed on YouTube that hid pornographic scenes.
June 2009	Support for Iranian dissidents.[21]
September 2009	Operation Didgeridie (Project Skynet). Aggressive first phase ("destructive operation") to protest against an Australian government bill to filter data on the Internet.
October 2009	Operation CyberDyne Solutions (Project Skynet). Informative second phase to educate people on how to bypass Internet blockages.
January 6, 2010	YouPorn Day (second edition) to protest against the closing of Lukeywes1234's account (called the king of /b/).[22]
February 10, 2010	Launch of Operation Titstorm. Protesting the decision of Australian authorities to ban the publication of pornographic images.[23]
September 2010	Operation Payback. Starts after an Indian company announced that it had conducted DoS attacks on Bit Torrent sites used for downloading free videos and music that are normally protected by copyright. In response, many sites associated with the film and music industry and artists are attacked.[24] A timeline of this operation is at myce.com.[25]

Anonymous is an Internet meme, a mass phenomenon propagated by multiple communities made up of Internet users acting anonymously toward a specific goal. An Internet meme refers to the sociological concept of a meme, a recognizable cultural element that is replicated and transmitted by the behavior of one individual being imitated by other individuals.

Defining the movement

Although Anonymous members hit the streets to protest against Scientology, their main combat ground is now the Internet, and their main actions consist of responding to any attempt to regulate the Internet. For them, online freedom is both about being able to distribute "trash" images and about fighting censorship in Iran. It's the ability to freely download music and videos without worrying about copyrights and to promote complete freedom when circulating information, even if it comes from sources that were not intended to become public. Thus it was obvious that Anonymous would support WikiLeaks as soon as it became clear that some wanted to silence it.

Anonymous is more of an idea than a group. It's a meme that its individual members can adopt to act anonymously.[26]

A distributed denial of service (DDoS) is a computerized attack that uses machines distributed across the network, usually part of a botnet (robot network). The goal is to make an Internet service unavailable to its users. It can be used to block a file server, cause a web server to be inaccessible, prevent email from being distributed in a company, or make a website unavailable. A denial of service (DoS) is caused by a single source.

Anonymous is a label that is assigned at a given moment to individuals carrying out specific actions, even if those actions are not very sophisticated. Although they seem to have no real leaders, they meet occasionally to carry out concerted actions—anything from fun (often in bad taste) to activism—for which they find a common motivation. Any Internet user can connect to an IRC chat network, participate in discussions, and join or suggest an "operation" on a topic. At its highest levels of activity, particularly during the Arab Spring or Operation Payback, the chat networks are said to have reached a peak attendance of 3,000 people connected simultaneously.

An operation most often consists of making one or more websites inaccessible. To do this, Anonymous members use various types of attack software; the most popular are LOIC (Low Orbit Ion Canon, an open-source network testing and DoS creation tool) and HOIC (the related High Orbit Ion Canon). With it, they overload a target site with queries until it is saturated. This is called a distributed denial of service (or DDoS), which is hard for any site to withstand.

Anonymous members usually post videos to announce and claim responsibility for operations. These often feature a synthesized voiceover, which has become the hallmark of Anonymous. Besides using IRC channels and videos, Anonymous members communicate through Twitter, Facebook, and various websites. Whatever the medium, the message always ends with the words, "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us." The quality of the videos and images shows that their range of skills includes graphic arts.

On November 28, 2010, Operation Cablegate began. Without revealing any crucial information, WikiLeaks began to publish U.S. diplomatic cables that provided an unprecedented viewpoint of the inner workings of power. Anonymous was displeased with the show of strength that followed attempting to silence WikiLeaks. They responded and moved to center stage.

WikiLeaks meets Anonymous

WikiLeaks was founded in 2006 by the Australian Julian Assange, who resolutely believes that access to information is far from being equal between governments and their citizens. To remedy this situation, he suggested becoming an intermediary between the public and the whistleblowers he promised to protect. To guarantee the anonymity of its informers, he turned to Jacob Appelbaum, an active participant in TOR (The Onion Project, free software that allows an Internet connection without revealing the IP address). Over the years, WikiLeaks has released public and, often, secret documents.

The following table lists a number of documents that were released between 2006 and November 2010, a milestone month in the history of Anonymous and hacktivism.

Key Dates in the Life of WikiLeaks

Date	WikiLeaks Publications
December 2006	A memo concerning a political assassination order in Somalia
August 2007	A report accusing the former president of Kenya, Daniel Arap Moi, and his family of corruption[27]
November 2007	U.S. Army manual from 2003 on the prison at Guantanamo Bay[28]
March 2008	An internal document from the Church of Scientology's Office of Special Affairs[29]
May 2008	Working document on the Anti-Counterfeiting Trade Agreement (ACTA)[30]
April 2009	Summary of hearings for Belgian pedophile Marc Dutroux[31]
July 2009	An internal document belonging to Iceland's Kaupthing Bank, describing various low-quality loans it is supposed to have approved, a few days before it was nationalized[32]
November 2009	Emails and files assigned to officials of the Climatic Research Unit of East Anglia (United Kingdom)
April 2010	Collateral Murders: A U.S. Army video showing two Reuters photographers killed in Bagdad during an air raid on July 12, 2007, taken from an Apache helicopter. Nicknamed "Project B" by Assange, this publication marks the beginning of the website's global fame.
July 2010	Afghan War Diary: 91,000 secret U.S. military documents on the war in Afghanistan (in collaboration with *The Guardian*, *The New York Times*, and *Der Spiegel)*
October 2010	Iraq War Logs: 391,832 secret documents on Iraq, covering a period from January 1, 2004, to December 31, 2009
November 28, 2010	Cablegate: WikiLeaks begins to reveal U.S. diplomatic telegrams. It announces that it has more than 250,000.

Like Jester, many hacktivists and hackers write using "leet speak" (or "elite speak"), the use of numerals or symbols that generally resemble the shape of the letters to make the result less understandable.

For example, *leet speak* can be written as:

- L33T 5P34K in base coding
- 1337 5p34k in light coding
- £33‡ šp3@ķ in medium coding
- |_ 33¯|¯ _/¯|°3/-\|< in high coding

(Source: Wikipedia. *http://en.wikipedia.org/wiki/Leet*)

On December 3, 2010, the WikiLeaks PayPal account was suspended; meanwhile the number of lawsuits grew. The hacker known as Jester (th3j35t3r), who calls himself a "hacktivist for good," claimed to have temporarily shut down the WikiLeaks site. To do this, he used his own DoS tool, called XerXes, which he regularly uses against jihadist websites.[33]

In response to concerns about limited accessibility, WikiLeaks was copied to about 20 "official" sites, most of which were located in countries with liberal digital legislation. On December 4, with the Internet community mobilized to help, several hundred mirror sites appeared around the world. One of these sites was established in Russia (mirror.wikileaks.info/IP: 92.241.190.202) by an Internet Service Provider (Heihachi Ltd.) known for its association with cybercrime. The domain wikileaks.org was then pointed to this particular site. Spamhaus warned Internet users of the dangers of this mirror.[34] The organization suffered DDoS attacks in return.

As financial penalties continued to be imposed on Julian Assange over the following days (by PostFinance, MasterCard, Visa International, and Amazon), Anonymous came on the scene. It set up DDoS attacks against anyone who opposed WikiLeaks. Operation Payback, which originally targeted opponents of Internet piracy, broadened to include new objectives. Volunteers were invited to download LOIC, which used its "hive mind" function to transform each machine into a voluntary bot to allow a coordinated attack. At the height of the attacks, there were as many as 3,000 supporters connected at one time.

WikiLeaks and Anonymous had already crossed paths a number of times. In 2008, the disclosures pertaining to Scientology and ACTA had uncovered their shared interests. At the end of March 2010, before launching the Collateral Murders video (showing the Reuters photographers killed in Baghdad during the July 12, 2007, air raid), Assange was in Reykjavik with Raffi Khatchadourian, a journalist for *The New Yorker*. The magazine reports that, when leaving for the press conference in New York, the WikiLeaks founder said the words, "Remember, remember the 5th of November."[35] This is a clear reference to the work of Guy Fawkes, the Anonymous hero who tried to blow up the English Parliament in 1605.

Around December 10, 2010, a group of hacktivists claiming to be from Anonymous altered their strategy. The arrest of some young LOIC users may have caused them to change their minds. The hacktivists announced Operation Leakspin, and called themselves "a spontaneous collective of people who share the common goal of protecting the free flow of information on the Internet. ... Anonymous is not always the same group of people: Anonymous is a living idea."[36] The collective asked Internet users to undertake their own investigative work on diplomatic cables published by WikiLeaks. The goal was to speed up the discovery process to publish commonly known facts that had not yet been revealed to the media. Anonymous called this crowd journalism, a participative form of journalism that works in a similar fashion to the Wikipedia model. The group suggested another initiative, Operation Black Face, to users frequenting social networks. On December 18, they were asked to replace their profile photos with a black background as a sign of support for WikiLeaks and for Julian Assange. Without much success, some Anonymous members also hit the streets to distribute leaflets (Operation PaperStorm).

Operation Payback: Calling for support of WikiLeaks

All types of operations sprang up throughout the month of December. These were overwhelmingly focused on defending WikiLeaks. Despite a drop in intensity due to calls for other types of actions, some DDoS attacks took place in late December with Bank of America as the main victim. With Jester at the helm, anti-WikiLeaks hackers tried to unmask the Anonymous members participating in the attacks. Within the movement, further divisions led to conflicts between those accused of being mere script kiddies, eager to hack indiscriminately, and those who preferred more militant actions against their targets.

The end of 2010 heralded a period of mudslinging and diversification. Zimbabwe was the first country to suffer the wrath of Anonymous. Let's analyze this example to understand how decisions are made within the group.

In mid-December 2010, the wife of President Robert Mugabe threatened the editorial staff of a local newspaper, which had used information from several diplomatic cables revealing that the country's first lady allegedly became rich through the illegal sale of diamonds.[37] The decision to attack the website of the president's party was made during the evening of December 28 on the IRC channel #operationBOA.AnonOps. At that time several members launched a discussion over their next target.[38] The discussion focused on the government sites of countries accused of somehow violating freedom of speech on the Internet. Hungary, Poland and Iran were mentioned, but the most compelling target was Zimbabwe. Just a few minutes later, the instigator of the project created the #OperationZimbabwe channel, containing instructions for configuring the LOIC software. One hour later, a government site was unavailable; and during the night one of the country's Ministry of Finance sites was defaced. Some of the home page's content was replaced by the message "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us."

A script kiddie is a derogatory term referring to someone who is often young and trying to pass for a hacker, despite limited or no knowledge of computer systems. They are often accused of using—and not mastering—scripts and programs they download from the Internet, without attempting to understand them.

Fifteen Months of Activity

In early January 2011, Anonymous decided to expand its scope, even though the WikiLeaks affair was still being discussed. During the first quarter of the year, the group encouraged the Arab Spring. Three months later, despite a bit of confusion, the group Lulz Security came on the scene. It conducted all-out hacking activities that eventually attracted attention. At the same time other attacks were reminiscent of the early activities of Anonymous, acting more for fun than for ideology against anything. In the middle of 2011, distinct centers of interest emerged to demonstrate the multiculturalism of Anonymous.

Law enforcement scored a few points by increasing the number of arrests in the United States, United Kingdom, and Holland. The police were the target of numerous attacks by AntiSec and by anyone accusing them of brutality at various gatherings organized by the Occupy or Indignant movements.

By the end of 2011, the media were fully aware of Anonymous, which remained active, although its divisions—and even manipulations—did not help others understand the movement. Attempts at coordinated actions between demonstrators and cyberdemonstrators still had little impact. It was not until the beginning of 2012 that numerous Guy Fawkes masks appeared in the streets.

Let's look at the highlights of this history.

Arab Spring

January 2, 2011, marked the start of the Tunisia operation. At first, it protested the blocking of the main point of access to the WikiLeaks site in the country. The attacks usually targeted an imaginary Tunisian named Ammar 404, a play on the "Error 404" message returned by web browsers when attempting to access one of the many sites blocked by the Ben Ali regime. Very quickly, the objectives broadened to a general protest against the sitting regime, in connection with the street protests that left dozens dead.

AMMAR 404: censorship of the web in Tunisia

After the fall of President Ben Ali on January 15, Anonymous felt it had played a substantial role in the Jasmine Revolution. The group claimed, "We are at war … a war that Anonymous is winning."[39]

This statement was hyperbole. The revolution was successful due to the Tunisian protestors who were not afraid to continually demonstrate in the streets. The Internet's share in the success of this revolution, and in those that followed, seems rather limited. Those Internet users who played a role did so primarily through social networks (Facebook and Twitter)—banding together local demonstrators and foreign journalists and providing information in real time.

In early 2011, Anonymous issued calls to mobilize for similar causes in Egypt (the first message on AnonNews was dated January 23), Saudi Arabia, Algeria (January 20), Libya (February 18), Iran (February 9), Bahrain (February 17), Syria, Jordan, Yemen, and Morocco (February 15).

The informal hacker group RevoluSec, which revolves around Anonymous, carried out operations to deface several official sites belonging to Syrian cities. The group created a digital memorial for the victims of the conflict, represented by many red human shapes. In this example, we can see how Anonymous provides a digital body of information to support the reality of local conflicts.[40] We'll discuss hacktivism in Syria, primarily the actions of the Telecomix group, in the section on cyberdissidents.

HBGary

Another highlight of the first quarter comes from *The Financial Times*. On February 5, 2011, the newspaper announced that Aaron Barr, the CEO of HBGary Federal, intended to provide the U.S. Federal Bureau of Investigation (FBI) with information he gathered about Anonymous.[41] The group immediately began attacking his company's servers. Through SQL injection, weak passwords, and social engineering, they were able to divert more than 70,000 emails, which were quickly made public. The content of some of those emails was so destructive to Barr that he resigned three weeks later.[42] The company was also heavily criticised in the media.

Anonymous published a file of its HBGary discoveries. It contained more than 130 names or usernames, along with personal data.

Lulz Security and denouncements

Since the end of the first quarter of 2011, part of the Anonymous movement has favoured political activism. It criticised the disorderly actions carried out by a small group of hackers said to be close to the Gn0sis group. In December 2010, Gn0sis hacked Gawker Media, a U.S. online media group with a long-standing difficult relationship with Anonymous and 4chan.[43] At that time Gn0sis was very active. Some of the group are suspected of being behind the HBGary hacking.

This group prefers fun in bad taste (lulz) to activism. They meet regularly on the popular IRC channel #HQ. When they interact with Sabu, who is apparently their leader, their usernames are Topiary, Kayla, Tflow, m_nerva, and Joepie91.

On May 7, 2011, under the name of Lulz Security (or LulzSec), the group began to claim responsibility for various acts of hacking. Their work is usually signed with the slogan "for the lulz." Two days later, as tensions mounted between the two clans, the website anonops.net/ru, the main entry point for the Anonymous community, was hacked by Ryan, a coadministrator who is close to Lulz. In the words of his opponents, he tried to organize a coup within Anonops and gain control of the site.

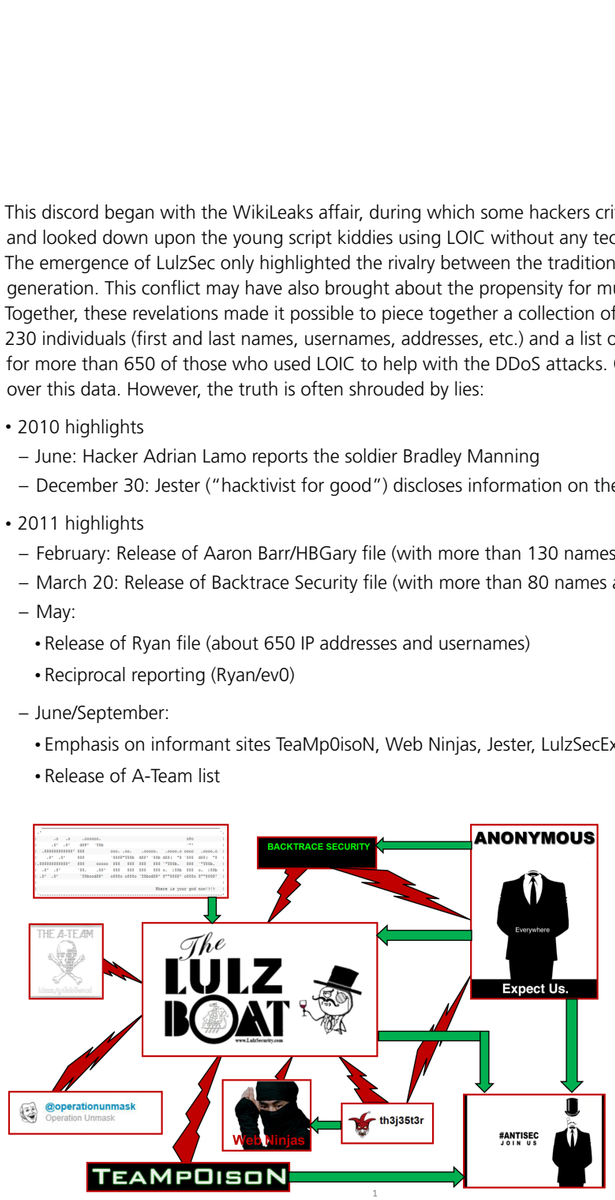
On May 18, journalist Barrett Brown, an unofficial spokesperson for Anonymous, gave an interview to Computerworld in which he denounces Ryan's irresponsible attitude.[44]

For 50 days, Lulz Security made headlines. The group took aim in turn at candidates of the X Factor television program, Fox News employees, the United States public television network PBS, the Canadian conservative party, Japanese giant Nintendo, and some security specialists close to the FBI.

Besides police departments around the world who are trying to locate LulzSec, several groups of hackers—including Jester and the Web Ninjas, A-Team, Backtrace, and TeaMp0isoN—are also trying to unmask them.

This discord began with the WikiLeaks affair, during which some hackers criticized the use of DDoS and looked down upon the young script kiddies using LOIC without any technical knowledge of it. The emergence of LulzSec only highlighted the rivalry between the traditional hackers and the new generation. This conflict may have also brought about the propensity for mudslinging throughout 2011. Together, these revelations made it possible to piece together a collection of personal data on more than 230 individuals (first and last names, usernames, addresses, etc.) and a list of username/IP address pairs for more than 650 of those who used LOIC to help with the DDoS attacks. Onlookers were delighted over this data. However, the truth is often shrouded by lies:

- 2010 highlights
  - June: Hacker Adrian Lamo reports the soldier Bradley Manning
  - December 30: Jester ("hacktivist for good") discloses information on the PayPal attackers
- 2011 highlights
  - February: Release of Aaron Barr/HBGary file (with more than 130 names and usernames)
  - March 20: Release of Backtrace Security file (with more than 80 names and usernames)
  - May:
    - Release of Ryan file (about 650 IP addresses and usernames)
    - Reciprocal reporting (Ryan/ev0)
  - June/September:
    - Emphasis on informant sites TeaMp0isoN, Web Ninjas, Jester, LulzSecExposed, etc.
    - Release of A-Team list



Relationships among LulzSec, Anonymous, and other movements

On June 17, LulzSec celebrated its 1,000th tweet. It also announced the end of its rivalry with Anonymous. Two days later, the two factions jointly launched Operation AntiSec. They accused governments of wanting to curtail freedom of speech on the Internet through security policies, and they called upon all of their sympathizers to attack the agencies and governments responsible.

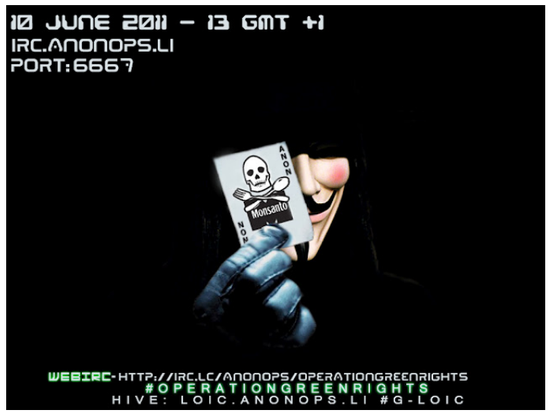
LulzSec announced the end of its operations on June 25. As a finale, it posted a series of files on Pirate Bay, with the title 50 Days of Lulz. The many police activities in progress as of that date (especially in the United States and United Kingdom) are widely responsible for their departure. LulzSec continued until September. To date, only their leader, Sabu, seems to have escaped legal trouble. Although he confirmed by a tweet on September 22 that most of his friends had been arrested, it was only in February 2012 that we learned of the deception he had carried out since his own arrest in June 2011.[45]

Sabu confirms in a tweet that most of his friends have been arrested.

Green rights

As we have seen, the members of Anonymous are not united toward a single goal. They have various motivations and often join, at a given moment, people who agree with one or other of them. Although the first actions of AntiSec created excitement among some, other hacktivists wanted to unite around an environmental ideal.

A few days after the typhoon and nuclear disaster in Fukushima, Japan, Anonymous members launched Operation Green Rights. The purpose of the operation was to protest the environmental effects and to speak out on social networks against the dependence on nuclear energy. Most supporters were recruited in France, Italy, the United States, and Latin America. Each attack was preceded by one or more manifestos translated into multiple languages. When the time of the attack arrived, a flyer was sent out with specific instructions on using LOIC.



Flyer in preparation for the Monsanto attack

After the attack in May 2011, Anonymous addressed other environmental concerns by rotating among the websites of various the electricity companies ENEL, General Electric, EDF, and ENDESA.[46] These attacks include:

- June: Protest against makers of genetically modified organisms (Monsanto, Bayer)
- July: The excesses of the oil giants (Exxon Mobil, ConocoPhillips, Canadian Oil Sands Ltd., Imperial Oil, The Royal Bank of Scotland, The Canadian Association of Petroleum Producers)
- December: Violations by railway projects in protected natural areas (high-speed train between France and Switzerland, Lyon-Turin rail link)
- December: The behavior of mining companies with respect to residents living in future operating areas (Guatemala and Peru)
- December 2011–January 2012: Defense of the Amazonian people facing the construction of a dam on the Xingu river

Other operations

During the second quarter of 2011, Anonymous ran two more operations. In May, Operation Blitzkrieg targeted far-right and neo-Nazi websites.[47] Operation SaveKids sought to identify and report people for child pornography.[48]

AntiSec, doxing, and copwatching

Although Lulz Security appears to have gone away, the AntiSec collective has taken up its banner. AntiSec is said to be an integral component of Anonymous, bringing together everyone who wants to go up against law enforcement, governments, and societies that closely or loosely infringe upon individual freedoms. For more on actions carried out under the AntiSec name, visit the Wikipedia page dedicated to them.[49]

Doxing consists of publishing photos, contact information, personal information, and family information in retaliation for an action by one or more individuals. Copwatching involves posting identification information and observations relating to law enforcement personnel on dedicated websites.

Illustration from a news article appearing in December 2011[50]

AntiSec's favorite weapon in 2011 was doxing. Under code names taken from insults launched at the police, the collective disclosed waves of data stolen from police department servers or from companies working directly with them.

Primary Doxing Attacks

Ch** la Migra (F*** the Border Patrol)**

Date	Targets
June 24, 2011	Arizona Department of Public Safety
June 29	Arizona Department of Public Safety
July 1	Arizona Fraternal Order of Police
September 2	Texas Police Chiefs Association

F* FBI Friday**

Date	Targets
June 5, 2011	Infragard
July 8	IRCFederal
July 29	ManTech
August 19	Vanguard Defense Industries
November 18	Fred Baclagan, Cybercrime Investigator
February 3, 2012	Boston Police Department

Isolated individuals (often police officers) have been victims of doxing. On September 24, 2011, a New York police officer sprayed tear gas on two female protestors. Two days later, a significant amount of data concerning him and his family was broadcast over the Internet. On November 18 on the University of California, Davis campus, a police officer sprayed demonstrators during a sit-in. His name and private information was promptly published.

Doxing is not limited to the United States. On September 26, AnonAustria published personal information on 25,000 Austrian police officers.[51] In France two days later, the Ministry of the Interior filed a defamation suit against a website (CopwatchNord-idf.org) that portrayed police in a negative light by showing images and testimonials of alleged blunders, along with offensive commentary.[52]

On August 6, Anonymous announced two data leaks in South America. One concerned the Federal Police of Brazil (8GB of data released), and the other contained personal information on 45,000 Ecuadorian police officers.[53]

Police responses

Since the DDoS attacks carried out during Operation Payback in late 2010, police forces have tried to flush out Anonymous members who went up against the law. Investigations, searches, and arrests were especially common in July 2011 and in February 2012.

The following table shows data from recent law enforcement activity. It is based on news articles that appeared between December 2010 and April 2012.

Approximate Number of Investigations, Searches, and Arrests During the Past 15 Months

Country	Total	Under age 18	18 to 28 years	Over age 28	Unknown age
United States	107	5	24	8	70
Turkey	32	8			24
Italy	15	5	10		
United Kingdom	16	6	9	1	
Argentina	10				10
Spain	7	1			6
Chile	6	2	4		
Netherlands	6	1	1		4
Colombia	5				5
France	3	1		1	1
Greece	3	2	1		
Poland	1		1		

There are significantly more active trials in the courts in the United States than elsewhere. But this does not necessarily mean the United States has a higher percentage of hacktivists in its population. U.S. law enforcement has attacked the problem by starting with the LOIC machines and not with IRC command servers. In the United States, LOIC users have been arrested and charged, but elsewhere, such as in France, only LOIC botmasters have been investigated.

Several key members, such as those associated with LulzSec, were located in Great Britain (ColdBlood, Peter, Ryan, tFlow, Topiary, Nerdo, NikonElite, Kayla, etc.).

There has been only one known operation carried out by Italian police, which identified one member with the username Phre.

There have been 32 arrests in Turkey. Those who were arrested had apparently participated in an operation on June 10, 2011, against various Turkish government sites.[54] They objected to the establishment of a large censorship filter, presented by the government as a way to "protect" the young people of the country.

In February 2012, Interpol launched Operation Unmask and carried out a string of arrests in Spain and Latin America. Those arrested were suspected of having carried out attacks against the Facebook and Twitter accounts of Columbian celebrities, Colombian government sites (July 2011), and the Chilean electricity company Endesa (May 2011).

OpCartel

In a video uploaded on October 6, 2011, a Mexican faction of Anonymous demanded the release of one of their members who had been kidnapped by Los Zetas, a criminal organization. The kidnapping allegedly took place between August 20 and 29, while the member was distributing leaflets for Operation PaperStorm in Veracruz. To support their request, the Anonymous members announced that on November 5 they would reveal the identity of journalists, police officers, and taxi drivers who were linked to the cartel if their friend was not released by that time.[55]

Los Zetas are known for violence. They do not hesitate to murder anyone who gets in their way, even police officers and journalists. At the time, they also tried to silence Internet users who used social networking to fight them. On September 13, the bodies of two online users were found under a bridge in Nuevo Laredo, near the U.S. border.[56] On September 24, the mutilated body of the editor of one of the city's daily newspapers was found nearby, with a message indicating that her murder was connected to her reporting on organized crimes using social networks.[57] A fourth murder was committed on November 9.

After the ultimatum, contradictory messages circulated over the Internet. Some called for caution, while others claimed that the operation was cancelled out of fear of retaliation. Los Zetas threatened to kill 10 people for each name that was revealed. However, despite the cartel's reputation, Anonymous announced on November 3 that the kidnapped person had been released.[58] Although the disclosure project had been canceled,[59] spokesman Barrett Brown, one of the few members to not wear a mask, threatened on YouTube that the operation would continue.[60]

Was the whole thing embellished, or did Anonymous successfully cause dangerous criminals to bend? It is impossible to know.

Anonymous in the streets

The current symbol of Anonymous (and some Occupy movements), the Guy Fawkes mask, was first seen in the streets in 2008, during a demonstration against Scientology. The masked protestors hid their faces to avoid retaliation.

Some members of Anonymous want to carry their digital protests into the real world. In early 2011, some street protests were extensions of actions started online (for WikiLeaks, for example). However, these attempts inspired very few demonstrators.

Others launched PaperStorm operations: These involved distributing leaflets in the street to attract the public's attention. But these calls to mobilize have so far received little response. In February 2012, PaperStorm ran in multiple countries (Germany, Spain, and Canada) on different days due to a lack of coordination.

Another faction tried to join with members of the Occupy and Indignant movements.

Operation BART, named after the San Francisco Bay area's commuter rail service, is a good example of these joint movements. It originated from the company's decision to jam wireless communications to disrupt the organization of any demonstrations by dissatisfied customers or other protesters. While the usual attacks took place on the Internet, 200 people wearing Guy Fawkes masks demonstrated in the street.

The international Indignant movement began in Spain in May 2011. It brings together individuals who periodically fill the streets to peacefully protest the economic and financial system of industrialized countries. In the United States, this movement is known as the Occupy Movement, or The 99%. Like Anonymous, these movements have no leaders. They wish to remain egalitarian and refuse to allow any authority within their ranks.

Anonymous in the Streets

	Street	Internet
December 18, 2010	Operation PaperStorm (support for WikiLeaks)	
March 20, 2011	International Bradley Manning Support Day	Operation Bradical, DDoS Quantico
August 13	Operation PaperStorm Revival. The reason for the protest (WikiLeaks, Anonymous arrests, etc.) is left up to the distributors.	
August 13–15	Sit-in at the San Francisco Civic Center Bay Area Rapid Transit (BART) station	#operationBART
September 17–24	Day of Rage (September 17)	Day of Vengeance (September 24)
October 2	Occupy Wall Street	Invade Wall Street
October 15	Global Protest—Occupy World	
October 26	#OccupyOakland	#OpUprise

In the United States, Occupy Wall Street was started by Adbusters, a network of anticapitalist activists with the slogan, "The one thing we all have in common is that We Are The 99% that will no longer tolerate the greed and corruption of the 1%."

Source: occupywallst.org

The first successful gathering between Anonymous and The 99% occurred on October 15, 2011. Unlike controversial actions often carried out by the AntiSec branch, these activists wanted to join with anyone driven by political motives. They also wanted to erase the image of the hacker and the joker, which they felt could harm them in the media.

In light of laws strengthening the fight against piracy (SINDE in Spain, ACTA, SOPA, and PIPA in the United States, HADOPI and LOPPSI in France, C-30 in Canada, etc.), Anonymous several times called upon its supporters to march. On February 11, 2012, and again on February 25, they filled the streets in many major cities in Europe.

Locations of protests held on February 11, 2012

Manipulation and pluralism

Because Anonymous lacks a leader or any official source of communication, anyone can propose an operation by listing it as a group proposal. Several times actions have been announced, only to have their authenticity quickly challenged. Depending on the circumstances, some labeled these calls to action as a bad joke, manipulation, misinformation, or internal differences. These obstacles were followed by contradictory information in the media. Some would blame Anonymous for indiscriminately choosing an action, while others would publish an unverified denial.

A classic example of this started with a video posted to YouTube on August 9, 2011, announcing the end of Facebook on November 5 (the anniversary of the downfall of Guy Fawkes). The social network was accused of not respecting user privacy. Despite how quickly the video was denied by other Anonymous members, the rumor did not die until November 6, once it was clear that no such event had taken place.

In contrast, in December contradictory communications stated everything and its opposite in the case of the Stratfor hacking, in which data from thousands of accounts (including those belonging to former U.S. Secretary of State Henry Kissinger) were stolen to carry out bank transfers to charities.[61] In February 2012, while WikiLeaks began to publish correspondence that was stolen on this occasion, it was clear that a branch of Anonymous was involved in this hack. The operation may have even been manipulated by the FBI.[62]

This history suggests we should remain skeptical of these online threats of actions, such as those pertaining to the U.S. power grid[63] or to DNS root servers (February 2012). In the latter example, the idea of temporarily bringing the web to a stop was proposed in connection with Operation Global Blackout, started in November 2011 as a massive campaign to protest against SOPA. Announced for March 31, the attack by reflective DNS amplification DDoS was full of orders and counterorders.

Denial of Operation Global Blackout by two Anonymous information channels

Operation Megaupload

On January 19, 2012, the shutdown of alleged pirated software site Megaupload in the middle of the debate over the Anti-Counterfeiting Trade Agreement (ACTA) led to "the largest DDoS attack in the history of the Internet," according to Anonymous.[64] Many websites fell victim to DDoS attacks. With supposedly more than 5,000 participants, the operation attacked many websites, including the U.S. Department of Justice (doj.gov), Universal Music (universalmusic.com), the Motion Picture Association of America (mpaa.org), the Recording Industry Association of America (riaa.com), the U.S. Copyright Office (copyright.gov), Broadcast Music Incorporated (bmi.com), and HADOPI (hadopi.fr).

Some supporters of the Anonymous movement were asked why they supported Megaupload's chief Kim Dotcom, whom many consider to be more a greedy cybercriminal than an advocate of a free and open Internet. When interrogated by the French newspaper *Le Nouvel Observateur*, Vador-M, a French-speaking member of Anonymous, summed up the thinking of his colleagues: "By shutting down Megaupload, we are being deprived of a freedom. We had to act. The prime motivation is not to defend Megaupload, but rather to fight censorship. We are not trying to defend Kim Dotcom, who is suspected of having mounted a mafia. But Megaupload was more than a company; it was an institution."

Communications

Social networks and websites

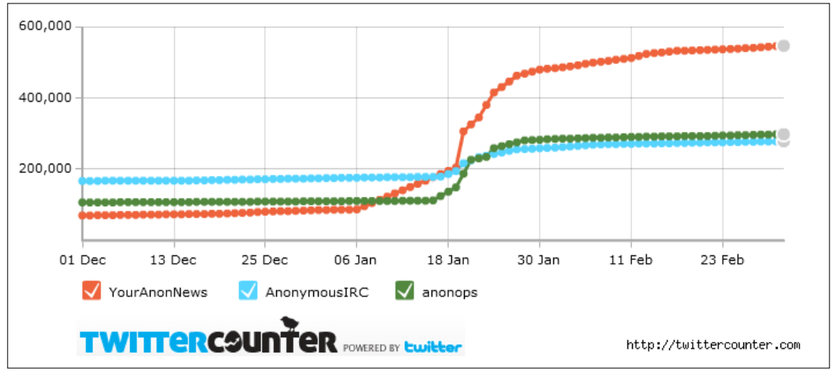
Many websites and social networking accounts claiming to speak for Anonymous appear to interfere with the movement and certainly cause confusion. As we noted before, some calls to action are immediately contradicted by others.

In particular, Anonymous' Twitter accounts attract many curious followers, security specialists, and, undoubtedly, public or private investigators. During the summer of 2011, the LulzSec Twitter account (The Lulz Boat) had more than 350,000 followers. When it became inactive in July 2011, the account belonging to its former leader, Sabu, took over (@anonymouSabu, 43,000 followers as of March 1, 2012). Yet Sabu's account represents just one faction of the group.

Five main Twitter accounts offer much of Anonymous' news:

- @AnonOps: We are fighters for internet freedom
- @AnonymousIRC: We are the #AntiSec embassy
- @YourAnonNews
- @AnonymousPress
- @Anon_Central: Anonymous Operations

These popular accounts received an influx of followers when Megaupload was shut down.



Twitter statistics in 2011–2012 for some Anonymous accounts

The top websites for Anonymous news:

- anonops.blogspot.com
- youranonnews.tumblr.com
- anoncentral.tumblr.com
- anonnews.org

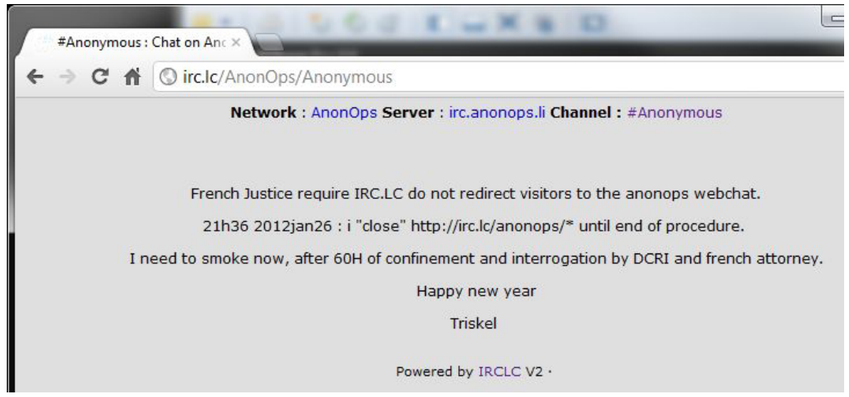
IRC

Internet Relay Chat (IRC) is the primary means of communication among supporters and the most active members of the group. IRC is a text-based instant-communication protocol using dedicated channels for group discussions. IRC also authorizes the takeover of the LOIC software for DDoS attacks.

The most active network is AnonOps. The connection can be made by web chat or more securely by an IRC client (such as XChat or mIRC).

A web chat is a web application (using HTTP) that allows a user to talk on IRC channels without client software. The web browser displays text messages on a webpage that must be periodically refreshed.

One French judge ordered an Anonymous supporter to cease offering web chat facilities to Internet users trying to reach AnonOps channels. That site is now closed but many others are available. For example, webchat.anonops.com, webchat.power2all.com, and search.mibbit.com allow many sympathizers to chat with AnonOps via IRC.



Announcing the end of one site's redirection to the AnonOps IRC server

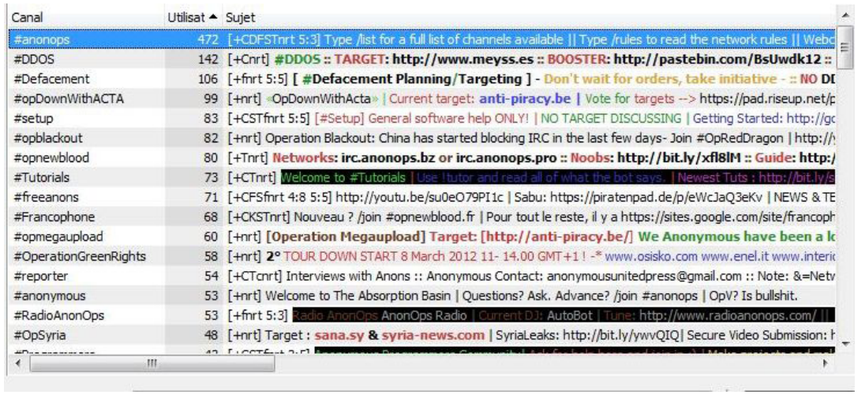
When using an IRC client, AnonOps is accessible through the following addresses:

- irc.anonops.li (now inaccessible)
- irc.anonops.bz
- irc.anonops.pro
- irc.anonops.su

On discussion forums, the connecting URL is often accompanied by a port number (for example, irc.anonops.li/6697) that is different than the default IRC port (6667). This option invites users to employ an SSL port[65] to secure the connection with encryption (as long as the client supports SSL).

Within the AnonOps network, there are many channels dedicated to current activities, discussions, and technical information. Some participants play a key role in a number of channels, while others are involved in only one or two IRCs at a time. The operators ("ops") hold a quasi position of authority. They are responsible for maintaining order. They can return or ban unwanted people. In the case of AnonOps, it is prohibited to continually connect and disconnect, to target the media, or to glorify violence.[66]

Some operators are there only to interact on the infrastructure, while others participate in most political operations conducted by Anonymous. Even if they are not the only ones to actively determine plans or operations, the opinion of operators is always heard.



The top AnonOps channels and their subjects (captured on March 8, 2012)

Anonymity

To remain masked, many Anonymous supporters use dedicated tools. One is TOR (The Onion Router). This routing software uses a proxy to pass Internet traffic through multiple nodes, making it difficult to identify the user and recover his or her IP address. Remember that TOR is intended to provide anonymity in traffic, not end-to-end encryption.

However, TOR is not easily compatible with the AnonOps IRC network. Anyone who wants to use it to connect must first set up a password and provide a hash of that password to a #help channel operator.[67] They can then connect using a URL (with domain ending in .onion) that is specific to the TOR network.[68] Other servers related to Anonymous and intended for other channels accept TOR connections. This is the case for AnonNews (irc.cryto.net), for example.

Considered by Anonymous as an "Internet within the Internet,"[69] I2P (Invisible Internet Project) is popular with hacktivists. This tool is an anonymous exchange protocol with end-to-end encryption that can be used by many applications found on the "regular" Internet. I2P supports, among other things, web browsing on specific sites (domains with .i2p), file exchanges between I2P users, and anonymous IRC chat. Because they can't remain anonymous on the rest of the Internet (using HTTP or HTTPS), many users wishing to remain unknown install I2P and TOR on their machines by creating multiple profiles for the Firefox browser.

There are other solutions for anonymous exchanges and, just as before, their use is not limited to Anonymous. With Commotion Wireless, any simple computer with a WiFi card can be part of the network and access the Internet through a third party. These nodes can also become a relay for another computer to access the Internet.[70] With Freenet,[71] an anonymous network that is distributed, encrypted, and (semi-)private, users can connect to Freesites, hold discussions in newsgroups, exchange messages using Thunderbird, and exchange and share files. Freenet behaves like a "Darknet," a network in which users can limit access to known friends.

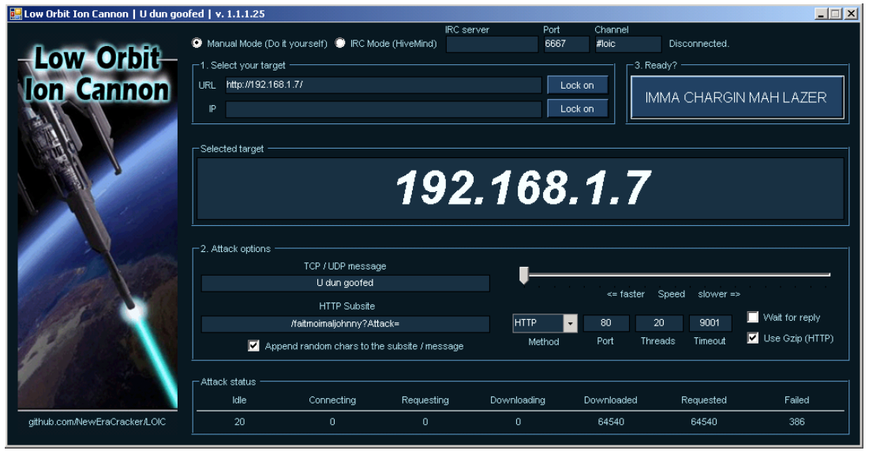
DDoS Tools

To carry out DDoS attacks, Anonymous members use various Internet tools. The best known is LOIC, which was developed for network testing. Easy to use, it allows nontechnical people to participate in attacks from their computers.

From its earliest versions, LOIC offered three types of attacks: HTTP flood, TCP flood, and UDP flood. These can be launched from the user's workstation by simply entering the site to be attacked, selecting the strength of the attack (low, medium, and high), and clicking "Fire!"

During Operation Payback (December 2010), modified versions of LOIC (Version 1.1.1.3, author NewEraCracker) appeared with IRC support. These releases can associate LOIC to a channel, set it up to run automatically, and wait for instructions. In effect, these are the first voluntary botnets. The program could also be launched in stealth mode, without a visible window and without appearing in the task bar. This makes it possible to secretly launch instances from public computers with open access.

A flood is an action that is usually malicious, consisting of sending a large amount of unnecessary data to a network to make it unusable. With LOIC, hackers can attack by flooding a server with TCP packets, UDP packets, or HTTP requests.



LOIC Version 1.1.1.25[72]

Other versions of LOIC have appeared since Operation Payback. JS LOIC, or LOIC Mobile, allows novices to participate in an attack by simply connecting to a web page from their browsers, which they leave open at the time designated for the attack. JavaScript code then opens web pages and launches a series of HTTP requests to saturate server resources. This is how members of Anonymous attacked the Vatican's website in August 2011 during World Youth Day (Operation Pharisee).[73]

Similar code that asked participants to select a target from a predefined list appeared after Megaupload was shut down.

The JS LOIC interface[74]

A version of LOIC was recently developed for Android. LOIC para Android by Alfred is currently in use in Latin America.[75]

HOIC is another tool for creating DDoS attacks. It can perform only an HTTP flood, but it has Booster Scripts,[76] which are configuration files that can add more requests and better hide them in regular traffic.

Anonymous is sometimes suspected of using other attack tools, such as Apache Killer (written by Kingcope), Slowloris (written by RSnake), r-u-dead-yet, and ZapAttack (on MacOS X). LOIC and its descendents (JS LOIC, WEBLOIC) seem to be the most widely used. Some media reports mentioned the RefRef project,[77] but this seems to have been only a hoax.

Cyberdissidents

The second branch of hacktivism comprises cyberdissidents, or cyberoccupiers. Although Anonymous firmly defends freedom of speech and exchange over the Internet, cyberoccupiers, who are anchored in the real world, view the Internet as a tool to help them in their struggle to achieve a freer society. In democratic countries, their actions are underreported because they are often located on the edge of legality. This struggle is generally good natured. It is often confined to an activist use of social networking, which becomes a means for communications and propaganda. When this political fight is set against a totalitarian or extremist regime, we often call these activists cyberdissidents. When they act, they do not hide their identity for fun or ideology, but rather to escape a violent backlash that could be exerted against them if they were recognized. Although we separate cyberdissidents and cyberoccupiers from the Anonymous movement, the border is sometimes unclear between these two groups. Some cyberdissidents sign their actions by claiming responsibility as Anonymous, while Anonymous members often launch one-time operations to support the Occupy movements.

Telecomix

The attention given to the Arab uprising built a stronger political consciousness in some hacktivists. This is true for the Telecomix group, created in April 2009 in Sweden. Its members function without a leader or a hierarchy. They are said to operate according to the concept of a "do-ocracy." "It is enough to have ideas, and then others can join in and help. Nobody has an overview of all projects," explain fo0 and Menwe.[78] According to Okhin, a "crypto-anarchist" and another agent of Telecomix, the group has 250 to 300 people. "We live in the network. We live by and for the network. If it is attacked, we will defend it."[79]

Do-ocracy, a contraction of "to do" and "democracy," can result in democracy through action. This is a flexible structure in which individuals assign themselves tasks and complete them, taking full responsibility.

In January 2011, Telecomix partially restored web access in Egypt, after Hosni Mubarak's government cut off the Internet for its 20 million users. Telecomix is reported to have set up telephone lines connected to 56K modems, and then broadcasted the information on Facebook and Twitter.[80] The group repeated the operation in Libya in February 2011.


TELECOMIX INTERNATIONAL

للتوزيع فوراً
FOR IMMEDIATE DISTRIBUTION

نحن تيليكوميكس نأتيكم بسلام. نحن نحاول مساعدتكم بتقديم أي من وسائل الاتصال المتوفرة. يرجى توزيع هذه المعلومات لكل الراغبين بالحصول على امكانية اتصال مجاني.
This is Telecomix. We come in peace. We are trying to help with providing every means of communications available. Please distribute this information to all those who are in need of free communication.

معلومات للوصول إلى الإنترنت
INTERNET DIAL-IN INFORMATION

استخدم المعلومات الموجودة أدناه مع مودم 56 كيلوبايت

An extract from the message Telecomix sent to the Egyptian people

When the civil war intensified in Syria, Telecomix activists sought to support those rebels as well, at the cost of receiving threats. The operation began in August 2011 with a mass message sent to Syrian Internet users. It explained how to bypass the online monitoring in the country. During the night of September 4–5, a large portion of the Syrian Internet was bypassed by simultaneous hacking from all TPLink routers.[81] Internet users could access only one page, which provided a survival kit to be used by opponents of Bashar al-Assad. "Your Internet activity is monitored. Here are the tools to get around this monitoring," explained a portion of the page, in English and Arabic. The kit contained security extensions (plug ins) for Firefox, TOR, secure instant-messaging software (hushmail), a VOIP service that competes with Skype (Mumble), a conversation encryption system (Pidgin with the Off-The-Record plug-in), an IRC client (Xchat), and a link to the Telecomix chatroom.[82] This 60MB package also included basic security guidelines to avoid revealing personal information on the Internet. In March 2012, support operations were still continuing.

Message to the Syrian people (on September 5, 2011)

Telecomix operates as if it were international web assistance for the people, acting on its own initiative, in the event that the Internet is cut off or restricted. Those who appreciate Telecomix point out that "they are not done through DDoS, and they do not hack."[83] In Geneva, Telecomix volunteers provide cryptography training for Reporters Without Borders. In a democratic country like France, Telecomix's actions may sometimes go beyond the limits of legality. Such was the case when they mirrored the "Copwatch" site the French authorities decided to close.

Other achievements

Although Anonymous came to light only in the last quarter of 2010, virtual protests and politically motivated attacks had multiplied by the start of that year. Some of these acts can be compared to actions from an organization such as Greenpeace, which often challenges national or international laws to raise awareness. In cyberspace, the following examples, despite being illegal, attracted some sympathy and were considered justified by some people.

- January 2010: A hacker in Turkey modified the computer system used to call worshipers to prayer. The messages were transmitted to 170 mosques in the country. The original messages were replaced by songs by an artist who died in 1996 and was known for his pioneering role in recognizing homosexuality in Turkey.
- February: In Latvia, the group 4ATA (Fourth Awakening People's Army) announced that they had obtained millions of income tax documents. They disclosed some of the information to shed light on corruption in the country. The chief suspect, an artificial intelligence researcher at the University of Riga, was identified in May.
- In April, a professor at the University of California, San Diego launched a virtual protest (a call to participate in a DDoS attack) against his university's own website to help create more opportunities for a larger number of disadvantaged students.[84]

- On July 14, a group of activists in France falsified the website of the Ministry of Foreign Affairs to show a fake spokesperson announcing measures to help Haiti.
- In "Climategate II" hackers exposed on November 24, 2011, more than 5,000 emails that appeared to confirm that some scientists were on a political mission—not a search for truth—when it comes to global warming.[85]
- On December 1, WikiLeaks revealed the Spy Files, nearly 1,100 documents from manufacturers on the monitoring and interception of telecommunications.[86] These revelations showed that there is a lucrative market for mass cyberspying and cybermonitoring at the national level. Opponents of these practices argued that the products, mainly developed in Western democracies, are sold everywhere, including to dictatorships that were still in place or suffering due to the Arab Spring.

The home page of Spy Files, highlighting France

- As demonstrations against rising oil prices shook up Nigeria, a website belonging to the national army was defaced on January 16, 2012, by hacktivists. The message left on the site was "Leave innocent protesters ALONE."[87]

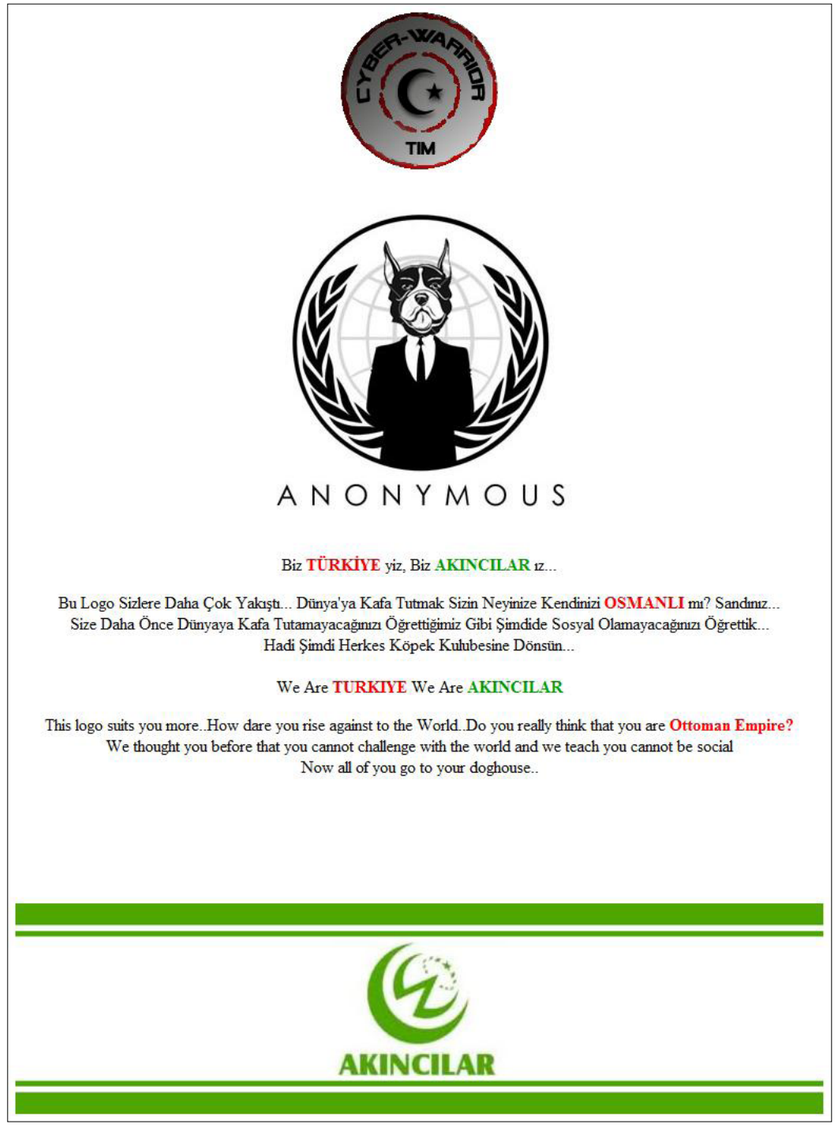
Patriots and Cyberwarriors

While Anonymous-related cyberoccupiers and cyberdissidents defend freedom of speech and stand up for minorities and people seeking to gain their freedom, other groups—often authoritarian and religious—that appear close to their governments respond to what they describe as interference. Unlike Anonymous, these "patriots" often act as fundamentalists while they too behave as hacktivists.

Whether they call themselves Russian nationalists, Chinese, Indian, or Pakistani patriots, or defenders of Israel and Palestine, all of these little groups carry out guerrillalike actions online against anyone they consider to be enemies. Grouped into (pseudo) cyberarmies, they set up voluntary botnets or deface and destroy the messages or actions of dissidents and adversaries.

Backlash against Anonymous

In June 2011, Anonymous launched Operation Turkey to support youths who were protesting against censorship of the Internet. For a few days, government sites were inaccessible as a result of DDoS attacks via LOIC botnet launched from outside the country. On July 16, the Akincilar group responded by defacing AnonPlus' home page, a new site that some Anonymous members had set up after being banned from Google+.



The Akincilar group attacks Anonymous

Supporters of Bashar al-Assad have been angered by actions in support of the Syrian people. On August 9, in retaliation for Anonymous' defacing the website of Syria's Ministry of Defense, the "Syrian Cyber-Army" hacked the AnonPlus site via DNS cache poisoning. In place of the usual page, Internet users saw photos of dead soldiers with a message implying that by supporting the opponents of the Bashar al-Assad's regime, Anonymous was supporting the Muslim Brotherhood.[88]

TeaMp0isoN

TeaMp0isoN first became known as a ruthless enemy of LulzSec and Anonymous, but the group later announced a merger with AntiSec. Since 2010, the three main members of the group, including its leader TriCk, have made their political and religious opinions clear. They have often signed their attacks jointly with the Mujahideen Hacking Unit when defending the Palestinian cause. When attacking Indian sites, they also list themselves as members of the Pakistan Cyber Army or the ZCompany Hacking Crew. Because of the messages they issue during these attacks, we classify them as a cyberarmy.

The group's achievements:

- June 2011: In retaliation for the military intervention in Iraq, TeaMp0isoN published the address book and some private information belonging to former U.K. prime minister Tony Blair.
- August: When Research in Motion, maker of BlackBerry devices, announced that it was cooperating with the police to stem the riots that shook up Great Britain, TeaMp0ison defaced the company's blog and threatened to publish confidential employee data if the company insisted on disclosing information about users of its phones. TriCk wrote, "We are all for the rioters that are engaging in attacks on the police and government."[89]
- August: The group hacked a NASA discussion forum and revealed details of the administrator account.
- November: TeaMp0isoN publishes information for accessing thousands of personal accounts as part of the United Nations Development Program.

In November 2011, TeaMp0isoN announced that it had teamed up with Anonymous and created p0isAnon, which launched Operation Robin Hood in solidarity with Occupy Wall Street.[90] In a video, a spokesperson stated that "Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe." Screenshots of payments to organizations such as CARE, the American Red Cross, and Save the Children from the bank accounts of various personalities were broadcasted over the Internet. The information allegedly came from the hacking of the Statfor website.

This operation damaged the image of Anonymous and was also a blow to nongovernmental organizations. Ultimately, the fraudulent payments had to be refunded to avoid having to pay chargebacks.

TriCk was arrested in the United Kingdom in April 2012. This 17-year-old Muslim claimed to be behind the release of highly sensitive telephone conversations from Scotland Yard's antiterrorist hotline.[91]

Other achievements

Although numerous, actions by cyberarmies have relatively little impact. The media report them only when someone touches an institutional site or a site belonging to a political party or politician.

Cyberarmies' favorite weapon is defacement. Every day, hackers deface thousands of (or more) sites. In about 10 percent of cases, this is the work of hacktivists who apparently relate to the ideology of cyberwarriors.

Statistics on defaced websites, from zone-h

Reason for Attack	Number of Sites
Heh…just for fun!	829,975
I just want to be the best defacer	289,630
Not available	94,017
Patriotism	58,970
Political reasons	57,083
Revenge against that website	45,093
As a challenge	44,457

Data from zone-h cites the leading reasons hackers claimed for attacking websites in 2010. More than 800,000 actions were "just for fun."[92]

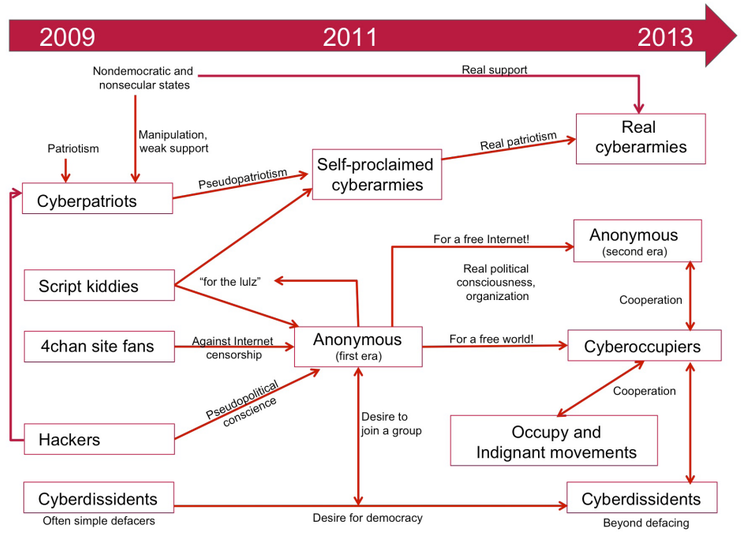
Examples of cyberarmies in action:

- Throughout 2010, Indian and Pakistani hackers struck one another with numerous cyberattacks. The Indian Cyber Army and the Pakistan Cyber Army claimed credit for the attacks.
- In April 2010, several Romanian hackers defaced French and English websites. They were protesting against the suggestion made by some members of the media that Romanians and Gypsies could be combined. In France, a sketch by Jonathan Lambert particularly irritated the protesters.
- In 2010, supporters of the Palestinian group Hamas distributed an animated video featuring the father of Israeli soldier Gilad Shalit. Immediately thereafter, sites supporting the Palestinian cause were defaced. In May, the Facebook accounts of many Israelis were hacked in response to the stopping of the Peace flotilla that was en route to Gaza.
- In the Philippines, official websites were defaced on August 27. The perpetrators demanded an investigation after eight tourists from Hong Kong were killed (on August 23) during an assault in Manila on a bus that led to 15 people being held hostage.
- In November, in retaliation for the distribution of videos showing torture against the Papuan people attributed to the Indonesian army, several nongovernmental websites, including Survival International's, were targeted by cyberattacks.
- In February 2011, Turkish patriots launched a campaign to protest the Armenian Genocide recognition process. More than 6,000 sites were affected. In France in December, government's move to outlaw the denial of genocides angered Turkish hacktivists. Defaced sites included the websites of Valérie Boyer, the member of parliament who initiated the text, and Patrick Devedjian, an Armenian member of parliament.
- During the first weekend of March, about 40 South Korean government websites were hit by DDoS attacks.
- In March, an informational site supporting the Thai opposition was said to have been infiltrated. The author of the attack allegedly submitted fake articles meant to discredit the media.

Conclusion

Sorting among Anonymous, cyberoccupiers, and cyberarmies can make it difficult to understand the actors and their motivations. Just as some activists illegally enter nuclear plants and other private property, hacktivists illegally enter private digital areas. Crippled by their lack of structure, some hacktivist operations are confined to jokes in bad taste (lulz), while others may be linked to mafialike activities (such as stealing bank data). These hacks are often of questionable value and difficult to understand. This apparent randomness of purpose suggests that some individuals are perhaps playing a double game, hiding illegal activities under the cover of political hacktivism. White-hat hackers point out that the lack of ethics in many operations suggest that some hacktivists may be controlled by government secret services.

Hacktivism, whether or not related to Anonymous, is a major phenomenon today. Just as criminals understood 10 years ago that the Internet could become one of their preferred playing fields, many Internet users discovered in 2010 that the web could become a collective platform for protests. Encouraged by Anonymous, which grasped this concept some time ago, hacktivists were very active during 2010 and 2011. Now let's take a look at their possible organizations in the next two years.



Possible evolution of the hacktivist movement

After playing vandals and noisy protestors, hacktivists with a true political conscious worked together to evolve and organize. Spawned from the Anonymous movement we know today, early hacktivists seemed to slowly transform, as recruits joined with new skills:

- Graphic artists for better communications
- Volunteer journalists for participative journalism similar to Wikipedia (crowd journalism)
- Experienced computer scientists for carrying out more sophisticated operations and to more powerfully damage their intended victims
- Tacticians for finding other ways to act and for bringing together activists and cyberactivists
- Lawyers for establishing the right to demonstrate online (such as the legalization of some forms of DDoS attacks)

For us in the online security industry, this last point may be surprising. Some supporters of hacktivism may be the digital globalization opponents of tomorrow; they actually argue for the legalization of an activism-inspired DDoS. In the preceding diagram, these people are the second era of Anonymous. A contact close to them confirmed to McAfee Labs that they find defacing a website analogous to displaying a banner and that they see launching a DDoS as similar to a sit-in blocking the entrance to a building. As some people apply for a permit to march and protest, the second generation of Anonymous imagines specifying the dates, targets, and duration of a DDoS blockage.

If hacktivists remain unfocused and continue to accept anyone who signs on to act on their behalf, we may be on the verge of a digital civil war. The entire hacktivist movement may fall victim to an increase in criminalization, as well as to governments fearing that their economic activities and critical infrastructures will be undermined as they become increasingly more dependent on information technology. However, if the hacktivists of 2012 manage to mature, organize, and even mobilize outside of the web, we could think of Anonymous as a Version 2.0 of nongovernmental organizations, ideologically questionable, perhaps, yet respected within our democracies. Links with political organizations of a new genre, such as the Pirate Party movement, may be an early step in this development.[93]

About the Author

François Paget is a senior malware research engineer at McAfee Labs in France. He has been involved in malware research since 1990 and was a founding member of Avert (now McAfee) Labs in 1995. Paget is a regular conference speaker at French and international security events, author of a book and numerous articles, and general secretary of the French Information Security Club (CLUSIF).

About McAfee Labs

McAfee Labs is the global research team of McAfee. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based service McAfee Global Threat Intelligence™. The McAfee Labs team of 350 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on finding new ways to keep our customers safe. www.mcafee.com

[1] "Hacktivism, From Here to There." Cult of the Dead Cow. Published online. McAfee Labs does not recommend visiting this site, which is marked "red" by McAfee SiteAdvisor.
[2] Cult of the Dead Cow. Published online.
[3] http://www.bris2600.com/hall_of_fame/ccc.php
[4] http://www.cert.org/advisories/CA-1989-04.html
[5] http://en.wikipedia.org/wiki/Intervasion_of_the_UK
[6] http://www.tommasotozzi.it/index.php?title=Netstrike_(1995)
[7] http://www.2600.com/hackedphiles/east_timor/
[8] http://findarticles.com/p/articles/mi_6914/is_2_22/ai_n28817798/pg_4/
[9] http://www.etoy.com/projects/toywar/
[10] http://www.fraw.org.uk/projects/electrohippies/archive/wto_prelease.pdf
[11] http://www.libertad.de/inhalt/projekte/depclass/spiegel/fr/info/review.html
[12] http://digital-stats.blogspot.com/2010/08/forum-4chan-receives-approximately-95.html
[13] http://techland.time.com/2008/07/10/now_in_papervision_the_4chan_g/
[14] Lulz is the plural of lol, and also means evil, malicious, or sardonic laughter.
[15] http://encyclopediadramatica.se/Main_Page. A new, supposedly more politically correct form of the site is available at http://ohinternet.com/Main_Page.
[16] http://cnews.canoe.ca/CNEWS/Crime/2007/12/07/4712680-sun.html
[17] ISBN 978-2-916571-60-7
[18] "Chanology" is a contraction of Chan (from the 4chan forum) and Scientology.
[19] http://cnews.canoe.ca/CNEWS/Crime/2007/12/07/4712680-sun.html
[20] http://musicmachinery.com/2009/04/15/inside-the-precision-hack/
[21] http://www.businesspundit.com/anonymous-joins-fight-against-tyranny-in-iran/
[22] http://www.guardian.co.uk/media/pda/2010/jan/06/youtube-porn-attack-4chan-lukeywes1234
[23] http://delimiter.com.au/2010/02/10/anonymous-attacks-govt-websites-again/
[24] http://knowyourmeme.com/memes/events/operation-payback
[25] http://www.myce.com/news/anonymous-operation-payback-timeline-infographic-36481/
[26] http://www.zonebourse.com/barons-bourse/Mark-Zuckerberg-171/actualites/Anonymous-prevoit-de-detruire-Facebook-le-5-novembre-prochain--13753673/
[27] http://www.guardian.co.uk/world/2007/aug/31/kenya.topstories3
[28] http://www.reuters.com/article/2007/11/14/us-guantanamo-manual-idUSN1424207020071114?pageNumber=1
[29] http://www.theregister.co.uk/2008/04/08/church_of_scientology_contacts_wikileaks/
[30] https://www.eff.org/files/filenode/EFF_PK_v_USTR/USTRcomplaint.pdf
[31] http://mybroadband.co.za/news/internet/14702-outcry-in-belgium-over-wikileaks-publications-of-dutroux-dossier.html
[32] http://icelandweatherreport.com/2009/08/kaupthings-loan-book-exposed-and-an-injunction-ordered-against-ruv.html
[33] http://en.wikipedia.org/wiki/Leet
[34] http://www.spamhaus.org/news/article/665
[35] http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian
[36] http://www.youtube.com/watch?v=_4LU7piK9X4
[37] http://www.thestandard.co.zw/local/27601-first-lady-gono-in-diamond-scandal-wikileaks.html
[38] http://cert.lexsi.com/weblog/index.php/2011/01/07/398-operation-zimbabwe-chronique-dune-cyber-attaque-contre-les-sites-gouvernementaux-zimbabweens-par-le-groupe-hacktiviste-anonymous
[39] http://temporaryartist.wordpress.com/2011/01/17/we-are-winning-the-thoughts-of-a-single-humble-anon/
[40] *Anonymous*, page 235, by Frédéric Bardeau and Nicolas Danet (ISBN 978-2-916571-60-7)
[41] http://www.ft.com/intl/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html
[42] http://www.guardian.co.uk/commentisfree/cifamerica/2011/jun/22/hacking-anonymous
[43] http://www.mediaite.com/online/exclusive-gawker-hacker-gnosis-explains-method-and-reasoning-behind-his-actions/
[44] http://blogs.computerworld.com/18307/face_of_anonymous_quits_exclusive_interview_with_barrett_brown
[45] http://www.foxnews.com/scitech/2012/03/06/hacking-group-lulzsec-swept-up-by-law-enforcement/
[46] ENEL: Ente Nazionale per l'Energia Elettrica, Italy; EDF: Electricité de France; ENDESA: Empresa Nacional de Electricidad, SA, Spain and Latin America
[47] http://www.tgdaily.com/security-features/55690-anonymous-launches-operation-blitzkrieg
[48] http://e-worldwar.com/~/index.php?option=com_content&view=article&id=86&Itemid=494
[49] http://en.wikipedia.org/wiki/Operation_AntiSec
[50] http://www.thetechherald.com/articles/The-FBIs-warning-about-doxing-was-too-little-too-late
[51] http://www.rtbf.be/info/medias/detail_le-groupe-de-pirates-anonymous-a-publie-les-coordonnees-de-25-000-policiers-autrichiens?id=6816493
[52] http://www.ladepeche.fr/article/2011/09/29/1179489-copwatch-gueant-porte-plainte-contre-le-site-anti-flic.html
[53] http://archives-lepost.huffingtonpost.fr/article/2011/08/08/2564639_anonymous-les-donnees-personnelles-de-la-police-americaine-sur-internet.html
[54] http://www.ft.com/intl/cms/s/0/e8a6694c-95bb-11e0-8f82-00144feab49a.html#axzz1nDE7Z4df
[55] http://globalvoicesonline.org/2011/10/31/mexico-fear-uncertainty-and-doubt-over-anonymous-opcartel/
[56] http://www.lanacion.com.ar/1406114-mexico-asesinados-y-colgados-por-denunciar-en-twitter-asuntos-narcos
[57] http://www.tadla-azilal.com/technologies/mexique-les-menaces-sur-la-presse-setendent-aux-reseaux-sociaux/
[58] http://www.pcmag.com/article2/0,2817,2395863,00.asp#fbid=EBREppl_iKE
[59] http://www.bbec.lautre.net/www/spip_truks-en-vrak/spip.php?article2121
[60] http://www.youtube.com/user/BarrettBrown
[61] http://www.f-secure.com/weblog/archives/00002290.html
[62] http://www.guardian.co.uk/technology/2012/mar/06/lulzsec-court-papers-sabu-anonymous?intcmp=239
[63] http://www.v3.co.uk/v3-uk/news/2154453/anonymous-laughs-nsa-claims-hacking-power-grid
[64] http://obsession.nouvelobs.com/la-fermeture-de-megaupload/20120123.OBS9528/anonymous-en-fermant-megaupload-ils-nous-ont-prive-d-une-liberte.html
[65] SSL stands for Secure Sockets Layer, a protocol for securing exchanges over the Internet, originally developed by Netscape and now often called TLS (Transport Layer Security).
[66] http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action
[67] This procedure is explained in multiple forums, including here: http://pastebin.com/hR9FakGs
[68] 2mjtgjozdqg2aumu.onion
[69] http://pastehtml.com/view/1e8t85a.html
[70] https://code.commotionwireless.net/projects/commotion/wiki/Newbie_How_it_Works
[71] http://freenetproject.org/whatis.html
[72] http://thanatos.trollprod.org/sousites/hoic/
[73] http://www.nytimes.com/2012/02/27/technology/attack-on-vatican-web-site-offers-view-of-hacker-groups-tactics.html?_r=1&pagewanted=all
[74] http://www.nbs-system.com/blog/analyse-de-loutil-de-ddos-loic.html
[75] http://blogs.mcafee.com/mcafee-labs/android-diy-dos-app-boosts-hacktivism-in-south-america
[76] http://blog.spiderlabs.com/2012/01/hoic-ddos-analysis-and-detection.html
[77] http://thehackernews.com/2011/07/refref-denial-of-service-ddos-tool.html
[78] http://www.rezocitoyen.fr/telecomix-hacker-pour-la-liberte.html?artpage=2-3
[79] http://www.siliconmaniacs.org/telecomix-on-ne-casse-rien-on-repare-on-ameliore-on-reconstruit/
[80] http://www.rue89.com/2011/08/18/hackers-libertaires-notre-but-cest-partager-la-connaissance-218241
[81] http://owni.fr/2011/09/14/opsyria-syrie-telecomix/
[82] This kit is still available: https://telecomix.ceops.eu/tcxnetpack.tgz
[83] http://reflets.info/internet-coupe-en-egypte-enfin-presque/
[84] http://www.theregister.co.uk/2010/04/09/virtual_protest_as_ddos/
[85] http://www.contrepoints.org/2011/11/24/57189-climategate-2-0-de-nouveaux-mails-entachent-la-science-climatique
[86] http://wikileaks.org/the-spyfiles.html
[87] http://observers.france24.com/fr/content/20120116-site-armee-nigeriane-hacker-activistes-mobilisation-internet-prix-essence
[88] http://www.branchez-vous.com/techno/actualite/2011/08/anonplus_anonymous_defacage_cyber_armee_syrie.html
[89] http://www.bbc.co.uk/news/technology-14476620
[90] http://www.theinquirer.net/inquirer/news/2128175/anonymous-team-poison-start-op-robin-hood
[91] http://www.huffingtonpost.co.uk/2012/04/12/mi6-phone-hack-attack-was-easy-trick-mi6_n_1420308.html
[92] http://www.zone-h.org/news/id/4737
[93] http://www.pp-international.net/

McAfee
An Intel Company
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com