The elements of hacktivist computer science essay

Technology, Computer

Hacktivism a portmanteau of hack and activism is the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development.[1] It is often understood as the writing of code to promote political ideology – promoting expressive politics, free speech, human rights, or information ethics. Acts of hacktivism are carried out in the belief that proper use of code will be able to produce similar results to those produced by regular activism or civil disobedience.

Hacktivist activities span many political ideals and issues. Freenet is a prime example of translating political thought into code. Hacktivismo is an offshoot of Cult of the Dead Cow; its beliefs include access to information as a basic human right. The loose network of programmers, artists and radical militants 1984 network liberty alliance is more concerned with issues of free speech, surveillance and privacy in an era of increased technological surveillance.

Hacktivism is a controversial term, and can often be misconstrued as cyberterrorism. What separates hacktivism from cyberterrorism is a distinctly political or social cause behind the haction. Some argue it was coined to describe how electronic direct action might work toward social change by combining programming skills with critical thinking. Others use it as practically synonymous with malicious, destructive acts that undermine the security of the Internet as a technical, economic, and political platform.

Essentially, the controversy reflects two divergent philosophical strands within the hacktivist movement. One strand thinks that malicious cyber-

attacks are an acceptable form of direct action. The other strand thinks that all protest should be peaceful, refraining from destruction.

Controversy

Some people describing themselves as hacktivists have taken to defacing websites for political reasons, such as attacking and defacing government websites as well as web sites of groups who oppose their ideology. Others, such as Oxblood Ruffin (the foreign affairs minister of Hacktivismo), have argued forcefully against definitions of hacktivism that include web defacements or denial-of-service attacks.[2]

Critics suggest that DoS attacks are an attack on free speech; that they have unintended consequences; that they waste resources; and that they could lead to a DoS war which nobody will win. In 2006, Blue Security attempted to automate a DoS attack against spammers; this led to a massive DoS attack against Blue Security which knocked them, their old ISP and their DNS provider off the internet, destroying their business.

Depending on who is using the term, hacktivism can be a politically constructive form of anarchist civil disobedience or an undefined anti-systemical gesture; it can signal anticapitalist or political protest; it can denote anti-spam activists, security experts, or open source advocates. Critics of hacktivism fear that the lack of a clear agenda makes it a politically immature gesture, while those given to conspiracy theory hope to see in hacktivism an attempt to precipitate a crisis situation online.

Elements of Hacktivist Hactions

A Haction usually has the following elements.

Politically motivated

Place a premium on humor, and often resembles a digital form of clowning

Owns a moderate Outlaw Orientation as opposed to severe

The result of aggressive policy circumvention – rather than a gradual attempt to change a policy

Always non-violent- a haction never places another in direct danger

Capacity for solo activity – while most forms of political activism require the strength of masses, hacktivism is most often the result of the power of one, or small group.

Is most often carried out anonymously, and can take place over transnational borders.

Forms of Hacktivism

In order to carry out their operations, hacktivists use a variety of software tools readily availble on the internet. In many cases the software can be downloaded from a popular website, or launched from a website with click of a button. Some of the more well known hacktivist tools are below:

1. Defacing Web Pages Between 1995-1999 Attrition. org reported 5, 000 website defacements. In such a scenario, the hacktivist will significantly alter the front page of a company’s or governemental agency’s website.

2. Web Sit-ins In this form of hacktivism, hackers attempt to send so much traffic to the site, that the overwhelmed site becomes inaccessible to other users.

3. E-mail Bombing Hacktivists send scores of e-mails with large file attachments to their targets e-mail address

Notable hacktivist events

The earliest known instance of hacktivism is documented by Julian Assange as follows:[4]

Hacktivism is at least as old as October 1989 when DOE, HEPNET and SPAN (NASA) connected VMS machines world wide were penetrated by the anti-nuclear WANK worm. [...] WANK penetrated machines had their login screens altered to:

W O R M S A G A I N S T N U C L E A R K I L L E R S

_____

__ _____ _____ _____ ____ ____ __ _____/

/ / / / / | | | | | / / /

/ / / / /__ | | | | | |/ / /

/ / / / / _____ | | | | | | /

_ /__ /____/ /_____ ____| | __ | | ____| | _ _/

_____/

/

Your System Has Been Officially WANKed /

_____/

You talk of times of peace for all, and then prepare for war.

One of the earliest documented hacktivist events was the Strano Network sit-in, a strike action directed against French government computers in 1995.

The term itself was coined by techno-culture writer Jason Sack in a piece about media artist Shu Lea Cheang published in InfoNation in 1995.

The hacking group milw0rm hacked into the Bhabha Atomic Research Centre (BARC) in 1998, replacing the center’s website with an anti-nuclear message; the same message reappeared later that year in what was then an unprecedented mass hack by milw0rm of over 300 websites on the server of hosting company Easyspace.[5]

In 1998, the Electronic Disturbance Theater conducted virtual sit-ins on the Web sites of the Pentagon and the Mexican government to bring the world’s attention to the plight of Indian rights in the Mexican state of Chiapas. A Mexican hacking group took over Mexico’s finance department website in support of the same cause.[5]

One of the more notorious examples of hacktivism was the modification of Indonesian web sites with appeals to Free East Timor in 1998 by Portuguese hackers.[6]

On December 29, 1998, the Legions of the Underground (LoU) declared cyberwar on Iraq and China with the intention of disrupting and disabling internet infrastructure. On January 7, 1999, an international coalition of

hackers (including Cult of the Dead Cow, 2600 ‘ s staff, Phrack’s staff, L0pht, and the Chaos Computer Club) issued a joint statement condemning the LoU’s declaration of war.[7] The LoU responded by withdrawing its declaration.

Hacktivists attempted to disrupt ECHELON (an international electronic communications surveillance network filtering any and all satellite, microwave, cellular, and fiber-optic traffic) by holding Jam Echelon Day (JED) on October 21, 1999. On the day, hacktivists attached large keyword lists to many messages, taking advantage of listservers and newsgroups to spread their keywords further. The idea was to give the Echelon computers so many hits they overloaded. It is not known whether JED was successful in actually jamming Echelon, although NSA computers were reported to have crashed inexplicably in early March, 2000. A second Jam Echelon Day (JEDII) was held in October 2000, however the idea never regained its initial popularity. JED was partly denial-of-service attack and partly agitprop.

The Electronic Disturbance Theater and others staged a week of disruption during the 2004 Republican National Convention in New York City, conducting sit-ins against Republican web sites and flooding web sites and communication systems identified with conservative causes. This received mixed reviews from the hacktivist community.[citation needed]

The Hackbloc collective started publishing Hack This Zine a hacktivist research journal

Hacktivists managed to break into computer systems at the Bhabha Atomic Research Center in India to protest against nuclear weapons tests.[citation needed]

Bronc Buster, later a member of Hacktivismo, disabled firewalls to allow Chinese Internet users uncensored access. The Crackers also defaced a Chinese website which explained what the people of China could access over the internet legally. Wired 01. 01. 98[citation needed]

Hacktivists worked to slow, block, or reroute traffic for web servers associated with the World Trade Organization, the World Economic Forum, and the World Bank.[citation needed]

Throughout 2006, Electronic Disturbance Theater joined the borderlands Hacklab for a number of virtual sit-ins, against the massacre in Atenco, in solidarity with striking french students and against the Minutemen and immigration laws.[8]

On March 25, 2007, hacktivists organized the event freEtech in response to the O'Reilly Etech conference, and started a series of West coast hackmeetings.

Electronic Disturbance Theater stages a virtual sit-in against the Michigan Legislature against cuts to Medicaid.

On January 21, 2008, a message appeared on YouTube from a group calling itself ' Anonymous'. The group declared Project Chanology, essentially a war on The Church of Scientology, and promised to systematically expel The

Church from the internet. Over the following week, Scientology websites were intermittently knocked offline, and the Church of Scientology moved its website to a host that specializes in protection from Denial-of-service attacks.

A computer hacker leaks the personal data of 6 million Chileans (including ID card numbers, addresses, telephone numbers and academic records) from government and military servers to the internet, to protest Chile’s poor data protection.[9]

Throughout early 2008, Chinese hackers have hacked the CNN website on numerous occasions in response to the protests during the 2008 Olympic Torch Relay and claims of biased reporting from western media. The majority of the DDoS attacks took place between March and August, at a time where Chinese nationalistic pride was at an all time high due to the 2008 Olympic Games.[10][11]

Electronic Disturbance Theater and the Hacklab stage a virtual sit-in against the war on Iraq and biotech and nanotech war profiteers, on the 5 year anniversary of the war, in solidarity with widespread street actions.

Intruders hacked the website of commentator Bill O’Reilly and posted personal details of more than 200 of its subscribers, in retaliation for remarks O’Reilly made on Fox News condemning the attack on Palin’s Yahoo email account [1].

In 2008 hacktivists developed a communications and monitoring system for the 2008 RNC protests called Tapatio.

In early 2009, the Israeli invasion of Gaza motivated a number of website defacements, denial-of-service attacks, and domain name and account hijackings, from both sides[12]. These attacks are notable in being amongst the first ever politically-motivated domain name hijackings.

During the 2009 Iranian election protests, Anonymous played a role in disseminating information to and from Iran by setting up the website Anonymous Iran[13]; they also released a video manifesto to the Iranian government.

On August 1, 2009, the Melbourne International Film Festival was forced to shut down its website after DDoS attacks by Chinese vigilantes, in response to Rebiya Kadeer’s planned guest appearance, the screening of a film about her which is deemed anti-China by Chinese state media, and strong sentiments following the July 2009 Ã? rÃ? mqi riots. The hackers booked out all film sessions on its website, and replaced festival information with the Chinese flag and anti-Kadeer slogans.[14][15]

In November 2009, computers of the Climate Research Unit of East Anglia University were hacked, and email purporting to expose a conspiracy by scientists to suppress data that contradicted their conclusions regarding global warming was made available on a Russian FTP server.[16]