Hacktivists Battle Government and Corporate Forces of Oppression

by James Ball via rayn - The Guardian *Saturday, Apr 21 2012, 12:24pm*
international / mass media / other press

> If there is a battle over the future shape of the internet – and society as a whole - then hacktivist groups such as Anonymous and Lulzsec, Wikileaks and the file-sharing site Megaupload.com are among the frontline battalions.

While the individual incidents and clashes involving these groups may seem disparate and unconnected, those at the core of online activism say all these organisations, plus relatively mainstream movements such as Occupy and the Pirate Party, are linked.

John Perry Barlow, lyricist for the Grateful Dead and co-founder of the well-known advocacy group Electronic Frontiers Foundation (EFF), says the over-arching motivation of such efforts, whatever tactics are used, was to shift the nature of society.

"What unites these groups is the belief that the future is not about vertical, hierarchical government, but horizontal [peer-to-peer] government," he said. "This pits the forces of the information age against those of the industrial age, as we move from scarcity of information to abundance. The last year has established our ability to have revolutions, but not to govern in their wake – but that's coming.

"Different groups are on a spectrum. Organisations like the EFF would be on the conservative end. Along the way is WikiLeaks and the Pirate party, with Anonymous at the more radical end."

Though ties between the groups are often tenuous, a broadly shared ideology of a libertarian distrust of government, belief in networks of free citizens, mistrust of copyright and intellectual property laws, and a drive for self-determination appear to unite the hacktivist fringe of the internet.

Barlow believes the US government has started aggressively pursuing political hackers such as Anonymous and Lulzsec. The groups mounted attacks taking US and UK government websites offline, targeted News International, allegedly taking a tranche of emails belong to staff of the Sun, and took the full email archives of US intelligence firm Stratfor and passed them to WikiLeaks.

"The government targets Anonymous for the same reason it targets al-Qaida – because they're the enemy. And in a way, they are. The shit is starting to hit the fan, but we haven't started to see the effects of that yet. The internet is the most liberating tool for humanity ever invented, and also the best for surveillance. It's not one or the other. It's both."

Barlow is working on a system to oppose the financial blockade imposed against WikiLeaks. In the wake of WikiLeaks' publication of US diplomatic cables, Senator Joe Lieberman called on US companies to cut off the site. Payment providers Visa, Mastercard and Paypal acceded to the request, despite no order or request coming from government, starving the site of funding.

Barlow is planning the establishment of a foundation aimed at funding any organisations affected by corporate blockades with first amendment implications.

"We hope it makes a moral argument against these sorts of actions," he says. "But it could also be the basis of a legal challenge. We now have private organisations with the ability to stifle free expression. These companies have no bill of rights that applies to their action – they only have terms of service."

As a result, battles over the future of the internet are becoming increasingly politicised as opposing sides try to set the legal framework. A huge network of grassroots organisations coalesced in the US to fight the stop online piracy act (Sopa). The bill was eventually stopped in its tracks as opposition mounted, but similar efforts in the EU and elsewhere have had more success proceeding through the legislature.

On other fronts, cyber-surveillance is increasing, with the UK government proposing a law to allow the monitoring of information on emails, social network and Skype traffic on all users in real-time. To fight such efforts, hacktivists are getting political.

The best known movement of this sort is the Pirate party, which was founded in Sweden by Rickard Falkvinge in 2006 and is marginal in the UK but is building up substantial influence across the world. The party has two MEPs in the European parliament, and recently took 7.4% of the vote in recent elections in the Saarland region of Germany – and according to recent polls it is now the third biggest in the country.

The party has even briefly had a cabinet minister, Slim Amamou, a Tunisian activist who served as sports and youth minister in his country for a brief period last year before resigning in protest over web censorship imposed by Tunisia's army.

Amelia Andersdotter, one of the party's two MEPs, thinks authorities tend to ignore the political element of hacking attacks by groups such as Anonymous.

"Some of these hacking attacks are misconstrued. Many are clearly politically targeted, attempts to register protest at something a government or organisation is doing," she says. "There is a lack of understanding in cyber-security. Things are seen as big and intimidating when they are often not.

"Suddenly, denial of service attacks [an attack which floods a site with fake traffic, preventing people visiting] which used to be legal in many member states, are being prosecuted. Most of these used to be for bad reasons, attacks by rivals, but now more than half are political and there are more prosecutions."

Andersdotter's priorities are looking into how public authorities' security efforts are regulated and held to account, attempting to reform the EU's intellectual property laws, and helping to spread fibre internet – faster broadband speeds – across the EU.

Others aren't content merely to lobby politicians for a free internet. Instead, they have built tools designed to make regulating the internet an impossible task. One of the most widely used is Tor,

short for "the onion router".

Tor, when used properly, anonymises all internet traffic coming from a machine by bouncing it around dozens of other computers around the world, taking a different path each time. This means an individual will only be identifiable when he or she chooses to log into a given site.

The system is not infallible, as it can be blocked – temporarily – by authoritarian governments, but provides a huge degree of protection, whether to activists working in oppressive regimes, or to those using the internet to smuggle drugs or share child pornography.

This dilemma has not gone unnoticed by the people behind the tools.

"Criminals will always be opportunists and will see new prospects before everyone else does," says the Tor project's executive director, Andrew Lewman. "Old-fashioned police work still works incredibly well against such people. Almost every transaction in the UK uses EFT [card payment], there is CCTV on every street, and monitoring of online communications – but you still have trafficking and other crimes.

"The benefits of the open internet work much the same as motorways or interstates: they outweigh the costs. In the US, police opposed the building of interstate roads, saying they would help criminals circumvent the law. But the police adapted, and the benefits of highways clearly outweigh the costs."

Lewman says the main motivating factor behind the Tor project is not to overthrow government, or even to engage in activism, but rather to give users control over how they use the internet and who is able to monitor their activity. But he is not surprised that governments are trying to regulate the internet.

"Governments are starting to realise a growing share of their GDP depends on the internet. Government like stability, not rapidly shifting ground," he concludes.

But government could be circumvented entirely, as coders haven't only been building ways of circumventing legal oversight: they have built a whole new stateless currency from the ground up.

The currency is known as Bitcoin, and relies on a series of mathematical algorithms to govern the amount of money in circulation and the future inflation rate. Each Bitcoin has a unique ID and transactions are recorded in public ledgers, making fraud far more difficult than most real-world currencies – but as Bitcoins aren't backed by a government, if they're stolen, they're gone forever, as some early adopters found out to their cost.

At the time of writing, there are more than 8.7m Bitcoins in existence, worth a total of around $42.3m (£26.2m). The combination of a stateless currency and untraceable internet use is a powerful one, as one underground site highlights.

The Silk Road is a website only accessible in the "dark" section of Tor, meaning it can't be viewed or traced on the general internet, and accepts only Bitcoins for payment. The site allows the buying and selling of illegal drugs, predominantly in the US, UK and Netherlands.

Its existence isn't a secret. In 2011 two senators wrote to the US attorney general asking for action to be taken against the site, which was described as a "one-stop shop for illegal drugs that represents the most brazen attempt to peddle drugs online that we have ever seen".

Action against the site, which operates in a similar manner to eBay, linking independent buyers and sellers, has so far proved impossible, and the publicity generated for the Silk Road only boosted its – and Bitcoin's – popularity.

Promoting such enterprises is not, though, the driving motivation for most of the people behind the development of Bitcoin.

One core member of Bitcoin's development team, Amir Taaki, explains the broad motivations of the hacktivist movement from a "hackspace" in east London – a loose members' club designed to let people build, code and tinker as they wish. Even the space's door is customised: it's tailored to open when members pass their Oyster card or similar radio-frequency ID nearby, and then plays a customised greeting (one has chosen the victory theme from Final Fantasy VII, a cult 90s videogame).

The first principle of hacker culture, Taaki says that "all authority should be questioned". He stresses this doesn't mean governments or police are necessarily corrupt, or aren't needed, but that the public should always be in a position to hold such authorities to account.

This leads to the second core principle: information should, generally speaking, be free. Copyright laws, patents, government secrecy and more are a huge target for the movement.

What this would mean for industries such as pharmaceuticals, where a pill may cost pennies to make but millions to research is unclear, though – and Taaki doesn't have the answers. What he does raise is a challenge. To date, it's the entertainment industries – Hollywood, music, television and publishers – that have felt the effects of piracy and filesharing. Developments in technology mean that may not remain the case for long.

Devices known as 3D printers are able to create real-life objects based on three-dimensional plans. The technology is expensive: a cheap commercial machine costs upwards of £10,000, but a build-it-yourself open source version has already been conceived. The RepRap can be built for just over £300. Intriguingly, a RepRap can currently produce around half the parts needed to make another one. Given enough time, the devices will likely be able to print out the parts to make a whole new 3D printer – a self-replicating machine.

It's a technology with impressive potential, the ability to "print" virtually any item that can be conceived – tools, toys, even food – but the applications to date are fairly basic, and costly. At present, the printers can mainly make novelty items – though early, successful attempts to clone plastic Warhammer toys led to lawsuits and a predictable backlash.

A technology that could allow anyone to manufacture any item, given the right blueprints, heralds a huge storm for any company relying on old-world business models – and today's hackers know it.

"The battle between pirates and the music or film industries is really nothing, it's a warm-up," Taaki says. "When this technology matures, manufacturers, agriculture businesses, technology firms, any of this could be easily replicated by almost anyone, anywhere. That's when we'll see the real fight – and they don't even see it coming."

http://www.guardian.co.uk/technology/2012/apr/20/hacktivists-battle-internet

Cleaves Alternative News. http://cleaves.lingama.net/news/story-3169.html