Dress code for an Anonymous vendetta (Image: Sander Koning/AFP/Getty)

Editorial: Democracy 2.0: The world after WikiLeaks

WHILE it is not, as some have called it, the "first great cyberwar", the digital conflict over information sparked by WikiLeaks amounts to the greatest incursion of the online world into the real one yet seen.

In response to the taking down of the WikiLeaks website after it released details of secret diplomatic cables, a leaderless army of activists has gone on the offensive. It might not have started a war, but the conflict is surely a sign of future battles.

No one is quite sure what the ultimate political effect of the leaks will be. What the episode has done, though, is show what happens when the authorities attempt to silence what many people perceive as a force for freedom of information. It has also shone a light on the evolving world of cyber-weapons (see "The cyber-weapon du jour").

WikiLeaks was subjected to a distributed denial of service (DDoS) attack, which floods the target website with massive amounts of traffic in an effort to force it offline. The perpetrator of the attack is unknown, though an individual calling himself the Jester has claimed responsibility.

WikiLeaks took defensive action by moving to Amazon's EC2 web hosting service, but the respite was short-lived as Amazon soon dumped the site, saying that WikiLeaks violated its terms of service. WikiLeaks responded via Twitter that: "If Amazon are so uncomfortable with the first amendment, they should get out of the business of selling books".

With WikiLeaks wounded and its founder Julian Assange in custody, a certain section of the internet decided to fight back. Armed with freely available software, activists using the name "Anonymous" launched Operation Avenge Assange, targeting DDoS attacks of their own at the online services that had dropped WikiLeaks.

These efforts have so far had limited success, in part due to the nature of Anonymous. It is not a typical protest group with leaders or an organisational structure, but more of a label that activists apply to themselves. Anonymous has strong ties to 4chan.org, a notorious and anarchic message board responsible for many of the internet's most popular memes, such as Rickrolling and LOLcats. The posts of unidentified 4chan users are listed as from "Anonymous", leading to the idea of a collective anonymous campaigning force.

This loose group has previously taken action both on and offline against a number of targets, including Scientologists and the Recording Industry Association of America, but the defence of WikiLeaks is their most high-profile action yet. Kristinn Hrafnsson, a spokesman for WikiLeaks, said of the attacks: "We believe they are a reflection of public opinion on the actions of the targets."

The "public" have certainly played a key role. The kind of DDoS attacks perpetrated by Anonymous are usually performed by botnets - networks of "zombie" computers hijacked by malicious software and put to use without their owner's knowledge. Although Anonymous activists have employed traditional botnets in their attacks, the focus now seems to be on individuals...
volunteering their computers to the cause.

"I think there are two groups of people involved," says Tim Stevens of the Centre for Science and Security Studies at Kings College London. The first group are the core of Anonymous, who have the technological know-how to bring down websites. The second group are ordinary people angry at the treatment of WikiLeaks and wanting to offer support. "Anonymous are providing the tools for these armchair activists to get involved," says Stevens.

The human element of Anonymous is both a strength and a weakness. Though the group's freely available LOIC software makes it easy for anyone to sign up to the cause, a successful DDoS requires coordinated attacks. This is often done through chat channels, where conversations range from the technical - "I have Loic set to 91.121.92.84 and channel set to #loic, is that correct" - to the inane - "please send me some nutella ice cream".

There are continual disagreements about who and when to attack, though new tactics also emerge from the chat, such as Leaksplin, an effort to highlight some of the less-publicised leaks, and Leakflood, a kind of analogue DDoS that attempts to block corporate fax machines with copies of the cables.

These chat channels are also occasionally knocked offline by DDoS attacks. Some blame "the feds", but could governments - US or otherwise - actually be involved? (see "Are states unleashing the dogs of cyberwar?")

The US Department of Defense's recently launched Cyber Command has a dual remit: to defend US interests online and conduct offensive operations. Cyber Command is meant to defend .mil and .gov web domains, but do commercial websites qualify too? "Is PayPal really that important to national security that the US military would have a role in defending it?" asks Stevens, who also teaches in the Department of War Studies at King's College London. "The US doesn't have an answer to that particular conundrum, and they're not alone - nobody does".

The difficulty comes in assessing whether DDoS attacks are an act of cyberwar, a cybercrime or more akin to online civil disobedience.

Individual LOIC users may not even be breaking the law. "All that DDoS does is send the normal kind of traffic that a website receives," says Lilian Edwards, professor of internet law at the University of Strathclyde in Glasgow, UK. "That has always been the legal problem with regulating DDoS - each individual act is in fact authorised by the site, but receiving 10 million of them isn't."

It's hard to say what will happen next. Anonymous might continue its attempt to cause as much disruption as possible, but it could just as easily become fragmented and give up. With no leaders or central structure, it is unlikely to be stopped by a few arrests or server takedowns but may equally find it difficult to coordinate well enough to have an impact.

More worrying is the prospect that more organised groups may follow Anonymous's example. If that happens, who will be responsible for stopping them - and will they be able to?

Read more: Are states unleashing the dogs of cyber war?

The cyber-weapon du jour
The main tool provided by the online activist group Anonymous is a piece of software written in the programming language C#, called the Low Orbit Ion Cannon (LOIC).

Originally designed to stress-test websites, it performs distributed denial of service (DDoS) attacks by flooding websites with access requests. LOIC has two modes, one in which the user manually chooses a target and another in which they connect to a central "hive mind" to be assigned a target, creating a volunteer botnet (see main story). The hive mind is coordinated through chat channels run by Anonymous.

The LOIC software has also been ported to Javascript, creating a browser-based version that can instigate DDoS attacks at the click of a mouse. This currently requires manual targeting, but a hive mind version is in the works.
Anonymous is constantly evolving its tools, using sites called pastebins to share snippets of computer code and discuss new features. More powerful High Orbit Ion Cannon software has also been released - though some Anonymous members have warned against using it until it has been checked for malicious code.

Still, using LOIC is not without risks. Researchers at the University of Twente in the Netherlands have shown that both the downloadable and web-based versions of LOIC make no attempt to mask the IP address of the user, potentially allowing attacks to be traced back. It is like, they say, "overwhelming someone with letters, but putting your home address on the back of the envelope".