Could Anonymous really shut down the internet?

In a statement posted online last month, hacker collective Anonymous announced plans to shut down the internet. Yes, you read that right.

Operation Global Blackout, planned for March 31, is apparently a protest against “SOPA [Stop Online Piracy Act], Wallstreet (sic), our irresponsible leaders and the beloved bankers who are starving the world for their own selfish needs”.

So how serious are these threats?

Well, for a start, it’s worth pointing out that the date of the take-down could be an indication of an April Fools joke – albeit one day early. And then there are the suggestions that whoever published the announcement does not really represent Anonymous. Instead, they appear just to be using Anonymous’ name and reputation to give their anti-SOPA campaign some publicity.

(Of course, in an organisation as decentralised as Anonymous, it’s difficult to say whether anyone really speaks for it.)

But even if the plans of “Anonymous” don’t come to fruition, would their take-down methods actually work? Is it possible to shut down the internet?

There is no mystery about what Anonymous (or the people claiming to be Anonymous) is planning to do. Anonymous specialises in distributed denial of service (DDoS) attacks, which they’ve used to great effect in the past.

In a DDoS attack, computers across the internet either wittingly or unwittingly send so many requests to a target server that the target becomes overwhelmed. In attempting to service all the requests it receives, the target server “loses” legitimate requests, causing genuine users to experience unacceptable delays or time-outs.

Anonymous is supposedly planning to attack the root servers of the internet’s Domain Name System (DNS). Traffic through the internet is transmitted based on IP addresses (72.21.214.128) but we humans are much more comfortable remembering the corresponding domain names (amazon.com).

When you enter a server name such as www.amazon.com into your browser, your browser uses the DNS to “resolve it” to an IP address, before attempting to connect you to the relevant site.

The DNS is a hierarchical system. Your local ISP will have a DNS service but if it can’t resolve a domain name to an IP address, it will refer it to another DNS service higher up the chain.

At the top of the hierarchy are the 13 root servers that Anonymous is apparently going to target. The idea is that if you take down all 13 root DNS servers, domain name resolution for the internet would eventually fail.

(I say “eventually” because results from the root servers are usually cached by servers at lower levels in the hierarchy for several hours. But more on that in a moment.)

So how feasible is it that a DDoS on the root servers would succeed? The answer: very unlikely. The internet’s root servers are such an obvious target that DDoS attacks have been carried out on them before, but with limited success.

In fact, there are a number of factors that make this kind of attack very difficult.

The biggest is that, while each root server has one IP address and appears to be one machine, these servers...
actually consist of many geographically distributed servers. Many more than 13 servers would need to be brought down to take down the internet’s DNS.

Of course, we shouldn’t discount Anonymous’ ability to marshall many hosts to an attack, but for this particular attack to succeed, an enormous number of hosts would be needed.

The second difficulty is that the root servers typically just act as a conduit to another server lower in the hierarchy. For instance, domain names that end in .au are forwarded on to the the DNS run by AusRegistry. In other words, not every domain name resolution request needs the root server to be successful.

Finally, even if the root servers could be brought down, most ISPs cache queries from these root servers for substantial amounts of time. For Anonymous to “take down” the internet, they would need to maintain a sustained attack. Only after the cached entries have timed out would the attack start to be noticed by users. This would likely take several hours; much longer than the minutes claimed by Anonymous.

So, all things considered, it’s very unlikely a DDoS attack on the internet’s root DNS servers would succeed. But that’s not to say there aren’t other weaknesses that could be exploited to shut the internet down.

The core of the net consists of devices called routers which decide where to transmit data. In 2010 a software fault in these devices briefly caused approximately 1% of the internet to go offline.

There are also vulnerabilities in the protocol at the core of the internet – the Border Gateway Protocol (BGP) – that have led to some failures. In 2010 a Chinese ISP caused a brief outage of a substantial part of the internet through what is thought to be a BGP configuration error.

Such vulnerabilities would be very difficult to exploit in the form of an attack – and I’m certainly not suggesting anyone should try.

Regardless, if the internet is ever brought down, I suspect it will be through something more sophisticated and more arcane than a DDoS of the net’s DNS root servers.