print this page

Greenwald writes: "Recall that all the way back in 2008, the Pentagon prepared a secret report (ultimately leaked to WikiLeaks) that decreed WikiLeaks to be a 'threat to the US army' and an enemy of the US."

go to original

Prosecution of Anonymous Activists Highlights War for Internet Control

By Glenn Greenwald, Guardian UK
23 November 12

The US and allied governments exploit both law and cyber-attacks as a weapon to punish groups that challenge it

Whatever one thinks of WikiLeaks, it is an indisputable fact that the group has never been charged by any government with any crime, let alone convicted of one. Despite that crucial fact, WikiLeaks has been crippled by a staggering array of extra-judicial punishment imposed either directly by the US and allied governments or with their clear acquiescence.

In December 2010, after WikiLeaks began publishing US diplomatic cables, it was hit with cyber-attacks so massive that the group was "forced to change its web address after the company providing its domain name cut off service". After public demands and private pressure from US Senate Homeland Security Chairman Joe Lieberman, Amazon then cut off all hosting services to WikiLeaks. Sophisticated cyber-attacks shortly thereafter forced the group entirely off all US website services when its California-based internet hosting provider, Everydns, terminated service, "saying it did so to prevent its other 500,000 customers of being

affected by the intense cyber-attacks targeted at WikiLeaks".

Meanwhile, Chairman Lieberman's public pressure, by design, also led to the destruction of WikiLeaks' ability to collect funds from supporters. Master Card and Visa both announced they would refuse to process payments to the group, as did America's largest financial institution, Bank of America. Paypal not only did the same but froze all funds already in WikiLeaks' accounts (almost two years later, a court in Iceland ruled that a Visa payment processor violated contract law by cutting of those services). On several occasions in both 2011 and 2012, WikiLeaks was prevented from remaining online by cyber-attacks.

Over the past two years, then, this group - convicted of no crime but engaged in pathbreaking journalism that produced more scoops than all other media outlets combined and received numerous journalism awards - has been effectively prevented from functioning, receiving funds, or even maintaining a presence on US internet servers. While it's unproven what direct role the US government played in these actions, it is unquestionably clear that a top US Senator successfully pressured private corporations to cut off its finances, and more important, neither the US nor its allies have taken any steps to discover and apprehend the perpetrators of the cyber-attacks that repeatedly targeted WikiLeaks, nor did it even investigate those attacks.

The ominous implications of all this have been never been fully appreciated. Recall that all the way back in 2008, the Pentagon prepared a secret report (ultimately leaked to WikiLeaks) that decreed WikiLeaks to be a "threat to the US Army" and an enemy of the US. That report plotted tactics that "would damage and potentially destroy" its ability to function. That is exactly what came to pass.

So this was a case where the US government - through affirmative steps and/or approving acquiescence to criminal, sophisticated cyber-attacks - all but destroyed the ability of an adversarial group, convicted of no crime, to function on the internet. Who would possibly consider that power anything other than extremely disturbing? What possible political value can the internet serve, or journalism generally, if the US government, outside the confines of law, is empowered - as it did here - to cripple the operating abilities of any group which meaningfully challenges its policies and exposes its wrongdoing?

But what makes all of this even more significant is the vastly disparate treatment of those who launched far less sophisticated and damaging attacks at those corporations which complied with US demands and cut off all funding and other services to WikiLeaks. Acting in the name of Anonymous, a handful of activists targeted those companies with simple "denial of service" attacks, ones that impeded the operations of those corporate websites for a few hours.

In stark contrast to the far more significant attacks aimed at WikiLeaks, these attacks, designed to protest the treatment of WikiLeaks, spawned a global manhunt by western nations and, ultimately, the arrest of dozens of mostly young alleged hackers, four of whom are now on trial in London:

> *"Four activists from the hackers collective Anonymous caused multimillion-pound losses to a number of firms in revenge for the backlash against WikiLeaks, a court has heard.*
>
> *"Using the name Operation Payback, the four flooded websites belonging to companies including PayPal and Ministry of Sound with messages and requests in order to bring them down. . . .The self-styled 'hactivists' caused losses worth more than £3.5m at PayPal and caused sites belonging to MasterCard and the recording industry to go offline.*
>
> *"Three of the group have admitted their role in the conspiracy. Christopher Weatherhead, 22, a*

> *student at Northampton University, is on trial at Southwark crown court accused of being 'part of a small cabal of leaders' of the cyber-attacks. . . .*
>
> *"The four used a free internet tool called Low Orbit Ion Canon (LOIC) as a 'destructive cyber weapon', the court heard. 'Once downloaded, the LOIC could be used to attack by sending internet traffic to a target computer,' [the prosecutor] said. 'When the volume of traffic sent to a computer becomes too much for it to handle it would suffer a denial of service. The more LOICs used, therefore, to attack a target computer, the more likely that a denial of service will take place.'"*

Last year, the FBI arrested 16 people in the US in connection with similar attacks on Master Card, Visa and Amazon, and charged them with crimes that carry 10-year prison terms.

The issue here is not whether Anonymous activists can be rightfully prosecuted: acts of civil disobedience, by definition, are violations of the law designed to protest or create a cost for injustices. The issue is how selectively these cyber-attack laws are enforced: massive cyber-attacks aimed at a group critical of US policy (WikiLeaks) were either perpetrated by the US government or retroactively sanctioned by it, while relatively trivial, largely symbolic attacks in defense of the group were punished with the harshest possible application of law enforcement resources and threats of criminal punishment.

That the US government largely succeeded in using extra-legal and extra-judicial means to cripple an adverse journalistic outlet is a truly consequential episode: nobody, regardless of one's views on WikiLeaks, should want any government to have that power. But the manifestly overzealous prosecutions of Anonymous activists, in stark contrast to the (at best) indifference to the attacks on WikiLeaks, makes all of that even worse. In line with its unprecedented persecution of whistleblowers generally, this is yet another case of the US government exploiting the force of law to entrench its own power and shield its actions from scrutiny.

Disclosure

Over the past couple months, I've been involved in discussions regarding the formation of a new organization designed to support independent journalists and groups such as WikiLeaks under attack by the US and other governments, one that would provide funding and a network for other means of support to enable them to operate. My role would be limited to unpaid board member. The group is not yet formed and my participation is only in the preliminary discussion stages, but disclosure still seems appropriate given the topic I'm writing about here. If and when this evolves further, as I hope it will, I will certainly write more on it.