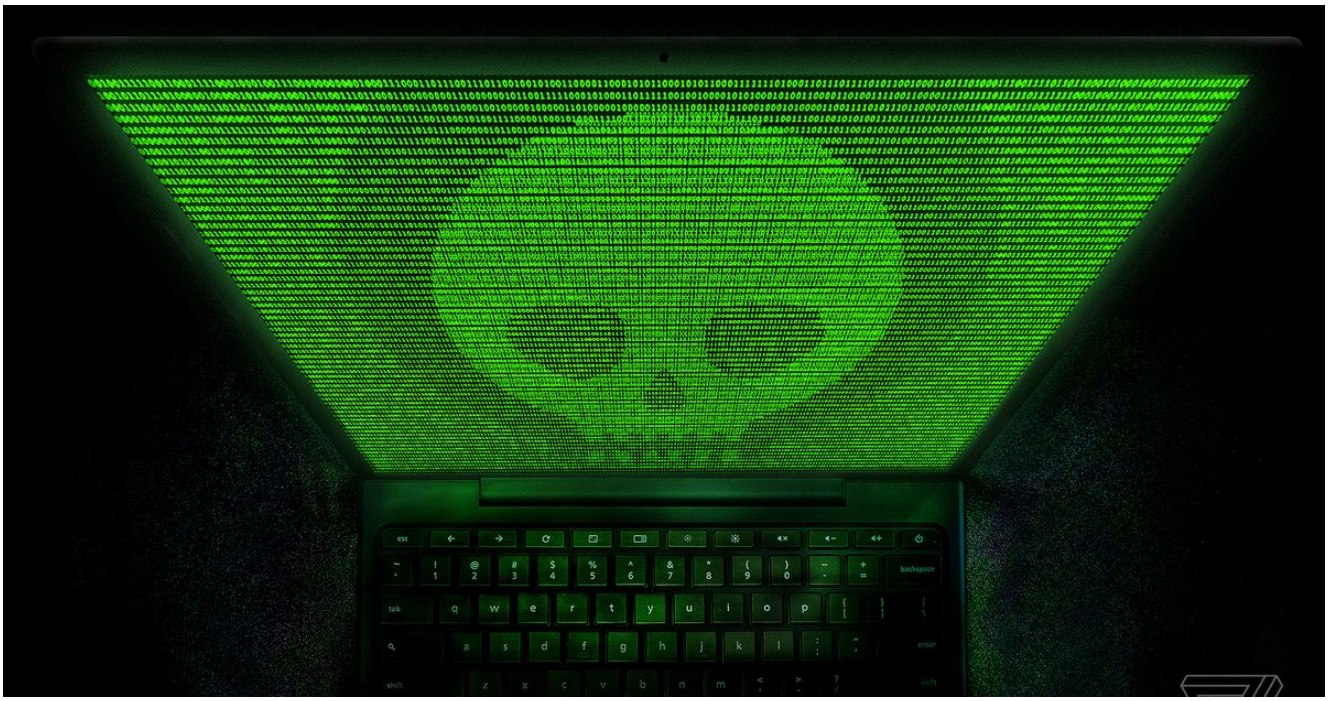
US Cyber Command has reportedly been aggressively targeting Russia's electrical grid



The United States Cyber Command has made a number of incursions into Russia's electrical infrastructure in recent months, according to a new report in *The New York Times*. Officials that the publication spoke with characterized the moves as a warning to Russia that the US is willing to operate more aggressively in this arena to deter potential cyberattacks.

According to the *Times*, "officials described the previously unreported deployment of American computer code inside Russia's grid and other targets." One senior intelligence official told the *Times* that "it has gotten far, far more aggressive over the past year," and that they are "doing things at a scale that we never contemplated a few years ago." The efforts amount to what is described as a "persistent presence" within Russia's infrastructure, and there is no

indication that the US has actually launched any sort of attack.

‘it has gotten far, far more aggressive over the past year’
Officials tell the *Times* that the US has been probing the country’s electrical grid since 2012, and that those efforts have stepped up significantly in recent months, sending “potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before.”

US officials have spoken about the need to be able to launch a cyberattack against the Russian government if the need arises. The *Times* says that Cyber Command didn’t outline what actions it had specifically undertaken with its newfound authorization. It also notes that the agency can undertake operations with authorization from the Secretary of Defense, without the approval of the President.

The newly-revealed actions parallel those that Cyber Command undertook in November 2018 to take down state-linked troll operations like the Internet Research Agency before the midterm elections. Those operations reportedly took the group offline and unable to access the internet, and it was one of the most aggressive actions made public after the Department of Defense authorized the Command to make more offensive campaigns in June.

The efforts appear to be part of a move by the Trump Administration deter potential attacks by demonstrating that the US is willing to delivering a cyber attack. At a conference earlier this week, National Security Advisor John Bolton said that the US made the response against election meddling their “highest priority last year,” and that they were ready to impose heavy costs on anyone who tried until they “[got] the point.”

https://www.theverge.com/2019/6/15/18680445/us-cyber-command-r

ussian-electrical-grid-cyberattack-deterrent-report