Hitting back at hackers: debate swirls on how far to go

1 November 2016, by Rob Lever

Some US analysts argue that hackers and states responsible for attacks should get a taste of their own medicine, but others fear doing so could spark a so-called 'cyber war'

After a seemingly endless barrage of cyberattacks, debate is heating up on hitting back at hackers where it hurts.

Amid calls for ways to punish and deter hackers without sparking a so-called "cyber war," a panel of experts assembled by the George Washington University Center for Cyber and Homeland Security said in a report Monday that US policies should be eased to allow "active defense" measures by both the government and private sector.

However, it stopped short of endorsing the idea of "hacking back" to disable systems used by attackers.

The panel envisioned measures such as taking down "botnets" that disrupt cyberspace, freeing data from "ransomware" hackers and "rescue missions" to recover stolen data.

The report follows a wave of high-profile attacks against US companies and government databases, and after Washington accused Russia of using cyberattacks to attempt to disrupt next week's presidential election.

It comes after President Barack Obama called for a "proportional" response to Russia, while leaving unanswered whether this would mean a cyber attack or measures such as diplomatic or economic sanctions.

'Shooting behind the rabbit'

Former national intelligence director and GWU task force co-chair Dennis Blair said the US has been moving too slowly in its response to cyberattacks.

"We are shooting so far behind the rabbit that we will only hit it if the rabbit makes another lap and comes back to where it was," he told a conference presenting the report.

Some analysts argue that hackers and states responsible for attacks should get a taste of their own medicine, and that US laws should be amended to allow for hacking back at the cyber criminals.

Some proposals call for private security firms to be "deputized" to carry out legally sanctioned hack-back operations when private firms are victimized.

"Department stores hire private investigators to catch shoplifters rather than relying only on the police. So too private companies should be able to hire their own security services," said a Hoover Institution paper written by scholars Jeremy Rabkin and Ariel Rabkin.

"There should be a list of approved hack-back vendors from which victims are free to choose."

Juan Zarate, a former White House national security advisor who now works with the

Foundation for Defense of Democracies, said such a model for action could be based on the early days of the republic when Congress issued "letters of marque and reprisal" for private merchant ships to bring in maritime pirates.

In an essay last year, Zarate called for a "cyber-privateering regime that rewards, enables, and empowers the private sector to help defend itself in concert with government."

Others warn of the dangers of empowering private actors to engage in reprisals.

Nuala O'Connor, president of the Center for Democracy and Technology and co-chair of the GWU panel, argued of unintended consequences of authorizing companies to break into outside computer networks.

"I believe these types of measures should remain unlawful," she wrote, adding that it remains difficult to be sure of cyberattacks' sources.

"The risks of collateral damage to innocent internet users, to data security, and to national security that can result from overly aggressive defensive efforts needs to be better accounted for."

'Cyber shooting war'

Steve Grobman, chief technical officer at Intel Security, also questioned whether private entities should be allowed to take counter-measures.

Because hackers can easily disguise their attacks, Grobman said a questionable retaliation could create an ugly situation.

"What I worry about is a terrorist entity creating an attack that appears to come from a nation state that creates a public push for some hack back and that leads to a live shooting cyber war," he said.

James Lewis, senior fellow at the Center for Strategic and International Studies, said the United States has pledged to its international partners to steer clear of these kinds of acts in cyberspace.

"We've told people the internet should be based on the rule of law, and (hacking back) would undercut that," he said.

"The question you always want to ask is whether this would make cyberspace more or less stable. This would make it less stable."

Patrick Lin, who led a study this year for California Polytechnic State University on the ethics of hacking back, said there is "a moral case for hacking back, but an under-developed case for its legality and effectiveness."

In the report, Lin wrote that while it is difficult to know whether hacking back has deterrent value, "doing nothing, as seems to be the case now, certainly offers no deterrence and likely encourages cyber-attackers to continue preying on others."