US should strike back at cyberattackers: report

October 31 2016

Although the scope of cyberattacks is understood, the solutions remain controversial

The US government and private sector should strike back against hackers to counter cyberattacks aimed at stealing data and disrupting important computer networks, a policy report said Monday.

A panel of experts assembled by the George Washington University Center for Cyber and Homeland Security said policies should be eased to allow "active defense" measures that deter hackers—differentiating that from 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 time for action on the issue of active defense is long overdue, and the private sector will continue to be exposed to theft, exfiltration of data, and other attacks in the absence of a robust deterrent," the report said.

"When private sector companies have a capability to engage in active defense measures, they are building such a deterrent, which will reduce risks to these companies, protect the privacy and integrity of their data, and decrease the risks of economic and societal harm from large-scale cyberattacks."

The report follows a wave of high-profile attacks against US companies and government databases, and after the Obama administration accused Russia of using cyberattacks to attempt to disrupt the November presidential election.

US policymakers are moving too slowly in dealing with a "dynamic" threat from cyberspace, former national intelligence director and task force co-chair Dennis Blair said.

The Obama administration accused Russia of using cyberattacks to attempt to disrupt the November presidential election

"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.

However, the panel did not recommend hacking back "because we don't want the cure to be worse than the disease," project co-director Frank Cilluffo said.

But "there are certain steps companies can take" to repel and deter cyberattacks, he added, advocating the establishment of a legal framework for them.

Although the scope of the problem is understood, the solutions remain controversial.

Some of the recommendations go too far by inviting companies to gain unauthorized access to outside computer networks, task force co-chair Nuala O'Connor, president of the Center for Democracy & Technology, said in a dissent.

"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."

© 2016 AFP

Citation: US should strike back at cyberattackers: report (2016, October 31) retrieved 20 April 2024 from https://phys.org/news/2016-10-cyberattackers.html