The Washington Post

The Cybersecurity 202: Hacking back may be less risky than we thought

Joseph Marks

October 2, 2019

The United States has historically been wary of punching back in cyberspace, fearing that a digital conflict could rapidly escalate to rockets and bombs. But those concerns may be overblown.

A pair of recent studies has found it's extremely rare for nations to ratchet up a cyber conflict, let alone escalate it to a conventional military exchange, and that the U.S. public may put extra pressure on leaders not to let a cyber conflict get out of hand.

“The emerging consensus among researchers is that cyberattacks aren’t unusually escalatory. If anything, the opposite is true,” writes Jacquelyn Schneider, a researcher at Stanford University's Hoover Institution, who was a co-author on one of the studies and detailed both of them in a Post analysis. The other study came from the libertarian-leaning Cato Institute.

The findings could be a boon for the Trump administration, which has announced a muscular new hacking back strategy in an effort to cow digital adversaries, such as Russia and China. That has included digital strikes against Russia to prevent election interference and against an Iranian computer system used to plan attacks on oil tankers. The administration is reportedly considering another round of digital retaliation to punish Iran for a drone strike against Saudi oil facilities.

That’s a major shift from the Obama administration, which preferred responding to adversary cyberattacks with just sanctions, indictments and other tools that didn’t risk sparking a tit-for-tat digital conflict.

But there’s also some bad news for the Trump team: The Cato study didn’t find much evidence that hacking back does anything to make adversaries stop hacking you in the first place, which could undermine the administration's main goal for the program.

“Attacks do not beget attacks, nor do they deter them,” the authors Brandon Valeriano and Benjamin Jensen wrote.

Schneider and her co-author, Cornell University professor Sarah Kreps, are more bullish on the Trump strategy — provided it’s focused on disabling adversaries’ infrastructure to prevent future attacks rather than scaring the adversary into not hacking us at all.

The Russia strike, for example, successfully disabled a notorious Russian troll farm, the Internet Research Agency,on Election Day 2018, but there’s no evidence it has dissuaded Moscow from launching cyberattacks since then.

They warn the public wouldn’t support a long and damaging cyberwar, though, often out of fears the United States, which is far more dependent on the Internet than its adversaries, would suffer more during a drawn-out conflict.

In many cases, the approximately 1,000 people they surveyed were unwilling to endorse digital retaliation even against a cyberattack that caused as much damage as a conventional attack, such as an airstrike.

“Deterrence hinges on public resolve for overwhelming uses of force and a willingness to escalate, which appears lacking in the cyber domain,” they write.