Operating in the shadows: US Cyber Command

May 25 2021, by Paul Handley

An aerial view of the US Cyber Command joint operations center on the NSA campus is seen on May 25, 2020, in Fort Meade, Maryland.

If the Pentagon's Cyber Command launches an online attack and nobody knows about it, does it deter anyone?

Many Americans are asking what the country's army of cyber warriors are doing after repeated attacks on US computer systems by Chinese, Russian and other hackers.

The answer may have been in the 780th Military Intelligence Brigade's subtle retweet on May 14 of a security firm's scoop that ransomware extortionist Darkside had been digitally shut down.

No one knows who took control of Darkside's servers, a week after the shady Russia-based hackers forced the closure of a major US oil pipeline, causing gasoline shortages across the Eastern US.

But suspicions are that the 10-year-old CyberCom may have stepped in, to punish Darkside and to signal the small army of ransomware providers operating out of Eastern Europe that they too are vulnerable.

Even as it remains quiet, CyberCom's role is hotly debated: is it to undertake strategic attacks during war, or to constantly joust online with adversaries' military and intelligence hackers, or to go after non-military hackers like Darkside, normally the purview of law enforcement?

Malware strike on Iran

The first sign that the US Defense Department was playing offense in the online world was in 2010 when it became known that a destructive, US and Israel-created computer worm Stuxnet had infected and damaged Iran's nuclear enrichment facilities.

Cyberwarfare then was seen as a way of attacking or deterring enemies by wrecking their infrastructure with devastating malware strikes.

Since then, however, the US government and private business have been hit time and time again, by Chinese stealing government databases and corporate secrets, Russia hacking US elections, North Koreans stealing bitcoins, and ransomware operators extorting hundreds of millions of dollars from companies, hospitals, and local authorities.

But without any news about their exploits, it didn't seem like the Pentagon was either punishing or deterring attackers.

Paul Nakasone, director of the National Security Agency (NSA) and commander of the US Cyber Command, speaks at a 2021 House Intelligence Committee hearing.

They are, General Paul Nakasone, CyberCom commander, told a recent Congressional hearing.

"When we see elements that are that are operating out of US, we try to impose the largest cost possible," he said.

"Imposing costs" meant exposing the hackers, or counterattacking, he said.

But he refused to give any examples of their work.

'Persistent engagement'

Jon Lindsay, a University of Toronto assistant professor who researches online military conflict, said the cyberwar strategy had shifted since Stuxnet.

At that time, "cyber was looked at as a digital weapon of mass destruction," something that could punish, or threaten to punish adversaries to deter their attacks.

"It was a very high level, presidentially controlled, covert action," to be used strategically and sparingly, Lindsay said.

Since then, it has become something else: an ongoing low-level fight that doesn't require top-level approval, called "persistent engagement," that does not focus on deterrence.

"It's very, very difficult, if not impossible, to deter adversarial activities in cyberspace. So what CyberCom needs to be able to do is be constantly engaged, constantly operating forward in the adversaries' networks," said Lindsay.

The Colonial Pipeline Houston Station: the FBI identified the group behind the hack of Colonial Pipeline as shadowy operation DarkSide.

Intelligence contest

That makes CyberCom more like ongoing intelligence operations, collecting information, blocking adversaries, and slightly escalating when the other side is seen to have gone too far.

Revealing what the Pentagon does could have deterrence value, according to Elizabeth Bodine-Baron, a senior information scientist at RAND Corp.

Some people, she said, believe that "if we never give concrete examples of, we went in, we did that, then no one's ever going to believe us."

But there is also a challenge of definitively attributing the source of an attack, especially when a state actor is suspected of being behind it.

But, she added, if there is certainty about an attacker's identity, going public with attribution "could potentially reveal something about our own capabilities."

In addition, boasting about CyberCom's exploits risks escalation—forcing adversaries to retaliate to satisfy their own public.

"So I think you see people kind of erring on the side of caution," not announcing what they do, said Bodine-Baron.

Lindsay said the US and its main adversaries now treat cyber conflict as a way of avoiding escalation.

"There's something about cyber that makes people unwilling to escalate," he told AFP.

"What we're looking at is not military warfare, it's an intelligence contest."

"Intelligence contests go on in peacetime. They shape the possibilities for war, but they try to make war less likely," he said.

"Actually, there is there is no good example of cyber escalating something to a kinetic conflict," he said.

Citation: Operating in the shadows: US Cyber Command (2021, May 25) retrieved 28 April 2024 from https://techxplore.com/news/2021-05-shadows-cyber.html