The U.S. Unleashes Its Cyberweapons

Stratfor: July 6, 2019

Highlights

- *The United States has made a strategic shift toward a more aggressive stance of conducting offensive cyberattacks to achieve strategic and tactical objectives.*
- *The change has been years in the making, shaped by the unique architecture of cyberspace and on continued cyberattacks that have necessitated a shift in strategy by several Western powers toward incorporating offensive capabilities.*
- *With the United States increasingly viewing the world through the lens of competition with China and Russia, the shift in strategy to incorporate the increasing use of offensive cyberoperations is likely to be permanent.*

In late June, an Iranian missile knocked a U.S. unmanned aerial vehicle (UAV) on a reconnaissance mission out of the sky and into the Gulf of Oman. The shootdown sent ripples of concern throughout the Persian Gulf that the incident could lead both countries down a path to greater conflict. But the U.S. military response barely made a splash. That's because instead of a conventional airstrike against Iranian forces, the U.S. response came in the form of a cyberattack targeting missile command and control systems of the Islamic Revolutionary Guard Corps.

That response heralded a fundamental shift in the U.S. approach to cyberwarfare. The likely tactical objective of the retaliation was to degrade Iran's ability to carry out similar attacks. It also had a strategic component — deterring it from similar actions. Significantly, the response appeared to mark a first for the United States under new rules meant to streamline the approval process for cyberattacks.

The Big Picture

Over the past three years, the United States has substantially refocused its defense posture to deal with emerging threats from what the White House calls "revisionist" powers Russia and China. One critical piece of the puzzle has been a shift in U.S. cybersecurity strategy to prioritize the response to threats from its near-peers and other state actors.

Whether the response achieved U.S. tactical objectives isn't clear; future Iranian actions will provide a measure of the success of its strategic goals. Whatever the outcome, the U.S. response itself marks a shift in the country's cyberwar strategy. The White House has not been shy about expanding the U.S. cyberwar capabilities, nor has it shied from the idea of taking the offensive in cyberspace. This was, after all, a central part of the 2018 National Cyber Strategy; such considerations will outlive the administration of U.S. President Donald Trump.

A Shift Years in the Making

Over the past two decades, the U.S. approach to cyberspace has evolved in parallel with the emergence of the technology as a key defense and commerce platform for state and nonstate actors alike. The rising stature of the U.S. Cyber Command tracks with the increasing focus on cyberspace at the Pentagon. The organization, which originated as a joint task force, became a subunified command under U.S. Strategic Command in 2009. In May 2018, U.S. Cyber Command was split off into its own separate unit. That was, in part, a culmination of U.S. thinking about exactly how cyberspace fit into its overall defense strategy. Historically, the primary U.S. concern centered on protecting the country's critical infrastructure – both civilian and military — an understandable objective. Indeed, the overall strategy in cyberspace pursued under former President Barack Obama had three pillars: raising the level of U.S. cyberdefense, deterring malignant cyberactivity aimed at the United States, and developing effective response and recovery from attacks. This paradigm is based on the concept of defending the United States, not on executing attacks abroad.

That said, the United States has not refrained from cyberspace offensives in the past, nor has it neglected to develop its offensive capabilities. The United States is strongly suspected of involvement in the 2010 Stuxnet virus attack that crippled the Iranian nuclear program. It also was rumored to have explored ways to use cyberwar techniques to sabotage the North Korean ballistic missile program. By their nature, classified programs such as these are difficult to verify, and there are often strategic reasons that the United States would refrain from publicizing such an attack. It would, for example, be more advantageous to allow the Iranians or North Koreans to believe that their own error caused the failure of a nuclear centrifuge or a missile test.

For the most part, however, the U.S. posture toward cyberspace was more defensive in nature and focused on strategic deterrence. The United States calculated that the perception of its retaliatory capabilities would make adversaries think twice before launching significant attacks targeting it. Leaks by National Security Agency contractor Edward Snowden detailing U.S. cyberactivity and the tools that the agency has at its disposal only reinforced the views of U.S. capabilities. In many ways, the split of U.S. Cyber Command away from Strategic Command, which oversees strategic deterrence, is emblematic of the shift in U.S. posture in cyberspace from defense toward what has been described as "persistent engagement."

In its 2018 Command Vision, the cyber command lays out its objective that the United States must "defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage." This belief was reinforced in the Trump White House's first full National Cyber Strategy released in September. If fully implemented, the strategy would entail frequent cyberactivity against aggressors in cyberspace — and in the case of the response after Iran's downing of the UAV, a willingness to retaliate for physical attacks through cyberwarfare.

A Change in Global Dynamics

While it may be easy to connect the more aggressive cybersecurity posture of the United States with Trump's America First strategy, multiple drivers have pushed the country in that direction.

It has become quite clear to many strategists that the classical concept of strategic deterrence has its limitations in cyberspace. While U.S. adversaries certainly calculate that a significant cyberattack against the United States could draw a U.S. response, they also know the difficulties of attributing those attacks to a specific state actor. That's why countries with such intent in cyberspace, including Russia, Iran and China, often employ nonstate actors to carry out offensives against the United States and its allies, giving them a higher degree of plausible deniability. This makes it difficult to rely on strategic deterrence, in which an adversary desiring to launch a cyberattack must first assess the probability of counterattack. This is why disruption, as opposed to deterrence, has become a more appealing option for U.S. strategists.

From an empirical perspective, the concept of deterrence hasn't held up in recent years, as the United States has faced dozens of state-backed cyberattacks from virtually every one of its adversaries. For Russia, online disinformation campaigns, of which its activities during the 2016 U.S. general elections are but one example, are extensions of its decades-old military strategy. But it does not limit its cyberspace activities to the shaping of perceptions. Its other cyberwar operations include a series of attacks testing the defenses surrounding critical U.S. infrastructure, including operations, still likely ongoing, targeting the U.S. electricity grid and its operators. While China has yet to carry out the same level of sophisticated disinformation campaigns as Russia, Chinese cyberattacks against U.S. infrastructure and network probes continue to be a key U.S. concern – although publicly released information detailing its activities is understandably rare. The simple fact is that, short of preventing a significant loss of life or economic activity, China's and Russia's actions show that the U.S. doctrine of deterrence has not held at the lower and middle levels. This same dynamic persists for North Korea and Iran – both of which have pursued actions targeting the United States in cyberspace despite the threat of retaliation. As the United States repositions its national strategy to focus more on the competition with other peer or near-peer powers like Russia and China, a shift in thinking on cyberspace has become almost a necessity. Both have shown a repeated willingness to take on the United States in cyberspace, making it necessary for the Pentagon to develop a holistic strategy to counter their actions. And in the event of a war, the United States will need to have offensive cybertools at its disposal. Malware, backdoors and other code needed to implement a cyberattack can't necessarily be developed and deployed on the fly. So if the United States wants to tap that option at a moment's notice, it will need to preemptively probe its adversaries' defenses and install the needed components before the outbreak of conflict.

Timeline of Notable Cyber Actions and Related Dates

Cyber action (attack or defensive action)

Cyber-related event

YEAR

2009

June 2009: U.S. Cyber Command is established as a subunified command under U.S. Strategic Command.

2010

October 2010: Stuxnet malware is discovered in Iran, likely a joint Israeli-U.S. cyberattack to disrupt Iran's nuclear program.

2011

August 2012: An Iranian group claims it used Shamoon virus to hack Saudi Aramco.

2012

October 2012: President Obama signs Presidential Policy Directive 20 (PPD-20), which requires a lengthy approval process for U.S. cyberattacks.

2013

June 2013: Edward Snowden releases classified documents detailing NSA cyber and surveillance programs, including PPD-20.

2014

March 2014: Chinese hackers breach Office of Personnel Management's data.

2015

April 2015: Pentagon says Russian hackers briefly gained access to an unclassified Defense Department network.

2016

November 2016: Shamoon virus is used against four Saudi agencies.

2017

July 2017: UK's GCHQ says state-sponsored hackers probably accessed industrial control systems of British energy companies.

2018

May 2018: U.S. Cyber Command becomes a fully independent operational command.

May 2018: U.S. pulls out of nuclear deal with Iran. An immediate surge of Iranian hacking activity is reported.

August 2018: President Trump reverses PPD-20, making it easier for the Defense Department to launch cyberattacks.

2019

February 2019: U.S. Cyber Command announces it blocked internet access to a Russian company involved in disinformation campaign in 2016 U.S. election.

June 2019: U.S. responds to Iranian shootdown of a U.S. drone with a cyberattack on the Islamic Revolutionary Guard Corps.

Although Iran is not a true U.S. peer in the sense of equal international power, it should come as no surprise that offensive U.S. cyber doctrine is extending to the Islamic republic. The U.S. cyberattack on Iran was clearly designed to degrade its capability to launch future attacks. This is thought to have been the first publicly acknowledged attack under new guidelines that the Trump administration put into place last year to streamline the approval process for conducting cyberattacks on U.S. adversaries, and it came just hours after the UAV was shot down — a testament to the Trump-era policy regarding cyberoffensives.

In August 2018, Trump issued an order reversing an Obama-era policy establishing intricate rules for an interagency process that must be followed before the United States could launch a cyberattack. After the reversal was publicly acknowledged, U.S. national security adviser John Bolton trumpeted the fact that the United States was no longer limited in its ability to carry out cyberoffensives. He has since delivered not-so-subtle messages aimed at Russia and China that the United States would go on the offensive in cyberspace. Trump's new marching orders, as outlined in the secret National Security Presidential Memorandum 13, are thought to grant the Pentagon greater authority to conduct cyberattacks – and to conduct hacks to set up those attacks – while reducing oversight by other U.S. agencies, like the State Department. That memo is also thought to give the Defense Department greater authority to act without presidential approval – a tactical necessity in a future hypothetical conflict between the United States and a near-peer power. While the cyberattack on Iran was publicly acknowledged, other U.S. efforts in this area have not been. The New York Times reported in June that the United States has stepped up attempts to penetrate the cybersecurity surrounding Russia's electric power grid, although U.S. officials have denied it.

The United States is not the only Western country developing its offensive cybercapabilities. In January, France unveiled a strategy shifting its own posture away from an "active defense" to incorporate offensive cyberoperations. It also announced a budget increase to expand its cyberwarfare force and said that France will not be scared of using offensive cyberoperations in the future. In 2018, The United Kingdom announced plans to create a new 2,000-strong offensive cyberforce to, in part, deal with the emerging threat from Russia. In 2013, the United Kingdom became the first Western country to announce that it had developed offensive cyberweapons. NATO, which indicated it will not conduct offensive cyberoperations itself, has said that that it would integrate and coordinate the activities of its member states.

In announcing the cyberattack in retaliation for Iran's kinetic attack on a U.S. drone, the United States has announced to the rest of the world that it will make full use of its cyberspace capabilities and will carry out offensive operations if need be. The rules and norms governing such activity in cyberspace among the United States, Russia and China will continue to evolve over time. This will invariably lead to the question of how such norms will be established, but thus far, the three leading cyberpowers have shunned the idea of talks over the topic, even grinding Europe-led and U.N.-led processes for establishing them to a halt. It is unlikely that even a clear set of norms governing cyberspace — much less a broad treaty — will occur, unless they are narrowly focused (such as a promise to refrain from attacks targeting one another's nuclear command and control systems). So with a click of the mouse, the United States has shown that it is now willing to take the gloves off in cyberspace.