US no longer has geography as defense, ally in cybercombat

January 28 2017, by Tami Abdollah

In this Sept. 30, 2011, file photo, a reflection of the Department of Homeland Security logo is seen reflected in the glasses of a cyber security analyst in the watch and warning center at the Department of Homeland Security's secretive cyber defense facility at Idaho National Laboratory in Idaho Falls, Idaho. Through history, the United States has relied on its borders and superior military might to protect against and deter foreign aggressors. But a lack of boundaries and any rulebook in cyberspace has increased the threat and leveled the playing field today. (AP Photo/Mark J. Terrill, File)

The United States has long relied on its borders and superior military might to protect against and deter foreign aggressors. But a lack of boundaries and any rulebook in cyberspace has increased the threat and leveled the playing field today.

It's unclear how President Donald Trump, who has emphasized an "America First" approach to domestic issues, will respond to cyberspace threats, which transcend traditional borders and make it easier and cheaper than ever for foreigners to attack the U.S. Whatever the approach, it will set the tone and precedent for global policies during a critical time when the ground rules are still being written.

At a hearing this month on foreign cyberthreats, the chairman of the Senate Armed Services Committee, Sen. John McCain, R-Ariz., ran through a list of recent operations the U.S. believes was carried out by foreign countries—Russia, China, Iran and North Korea. The targets: the White House, State Department, Office of Personnel Management, Joint Chiefs of Staff, Navy, major U.S. financial institutions, a small New York dam and Sony Pictures Entertainment Inc.

"Our adversaries have reached a common conclusion, that the reward for attacking America in cyberspace outweighs the risk," McCain said.

With most of the U.S. critical infrastructure in private hands and Americans among the most connected citizens in the world, the potential attack surface for any hacker is vast and increasing. U.S. officials and lawmakers have argued that because there is no official policy on cyberwarfare, the response to any attack can be slow, politicized and ultimately ineffectual.

The U.S. took two months, after publicly accusing Russian government hackers of trying to influence the presidential election, to respond with economic sanctions and other more symbolic measures.

The reality is that the "nature of conflict has moved to the information space instead of just the physical kinetic space, and it now operates at greater scale and quicker speed," said Sean Kanuck, who served as the first U.S. national intelligence officer for cyber issues in the Office of the Director for National Intelligence.

Under the Obama administration, the U.S. proposed international cyber rules for peacetime, including that countries should not target another's critical infrastructure. But otherwise, it has maintained existing international laws and reserved the right to respond to any cyberattack.

The Trump administration is reviewing cyber policies, but it has said it will prioritize developing defensive and offensive cyber capabilities. It has also said it will work with international partners to engage in "cyberwarfare to disrupt and disable (terrorist) propaganda and recruiting."

Unlike conventional warfare, the costs in cyberspace can have rippling impacts for both the victim and attacker. Malicious software may end up spreading in an unforeseen and unplanned manner, and a hacker who gets into a single computer can cause unpredicted effects to a network.

"Look at what North Korea did to Sony or what China did to us via the OPM hack," said David Gioe, a history fellow at the Army Cyber Institute at West Point and a former intelligence officer. "You've got all of these aircraft carriers and all of this ocean, and it really doesn't matter because we're still feeling effects. They're not kinetic effects, but they're surely effects."

More than 20 million people had their personal information compromised when the Office of Personnel Management was hacked in what the U.S. believes was a Chinese espionage operation.

"Really it's our geeks versus their geeks," Gioe said. "In the same way as single combat. It doesn't matter how good my army is or your army is, it's me versus you."