

WIRED

The US Gives Cyber Command The Status It Deserves

Lily Hay Newman

August 19, 2017

Between Russian meddling in multiple democratic elections, massive Chinese data exfiltration from troves like the US Office of Personnel Management, and out-of-control ransomware spreading from North Korea, nation-state cyber-aggression has become markedly more prominent in recent years. That escalation provides the backdrop for a new Trump administration directive to elevate United States Cyber Command, currently a division of the National Security Agency, to the status of a unified military command.

“This new Unified Combatant Command will strengthen our cyberspace operations and create more opportunities to improve our Nation’s defense,” President Trump said in the statement. “The elevation of United States Cyber Command demonstrates our increased resolve against cyberspace threats and ... will also help streamline command and control of time-sensitive cyberspace operations. ... Elevation will also ensure that critical cyberspace operations are adequately funded.”

Created in 2009 by then-Defense Secretary Robert Gates, Cyber Command works to unify oversight of the military’s digital offensive and defensive operations and cybersecurity resources. Cyber Command also coordinates and leads military network defense. Since the tools and strategies that enable digital intelligence-gathering are similar in many ways to those required for cyberwarfare, the NSA made for a natural first home for Cyber Command. As the division has grown, though—and its role grows more pivotal—it has become increasingly clear that Cyber Command would eventually level up.

“This is definitely the right move; they were already talking about [the elevation] just for organizational reasons,” says Joseph Loomis, CEO of the security firm CyberSponse, a current security contractor and advisor to multiple branches of the US government. “It had become too big to manage as a subordinate, and it became kind of a problem because there were too many things going on and there wasn’t enough infrastructure and leadership in place.”

As part of transition to the status of a unified command, Secretary of Defense James Mattis will nominate a new Cyber Command leader. Previously, NSA director Michael Rogers oversaw the group. But Mattis is also mulling a potential separation from the NSA, the White House said Friday, which would be a much more intriguing step for Cyber Command.

“It takes the same expertise to infiltrate for offensive purposes or intelligence until the last step, so that was the logic behind lumping them together with the NSA,” says Julian Sanchez, a senior

fellow at the Cato Institute who studies national security and intelligence surveillance. “But that last step is something where those two missions are fundamentally at odds, because an intelligence agency is focused on preserving access over time, while in offensive operations you’re usually alerting the adversary to your presence, and ultimately burning your access. So there has been a sense of tension between the mission of the NSA and Cyber Command.”

The US shouldn't rush into that separation, though. Coordination between military operations in cyberspace and digital intelligence gathering is still crucial, even with increased separation between the two disciplines. Sanchez and other experts note that if the NSA and Cyber Command do separate, they'll still need to collaborate, since the two organizations will continue to utilize many of the same tools and conduct operations around many of the same targets.

“The decision to not fully separate them was a smart one,” says Greg Martin, a former security adviser to government agencies like the CIA and NASA and CEO of the security firm JASK. “It’s going to take time to do it right and this at least guarantees that there’s no immediate operational disruption to the way that the NSA functions. It’s going to take time to get to the point where they fully separate if they ever do.”

Even the first step of elevating Cyber Command to a unified command, though, sends a geopolitical message that the US military has prioritized its digital offense and defense, while also streamlining recruitment and funding for this initiative. Though Friday’s announcement was met with bipartisan support and support from the security community, there is also awareness of how it may stoke the ongoing cyberarms race around the world.

“It’s certainly going to signal to the rest of the world that there will be a US cyber-capability buildup and adversaries are only going to be more emboldened by this news,” Martin says. “But having the best cyberweapons and capabilities is the job of our military, so we just need to be thinking carefully about defense. It’s one thing to have the biggest, baddest cyber nuke, that’s all great, but you also need to protect against the adversary’s weapons.”

The elevation of Cyber Command will likely be an intermediary step in a larger evolution, but by removing a level of subordination and making the unit more independent, the move already opens the door to changes in how the US military incorporates and recognizes digital offense and defense.

“Cyber was always just an intel thing back in the day, now it’s become more of an operational capability with a need to militarize it,” CyberSponse’s Loomis says. “The first step starts the initiative and that cultural shift, they might even have a Cyber Command academy just like you have the Naval Academy. But especially when you have so many intertwined intricacies between NSA and Cyber Command the phased approach makes sense. You can’t just run out of the building and set up a shop across the street.”