

from Net Politics and Digital and Cyberspace Policy Program

What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?

The White House has reportedly made it easier for U.S. Cyber Command to conduct offensive cyber operations, leading some observers to fret that it will create undue risks of escalation. Those concerns might be overblown.



National Security Agency Director General Paul Nakasone addresses a briefing on election security in the White House press briefing room at the White House on August 2, 2018. Carlos Barria/Reuters

Blog Post by Guest Blogger for Net Politics

September 10, 2018 10:18 am (EST)

Erica D. Borghard is an assistant professor and Shawn W. Loneragan is a research fellow at the Army Cyber Institute at West Point. Loneragan is also a U.S. Army Reserve cyber officer assigned to 75th Innovation Command. You can follow them @eborghard and @Shawn_Loneragan.

The Wall Street Journal recently reported that the Donald J. Trump administration removed some of the restrictions governing the approval process for offensive cyberattacks conducted against U.S. adversaries under Presidential Policy Directive 20 (PPD-20). With the elevation of U.S. Cyber Command to a unified combatant command in May 2018—on par with the Pentagon’s other combatant commands—the logic behind the reported revisions was that the commander of Cyber Command should have authority to take action comparable to that of other combatant command commanders.

Is the Trump administration’s change a good thing? It depends on who you ask. The news about loosening some of the restrictions on Cyber Command has been met with concern in some cyber policy circles, on the grounds that making the approvals process less rigorous creates undue risks of escalation and threatens to prioritize military over intelligence requirements.

There are certainly important considerations that should be heeded, such as how the success of offensive cyber operations are measured and the important roles of civilian oversight and interagency coordination. Additionally, some risks can be mitigated through developing standing rules of engagement (ROE) for operations conducted by U.S. Cyber Command, and maintaining the dual-hatted authorities of Cyber Command/National Security Agency (NSA) leadership.

For critics of the reported PPD-20 revisions, the risk that devolving authority to the combatant commander will generate potential escalatory pressure looms large. They fear a more proactive, offensively-postured U.S. Cyber Command may prompt U.S. adversaries to respond in turn by ratcheting up their own cyber operations against the United States. This could lead to an escalatory spiral of increasingly costly cyber operations in a context where the United States is highly vulnerable.

But, there are reasons to be skeptical about these claims—even under a hypothetical condition in which Washington becomes more aggressive in countering adversaries in cyberspace.

Cyber operations have self-dampening mechanisms. This stems from several factors. Attribution can take time—and there may be varying thresholds for confidence in attribution, particularly in a high-stakes scenario. But, beyond the attribution issue, time also affects a target's ability to marshal a response, let alone one that is escalatory. It takes a significant investment in time and resources to develop and maintain offensive capabilities, as well as persistent access to predesignated target sets. Therefore, at the time of desired execution, there may be a mismatch between available tool and access, and ideal target.

Relatedly, cyber weapons lack the universal lethality of most conventional weaponry. A strategic bomber, for instance, can reliably and consistently deliver measurable, destructive effects against any number of nearly interchangeable targets. In contrast, cyber weapons developed to target strategic assets such as nuclear power plants, dams, and air defense systems typically require unique accesses and custom-tailored capabilities.

Finally, there are inherent limitations to the scale and magnitude of the costs that can be imposed solely through cyber campaigns. Cyber weapons lack the inherent violence of conventional and nuclear forces, or even terrorist attacks. They simply do not produce destruction or elicit fear in the same way or to the same extent. Therefore, it is unlikely that even the most strategic use of cyber weapons, such as a cyberattack against a state's power grid, would generate a political imperative to escalate *comparable* to other types of kinetic attacks.

Taken together, these factors could limit the ability to strike strategic targets through cyber means in a true escalatory fashion. This creates breathing room for decision-makers to assess potential options and responses to adversary actions.

But, what about cross-domain escalation? It is conceivable that the inherent limitations on cyber response options in a crisis could produce escalation to the kinetic realm. However, it is hard to see how a more aggressive U.S. posture in cyberspace would elicit escalatory adversary responses in the conventional military domain. This is due to the reality that the United States possesses a comparative advantage in conventional domains that it could leverage to contain competition to cyberspace. The caveat, however, is that this conventional asymmetry may prompt U.S. adversaries to seek other (non-cyber) asymmetric—and potentially effective—means of contesting or responding to U.S. behavior in cyberspace.

Even if the escalation risks are greater than we assume, they can be adequately managed with the development of clearly-defined standing ROE. All U.S. combatant commands operate under established ROE that govern the use of force within an area of operations. Though many cyber operations may fall below the use of force threshold, U.S. Cyber Command nevertheless merits its own ROE to address two conditions: 1) engaging the adversary in the context of a named military operation; and 2) responding to offensive cyber operations directed against the United States and its interests. Such ROE should be nested within the broader U.S. strategic vision and diplomatic goals for cyberspace.


Developing a standing ROE would mitigate some concerns about escalation, as well as civilian oversight and interagency coordination. This is because the process to establish them could identify and codify those concerns. It would also enhance Cyber Command's operational efficiency through enabling pre-planning, driving capability development and proper staffing, and reducing decision-making friction.

Second, critics of the PPD-20 reform could argue that limiting the role of the intelligence community in decision-making about offensive cyber operations could result in prioritizing military operations over intelligence needs. This is a valid concern and one that is deeply embedded in the 2009 decision to establish the leader of U.S. Cyber Command and the NSA as a dual-hatted authority. Given the PPD-20 reform, the reportedly forthcoming decision to separate the dual-hat authority would be a mistake. Cyber operations and intelligence capabilities are mutually intertwined—cyber operations fundamentally rely on intelligence to deliver desired effects, and many operations also necessitate decisions about intelligence gain-loss tradeoffs. Managing the equities and operational effectiveness of interdependent communities is hampered without centralized leadership. While the dual-hat is not a stand-in for the entire U.S.

intelligence community, preserving those authorities would support that critical nexus between intelligence and military cyber operations, and enable the combat support role played by the NSA.

The Trump administration's reported changes to PPD-20 raise important questions, particularly concerning escalation risks and the role of the intelligence community. However, both could be addressed through a standing ROE and maintaining the dual-hatted relationship between Cyber Command and NSA.

The views expressed in this article are personal and do not reflect the policy or position of the Army Cyber Institute, U.S. Military Academy, Department of the Army, Department of Defense, or the U.S. government.

 Creative Commons: Some rights reserved.