A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem

Categories : Government, Publications, U.S. Strategy

“The second category for the NFU policy is cyber attacks that threaten the control of nuclear forces. These are cyber attacks that directly impede a nation’s ability to launch—or call back—nuclear platforms. These are not cyber attacks that affect intelligence, surveillance, or warning, which may be dangerous to overall nuclear stability but are more difficult to differentiate from cyber attacks on conventional military systems (which are often entangled with these intelligence, surveillance, and reconnaissance, or ISR, capabilities)… Despite the arguments for NFU, the United States has never implemented a clear declaratory NFU policy for nuclear weapons. Does that mean cyber NFU is dead in the water? In order to answer this question, it is important to first understand why the United States has never adopted a nuclear NFU policy and to see if the arguments hold up in the cyberspace domain.”

Read the full article, originally published in the summer 2020 issue of The Washington Quarterly, here.

(Image credit: Air Force 108th Wing)