CSBA
Center for Strategic and Budgetary Assessments

STUDIES

Cyber Warfare: A "Nuclear Option"?

August 24, 2012 | **Andrew F. Krepinevich**

Resources: Future Warfare & Concepts

A number of recent high profile developments have pushed the issue of cyber security into the spotlight. Revelations regarding the Stuxnet program, a cyber weapon that targeted Iranian uranium enrichment centrifuges, emerged in June 2012, along with reports regarding Flame, an alleged effort to extract data from the computers of Iranian nuclear scientists. The following month, President Obama penned an op-ed for the *Wall Street Journal* describing critical U.S. infrastructure as vulnerable to cyber attack. Secretary of Defense Leon Panetta went further in warning that "The next Pearl Harbor we confront could very well be a cyber attack that cripples our power systems, our [electric] grid, our security systems, our financial systems, our governmental systems."

How valid is the growing concern among senior U.S. leaders that state and non-state actors will become increasingly capable of executing cyber attacks with catastrophic consequences? Does the expansion of the military competition into the cyber domain represent a major shift in the character of warfare? Dr. Andrew Krepinevich, President of the Center for Strategic and Budgetary Assessments, examines these questions in his report, *Cyber Warfare: A "Nuclear Option"?*

The assessment finds the concerns of leaders like Secretary Panetta regarding cyber war have merit: the United States and other developed countries are ill-prepared to defend against a cyber attack on their critical infrastructure. Yet Krepinevich concludes that the damage inflicted by a major cyber attack would pale in comparison to the devastation of a nuclear strike, while suggesting that a major cyber attack is also far more likely to occur than a nuclear attack. Indeed, he argues that the long-term consequences of such an attack are likely to be in the form of the considerable and enduring cost states will incur in adapting their critical infrastructure to limit the damage from such attacks to an acceptable level.