To this day it remains one of the most sophisticated and mysterious offensive operations ever launched: Stuxnet, the computer virus specifically engineered to attack Iran's nuclear reactors. Discovered in 2010 and now widely believed to be a collaboration between the U.S. and Israel, its existence raised an urgent question: Just what is the U.S. government doing to attack its opponents in the cyber-realm?

Stuxnet's origins have never been officially acknowledged, and the extent of American meddling in malware is still unknown. But for the past few years there’s been something new developing within the U.S. military that has taken "cyber" from a theoretical idea to a deliberate—if secretive—part of U.S. policy.

The first ripple came in January 2013, when the Washington Post reported that the Pentagon was significantly expanding its cybersecurity forces across all the service branches. By that October, the U.S. Army had launched two teams of technical experts dedicated purely to the cyber realm. Just a year later, the number was up to 10.

The growth has been snowballing. Last year, the secretary of the Army created a new branch for cyber—the first new Army branch since Special Forces was created in 1987. By October of this year, there were 32 teams, coordinated out of a new joint force headquarters for cyber opened last year in Fort Gordon, Georgia. By next summer, the Army expects to have 41.

More...