AMERICAN FOREIGN POLICY COUNCIL

SYMPOSIUM: The New Cold War?

December 27, 2012 **Ilan I. Berman** *International Economy*

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Iran; Russia

In late October, speaking at the Intrepid Museum in New York, U.S. Secretary of Defense Leon Panetta delivered a stark warning. The United States, Panetta said, could soon face a mass disruption event of catastrophic proportions, a "cyber Pearl Harbor" of sorts.

"An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches," cautioned the Defense secretary. "They could derail passenger trains, or even more dangerous, derail trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country."

Such a scenario is grim, but it is entirely feasible. The past quarter-century has seen a profound transformation of virtually every aspect of American society as a result of the internet. But with the popularity of the worldwide web has come the proliferation of new threats to U.S. security emanating from it.

Of these, the most prominent is China. The People's Republic has erected a formidable cyber warfare capability over the past decade—one that it has used to carry out espionage against the United States on a massive scale. And if Washington and Beijing ever come to blows (over Taiwan or some other issue), there's good reason to believe that cyberspace would be part of China's strategy of "unrestricted warfare."

Russia is also a distinct cyber danger. In recent years, the Kremlin has exploited cyberspace to decisive effect in its dealings with both Estonia and Georgia, and government-linked cyber activists have helped suppress and silence the country's political opposition. Russian criminal enterprises, meanwhile, have moved online en masse, where they have begun targeting foreign marks—American financial institutions among them.

A newer, and more unpredictable, cyber foe is Iran. Recent attacks on U.S. financial institutions and Middle Eastern energy firms have served notice of the Islamic Republic's growing capabilities in cyberspace. They are also a foretaste of what could happen if the deepening international standoff over Iran's nuclear ambitions results in outright conflict.

Beyond Iran, a range of other actors—from North Korea to al Qaeda—all have demonstrated a growing desire to act, and act aggressively, in cyberspace.

America's response to these challenges is still a work in progress. Movement toward a comprehensive strategy for cyberspace has fallen victim to election-year politics in Congress, where several such plans now languish. U.S. military doctrine, meanwhile, remains ambiguous as to what exactly constitutes an act of war in cyberspace, and what America can and will do in response. U.S. cyber strategy, in the words of one expert, "is akin to where anti-terror efforts found themselves shortly after the attacks of 9/11."

That represents a dangerous deficiency. Warfare of the conventional variety is certainly not a thing of the past. But it's impossible to ignore the fact that cyberspace is emerging as a new domain of conflict—and that America's adversaries are increasingly active in it. Washington needs to be prepared to fight there as well.