2011

The Coming Cyberwar

Arquilla, John

The Coming Cyberwar

The United States is vulnerable. DoD's security policy does nothing to allay the cyber threat.

John Arquilla

July 29, 2011

Despite having had decades to absorb the implications of a range of advances in information technology, the U.S. government remains largely unprepared for cyberwar. A case in point is provided by the Pentagon, which has just released its security policy toward cyberspace. The strategy it sketches out is replete with "initiatives," all of which are long on setting goals but curiously bereft of the means by which they might be attained. Even where there are some signs of the methods to be used, they seem for the most part quaint, rekindling as they do the concepts I remember being bruited about in the early 1990s.

The first initiative, for example, reiterates a two-decades-old point about recognizing cyberspace as an "operational domain." It then embraces the equally hoary organizational mantra aimed at "synchronizing and coordinating" all activities—albeit under the rubric of yet another new military hierarchy, the Cyber Command. Given the balkiness and mixed operating records of other big-line organizations created since 9/11—the Department of Homeland Security and the Directorate of National Intelligence—it is sad to see the Pentagon's failure to seize the opportunity to approach cyber issues in a more networked way. That is, with no central command, but lots of crosstalk and sharing of best practices between the services.

Once the big new organization is up and running, it will have to be defended, which is the subject of the second strategic initiative. This one calls for new concepts but then falls back on traditional notions of "cyber hygiene" (a term used repeatedly) and "hardening" of systems—both of which have been emphasized for at least fifteen years, neither of which has made the defense cybersphere safe from intrusion. Nowhere is this adequately acknowledged, nor is there any mention of how much more secure systems would be if, instead of relying on Maginot Line-like firewalls, widespread employment of very strong encryption—both for data in transit and data "at rest"—were the norm.

Given that much of the military's information systems are highly reliant on commercial products, often from abroad, it is necessary to think in terms of working in conjunction with the private sector and other departments of government to try to ensure "supply-chain security." This is the subject of the third strategic initiative, which gets pretty philosophical about the need to develop "whole-of-government approaches for managing risks associated with the globalization of the information and communications technology sector." Again, this is a chestnut from the 1990s, when every commission looking at cyber security called for such cooperation. The problem is that this call is not a strategy. Rather, it is a symptom of the danger posed by market forces that drive us to seek the lowest cost, with less attention given to the security of the products in question. It is time to remember that even the great prophet of laissez-faire,Adam Smith, called for "free trade in all things save gunpowder and sailcloth," the key military products of the eighteenth century. If he were alive in the twenty-first, he'd no doubt call for great circumspection regarding "microchips and software."

Another aspect of international affairs, working with allies, emerges as the focus of the fourth initiative. Here the Pentagon's proffered solution goes well back before the 1990s, all the way to the beginnings of NATO over sixty years ago, with a call for "collective security." This is the notion that an attack upon one is an attack upon all. It was a powerful idea, one that animated many to join NATO and comforted them in the face of a looming Soviet threat. But it was based on the notion that an attack on one crippled only the one, leaving the strength of others intact to mount the liberating campaign. The problem with collective security in a cyber age is that a serious intrusion into—or attack upon—one ally's information systems could lead to the crippling of the whole alliance. With this in mind, the Pentagon's strategic analysis should contemplate the point that, whatever benefits allies bring—in political and/or military terms—when it comes to cyberspace they now carry very large risks as well.

Whatever might be needed to pursue the first four strategic initiatives, or to mitigate the risks that accompany them, the Pentagon's fifth goal is to solve all difficulties with "rapid technological innovation." The problem here is that such advances may do little to grapple with fundamental organizational challenges. Networks are needed now, not hierarchies. Another gap in Pentagon thinking is that technology itself, no matter how sophisticated—as some cyber weapons are—when not employed in conjunction with a clear-eyed concept of operations, can lead to disaster in the field. The Maginot Line was a marvel of advanced technology—but it couldn't move, a fatal flaw in the age of mechanization. The Line was outflanked in just days by German panzers during the spring of 1940. Pentagon strategy should therefore be focused on seeing how advanced information technology can foster overall doctrinal innovation.

1 2 next › last »

Topics:

CYBER SECURITY
CYBERWAR
DEFENSE
SECURITY

Regions:

UNITED STATES

More stories by:
John Arquilla

Seven Ways a New Cold War with Russia Will Be Different

"Some of the differences would be good for America, some would be bad—and one could be ugly."
Paul J. Saunders

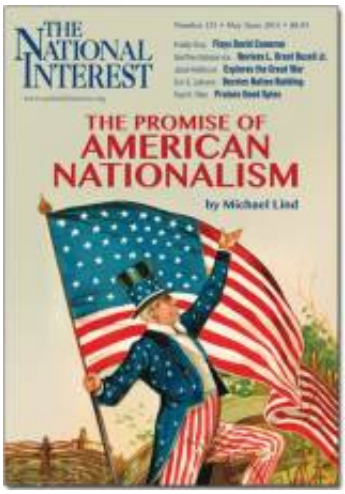
Ukraine and Latvia: Welcome to "The Clash of Civilizations"

"Like Ukraine, Latvia is a cleft country, with ethnic Russians making up nearly 30 percent of the population and the Russian language being the native tongue for nearly 40 percent."
Robert W. Merry

The Case for American Nationalism

Enlightened self interest, rather than grand postnationalist designs, would put the United States back on the path to greatness.
Michael Lind

• Latest Issue •



May-June 2014

Misusing History

Table of Contents

• Most Popular •

Seven Ways a New Cold War with Russia Will Be Different

Welcome to Russian Nuclear Weapons 101

China's Cruise Missiles: Flying Fast Under the Public's Radar

How Germany Could Have Won World War I

Ukraine: Part of America's "Vital Interests"?