It's been a while since we've had a decent cyber-warfare story to tell you about. It's not like there haven't been lots of stories in the news; but nothing has really caught our eye.

Until now.

You know, if you're a long-time reader of this blog, that we don't just confine ourselves to government cost accounting, contract compliance, or even fraud-related stories. We also, from time to time, address new technologies and new development programs that we think might be of interest to our readership. In that vein, we've published several stories about cyber-security, cyber-warfare, and how we think the future of warfare will be less "kinetic" (as they say), and more "cyber." We offer, as but one example, **this story** published about eighteen months ago.

In that story, we told our readers—

We think we are all watching history being made. We believe that 2011 will one day be noted for the beginning of the cyber-wars.

No, we don't think we're being overly alarmist. Just ask Lockheed Martin, or L-3 Communications, or Citigroup, or the IMF. Our website was attacked and wiped-out a few weeks ago—and we had taken the precaution of blocking all IP addresses based in China. (Fortunately, our back-ups worked and we were up and running again within 72 hours.)

We think the U.S. has fallen behind other countries, and parastatial entities, in the strategy and tactics of cyber-warfare. Like the French and their Maginot Line, the U.S. has spent billions on its military assets, without adequately securing the information grid that is the true

backbone of its high-tech military. We think the U.S. military is vulnerable; we think corporate America is vulnerable. And we're pretty sure you are vulnerable as well.

In the past eighteen months the U.S. has taken steps to address what we asserted were deficiencies in its ability to conduct cyber-warfare. We can argue whether those steps are proactive or too-little/too-late reactive, but the fact of the matter is that forward progress is being made—as **this story** over at NextGov demonstrates.

According to the NextGov story, DARPA is "setting up a technology incubator for Defense-funded developers to stitch together computer code to automate offensive cyber operations." The incubator, dubbed the "Collaborative Research Space," will be located in Arlington, VA. (Of course. Why would you want to locate it in Silicon Valley? But we digress.) The goal of the CRS (according to NextGov, who quoted a DARPA solicitation document) is to develop "an end-to-end system that enables the military to understand, plan, and manage cyberwarfare in real-time." This will be the testing ground for "Plan X," according to the story.

The NextGov story provided some light details of "Plan X," reporting—

Plan X, also called 'foundational cyberwarfare,' signals an increasingly aggressive turn in the Defense Department's approach to addressing threats to its networks. The laboratory, a designated Collateral Secret area, is described as a collaborative space for contractors and the military. "DARPA intends to arrange program interaction with a variety of users from DoD and other government agencies, including onsite military personnel who will be testing and using the Plan X system on a daily basis,' contract databases indicate.

Further, NexGov stated—

With algorithms that can help calculate the resources and tools needed to infiltrate networks, assess possible collateral damage from targeting enemy systems, and capabilities to model opponent moves, DARPA hopes that planners will be able to draw up a plans of action more quickly.

Once a cyberwarfare mission plan can be drawn up for an operation, 'the next step is to compile or synthesize the plan into a fully encapsulated executable program or script,' according to the tender. DARPA wants researchers to think about how to build 'automated techniques that allow mission planners to graphically construct detailed and robust plans that can be automatically synthesized into an executable mission script.' While automation could speed up the response time of the military, moves to reduce human control could raise concerns, especially if computer glitches go unchecked.

NextGov also noted—

The initiative comes as the National Cyber Range for Defense personnel to hone computer attack capabilities is slated for a multimillion dollar boost as the system transitions from research laboratories into deployment. President Obama in October signed a secret directive giving the military additional leeway to address computer threats, according to reports.

Okay. This cyber-warfare stuff is getting real. If you are a small business with expertise in these areas (and appropriate clearances) you might want to get the DARPA solicitation and see if you can play in the new CRS sandbox. If you are a U.S. adversary, you might want to think twice about going toe-to-toe with this country, as it appears to be moving quickly to position itself to respond to attack by launching its own cyber counter-attacks.

As has been said before, by many others, we are truly living in the future.