Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland by Anthony H. Cordesman

*By Mark Nance**

"Government is naturally obsessed with itself," writes Anthony Cordesman of the Center for Strategic and International Studies in *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Perhaps it is an understatement, but one borne out nonetheless by dozens of pages quoting "findings" and "recommendations" by numerous federal organizations empanelled to sort out the nation's critical infrastructure vulnerabilities. The fact that the author devotes only a one-page chapter to the role of local and state governments, and only two pages to Chapter 7, *Role of Private Industry* is telling. Without a doubt there are areas where the federal government will play first (and only) chair in cyberwarfare and defense, but the feds will not find the resources to maintain superiority by looking inward. Much of the excerpted testimony and quoted government-speak in *Cyber-Threats* seems to fall in the category of bureaucratic navel gazing. That is not to say that valid points are not made, it is more to say that the same points seem to get made year after year in study after study.

Professor Cordesman provides a valuable digest of both obvious and not so obvious issues in his *Conclusions and Recommendations*, where he advises that:

> There is no practical way that the federal government will ever develop the technical skills, and overcome its lack of specialized competence in ways that enable it to defend the vast majority of physical nodes in America's critical infrastructure or critical e-commerce, computer, and information systems. In fact, 90% of the burden of the day-to-day defense must fall on the private user or corporation.

In this passage, the author is attempting to distinguish between *cybercrime* and *cyberwarfare*, which given what we have learned about al Qaeda since September 11, seems like a somewhat academic exercise, notwithstanding the obvious questions of degree with respect to cybercrimes. Asymmetric warfare, such as that likely to be waged against the U.S. in the near future**,** presents more of a Potter Stewart "know it when I see it" definition rather than a neat taxonomy. The importance of this sort of flexibility further highlights the value of active participation by the private sector and local governments. Professor Cordesman is also critical of the federal government's apparent myopic focus on defensive capabilities, especially solely technical solutions such as firewalls, versus a more complete orientation that includes offensive capabilities combined with an integrated defensive posture.

Notably missing from the book is a discussion of the role and capabilities of domestic U.S. intelligence and law enforcement agencies, principally, the FBI. Current and former federal law enforcement officials report that they are somewhere between 8 and 10 years behind private sector technology capabilities. In terms of remediation, the press reports that the FBI is now buying new PCs, and reassigning personnel from garden-variety criminal cases to work on national security issues—things that might properly have been done some time ago (but the federalization of the criminal code is another issue). The FBI is composed largely of intelligent and motivated agents. Unfortunately, it does not yet appear that all of them have been convinced of the gaping holes in their computer and data competencies. This ramp up in technology apexed in the private sector around Y2K with the purchase of some rather questionable systems and solutions. Today's corporate consumer is pretty sophisticated and unlikely to buy much in the way of snake oil.

The networked computer has (or should have) supplanted the firearm as law enforcements' primary non-organic tool. Accordingly, technical and personnel proficiency at all levels of computer and network security are vital so that personnel are able efficiently to use the vast assets that should be made available to them for national security and other criminal investigative purposes. Like any other large bureaucracy, there are members of the FBI and other agencies who are content to remain blissfully ignorant of the state of the art. We should no more tolerate outdated professional skills in our federal law enforcement ranks than we do in our physicians or military leaders.

Cyber-Threats provides a quick tour through some of the executive and legislative history surrounding critical infrastructure defense issues as a well as a brief look at the threat (as seen through the eyes of policy makers). Its target audience is wonks not technology professionals. Perhaps the best reading in the book is to be found in the final chapter where Professor Cordesman proposes thirty recommendations to improve U.S. capabilities in cyberwarfare and defense, which should alleviate the need for any more blue-ribbon panels. In the final analysis, however, the book would be well-served by additional attention to the private sector and local government contributions, especially where industries such as financial services have invested so heavily in effective counter-measures.

* Mark Nance has served as General Counsel to two technology companies, and has a background in military communications.