Cato scholar blazes path of cyber-sanity

The Underwhelming Threat of Cyberterrorism

In 1983, Americans watched as Matthew Broderick, armed with only a personal computer, brought the world to its knees. In the popular movie *WarGames*, Broderick played a young hacker who broke into the military's electronic network and nearly started World War III. In recent years, as fear of terrorism continues to overwhelm rational threat assessment, the *WarGames* scenario looks a lot like what so-called cybersecurity experts and their federal government allies tout.

The problem with "cybersecurity," says Jim Harper, director of information policy studies at the Cato Institute, is that we're convincing ourselves that cyberspace is an endless sea of vulnerabilities that leave us weak and exposed. It's not. Harper has emerged as the voice of reason among breathless news reports of "cyber attacks" and calls for Washington to take over security of the nation's computing infrastructure. In his papers, congressional testimonies, and numerous media appearances, Harper emphasizes the need to better understand the nature of cyberspace, to appreciate the improvements in cybersecurity civil society is constantly generating, and to recognize the near impossibility that terrorists might inflict significant harm using computers.

"It's helpful to imagine 'cyberspace' as organized like the physical world," Harper says. "Think of personal computers as people's homes. Their attachments to the network analogize to driveways, which connect to roads and then highways. E-mails, financial files, and pictures are the personal possessions that could be stolen out of houses and private vehicles, leading to privacy loss."

Cyberspace will be secured the way real space is. Computer owners, like homeowners and businesses, should be the first line of protection for their own property, Harper says. They should install the latest patches and place their systems behind firewalls. What the government wants—to come up with a national cybersecurity plan and force it upon network, data, and computer owners—is akin to cutting down crime in neighborhoods by stationing police officers in livingrooms and dictating what sorts of door locks and alarm systems must be in all new homes.

"The analogy between cyberspace and real space shows that 'cybersecurity' is not a small universe of problems, but thousands of different problems that will be handled in thousands of different ways by millions of people," Harper says.

This analogy is particularly important when the topic shifts from broad "cybersecurity" to the narrower threat of "cyberterrorism." The popular view of such attacks, like *WarGames*, is nonsense, according to Harper. "With communications networks, computing infrastructure, and data stores under regular attack from a variety of quarters—and regularly strengthening to meet them—it is highly unlikely that terrorists can pull off a cybersecurity event disruptive enough to instill widespread fear of further disruption," Harper says. If they could do it at all, taking down websites, interrupting financial networks, or knocking out power systems does not terrorize. In a 2009 speech about cybersecurity, President Obama spoke about "weapons of mass disruption," a poor relation of the instruments that truly threaten violence and chaos.

The federal government plays a significant role in protecting Americans from genuine terrorism. And, even though the threat of cyberterrorism is dramatically overblown, the government can improve security in that area, too. But it should not do so through regulation, Harper says. Instead, it can take advantage of its position as a large purchaser of information technology and, through the market, guide technology producers to meet better security standards.

The politicians in Washington should realize that the easiest way to protect critical data and infrastructure is not to make it vulnerable in the first place. "Where security is truly at a premium," Harper says, "the lion's share of securing infrastructure against cyberattack can be achieved by the simple policy of fully decoupling it from the Internet."

JIM HARPER, director of information policy studies at the Cato Institute, has been a consistent voice of reason in the debate over cyberterrorism and computer security.

Harper's level-headedness is getting attention. The Obama White House cited a paper he wrote in the executive summary of its *Cyberspace Policy Review*. In it, Harper argued that updating tort law to allow those harmed by insecure computer products to recover damages from providers and manufacturers is a better path to true security than government regulation of the market. And he was called before the House Subcommittee on Technology and Innovation to testify about how the federal government should respond to cyberterrorist threats and how it should approach securing the nation's information-technology infrastructure.

Harper is adamantly clear that cybersecurity is important. While arguing that the federal government should not directly regulate computer security, he is careful not to downplay the need to secure our computer networks. But such security, like in the brick-and-mortar world outside the Internet, is a matter of personal responsibility, business interest, and common sense.

That same common sense should lead us to recognize that cyberterrorism does not exist and that threat of cyberwarfare is minimal. Claims to the contrary result from technological illiteracy and the incentives of government officials and contractors that favor inflating threats.

Cyberterrorism is "cyber–snake oil," Harper says. ■