What Americans should fear in cyberspace

January 24 2014

A recent Pew poll found that Americans are more afraid of a cyber attack than they are of Iranian nuclear weapons, the rise of China or climate change. Such fears are not only out of proportion to risk; if they take hold, they could threaten the positive gains of the digital age.

Certainly there are growing threats in the cyber world, and the stakes are high. But there is also a high level of misinformation and plain old ignorance driving the fear. Despite the Internet now enabling us to run down the answers to almost any question, a number of myths have emerged about online security and what it means for us offline. The result is that some threats are overblown and overreacted to, while other quite legitimate ones are ignored.

Every computer user has had to make cyber-security decisions: whether to trust online vendors with credit card information and how often to change an email password, to name two. But these decisions are too often based on scant understanding.

The problem is even more acute in business and government. Some 70 percent of executives have made a cyber-security decision of some sort for their firms. Yet MBA programs still aren't routinely teaching cyber security as part of normal management responsibility, nor do the schools that train diplomats, lawyers, generals, journalists and others who have to make important decisions in this regard every day. Whether in the boardroom or the White House situation room, crucial matters are often handed off to so-called experts, which is a good way to be taken advantage of - and to feel more secure than you actually are.

Instead of focusing on what we need to learn, we've instead fed on hype that fuels fears but doesn't solve problems. For instance, Americans have repeatedly been told by government leaders and media pundits that cyber attacks are like weapons of mass destruction and that we are in a sort of Cold War of cyberspace.

But the zeros and ones of malware are nothing like the physics of nuclear weapons, nor are the political dynamics they fuel. Moreover, the globalized network in which the NSA, Chinese hackers, Anonymous, Google, Target and you and I all play is hardly the kind of bipolar world that spawned the Cold War.

There is certainly a battle of ideas online, but it's as likely to focus on which boy Katniss of "The Hunger Games" should choose in the end (Peeta, of course) as it is to focus on competing political visions. Rather than looking to the Dr. Strangelove era of the Cold War for inspiration, we'd be better off studying other historical lessons, focusing on how the government has effectively approached other new problems areas, from how the seas were made safe to the success story of the Centers for Disease Control and Prevention in public health.

Despite its central position in both congressional testimony and Hollywood movies, no person has actually been hurt or killed by an act of cyber terrorism. Indeed, squirrels have taken down power grids, but hackers never have. But that is not to say there's no threat. Indeed, our own creation, the Stuxnet worm, which attacked Iran's nuclear infrastructure, demonstrated that cyber weapons can cause damage.

But the fiction of a "cyber Pearl Harbor" gets far more attention than the real, and arguably far greater, impact of the massive campaign of intellectual property theft emanating from China. As with 9/11, the way that we react (or overreact) to an attack, terrorist or otherwise, is what truly determines the impact of it. Understanding the difference between

hackers doing something annoying and doing something with the capacity to cause serious harm will better direct our fears and resources.

Cyber security has to be seen as an management problem that will never go away. As long as we use the Internet, there will be cyber risks. The key is to move away from a mentality of seeking silver bullets and ever-higher walls and instead to focus on the most important feature of true cyber security: resilience. In both the real and online worlds, we can't stop or deter all bad things, but we can plan for and deal with them.

In treating cyber security as a matter only for IT experts, computer users often neglect the most basic precautions that go a long way toward protecting both the Internet's users and the network itself. Indeed, one study found that as much as 94 percent of attacks could be stopped with basic "cyber hygiene." Perhaps the best example is that the most popular password in use today is "123456," with "password" No. 2.

The 19th century poet Ralph Waldo Emerson never could have conceived of the Internet. But it is what allowed me recently to look up a quote by him that is perhaps the best guide for our age of cyber insecurity: "Knowledge is the antidote to fear."

More information: P.W. Singer is director of the Center for 21st Century Security and Intelligence at the Brookings Institution and co-author of "Cybersecurity and Cyberwar: What Everyone Needs to Know." He wrote this for the Los Angeles Times.