2009

Click, click... counting down to Cyber 9/11

Arquilla, John

Click, click {hellip} counting down to Cyber 9/11

John Arquilla
Published 4:00 am, Sunday, July 26, 2009

When it comes to national security, our leaders are overly focused on nuclear weapons of mass destruction; more thought should be given to the looming threat of cyber "mass disruption."

Yes, Russia has lots of warheads, but so do we. The situation is stable. North Korea might have a few big weapons that work, but our retaliatory capability would wipe them out. The same would hold for the Iranians, should they ever get the bomb.

But in the virtual world of debilitating logic bombs, fast-spreading viruses and remotely controlled "botnets" of thousands of slave computers, a grave and growing capacity for crippling our tech-dependent society has risen unchecked. And all the warning signs have been evident for years.

A decade ago, one of our own military exercises - still classified, so little can be said openly - revealed serious vulnerabilities. This was soon followed by actual intrusions into our defense information systems, apparently emanating from a site in Russia, that were persistent and wide-ranging.

More exercises followed, to test new security standards, with names like Silent Horizon and Cyber Storm. They showed that we were still quite open to attacks against crucial infrastructures. And more real events came into play - this time apparently connected in some way to China: a swarm attack that nearly took down the power grid in Southern California several years ago and, more recently, another series of cyber raids on sensitive military data.

Beyond our own direct experiences - the latest being some relatively minor attacks on the Fourth of July that also hit South Korea - others also have started to feel the cyber heat. Estonia came under cyber attacks in April and May 2007, and so did Georgia in August 2008. Both apparently were staged from Russian and other servers, and the effects were so serious that Estonia had to reboot by cutting its cyber links to the outside world. The Georgians lost the ability to communicate with their own armed forces - in the middle of a Russian invasion.

And the Russians are hardly alone in waging this sort of cyber-war. Israeli ground forces dealt punishing blows to the Palestinians in Gaza in the January 2009 fighting, but a Muslim cyber-militia, apparently operating out of Iran, struck back effectively against a number of key Israeli sites - including one that provided civil defense instructions for what to do when under rocket attack.

These cyber attacks were on smaller countries, but if such actions were aimed at us, they would be exceptionally costly. That makes it most puzzling that so little has been done that actually improves our defenses.

To be sure, a whole business model based on selling firewalls and security updates has emerged. But, as one master hacker I know likes to say, "There are no firewalls. They only recognize what they already know to be threats and have great trouble when intrusion and attack tools are even slightly tweaked."

Or, as I like to tell my military masters, we are steeped in a Maginot Line mentality - our cyber defenses are as easy to outflank as the French fortifications were in 1940. Instead, we have to "imagine no lines" and accept that the bad guys will get into our systems.

Against this threat, we must rely more on strong encryption - so intruders won't even know what they're looking at - and conceal our most important information by parceling it out in encoded portions in myriad hiding places in "the cloud" of cyberspace.

Commercial companies are just starting to take steps like these. But their pace of change is far too slow, and their intellectual property continues to be plundered by cyber raiders. Individuals are even more vulnerable - millions of Americans are unknowingly turned into zombies, their computers enslaved by virtual body snatchers. And our military, whose efficiency depends on secure connectivity, remains at risk.

In the face of all this, we must of course strive to reduce vulnerabilities. But there is one other thing we might do: engage in cyber arms control. Not the sort that seeks to prevent the spread of technology, because this cannot be done. All computers can be used as weapons, and they are everywhere. So instead of trying to control hardware, we have to strive to control our own behavior.

Perhaps this would take the form of a multilateral agreement to refrain from intruding into or attacking others' information systems except in response to acts or imminent threats of virtual or physical aggression. Ironically, it was the Russians - now so adept in cyberspace - who first floated this idea 13 years ago in a meeting with their American counterparts.

When the Russian position was communicated to higher-ups in the U.S. government, the response was negative. I know because I was part of the American team, and I urged acceptance of the Russian offer. But the prevailing view was that Moscow's offer was a sign that we were ahead - and should keep ahead, not give up an advantage. So a cyber arms race arose, like the nuclear arms race that ensued after the United States refused to join a global ban on nuclear weapons about 60 years ago.

All the evidence to date suggests that we are not ahead in this race. In fact, our open society provides the biggest and richest set of targets in the world. Yet we continue to oppose a behavior-based form of cyber arms control that might look something like the Chemical Weapons Convention - one of the world's great successes in renouncing the use of terrible weapons that almost anyone can easily produce.

Yet there is still time - just barely - to act. We must begin by moving away from cyber defense strategies that just don't work, and then we should embrace a behavior-based arms control effort. The alternative will be, inevitably, a cyber 9/11 that could have dire consequences for the economy or for our troops in the field if they are engaged in battle when the digital storm hits.

If such an attack does come, no commission will be able to conclude that it could not have been foreseen. The portents have been there for all to see. There can be no excuse for failure to take action now.