

“Cybersecurity: Next Steps to Protect Critical Infrastructure.”

February 23, 2010

Senate Commerce Committee

James A. Lewis, Center for Strategic and International Studies

Cybersecurity has become an important issue over the last decade as the internet changed from being a collection of auxiliary devices to become a significant global infrastructure. The U.S. in particular has woven computer networks into so many of its economic activities that we are as reliant on the internet as we are on any other critical infrastructure. Networked activities can be cheaper and more efficient, so companies large and small have migrated to the internet because it can provide competitive advantage. The U.S. has also moved to a reliance on networks to give it military advantage. The internet, digital devices, and networks reinforced existing trends in military the realization that intangible factors – greater knowledge, faster decision making increased certainty – would increase effectiveness more than additional tanks or airplanes. Networked forces have an advantage.

This dependence has brought growth and greater efficiency in business, research and government. The U.S. in particular has woven computer networks into so many of its economic activities that we are perhaps more reliant on the internet than any other nation. Networked activities can be cheaper and more efficient, so companies large and small have migrated to the internet because it can provide competitive advantage. The U.S. relies on networks to give it military advantage. Digital devices, and networks reinforced existing trends in military thinking on the importance of intangible factors – greater knowledge, faster decision-making, and increased certainty – would increase the effectiveness of military force.

That the technologies designed in the early 1970s have worked so well and have so cleanly scaled to support more than a billion users is an amazing triumph, but anyone with malicious intent can easily exploit these networks. The internet was not designed to be a global infrastructure upon which hundreds of millions of people would depend. It was never designed to be secure. The early architects and thinkers of cyberspace in the first flush of commercialization downplayed the role of government. The vision was that cyberspace would be a global commons led and shaped by private action, where a self-organizing community could invent and create. This ideology of a self-organizing global commons has shaped internet architecture and policy, but we must now recognize its inadequacy.

There are two reasons for this inadequacy. First, private efforts to secure networks will be always be overwhelmed by professional military and criminal action. The private sector does not have the capability to defeat an advanced opponent like the SRV or the PLA, organizations that invest hundreds of millions of dollars and employ thousands of people to defeat any defense. We do not expect airlines to defend our airspace against MiGs and we should not expect private companies to defend cyberspace against foreign governments.

Second, absent government intervention, security may be unachievable. Two ideas borrowed from economics help explain this - public goods and market failure. Public goods are those that benefit all of society but whose returns are difficult for any individual to capture – basic research is an example of a public good. Adam Smith, the intellectual father of market capitalism in the

Wealth of Nations, identified highways, insane asylums and national defense – and the internet combines element of all three - as public goods that the private sector would never adequately fund. Cybersecurity is a public good that the market has failed to produce in sufficient quantities.

Like other new technologies in the past – airplanes, cars, steam engines – the appeal and the benefits are so great that we have rushed to adopt the internet despite serious safety problems. These problems are amplified by the global connectivity of the new infrastructure, as the speed of internet connections means that geographical distance provides little in the way of protection. For those earlier technologies, safety came about through innovation driven by government mandates, and by agreements among nations. The same process of maturation is necessary to secure cyberspace, but this will require shedding some of our old ideas about its nature.

Important step for increasing reliability of system we now depend on

Similar to other episodes – cars. Electricity phones, where a new public utility

Some important differences – global, embedded in many devices

What incentives to get people and companies to adopt best practices and safer technology

What steps to come up with agreements and rule with other states.

Criticism you will hear

Not a perfect solution- const says more perfect, not perfect

Can't measure or certify. This may explain why we are in such mess

Starting to collect data that lets us see what works and what doesn't

Let market fix it. Wrote this one myself in 1996, stil waiting

Don't get in way of innovation- requiring safer cars didn't kill innovation or we'd still all be driving 1956 de sotos

Private sector can do. Airlines against Migs

Why so hard

