Cyber Insecurity: Dealing Effectively with the Greatest Threat To Global Economic Development in the 21st Century

Steven S. Myers

November 5, 2012

In October of this year a sobering example of the power of cyber intrusion was demonstrated by a low level employee of Aramco, the world's largest oil company. In a matter of moments he destroyed the hard drives on some 55,000 computers and erased all of their data with a viral mix of off-the-shelf software and downloads from hacker sites provided to him by Iran. The economic consequences of his actions will likely never be revealed, but must be staggering.

Cyber crime, cyber terrorism, and cyber attacks are the result of successful intrusions into computers and networks. Intrusion may be aimed at stealing military secrets and technology, disrupting military command and control capabilities, or taking over the remote operations of another country's military capabilities. Intrusion may also be about financial theft, fraud, or trespassing into national critical infrastructures. It may be about stealing trade secrets and intellectual property. Or, it may be about the physical destruction of public and private property. Motivations can range from simple mischief to economic gain, revenge or extortion, state sponsored terrorism, and even war. The world has experienced all of these variations in recent years with alarming frequency and potency.

Governments recognize that adequately protecting their cyber environment is critical to defending their economies. What is most challenging is reaching consensus on how best to do it. An internationally sanctioned, coordinated cyber strategy is essential to developing, and then implementing effective cyber security around the world. But, the attendant technical, social and political issues involved are complex and daunting.

First, because the cyber environment is so complex it is difficult for most people to understand it. It is a "medieval" landscape in which the vast majority of businesses are much like families of cyber serfs living in mud huts, perhaps as part of collectives surrounded by wooden fences. Large companies and most governments are more like fiefdoms with defenses that are more difficult to penetrate, but not insurmountable. Walls, moats, gates, guards, and significant resources dedicated to the protection of their enterprises create more challenging barriers. But, even these efforts are no match for the increasing rate of penetrations by ever more sophisticated intruders.

Second, there are no existing, credible law enforcement mechanisms or cyber police forces to protect most civil government functions or businesses, large and small, around the world from state sponsored raiders, terrorists, roving gangs of marauders and lone wolf hackers with nefarious intentions. The US and NATO military allies are doing better in addressing cyber warfare threats, primarily because they are more focused on the problem with significant resources, and because they plan for offense, not just defense.

By far the most serious obstacle is political partisanship. The unsuccessful effort this summer by the U.S. Congress to pass a comprehensive cyber security bill would have been an important step forward. Yet, those that have successfully opposed the bill are working unwittingly against the very interests they believe they are protecting.

The numbers are getting worse – dramatically worse. In 2011 U.S. cyber emergency response teams received 106,000 incident reports from Federal agencies, critical infrastructure, and industry partners, and are already up over 35% for this year.

So then what can we do about it? The situation we face in cyber security is not unlike the one we faced in air travel in the 1930's. The Federal Aviation Administration (FAA) and its European counterparts had the foresight and courage to put in place the regulatory foundation needed to promote long-term aviation reliability and safety through certification standards for aircraft, the crews that operate them, and the air and ground infrastructure that they operate within.

Imagine what the impact to global commerce would have been if airplanes had routinely fallen out of the sky, or crashed because of incompatible equipment or miscommunications? People would have very quickly stopped flying. By 1947, the International Civil Aviation Organization (ICAO) was ratified as a special agency of the United Nations. Its mission was to ensure that every country wanting aircraft from foreign countries to come into their airspace, or any of their country aircraft flying into foreign countries would meet an internationally accepted set of standards. As a consequence aviation became one of the pillars of global economic growth in the 20th Century.

This monumental achievement was not accomplished through coercion, or presuming to impose regulatory requirements on other countries. To take advantage of the economic benefits of international aviation commerce, countries applying for membership in ICAO had to prove that they conformed to the standards set by ICAO. That is why air traffic controllers everywhere speak English and why entry and exit processes and security procedures look pretty much the same worldwide.

Cyber has become the comparable driver for global economic growth in this century. This can only continue if the medieval landscape that characterizes the cyber world gives way to a sustainable environment that ensures ever better cyber security. The US and the EU together must lead the effort to accomplish this. The ICAO model is a great starting point.

Steven Myers is a member of the U.S. Department of Homeland Security Task Force on Cyber Resources, and the U.S. State Department Advisory Committee on International Economic Policy. He is a four-time serial entrepreneur and an Ernst & Young “Entrepreneur of the Year”. Myers graduated from Stanford University, is a two-time Air Force veteran, and pilot with 5,600 hours of flight time and ten jet type ratings.