New American

Written by Kurt Hyde on March 9, 2012

Is America Vulnerable to an E-Attack?

Frequently, the most important news items are not those that make the front page, but rather those details that are, when reported at all, relegated to the back pages. The November 22, 2011 Presidential Debate may be an example of this. The final question asked of the Republican presidential candidates that evening was posed by Mark Teese, a visiting fellow at the American Enterprise Institute. Unfortunately, there has been very little follow-up on this topic at the subsequent Presidential Debates.

Teese prefaced his November 22nd question by noting that in 2000, Candidate George W. Bush was never asked about al-Qaeda, but once he was in office that's what dominated his presidency. Teese's question to each of the candidates was:

> What national security issue do you worry about that nobody is asking about, either here or in any of the debates so far?

The most mentioned topic by the candidates, three of them, was the threat of an electronic attack, also known as an E-attack. That is an attack on our country by turning our computers and other electronic devices into weapons against us rather than being the helpers we have come to rely on. Texas Governor Rick Perry specifically referred to China's military capabilities in cyber warfare, which some experts believe is superior to ours. Former Federal Reserve banker Herman Cain used the term cyber attacks. Former Speaker of the House Newt Gingrich mentioned two forms of attacks on our computer systems, an electromagnetic pulse attack that would attack our computers at the hardware level and a cyber attack.

An E-attack can take many forms. It can be in the form of planting malware in business or personal computers. It could be false signals to computer-controlled equipment thereby causing damage to the equipment itself or other equipment affected by it. It can also cause the equipment to malfunction to the point of becoming a threat of injury or death to people. It could be false information being fed into financial databases or destruction of data within those databases. Either of those would wreak havoc within our economy. An E-attack could also include shutting down all or part of the Internet as well as mobile phone usage. The Internet or mobile phone shutdowns could be accomplished by the attackers or done by the government in response to the E-attack in a manner similar to how the Egyptian government reacted in January of 2011.

Many computer experts have been warning for years that we are vulnerable to an E-attack and it could have serious consequences. Many companies are inadequately prepared for anything worse than a temporary unavailability of the Internet. If an E-attack crippled America's computer systems for an extended time, many dairy products and other perishables would spoil rather than be delivered for lack of computerized instructions for transporters. Credit cards are dependent on computers to authorize purchases, so only cash or barter would be useful in trade. The long-term economic effects could be devastating to the American middle class as many companies could declare bankruptcy and cancel the companies' shares on the stock market. This would greatly reduce or even wipe out many 401(k)s and other retirement accounts. Of course, the executives of the companies could replace their stock losses by awarding shares to themselves as part of their compensation packages as the companies emerge from bankruptcy proceedings and restart with new shares.

The number of American deaths in an E-attack could easily eclipse the number of people killed on September 11, 2001. For example, many cars have the ability to be started remotely. If an enemy cyber warrior obtains the required access to electronically emulate cars' owners, he could start many cars while they are parked in people's garages, thereby causing many deaths across the nation due to carbon monoxide poisoning in their homes. Even though carbon monoxide emissions have been greatly reduced in recent years, the risk still exists, especially if there are multiple vehicles in an enclosed space or if the emissions equipment malfunctions and additional carbon monoxide might be emitted. Additional motor vehicle deaths could be caused by disruption of traffic signals on our nation's roads. If transportation of food is disrupted, there would be food riots and certainly many people would die in them. These examples barely scratch the surface of the many deaths that could be caused directly or indirectly as a result of a well-coordinated, nation-wide E-attack on America.

While Governor Perry, Mr. Cain, and Speaker Gingrich deserve kudos for their awareness of the existence and significance of this threat, not one of them mentioned the role played by our federal government in making our computer systems more vulnerable than they ought to be. Also, not one of them mentioned what they would do to obey the U.S. Constitution and otherwise preserve independence and freedom for Americans during their responses to a terrorist E-attack if one should occur.

Federal Involvement That Has Increased The Risk Of An E-Attack:

Today, computers are connected with each other almost universally via the Internet, which is largely an outgrowth of the ARPANET. ARPANET was developed largely by grants from the federal government's Advanced Research Projects Agency, also known as ARPA. ARPA was started under the Eisenhower administration in 1958 during the emotional reaction to *Sputnik*. There were other computer networking technologies that were being developed in the private sector and many of them were inherently more secure, but the government-sponsored technologies became the de facto standard largely because so many government agencies adopted them. If we had just obeyed the U.S. Constitution and left the development of this technology to the private sector we'd have fewer security weaknesses in the environment for connecting computers and sharing data than we do today.

Immigration is another way in which the federal government is increasing our risk to an E-attack. At the same time we claim we are concerned about potential terrorist attacks on our computer systems, the federal government grants visas to people from nations that are high-risk for exporting terrorists to work in our country.

Consider Huda Salih Mahdi Ammash, also known as Mrs. Anthrax or Chemical Sally. She got another nickname, Five of Hearts, because she was one of the 52 people pictured on playing cards designed by the U.S. military to be carried by the soldiers enabling them to remember high priority persons to be captured in Iraq. According to the Wikipedia, she has college degrees from Texas Woman's University and the University of Missouri. While she isn't a computer specialist, her story is indicative of the ease with which people from countries like Iraq, which has been on and off the list of terrorist exporting nations a number of times, come into our country legally. The vast numbers who come here illegally also increase the terrorist threat.

Affirmative action is another way in which the federal government makes America more vulnerable to terrorist attacks. Consider the case of Midal Malik Hasan, the Army major who is the suspect in the Fort Hood shooting incident. He was eligible for preferential treatment under affirmative action. Government agencies at all levels are notorious for their aggressive use of affirmative action in hiring, training, and promotion. Foreigners, including those from nations that are high-risk for exporting terrorist, are frequently given preference in hiring over Americans because of affirmative action programs.

Once hired, either directly or indirectly by American companies or for government jobs, many foreign companies or people from foreign countries get privileged accounts to computer systems that are vital to our economy or emergency services. They then have the level of access needed to aid and abet an E-attack on our country, such as helping to plant malware software or simply by leaving trap doors available for enemy cyber warriors to gain access to our computers at a later date.

What Will Be Worse — The Action Or The Reaction?

Sometimes the biggest danger to a terrorist attack is not the attack itself, but the response to it. While none of the candidates had time to explain what they would do as President if such an attack were to occur, Mr. Gingrich's response included a very frightening statement that in his opinion such an attack would be "outside the current capacity of our system to deal with."

Recent attempts to implement unconstitutional federal controls over the Internet, such as SOPA (Stop Online Piracy Act) and PIPA (Protect IP Act) have thankfully failed in Congress. But a quick glance at history shows that unconstitutional legislation frequently passes during the aftermath of a major catastrophe.

We must not allow an E-attack to become an excuse for the federal government to take control over the Internet. That would be very tempting considering how many advocates for constitutional reforms rely on the Internet. For example, when former Miss USA Susie Castillo was molested in the name of security at DFW Airport, she pleaded her case directly to the American people and started her TSA Petition to Congress via the Internet. Many conservative news sources as well as non-conservative news sources abound on the Internet where they exercise their rights to free expression. While we may agree with some and disagree with others, we must agree that our rights to free expression are protected only as long as the rights of those who disagree with us are protected also.

What Should We Do?

The first thing we need to do is to admit what we've done wrong. The federal government needs to issue a warning that the threat of an E-attack is real and companies should be prepared with backup plans for doing business in case of an E-attack. Because federal, state and local governments have become huge customers of many businesses, these government entities need to acknowledge that their customers and suppliers may want to migrate over time to other technologies for computer connectivity and be prepared to support the different technologies that may develop. This is especially critical in the areas of order entry and payments.

We must repeal our affirmative action laws. They are not reverse discrimination. They are a form of discrimination. They hurt American companies' competitiveness and, therefore the American economy as a whole, when companies can't hire the best qualified people for a job and are required to hire someone else instead. They are also an avenue by which high risk people, such as Major Midal Malik Hasan, can sometimes get preferential treatment in hiring, training and promotions.

We must shut down the unconstitutional Emergency Alert System (EAS). The first national test of The Emergency Alert System was on Wednesday, November 9th, 2011. According to the press release announcing this test, posted on June 9, 2011 by the FCC Federal Communications Commission) and FEMA (Federal Emergency Management Agency), "The EAS is a national alert and warning system established to enable the President of the United States to address the American public during emergencies." This federal power is not only unconstitutional, it's too much of a temptation for any President to welcome a nationwide Internet or mobile phone shutdown as the EAS could easily become a vehicle to give the President a monopoly over electronic communication with the American people.

Our military services are making preparations for response to an E-attack. We must be careful to limit the scope of our military response to an E-attack to defending our military and other government computers and to giving advice to those who need it to recover from such an E-attack.

The good news is that Newt Gingrich is wrong. It is not outside our current capabilities to defend ourselves from an E-attack. We can do so without violating the U.S. Constitution, but the time to prepare for it is now and let's start by eliminating the governmental involvement, especially at the federal level, that is increasing the risk.