Increased Cyber Security Threat Represents Opportunity for International Defense Cooperation

By Van D. Hipp, Jr.

The increased threat from cyberspace, as well as the possibility of a biological attack, consistently rank as the top two Homeland Security threats facing the United States today. Depending on who you talk to and the current threat assessment, these two go back and forth as the number one threat facing the country.

Fortunately, several nations friendly to the United States have had a great deal of experience in combating the cyber threat long before it became a major threat here at home. Recent indications are that both the North Atlantic Treaty Organization (NATO), as well as certain parts of the U.S. Government, have gotten the message and are working more closely with allies, and implementing new and promising cyber security technologies from friendly countries in order to combat the ever-growing cyber threat. This is welcomed news and should, hopefully, pave the way for increased international defense cooperation among the United States and our allies.

Since 9-11, the unmanned aerial vehicle (UAV) has been one of the United States' most effective tools in combating terrorism. Unfortunately, the threat from cyberspace has found its way into the UAV realm and has posed major challenges. Specifically, the revelation that al Qaeda hackers have been able to "see" what our drone aircraft were viewing while over Afghanistan and Pakistan underscored the need to urgently strengthen our cyberspace defenses.

Hacking for intelligence-gathering purposes has been done often by Chinese sources, as well as by operatives of other governments. The U.S. Government works steadily to thwart these activities. The greater threat is that a hostile breach of our cyber defenses could, in the future, lead to disruption of our electrical grid and computerized financial system, not to mention wreak havoc with our military efforts.

After a Chinese cyber attack in Summer 2007, then-President Bush signed an Executive Order establishing the Comprehensive National Cybersecurity Initiative (CNCI). This put the Department of Homeland Security in charge of better protecting our network systems from cyber attack. It established an around-the-clock watch-and-warning center for the Federal Government's Internet infrastructure.

It also established the EINSTEIN program to identify unusual network traffic patterns and trends which signal unauthorized traffic so that security personnel may quickly identify and respond to potential threats.

These programs are strong steps in the right direction; however, it is essential to our global security that we continue to strengthen our cyber defense perimeter. Along these lines, it is vital that the U.S. Government reach out to our allies and friends across the Atlantic who have great expertise and many more years of experience in dealing with very real cyber security threats.

Cyber attacks have had serious consequences in recent years. In Spring 2007, such an attack on Estonia blocked websites and paralyzed the small country's entire Internet infrastructure. Bank cards and mobile phone networks were out temporarily. The attack came at a time when the Estonian Government was in a dispute with Russia over the removal of a Soviet-era war memorial in Estonia's capital, Tallinn. The Estonian Ministry of Defense was convinced the cyber attack was the work of agents of the Russian Government because it was too well coordinated to be the work of a lone hacker.

In August 2007, shortly before Russian army forces entered the Republic of Georgia, the latter's entire government computer system was inexplicably shut down. As a result, in May 2008, NATO established the Cooperative Cyber Defense Center of Excellence (CCDCOE) in order to expand its cyber defense capability. Based in Tallinn, the CCDCOE acts as coordinator of cyber defense initiatives and advances between NATO members and partners. Consequently, some of the best IT (information technology) and cyber technology, including counter measures, emanates from the Baltic region.

The establishment of the CCDCOE presents our nation with an opportunity to benefit from the work being done there. The U.S. should play a more significant role than it has with the CCDCOE in order to take advantage of "lessons learned" and of new cyber security technology and developments.

Recently, the NATO's CCDCOE has begun using a proactive Finnish cyber security tool known as "Defensics" from the company Codenomicon, in order to combat the ever-increasing cyber threat. The Codenomicon "Defensics" technology is sort of like a "hacker on steroids" and is able to proactively discover unknown vulnerabilities before they can potentially impact a critical military mission.

Currently, the greatest software security challenge is the discovery and remediation of unknown vulnerabilities before they can potentially impact operations. In an era of state-supported cyber warfare, growing shares of vulnerabilities are never disclosed publicly. Instead, they are sold and/or distributed within underground hacker communities to further the supporting state's agenda.

The United States and its allies can no longer afford to wait for patch releases from vendors, nor can they rely on user communities to find and report these bugs. America and its allies, through international defense cooperation, need to find new and proactive ways to protect their critical infrastructures and military and non-military assets. NATO, with its CCDCOE, has put that into practice by implementing the "Defensics" technology.

Indications are that certain elements of the U.S. Government are now following suit. This is welcome news and an example of the type of international defense cooperation that we must pursue along with our allies in order to combat major defense and Homeland Security threats.

In conclusion, it is imperative in an era of limited resources and budget constraints that the United States engage its international partners who have far greater experience and expertise with niche technologies in specific cyber threat areas. Taking that course will help ensure the safety here at home and abroad through the most cost effective means.

Van D. Hipp Jr. is Chairman of American Defense International, Inc., a Washington, D.C.-based consulting firm specializing in government affairs, business development and public relations. He is the former Deputy Assistant Secretary of the U.S. Army. Since the September 11th attacks on the United States, Mr. Hipp has appeared on the Fox News Channel well over 400 times as an expert commentator on the War on Terror.

CCD COE is located in Tallinn, Estonia, on the premises of the Estonian Signals Battalion. The building itself was built by the Tsarist military in 1905 as a barracks, but it has now been completely renovated, and blends cutting-edge technological solutions within its beautiful, historic walls. CCD COE now hosts one of the most advanced cyber defence research centres in the world.