

Citizen Soldiers ready to defend cyberspace

By MAJ Aaron Munn and John Galeotos

Human capital and ingenuity have been and still are one of our nation's most precious assets. We are a nation of leaders, scientists, technological innovators, and corporate visionaries with diverse backgrounds and beliefs; and nowhere in the military is this diversity so embraced as it is in the ranks of the National Guard. A Citizen Soldier not only brings to the fight the same high levels of integrity, loyalty, professionalism, and duty as their active duty counterparts but, they also cultivate a diverse spectrum of civilian skills and experience that he or she provides during drills or deployments.

In today's modern society, the additional skills that the citizen Soldier brings to the table along with their military occupational specialty training are becoming increasingly technical in nature. It is not at all uncommon to find a Guardsman, who as a civilian, works for an intelligence agency or information technology contractor, a computer manufacturing or software programming corporation, or work in another related high tech field.

The Guard appeals to this patriot; they are leaders in their professional life with successful jobs or businesses, but they also want to serve our nation to feel a sense of pride in performing their duty and the esprit de corps that comes from serving with other noble men and women.

Those in the National Guard are prepared and trained to defend our nation for domestic and overseas contingencies. These ready and adaptable forces present additional capacity and capability that must be leveraged for defending Department of Defense, as well as federal and state government networks. In many cases the Guard is already part of the cyber fight through "Access," "Capability," and "Experience" to operate in this evolving environment.



Access

The National Guard is in each state and territory as well as The District of Columbia. It is this access at the local levels that enables the National Guard to execute cyber missions where other agencies have difficulty. This distribution of forces has obvious advantages for domestic response options and by defending networks at a local level the nation's cybersecurity

posture is bolstered. Additionally, the citizen-Soldier works in the cities and towns where private industry, corporations, and local, state organizations will also benefit from their training and expertise.

National Guard leaders have developed strong relationships with state emergency response entities that provide assistance in the event of crisis situations in the physical world; and it is those relationships that are being leveraged to increase the Guard's capability to assist local first responders in

the event of a crisis within the notional world we call cyberspace.

These relationships as a matter of public safety and national security must be shaped and formed to develop cyber incident response plans and contingencies because, as abstract of an idea cyberspace is, it touches nearly every part of our daily lives.

Currently, these relationships between the National Guard and their state and Local governments are being drafted, refined, and socialized to expand the individual efforts into a national capability. These efforts identify policies, authorities, roles, and responsibilities for National Guard cyber-capable forces to prevent or recover from possible catastrophic effects of a cyber-attack. As state National Guard units establish integrated cyber incident response plans with their local authorities, our cybersecurity as a nation grows.

The National Guard also has its' federal relation

ships with Department of Defense. The National Guard's relationships with both state and federal organizations provide unique opportunities to facilitate cyber incident response options that can be leveraged for local and national requirements. Ultimately, the National Guard's access within state, federal, and Department of Defense organizations can provide an integrating function for our nation's cybersecurity efforts and provide value to the advancement of a cyber-common operating picture shared between state and federal entities.

Capability

The Guard currently has cyber forces conducting both defensive and offensive cyber operations in Title 10 USC and Title 32 USC status. These forces are generated from a mix of Signal, Military Intelligence, Information Operations, Electronic Warfare units, as well as Air National Guard Cyber units. The elements range in size from squad to company size, so capabilities can vary dramatically per command.

In addition to these domestic and federal capabilities, the National Guard has international partnerships. The State Partnership Program matches individual state National Guards with sister nations to promote long term, enduring and mutually beneficial security relationships with friendly and allied nations around the globe.

The National Guard SPP provides forces to the Combatant Commands that encourage international cooperation and understanding, develop enduring relationships, and build mutual capacity to tackle the world's toughest challenges - to include cyber. The U. S. European Command has the most mature cyber SPP with eight of its twenty-two SPPs actively involved in cyber engagements with their sister nations. The National Guard states involved are Alabama, California, Colorado, Connecticut, Indiana, Maryland, Michigan, Minnesota, North Carolina, Nebraska, New Jersey, Ohio, Pennsylvania, New Jersey, Tennessee, Virginia and Vermont have all conducted exchanges with their partner nations.

Recently, the Virginia Army National Guard's Data Processing Unit, a cyber-capable unit located in Fairfax, Virginia, and the United Kingdom's Land Information Assurance Group, demonstrated a model for an effective first-of-its-kind cyber exchange. This exchange enabled each participant to learn how the other addressed cyber defense and to train together in an environment where the gaps could be identified and bridges built; both technical and policy in nature.

The exchange was conducted in two phases. In the first phase, the United Kingdom and National Guard Soldiers attended training on Camp Robinson, Arkansas at the Army National Guard's Professional Education Center, and then ended their engagement in Virginia.

This training consisted of familiarization with the Army National Guard's cyber simulation environment, providing operator level familiarization as well as high level system architecture exposure to understand how the flexibility of simulation platform could be adapted to various training requirements. In Virginia, the two units conducted a cyber exercise where they focused on detecting threat traffic and implement mitigation techniques.

The exercise scenarios ranged from denial of service attacks to various different means of data exfiltration to attacks against email and other critical system services. Multiple scenarios were run against the team often simultaneously. The next part of this exchange will take place in the United Kingdom. The Virginia DPU will travel to the United Kingdom sometime in early Fall 2012 and conduct a reciprocal event.

Even though many of the questions that complicate the military's role in the defense of cyberspace are still to be answered, the Guard continues to make progress and grow capability in spite of the numerous difficulties presented by outdated public policy and laws that create legal gray areas. The Guard's unique command structure enables its forces to individually address how they will respond to new cyberspace operations missions. The flexibility is evident in the diverse organizational structures that currently exist within the Guard in response to this problem set.

Experience

Some of America's most significant scientific advances, innovations, trade secrets, formulas and algorithms exist simply as data stored and processed on our nation's networks. How do we protect these incredibly valuable intellectual assets; especially with the difficult and complex landscape we call cyber? As it has been since the birth of our nation, the National Guard stands ready to answer this call.

It is important to understand the focus of the National Guard's efforts when we discuss cyber missions. The National Guard supports both domestic and federal missions. This dual-use function is the essence of what defines the "Guard" and distinguishes its ability and access to support cyber defense and response to defend the homeland. When a hurricane or wildfire threatens the citizens of a state, the experience is something very tangible, frightening, and occasionally tragic. In these situations, the citizens of our great nation welcome the assistance and protection of the National Guard, in fact they assume the Guard will be there and ready to respond. For over 327 years, the "Minutemen" have been there.

The cyber threat is subtle and insidious. It's not an enemy trail you can easily observe with your eyes.

(Continued on page 36)



“We will work with all the key players - including state and local governments and the private sector - to ensure an organized and unified response to future cyber incidents. Given the enormous damage that can be caused by even a single cyber attack, ad hoc responses will not do. Nor is it sufficient to simply strengthen our defenses after incidents or attacks occur.”

- President Barack Obama - May 29, 2009

(Continued from page 35)

It is not a rolling grey plume of dust devouring our cities. It is a difficult problem set that requires a different approach from responses to physical events like earthquakes or fires. The recovery from a large scale cyber attack is not as straight forward as a truck loaded with supplies after a hurricane or a plane filled with fire retardant to engage a wildfire. None-the-less the response to a major cyber attack is a mission that we must support because it is vital to the security of our nation.

In President Obama’s speech on cybersecurity, May 29, 2009, he states “We will work with all the key players -- including state and local governments and the private sector -- to ensure an organized and unified response to future cyber incidents. Given the enormous damage that can be caused by even a single cyber attack, ad hoc responses will not do. Nor is it sufficient to simply strengthen our defenses after incidents or attacks occur.”

The Guard has the experience needed to accomplish this mission. The Guard is already there.

Summary

There are many challenges ahead of us as we address the com-

plexities of operations in cyberspace. Beyond what types of cyber units are needed to fight the fight, recruiting, training, and retaining the highly skilled workforce needed in order to conduct cyberspace operations is daunting. Cyber can be considered a specialized craft and in order to grow cyber capability and capacity, it will require innovation in many ways to include retention. Arguably, the cyber profession may need to be treated like Aviators and pilots, doctors, or Special Forces operators: highly specialized and in high demand. These professions have tailored programs providing mechanisms to improve overall retention; cyber may and perhaps should have the same approach and philosophy.

The Guard is where these forces are needed. For over three centuries the Guard has favored its civilian nature in peace and donned the fierce aspect required during times of war.

John Galeotos, CISSP, CCNA Se-

curity, works for CACI International Inc. as a cyber subject matter expert. He is also a CW2 251A in the District of Columbia National Guard as a CND-team chief. He has worked for the Wyoming Army National Guard, White House Communication Agency, Department of Commerce, and currently at the National Guard Bureau in Information Management Governance on the ARNG Cyber Working Group.

MAJ Aaron Munn is currently serving as Army National Guard’s cyber operations project officer. His military background and qualifications include information operations, public affairs, Signal, and air defense. MAJ Munn has served in the Army National Guard for over 20 years with assignments in three states and three mobilizations. His civilian experience includes high tech investigations, information security, and network administrator. He is a Certified Information Systems Security Professional, Microsoft Certified Systems Engineer, and A+ Certified Technician.

ACRONYM QuickScan

DPU – Data Processing Unit
 USC – United States Code
 SPP – State Partnership Program