Cyber Warrior: The Role of the National Guard

by

Lieutenant Colonel Gary A. Ropers
United States Army National Guard

United States Army War College
Class of 2014

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.
The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.
The National Guard has a long history of providing assistance to state and local communities in the wake of a hurricane, tornado, floods, forest fires or other natural disaster strikes. It is now time for the National Guard to build the next type of unit or section to help respond to the next potential man-made disaster, that being a cyber attack. The Department of Defense, the Active Army and Army National Guard should embrace the creation of Cyber Protection Teams in the National Guard. The National Guard has a strong relationship with civilian agencies, and these citizen-soldiers can play and increasing role in the cyber domain by leveraging National Guard personnel who already possess many of the core technological skills as a result of their civilian occupations. The cyber defense mission requirements performed at a home station can be expanded to provide DOD and the Governors with a synergistic capability.
USAWC STRATEGY RESEARCH PROJECT

Cyber Warrior: The Role of the National Guard

by

Lieutenant Colonel Gary A. Ropers
United States Army National Guard

Mr. William O. Waddell
Center for Strategic Leadership and Development
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the United States Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013
Abstract

Title: Cyber Warrior: The Role of the National Guard

Report Date: 15 April 2014

Page Count: 35

Word Count: 5617

Key Terms: Cybersecurity

Classification: Unclassified

The National Guard has a long history of providing assistance to state and local communities in the wake of a hurricane, tornado, floods, forest fires or other natural disaster strikes. It is now time for the National Guard to build the next type of unit or section to help respond to the next potential man-made disaster, that being a cyber attack. The Department of Defense, the Active Army and Army National Guard should embrace the creation of Cyber Protection Teams in the National Guard. The National Guard has a strong relationship with civilian agencies, and these citizen-soldiers can play and increasing role in the cyber domain by leveraging National Guard personnel who already possess many of the core technological skills as a result of their civilian occupations. The cyber defense mission requirements performed at a home station can be expanded to provide DOD and the Governors with a synergistic capability.
Cyber Warrior: The Role of the National Guard

The National Guard should provide assistance in the wake of a cyber attack just as they do when a hurricane, (tornado, floods, forest fires) or other natural disaster strikes.

—Rep. Steve Israel
D-N.Y. ¹

Have you ever stopped to think of all the things you do on a daily basis that is either directly or indirectly connected to the cyber domain? It’s the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation.² The networks and the power grid are part of what is considered our Nation’s critical infrastructure, the assets, systems and networks vital to nation. With approximately 85 to 90 percent of the U.S. critical infrastructure privately owned and operated, the private sector is having an increasingly important role in the security of the networks they operate. The cyber domain also includes the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history.³ We, as a nation, must secure our cyberspace to ensure that we can continue to grow the nation’s economy and protect our way of life.⁴

President Obama has declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation”⁵ and that “America’s economic prosperity in the 21st century will depend on cyber security.”⁶ The National Guard Association of the United States (NGAUS) is a big proponent of the expanding the role of the National Guard in the cyber security operations. NGAUS states that “cyber security is an increasingly important mission area, impacting both public and private sectors.”⁷ Current advancement in computer technology and the increased
reliance on electronic data to carry out day-to-day activities have left companies open to cyber espionage, intellectual property theft and exploitation of vulnerabilities in our critical infrastructure. On a daily basis hackers, ranging from high school kids to organized foreign governments, search for ways to gain access, take control or disrupt the information on networks in which critical infrastructure sectors operate on. State Governors are another group that have become very focused on cyber security and are looking for tools and resources available they can use to better protect critical infrastructure and assets that reside in their states. One of the assets the Governor’s are looking to utilize is they have at their disposal and that is the Army and Air National Guard units. Just as 85 percent of the critical infrastructure is owned by the private sector, private citizens work for those companies and some of those private citizens are also Guard members, sometimes called citizen-soldiers.

As citizen-soldiers, the National Guard (NG) can easily be utilized in the cyber domain with its unique access to a wealth of information technology talents within its ranks, including Guardsmen working as network defenders at top information technology, banking, medical and defense companies. General Craig McKinley, former Chief of National Guard Bureau stated it this way:

…the NG (National Guard) can play an increasing role in the cyber domain by leveraging NG personnel who already possess many of the core technological skills as a result of their civilian occupations…These types of personnel and forces can support a range of offensive and defensive mission requirements performed from their home station that can also be expanded to provide DOD and the Governors with a synergistic capability.

This paper will examine the National Guard Bureau’s (NGB) plan and guidance for the building, training, stationing (state selection) and the mission of the cyber protection teams. It will show the history of the National Guards role in the cyberspace,
to include the current capabilities both the Air and Army National Guard. The focus will be on how the cyber protection teams will be structured and manned, their specific roles and responsibilities, the method and procedures to train them and how they will be stationed in the states. Recommendations are provided on how to best train, organize, and stationing of the cyber protection teams.

Background

Political leaders and strategic leaders are becoming increasingly aware of the threat posed by cyber warfare. The current National Security Strategy (NSS), published in May 2010, serves as the Obama Administration’s document for national security. It mentioned the word cyber 24 times. It also dedicated an entire section to securing cyberspace stating, “The very technologies that empower us to lead and create also empower those who would disrupt and destroy.” The technology gives our military superiority, but our unclassified government networks face a range of criminal hackers. Additionally, the NSS states the nation's digital infrastructure is a strategic asset, and protecting it is a national security priority. It charges the nation to deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by: (1) investing in people and technology and (2) strengthening partnerships.

One of the ways to build upon both of the previous mentioned areas is to work with the National Guard. The 2011 National Military Strategy (NMS) states the military will continue to dedicate, fund and train a portion of the National Guard for homeland defense and defense support of civilian authorities (DSCA). The Department of Homeland Security (DHS) is the lead and key Federal agency involved in cyber security within the homeland defense structure. DHS’s Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise states that today’s threat
to cyber security requires the interaction of multiple federal departments and agencies, as well as, operational collaboration across federal, state, local, tribal, territorial governments, nongovernmental organizations and the private sector, and members of the public. The potential for collaboration between DHS and the Guard in the cyber domain is significant, just as the two have worked together in response to natural disasters in the past.

Cyber-teams within the Guard is not a new concept, cyber force structure is already in place within the Army National Guard and include the computer network defense teams (CND-T) –eight-soldier teams that perform defensive cyber operations. Similarly, the Air National Guard has a range of “network warfare” and “information warfare” squadrons of varying sizes, structures and skill levels. According to cyber expert Jason Healey, some of these Air Guard units are impressive, “[There’s] the 262nd Network Warfare Squadron in Seattle (which includes soldiers who work for Microsoft, Google, Cisco and Boeing), [and] the 175th Network Squadron [Maryland Air National Guard] at Fort Meade who is deeply embedded in NSA work.” Many of these members are performing similar duties on their day jobs as they do for the military.

2013 Cyber Warrior Act

New Congressional legislations, H.R. 1460 and S. 658, introduced by a bipartisan group of both senators and representatives in March 2013 called the Cyber Warrior Act of 2013, would establish Cyber and Computer Network Incident Response Teams (CCNIRTs) in each of the 50 states and four U.S. territories under the direction of the National Guard Bureau, much like the [Weapons of Mass Destruction – Civil Support Team] WMD-CSTs. Although at the time of this paper no additional progress has been made on either of the acts, the cyber security issue is still recognized as a
major problem in Congress. Under the new legislation, a governor or the secretary of
defense could activate CCNIRTs, also known as “Cyber Guards,” in response to a cyber
attack.23 The Act states,

The Secretary of Defense shall establish in each of the several States and
the District of Columbia a separate team of members of the National
Guard under section 2310(d) of title 10, United States Code (as amended
by subsection (b)), and section 510 of title 32, United States Code (as
added by subsection(c)), to perform duties relating to analysis and
protection in support of programs to prepare for and respond to
emergencies involving an attack or natural disaster impacting a computer,
electronic, or cyber network.24

Additionally, the Act requires,

The homeland defense activities for which the Secretary is authorized to
provide funds to a governor for National Guard units to include: The
National Guard provision of cyber emergency education and training for
state and local law enforcement and governmental personnel and…order,
the National Guard’s performance of activities undertaken by state and
local governments to prepare for and respond to such emergencies.25

General Keith Alexander, the (outgoing) chief of both CYBERCOM and the
National Security Agency (NSA) stated, “The Guard can play a huge role. There’s two
key things that they can do. First… it gives us additional capacity that we may need in a
cyber conflict. The second part is, it also provides us an ability to work with the states.”26

As with any Guard unit, the legislation would allow Governors to call up their
Cyber Guard to address a local cyber emergency, boosting the capacity to protect
computer networks in the homeland where the active military may not play a role.27 The
act would also allow Governors to get the Guard to help train State and Local Law
Enforcement and other Cyber Responders in cyber security, and help them develop
sound best practices that allow more cohesive interaction with Federal-level
responders.28 While at the time of this paper, March 2014, no additional progress on the
Cyber Warrior Act of 2013 has occurred since the introduction of the act, but what can
be said about the legislation is that it did what is was meant to do and that was to drive the discussion of having the DOD include the National Guard in cyber operations.


The 2014 National Defense Authorization Act (NDAA) called for the Department of Defense (DOD) to conduct a formal evaluation of the role that the National Guard could play in bolstering network defenses against attack.\(^{29}\) The law’s wording is pushing for DOD to rely more heavily on the National Guard for cyber warfare operations that don’t require deployment overseas, calling for a report on how the DOD would recruit, organize, and train such a force, and what it would cost.\(^{30}\) As this paper is being written the results of this formal evaluation have yet to have been released. According to the National Guard Bureau, the legislation will provide the National Guard an opportunity to influence its position and role by assisting in the evaluation of potential reserve component cyber roles as well as the ability of the National Guard to support domestic cyber missions and help fulfill U.S. Cyber Command (USCYBERCOM) requirements in either state active duty or Title 10 status.\(^{31}\)

General Frank J. Grass, the Chief of the National Guard Bureau, (CNGB) established a General Officers Advisory Council (GOAC) to study the role of the Guard in cyber defense. The GOAC members include current Adjutant Generals (TAG) and other key individuals associated with U.S. Cyber Command (USCC), Air Force Cyber (AFCYBER), Air Force Space Command (AFSPC) and Army Cyber (ARCYBER). The mission of the GOAC is to first serve as an advisory board to General Grass on subjects related to the development of “National Guard cyber forces, capabilities and operations.”\(^{32}\) This will include providing recommendations that pertain to the “strategy, policy, plans, capabilities, organizations, manpower, resources, legislative actions, and
training” related to National Guard cyberspace activities. The second mission is to recommend the courses of action that will “facilitate unified positions within the National Guard with the Services, Combatant Commands, Office of Secretary of Defense and other stakeholders.” The third mission of the GOAC is to make recommendations for initiatives that “accelerate the development and fielding of National Guard cyber forces” to meet the wide array of cyberspace security needs.

The Guard is Uniquely Suited for Cyber Defense

The National Guard already has a strong relationship with civilian agencies, working in support of policy in developing capabilities and threat assessments in domestic response when civilian entities are overwhelmed. The Army National Guard has bases and armories in more than 2,600 communities and relationships with the owners and operators of privately owned and operated infrastructure vulnerable to cyber attacks. The number of communities increases to more than 3,000 when the Air National Guard is taken into account, with nearly every zip code being represented by a Guardsman. Figure 1 shows the footprint of the Army National Guard across the United States. While the number of Army locations has decreased from the 2012 number of 2,899 there are still a vast number of communities with a National Guard presence.
The National Guard can make use of its relationships and inherent hometown history as a force multiplier, by bringing together local, state and federal leaders to educate and develop best practices. A recent example of a cyber security initiative focused on bringing private, local and federal leaders together can be seen in the State of Michigan. The Michigan’s cyber range center allows for testing of cyber security in a virtual town consisting of a school, a library, a city hall and a power company. The range pairs extensive cyber security resources with hands-on training opportunities to help protect computer systems and sensitive data. Areas identified to benefit from the
cyber range include infrastructure defense, homeland security and criminal justice to
name a few. Additionally, the Guard’s unique civilian roles and skills, as computer
coders and network technicians, gained by working in private sector captures a
centralized repository of information and high-tech skills lacking in the active
components. 43

Colonel David Collins, the National Guard Bureau’s chief cyber staffer (NGB-J6),
points out that the National Guard does have advantages over the Active Duty force if
allowed to help in the homeland defense domain. The first and maybe the most
important is “Guard troops are physically present in armories, communities, and indeed
civilian workplaces across the country, and not concentrated in a few large bases.” 44
That puts them in contact with civilian networks and their operators where a cyber event
may occur. The second is the National Guard has the ability to “operate across the
entire cyber spectrum under federal orders (so-called Title 10 status) or on the orders of
the state governor (State Active Duty or Title 32).” 45 National Guard troops under the
governor’s command are not bound by the Posse Comitatus Act or other restrictions on
using federal troops for law enforcement. More on the type of orders and Posse
Comitatus will be explained in the next section. The third advantage is as part-time
troops, “Guard cyber warriors would have full-time jobs in the civilian information
technology world, giving them a different and often deeper expertise than the active-
duty forces, which tends to be younger.” 46

Colonel Collins points out an additional advantage which should be taken into
account to build upon the three above and add a plus one concept. The plus one
concept is a “Cyber Skills Retention Pool” to where the National Guard cyber protection
units could be a place to “recruit and retain highly skilled and trained cyber warriors who are leaving Active Duty.” While they may be separating from Active Duty many service members have a desire to continue to serve, and the National Guard provides them an opportunity to pursue a civilian careers while continuing to serve their country.

Authorities and Law

An advantage that the National Guard possesses is the ability to draw authority from different levels of the government and support cyber operations across the entire spectrum of these authorities as mentioned by Colonel Collins. These Federal and State authorities fall under one of the following three, State Active Duty (SAD), Title 32 (T32), or Title 10 (T10). The National Guard cyber protection team members would be able to perform all types of cyber operations under the Title 10 authority and all but a select few Offensive Cyber Operations in either the Title 32 or SAD status.

There are differences between the authorities and laws pertaining to State Active Duty, Title 32 and Title 10. State Active Duty and Title 32 fall under the authority of the Governor of the State, who is the commander-in-chief when National Guard units are not under federal control.

A National Guardsman can be placed in a “State Active Duty” status, which occurs when the Governor activates the National Guard in response to “natural or man-made disasters or a Homeland Defense missions.” State Active Duty is based on each individual States’ statute and policy in which the Soldiers and Airmen remain under the command and control of the Governor. The Posse Comitatus Act (PCA) does not apply to this duty status. The Governor can activate the National Guard in the following forms of active service, which is the status the Cyber Protection Teams would be put under in the response to a cyber security incident within the state.
The second status the Guardsman could be placed in is the “Title 32” or Full-Time National Guard Duty status, which means a status of training or other duty performed by a member of the National Guard. Title 32 allows the Governor, with approval of the President or Secretary of Defense (SECDEF), to have members conduct operational Homeland Defense activities.

The third status a Guardsman could be activated in is Title 10 of the U.S. Code. While serving under Title 10 a Guardsman is considered Active Duty, meaning they are on full-time duty status orders and commanded by active military service of the United States. For a National Guardsmen to be placed in a Title 10 status the President would need to “federalize the National Guard forces by ordering them to active duty in their reserve component status or by calling them into Federal service in their militia status.”

A key to state active services (SAD and Title 32) is that Federal Law provides the Governor the ability to place soldiers in a full-time duty status under the command and control of the State but funded with Federal dollars. Another benefit of the state active service is it has a statutory exception to the Posse Comitatus Act, which forbids the use of the federal military personnel to execute civil law unless authorized by the Constitution or an Act of Congress. Posse Comitatus gives the Governor the ability to use the Guard in a law enforcement capacity while maintaining command within the State.

Current Capacities in the Air and Army Guard

The Air National Guard (ANG) currently has cyber capability in each of the 54 States, Territories, and the District of Columbia. The ANG cyber workforce missions align with the military and Domestic Operations (DOMOPS) dual-use capability.
Air National Guard provides cyberspace capability in four areas: (1) Cyberspace Defense, (2) Cyberspace Force Application, (3) Cyberspace Support, and (4) Cyberspace Intelligence, Surveillance, and Reconnaissance. These units relate to the Network Warfare Squadron (NWS), the Information Operations Squadron (IOS) and the Information Aggressor Squadrons (IAS). The Air National Guard have 8,558 individual slots assigned to the cyberspace missions, which is 7.4 percent of the total Air National Guard workforce. But less than 30 percent of the total work forces assigned to the cyberspace domain are full time. The remaining cyberspace work forces support drill operations and prepare for their go-to-war type missions. Current states with extensive Air National Guard operational cyberspace units are Rhode Island, Delaware, Maryland, Washington, Vermont, California, Texas, Utah and Kansas. See figure 2, for the size and location of these units.
The Army National Guard (ARNG) as stated previously has the CND-T with a Defensive Cyber Operation (DCO) mission in all 54 States, Territories and District of Columbia. The Army National Guard also has two units located in Virginia who work on the Offensive Cyber Operations (OCO), DCO, Planning and Information Analysis (IA) missions. As you can see from the graph below the CND-T units, as of 20 Feb 13, are not filled to a 100 percent level, they are currently showing a fill rate of 69 percent. See Figure 3, showing the size and location of the Army National Guard cyber units.
At the time this research paper is being written the Army National Guard is training a 39 person Title 10 Cyber Protection Team (CPT). Figure 4 shows the duty title, rank, MOS and quantity of the Title 10 CPT positions, which will includes seven Officers, 16 Warrant Officers, and 16 enlisted soldiers, with Signal and Military Intelligence (MI) being their main composite skill set. The Army National Guard Title 10 CPT is currently attending cyber training courses at the National Guard Professional Education Center (PEC) located in North Little Rock, Arkansas. They are being trained to the same standards as the Active Duty Cyber Mission Forces. These 39 personnel plus four additional team members were built from a pool of 86 applicants, of which 58 were considered based on their background and education. Team members were required to have previous job experience in “cyber security, networking, and/or
information technology, along with experience with the DOD Computer Network Operations and working targeting at Echelons above Division.”

As part of their training these individuals will receive mission specific required training as part of their assignment to include Certified Ethical Hacker, Joint Network Attack Course (JNAC), and Joint Computer Attack Course (JCAC). The Army National Guard is currently working with Army Cyber (ARCYBER), United States Cyber Command (USCC), and PEC to prepare an Intermediate Cyber Core (ICC) equivalency packet to be submitted to USCC for validation of the training taught at PEC. Once the National Guard Title 10 team has completed their training they will be assigned to a 3 year active duty assignment supporting ARCYBER. In March 2014 it was announced the Army National Guard T10 team would be temporally stationed at an Army National Guard Armory located in Laurel, Maryland until a permanent facility is built to station them at Fort Gordon in Georgia.
A potential issue with the training provided by USCC/National Security Agency (NSA) has been raised by the National Guard Reserve Director (USCC/GRD), a National Guard Brigadier General assigned to USCC. The concern is around the availability of the military’s high-end training slots provided by the Active Duty training schools and those by USCC/NSA, who also serve/train the Air Force, Navy and Marines. At the time of this paper, only the Active Duty Cyber Mission Forces (CMF) had priority and access to the USCC/NSA training courses. To put it into perspective the current National Guard personnel needing the cyber training would be considered excess and would only be allowed to attend if seats are available. As the Active Army begins to build its cyber force, fewer slots will be available to appropriately train the individuals being assigned to the National Guard Cyber Protection Teams. Another way

<table>
<thead>
<tr>
<th>Duty Title</th>
<th>Rank</th>
<th>MOS</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detachment Chief</td>
<td>MAJ</td>
<td>53A</td>
<td>1</td>
</tr>
<tr>
<td>Detachment NCOIC</td>
<td>SFC</td>
<td>35N</td>
<td>1</td>
</tr>
<tr>
<td>Operations Officer</td>
<td>CPT</td>
<td>53A</td>
<td>1</td>
</tr>
<tr>
<td>Network Warfare Cyber Planner</td>
<td>CW3</td>
<td>255S</td>
<td>1</td>
</tr>
<tr>
<td>CND Manager</td>
<td>CPT</td>
<td>24A</td>
<td>3</td>
</tr>
<tr>
<td>Systems Architect</td>
<td>W2</td>
<td>255A</td>
<td>10</td>
</tr>
<tr>
<td>Cyber Security Analyst</td>
<td>E5</td>
<td>25B</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>E6</td>
<td>25B</td>
<td>2</td>
</tr>
<tr>
<td>Network Infrastructure Service Specialist</td>
<td>W2</td>
<td>255N</td>
<td>5</td>
</tr>
<tr>
<td>Close Access Network Operator (CANO)</td>
<td>E6</td>
<td>35N/35P/35S/35T(35Q)</td>
<td>4</td>
</tr>
<tr>
<td>Close Access Network Operator (CANO)</td>
<td>E5</td>
<td>35N/35P/35S/35T(35Q)</td>
<td>1</td>
</tr>
<tr>
<td>All Source Intelligence Analyst</td>
<td>E5</td>
<td>35F</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>E6</td>
<td>35F</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total Personnel</strong></td>
<td></td>
<td><strong>39</strong></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4: Title 10 Cyber Protection Team MOS/Grade Breakdown

According to the table above, the Duty Title for Detachment Chief is MAJ, the Rank for Detachment NCOIC is SFC, the MOS for Operations Officer is 53A, the MOS for Network Warfare Cyber Planner is 255S, the MOS for CND Manager is 24A, the MOS for Systems Architect is W2, the MOS for Cyber Security Analyst is 25B, the MOS for Network Infrastructure Service Specialist is W2, the MOS for Close Access Network Operator (CANO) is 35N/35P/35S/35T(35Q), the MOS for All Source Intelligence Analyst is 35F.
to help reduce the training timeframe is by looking at what civilian acquired cyber skills and training the National Guard personnel have and see if constructive credit can be given to those individuals.

An additional impending concern of building the Cyber Protection Teams in the National Guard compared to the Active Duty is the active component will have the ability to use Department of the Army (DA) Civilians to fill 16 positions whereas, the National Guard teams will be filling these positions with Warrant Officers. The 16 positions are as follows: one Network Warfare Cyber Planners (255S), the 10 Systems Architects (255A) and the five Network Infrastructure Service Specialists (255N) as identified in Figure 4. As of July 2013, the Army National Guard as a whole only had seven qualified Network Warfare Cyber Planners with one required in each team. There is a tremendous amount to time needed to develop an individual into a Network Warfare Cyber Planner Warrant Officer.

For a soldier to become a Network Warfare Cyber Planner Warrant, they would have to be a Staff Sergeant (E-5) or above, had 36 months of rated time as a Non-Commissioned Officer (NCO), 4-years of Information Technology (IT) experience, a Bachelor or Masters Degree. All of this would get them ready for selection as either a System Architect or Network Infrastructure Service Specialists position, where they would have to take additional training courses and obtain the rank of Warrant Officer 2 (CW2) or Warrant Officer 3 (CW3). Only after obtaining the rank of CW2 or CW3 is an individual eligible apply for and eligible to become a Network Warfare Cyber Planner. At a minimum it will take a new soldier in the Army National Guard at least nine years, but
more along the lines of 12 years, to become eligible for a Network Warfare Cyber Planner position.

Cyber Protection Teams Mission

The 7th Signal Command, based at Fort Gordon in Georgia, states the Cyber Protection Team are “prepared to defend the nation in response to hostile action and imminent cyber threats.”

They describe a Cyber Protection Team as a:

…Cyber Protection Teams (CPTs) (will) conduct global cyberspace operations to deter, disrupt, and defeat our adversary’s cyberspace operations, and defend the United States through specialized Cyber support missions. Cyber Protection Teams consists of dedicated defensive operations, analysts, planners, and leaders who conduct operations to protect specified missions or national assets in ant throughout cyberspace. Our teams are prepared to rapidly evaluate, and act in response to unexpected and dynamic cyber situations.

Each of the 39 member cyber teams are task organized into a Headquarters (HQ) section and five squads. The Headquarters section will have four individuals assigned while each of the squads will have seven individuals assigned. The five squads are organized depending on their specific mission set (Figure 5). The first team is the Mission Protection or Blue Team which will provide risk mitigation for DOD teams, along with providing a quick response force. Their primary focus will be on fortifying the posture and processes from inside-out. The second team is the Discovery and Counter-Cyber or Hunt Team which will actively pursue threats on Blue (friendly) networks and eliminates threat activity. The third team is the Cyber Threat Emulation or Red Team which provides a team to emulate the threat against the DOD cyber terrain to help fortify posture and processed from outside-in. The fourth team is the Inspection Forces or White Team which has the task of ensuring the compliance DOD policies and providing input to optimize performance and best practices. The fifth team
is the Cyber Support or Green Team which is tasked to provide technical assistance when requested to enhance cyber security, along with help in training gaps. is the Cyber Support or Green Team which is tasked to provide technical assistance when requested to enhance cyber security, along with help in training gaps. is the Cyber Support or Green Team which is tasked to provide technical assistance when requested to enhance cyber security, along with help in training gaps. is the Cyber Support or Green Team which is tasked to provide technical assistance when requested to enhance cyber security, along with help in training gaps.

Figure 5: Cyber Protection Team Mission and Organization

Stationing of the Cyber Protection Teams

One of the biggest questions after assuring the cyber teams have the ability to be trained is where is the Army National Guard going to station them. The Army National Guard Training Division (G3) Information Operations (ODI) section was tasked to provide the different Course of Actions (COAs) on the stationing of the ten teams by the end of FY17. The goal was to develop the Army National Guard’s plan to build and station three of the cyber protection teams no later than the end of FY15, followed by
four teams in FY16 and three teams in FY17. Some of the selection criteria for the Cyber Protection Team included the availability of a Sensitive Compartmented Information Facility (SCIF) with a capacity for the 39 members, proximity to at least one Military Intelligence and one Signal units, and be located near both an Academic and Industrial Centers of Excellence who are focused on cyber related fields.

Two distinct COAs were developed as the outcome of their analysis. The first was to have the teams aligned with the Federal Emergency Management Agency (FEMA) and the second based on best a state's ability to provide trained individual for a cyber protection team. There are ten FEMA regions across the United States making it a natural selection for placing one team in each of the regions. Another advantage to the FEMA aligned course of action is it would enhance regional support to the Defense Support of Civil Authorities (DSCA), which is a mission of the National Guard. One of the advantages pointed out in the best capable COA was lifecycle management of soldier in the MI and Signal units. Although not used as part of the selection criteria the ARCYBER recommended that there should not be any split Cyber Protection Teams. The Army National Guard has a tradition of putting smaller sections of a unit in several states. This has been a practice in the Aviation, Maintenance and Engineer units to ensure geographic distribution of structure.

Role of ARCYBER

The U.S. Army Cyber Command role of responsibility spans the entire Army from the tactical edge to the strategic enterprise level. The ARCYBER Active Duty Cyber Protection Teams are being built to support one of following missions, first to support USCYBERCOM in the “Defend the Nation” role, second in support of the Defense Information Systems Agency (DISA) to secure, operate and defend the Department of
Defense Information Network (DODIN), third in support of the Regional Combatant Commanders such as those at U.S. Pacific Command and U.S. Central Command, and Functional Combatant Commanders such as those at U.S. Transportation, and forth in support of the services (i.e., Army, Navy, Air Force or Marines).  

Although the Secretary of the Army has yet to approve the building of the Army National Guard Cyber Protection Teams, there has been a resource segment set aside for them. While the Army National Guard T10 Cyber Protection Team will receive their missions from ARCYBER, they will be assigned to 7th Signal Command for operational control (OPCON) and the Army National Guard will retain administrative control (ADCON) over them. The addition of this one Army National Guard T10 cyber protection team will give ARCYBER a total of nine teams, resulting in approximately a 13 percent increase in capacity and capability.

Lieutenant General (LTG) Edward Cardon, the chief of Army Cyber Command, said it will take a partnership between the active Army, the Army National Guard, the Army Reserve, civilians, other government agencies, and industry partners “to protect and defend our mission in cyberspace, a domain of infinite possibilities and ever-changing threats.” He has also pointed out the challenge it will be in getting the National Guardsmen into the high-end cyber training schools.

Recommendations

Throughout the paper we have seen the challenges ahead that the National Guard Bureau and the Army National Guard will face as they begin to train, organize and build, and station the Cyber Protection Teams. The recommendation for the training is that the National Guard Bureau should continue to work with both USCC/NSA and ARCYBER on getting more cyber training courses at PEC certified. There may certainly
be some courses that would still need to be taught at the USCC/NSA and ARCYBER training sites based on training exercises at the TSC/SCI level. However, PEC could train core cyber courses leaving, USCC/NSA and ARCYBER courses open to the 6,000 Cyber Mission Forces as directed by the 2014 Quadrennial Defense Review (QDR).

The recommendation for the organization and building of the teams is that the states will need to develop a process to identify individuals who have the potential of becoming a Cyber Warrant Officer. This development process is needed to initiate the training and gain the years of experience needed to become a Warrant Officer. The use of Warrant Officers in lieu of Department of Army Civilians in 16 of the positions will require a rapid and continuous buildup of talented soldiers wanting to work in cyberspace.

The recommendation for the stationing of the 10 Title 32 Cyber Protection Teams is that they should be based on the FEMA regional course of action laid out by the NGB-G3 section, with the addition capability of a split-state structure as long as the states are within the same FEMA region. The split-state arrangement would give the teams a larger pool of individuals to select from in the initial phase of building them.

The final recommendation is on the mission of the Title 32 Cyber Protection Teams. The mission set of these teams needs to be based around the cyber defense mission with the capability to partner with the public and private sector in creating training environments similar to the Michigan cyber center. The ability of the National Guard teams to utilize the five different sections of the task organization with the public and private sector can be a force multiplier by bringing together the local and state leaders to educate and develop best practices.
Conclusion

Many of our adversaries lack the ability to confront our forces physically, choosing instead to employ virtual weapons with potentially devastating effect. We must take full advantage of these technologies, building our own capabilities to operate in cyber-space with the same level of skill and confidence we enjoy on the land. We will either adapt to this reality or risk ceding the advantage to future enemies.\(^7\)

The above quote by the Chief of Staff of the Army General Raymond T. Odierno, points out there needs to be an increased awareness and focus on cyberspace and its associated threats. One of the key partners in this focus should be the Army National Guard and their ability to stand up Cyber Protection Teams to help in the defense of cyberspace, not only as a resource for the Army but as a resource the state Governors can use in a time of a cyber incident within their state. The National Guard has a long history of working with state and local officials on disaster responses, cyber attacks are the next disaster they need to be ready to respond to.

Endnotes

1 Ron Jensen, "Cyber Sense," *National Guard*, June 2013,.


3 Ibid.

4 Ibid.


Ibid.


Ibid.

Craig McKinley, Chief, National Guard Bureau, “The Role of the National Guard in “A Balanced Strategy,”” Information Memorandum, January 2009.

Obama, National Security Strategy, 27.

Ibid.

Ibid.

Ibid., 28.


Ibid.


Ibid.

25 Ibid.

26 Freedberg, “National Guard Fights For Cyber Role in 2015 Budget.”


28 Ibid.


30 Ibid.


33 Ibid.

34 Ibid.

35 Ibid.

36 Ott, “Issue: Expand Cyber Security Operations.”


38 Ibid., 16.

39 Army National Guard G5, ARNG 101 Core Briefing, March 27, 2014, 59.

40 Ott, “Issue: Expand Cyber Security Operations.”


42 Ibid.

43 Ott, “Issue: Expand Cyber Security Operations.”

44 Freedberg, “National Guard Fights For Cyber Role in 2015 Budget.”
45 Ibid.

46 Ibid.


48 Ibid.


50 Ibid.

51 Ibid.

52 Ibid.


55 Ibid.

56 Ibid.

57 Ibid.

58 Image borrowed from National Guard Bureau, ARG ARNG Cyber Forces as of MAR2013 (Arlington, VA.: NGB-J6).

59 Ibid.


61 NGB Cyber GOAC, GOAC 6th Meeting as of 06DEC2013 (Arlington, VA” NGB GOAC, December 6, 2013).


64 7th Cyber Mission Unit, Cyber Protection Team Recruiting Brochure.

Ibid.

Ibid.

Ibid.

Ibid.

Ibid.


