Hampton Roads Cyber Corps Initiative

A potential regional model for the Commonwealth of Virginia

Prepared by: Michael B. Feggans

*The views expressed are those of the author and do not reflect the official policy or position of the US Air Force, Department of Defense, US Government, or the Commonwealth of Virginia.

TABLE OF CONTENTS

INTRODUCTION

In the event of a domestic cyber-attack on a civilian target such as a hydroelectric plant, who has the authority to defend and responsibility to respond to the attack. While it may seem like a simple answer-the government, it is a much more complicated answer.

The true answer is that even the Department of Defense is unsure about who is ultimately responsible for tackling a large cyber-attack on civilian resources, per a recent GAO report titled CIVIL *SUPPORT DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, per the GAO:

"DOD officials acknowledged the limitations of current guidance to direct the department's efforts in supporting civil authorities in a cyber incident and discussed with GAO the need for clarified guidance on roles and responsibilities. DOD officials stated that the department had not yet determined the approach it would take to support a civil authority in a cyber incident and, as of January 2016, DOD had not begun efforts to issue or update guidance and did not have an estimate on when the guidance will be finalized. Until DOD clarifies the roles and responsibilities of its key entities for cyber incidents, there would continue to be uncertainty about which DOD component or command should be providing support to civil authorities in the event of a major cyber incident."

With that uncertainty at the federal level, it becomes even more evident that local and state officials will have to prepare themselves to protect their information networks from attacks until a true comprehensive federal response to

cyber-attacks can be fully fleshed out and tested. It then becomes imperative for commonwealths & states to take the lead in providing both strategic and tactical guidance so not only elected officials but constituents have a clear understanding of the technical capabilities and responsibilities that are available at the state level. This paper will look at the feasibility of creating a civilian cyber corps in the Hampton Roads region of Virginia that if successful could be rolled out and utilized across the rest of the commonwealth.

BACKGROUND

While this analysis is not designed to answer all of the overarching roadblocks and issues that might arise from creating a regional cyber corps, the hope is that it will ignite a great starting point for further in-depth discussion and critique. The ultimate end goal though is to create a ready technical volunteer force that is able to help defend the Commonwealths local population, intellectual property, and physical assets from a large scale directed cyber attack

When looking at creating a regional cyber corps for the Commonwealth of Virginia, it's important that some of these questions are first answered:

- What exactly is the cyber corps?
- Who had identified a need for a cyber corps?
- What is the geographical, population, and political area of responsibility?
- What is the proposed structure and capabilities of the cyber corps?
- What unique challenges are presented with creating a regional cyber corps?
- What does the Hampton Roads region workforce pool offer in technical subject matter experts?
- What other areas have successfully implemented their own cyber corps?

ANSWERS & SUGGESTIONS

Question 1: What exactly is the cyber corps?

Answer: The cyber corps are devised as a volunteer force of information technology (IT) subject matter experts (SME) who are willing to volunteer their time and technical skills to help defend the digital domain during a crisis and to support the needs of the Commonwealth. These volunteers may come from a wide variety of areas such acedia, private industry, federal and state, and retirees. All volunteers will be properly vetted with background checks and job specific training will be offered to augmented the proven technical skills that they currently possess. By pooling resources from the local talent pool this will allow the cyber corps the agility to respond to a crisis within their area of responsibility and will also foster much needed regional partnerships within the Hampton Roads area.

Question 2: Who has identified a need for a cyber corps?

Answer: Within the Commonwealth of Virginia report titled *Cyber Security Commission First Report, August 2015 "Threats and Opportunities"* a proposal was made by the Education Work Group to create a cyber corps This proposal stated that "*Commonwealth Cyber Corps: The Corps would consist of volunteer experts in cyber security from Virginia's corporations and government agencies who could be certified to serve as Adjunct Faculty at the state's community colleges and universities. The Corps could also sponsor an Industry-Government Exchange Program to permit cyber experts from the private sector to work for a time in the Commonwealth government, and vice versa, sharing their expertise."*

By expanding upon the last sentence in the proposal, the cyber corps could potentially become a force multiplier to assist local and state resources during a crisis.

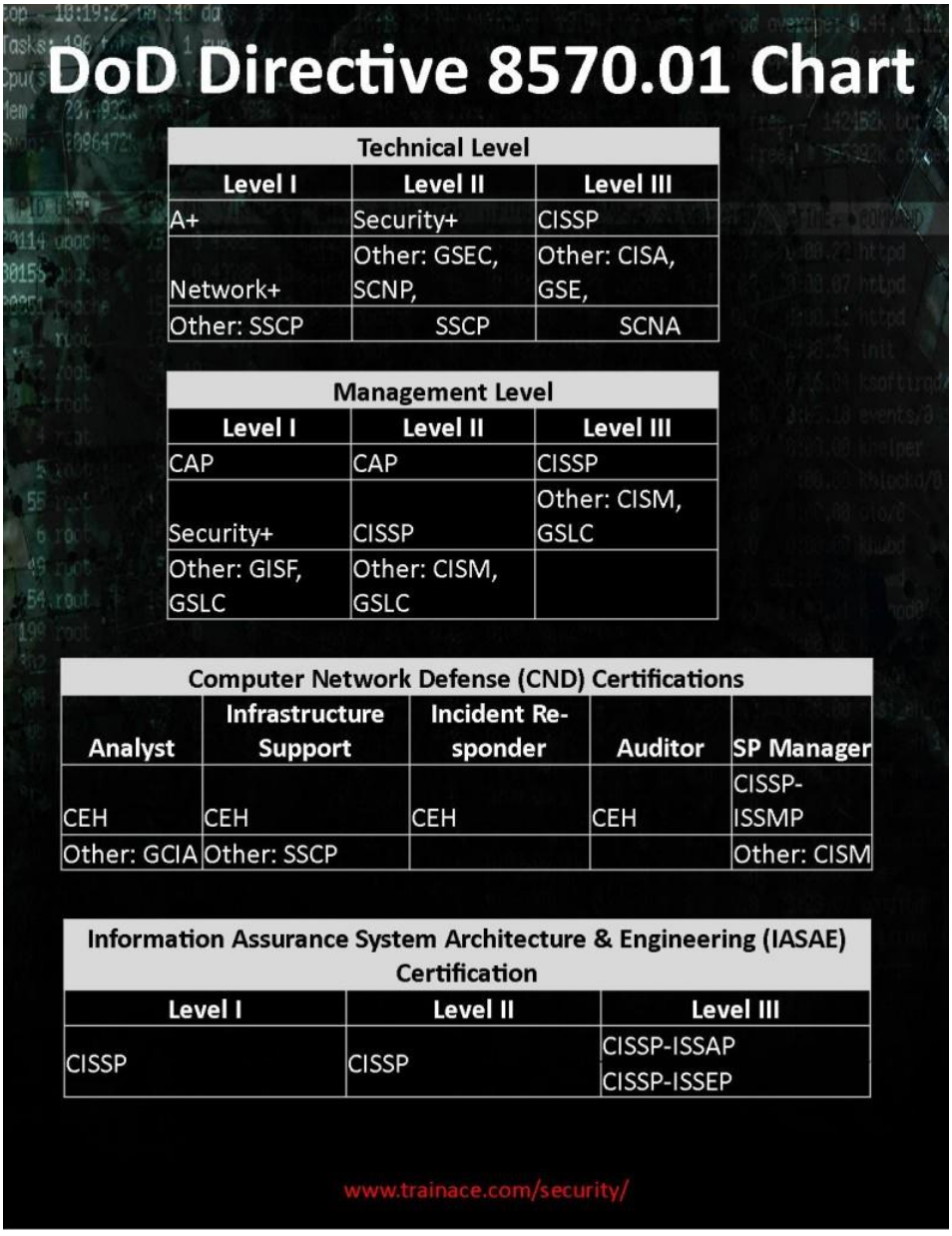
Question 3: What is the geographical and population area of responsibility? What role would volunteer in a large scale cyber-attack?

Answer: Geographically, the Hampton Roads area encompasses over 526 square miles of land. The area contains 1.8 million residents. All volunteers are to facilitate and assist. Volunteers would assist in efforts such as stabilizing networks, providing restorations of users and servers, providing path management, and many other defensive operations. All volunteers are barred from any sort of offensive or retaliatory operations as such acts are under the purvey of the federal government. Again, the cyber corps volunteers would act in only a defensive and cleanup nature and are barred from conducting any sort of offensive capabilities, which are illegal except when conducted by the federal government under certain federal provisions.

Question 4: What is the proposed structure and capabilities of the cyber corps?

Answer: Volunteers would be vetted to see what capabilities each one possesses and the then aligned with the required need. Those volunteers with leadership and the correct cybersecurity certification and experience would be expected to take on the role as team leads. Background checks would be expected to be conducted and technical competency exams would be held.

The DoD 8570 IT workforce model would be a great starting point in graphing out who has what type of capabilities based on their certification skillset. It also provides a visual of the hierarchy when comparing technicians to managers



(chart provided by trainace.com)

Question 5: What unique challenges are presented with creating a regional cyber corps?

Answer: There are expected to be multiple layers of challenges presented when attempting to develop and deploy the cyber corps in a defensive team and non-adjunct faculty role. There are expected to be issues such as private industry buy in for those companies who might be hesitant or even dismissive of the state offering to provide IT assistance during a cyber-attack. There is also expected to be regional pushback from the localities who may feel that the state is stepping into their domain of protecting their area of responsibility. Other areas that would most likely experience challenges would be in recruiting and retaining volunteers.

Question 6: What does the Hampton Roads region workforce pool offer in technical subject matter experts?

Answer: Due to the heavy precision of the military in the area, the Hampton Roads area provides offers a large potential pool of both military and civilian volunteers from companies such as CACI, General Dynamics, Northrop Grumman, and many other small cybersecurity firms.

Question 7: What other areas have successfully implemented their own cyber corps?

Answer: Currently, the state of Michigan has developed and deployed a team called the Michigan Civilian Cyber Corps or the MiC3. Tom Powers, one of the MiC3 team leads, provided this information on how their team is situated:

“The MiC3 member team thus far are providing Subject Matter Expertise around our Cyber Security training and Policy/Procedure best practices. This has proven to be very valuable to the State of Michigan (SOM). Our

cyber security foundation bar has been raised by having access to these 'Smart' and 'Experienced' SME's that the SOM probably could not afford otherwise.

Although they are contacted when we need help in creating Policy/Procedures, solving problems or even with responding to Cyber Incidents. At present they do not formally get sequestered to come on site and work with the SOM SOC. So currently we do not have any p/p in place to accommodate your liability concerns.

We are actually working through that right now. Our process:

1.) We are starting with creating a 'Volunteer Handbook'

2.) Creating a Volunteer and Employer Agreement

3.) After we have the draft approvals we will be working with the State Atty Generals office to work through the liability questions that you too are concerned with.

Currently we do a background check on every volunteer member.

Technologically our mitigation plan options are:

1.) Having a NAC system that will vet out non-compliant hardware that attached to our system to accommodate BYOD.

2.) pre-Virtual Machine assignments after their BYOD has been vetted and authorized

3.) Providing State Equipment to each member

4.) Having a pool of physical machines that are only used in case of emergency and used by 3rd party vendors or MiC3 members

5.) Having a pool of virtual machines that are only used in case of emergency and used by 3rd party vendors or MiC3 members after their BYOD has been vetted an authorized”

CONCLUSION

The creation of a Hampton Roads Cyber Corps for defensive operations during a cyber-attack affecting the Hampton Roads region could potentially benefit already in place National Guard cyber assets by providing them with additional technical resources. These same sort of non-governmental organizations resources (Team Rubicon, Red Cross, Christians in Action, etc.) are available during physical natural disasters events. The Cyber Corps could provide digital “Red Cross” assistance to constituents and private business that have been affected. The creation of a Cyber Corps could also possibly provide a positive PR moment for the region and the Commonwealth by displaying the effectiveness of communities and other partners joining together for a common good. While funding and resources are always an important hurdle to cross, there are possibly multiple funding options that may exist for funding and fielding the team. While there are multiple other areas to investigate such as hardware and software support, physical infrastructure location of a possible operations center, and questions regarding liability concerns surrounding non employees entering into the networks of private business and citizens, those previously hurdles should not deter further pursuit of fielding a team simply because a 100% solution has not fully developed as of yet. If the Hampton Road Cyber Corps were deemed a success, then this model could possibly be employed within other regions in the Commonwealth to protect the critical digital and physical resources at hand.

RESOURCES

CIVIL SUPPORT DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents
http://www.gao.gov/assets/680/676322.pdf

Cyber Security Commission First Report, August 2015 “Threats and Opportunities
https://cyberva.virginia.gov/media/4396/cyber-commission-report-final.pdf

Michigan Cyber Civilian Corps
http://www.micybercorps.org/