CYBER CONFLICT ESCALATION EXERCISE

POST CONFERENCE LESSONS LEARNED REPORT

The Cyber Security Forum Initiative (CSFI) is a non-profit organization headquartered in Omaha, NE and in Washington, DC with a mission "to provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners." CSFI was born out of the collaboration of dozens of experts, and today CSFI is comprised of a large community of nearly 18,000 Cyber Security and Cyber Warfare professionals from the government, military, private sector, and academia.

CSFI is founded on 3 main pillars supporting our mission: Collaboration, Knowledge-Sharing, and Training/Education. Our collaboration efforts have helped to break down stovepipes and "closed networks" that exists inside government and industry to enable greater information sharing and increased capabilities. We practice what we preach and have developed a capability to collaborate on special projects to breakdown, decompose, and develop threats and topics to create white papers, analytical products on unique and sophisticated cyber attacks, and not only show problems, but solutions. Such collaboration has created countermeasures that promote a stronger cyber national security posture.

Complimentary to our collaboration efforts, CSFI is engaged in creating Cyber Warfare training materials to promote a stronger background for our men and women in uniform and also throughout the cyber security community. CSFI is in a unique position to attract some of the foremost Cyber Warfare Strategists, Hackers, and Intelligence Professionals to develop high caliber training on a topic that has yet to be fully defined, let alone explored and explained.

This page left intentionally blank

TABLE OF CONTENTS

EXERCISE PARTICIPANTS

Moderators:

Nicholas Andersen
The Cyber Security Forum Initiative

Connie Peterson Uthoff
George Washington University

Panel Members:

Paul de Souza
The Cyber Security Forum Initiative

Punch Moulton
Major General (Retired) USAF
Stellar Solutions/CSFI

Victoria Ekstedt
Swedish Armed Forces

Maeve Dion
Talare

Janne Haldesten
Cybercom

Roland Heickerö
The Swedish National Defence College

Lars Nicander
The Center for Asymmetric Threat Studies, Försvarshögskolan

Christopher Taylor
CyTech Services

INTRODUCTION

CSFI recently completed development of their proprietary Cyber Tabletop Exercise, the result of months of hard work by project members around the globe. The purpose of this tabletop exercise is to highlight the need for leveraging relationships and fostering collaboration to strengthen the cyber security posture of the international community.

The first iteration of this tabletop exercise program was delivered at the Internetdagarna conference in Stockholm, Sweden on 24 October 2012, thanks to the help of CSFI Gold Sponsors CyTech Services, George Washington University, Stellar Solutions, and L3. At this conference, the distinguished panel participated in a spirited discussion on cyber warfare scenarios involving critical infrastructure, financial infrastructure and various issues arising from the employment of cyber weapons in today's world.

The panel, consisting of both Swedish and American experts, was able to create a wonderful dialogue discussing issues including matters of strategic communication, application of international laws and treaties to cyber issues, safety and security of a population and national security. Not only did the tabletop exercise provide the opportunity for conference attendees to learn from experts, but it also provided the opportunity for conference participants to interact with the panel through an audience question and answer session. Through the audience interaction, greater attention was able to be placed on local issues and issues that were of concern to conference attendees.

In the weeks following the CSFI presentation at Internetdagarna, CSFI members, panelists and moderators were given a further opportunity to review the exercise in order to determine best practices and capture information for a Lessons Learned report. Individuals were selected to pinpoint areas for improvement and isolate significant strengths to be used to shape future exercises and dialogue.

The following is the result of their findings.

Introduction to Format

The purpose of the tabletop exercise was to highlight the need for leveraging key relationships and fostering international collaboration in order to strengthen global cyber security. Collaboration, and consequently integration, between public and private entities is at the forefront of national concerns. As a result, this exercise was created to stress the importance of having well established relationships prior to the occurrence of an incident.

In this tabletop exercise, CSFI presented two scenarios, an attack on the critical infrastructure and an attack on the financial support infrastructure involving different nations. Each scenario was positioned to lead in-depth discussions on issues of collaboration, communication, development of appropriate response policy, recovery efforts, issues of jurisdiction and legality of response for both sovereign nations and international organizations such as NATO, the UN and the EU.

The exercises were presented in two separate sessions, each approximately seventy minutes in duration, with a half hour break in between. CSFI introduced the first scenario, a well-staged cyber-attack involving a welfare program in the United Kingdom during the height of a recession. The attack was presented in stages and highlighted national security concerns that might occur naturally as a result of an impending financial crisis.

This first exercise was followed by a robust panel discussion, including moderated questions related to the events as well as contributions and questions from audience participants.

After the break, CSFI led the second exercise which involved the use of cyber weapons against US oil refineries. This scenario had elements of both traditional and cyber warfare, with emphasis on the use of a cyber-attack as a force multiplier and within the context of a larger state sponsored agenda.

This presentation was also followed by a panel discussion and the floor was open to contributions from members of the audience.

BRIEF DESCRIPTION OF SCENARIOS

Scenario 1: UK Financial cyber attack

Nation State A, 5 years into an economic recession, is experiencing country-wide civil protesting because one of its programs (welfare) is no longer distributing payments. The citizens of Nation State A believe that the government, struggling to balance the budget, has run out of funds to pay the new universal credit (welfare program). Regardless of the reason, citizens who require welfare assistance have not been paid and the nation is in turmoil; people are going hungry and unable to afford food without the payments being distributed. Furthermore, the country's ATM systems appear to also be down, an indication that there may be an impending financial crisis.

In reality, Nation State A's government is scheduled to vote on further reform to the welfare system and other key social benefit programs during the following week. Currently, the government has not cancelled its welfare program, and does not yet understand why the funds are not being distributed to the respective parties. Internally, the payments appear to have been sent successfully. As a result, Nation A started an investigation into the welfare payment system and payment histories in order to understand why the payments are not being distributed. Initial findings indicate that the payment system is fully operational. Of greater concern, findings indicate that unusual network activity originating from Nation State B has coincided with payment distributions.

The investigation takes longer than expected due to a variety of factors. First, mass physical protesting against government sites prevents government employees from coming into the office. Next, recent outsourcing of key network infrastructure components to private companies has slowed the investigation, in part, because third party suppliers will not allow automatic rights of audit. Finally, suspicious network traffic from Nation State B is proving difficult to resolve because Nation State B has a 10 hour time offset. Nation State A is also having trouble tracking down the correct contacts. As a result of delays and protests, Nation State A has an increasingly difficult time with social unrest and maintaining order.

Scenario 2: Cyber Attack on US Critical Infrastructure

This cyber-attack scenario takes place in the San Francisco Bay Area. Two oil refineries are simultaneously attacked by a cyber-weapon consisting of two parts: a cyber-delivery vehicle and a DCS targeting cyber warhead.

The attacker is a nation state and its goal is to use this cyber-attack to weaken US military response capabilities and to create wide spread panic in the nation. Using this emergency situation as a means to keep the US government focused on the domestic security issues, the nation state attacker occupies an area of strategic interest for US - International security.

LESSONS LEARNED

The conflict exercise provided a dynamic foundation for discussion and collaboration among panelists and audience members alike. Initial feedback was positive and there was significant and sophisticated participation from panelists and audience members; however, like most pilot programs, we discovered minor areas for future improvement. In order to more effectively assess results, we divided the exercise into two separate areas for review: scenario based lessons and discussion based lessons.

The scenario based lessons learned section examines potential areas for improvement to the scenarios themselves. We reviewed content, flow, accuracy and function. The discussion based lessons learned section suggests items for improvement in relation to dialogue, collaboration, participation and necessity. For this report, only some of these topics are addressed.

Scenario Based Lessons Learned

The scenarios were well constructed, based in part on actual events and had an impressive level of technical sophistication that lent to the credibility of the exercises. The storylines were complex and represented deep issues that require serious consideration; however, there were some areas for minor improvements. They include the following:

1. It is important that future scenarios reflect a deeper understanding of the political, diplomatic and military context/relationships among nations and how they may or may not influence how events unfold. (i.e. US-Sino)
2. In regards to time and focus, it may be more constructive to have one scenario per panel discussion. Another suggestion was to create one scenario that builds increasingly toward a more escalated cyber- attack.

3. The conference was not inherently security-driven. Though this initial presentation had a good audience base, this type of exercise would also be very well suited for a cybersecurity focused event.
4. It is important to make sure that the scenarios do not appear to focus too narrowly on domestic issues as that may limit opportunities for international discussion and collaboration.
5. Though the presentations were extremely technology savvy, it is important to double check other facts. One scenario missed a key point concerning US oil partners. This impacts the reality/credibility of portions of the exercise.
6. It is important to shape the exercise to include areas that are not currently covered by international laws and treaties (i.e. LOAC). It is also essential to move away from cyber events that are mostly covered by domestic laws, treaties and jurisdiction in order to include discussion of issues that also involve international organizations.

Discussion and collaboration based

One purpose of this exercise was to discover, through dialogue, a more effective approach to secure the cyber environment and to examine areas of appropriate response, recovery and jurisdiction. In several ways, this panel of experts represented a microcosm of the greater/macro conversation. The discussion that followed each exercise included robust dialogue about real and pressing cyber issues as well as some pitfalls to conversation, much like those in the larger global community. CSFI was fortunate to share the panel with highly knowledgeable and engaged participants; resulting in significant and essential contributions from both panelists and the audience.

Some key takeaways from the panel include:

1. Discussing the 'international community' as though it is one body limits conversation and is basically a poor approach. To thoroughly engage, questions and conversation should be more specifically focused to include the roles and relationships of various international bodies.
2. One suggestion for future exercises was to expand the range of panel experts and to include other areas of expertise to the conversation (i.e. a SCADA expert). The current panel was full of brilliant subject matter experts, but other exercises might call for added points of view depending on the end goal.
3. An insight about the importance of doctrine and dialogue: It was easy to see that as scenario events were unfolding in real time, it would be difficult if not

impossible to shape or determine lasting strategy in the midst of crisis. Domestic and international approach, partnerships and doctrines should be created prior to an event in order to minimize the potential damage of such an attack.

4. One sobering comment: In regards to the nature of policy/doctrine making nations are collectively slow, though advances in cyberspace are not. It may take a major cyber event to be the catalyst for collaboration and the creation new policies, treaties or doctrine. Examples include Pearl Harbor, Hiroshima, 9/11. The necessity for action is now, but it may not reflect the reality.
5. Due to time constraints, there were many international issues related to the scenarios that were not addressed, but could be (should be) at a future time.
6. Deeper issues involved unaddressed concerns around how a government and/or its allies should collectively respond to cyber-attacks from non-state actors against the private sector; against an ally or a partner. Related questions include: How can we further develop public/private partnerships? Is that the right question or approach? What does collective self-defense look like in cyber-space? How do we address the growing threat against the critical infrastructure?
7. Need for more discussions. The panel was clear that the dialogues held in Sweden were by no means final, but rather a beginning. There is an overwhelming consensus that there is a pressing need for further conversation.

.

Final Thoughts

One goal of the Cyber Conflict Escalation Exercise was to 'stress the importance of having well established relationships prior to the occurrence of an incident.' In this respect, the exercise was highly successful. The scenarios also helped to reinforce the overwhelming need for continued dialogue. It is essential to discuss these critical and pressing issues as well as their impact on local, national and international security. (And, we must act!). Challenges in cyberspace, which include exponentially developing threats and attack surfaces, will not wait for policy, laws or collaboration to catch up. The time for discussion is now.

.

ACKNOWLEDGEMENTS

CSFI would like to thank the following contributors. These individuals contributed to the Scenarios and without their tireless work, the exercise would be incomplete.

Ian Ahl, CISSP
Sr. Securtiy Engineer
Jorge - Cyber Solutions Group

Nicholas Andersen
Chief Security Officer
Cyber Security Forum Initiative

Prof. William Butler
Graduate School of Information Assurance
Capitol College

Marco Carter, CCNA, C|EH, C|HFI
Sr. Network Security Engineer

David Escaloni
Systems Administrator, MCTS
Texas Conference of Urban Counties

Rick A. Gilmore, CISSP CISO

Michael Harrison
Gentoo Security Contributor

James Keegan, CISSP
US Financial Sector (Private)
Information Security Officer

Lydia Kostopoulos, PhD
Political/Security Strategy Contributor

Laura Kraft

Mark O'Brien, MSIT-IA
Kansas Army National Guard CND

Kimberly Sanders, CISSP

Mark Stanhope
Senior Executive Secretary (EMEA Region)
Cyber Security Forum Initiative-CWD

Prof. William Stauffer Telles, CDFI
NID Forensics Academy

Monte Toren, CISSP, CISA, CISM, CCSK
Owner, Cryptix.com Security, LLC

David Willson
Attorney at Law
CISSP, Security+
Titan Info Security Group