46th Test Squadron Detachment 2

War-winning Capabilities…On Time, On Cost

U.S. AIR FORCE

Offensive Cyber Operations (OCO) Range Vision

Lt Col Shelly Bruemmer
Ms. Carrie Hernandez
46th Test Squadron, Det 2
14 November 2013

This presentation is classified:

UNCLASSIFIED

Overview

War-winning Capabilities…On Time, On Cost

- Introduction
- Intelligence and Cyber Operations
- OCO Capability Development Approach
- OCO Cyber Range Methodology
- Characteristics of an OCO Cyber Range
- Recommendations

Introduction

War-winning Capabilities…On Time, On Cost

- **What's so challenging about range environments for Offensive Cyber Ops?**
- Test and training environments for cyber must be flexible, reliable, representative of the operational environment, have high technical fidelity, and allow for instrumentation, data collection and monitoring and control

  .....and not cost more than all of the capabilities they support!
- Cyber capabilities are complex but generally low dollar efforts
  - Thousands versus millions of dollars – very few ACAT 1D systems
  - Thousands versus millions of lines of code
- Meeting all of these requirements presents a significant challenge to the organizations that support offensive cyber operations testing and training
- And…. the intelligence products required to create a cyber range that meets the above criteria are frequently unavailable, insufficient or not timely enough to meet the demands of the operational community.
- So, what to do?

Intelligence and Cyber Operations

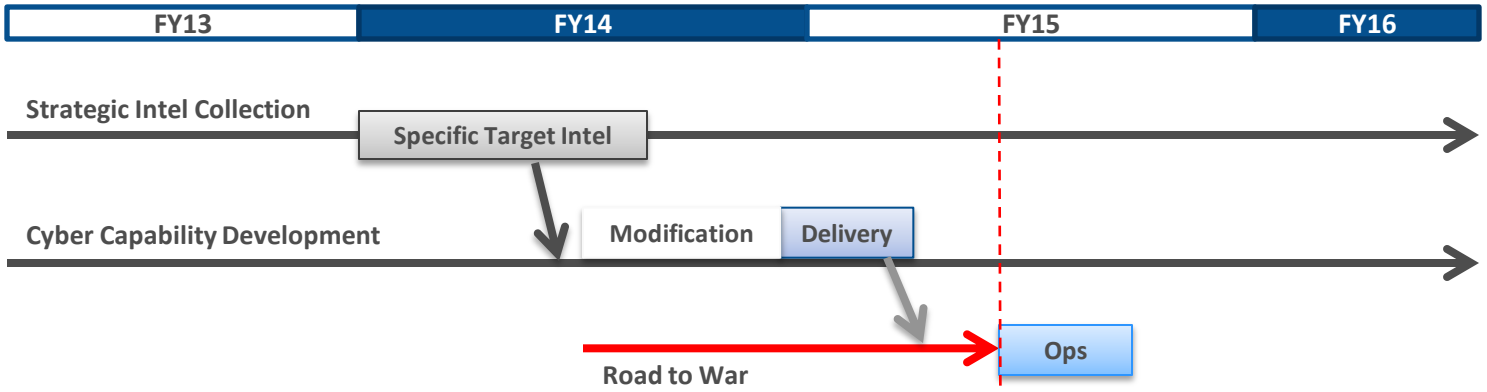
War-winning Capabilities…On Time, On Cost

- **Intelligence for cyber capability development, testing and operations is fundamentally no different than any other domain, but required data is often more complex, detailed, variable, and time-sensitive**
  - Intelligence requested at the beginning of the effort is not likely to match the intelligence needed at the time of operational fielding
  - Capabilities tailored for specific cyber targets cannot currently be produced in time to meet operational need
- **One solution to this problem is to build configurable OCO capabilities against classes of devices, i.e., routers, switches, operating systems, etc.**
  - The majority of the capability can be developed in advance of any operational need using generic intelligence, commercial best practices, industry standards and solid technical assumptions
  - The capability can be modified as specific intelligence is produced or operational demand dictates
  - Performing minor modifications to an OCO capability is timelier than starting a major acquisition on short notice

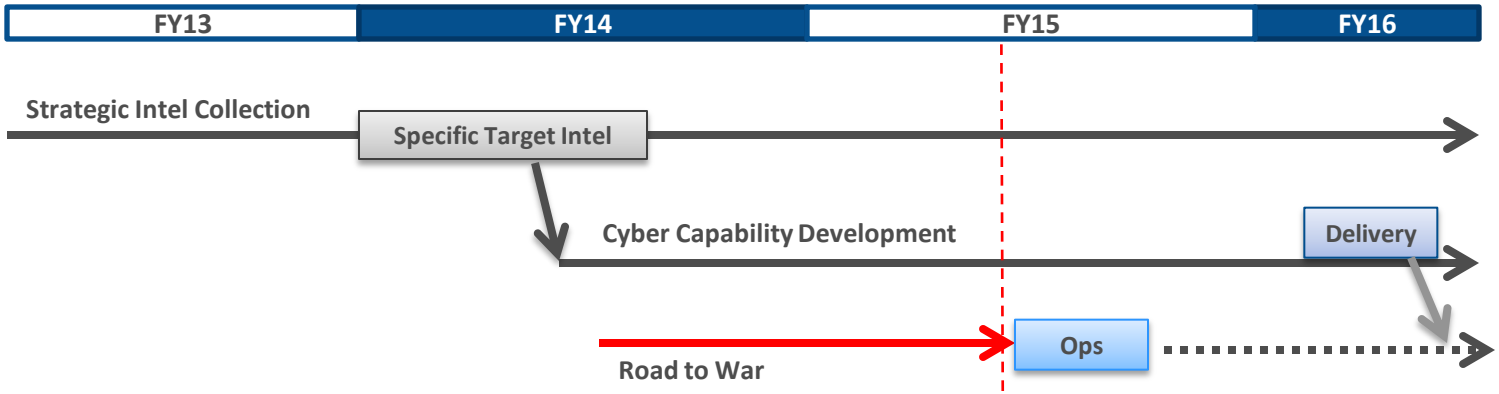
Intelligence and Cyber Operations

War-winning Capabilities…On Time, On Cost

- **Approach #1 – Build and Modify**



- **Approach #2 – Wait for target specific intel**



OCO Capability Development Approach

War-winning Capabilities…On Time, On Cost

- **Technical assumptions about communication system architectures based on limited intelligence, commercial best practices and industry standards used in adversary countries should be used as a starting point for any development**

- **Capability development against classes of hardware/software used in the IT industry takes advantage of the fact the companies prefer their platforms/firmware be standardized and consistent**

- **The general categories for communications equipment are *Core*, *Edge* and *End User***
  - ***Core*** network components (big routers, long haul comms) are typically the last thing to change in any network.
    - Small variety of commercial vendors and types of equipment
    - Development or purchases are useful against multiple adversary networks
  - ***Edge*** network devices (smaller routers, switches, encryptors, etc.) are more reliant on specific and detailed intel to build an effective OCO capability
    - Large variety of commercial vendors, equipment types
  - ***End user*** devices (servers, operating systems, applications, etc.) are the easiest items to acquire and the most difficult to collect validated intelligence on adversary use

OCO Cyber Range Methodology

War-winning Capabilities…On Time, On Cost

- **Cyber ranges face similar issues to those presented for OCO capability development**
  - Need to be flexible, configurable, distributed architectures that can operate at multiple security levels
  - Require varying levels of realism dependent on the specific activity requested, such as demonstration & exercises, developmental testing, operational testing or training & mission rehearsals
    - *For example, it is more important for a cyber range used for developmental test to be technically representative than operationally realistic*
  - Intended use drives the relative importance of different range characteristics
  - Building ranges that meet all of these criteria in a timely and cost effective manner is the key challenge facing range providers

Characteristics of an OCO Cyber Range

War-winning Capabilities…On Time, On Cost

- **Scale:** The complexity and size of a cyber range
  - Impractical to build a single range configuration that represents any and all possible range environments for a single adversary or mission area
- **Flexibility and Sustainability:** Ability to change quickly and be used over a sustained period of time
  - Designing the environment so that it can be modified in a cost effective and timely manner is critical
- **Interoperability:** Ability to connect or integrate with other ranges
  - Connectivity to Joint Mission Environment Test Capability (JMETC), Joint IO Range (JIOR) and/or capability to physically integrating components into other range environments
- **Security:** Ability to build range configurations at any security level required for an event
  - Limited number of approved technical solutions approved that allow multiple events to occur on the same range at different classification levels
- **Availability:** Ability to support multiple projects with constantly changing operational needs and acquisition timelines
  - Cyber ranges require enough capacity to support multiple range events simultaneously

Recommendations

War-winning Capabilities…On Time, On Cost

- **Build configurable OCO capabilities against classes of devices, i.e., routers, switches, operating systems, etc.**
  - Modify as specific intelligence is produced or operational demand dictates

- **Invest in technologies that improve scale, flexibility, interoperability, security and availability of cyber ranges**
  - Virtualization
  - Hardware Emulation
  - Connectivity
  - GOTS instrumentation
  - Security solutions, policies, procedures