NDIA

The Cyber Secret SoS

Cyber Resiliency Across Foreign System of Systems

Eric Conyers and Rahul Parwani

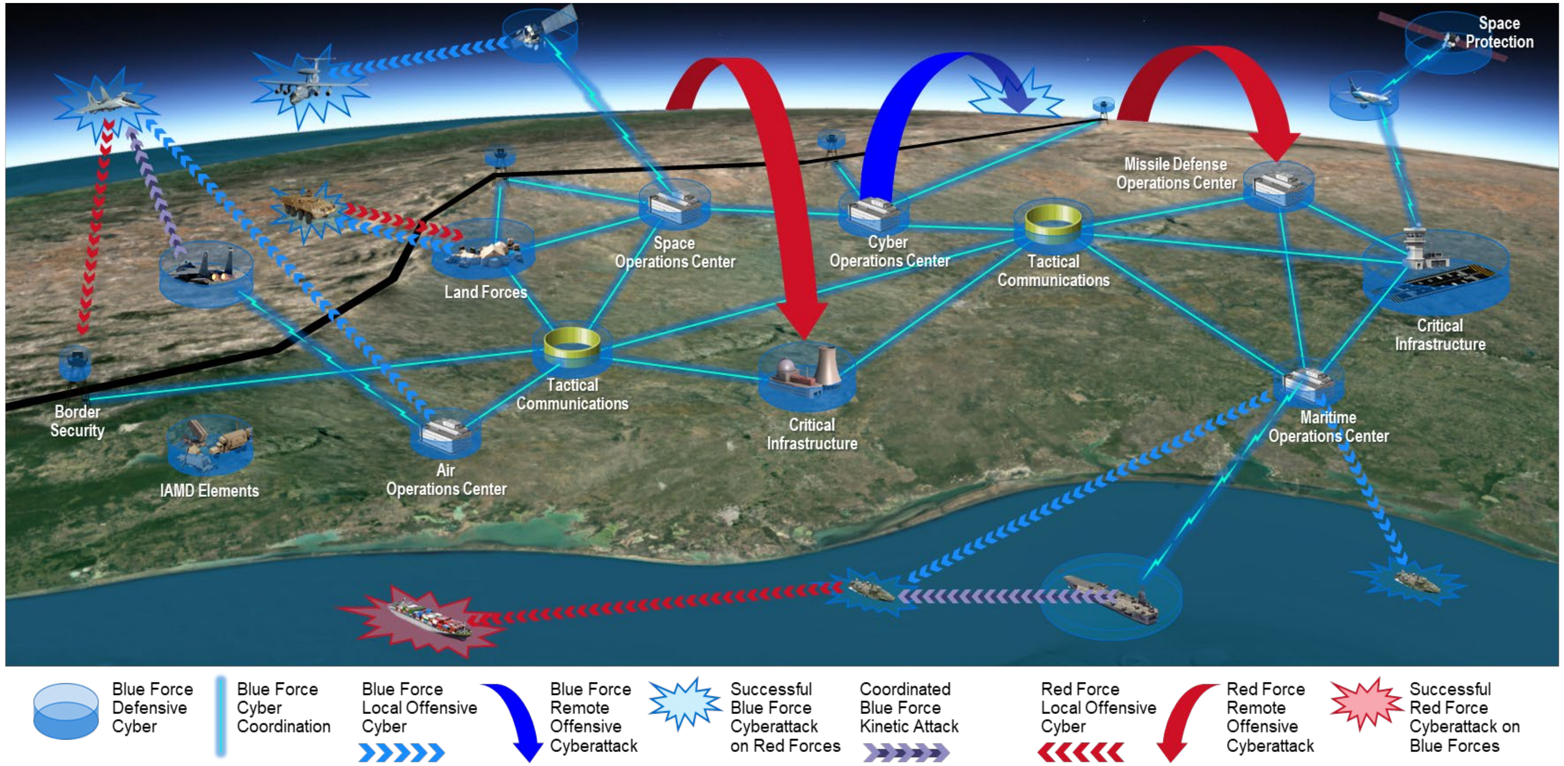
11/18/2024

The Cyber Secret SoS

OVERVIEW

The Cyber Secret SoS

- **Battlespaces are evolving into interconnected System of Systems (SoS) for mission management**
  - Coalition partners
  - Regional partner nations
- **With each interconnected Foreign SoS the threats increase**
  - Each system is reliant on others to protect boundaries or distributed networks
- **Unified Cyber Resiliency approach is needed for consistency and assured interoperability**
  - Flexible high-level approach to achieve cyber resiliency
- **Not all SoS environments are the same**
  - What works for one solution may not work for another


Space Protection
Missile Defense Operations Center
Space Operations Center
Cyber Operations Center
Tactical Communications
Land Forces
Critical Infrastructure
Border Security
Tactical Communications
Critical Infrastructure
Maritime Operations Center
IAMD Elements
Air Operations Center
Blue Force Defensive Cyber
Blue Force Cyber Coordination
Blue Force Local Offensive Cyber
Blue Force Remote Offensive Cyberattack
Successful Blue Force Cyberattack on Red Forces
Coordinated Blue Force Kinetic Attack
Red Force Local Offensive Cyber
Red Force Remote Offensive Cyberattack
Successful Red Force Cyberattack on Blue Forces

Plan, execute, and sustain defensive and offensive cyber operations, integrated with kinetic battle to achieve commander's intent

The Cyber Secret SoS

POLICY: DEVELOPMENT AND STANDARDIZATION

The Cyber Secret SoS – Policy

- Definition of standards and requirements flow is critical to Foreign SoS cybersecurity alignment
- Overarching requirements and commonality must be established
  - Extremely critical for atypical deployments like in many Foreign Partners
  - Disparate requirements between nations (RMF, ISO 27000 series, NATO NCF, etc)
- Identify boundaries and gain alignment of common enterprise services/requirements (must be documented and well understood by all stakeholders)
  - Establish classifications and identify where Cross Domain Solutions (CDS) are required and owners of such devices

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

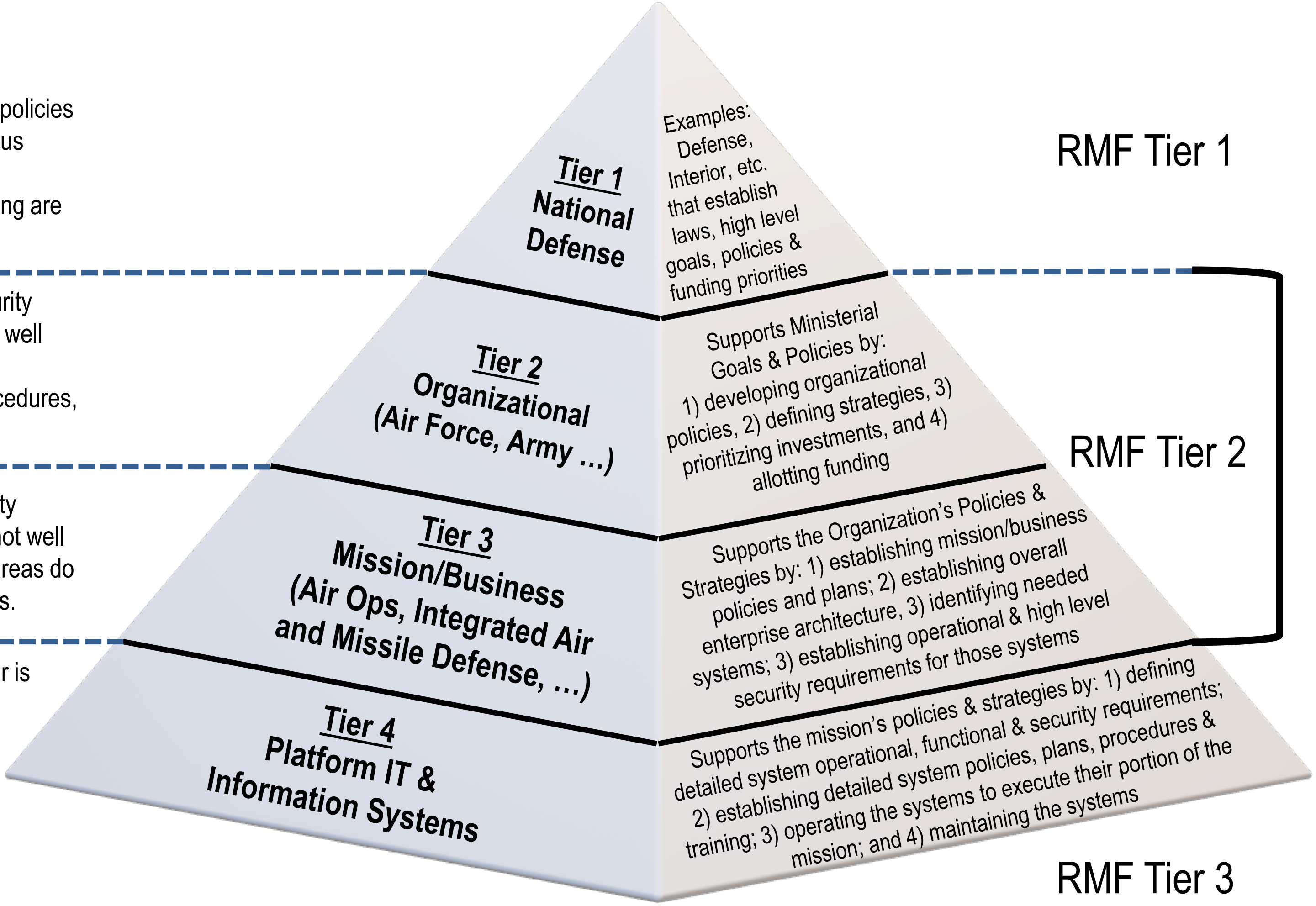
The Cyber Secret SoS – Policy

High level National Defense security policies and strategies typically exist for various armed forces Typically no lower level security plans, procedures, and training are developed.

The existence of Organizational security policies and plans, in general are not well understood in foreign environments. Typically no lower level security procedures, and training are developed.

The existence of Mission level security policies and plans are, in general is not well understood. Some nations' Mission areas do have a few security policies and plans.

This the level that each system owner is developing Security Policies, Plans, Procedures and Training



Tier 1
National Defense

Examples: Defense, Interior, etc. that establish laws, high level goals, policies & funding priorities

Tier 2
Organizational (Air Force, Army …)

Supports Ministerial Goals & Policies by: 1) developing organizational policies, 2) defining strategies, 3) prioritizing investments, and 4) allotting funding

Tier 3
Mission/Business (Air Ops, Integrated Air and Missile Defense, …)

Supports the Organization's Policies & Strategies by: 1) establishing mission/business policies and plans; 2) establishing overall enterprise architecture, 3) identifying needed systems; 3) establishing operational & high level security requirements for those systems

Tier 4
Platform IT & Information Systems

Supports the mission's policies & strategies by: 1) defining detailed system operational, functional & security requirements; 2) establishing detailed system policies, plans, procedures & training; 3) operating the systems to execute their portion of the mission; and 4) maintaining the systems

RMF Tier 1

RMF Tier 2

RMF Tier 3

Cybersecurity Governance for Mission Systems atypical of standard DoD Structures

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

The Cyber Secret SoS

TECHNICAL IMPLEMENTATION

The Cyber Secret SoS – Technical Implementation

Common Controls Set Across all SoS Entities

- **Establish requirements and overarching documents for SoS**
  - Even if only Minimum Viable Product (MVP)
- **Establish the criteria and the risk assessment used for the environment**
  - Identify Critical Components (CC) and Critical Program Information (CPI)
- **Establish a SoS System Security Plan or Cybersecurity Implementation Plan identifying the key requirements and approach**
  - Identify and establish common security controls and capabilities that all systems can leverage
- **Identify tailoring process for different types of mission systems**
  - Tailor to organizational structure

Cyber Resiliency on Multiple Levels

- **Policy Governance across different types of systems**
- **Technical implementation**
  - A threat to one system is a threat to all in a SoS model
  - Cybersecurity governance/Security Oversight is critical in this model
- **Partner Mission Systems must protect the SoS environment and their own systems**
- **Common understanding of layers and protection**
- **Threats must be evaluated both at the SoS layer and correlated at each individual system**
- **Coordinate system wide and individual system vulnerability assessments to understand risk and best practices**

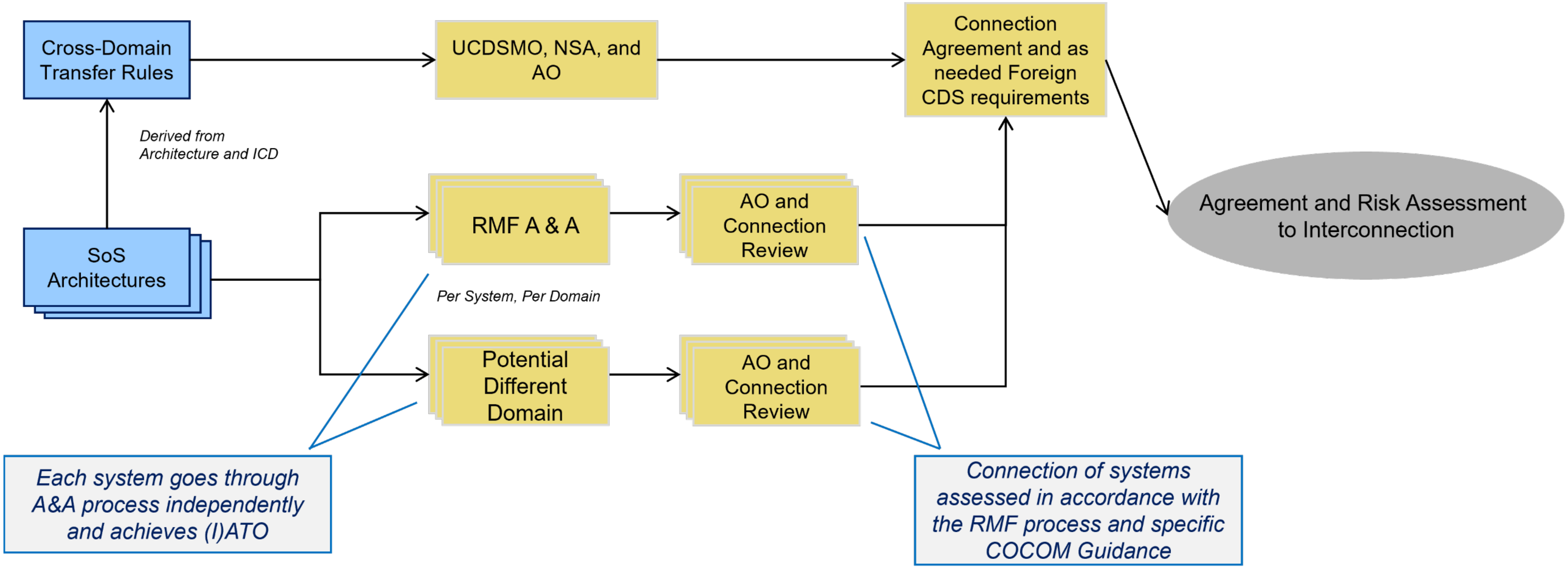
Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

The Cyber Secret SoS – Technical Implementation

- Overarching approach follows DODI 8500.01 Cybersecurity Policy
- Employs DoDI 8510.01 DoD IA Risk Management Framework (RMF) for DoD Information Technology (IT)
- Employs the CNSSI 1253 Security Controls as the “standard”
- Includes tailored inputs from NATO National Cyber Security Framework and ISO 27001/27032
- Assess and Authorize (A&A) (Formerly C&A) is done independently for each domain (classification level)
    - Each system implements Cyber protections and is independently assessed and then authorized by the corresponding Approval Authority (AO) with SoS direction and final risk acceptance
    - Connections between systems are mutually authorized by the corresponding AOs, in accordance with a risk management assessment process
- SoS Owner needs to provide common services and governance to the rest of the systems
- This process is not commonly aligned across different countries

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

The Cyber Secret SoS – ATC and ATO Example


Cross-Domain Transfer Rules
UCDSMO, NSA, and AO
Connection Agreement and as needed Foreign CDS requirements
Derived from Architecture and ICD
RMF A & A
AO and Connection Review
Agreement and Risk Assessment to Interconnection
SoS Architectures
Per System, Per Domain
Potential Different Domain
AO and Connection Review

Each system goes through A&A process independently and achieves (I)ATO

Connection of systems assessed in accordance with the RMF process and specific COCOM Guidance

It is through the System Connection process that we apply the DODI 8500.01 and COCOM Direction Cybersecurity process across the SoS

Each system is different, the process remains the same

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

The Cyber Secret SoS

TRAINING APPROACH

The Cyber Secret SoS – Training Approach

Unified Training Approach for Success

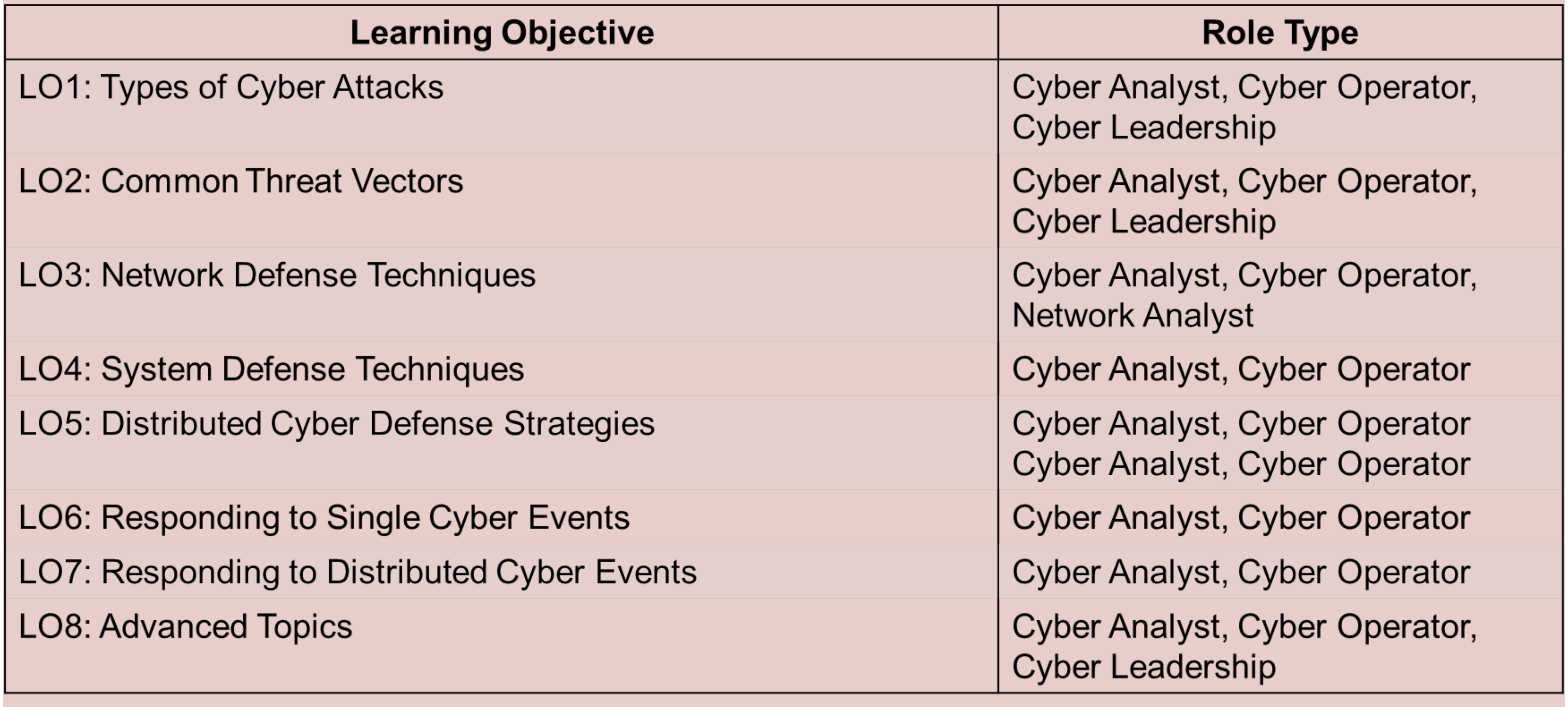
- Establish Fundamental Training Requirements and Roles
- Understand Roles and Responsibilities
- All Nations Receive Same Training Curriculum
- Simulate Day-to-Day activities
- Real World Scenarios for Training
- Identify external training requirements and pre-requisites

Image Source: https://d1ldvf68ux039x.cloudfront.net/thumbs/photos/0911/224817/1000w_q95.jpg

Unified training approach ensures operational success

The Cyber Secret SoS – Training Approach

Example Learning Objectives by Role Type



Learning Objective	Role Type
LO1: Types of Cyber Attacks	Cyber Analyst, Cyber Operator, Cyber Leadership
LO2: Common Threat Vectors	Cyber Analyst, Cyber Operator, Cyber Leadership
LO3: Network Defense Techniques	Cyber Analyst, Cyber Operator, Network Analyst
LO4: System Defense Techniques	Cyber Analyst, Cyber Operator
LO5: Distributed Cyber Defense Strategies	Cyber Analyst, Cyber Operator Cyber Analyst, Cyber Operator
LO6: Responding to Single Cyber Events	Cyber Analyst, Cyber Operator
LO7: Responding to Distributed Cyber Events	Cyber Analyst, Cyber Operator
LO8: Advanced Topics	Cyber Analyst, Cyber Operator, Cyber Leadership

All nations receive common training curriculum to ensure cohesive collaboration

The Cyber Secret SoS – Training Approach

- Cyber for Foreign SoS takes time and planning

- When done right and aligned to a centralized methodology, it can reduce risk for all connected systems

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

BIOs

Rahul Parwani, Cybersecurity Technology Area Lead and Deputy Product Cybersecurity Officer

Rahul Parwani is a recognized subject matter expert and leader in cybersecurity supporting Systems Engineering and Cybersecurity roles across Raytheon. His current roles include Raytheon Cybersecurity Technology Area Lead (TAL) and Deputy Product Cybersecurity Officer (PCO), providing Product Cyber Direction and Strategy, and he is recognized as a cybersecurity SME within both Raytheon and external communities such as United States Government (Air Force Life Cycle Management Center (AFLCMC), US Central Command, NAVSEA and Army Project Offices), and Foreign Military (Qatar Armed Forces).

E-mail: Rahul.Parwani@rtx.com

Eric Conyers, CISSP

Eric Conyers is a Senior Principal Systems Engineer for Raytheon, currently serving as the Cyber Technical Lead for the Raytheon C5i Product Line. He is a veteran of the US Air Force and joined Raytheon in 2019. He has held a variety of cyber and systems engineering roles throughout his career. Eric holds Bachelor’s of Science degree in Computer Information Systems – Information Security from DeVry University, he is also CISSP certified.

E-mail: eric.m.conyers@rtx.com

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.