C-SCRM & Asset Management

Supply Chain Attack Vector Illumination

Ms. Julienne Picot Chappell, SAF/CNZP

DAFITC 2025

Topics

- Asset Management Introduction
- Inventory
- Configuration Assessment
- Authenticity
- Source Evaluation
- Automation

Asset Management Introduction

- C-SCRM requires visibility and comprehensive enterprise-wide grasp of Information and Communications Technology (ICT) infrastructure components and structure.
- Without a complete asset inventory, consistently identifying potential vulnerabilities and assessing supply chain attack vectors is not attainable.
- Asset related C-SCRM imperatives are addressed in numerous executive and statutory issuances, including:
  - EO 13757, *Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*
  - EO 14028, *Improving the Nation's Cybersecurity*
  - (Amended) EO 14144, *Strengthening and Promoting Innovation in the Nation's Cybersecurity*
  - Proposed House ROUTERS act - This bill requires the National Telecommunications and Information Administration to conduct a study on the national security risks posed by consumer routers and modems (including devices that combine a modem and router) and provide the results of the study to Congress. The study must address devices developed, manufactured, or supplied by persons (i.e., individuals and entities) owned by, controlled by, or subject to the influence of China, Iran, North Korea, or Russia.

Scenario

- A supply chain threat is identified, rising to National prominence in the news. A common ICT device supply was subverted, resulting in device tampering and counterfeit substitution prior to customer delivery.
- Congress issues a request for information on:
  - Potential impacts from compromised devices
  - Found compromised incident counts
  - Remediation actions taken
- Response required within 5 days

Baseline Inventory Capability – Bare Minimum

- Network endpoint identification
- Make / Model / Serial Number
- Accountability
- System Assignments

- CM-2 *(Baseline Configuration)*
- CM-8 *(System Component Inventory)*
- CM-8(4) *(Accountability Information)*
- CM-8(9) *(Assignment of Components to Systems)*

Comprehensive Asset Inventory

- Minimum Baseline
- Stand-alone asset capture
- Product ID (PID)
- Device analysis
  - Sub-component identification (compare to HBOM)
- Configuration scanning
- Inventory de-duplication
- Automation & Repository

- CM-2 *(Baseline Configuration)*
- CM-2(2) *(Automation Support for Accuracy and Currency)*
- CM-8 *(System Component Inventory)*
- CM-8(1) *(Updates During Installation and Removal)*
- CM-8(2) *(Automated Maintenance)*
- CM-8(3) *(Automated Unauthorized Component Detection)*
- CM-8(4) *(Accountability Information)*
- CM-8(6) *(Assessed Configurations and Approved Deviations)*
- CM-8(7) *(Centralized Repository)*
- CM-8(8) *(Automated Location Tracking)*
- CM-8(9) *(Assignment of Components to Systems)*

Configuration Assessments

- Compliance
  - Comply to connect
  - Zero Trust overlay controls
  - CVE remediation and patching
- Specs comparison
  - Benchmark checking
  - Found vs documented
- Behavior monitoring
  - Power / Heat / Fan performance levels
  - Communications

- CM-7 *(Least Functionality)*
- CM-7(2) *(Prevent Program Execution)*
- CM-7(4) *(Unauthorized Software – Deny-by-exception)*
- CM-7(5) *(Authorized Software – Allow-by-exception)*
- PE-20 *(Asset Monitoring and Tracking)*
- RA-20 *(Vulnerability Monitoring and Tracking)*
- SI-2 *(Flaw Remediation)*
- SI-4 *(System Monitoring)*

Authenticity Assessments

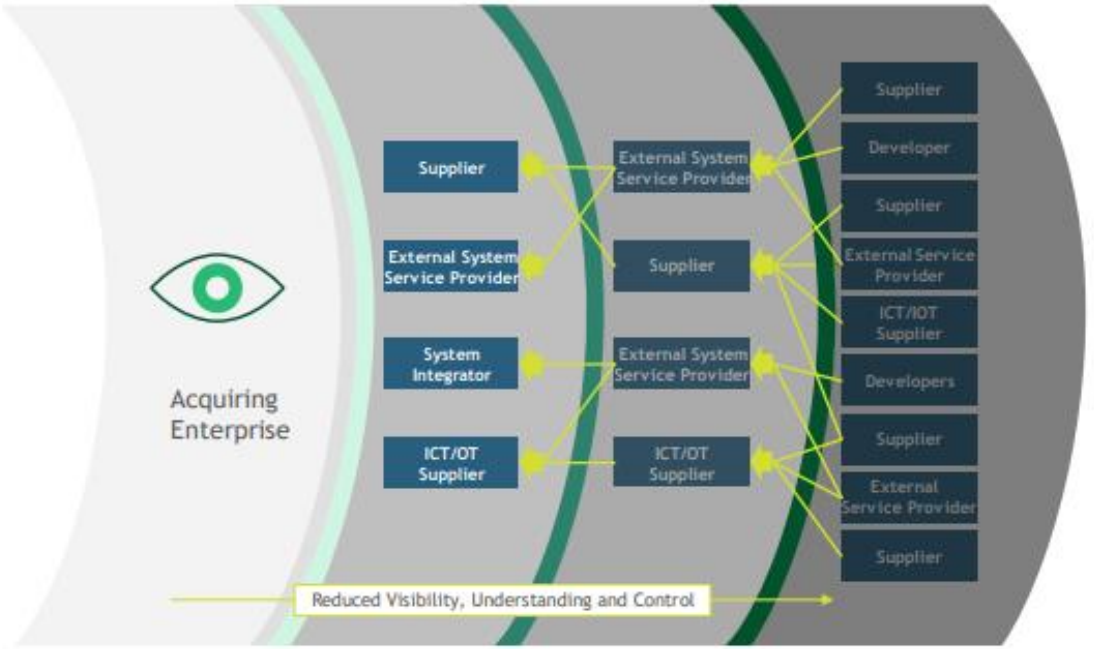
- Device sub-component validation
- Chipset verification
- Firmware verification
- Software image verification
- BOM verification

- CM-8(3) *(Assessed Configurations and Approved Deviations)*
- RA-5 *(Vulnerability Monitoring and Scanning)*
- SI-7 *(Software, Firmware, and Information Integrity)*
- SR-4 *(Provenance)*
- SR-4(3) *(Validate as Genuine and not Altered)*
- SR-11 *(Component Authenticity)*

Source Evaluation

- Restricted suppliers
  - Statutory or regulatory acquisition restrictions
- Device and sub-component vendors
- White-list / White Label
  - Original source identification
  - Devices or sub-components
  - (within a defined degree of confidence)

- SA-4 *(Acquisition Process)*
- SA-12 *(Supply Chain Protection)*
- SR-4 *(Provenance)*
- SR-4(4) *(Supply Chain Integrity - Pedigree)*



Automation

- API capable asset mgmt. tool
  - Two-way traffic
- Continuous monitoring
  - Network scanning
  - CVE impacts
- A&A package integration
  - System assignments
  - POC accountability
  - Incident alerting
  - POA&M remediation
- Non-cooperative BOM generation

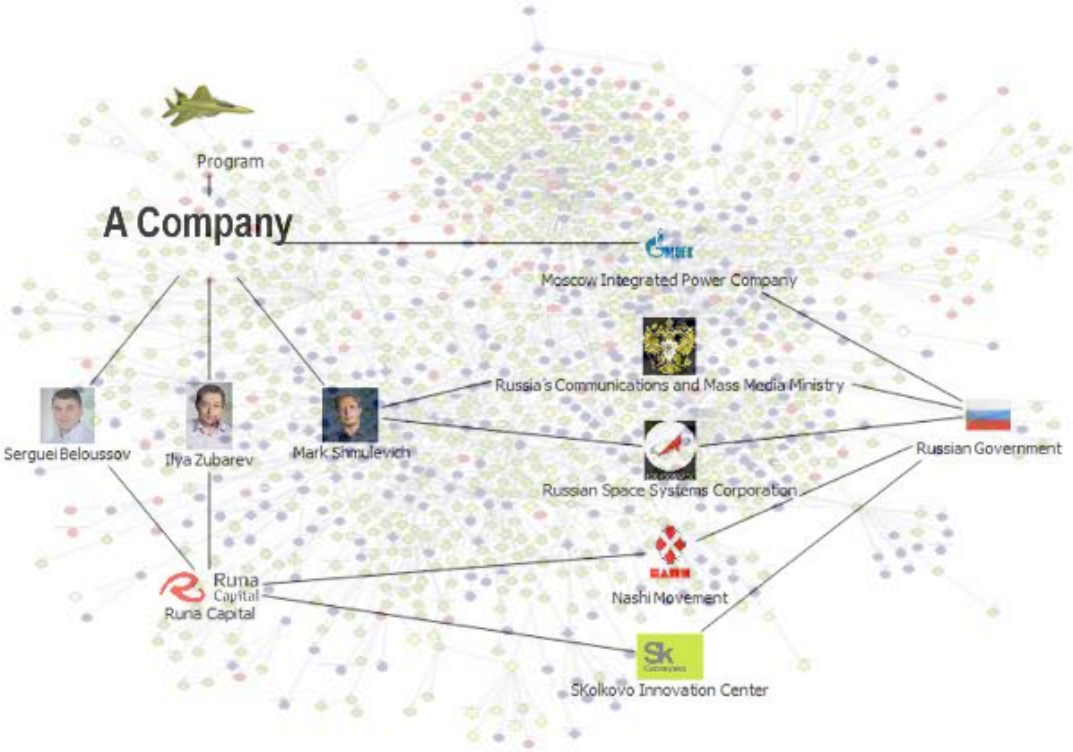
- *Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders*
- *GV.SC-03: C-SCRM is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes*
- *GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship*
- *GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle*

Questions?

julienne.chappell@us.af.mil

Supply Chain Complexity

- System interdependencies increase Enterprise risk exposure
- Massive, complex, geographically disbursed, multi-tiered supply chains
  - Thousands of entities, large supplier eco systems
  - Multi-hemispheric, widely dispersed supply chains
    - A Company - example down to 4th tier
    - Suppliers are plotted across the globe and each of these suppliers are assessed through the 8 SCRM lenses to identify risks to the weapons systems
    - Red dots on the map indicate a high risk throughout exposure

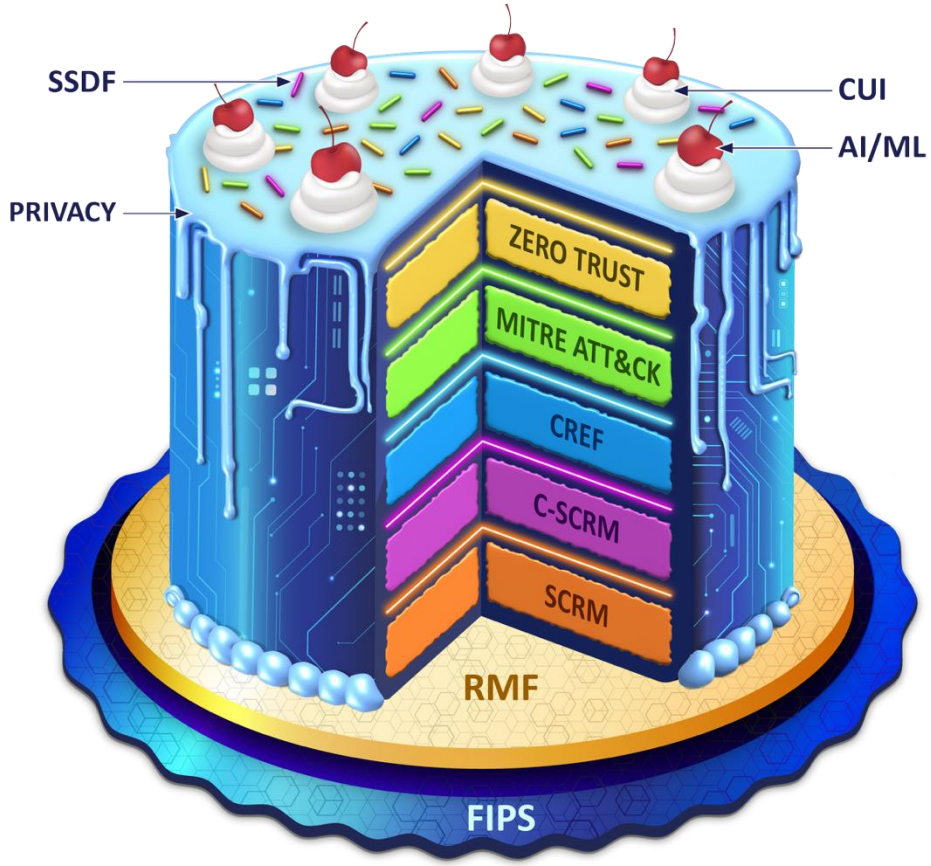


Acquisition Intersections

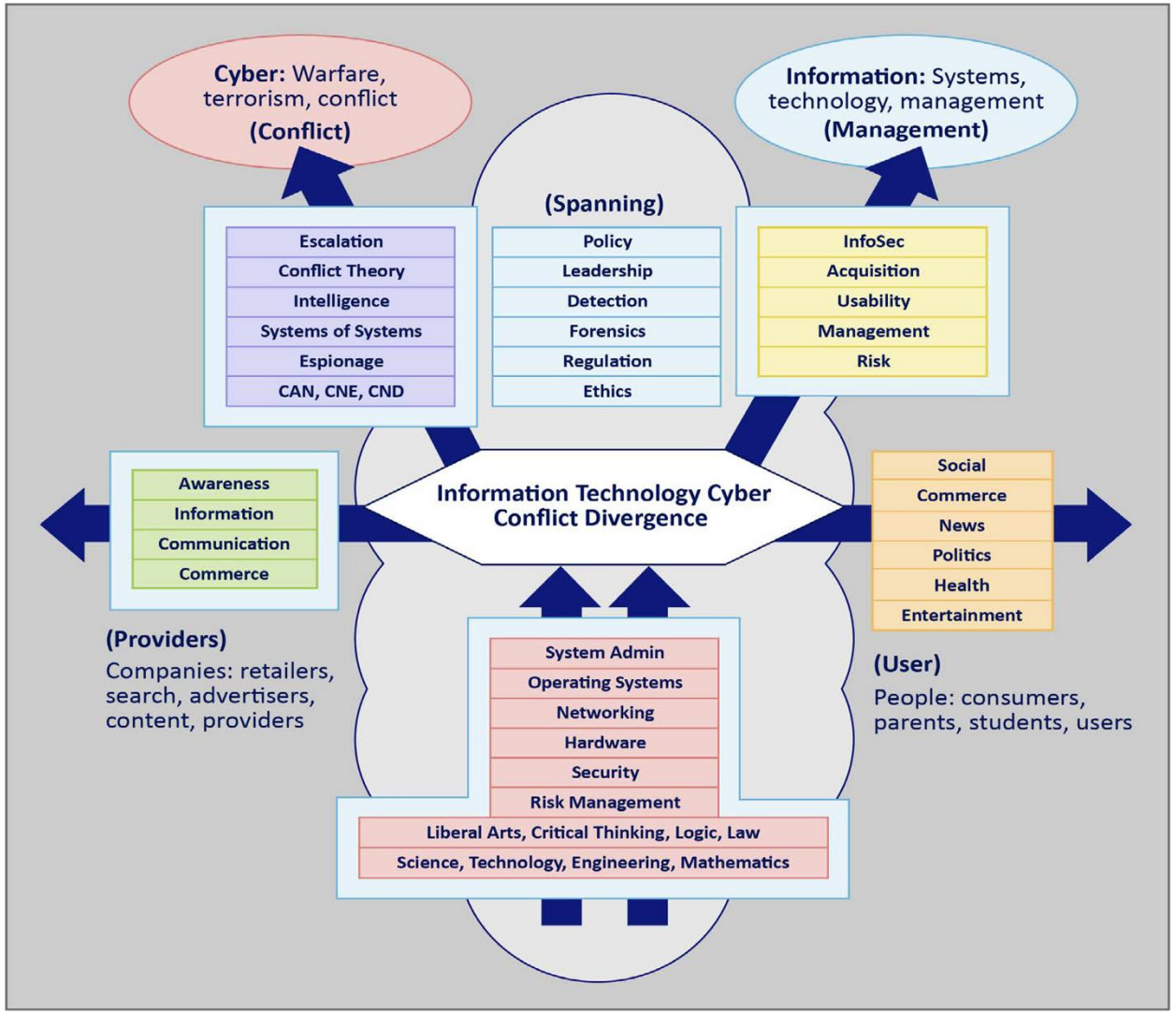
Source of Supply, Product, or Service Characteristics	Risk Indicators, Analysis, and Findings
• Features and functionality • Access to data and information, including system privileges • Installation or operating environment • Security, authenticity, and integrity of a given product or service and the associated supply and compilation chain • The ability of the source to produce and deliver a product or service as expected • Foreign control of or influence over the source (e.g., foreign ownership, personal and professional ties between the source and any foreign entity, legal regime of any foreign country in which the source is headquartered or conducts operations*) • Market alternatives to the source • Provenance and pedigree of components • Supply chain relationships and locations • Potential risk factors, such as geopolitical, legal, managerial/internal controls, financial stability, cyber incidents, personal and physical security, or any other information that would factor into an analysis of the security, safety, integrity, resilience, reliability, quality, trustworthiness, or authenticity of a product, service, or source	• Threat information includes indicators (system artifacts or observables associated with an attack), tactics, techniques, and procedures (TTPs) • Security alerts or threat intelligence reports • Implications to national security, homeland security, national critical infrastructure, or the processes associated with the use of the product or service • Vulnerability of federal systems, programs, or facilities • Threat level and vulnerability level assessment/score • Potential impact or harm caused by the possible loss, damage, or compromise of a product, material, or service to an enterprise's operations or mission and the likelihood of a potential impact, harm, or the exploitability of a system • The capacity to mitigate risks is identified

What is the Cyber C.A.K.E.?

- Continuous Assessment, Knowledge, and Education (CAKE)
- The Cyber CAKE concept provides a structured, transparent framework that demystifies cybersecurity
- Easy to understand, relatable, useful analogies convey core cybersecurity concepts
- Each layer represents foundation elements of cybersecurity and offers tangible practitioner strategies for grasping the “why” and confidently implement and assess cyber strategies
- Aligned to the Cybersecurity Awareness and Training category within the **Protect** function of the NIST Cybersecurity Framework 2.0 with relevant core “Cookbooks” cited and referenced throughout
- The result of the Cyber CAKE concept is “baked in cybersecurity” and compliance used as strategy to measure resilience



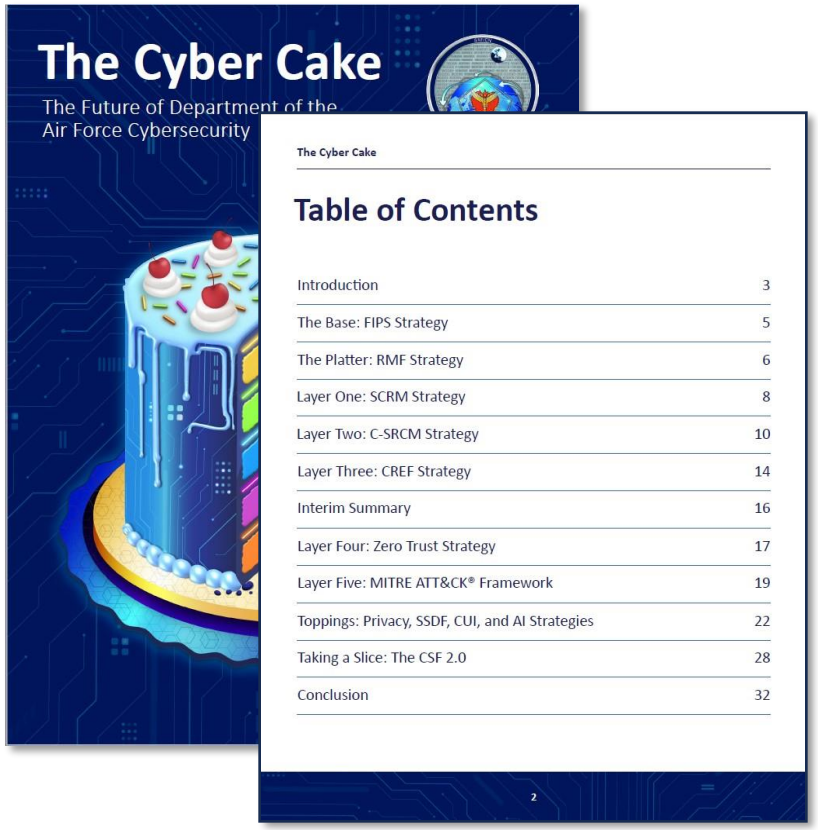
Why the Cyber C.A.K.E.?



- Cyberspace is a complex, multidimensional domain that encompasses not only conflict, but also communication, commerce, and societal development
- The knowledge base is inherently fragmented
- There is no true cyberspace "expert"
- Need: transform a daunting obstacle course into a series of manageable steps

Cyber Cake Materials

- 32-page comprehensive and foundational document*
- Each layer described in depth with corresponding figures and graphics for ease of reading



- 10-slide executive brief
- Presents highlights of Cyber Cake document for quick reading and reference

*all Cyber Cake content is Unclassified and derived from public sources

Spicy Carrot Cake – Recipe

Spicy Carrot Cake

- 1 ½ cups vegetable oil (use extra virgin olive oil)
- 2 ½ cups sugar
- 4 eggs, separated
- 5 Tbsp hot water
- 2 ½ cups all-purpose flour
- 1 ½ tsp baking powder
- ½ tsp baking soda
- ¼ tsp salt
- ½ tsp nutmeg
- 1 tsp cinnamon
- 1 tsp ground cloves
- 1 ¾ cups raw carrots, grated, divided
- 1 cup pecans, chopped (optional)

Instructions

- Preheat oven to 350° F
- Grease and flour 10-inch tube cake pan
- Mix oil and sugar. Beat in egg yolks one at a time.
- Continue to beat and add hot water
- Sift together flour, baking powder backing soda, salt and spices.
- Add dry ingredients to egg mixture
- Reserve ¼ cup grated carrots for garnish and stir in the remaining carrots and pecans
- Beat egg whites till soft peaks begin to form, then fold in
- Pour batter into prepared pan and back at 350° F for 60-70m, or until cake tests done
- Cool pan right side up for 15 minutes, then turn out to finish colling on cake rack
- Drizzle glaze in a circle on top of cake and sprinkle with reserved grated carrot

Glaze

- ¾ cup confectioners' sugar
- 3 Tbsp lemon juice

Instructions

- Mix ingredients until smooth

The Williamsburg Cookbook (1971)