OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

A Common Cyber Threat Framework:
A Foundation for Communication

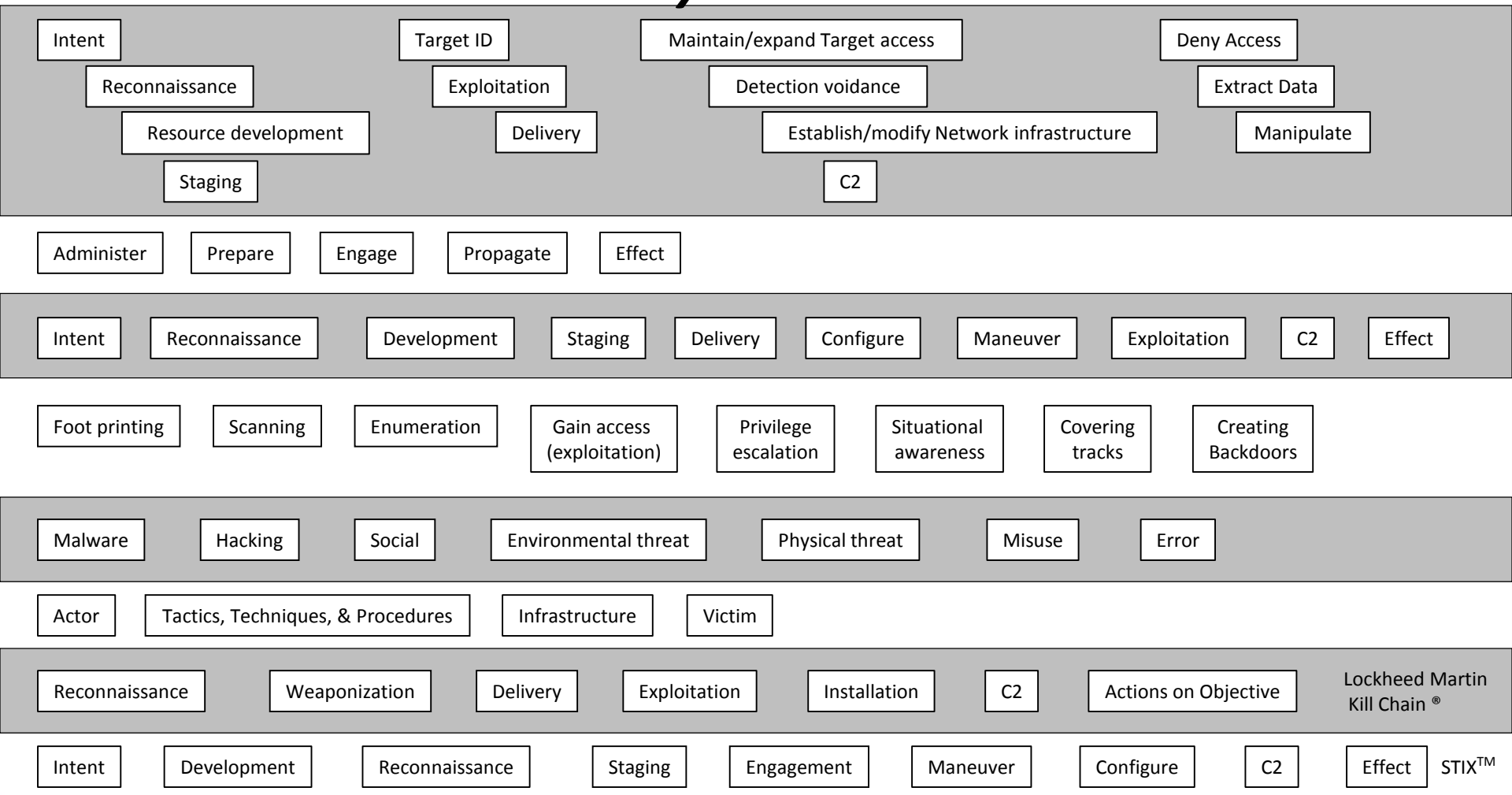
LEADING INTELLIGENCE INTEGRATION

Overview

- Why did we build one?
- What are its attributes?
- What does ours look like?
- How has it worked in practice?
- Current status/what's next?

With So Many Cyber Threat Models or Frameworks

Why build another?



… Because comparison of threat data across models and users is problematic

Following a common approach helps to:

- ***Establish a common ontology*** and ***enhance information-sharing*** since it is easier to map unique models to a common standard than to each other ('N-to-1' easier than 'N-to-N')
- ***Characterize and categorize threat activity*** in a straightforward way that can support multiple missions ranging from strategic decision-making to analysis and cybersecurity measures, and users from generalists to technical experts
- ***Achieve common situational awareness*** across organizations

Our Intent

- Began as a construct to enhance data-sharing throughout the US Government
- Facilitate efficient situational awareness based on objective (typically, sensor-derived) data
- Provide a simple, yet flexible, collaborative way of characterizing and categorizing threat activity that supports analysis, senior-level decision making, and cybersecurity
- Offer a common approach ('cyber Esperanto')
- Facilitate cyber threat trend and gap analysis, assessment of collection posture
- Support (not replace!) analysis – and free the human to spend more time *doing analysis*

Goals of a Common Approach

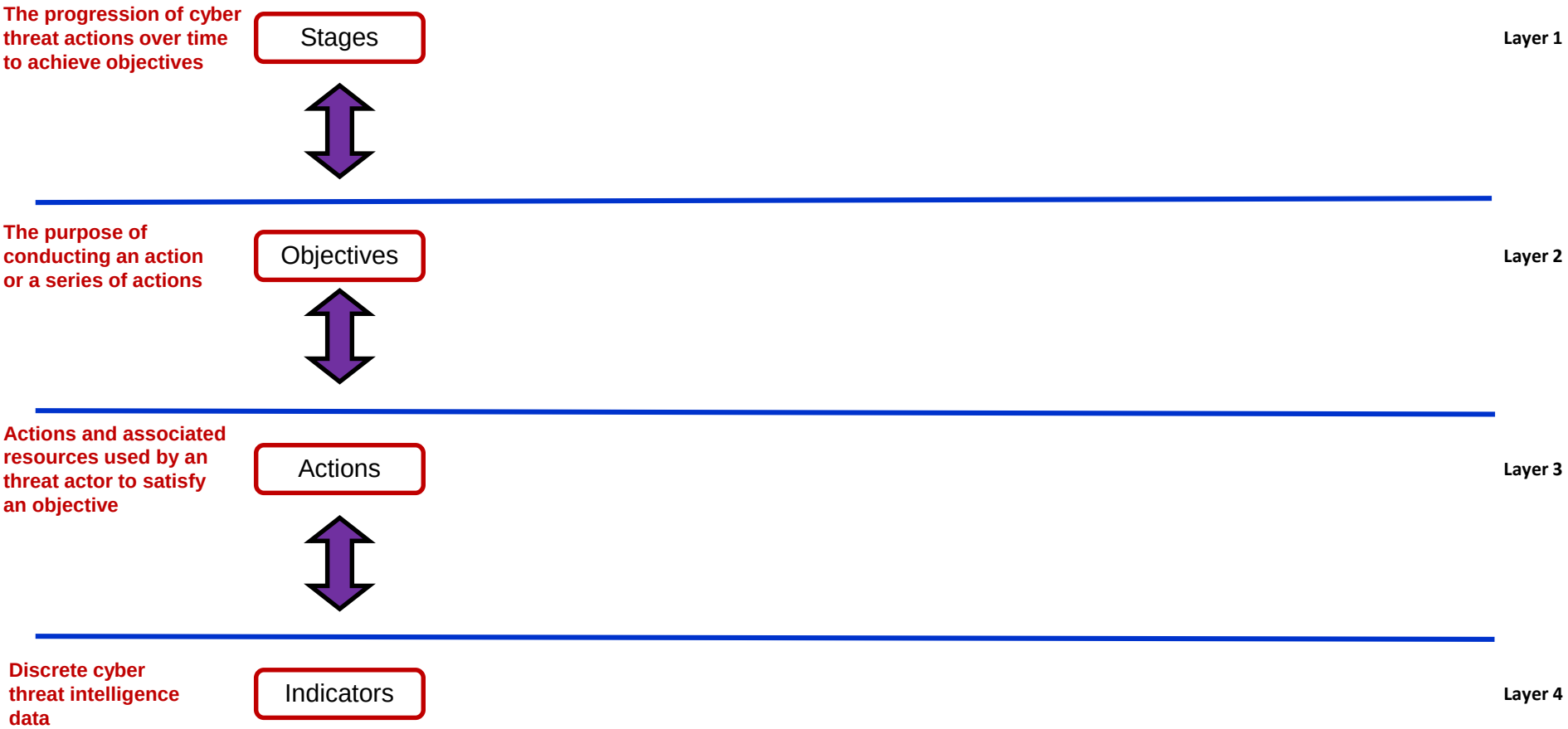
- Key Attributes: a model that is ***hierarchical***, ***structured***, ***transparent*** *and* ***repeatable***, tied to ***explicit definitions***
- An optimized cyber threat framework
  - Is focused on empirical and often sensor-derived data; serves as the foundation for subsequent analysis and decision-making
  - Supports analysis and the characterization and categorization of cyber threat information through the use of standardized language
  - Accommodates a wide variety of data sources, threat actors and threat activity
  - Information arranged hierarchically and organized in increasing "layers" of detail
  - Can be tailored or customized to meet individual needs

Ground Rules as we built our approach

- No one's current model is 'wrong'
- …And we are not advocating that anyone stop using their own!
- Map your model to the common backbone and tell the rest of us how you've done it
- …Or use the common backbone and customize it as needed

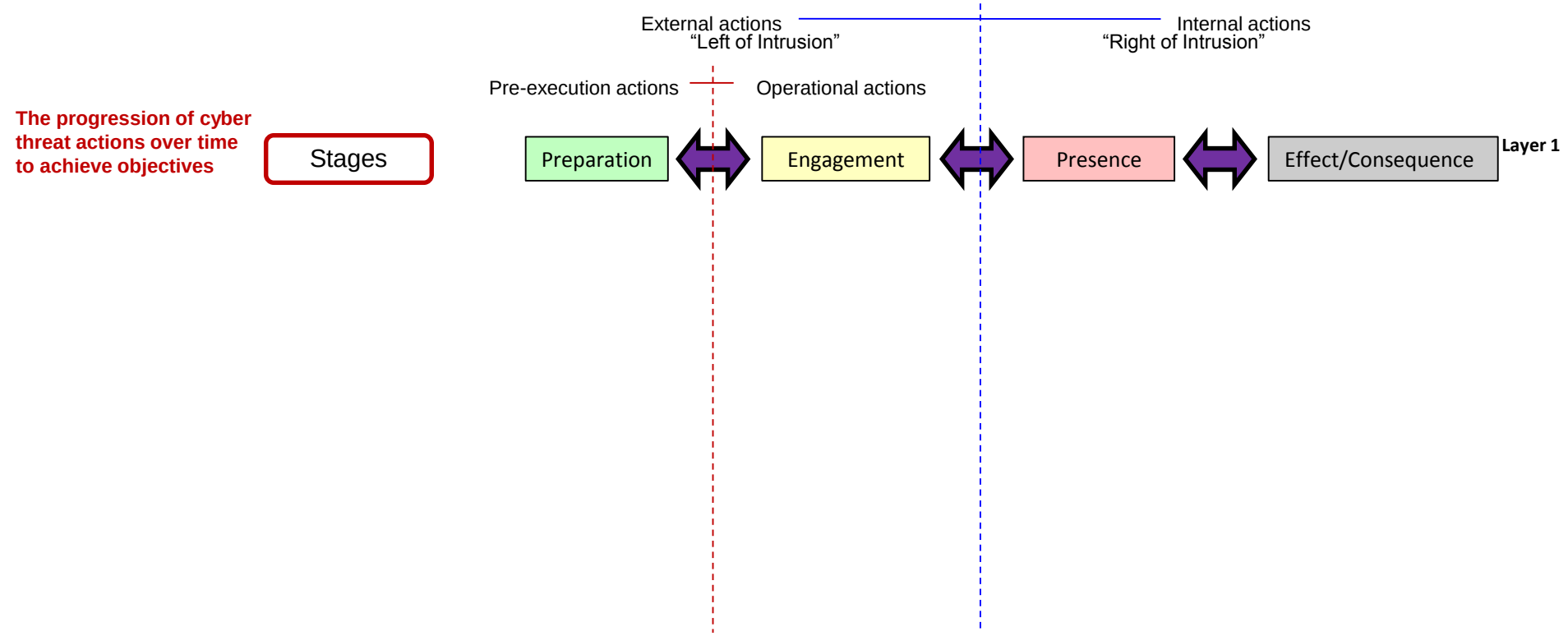
Common Cyber Threat Framework

A Hierarchical Approach



Common Cyber Threat Framework

Structured around a Simplified "Threat Lifecycle"



Common Cyber Threat Framework

Threat Actor Objectives within the "Threat Lifecycle"

The progression of cyber threat actions over time to achieve objectives

Stages

Layer 1

Preparation	Engagement	Presence	Effect/Consequence

Layer 2

The purpose of conducting an action or a series of actions

Objectives

Preparation	Engagement	Presence	Effect/Consequence
Plan activity	Deploy capability	Establish controlled access	Enable other operations
Conduct research & analysis	Interact with intended victim	Hide	Deny access
Develop resources & capabilities		Expand presence	Extract data
Acquire victim specific knowledge	Exploit vulnerabilities	Refine focus of activity	Alter data and/or computer, network or system behavior
Complete preparations	Deliver malicious capability	Establish persistence	Destroy HW/SW/data

Layer 3

Actions and associated resources used by an threat actor to satisfy an objective

Actions

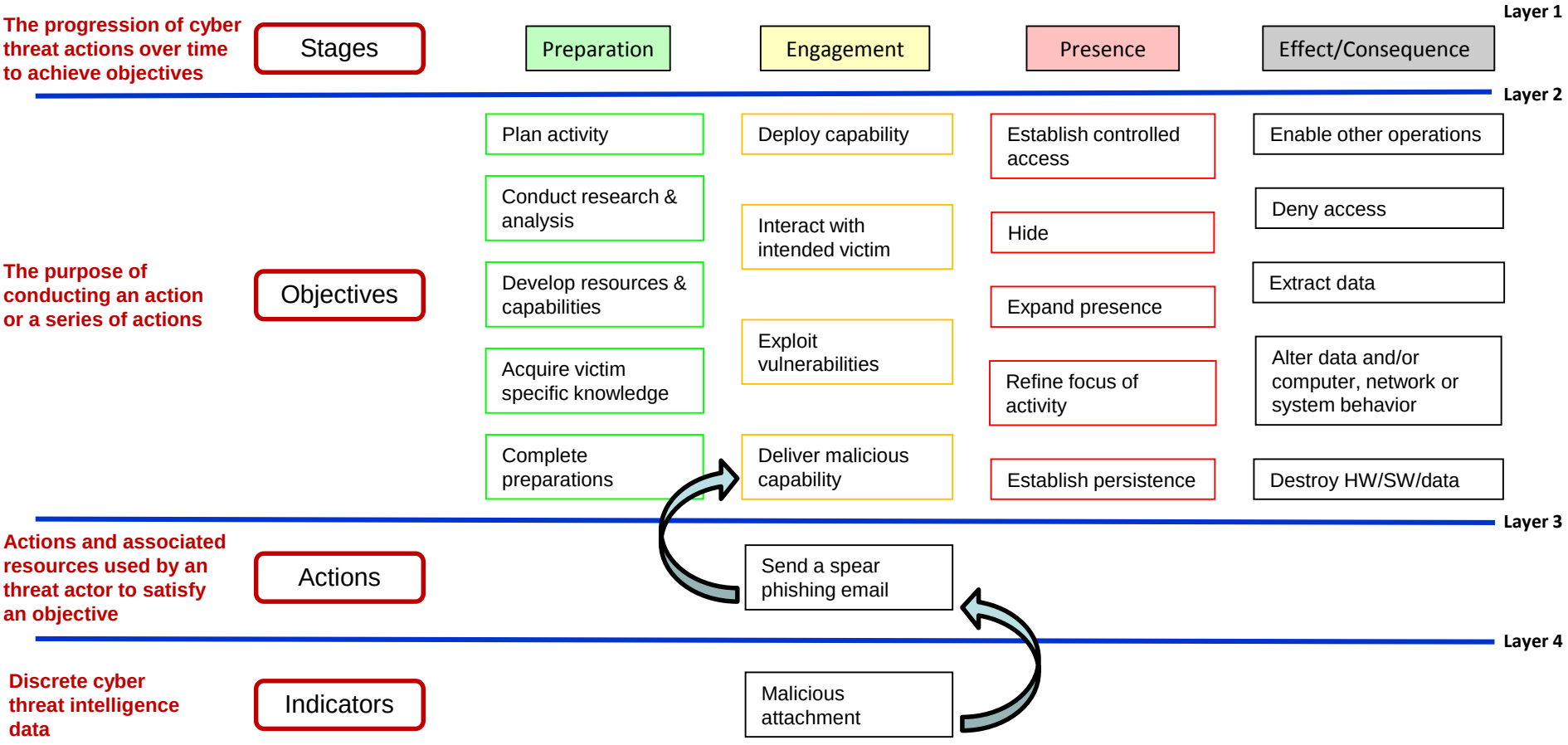
Layer 4

Discrete cyber threat intelligence data

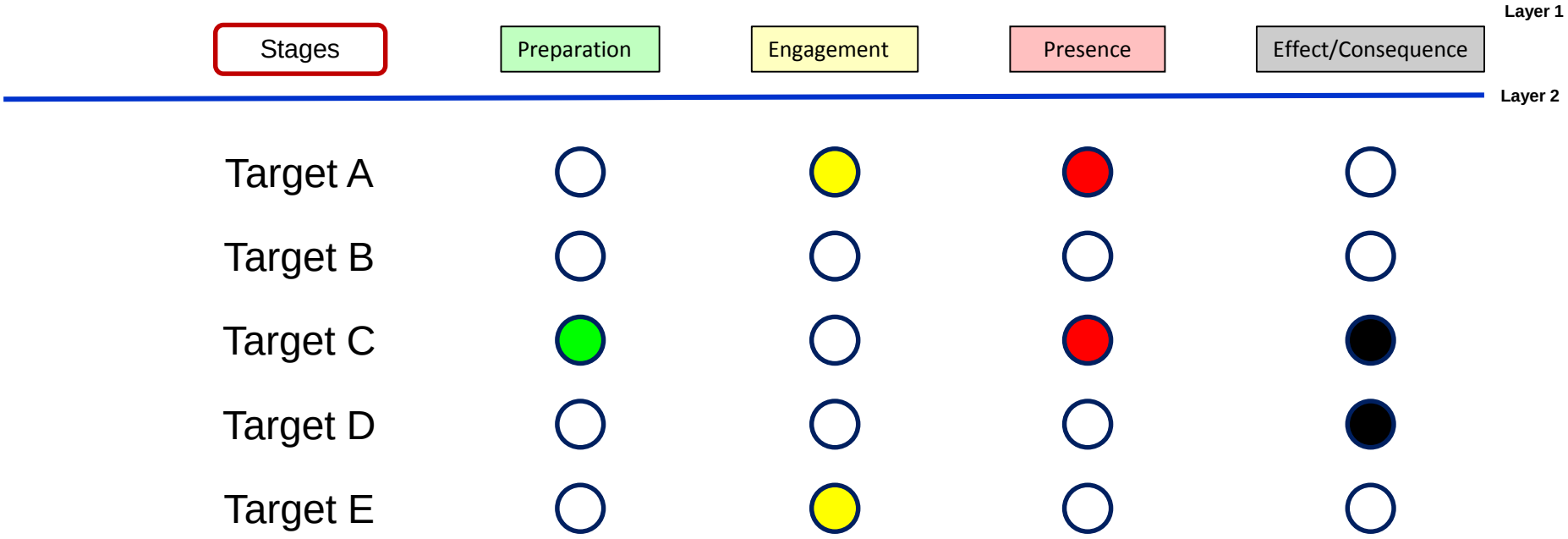
Indicators

Common Cyber Threat Framework

Actions and Indicators are the Details of Threat Activity

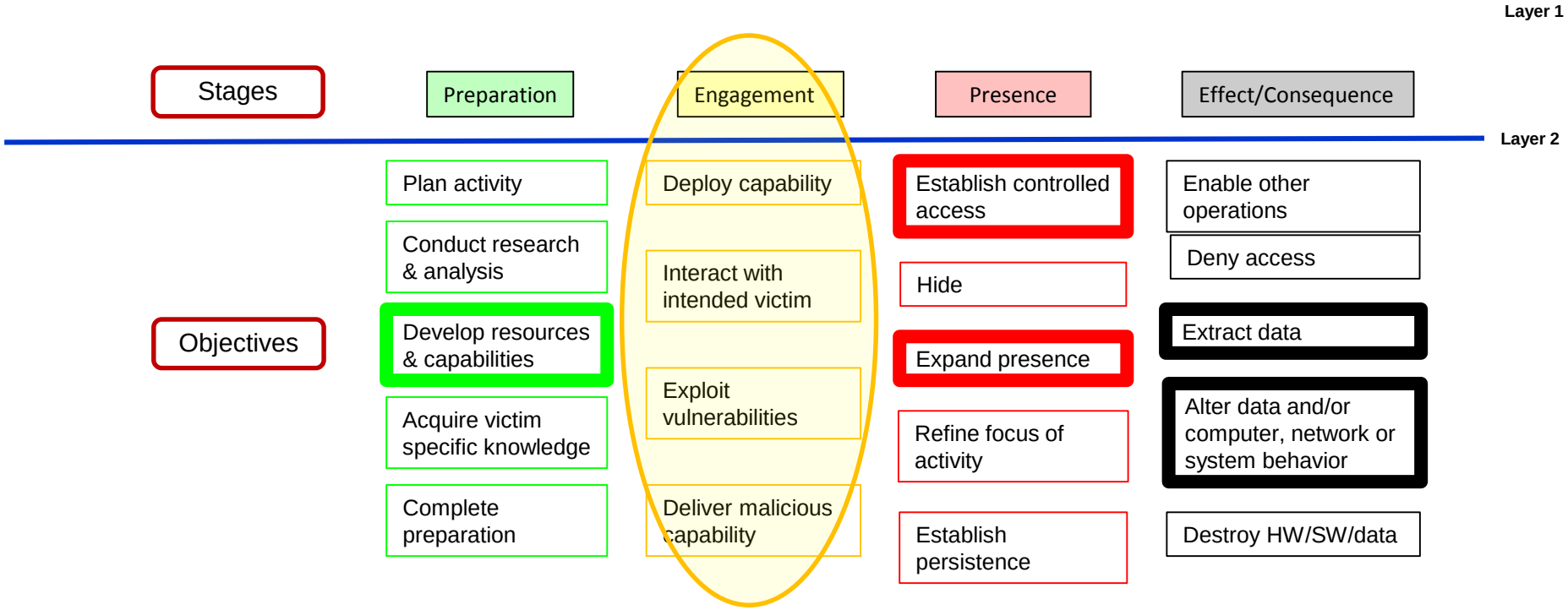


Real Use cases: Cyber Threat Activity Analysis



- Where is my greatest threat?
- What actions should I be taking to protect myself?

Real World Use case: Link or Gap Analysis



The Missing Link?

- Am I looking in the wrong place?
- Is there nothing illicit to see? (insight into adversary behavior)

Recap: With So Many Cyber Threat Models or Frameworks *Why build another?*

Intent
Reconnaissance
Resource development
Staging

Target ID
Exploitation
Delivery

Maintain/expand Target access
Detection voidance
Establish/modify Network infrastructure
C2

Deny Access
Extract Data
Manipulate

Administer | Prepare | Engage | Propagate | Effect

Intent | Reconnaissance | Development | Staging | Delivery | Configure | Maneuver | Exploitation | C2 | Effect

Foot printing | Scanning | Enumeration | Gain access (exploitation) | Privilege escalation | Situational awareness | Covering tracks | Creating Backdoors

Malware | Hacking | Social | Environmental threat | Physical threat | Misuse | Error

Actor | Tactics, Techniques, & Procedures | Infrastructure | Victim

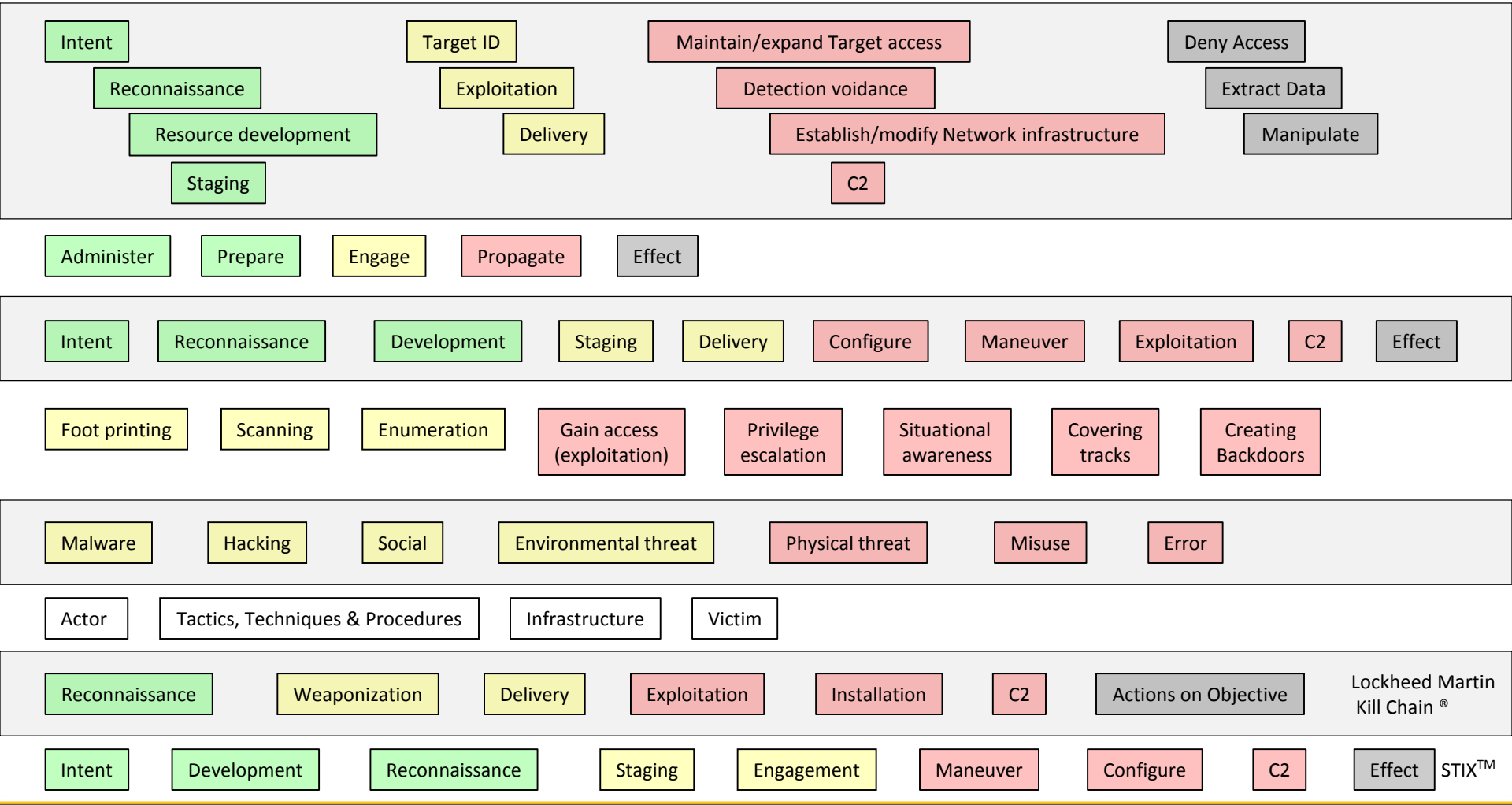
Reconnaissance | Weaponization | Delivery | Exploitation | Installation | C2 | Actions on Objective

Lockheed Martin Kill Chain ®

Intent | Development | Reconnaissance | Staging | Engagement | Maneuver | Configure | C2 | Effect

STIX™

…because a Common Approach Facilitates Grouping and Comparison of Cyber Threats from Different Perspectives



Common Cyber Threat Framework

Current Status

- Used in threat products by multiple US Government agencies and some Allies
- Adoption across the Executive Branch high priority for 2018
- Under consideration by NATO and Asian allies to facilitate a common operating picture and enhance information sharing
- Being taught to new US Government cyber analysts
- Included in curricula and research at multiple universities
- Evolution continues based on use and ongoing outreach to industry, academia, government, and international partners

Framework materials available at DNI.GOV