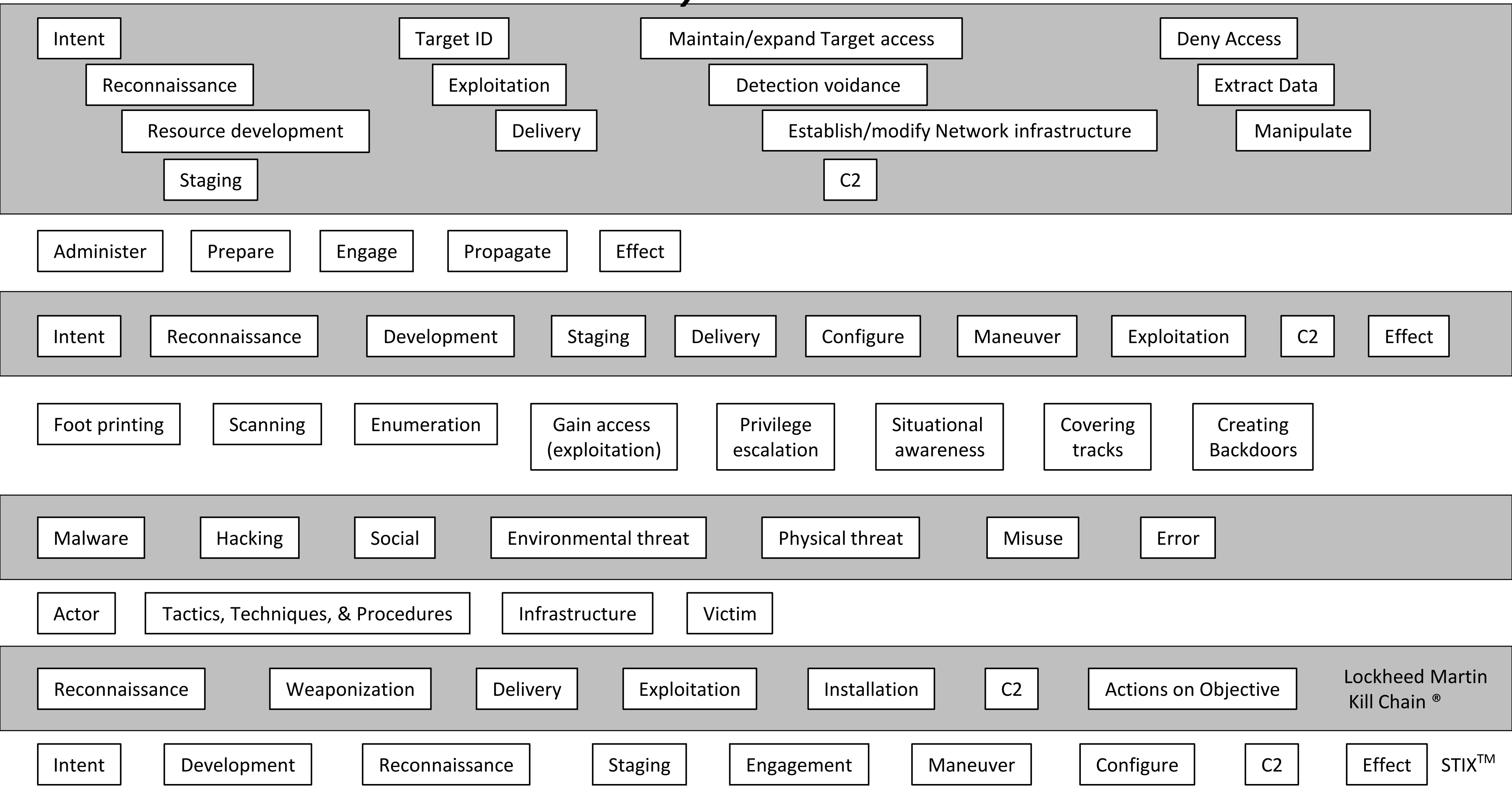
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

A Common Cyber Threat Framework:
A Foundation for Communication

LEADING INTELLIGENCE INTEGRATION

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 comparison of threat data across models and users is problematic

Following a common approach helps to:

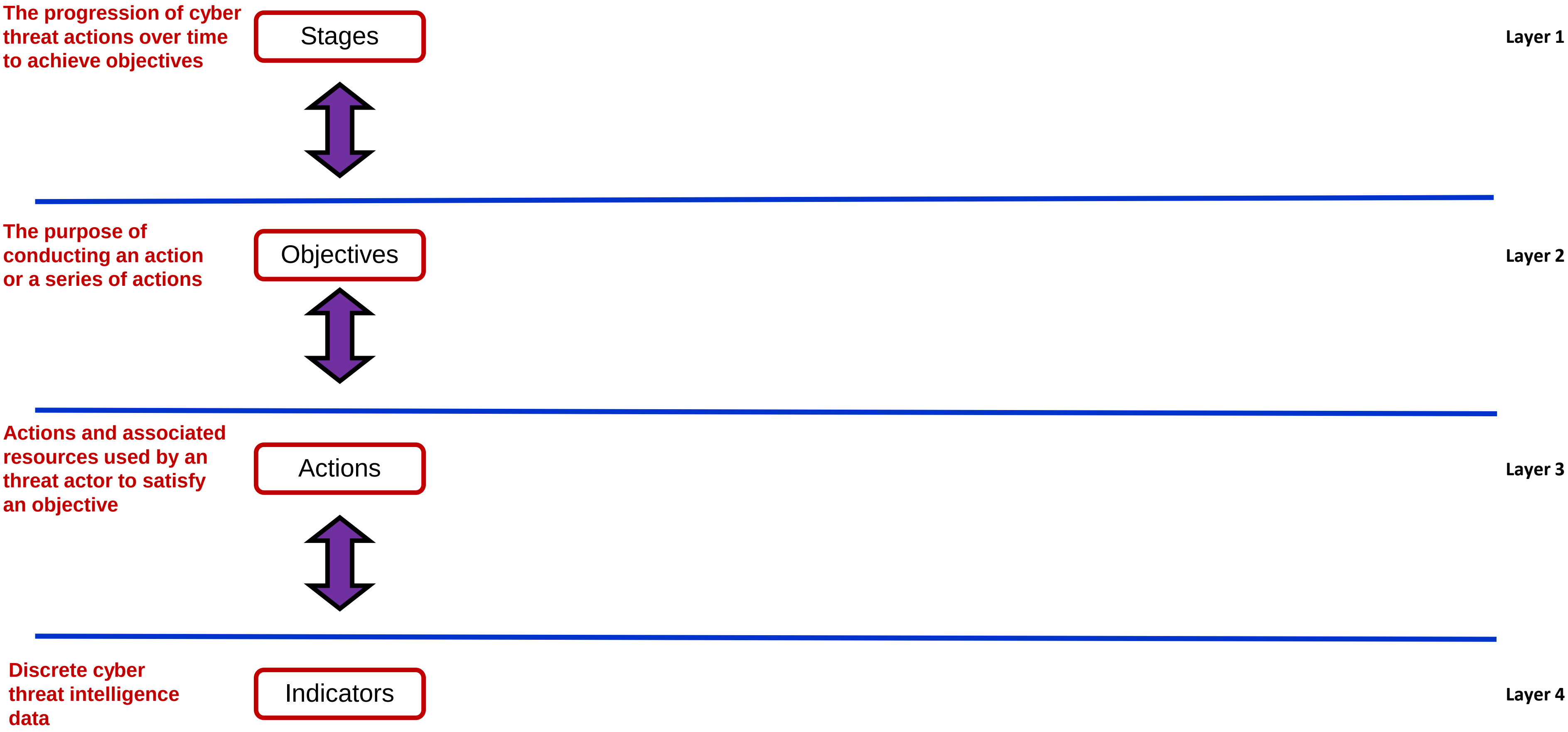
- ***Establish a common ontology*** and ***enhance information-sharing*** since it is easier to map unique models to a common standard than to each other
- ***Characterize and categorize threat activity*** in a straightforward way that can support missions ranging from strategic decision-making to analysis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

Goals of a Common Approach

- Key Attributes: a model that is *hierarchical*, *structured, transparent and repeatable*, featuring *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
  - The information captured within is arranged hierarchically and organized in increasing “layers” of detail
  - Is tailorable to meet a host of individual needs

Common Cyber Threat Framework

A Hierarchical Approach



The progression of cyber threat actions over time to achieve objectives

Stages

Layer 1

The purpose of conducting an action or a series of actions

Objectives

Layer 2

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

Actions

Layer 3

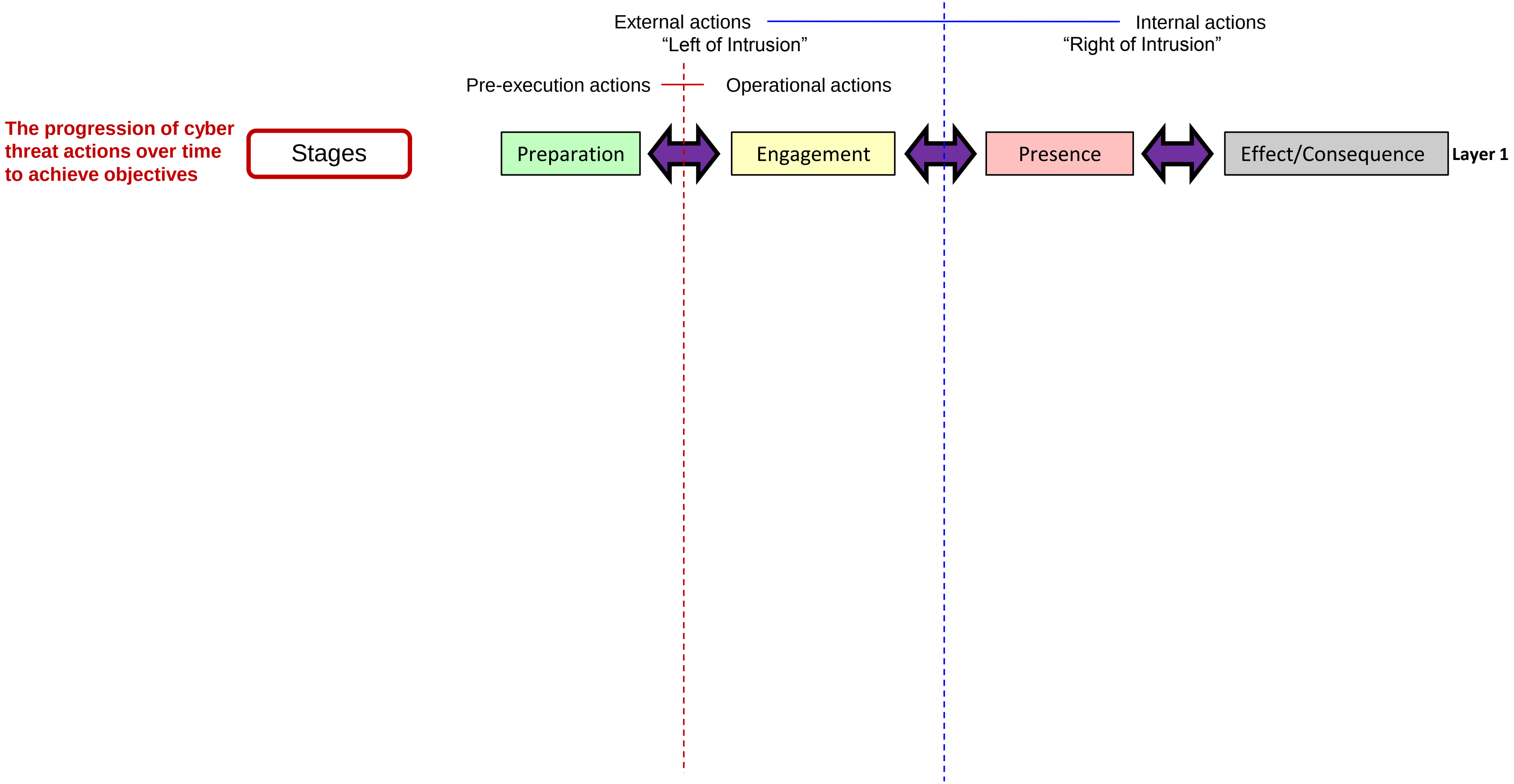
Discrete cyber threat intelligence data

Indicators

Layer 4

Common Cyber Threat Framework

Structured around a Simplified "Threat Lifecycle"



External actions
"Left of Intrusion"

Internal actions
"Right of Intrusion"

Pre-execution actions

Operational actions

The progression of cyber threat actions over time to achieve objectives

Stages

Preparation

Engagement

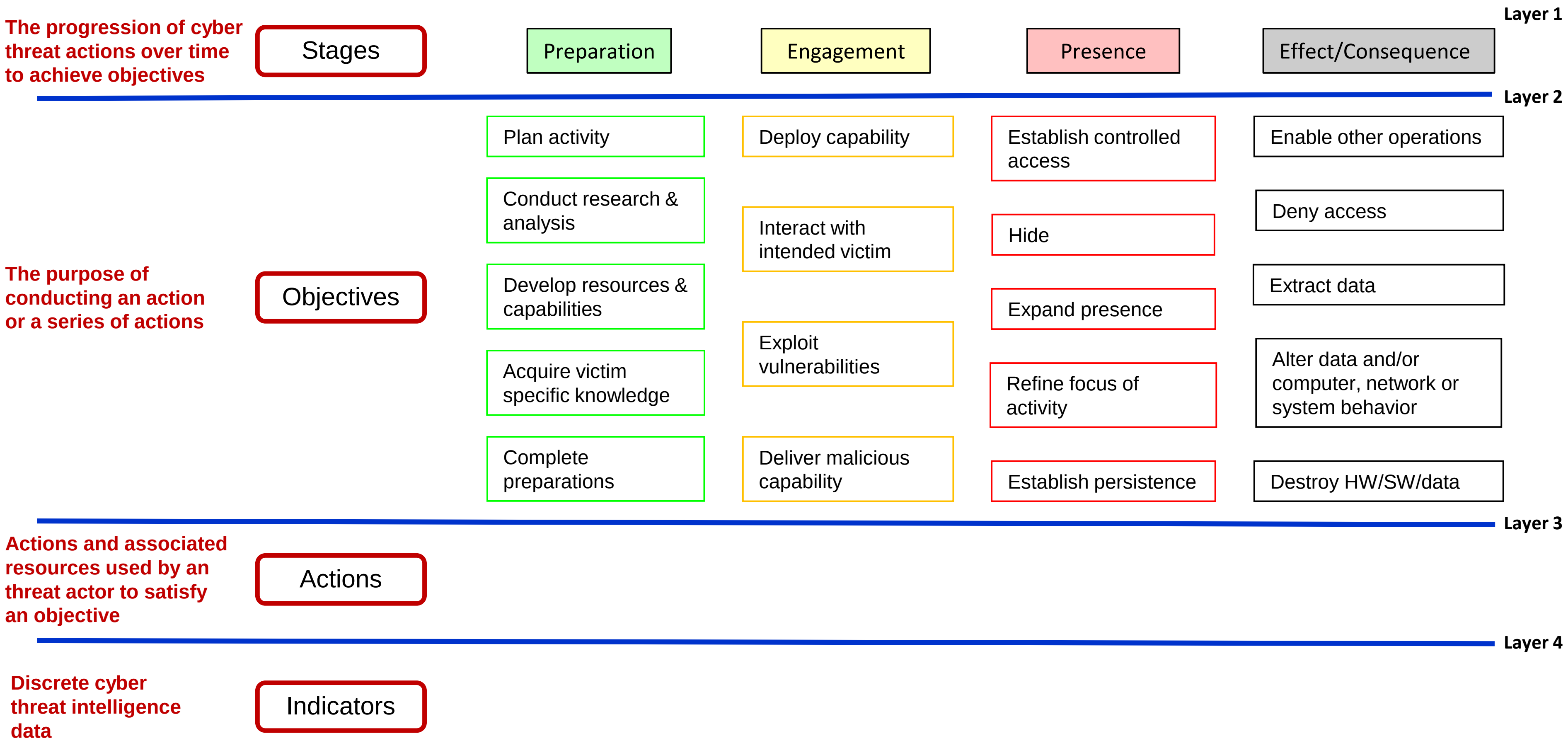
Presence

Effect/Consequence

Layer 1

Common Cyber Threat Framework

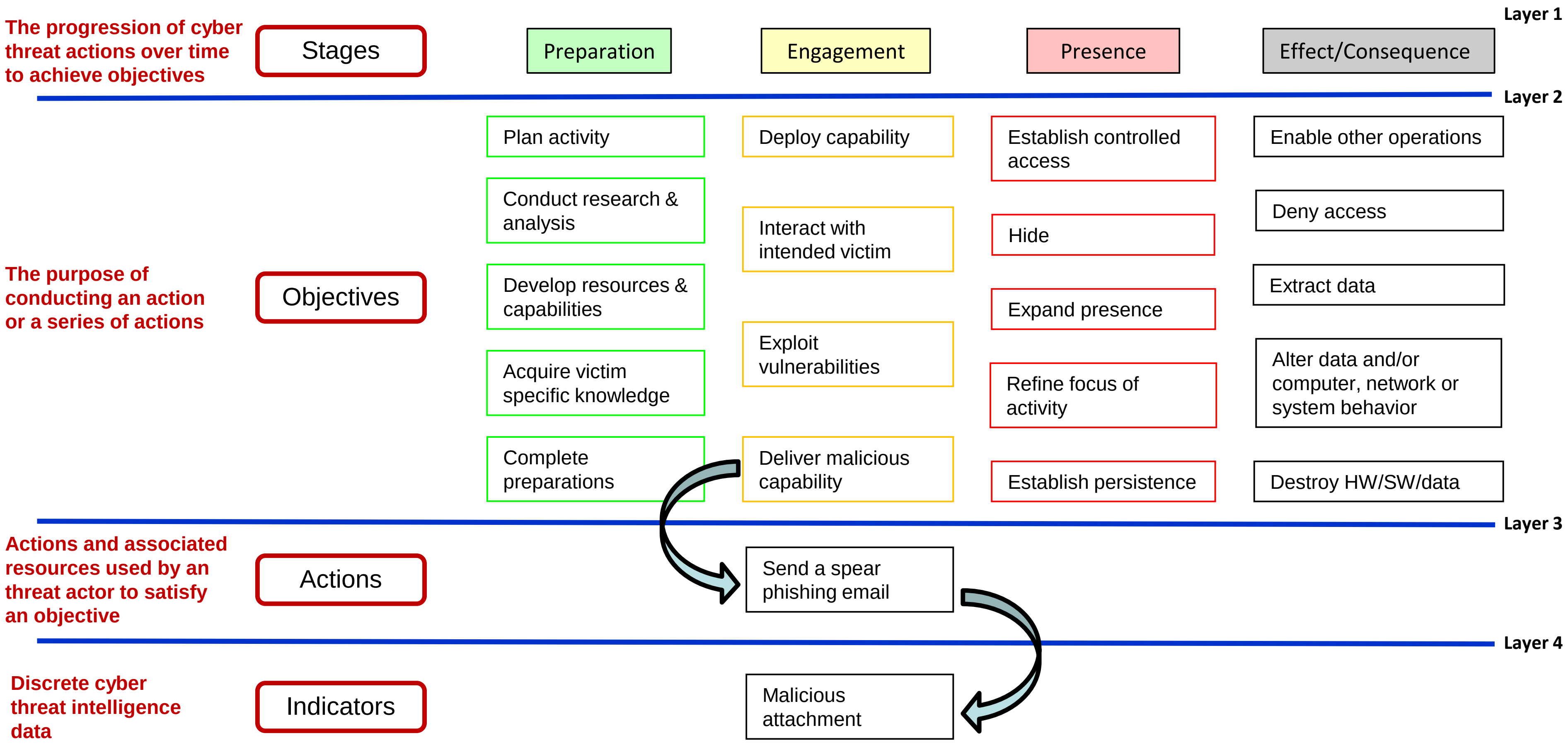
Threat Actor Objectives within the “Threat Lifecycle”



The progression of cyber threat actions over time to achieve objectives	Stages	Preparation	Engagement	Presence	Effect/Consequence	Layer 1
The purpose of conducting an action or a series of actions	Objectives	Plan activity Conduct research & analysis Develop resources & capabilities Acquire victim specific knowledge Complete preparations	Deploy capability Interact with intended victim Exploit vulnerabilities Deliver malicious capability	Establish controlled access Hide Expand presence Refine focus of activity Establish persistence	Enable other operations Deny access Extract data Alter data and/or computer, network or system behavior Destroy HW/SW/data	Layer 2
Actions and associated resources used by an threat actor to satisfy an objective	Actions					Layer 3
Discrete cyber threat intelligence data	Indicators					Layer 4

CommonCyber Threat Framework

Actions and Indicators are the Details of Threat Activity



Layer 1

The progression of cyber threat actions over time to achieve objectives

Stages

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

Send a spear phishing email

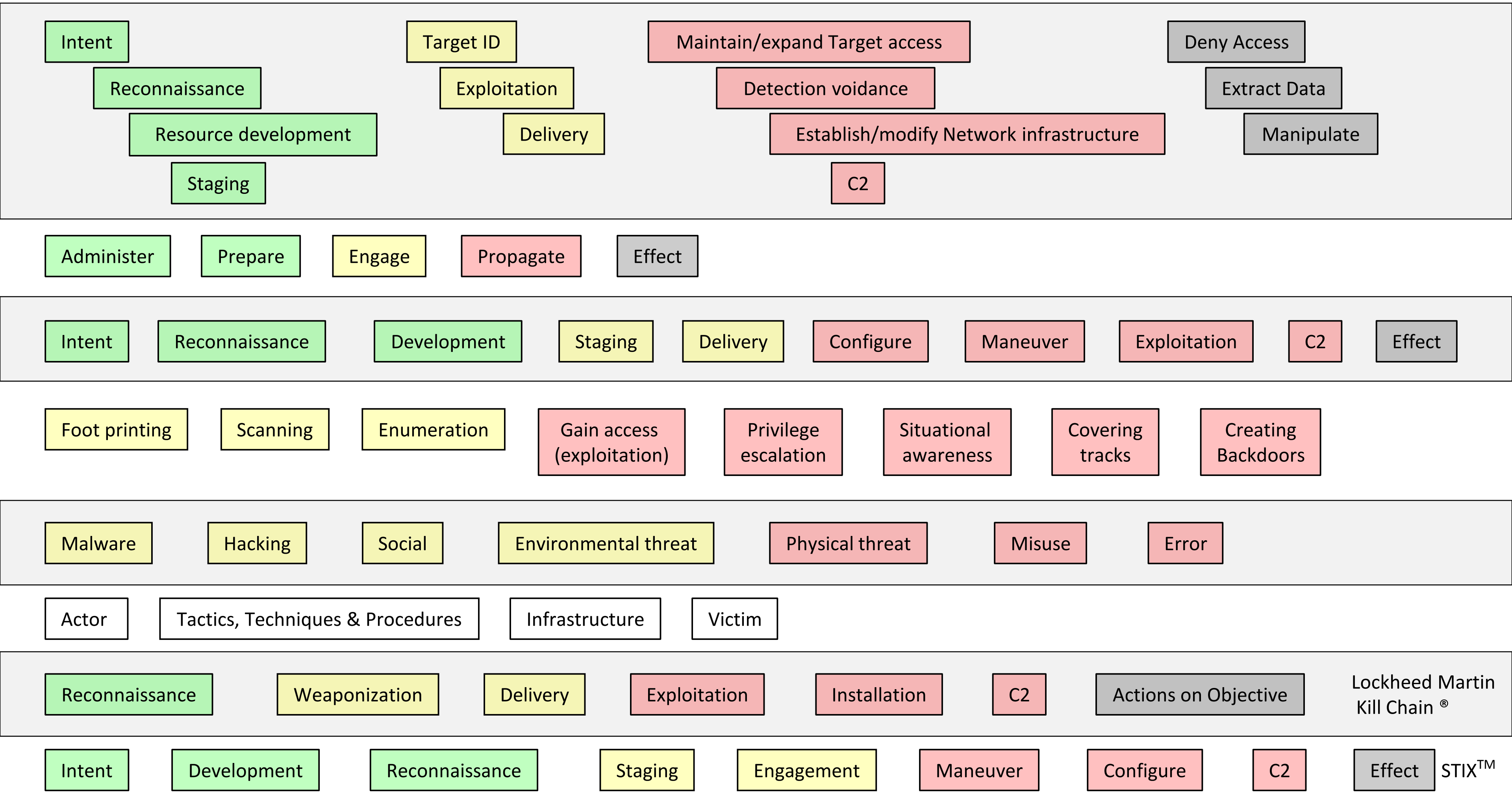
Layer 4

Discrete cyber threat intelligence data

Indicators

Malicious attachment

This Common Approach Facilitates Grouping and Comparison of Cyber Threat Activities Seen from Different Perspectives



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^{TM}

Common Cyber Threat Framework

Current Status

- Framework and associated Lexicon available at DNI.GOV
- Used in threat products by DHS, FBI, and the ODNI's Cyber Threat Intelligence Integration Center (CTIIC)
- Being taught to new US Government cyber analysts
- Included in curricula and research at multiple universities
- Under consideration by international partners to facilitate a common operating picture and enhance threat information sharing
- Evolution continues based on use and ongoing outreach to industry, academia, government, and international partners

Questions?

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu