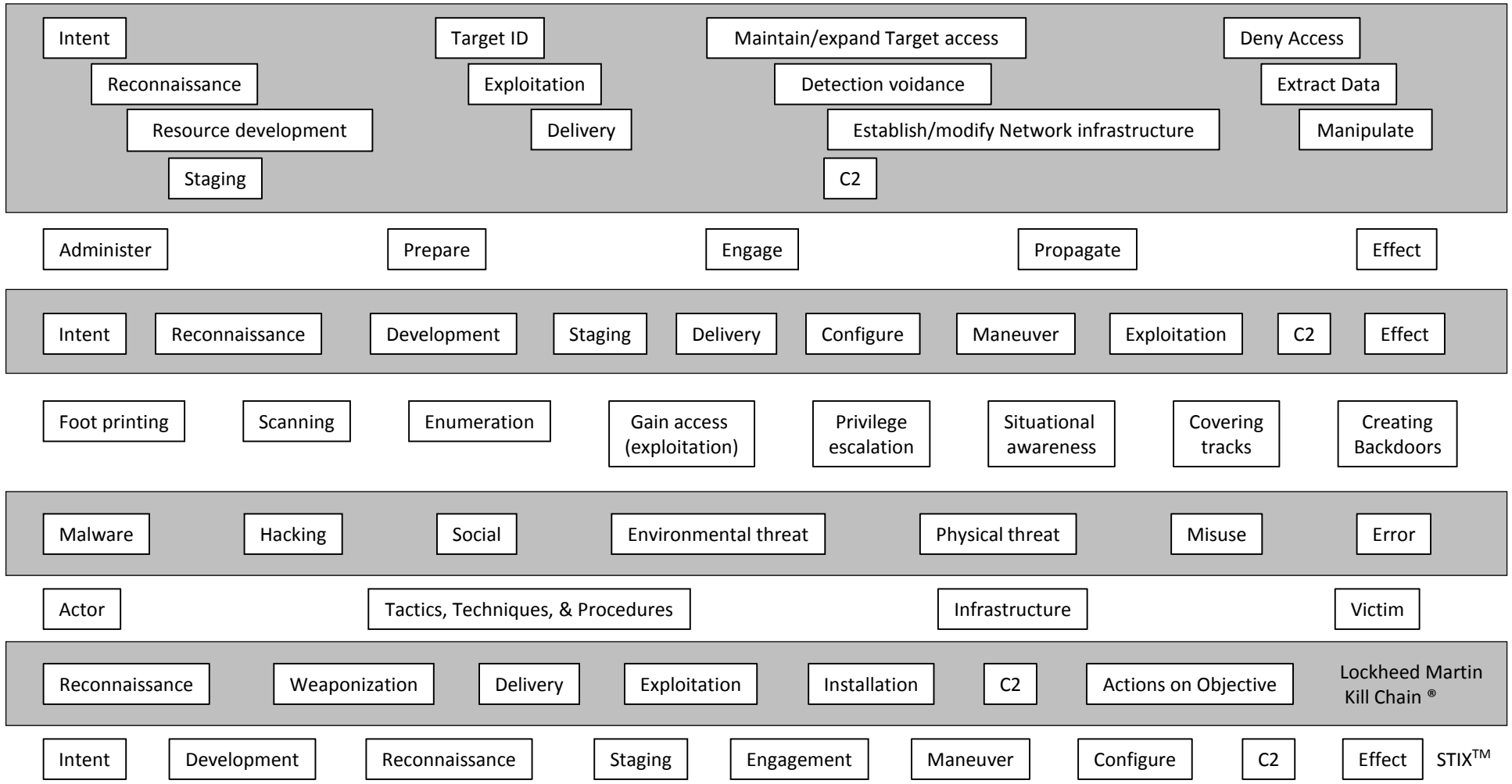
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

A Common Cyber Threat Framework:

A Foundation for Communication

James Richberg
National Intelligence Manager for Cyber
National Security Partnerships
July 18, 2018

With So Many Cyber Threat Models or Frameworks, why build another?
…because comparison of data across them can be problematic



Goals for a Common Approach to Threat Frameworks

Following a common approach helps to:

- *Establish a shared ontology* and *enhance information-sharing* since it is easier to maintain mapping of multiple models to a common reference than directly 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 experts
- *Support common situational awareness* across organizations

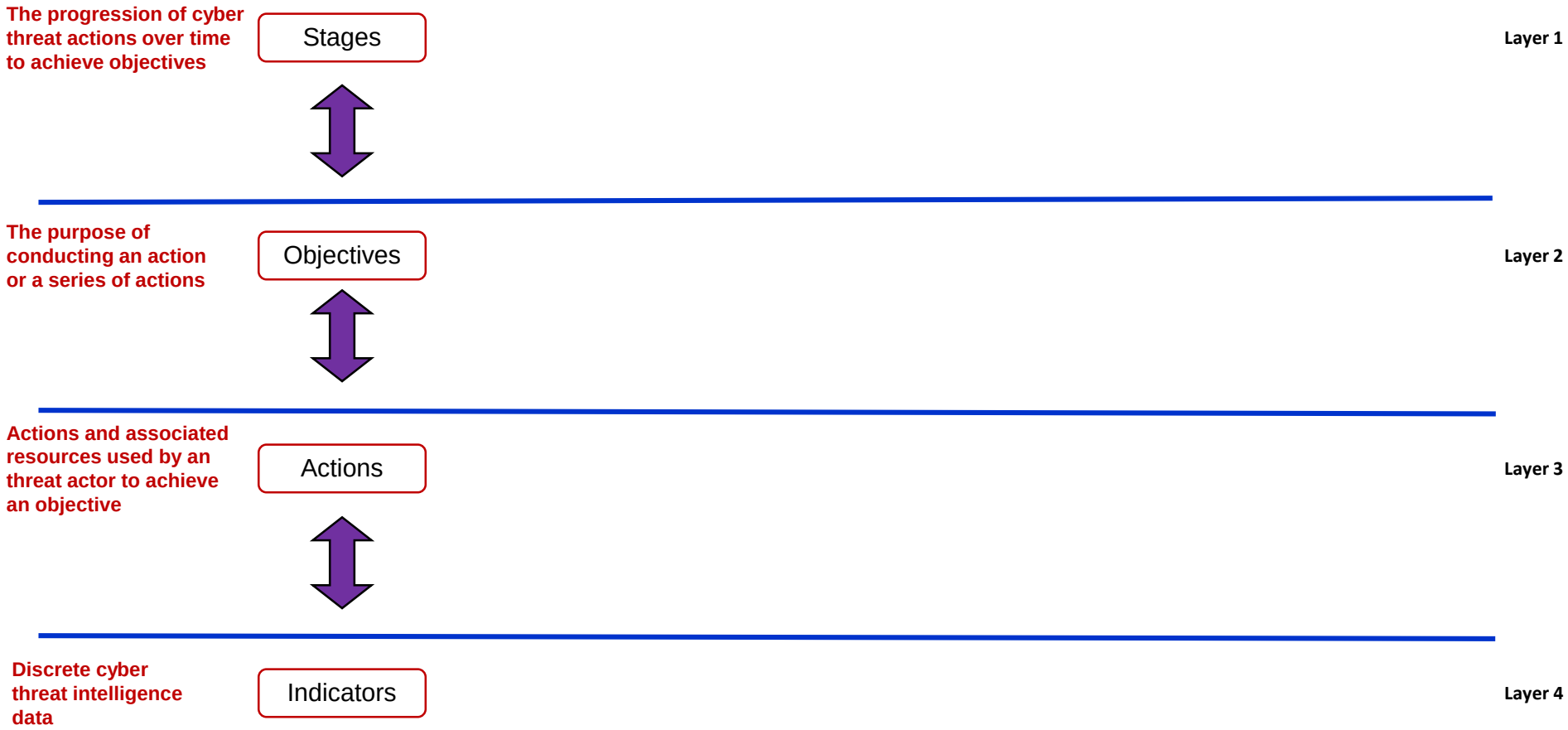
Key Attributes and Goals in Building a Cyber Threat Framework

- Incorporate a *hierarchical/layered perspective* that allows a focus on a level detail appropriate to the audience while maintaining linkage and traceability of data
- Employ *Structured and documented categories* with explicitly *defined terms* and labels (lexicon)
- Focus on *empirical/sensor-derived 'objective' data*
- Accommodate a wide variety of data sources, threat actors and activity
- Provide as a foundation for analysis and decision-making

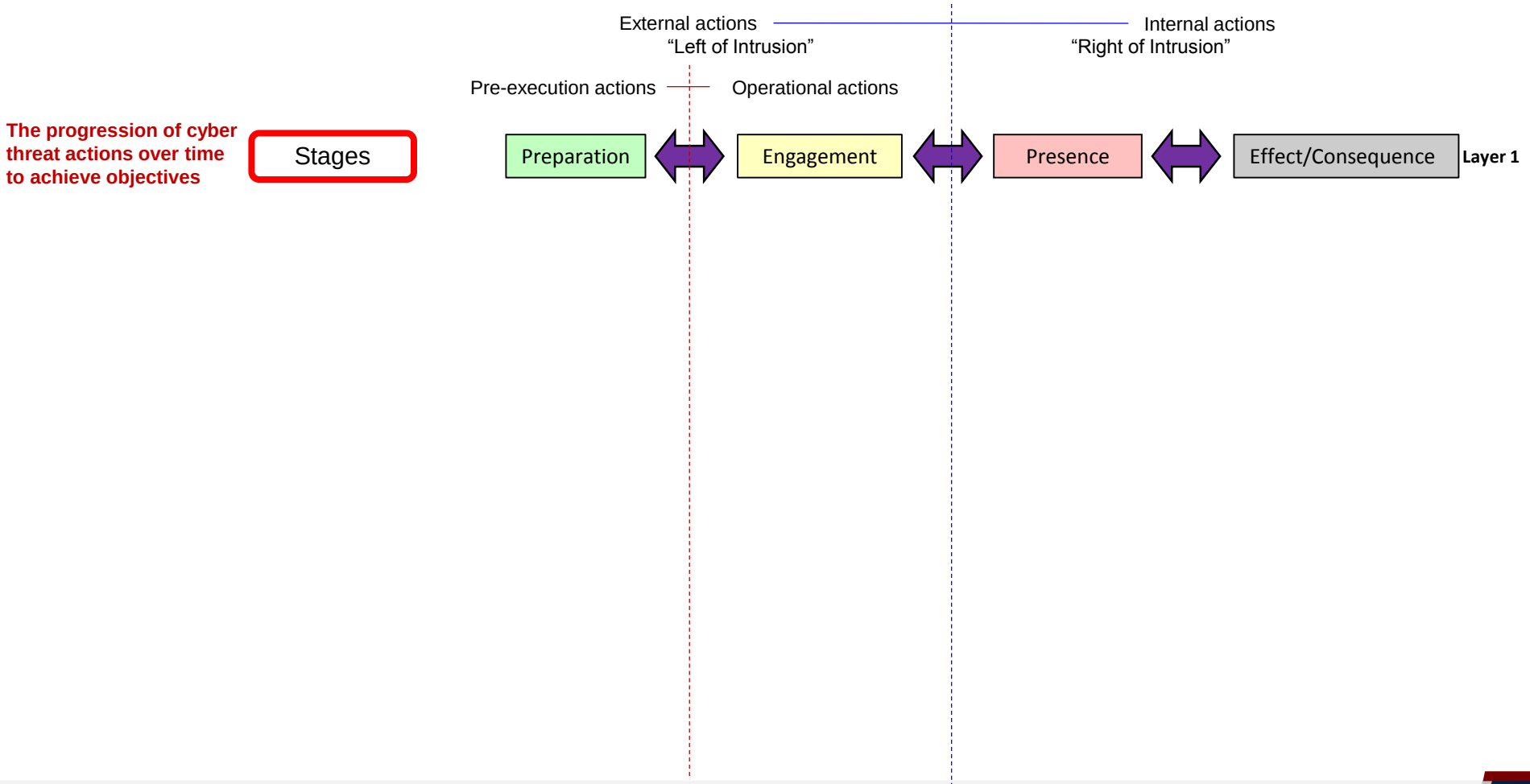
The Common Cyber Threat Framework

- Since 2012, the Office of the DNI has worked with interagency partners to build and refine The Common Cyber Threat Framework reflecting these key attributes and goals
- The Common Cyber Threat Framework is not intended to displace or replace an organization's existing model which is tailored to its specific mission and requirements; rather, it is intended to:
  - *Serve as a viable Universal Translator* (a cyber Esperanto or Rosetta Stone) facilitating efficient and possibly automated exchange of data and insight across models once each has been mapped to it and the mappings shared
  - *Provide a Starting Point* featuring a simple threat model and value-neutral concepts. It can be customized for any organization as needed—and any deviations from the common approach are readily apparent, facilitating mapping and data exchange.

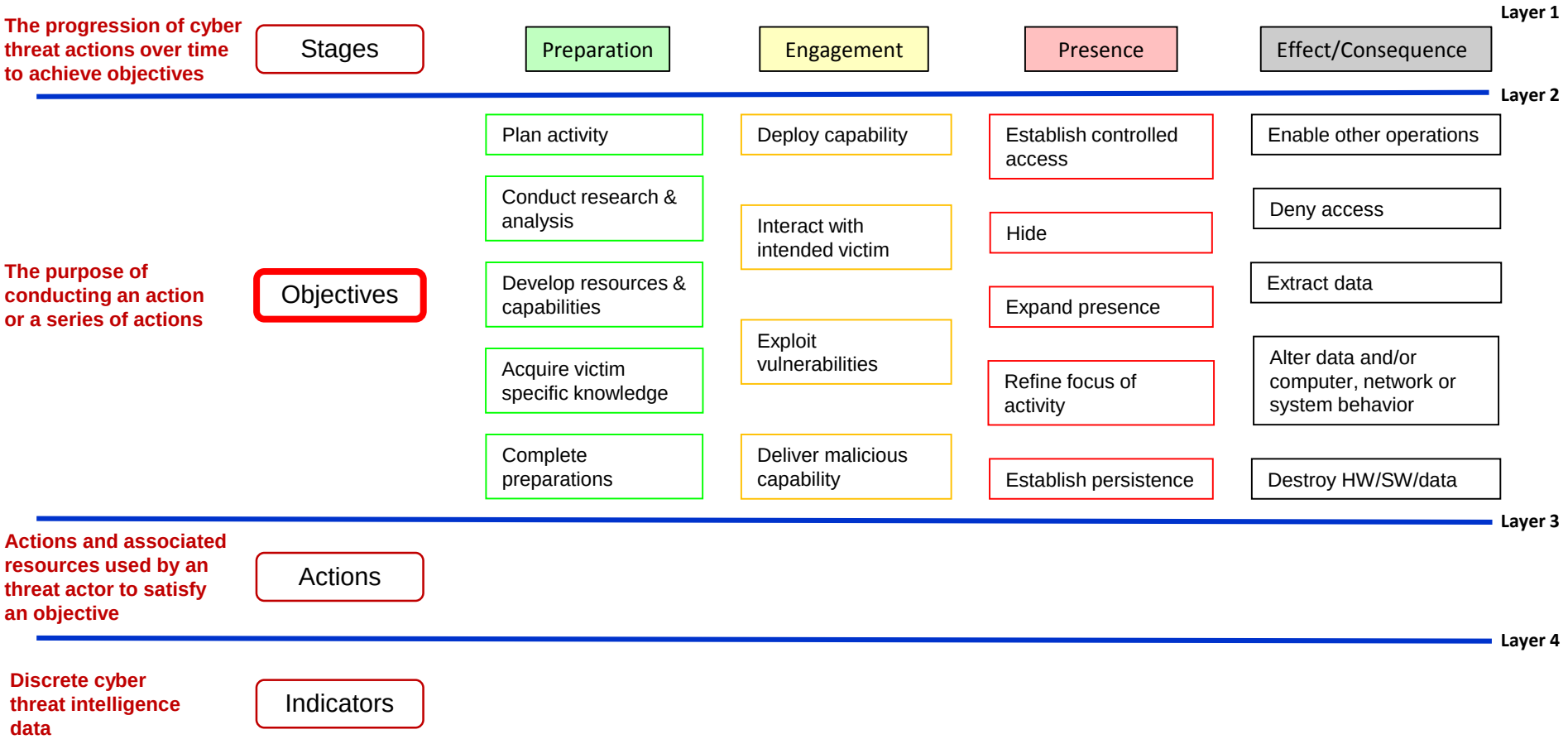
The Common Cyber Threat Framework
A Hierarchical, Layered Approach



The Common Cyber Threat Framework
Structured around a Simplified "Threat Lifecycle"

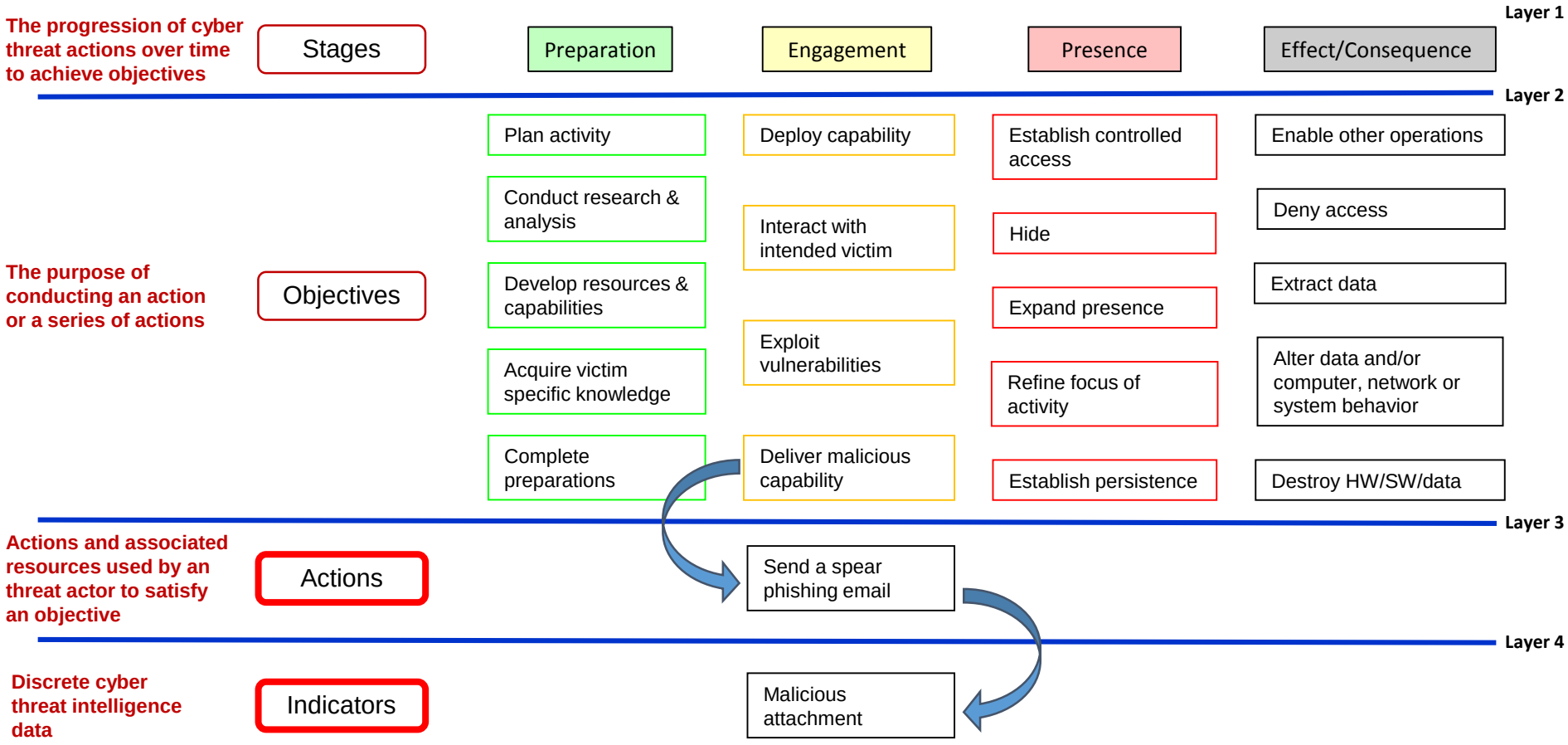


The Common Cyber Threat Framework
Threat Actor Objectives within the "Threat Lifecycle"

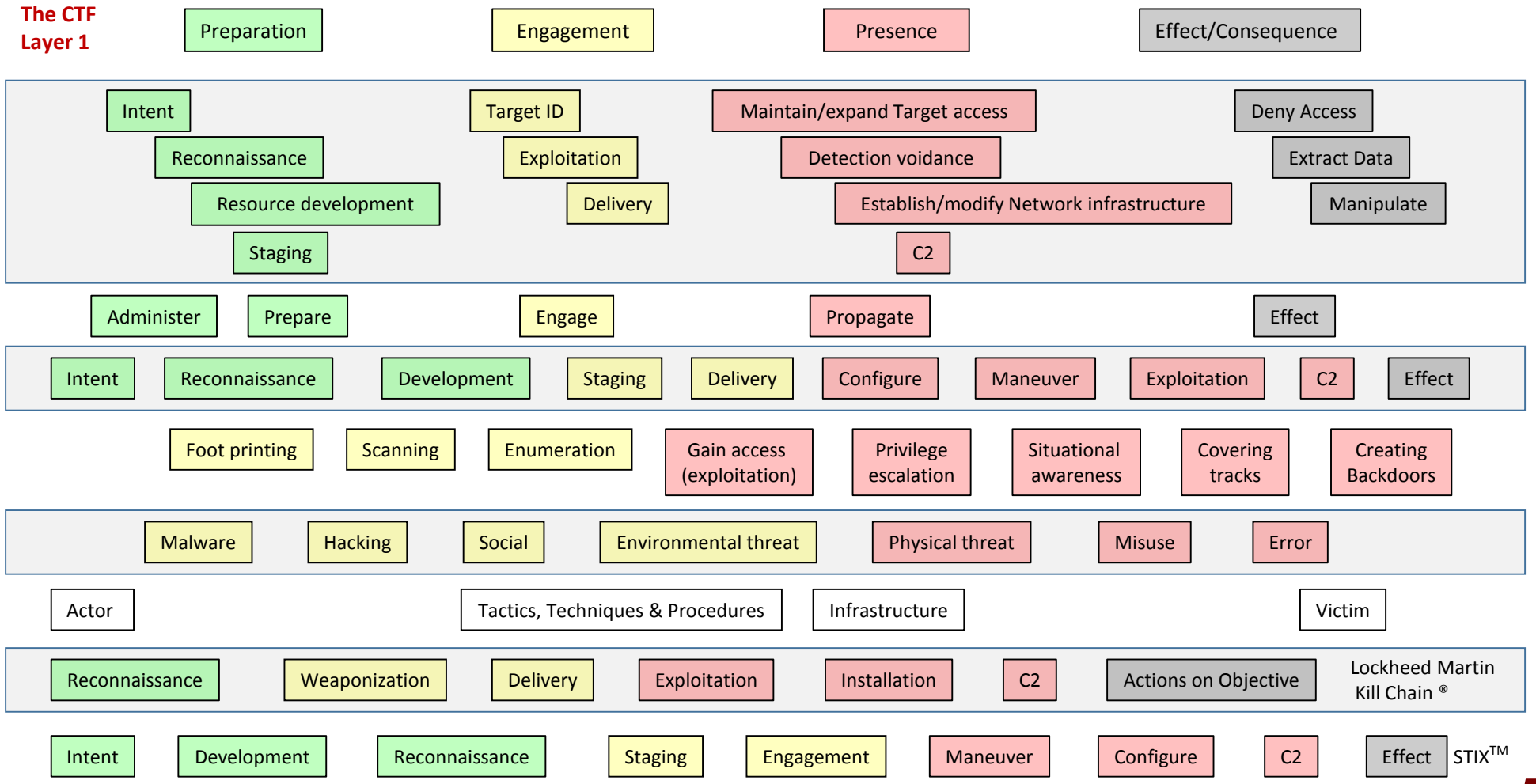


The Common Cyber Threat Framework

Actions and Indicators are the Details of Threat Activity



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



Status of Framework Socialization and Use

- Foundation of threat activity in US government's Cyber Incident Response Schema since 2013
- 2018 OMB priority for implementation across the Executive Branch
- Used in threat products by DHS, FBI and the ODNI
- DHS prototyping use with states and fusion centers and preparing to teach the Framework to state and local partners
- Mapped to the NIST Cybersecurity Framework
- Shared serially with industry and academia; included in curricula and research at multiple universities
- Shared with ~40 partner nations and international organizations; some have adopted it and are exploring its use to create a regional common operating picture and enhance information sharing
- The 'threat description' in NATO's evolving Cyber Defense Strategy
- Research underway on a shareable 'cookbook' on applying the Framework approach to visualization and knowledge discovery
- Framework and associated Lexicon available at DNI.GOV