32nd Annual INCOSE international symposium
hybrid event
Detroit, MI, USA
June 25 - 30, 2022

# An Introduction to Semantic Threat Analysis for Systems Security Engineering

Richard S. Potember, Ph.D.
The MITRE Corporation

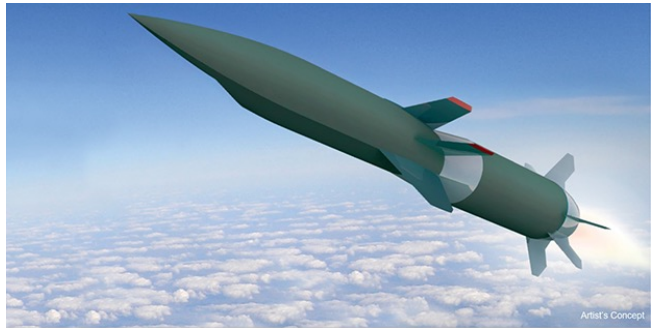
Carlos d'Aragona Balhana
The MITRE Corporation

Leo J. Obrst, Ph.D.
The MITRE Corporation

# Systems Security Engineering (SSE)

- SSE is a specialty of systems engineering that applies scientific and engineering principles to provide a, system-level perspective of system security.
- The primary objective of SSE is to minimize or contain a system's vulnerabilities and to ensure that established countermeasures can protect against these threats.
- SSE principles and practices must be applied to all phases of a threat landscape to identify and reduce vulnerabilities as identified in the system.
- As such, we must understand a systems vulnerabilities to develop appropriate and countermeasures

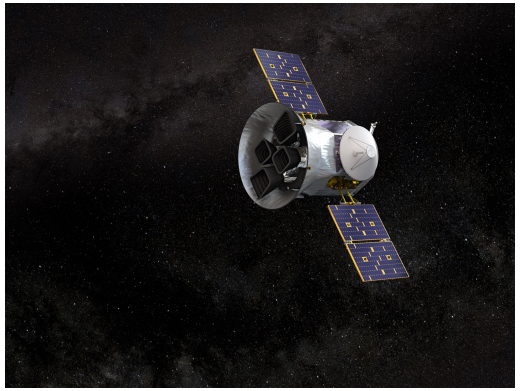
# Critical Platforms Require SSE




Source: DARPA

Source: MDA

Source: U.S. Air Force



Source: NASA

Source: U.S. Navy

# Protecting Critical Systems

- Threats to complex systems are growing at alarming rates
- Adversaries are using ever increasingly sophisticated techniques to try to attack vulnerable systems
- It may not be possible to control an adversary's intentions or capabilities, but it is possible to prevent an attack by denying an adversary an opportunity to do harm
- Preventing an attack or dramatically reducing the harm of an attack can be analyzed, modeled and understood
- Once understood, effective countermeasures can be implemented to reduce the risk of future attacks and protect our critical systems

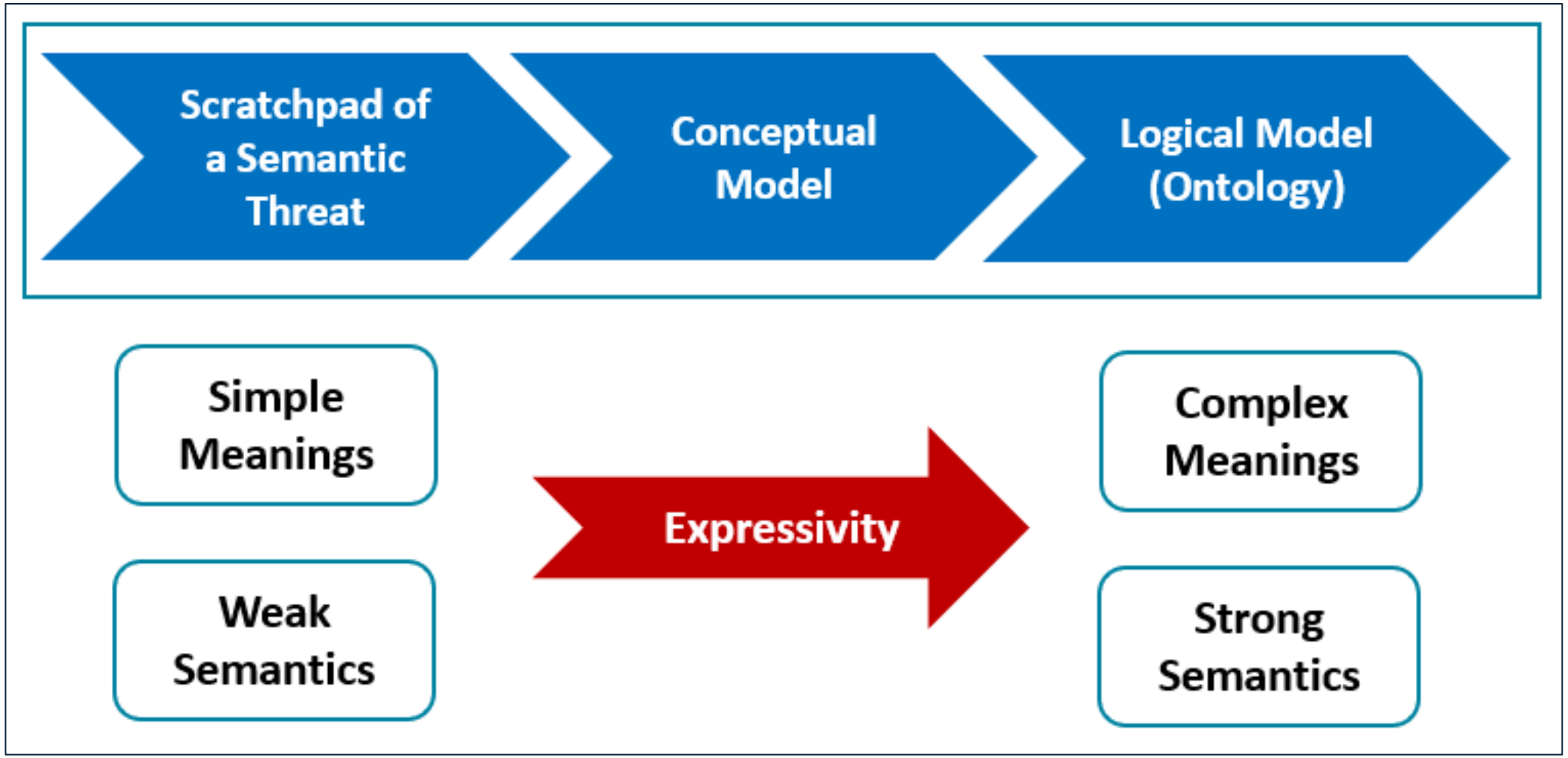
# Systems Security Engineering (SSE)

SSE leverages many security specialties and focus areas that contribute to systems security engineering activities and tasks

These areas include:

- computer security
- communications security
- transmission security
- anti-tamper protection
- electronic emissions security
- physical security
- information software and hardware assurance
- technology specialties such as biometrics and cryptography

# Semantic Expressivity Spectrum



# Threat Domain
# A Conceptual Model

# Conceptual-model Approach

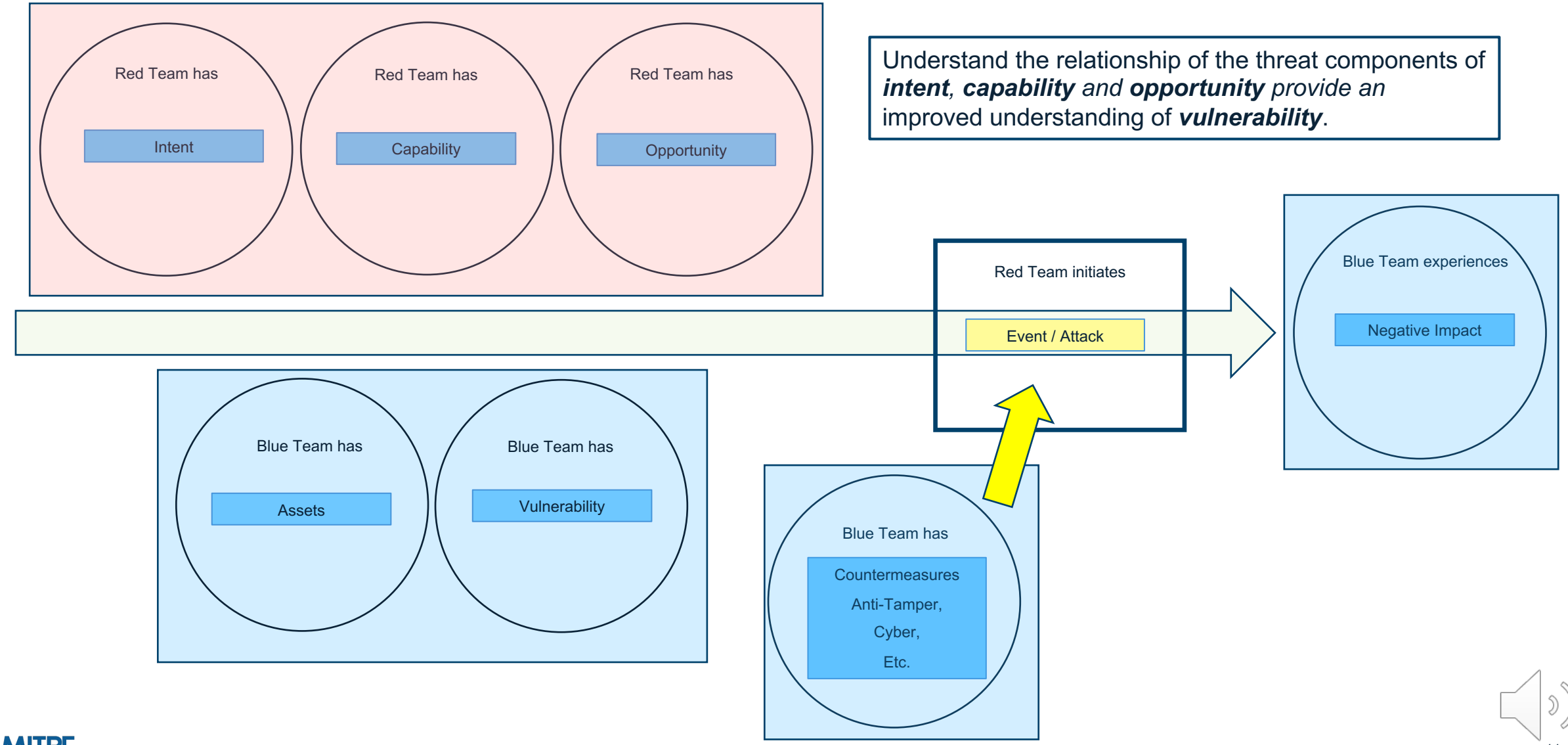
- Securing large complex systems is difficult
- Threats continually change as defensive capabilities are upgraded and attackers develop innovative techniques to adapt to in an ever-evolving threat landscape.
- A threat management approach shows all of the possible interactions and how they interact with one another
- A Conceptual-model can significantly improve SSE's knowledge of current threats, vulnerabilities, assets, and countermeasures

# Build a Model of an attack

A conceptual model captures:

- The framework of potential attacks
- Technologies used by the attacker
- Source and target of an attack
- Impact on the system components affected by the attack
- Vulnerabilities exploited by the attack
- Countermeasures and policies for mitigating these attacks

# Threat Components



# Threat Diagram

It is a pictorial representation of the complex processes used to secure a system

A Threat Diagram can help us to represent and analyze **threats** to protect an enterprise's **assets**.

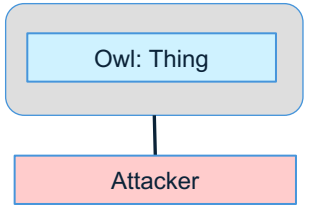
This approach provides a methodical way to determine viable threat vectors (who, why and how a system can be compromised).

It can be defined as a diagram that represents a **threat** domain.

**Legend**

Attacker = Red
Defender = Blue

Ontology in Development

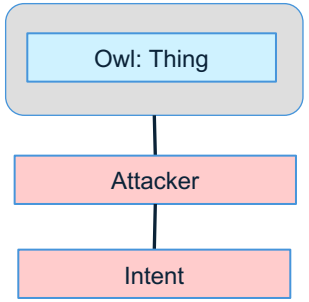



**Attacker** - Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

**Legend**

Attacker = Red
Defender = Blue

Ontology in Development



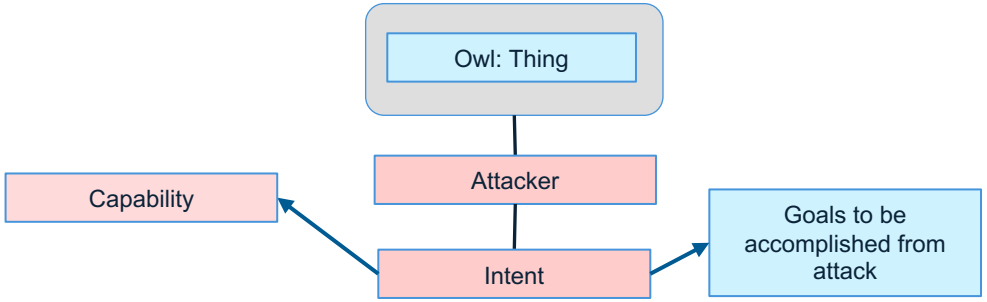

**Intent** is resolved or determined to do harm to U.S. Assets.

MITRE

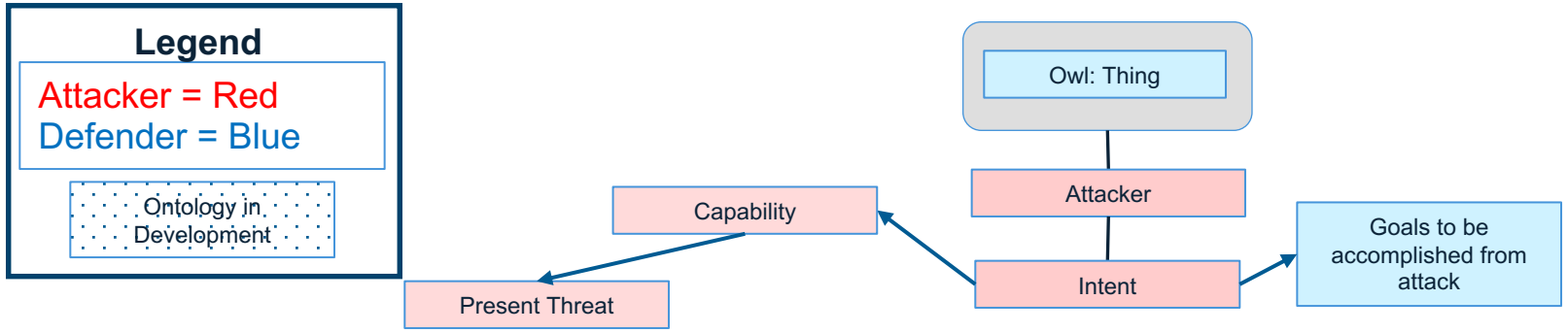
**Legend**

Attacker = Red
Defender = Blue

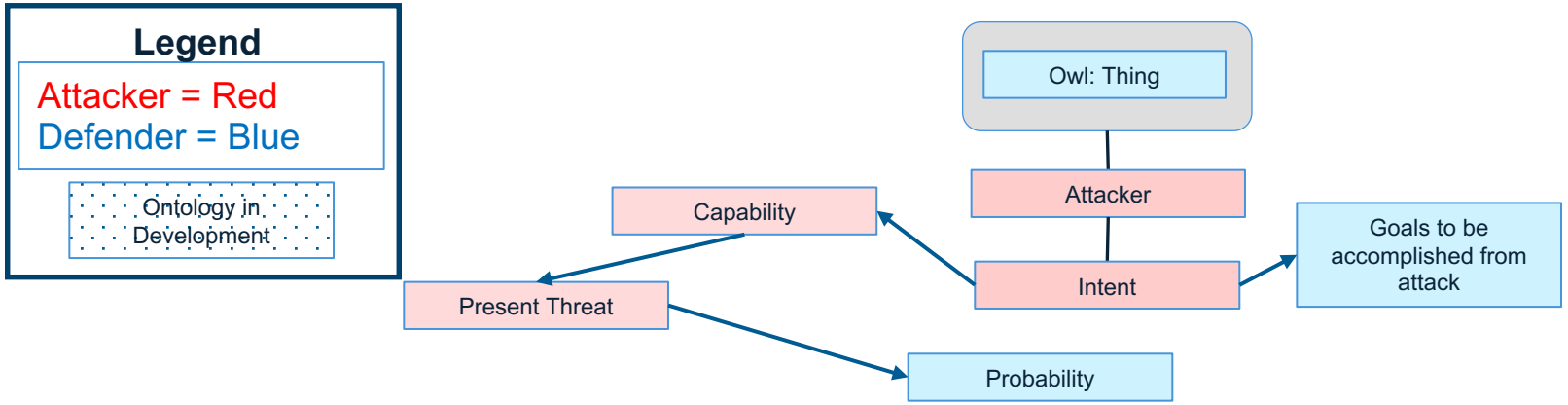
Ontology in Development

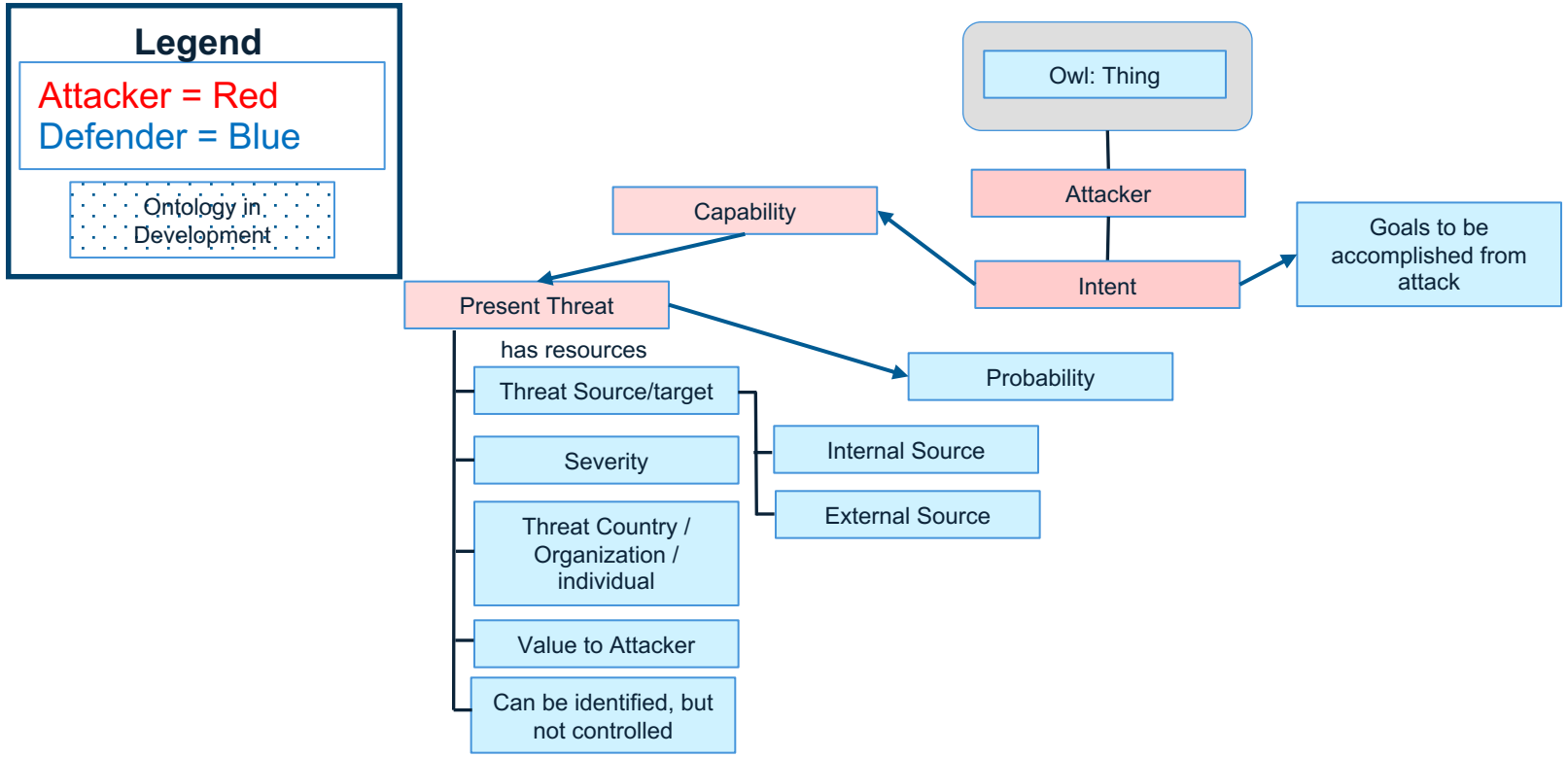


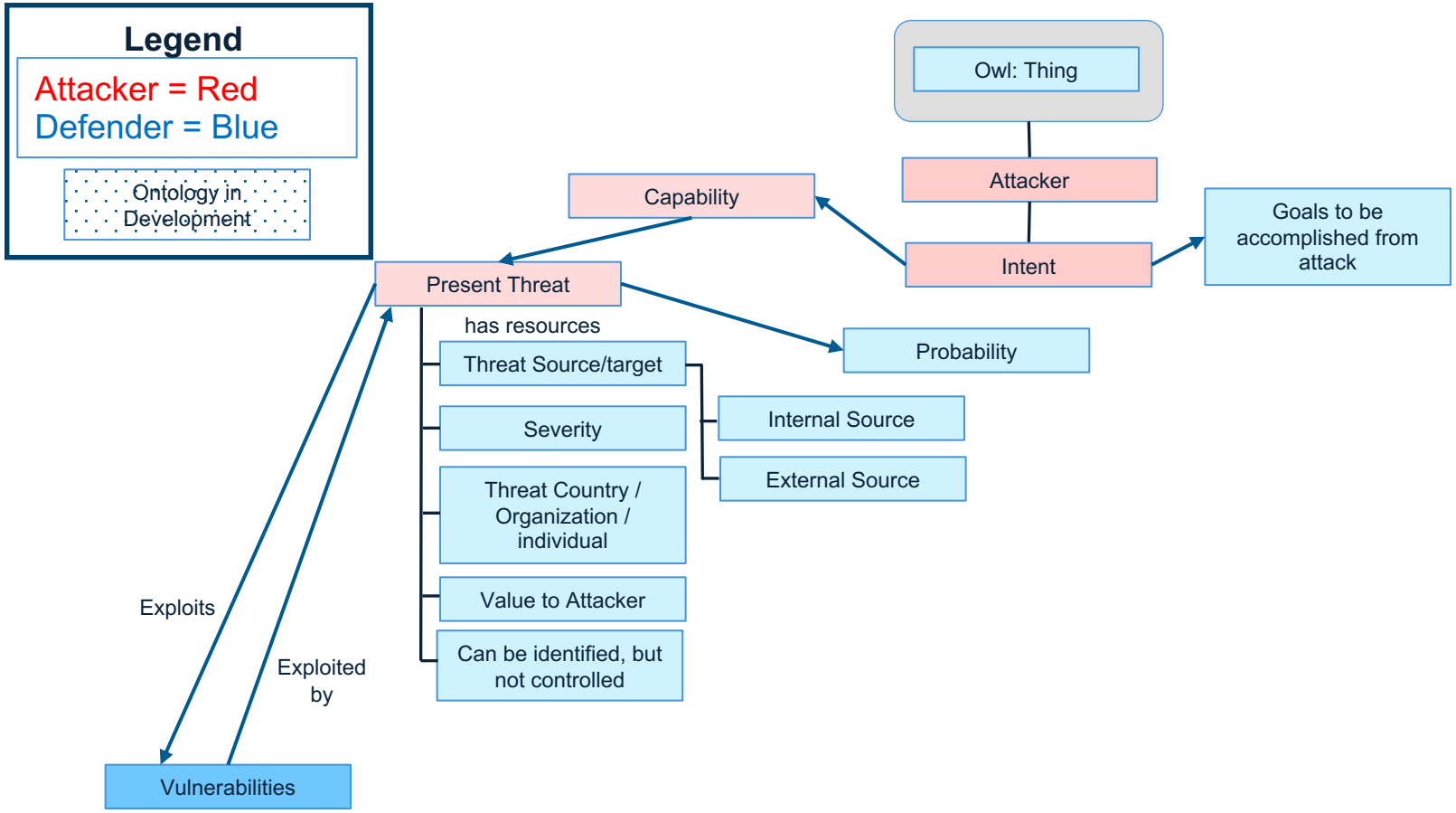

**Capability** is the power or ability to cause harm.



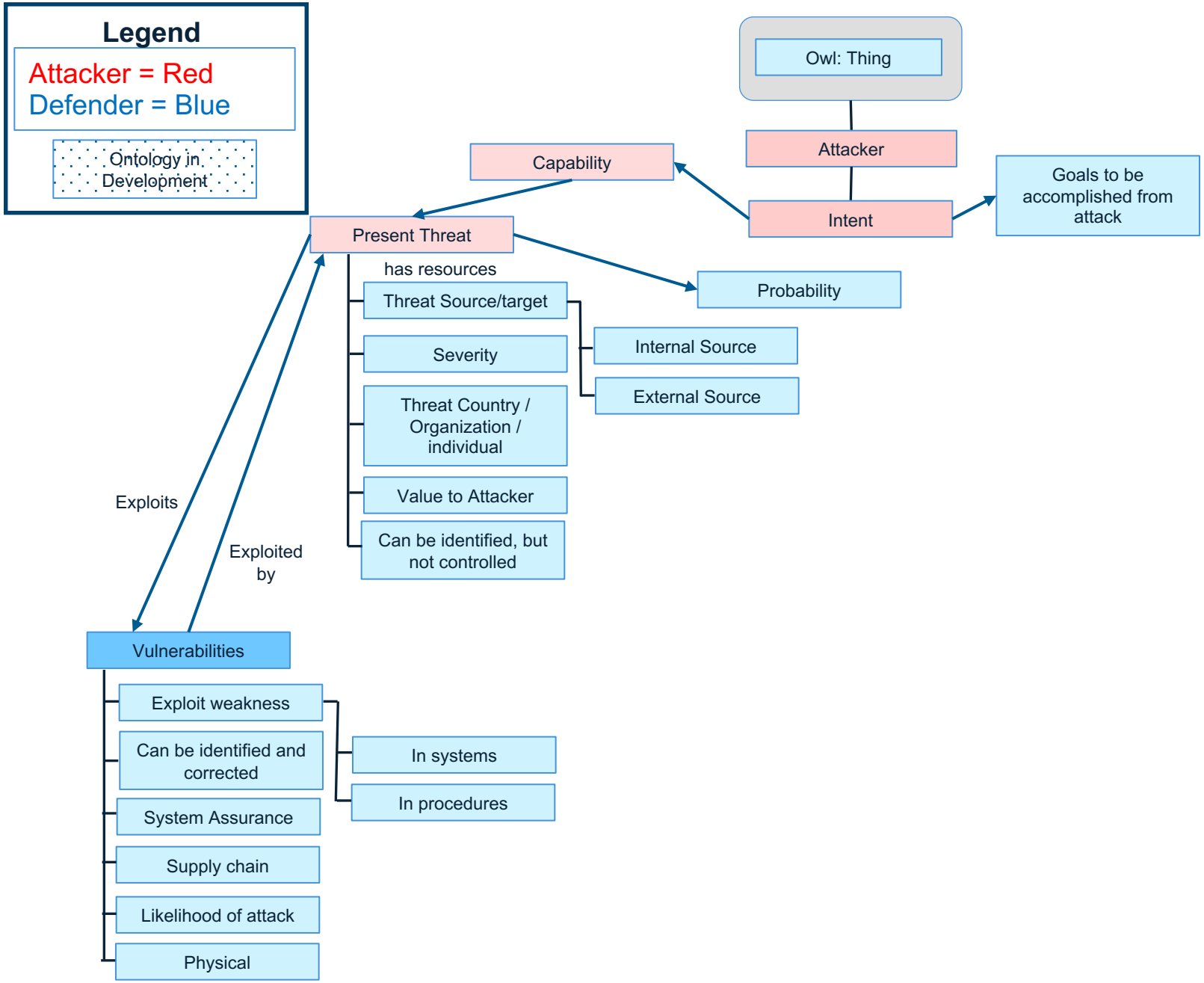

A **threat** can be defined as “a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm”

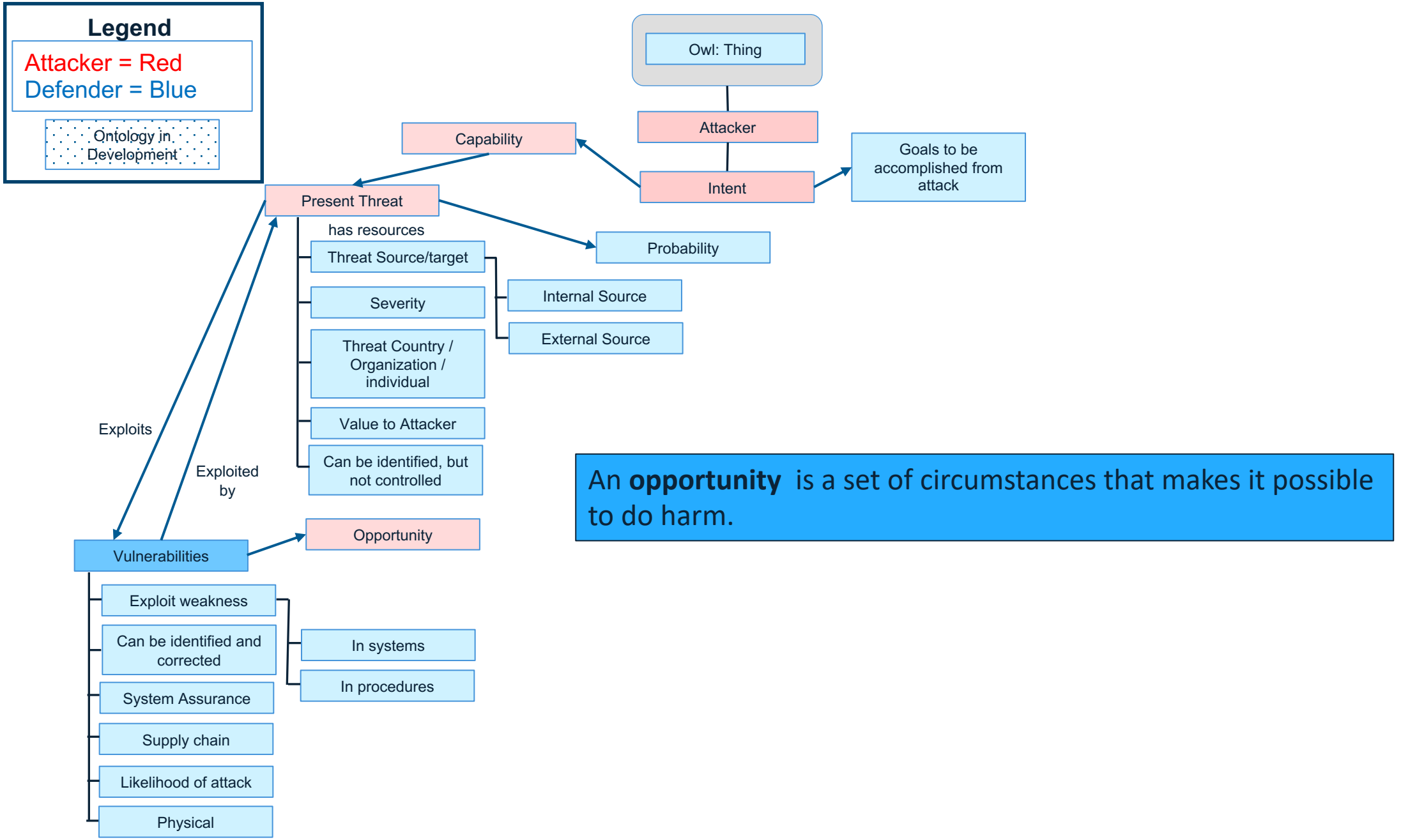




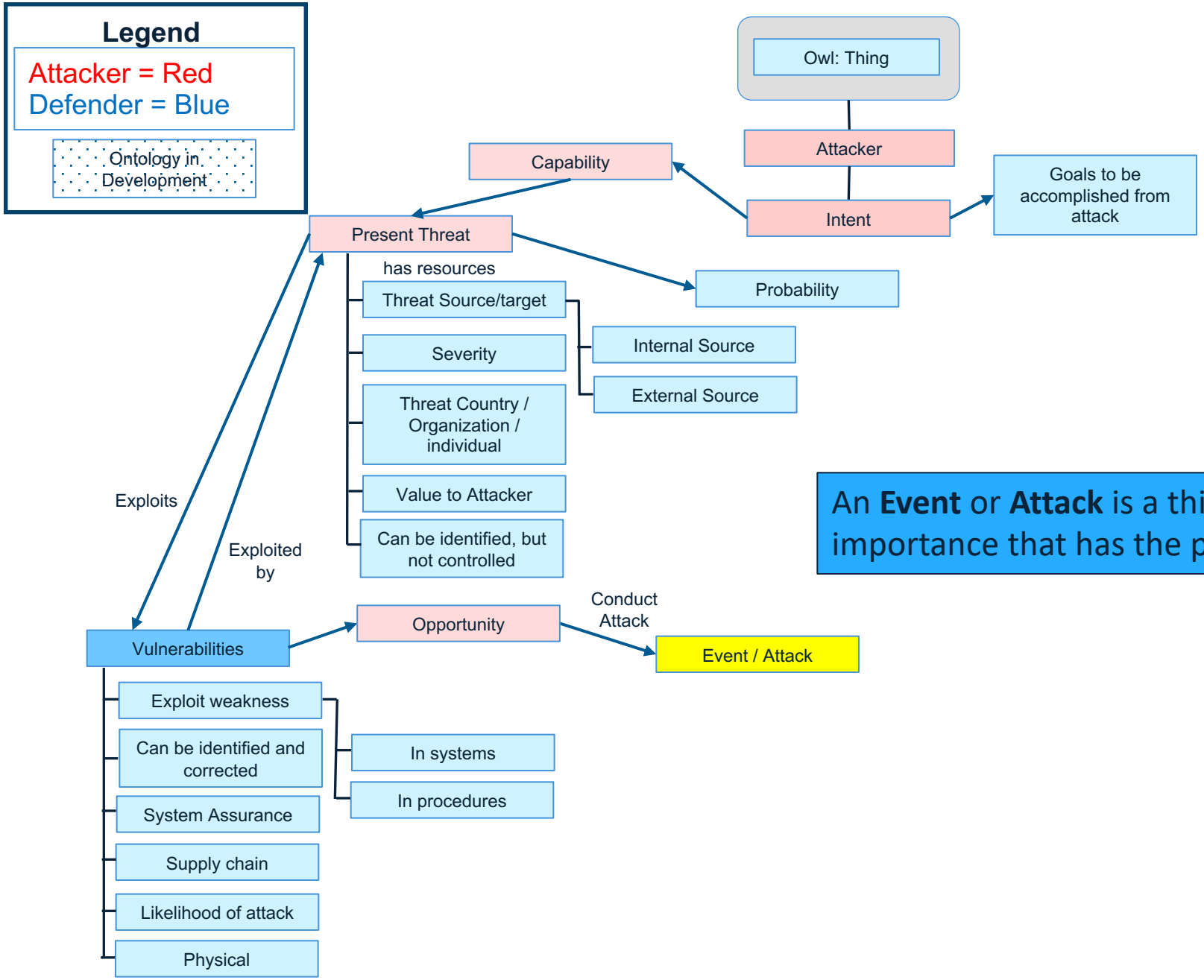



A **vulnerability** is the state of being exposed to the possibility of being attacked or harmed.

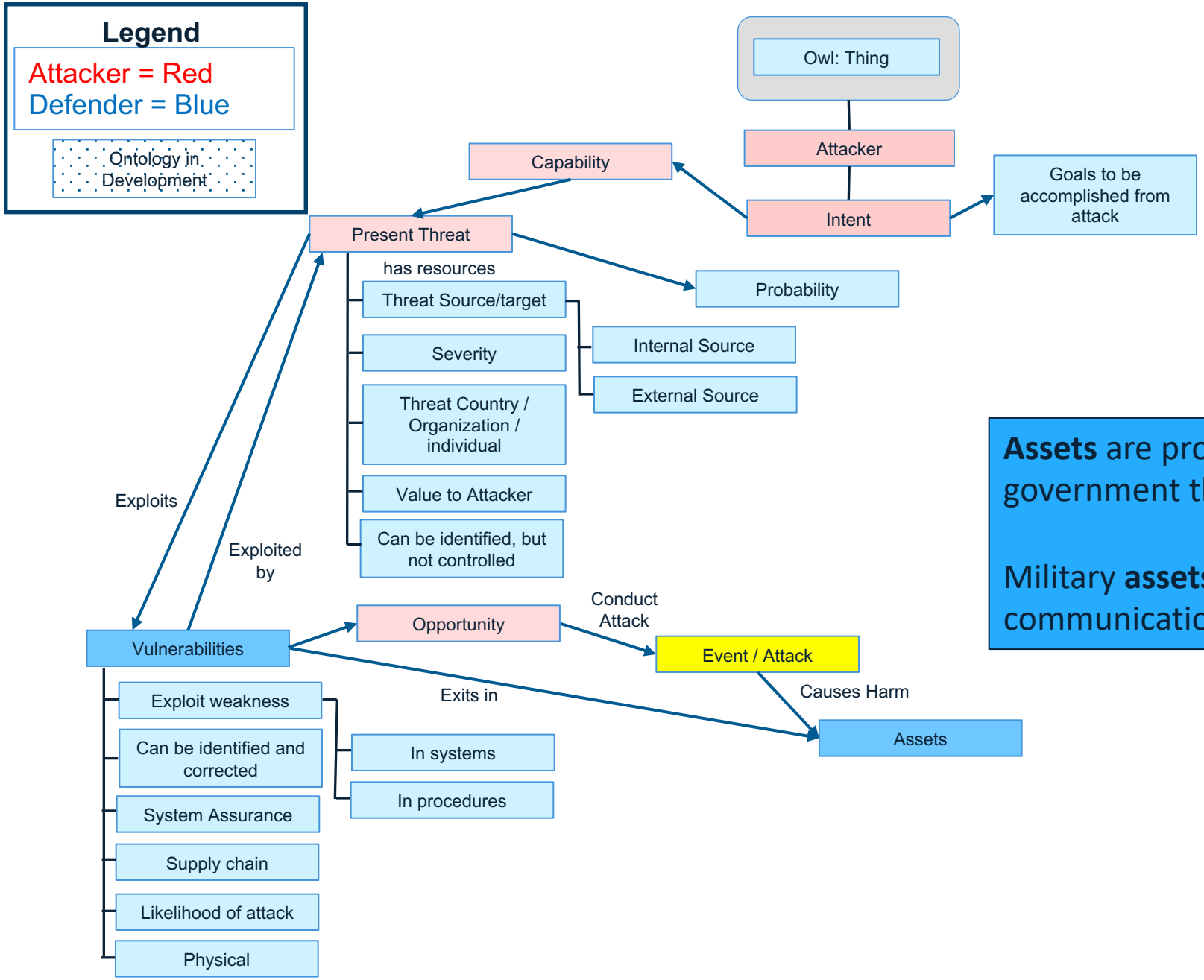





An **opportunity** is a set of circumstances that makes it possible to do harm.



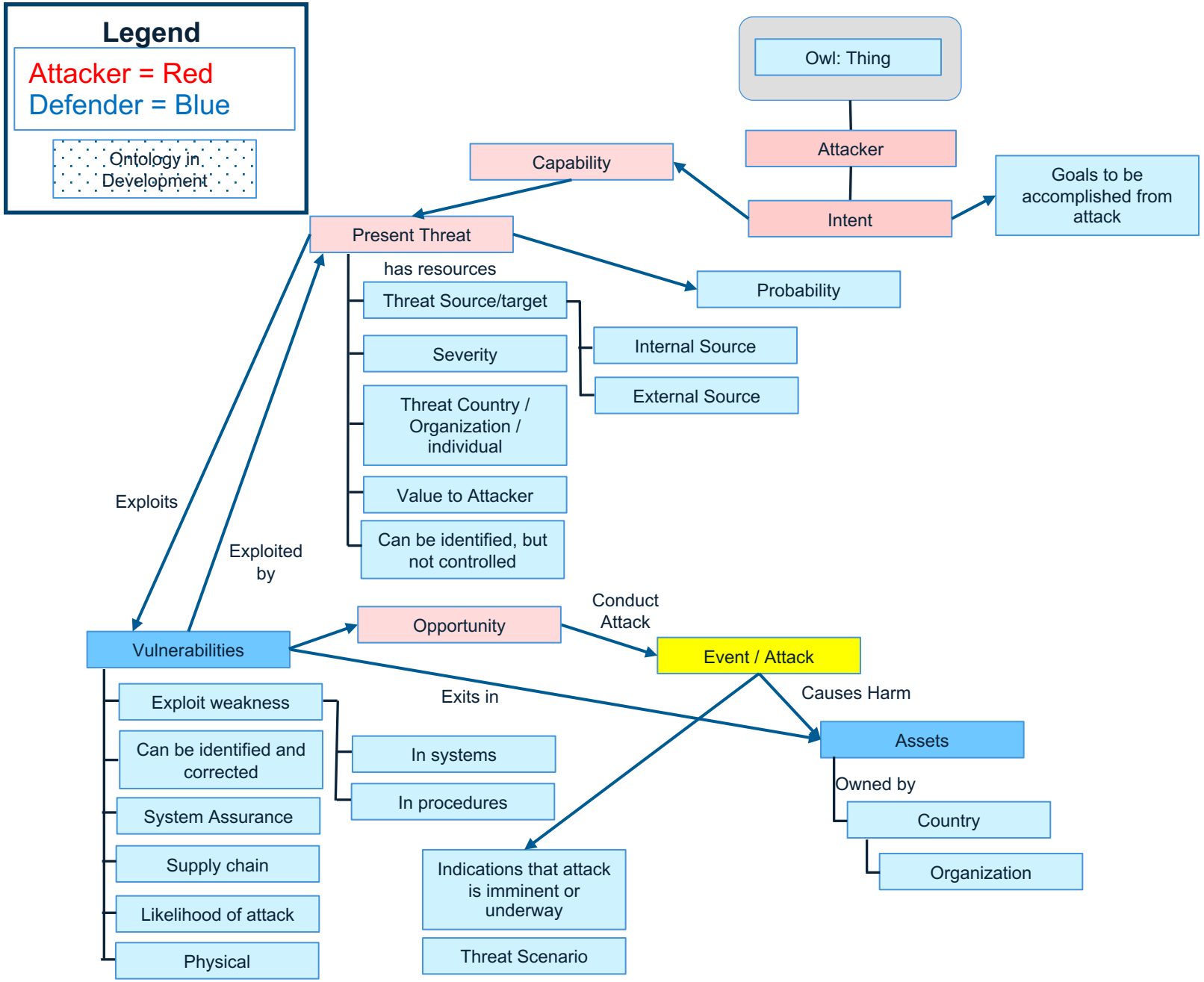

An **Event** or **Attack** is a thing that happens, especially one of importance that has the potential to cause harm.

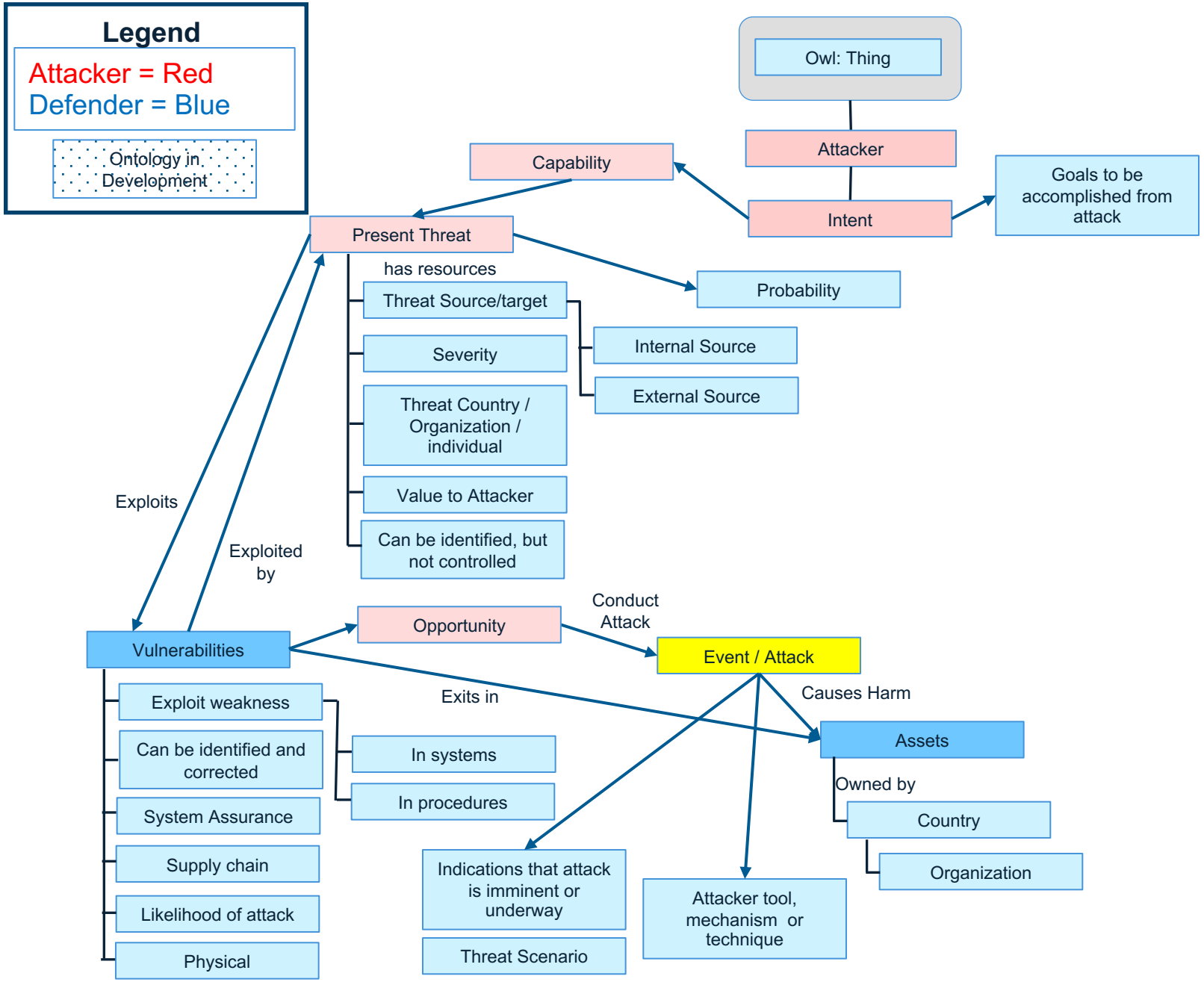


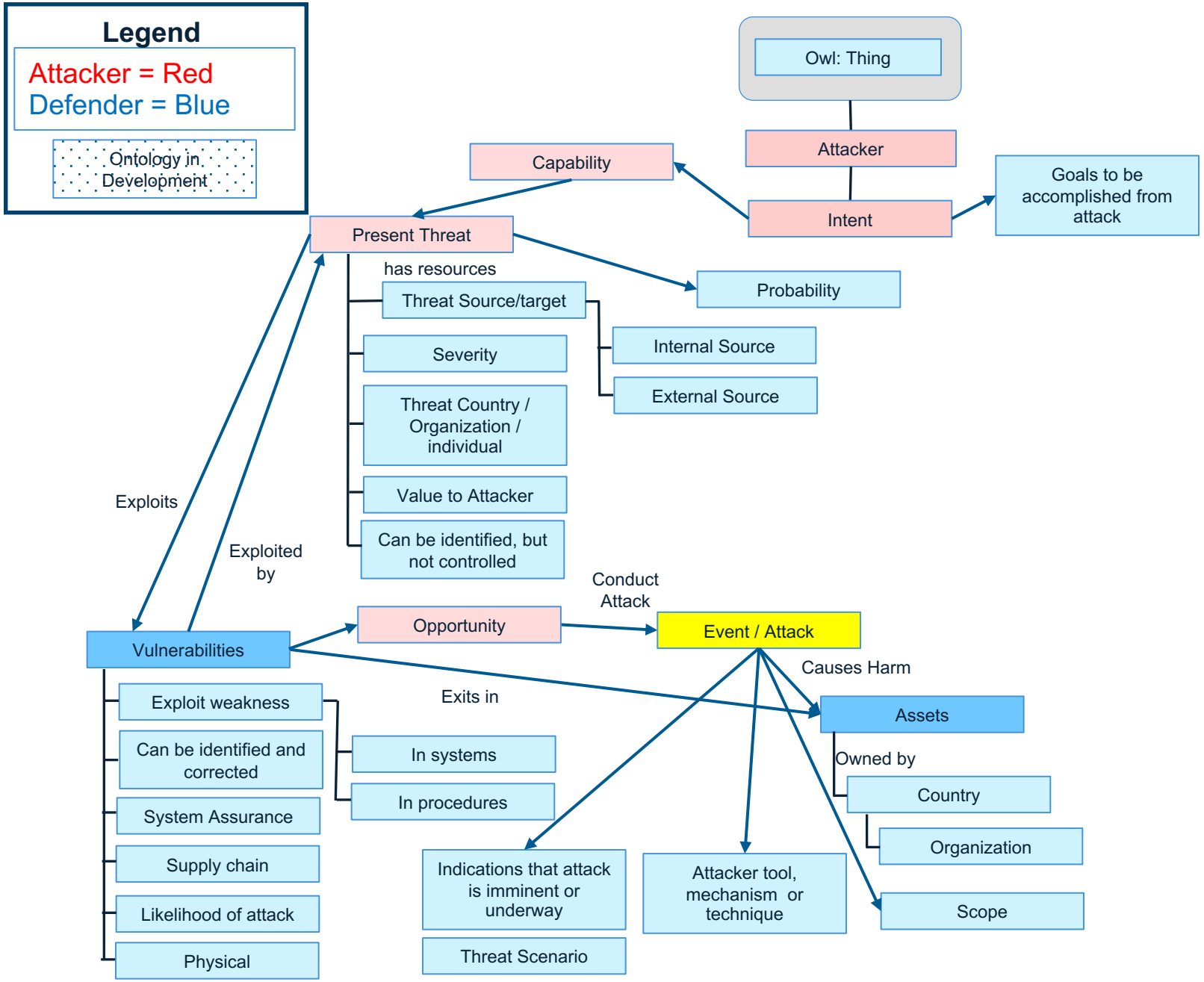

**Assets** are property owned by a person or company or government that has value

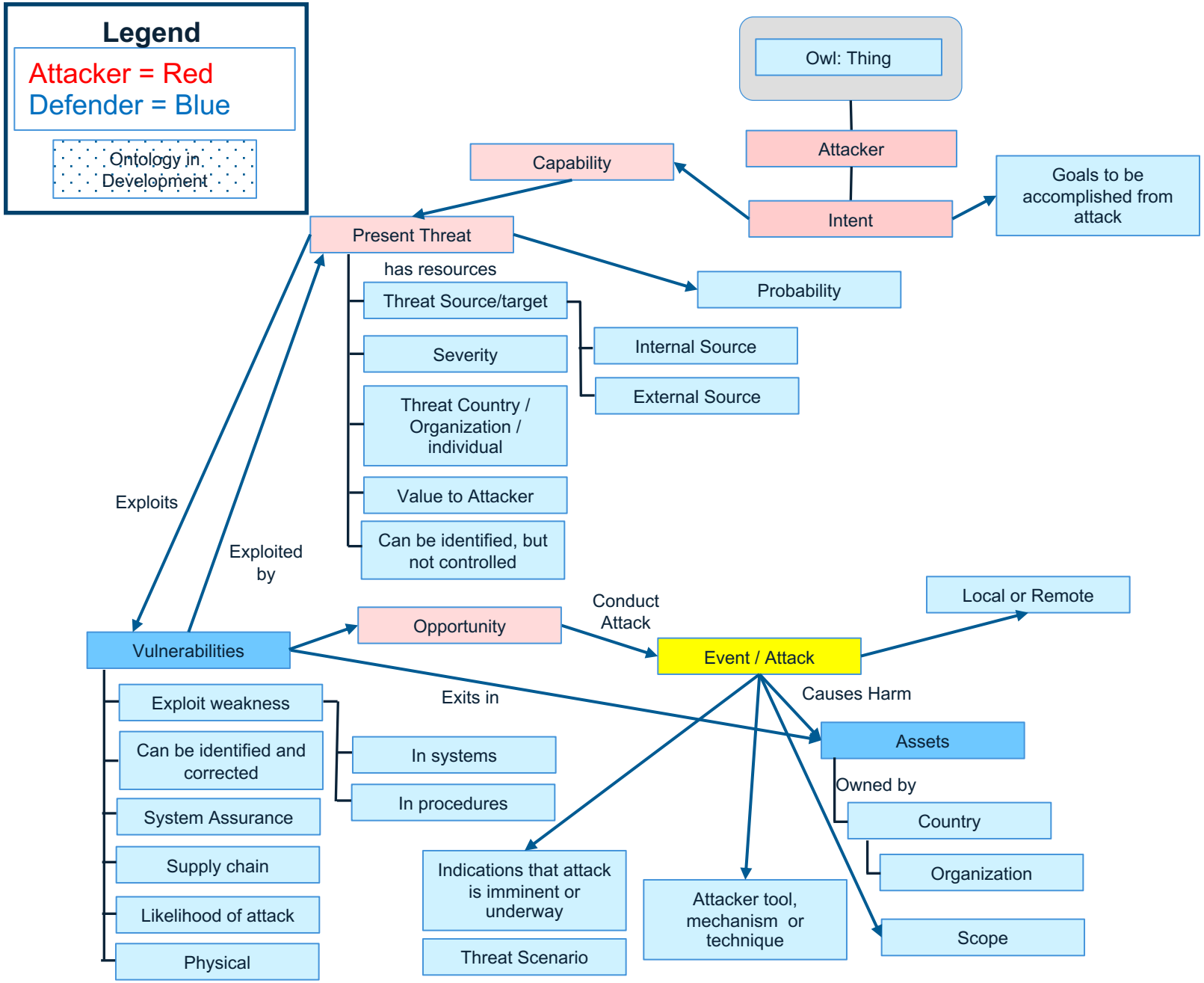
Military **assets** are equipment, such as planes, ships, communications and radar installations, etc.

MITRE

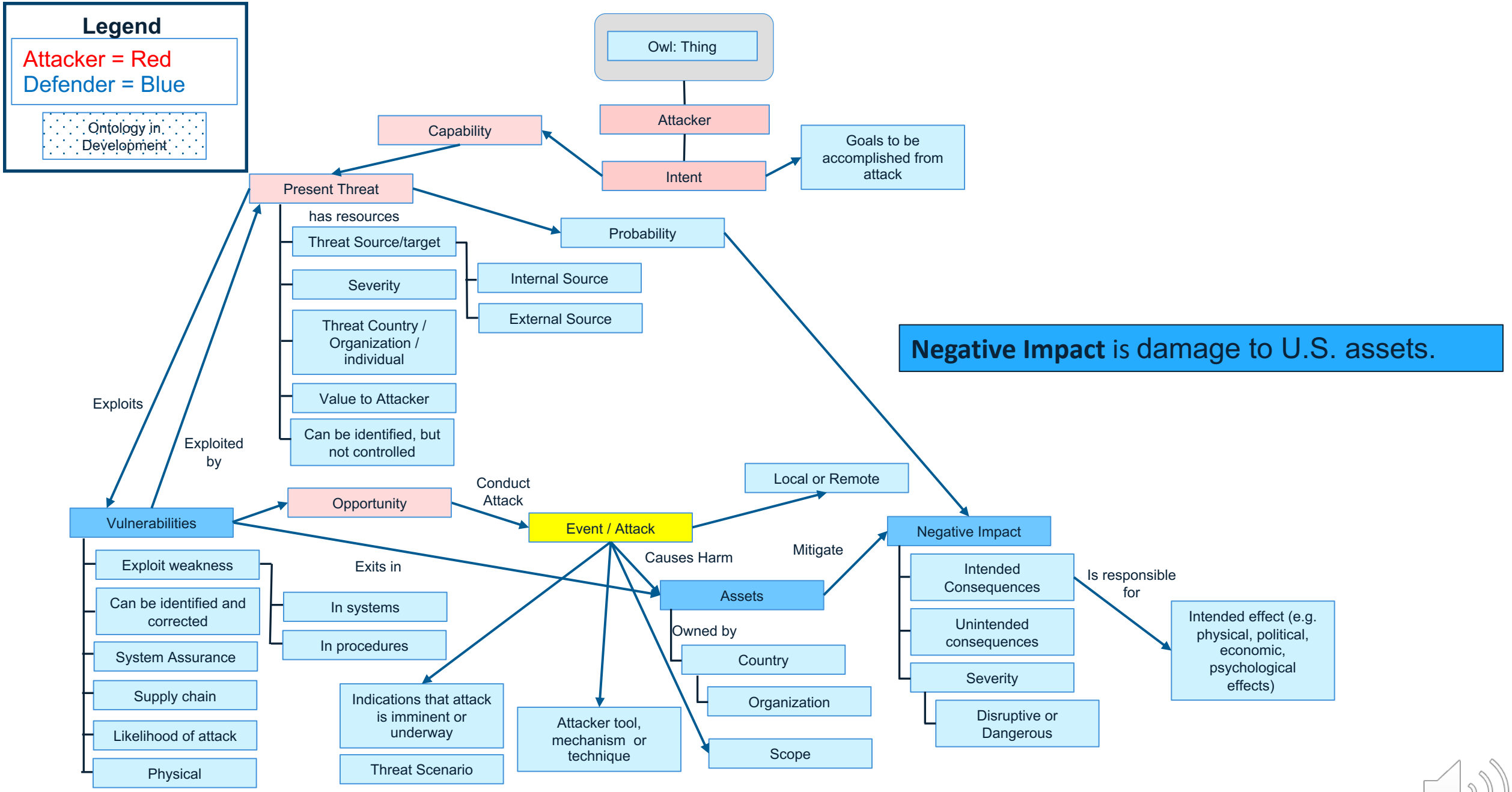


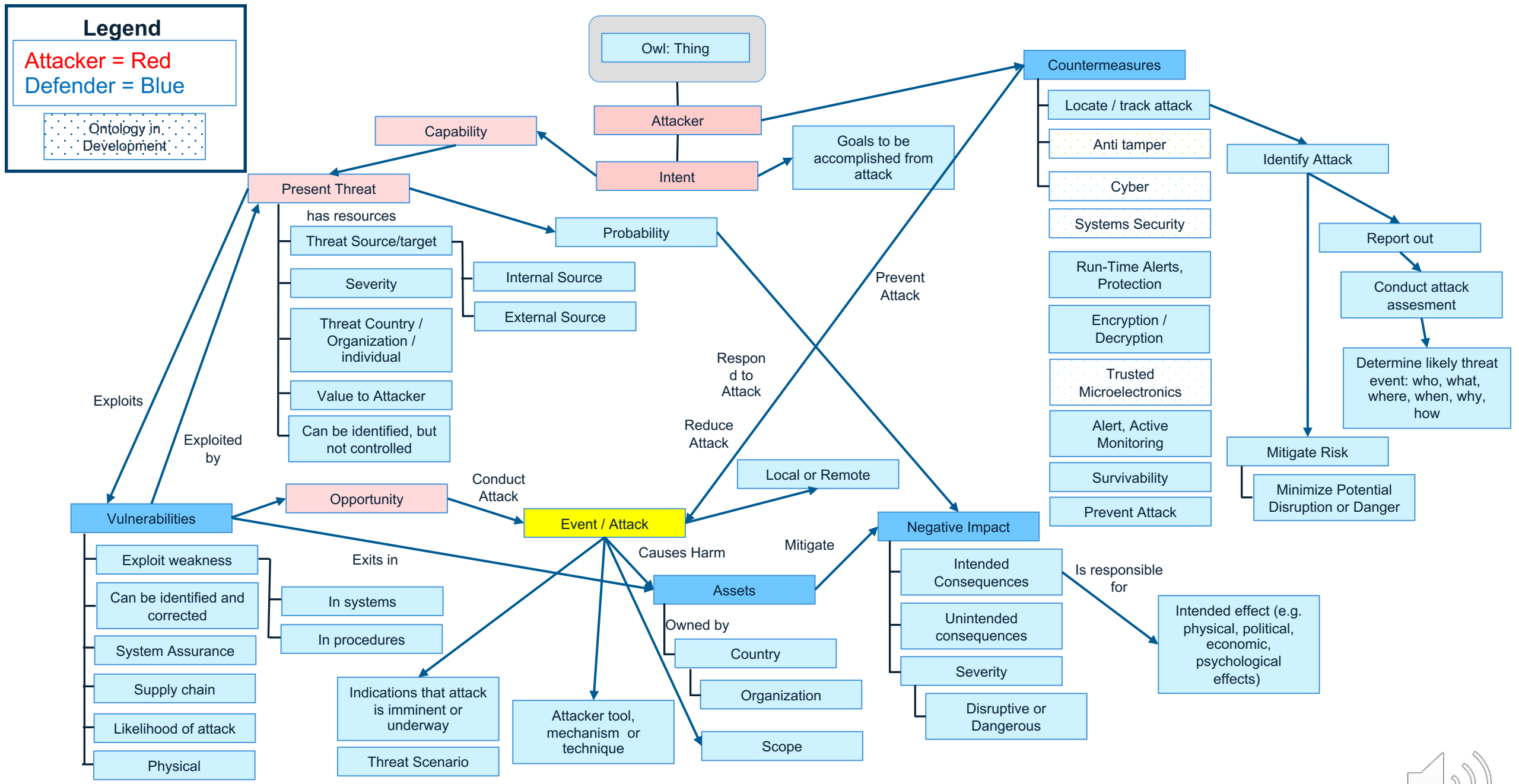


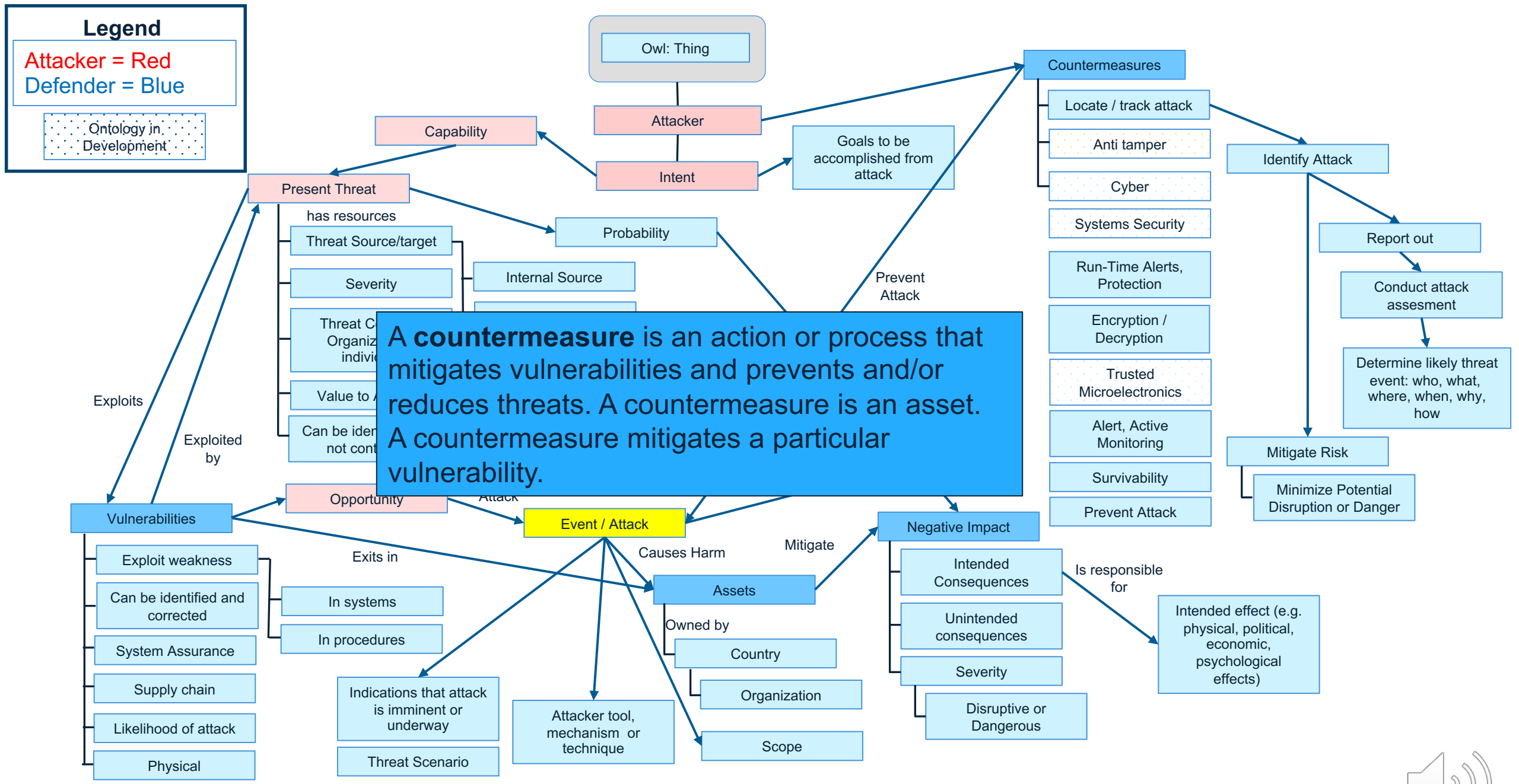





MITRE







# Multiple applications for the conceptual model

- Construct a Taxonomy and Ontology
- Guide Research and Development to assure the SSE is integral to the effort
- Assure that SSE principles are built into a System's Life Cycle
- Use in Contracting
- Develop Requests for Proposals, Broad Area Announcements, Announcements of Opportunity that incorporate SSE tenants
- Test countermeasures
- Build enhanced countermeasures
- Develop effective scenarios or use cases
- Support tabletop exercises
- Create a repository of technical data and determine what data is needed
- Standards and shared definitions
- Train personnel

# Construct an ontological model for systems security

- The conceptual model can be used to construct an ontology for each countermeasure
- The visual framework facilitates the development of the ontology
- Within an OWL-based framework, Intent, Opportunity, Capability, Threat, and Vulnerability are classes, and the exploitation of system elements by these classes is represented as object properties
- By representing a threat space in an ontology, we can overcome the difficulties of describing threats by complex and imprecise terms

# Thank you.

Richard S. Potember, Ph.D.

rpotember@mitre.org

240-274-1086

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™