IDA
Institute for Defense Analyses
4850 Mark Center Drive • Alexandria, Virginia 22311-1882

Cyber Ontology: Is it the World Squared?

STIDS 2012
October 25, 2012

Brian Haugh (bhaugh@ida.org)

IDA

Cyber : Defining Terms

- Cyber(space) Definitions:
  - *“.. in current usage the term "cyberspace" stands for the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems*.” [http://en.wikipedia.org/wiki/Cyberspace]
  - cyberspace — *A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.* [Joint Pub 1-02, 2011]
- Ontology
  - *An ontology is an explicit specification of a conceptualization.* [Gruber, Thomas R. (June 1993). "A translation approach to portable ontology specifications." *Knowledge Acquisition* **5** (2): 199–220.]

IDA

Cyber Ontology: Defining Scope

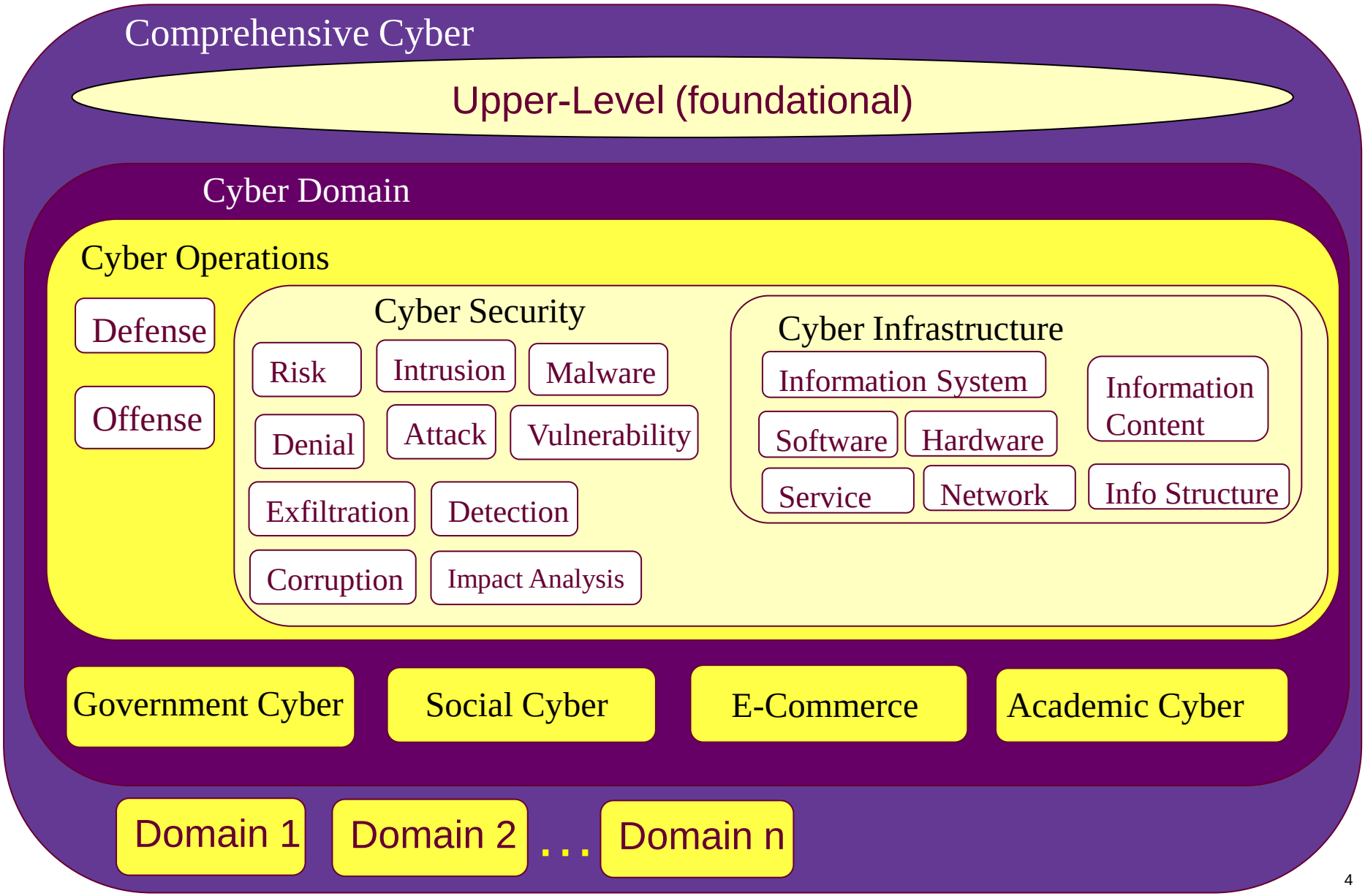
- Comprehensive Cyber(space) Ontology
  - All ontological elements ever needed in systems designed to analyze aspects of the cyber(space) domain
  - Requires the “world squared”
- Cyberspace Domain Ontology
  - Focused on principal ontological elements in the cyber domain
  - Augmented with separate upper and middle level ontologies
  - Not the “world squared”, though far reaching
- Cyberspace Security Domain Ontology
  - Focused on ontological elements in cyber security domain
  - Cyber-Security Sub-domains
    - Offense
    - Defense
    - Impact Analysis & Response

Cyberspace Security Domain Ontology

- Numerous Cyberspace Security Concepts Needed
  - Cyber Activity
  - Cyber Attack
  - Cyber Counterattack
  - Cyber Data Collection
  - Cyber Defense
  - Cyber Denial of Service
  - Cyber Exfiltration
  - Cyber Force Application
  - Cyber Information Sharing
  - Cyber Intrusion
  - Cyber Intrusion Vector
    - Worm
    - Virus
    - Malware, …
  - Cyber Operation
  - Cyber Pre-emption
  - Cyber Retaliation
  - Cyber Sabotage
  - Cyber Scanning
  - Cyber Superiority
  - Cyber Threats
  - Cyber Vulnerability
  - Cyber Networks
  - Network Node
  - Network Link
  - Data Center
  - Processors
    - CPU, GPU, FPGA, …
  - Cyber Media
    - Disk Image
    - Computer File, …
  - Cyber Service
  - Software
  - Information Architecture (DM2 ontology)
  - Information Bearing Entity
  - Information Content Entity
  - Information Operations
  - Information Security
    - Availability
    - Confidentiality
    - Integrity
  - ….

IDA

Some Possible Cyber Ontologies



IDA

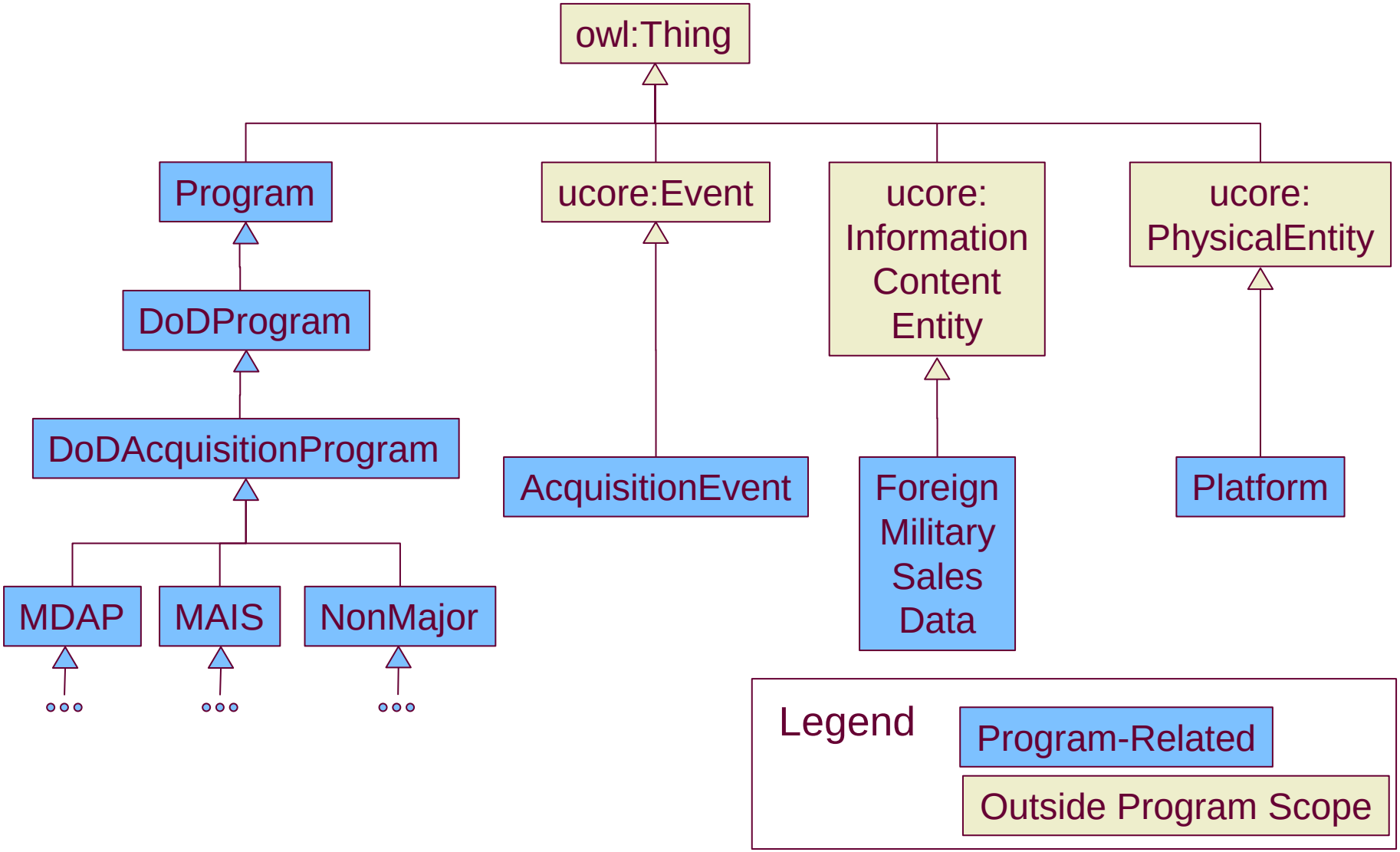
Example Cyber Ontology Application

- In 1Q 2011, IDA began a task assessing the impact of system compromises
- Some of the information needed to be modeled using concepts from existing Department of Defense (DoD) databases
  - Records and tracks events judged potentially compromising
  - Also records reactions and responses to those events
- Recording these items requires describing the DoD program(s) affected by the compromised systems

How should a DoD program be described?

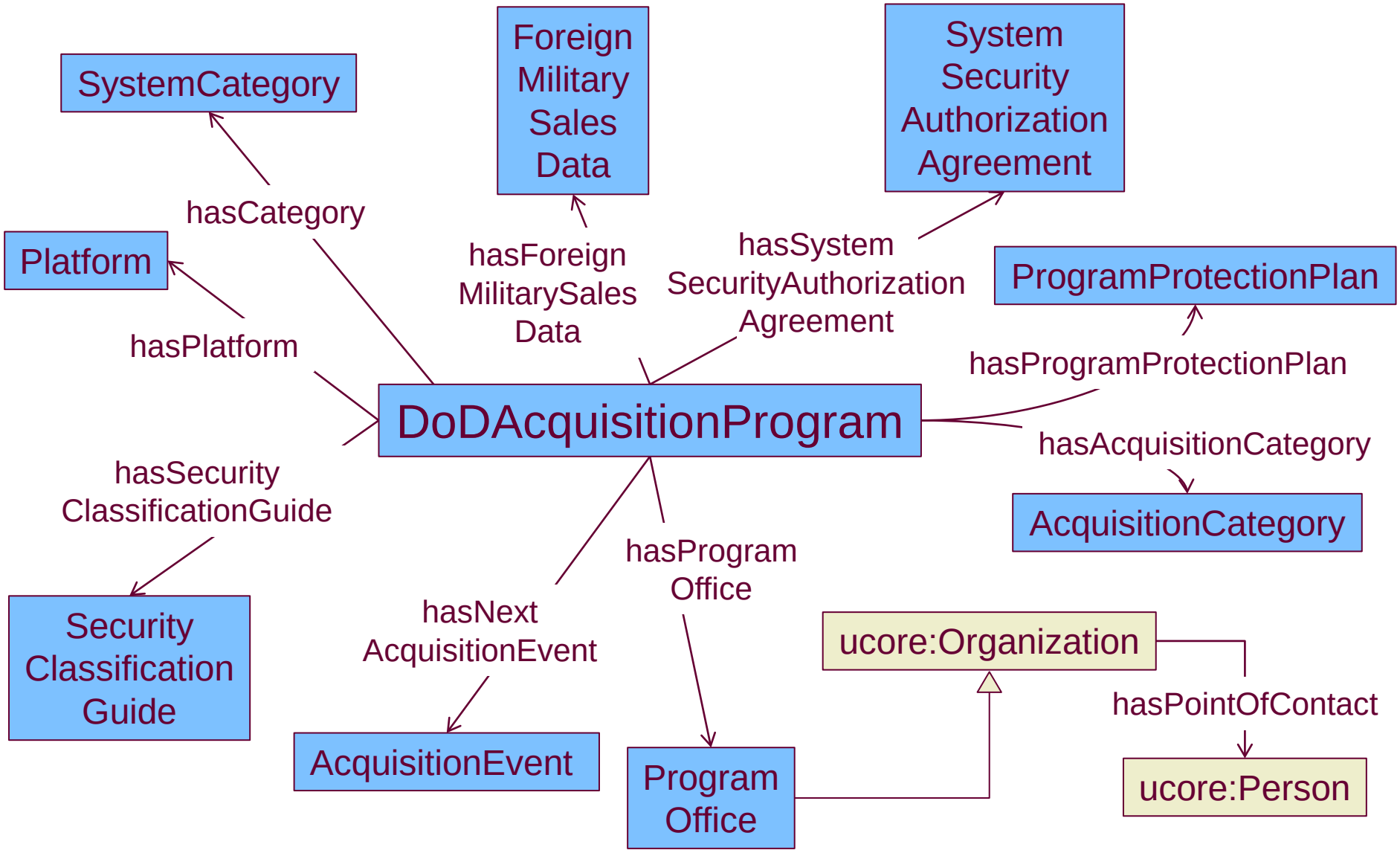
IDA

Ontology Snippet: Class Hierarchy



IDA

Ontology Snippet: Properties

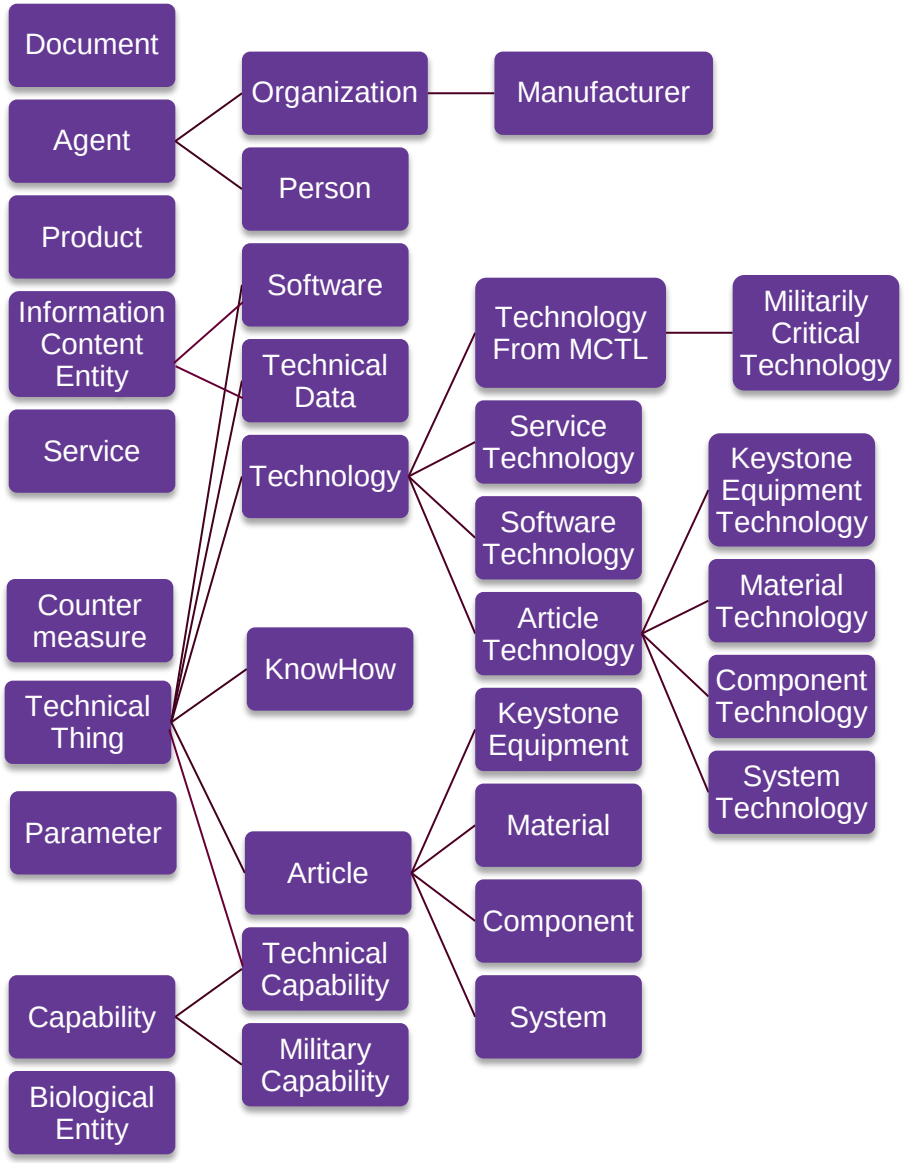


IDA

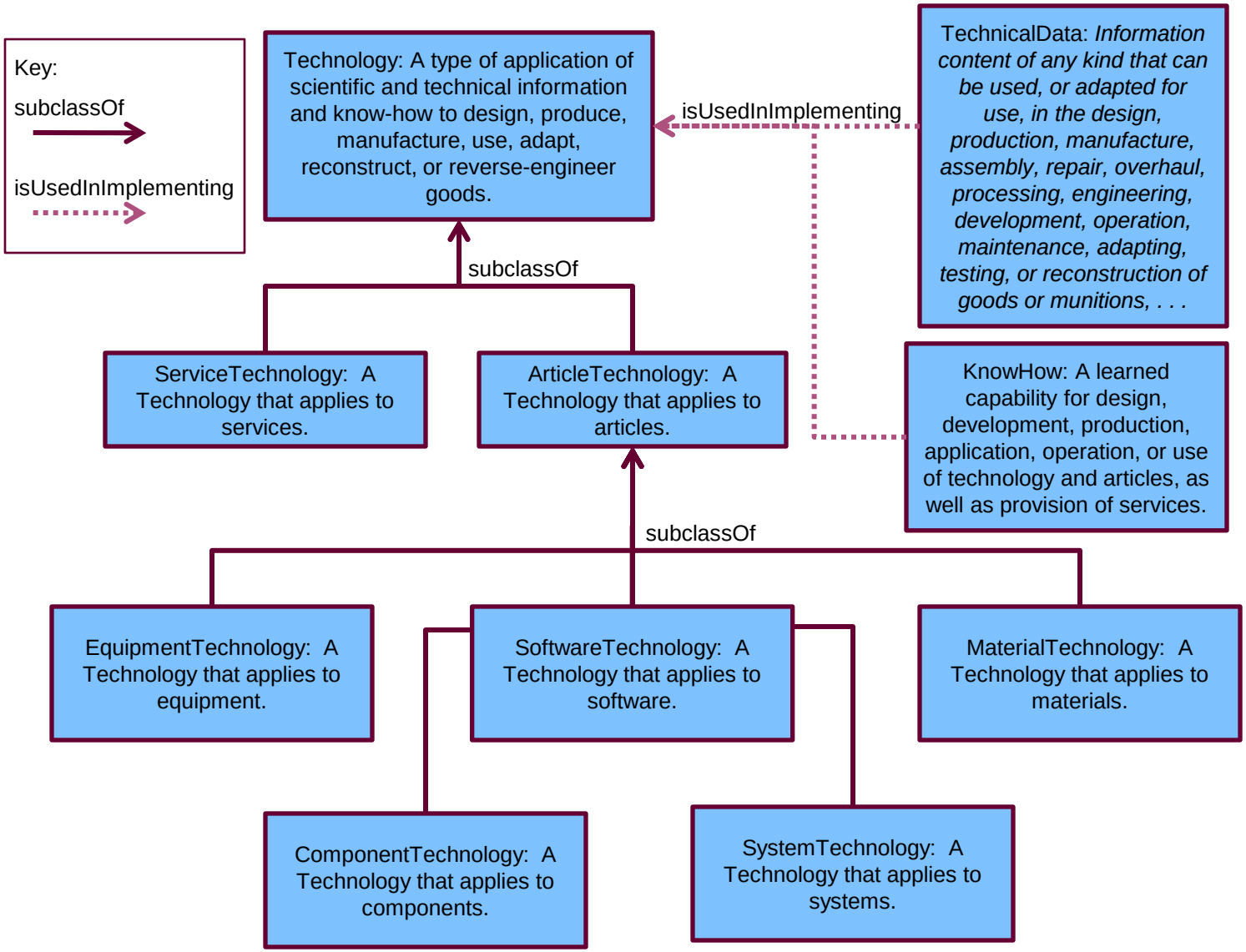
Program Ontology in Context

- Program Ontology is part of an ontology suite:
  - Damage assessment
  - Militarily critical technologies
  - Electronic warfare
  - Joint capability areas
  - Metadata
- Ontology suite metrics:
  - 2,987 classes
  - 345 object properties
  - 117 datatype properties
  - 5,261 individuals

Technology and Related Classes

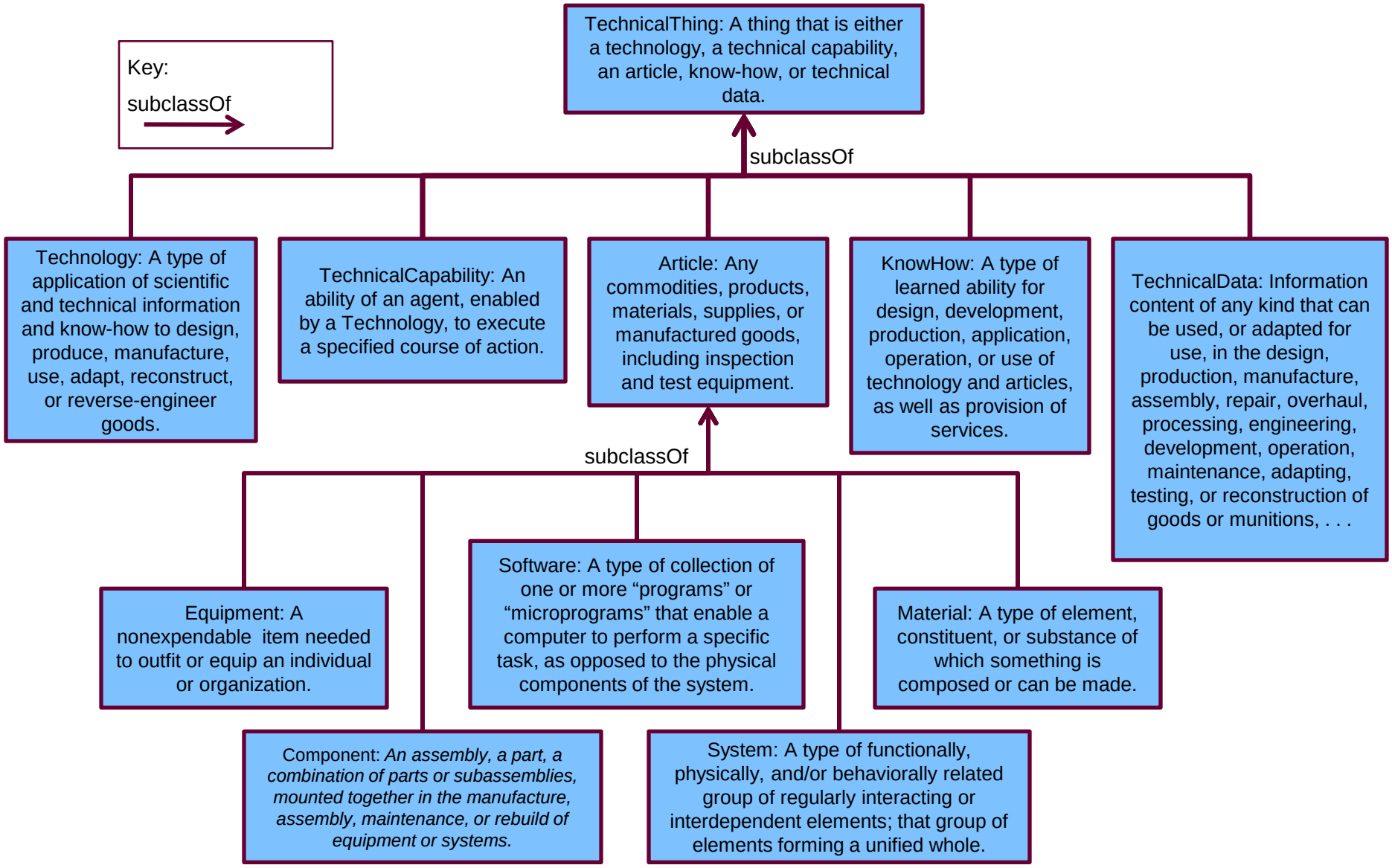


Technology Base Structure

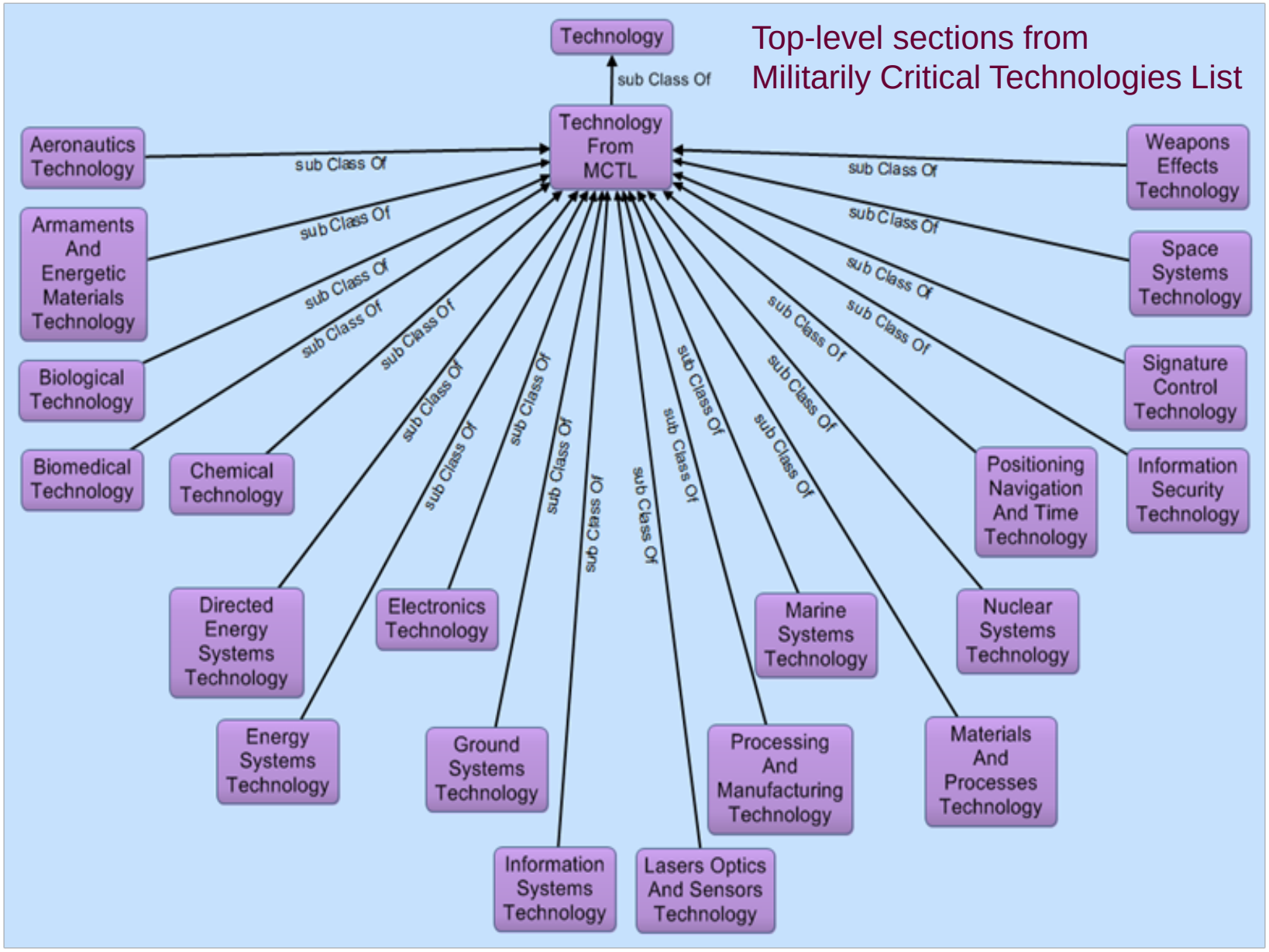


10

Subjects of Technology Lifecycle Relationships



Militarily Critical Technology Classes



IDA

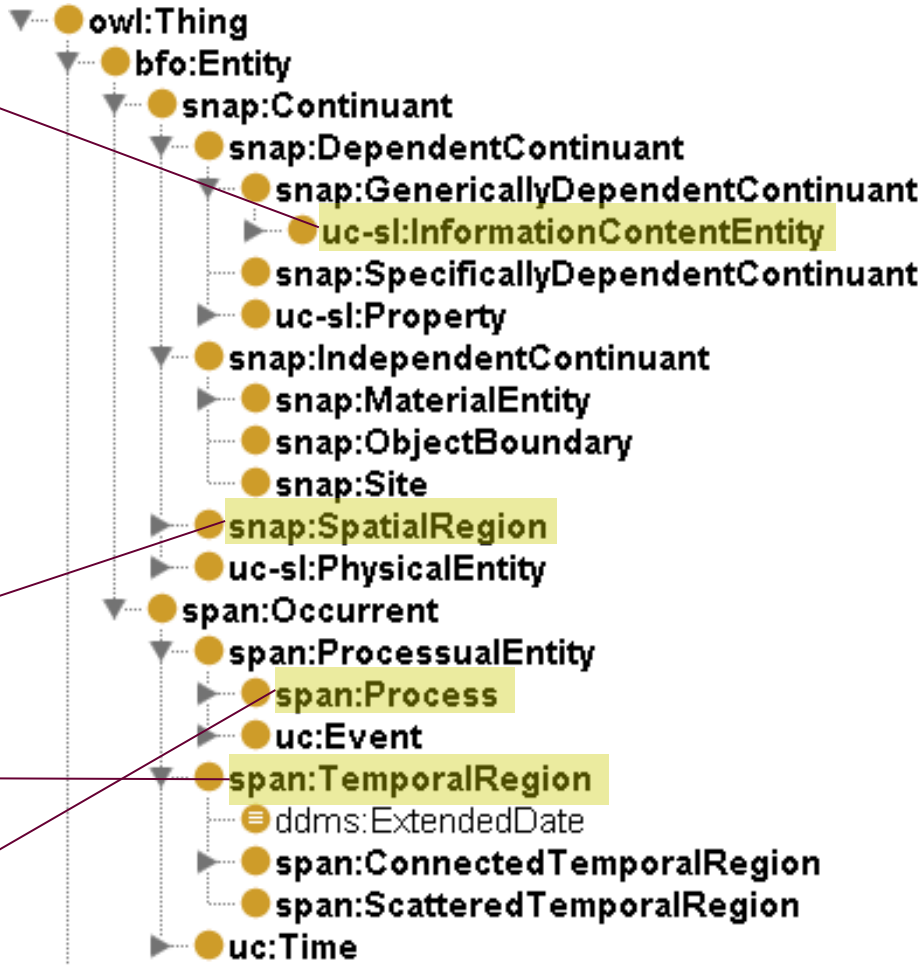
Technology Usage Relationships

Relationship	Allowed Subject Types	Allowed Object Types	Inverse
isUsedInRequirementsAnalysis	TechnicalThing	Article or ProcessType	hasRequirementsAnalyzedUsing
isUsedInDesigning	TechnicalThing	Article or ProcessType	isDesignedUsing
isUsedInManufacturing	TechnicalThing	Article	isManufacturedUsing
isUsedInIntegration	TechnicalThing	Article or ProcessType	isIntegratedUsing
isUsedInTesting	TechnicalThing	Article or ProcessType	isTestedUsing
isUsedInInspecting	TechnicalThing	Article	isInspectedUsing
isUsedInOperating	TechnicalThing	Article (except Material)	isOperatedUsing
isUsedInMaintaining	TechnicalThing	Article	isMaintainedUsing
isUsedInDisposingOf	TechnicalThing	Article	isDisposedOfUsing
isUsedInRefurbishing	TechnicalThing	Article	isRefurbishedUsing
isUsedInOverhauling	TechnicalThing	Article	isOverhauledUsing
isUsedInReverseEngineering	TechnicalThing	Article, Technology, Software	isReverseEngineeredUsing
isUsedInReplicating	TechnicalThing	Article, Software, ProcessType	isReplicatedUsing
isUsedInCopying	TechnicalThing	Software, Document	isCopiedUsing
isUsedInCloning	TechnicalThing	BiologicalAgent	isClonedUsing
isUsedInImplementing	TechnicalThing	Technology, Software, ProcessType	isImplementedUsing
isUsedInDeveloping	TechnicalThing	Technology, Article, Software, ProcessType	isDevelopedUsing
isUsedInEngineering	TechnicalThing	Article, Software, ProcessType	isEngineeredUsing

13

Organizing Metadata classes in context

- Much metadata is an Information Content Entity
  - Enumerations (country code, security marking, …)
  - Person's name
  - Copyright specifications
- GML data components are spatial regions
- Dates and timestamps are temporal regions
- An IRM Activity is a Process



Summary

- Comprehensive Cyberspace Ontology
  - The “world squared”
- Cyberspace Domain Ontology
  - Not the “world squared”, though quite substantial
- Cyberspace Security Domain Ontology
  - More focused, though still requires broad range of concepts
  - Requires integration with upper level ontologies to establish context and aid interoperability
  - Requires integration with middle level and extension ontologies to address specific applications