Federated Command and Control Infrastructure for Adaptive Computer Network Security

Thomas C. Eskridge | Florida Institute of Technology

13 July 2017

Homeland Security

Science and Technology

Team Profile

Florida Institute of Technology

Harris Institute for Assured Information

- Marco Carvalho, Ph.D. (PI)
- Thomas Eskridge, Ph.D.
- Troy Toggweiler
- Evan Stoner
- Adrian Granados
- Rebekah Lee

- DHS S&T PM: Edward Rhyne

Designated a **National Center of Academic Excellence in Information Assurance Research (CAE/R)** by the National Security Agency and the U.S. Department of Homeland Security.
For Academic Years 2014-2019

Florida Institute of Technology
Harris Institute for Assured Information

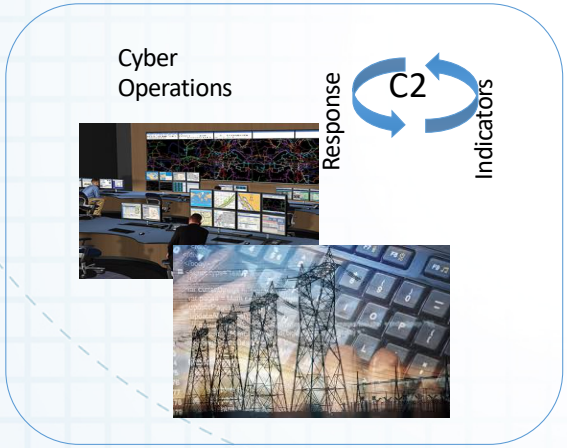
Motivations and Need

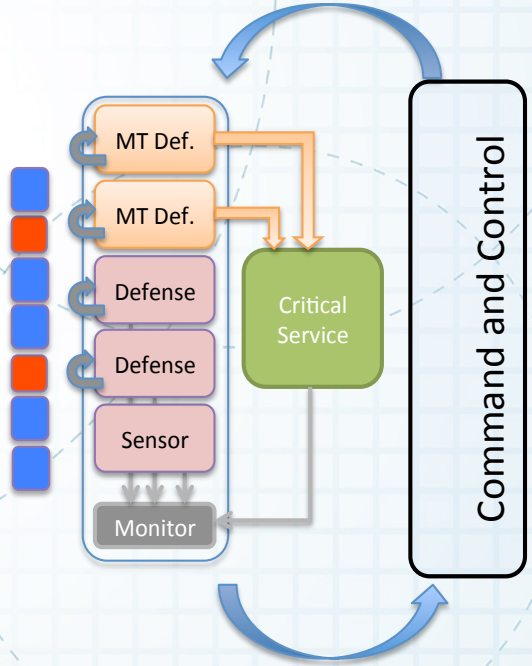
- New **investments and advances** in the design of defensive tools and capabilities for cyber operations
- Increasing adoption of defenses that are significantly more **complex, diverse, and dynamic (e.g. Moving Target Defenses)**
- Increasing acceptance and deployment of **common specifications for automated exchange of threat information**

The FC2 Project addresses the critical need for **Resilient Federated Command and Control Infrastructures** for Cyber Operations and Moving Target Defenses

Project Goal

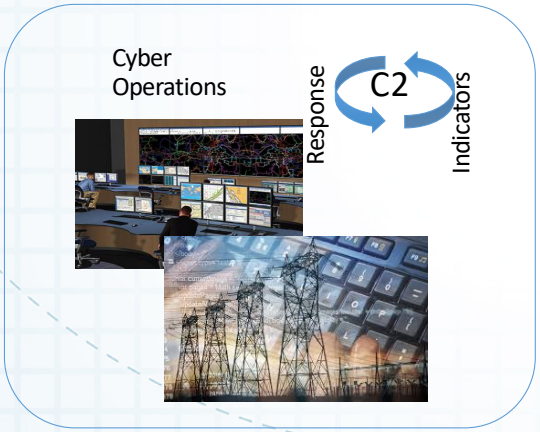
- Enabling Cyber Command and Control
  - Resilient C2 for dynamic and moving target defenses

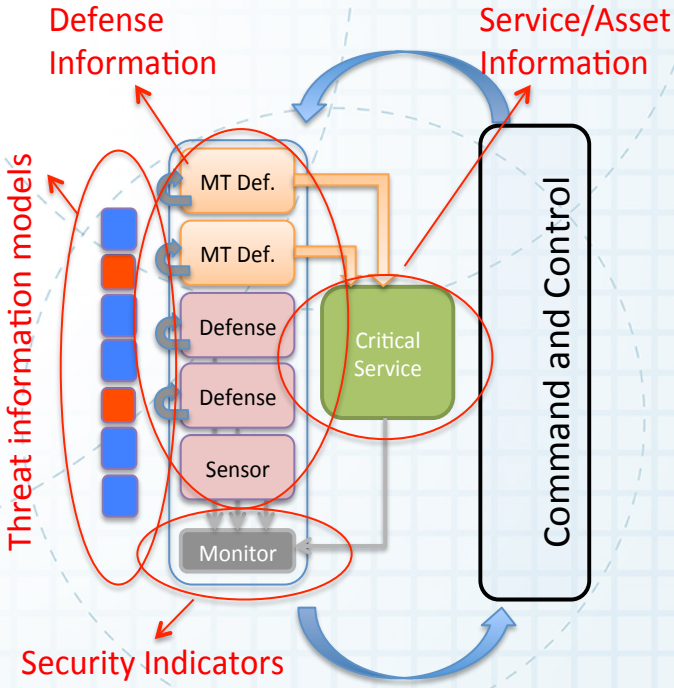




Project Goal

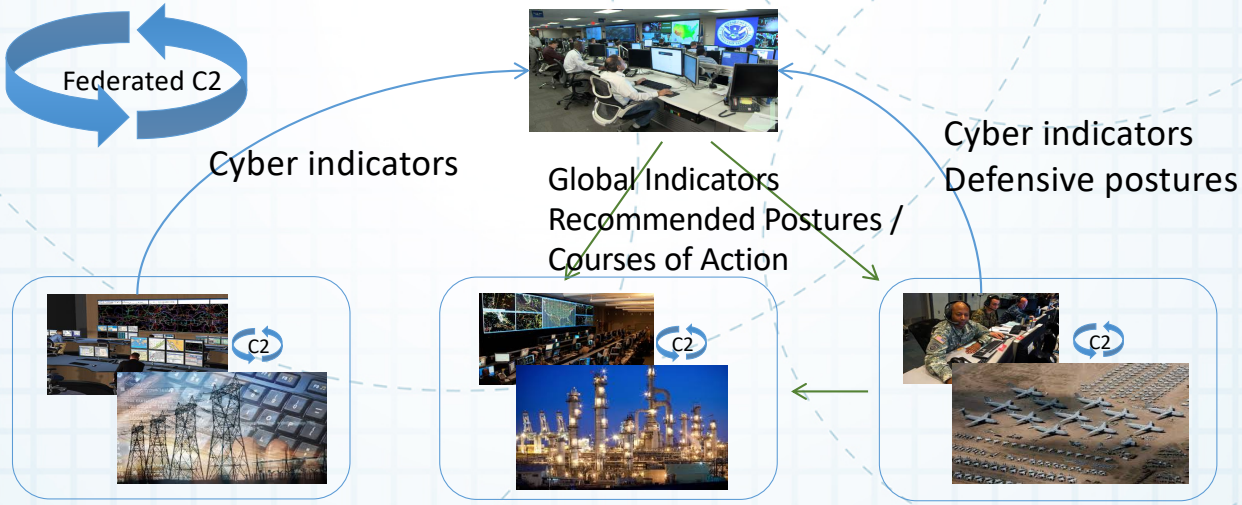
- Enabling Cyber Command and Control
  - Integration, control, and management of third party sensors, defenses, and services





Project Goal

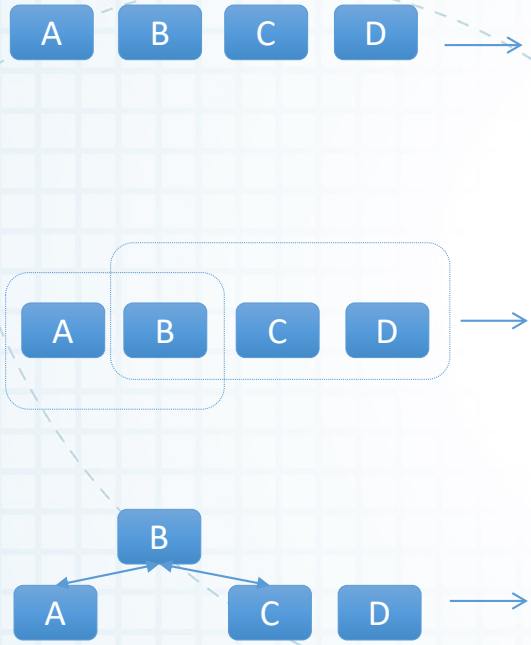
Enable the semi-automated federation of multiple cyber C2 infrastructures to form a Federated Command and Control Infrastructure



FC2 Requirements

- Flexible Structure
  - Overlapping, Hierarchical, etc.
- Scalable
  - From enterprises to commodity routers
- Resilient
  - Able to resist and recover from failures and attacks
- Trusted
  - Policy delegation, authentication
- Extensible
  - External services, enterprises, defenses, and C2 implementations
- Participation models
  - Voluntary participation, incentive models, regulatory models, etc.

Building a Federated C2

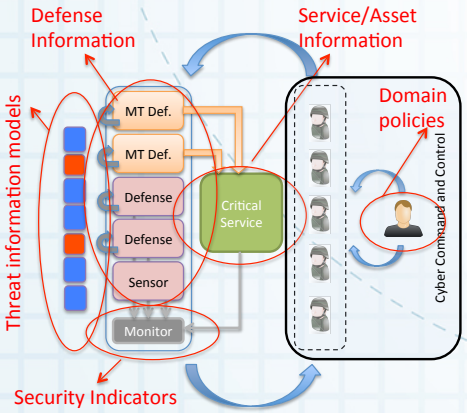


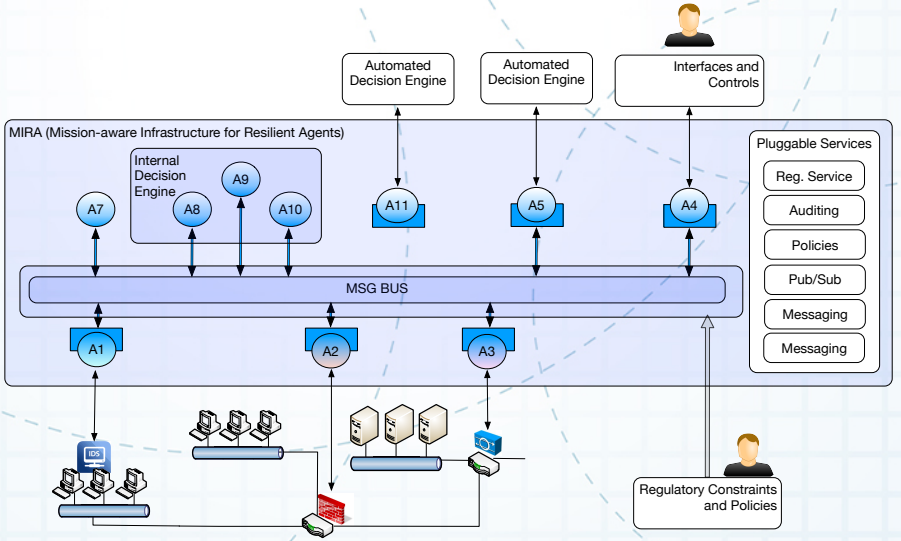
Automating Federation Formation

- **Initial Federation Formation**
  - Policies and mechanisms for federation formation
- **Organization Policies**
  - Defining contexts and information sharing policies
- **Federation Policies**
  - Defining policies for sharing responses amongst federation members, and across federations

Approach

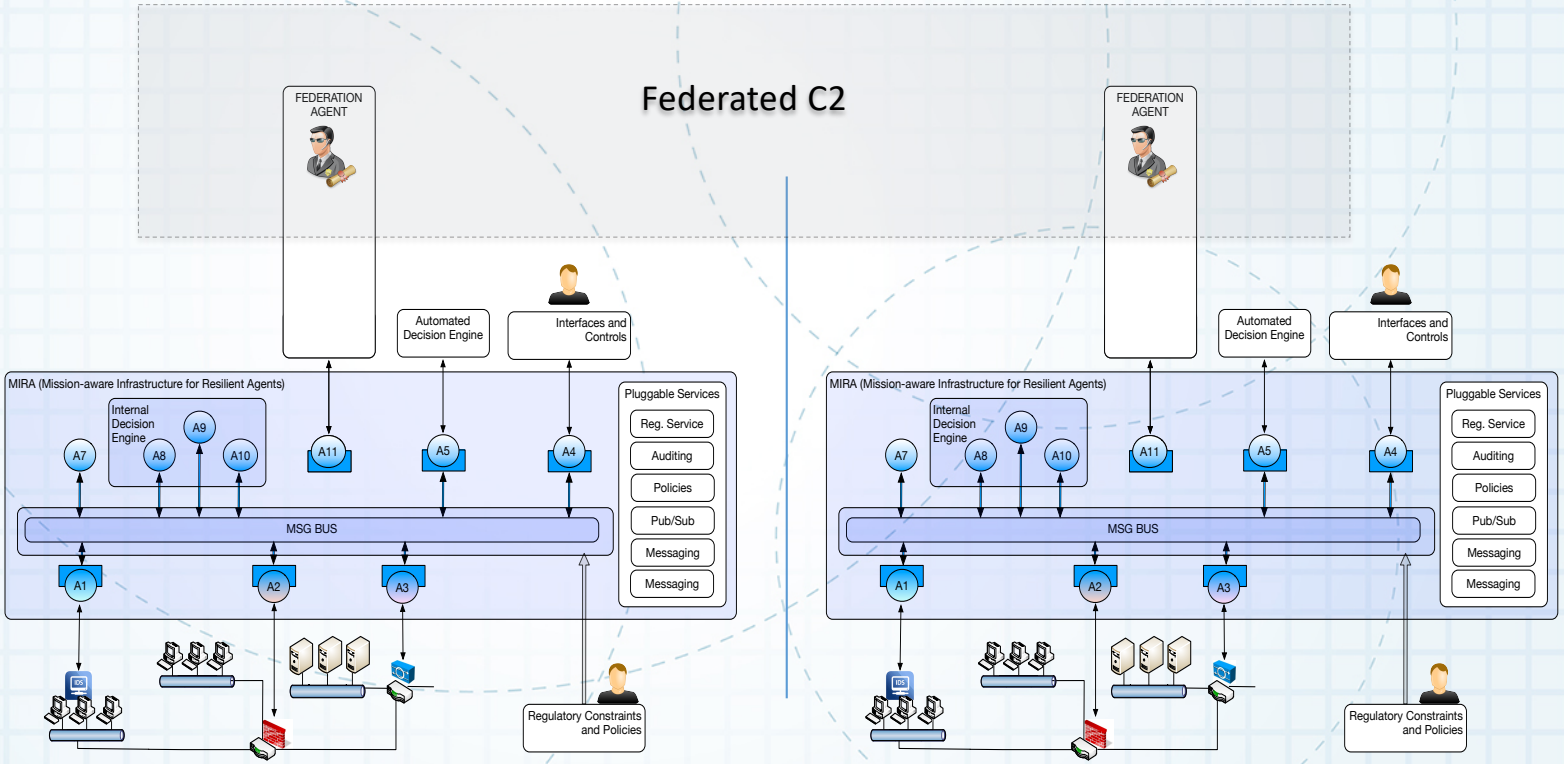
- Building on prior Cyber C2 Frameworks (sponsored by DoD) developed at Florida Tech
- MIRA: Mission-aware Infrastructure for Resilient Agents
  - Human-assisted command and control automation for cyber operations.





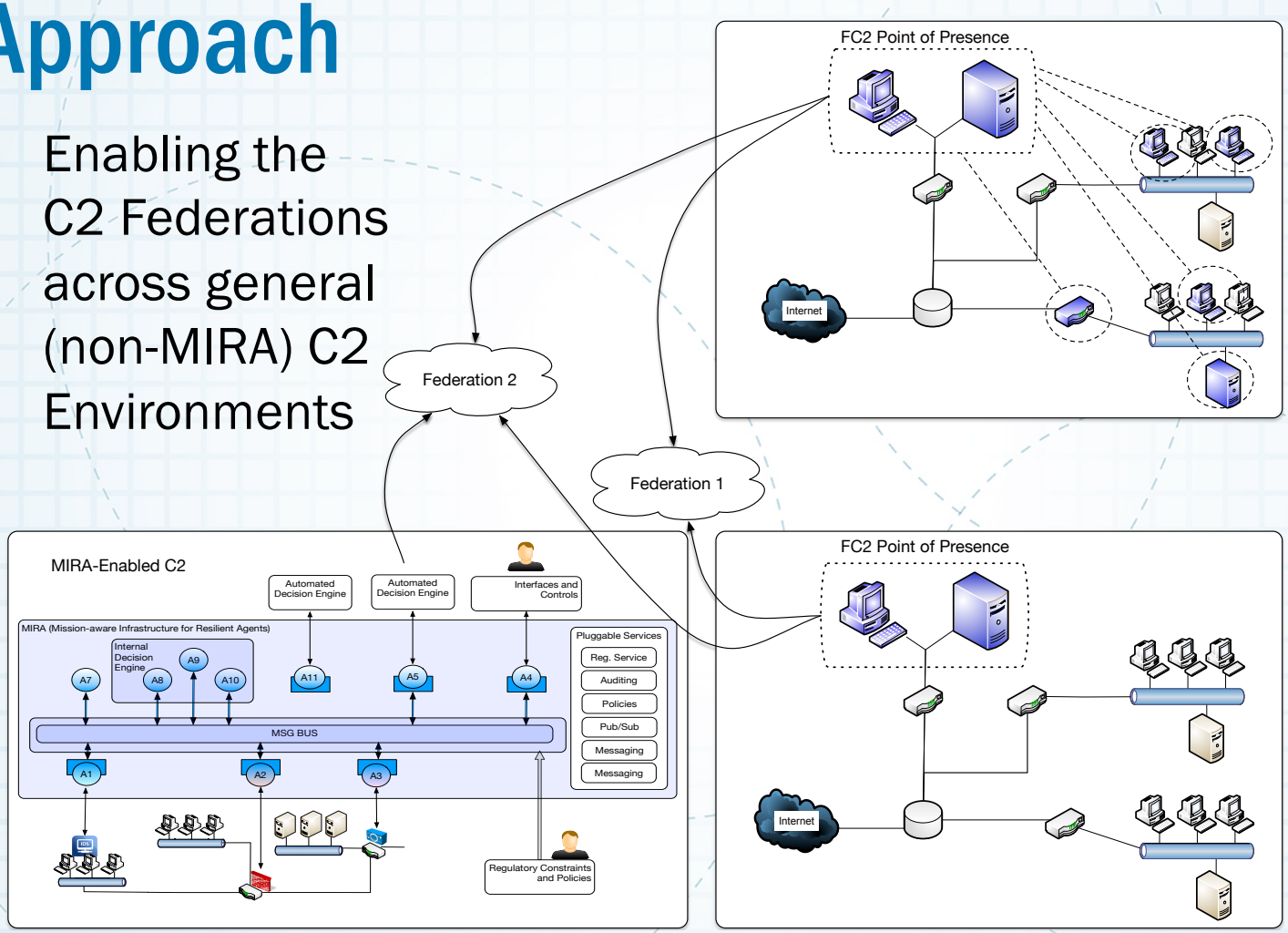
Approach

- Enabling the C2 Federations



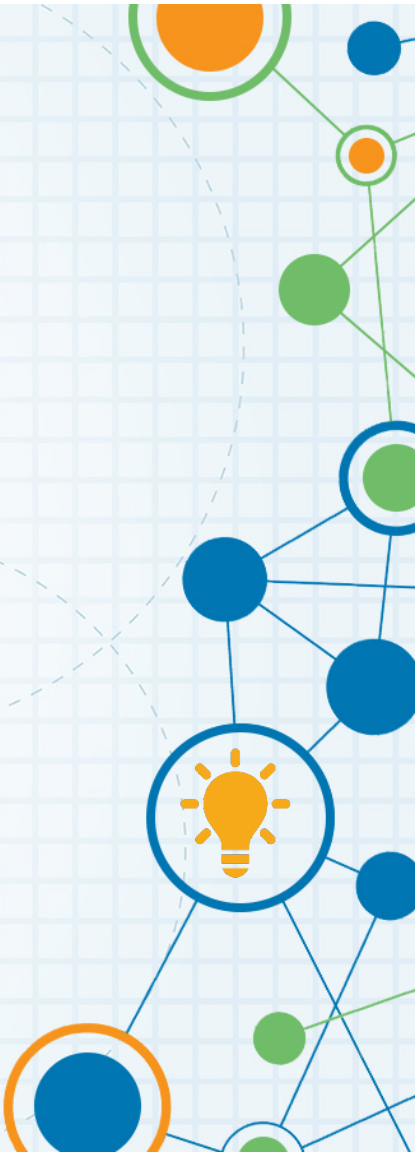
Approach

- Enabling the C2 Federations across general (non-MIRA) C2 Environments



Benefits

- Enabling Federated C2 Operations
  - **Integration of Efforts**: Brings together prior research in the field, *enabling the development of new capabilities through coordination and control*
  - **Context-dependent policies**: *Context changes may trigger new sets of policies* for federation members
  - **Automated process**: *Policy negotiation and enforcement happens automatically*, based on pre-defined preferences from individual members
  - **Maintaining and Leveraging Diversity**: FC2 thrives from the *diverse experiences of member environments*
  - **Multiple participation modes**: *Federation members may define or modify policies at any time*, adjusting their level of involvement in the federation



Competition

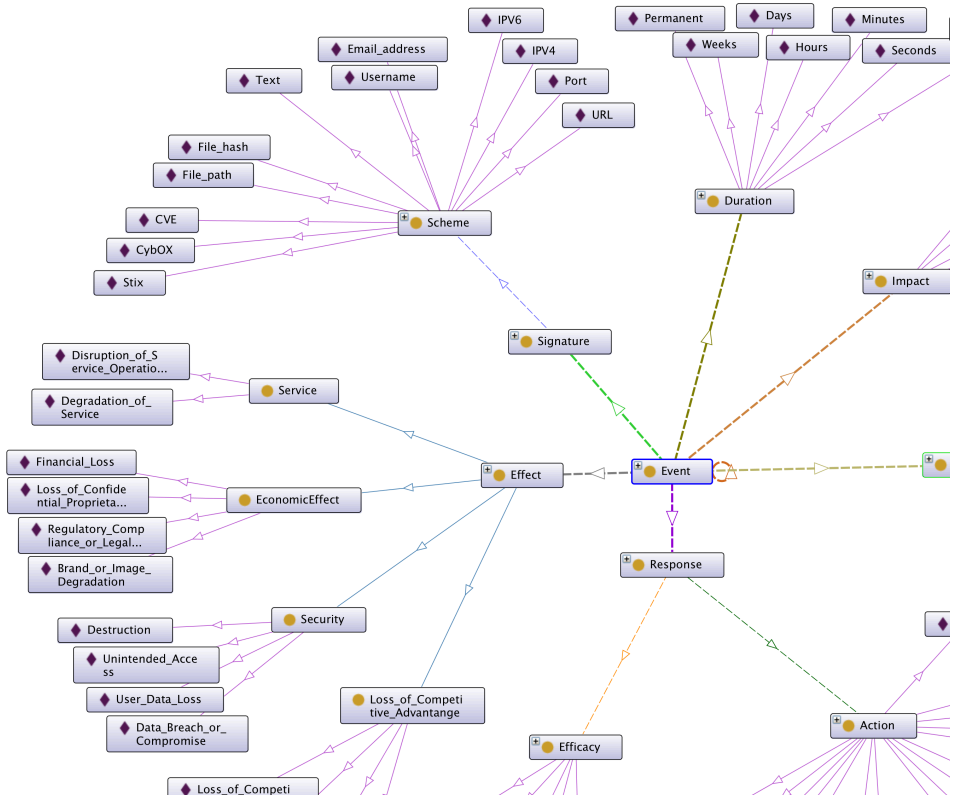
- Other sharing techniques
  - No reasoning component on sharing
  - No generalized connection between response and actuator
- Other orchestration techniques
  - Single vendor
  - Varied assimilation of other sensors and defenses
  - Varied actuation of responses

Current Status

- Created Federation ontology to share information and integrate diverse sensors and defenses
- Federation-wide integration of secure computation method
- Policies for joining, and contributing and acting on federation data
- Integrated third-party command and control
- Demonstrated five enclaves dynamically creating and joining in three different federations
- MIRA C2 integrated control of defenses from six different DHS performers

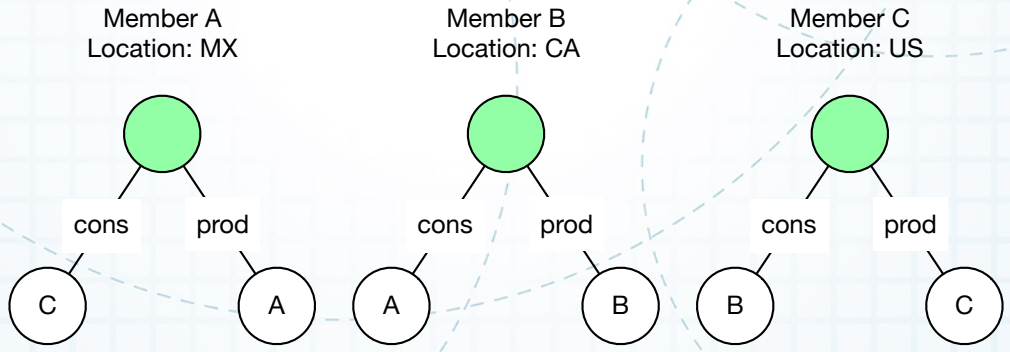
Current Status: Federation Ontology

- High-level concepts describing
  - Signatures
  - Events
  - Responses

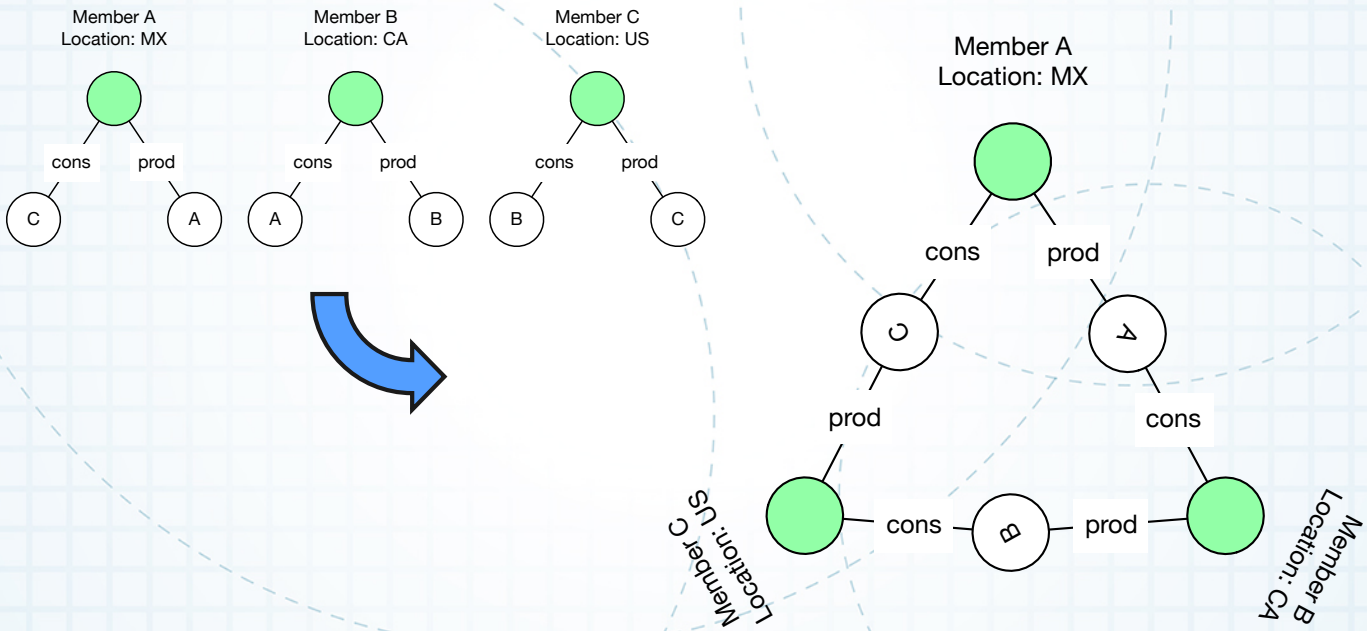


Current Status: Automatic Federations

- Federations are automatically formed and dissolved based on enclave preferences
- Enclaves can conditionalize federation membership based on what other members share

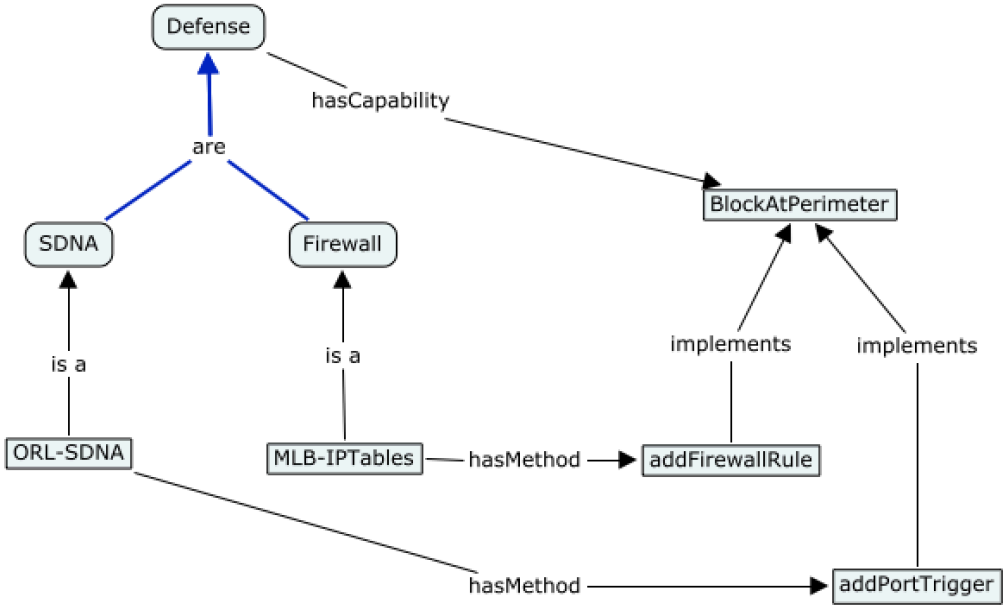


Current Status: Automatic Federations



Current Status: Generalized Control

- Generalized events and controls are shared between enclaves
- Each enclave implements response according to their capabilities



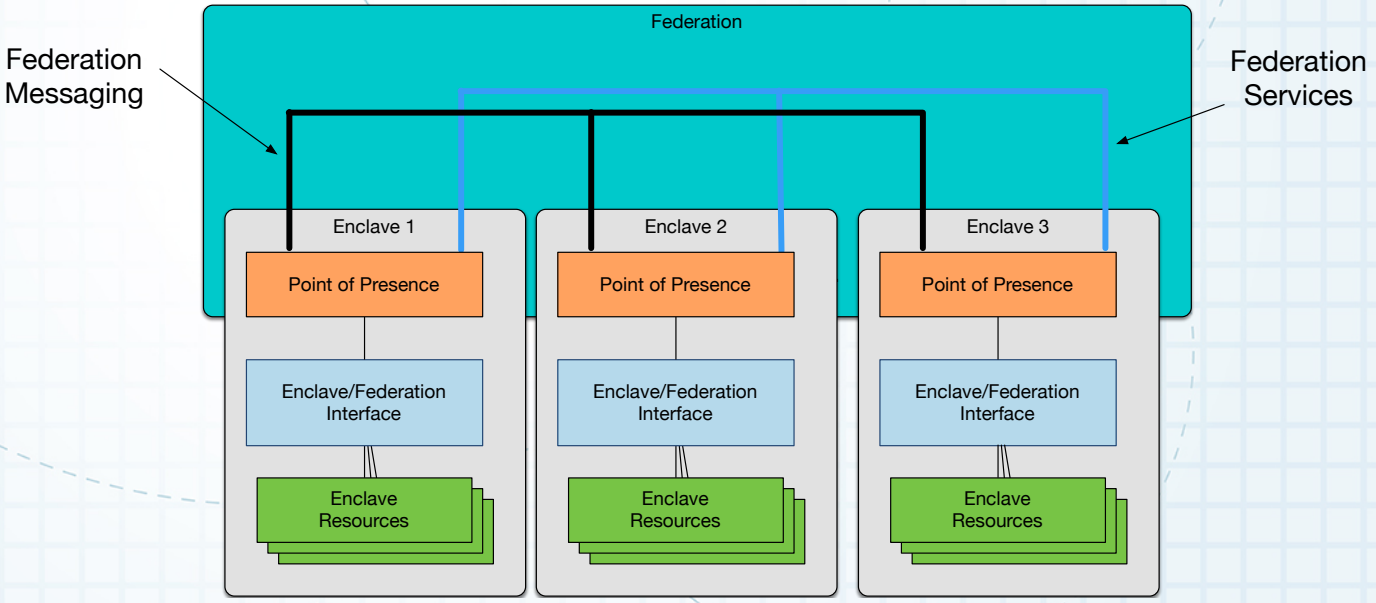
Current Status: Integration with Third-Party Capabilities

- Semantic representation of events and response allows integration of diverse set of capabilities

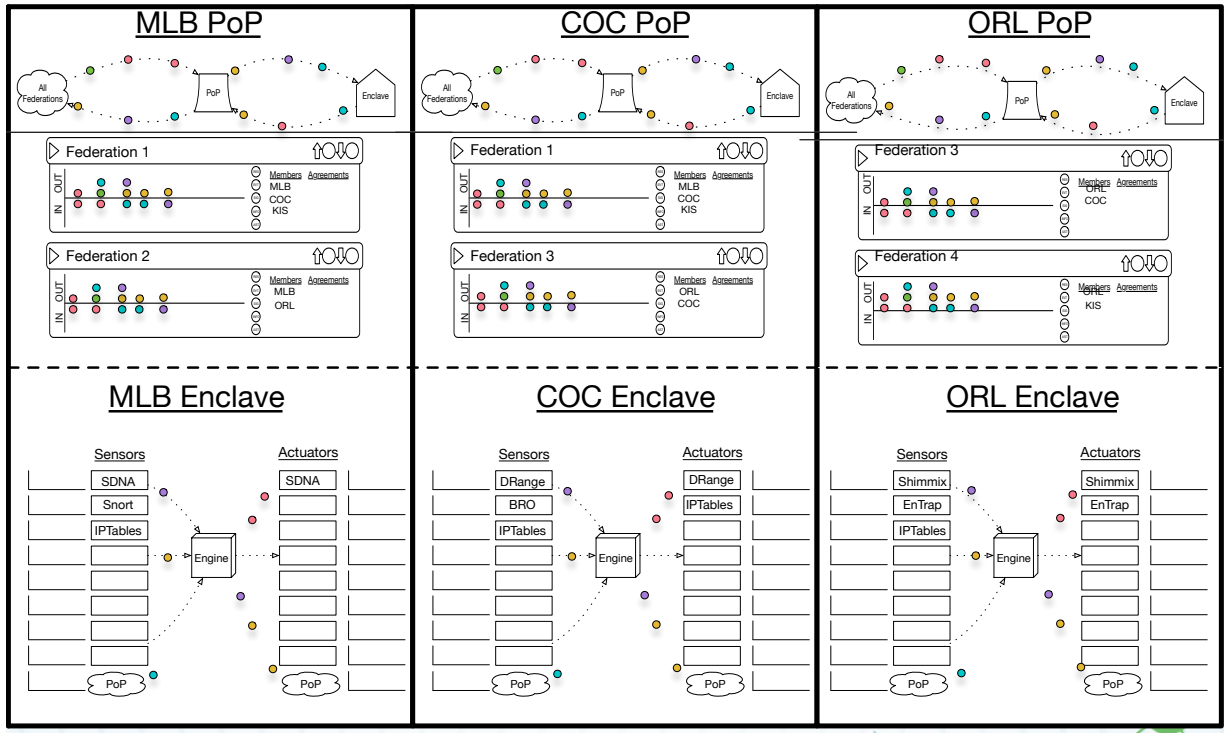
Defense	Services	Command and Control
SDNA – I-A-I Shimmix – Def-Logix Entrap – Def-Logix DRANGE – Sandia National Labs Application Diversity – Florida Tech	Multi-party Computation – MIT/LL	MIRA – Florida Tech Thimblerig - SEI

Current Status: Integration with Third-Party Capabilities

- Federation-level services provide additional capabilities to members

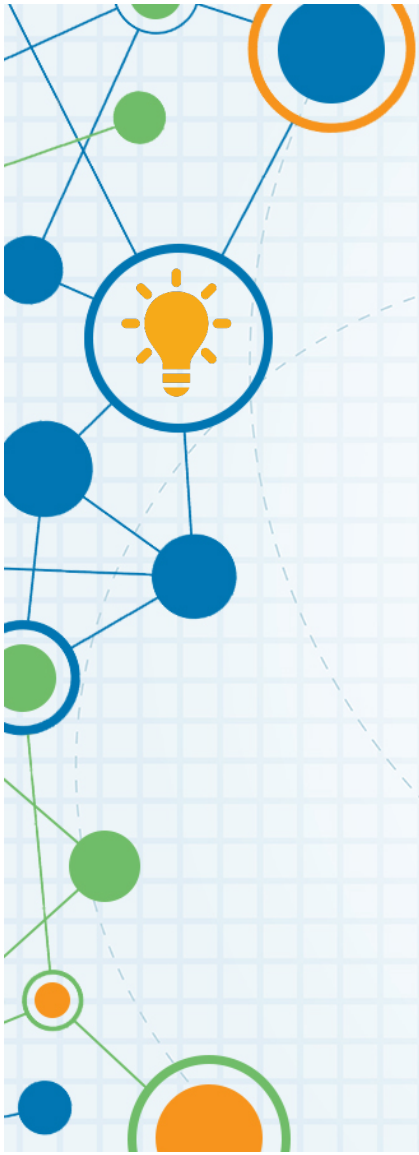


Current Status



Transition/Completion Activities

- Open source efforts
  - In the process of open-sourcing MIRA, the support infrastructure for FC2
- Community development efforts
  - Developing a project website for the distribution of
    - Points of presence and documentation
    - Support infrastructure and communities of interest
- Commercial application efforts
  - Investigating requirements for commercial offering
  - Vertical markets are first target



Lessons Learned

- Communication is key
  - Large group of performers regularly met as a group and often individually to discuss integration and control issues
- A general and extensible representation is useful for integrating a wide range of sensors and defenses
- Even very general contracts between federation members can be very useful

Contact Info

Dr. Thomas C. Eskridge

Florida Institute of Technology
Harris Institute for Assured Information

Associate Professor, School of Computing
Harris Institute for Assured Information
College of Engineering and Computing
Florida Institute of Technology
Melbourne, FL
Office: (321) 674-7455

2017 Cyber Security R&D Showcase and Technical Workshop

July 11 - 13, 2017 | Washington, D.C.

Homeland Security

Science and Technology