



Homeland
Security
Science and Technology

2016 | Cyber Security Division
R&D SHOWCASE AND TECHNICAL WORKSHOP

(FC2) A Federated Command and Control Infrastructure

Harris Institute for Assured Information

Florida Institute of Technology

Dr. Marco Carvalho

February 17, 2016

The FC2 Team



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

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

DHS S&T PM: Edward Rhyne



Florida Institute of Technology

Harris Institute for Assured Information

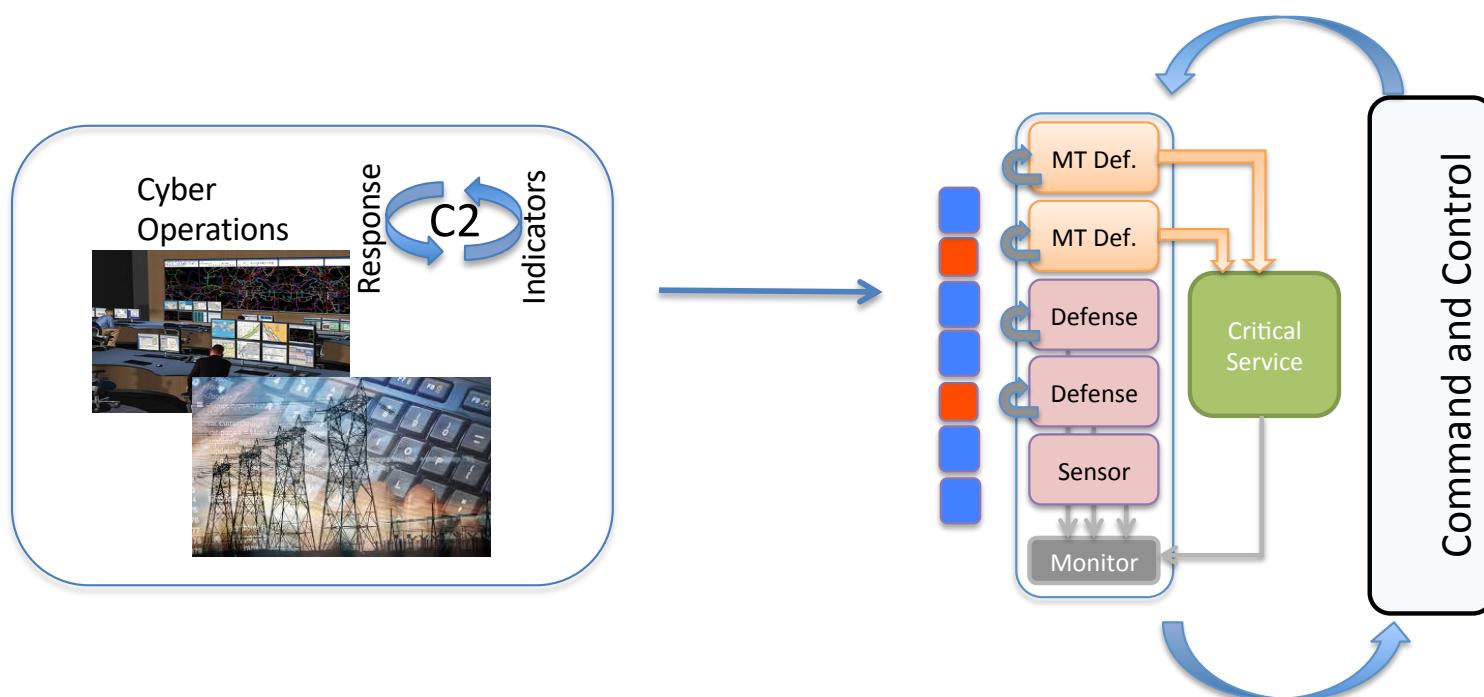
Motivation

- 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

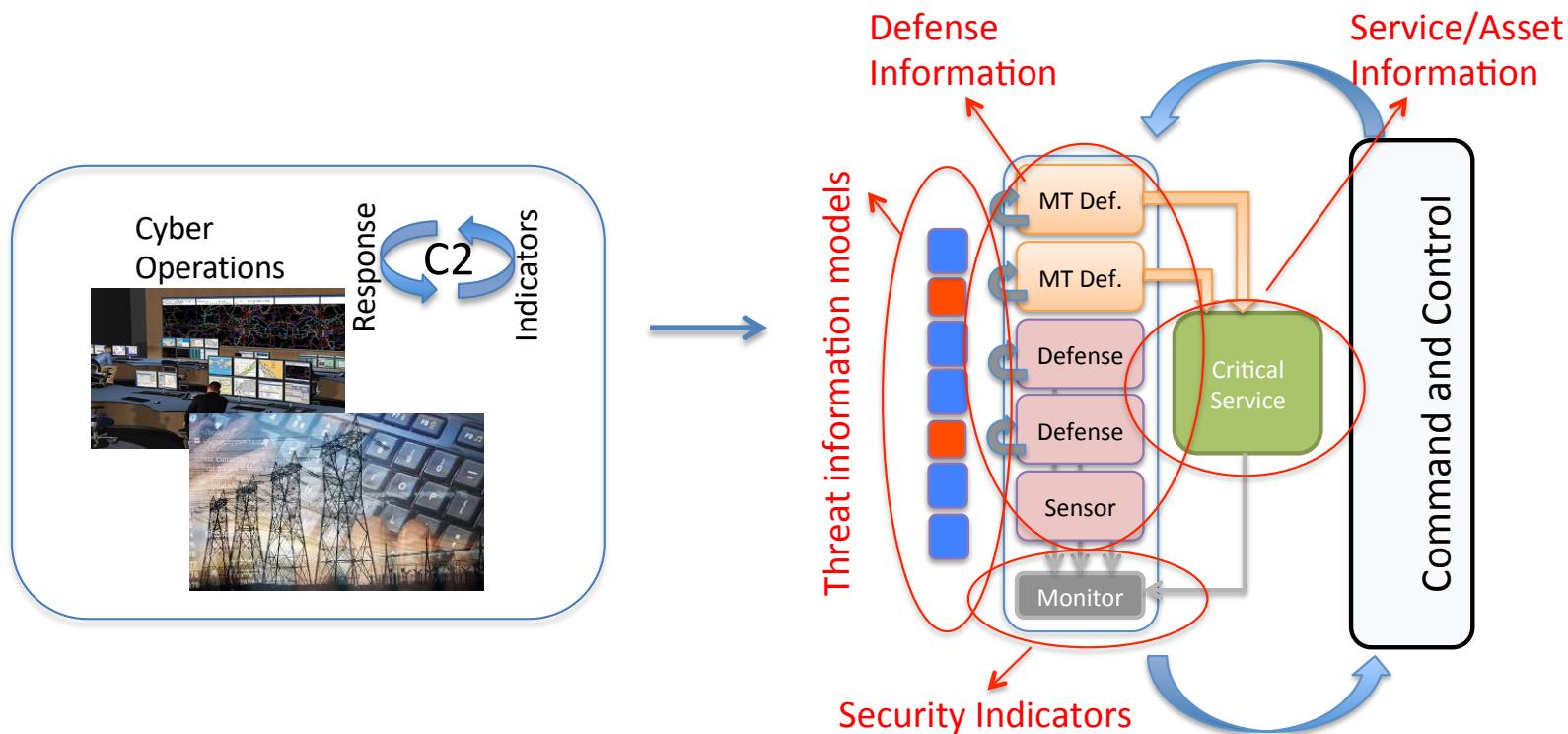
Project Goal

- Enabling Cyber C2
 - A resilient Cyber C2 Capability for dynamic and moving target defenses



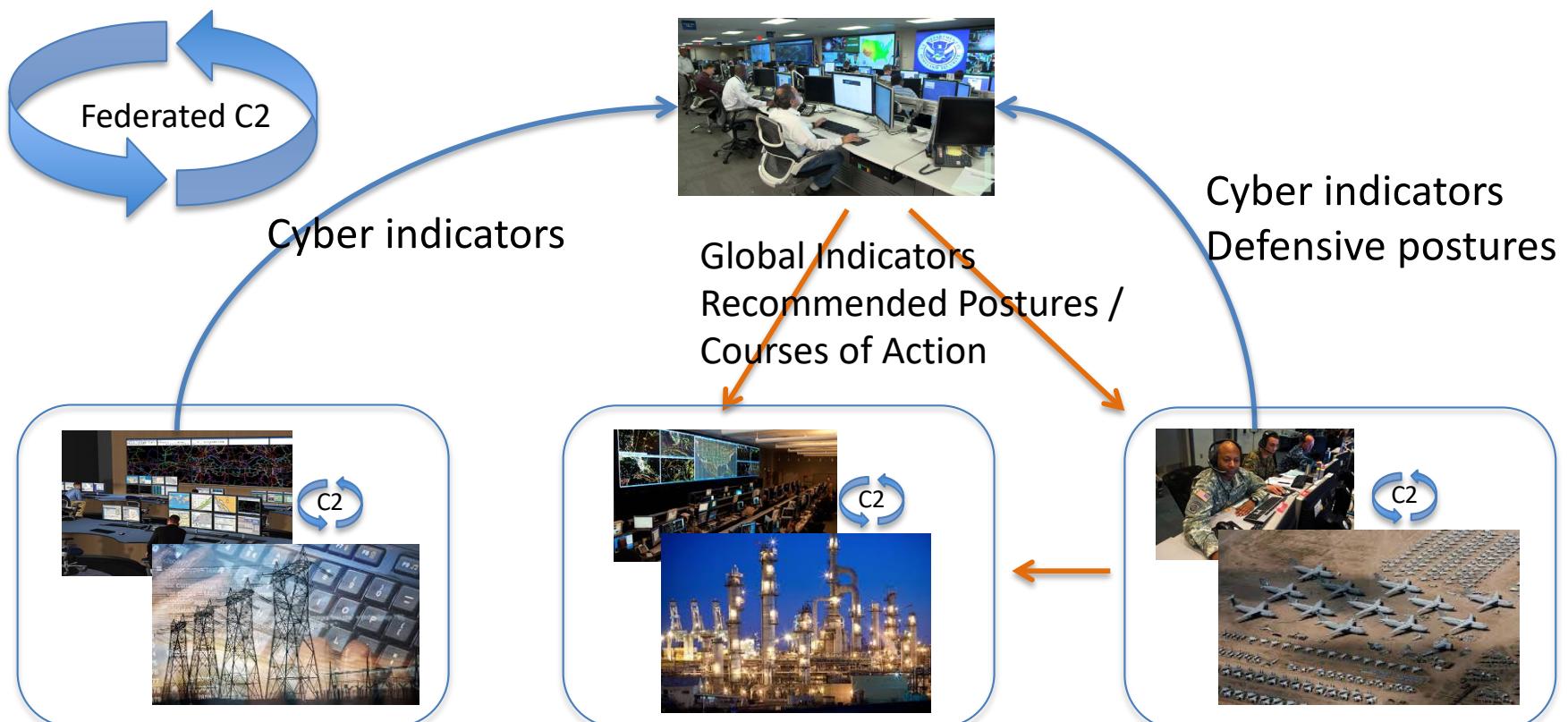
Project Goal

- Enabling Cyber C2
 - Integration, control, and management of third party sensors, defense, and services



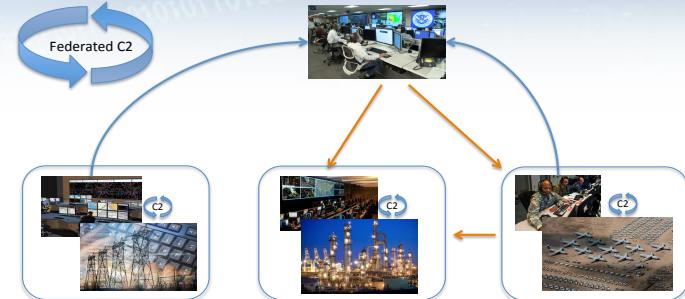
Project Goal

- 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.



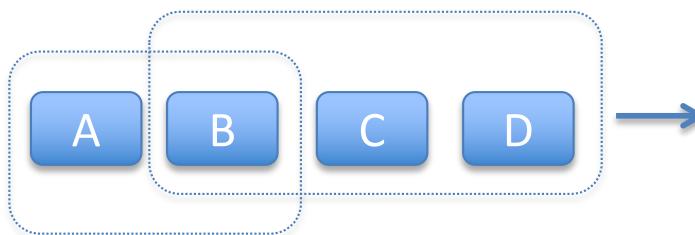
Building a Federated C2



Automating Federation Formation

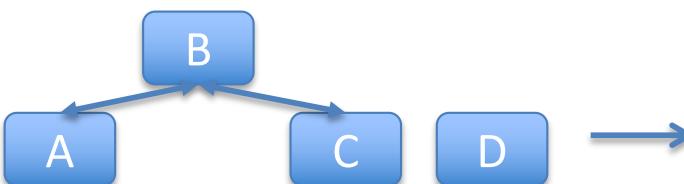
- **Initial Federation Formation**

- Policies and mechanisms for federation formation



- **Organization Policies**

- Defining contexts and information sharing policies

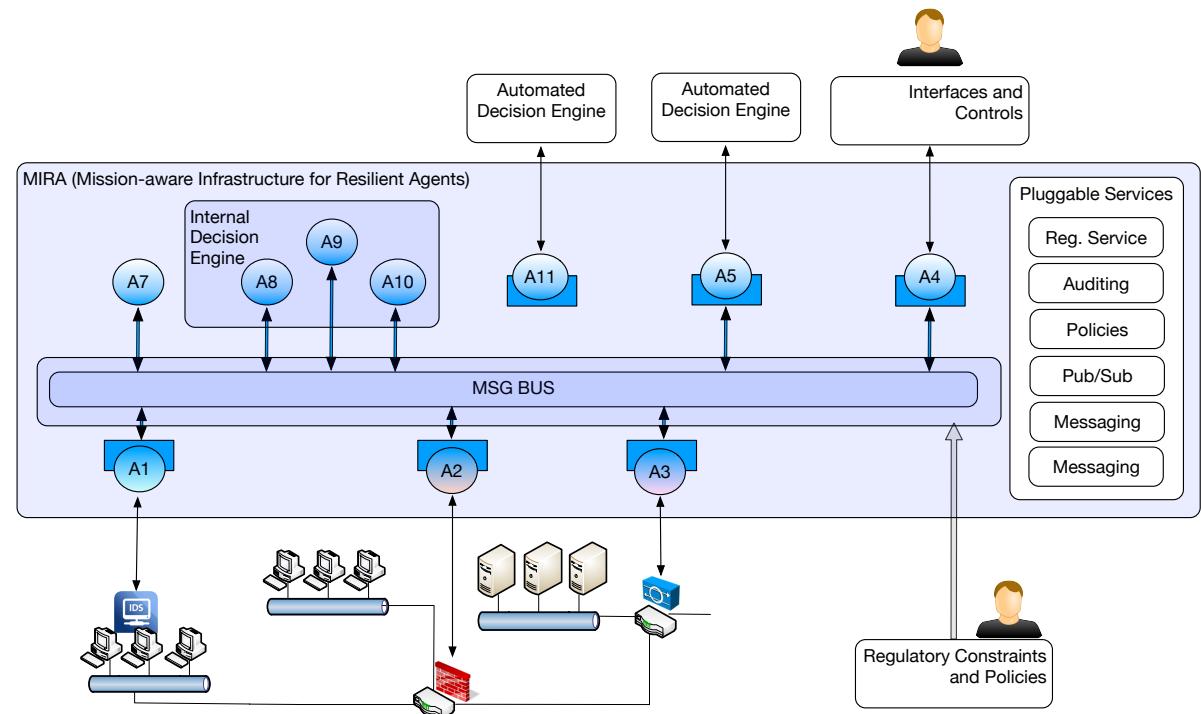
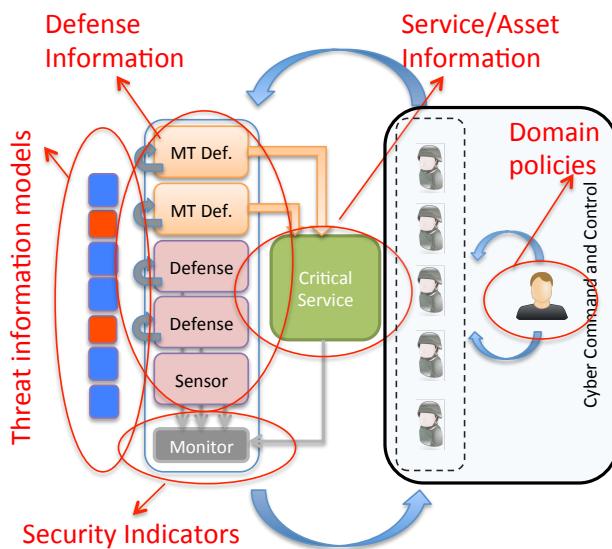


- **Federation Policies**

- Defining policies for sharing recommendations (and optionally control) amongst federation members, and across federations

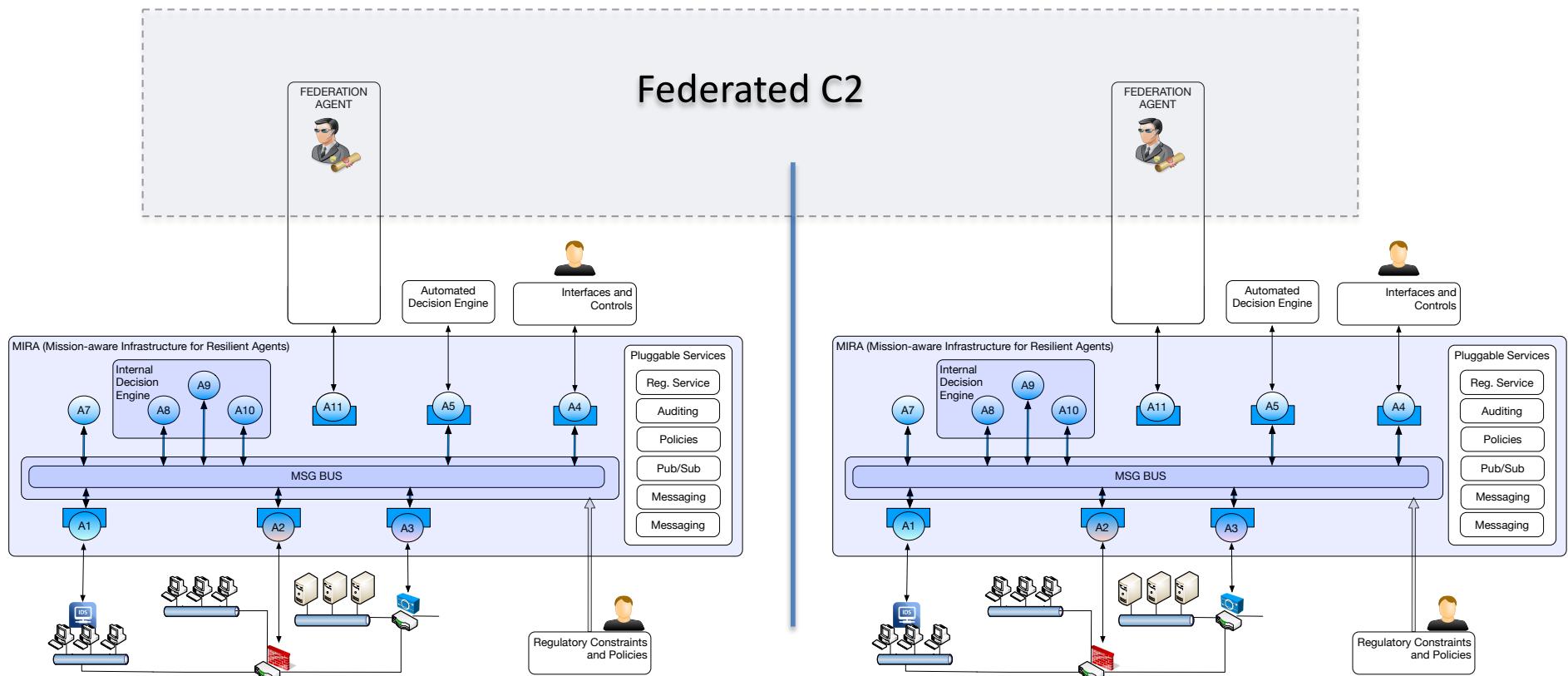
Approach

- Building on prior research efforts at Florida Tech, on Cyber C2 Frameworks (Sponsored by the DoD)
- MIRA: Mission-aware Infrastructure for Resilient Agents
 - Human-assisted command and control automation for cyber operations



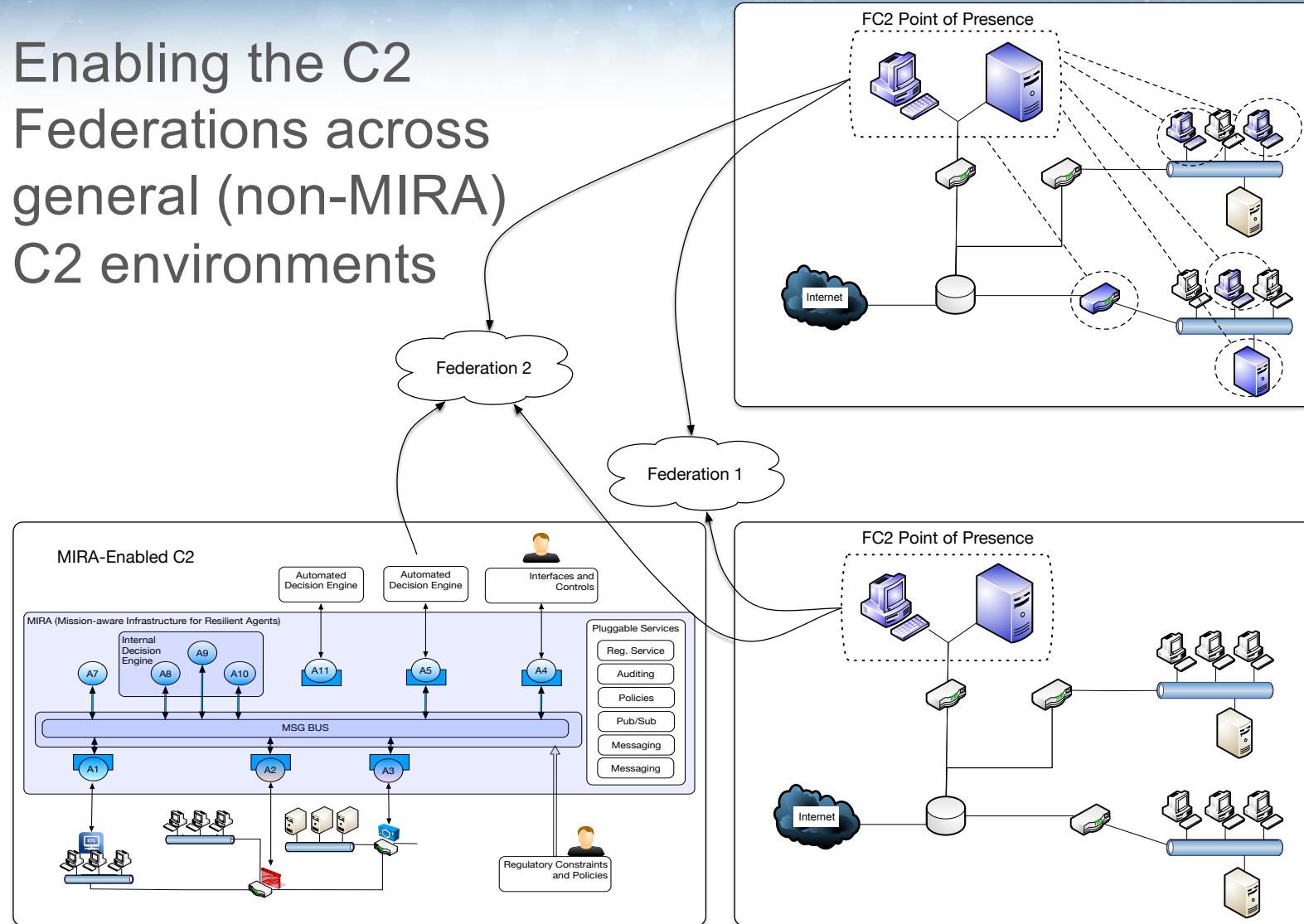
Approach

- Enabling the C2 Federations



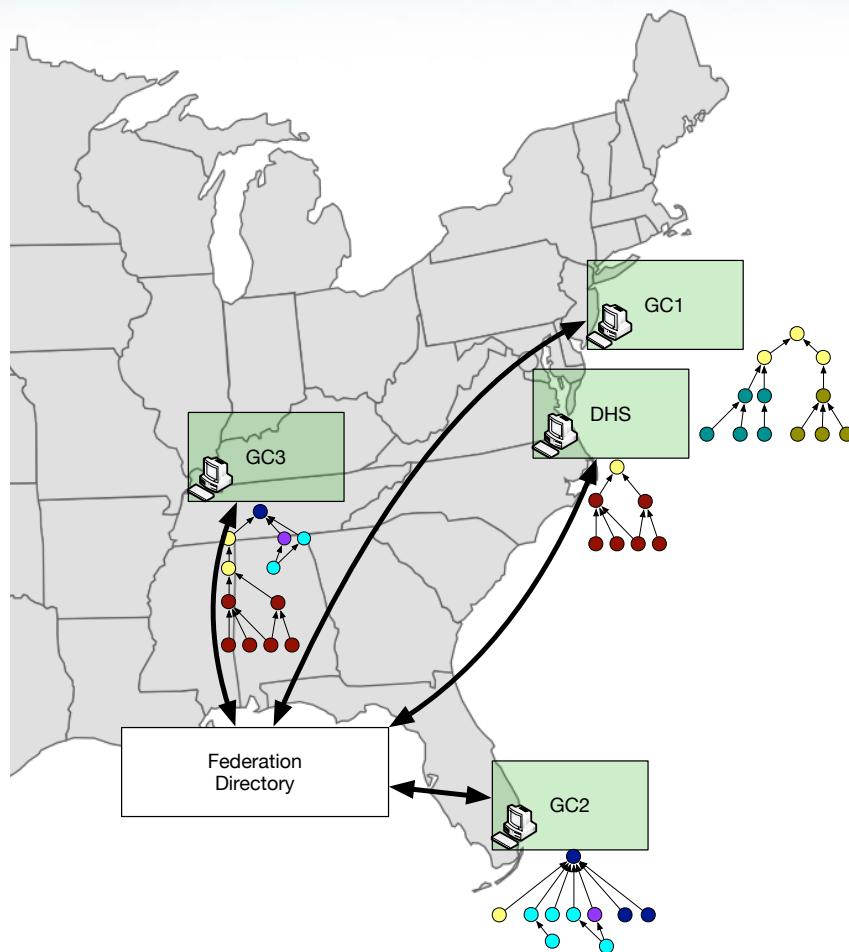
Approach

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



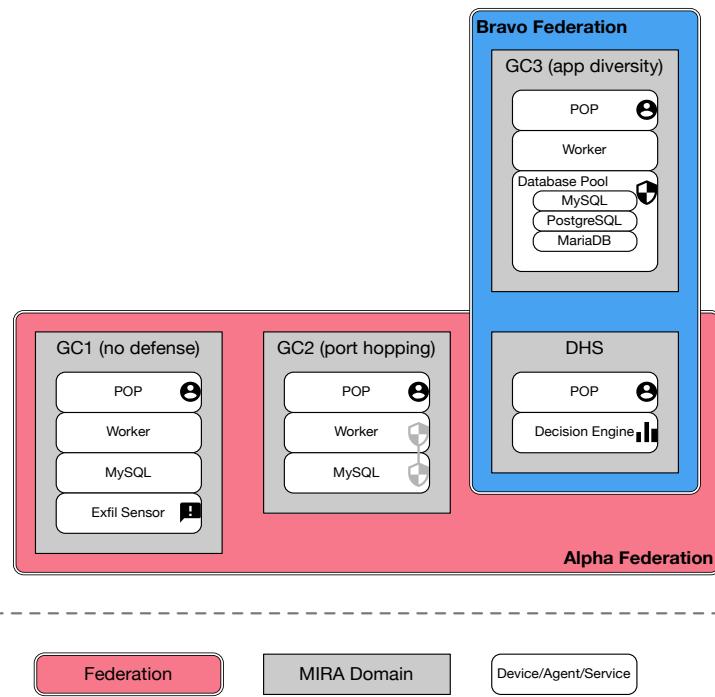
Current Status

Example Scenario: Federation Formation



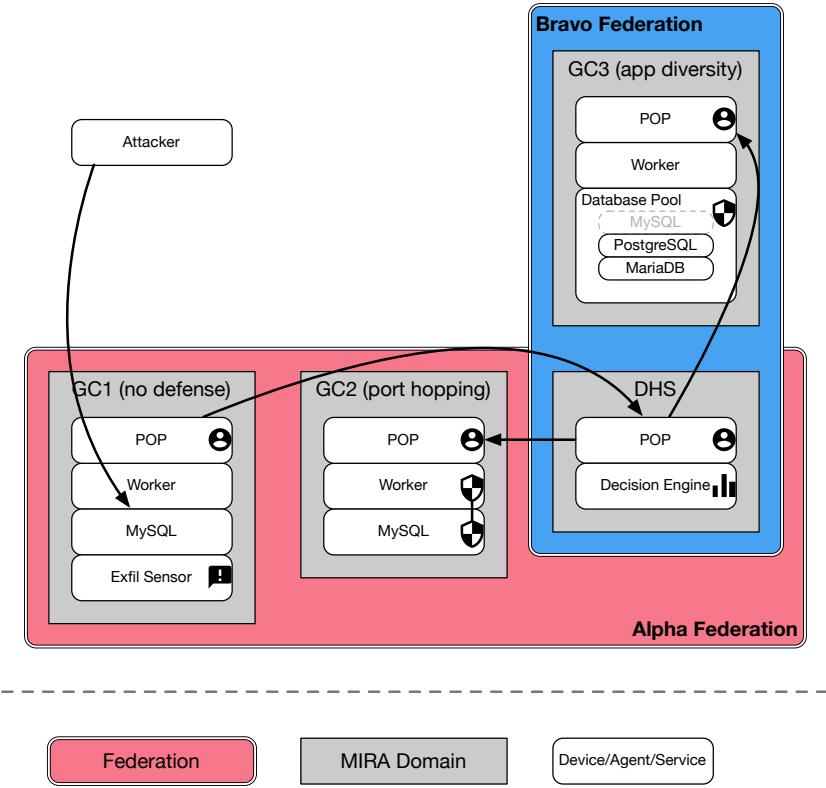
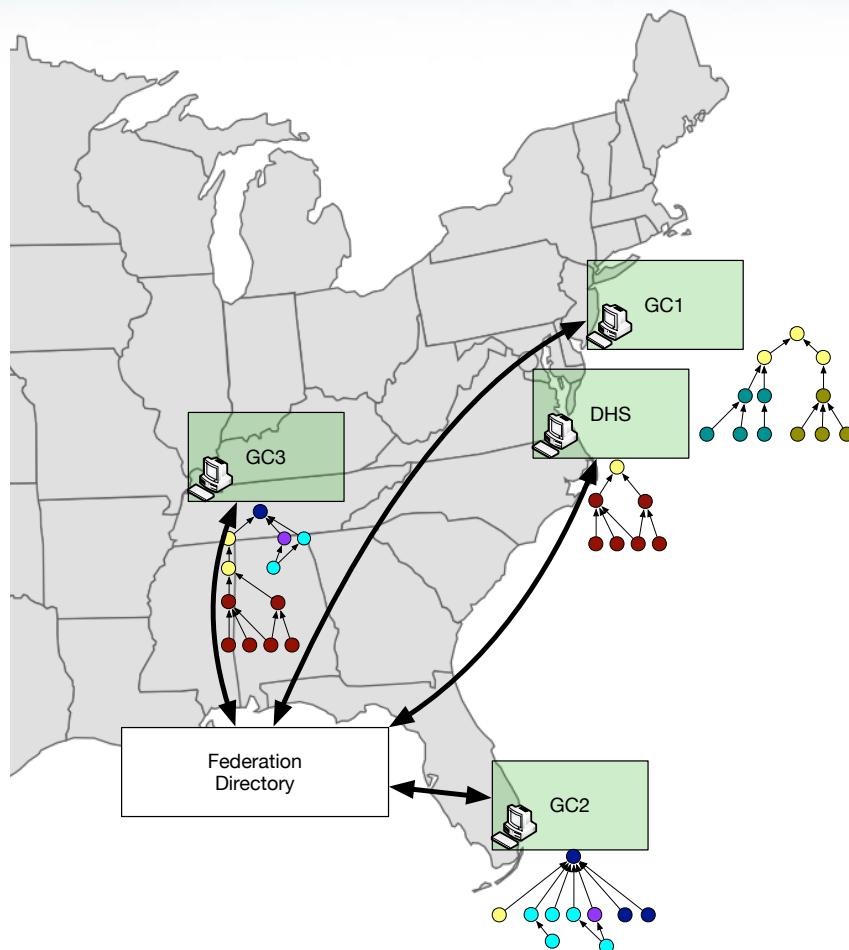
CommsCompany
 sector: Communications
 type: wireline
 provides: internet-communications
 network: communications-network-1132
 customer: business
 location: region-A

ITCompany
 sector: Information Technology
 type: security services
 requires: internet-communications
 provides: spam-email-filtering
 customer: business, individual
 location: region-A



Current Status

Example Scenario: Sharing Indicators



Summary and 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:** Different policies for different contexts 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

Next Steps on FC2

- In coordination with DoD, we are in the process of open-sourcing the MIRA framework
- Internal transition efforts within the University
 - Initial deployment (underway) within the different organizational domains
- Collaborating with DoD and others on related deployment efforts
 - Working with collaborators (Industry, Government, and Academia) on the integration of defenses through federated sites

Learn more about FC2 and Participate!

Come visit us at the Exposition Hall!

We have a **Poster** and **Demonstration** illustrating the processes of Federation Formation, Maintenance, and Control, across multiple enterprises.

Participate!

We welcome new collaborators interested in participating in pilot cyber federations. With the support of DHS S&T, we continue to integrate new sites, tools, and capabilities on pilot federations for test and evaluation. Let us know if you'd like to be part of team!

Contact Information



Florida Institute of Technology

Harris Institute for Assured Information

Dr. Marco Carvalho

Executive Director, Harris Institute for Assured Information
Harris Chair for Assured Information
Head of the Department of Cybersecurity and Data Sciences
Florida Institute of Technology
Melbourne, FL

mcarvalho@fit.edu
(321) 674 8767



Homeland
Security

Science and Technology

2016 | Cyber Security Division

R&D SHOWCASE AND TECHNICAL WORKSHOP