Problem: Critical cyber infrastructures (CCI) consist of a variety of heterogeneous and dynamic components including processors, devices, networks, mechanisms, protocols, services and their surrounding physical spaces. These systems often exist on isolated networks, in an attempt to make unauthorized access difficult and limit attacks.

These systems are:
- Statically configured
- Incompatible
- Incapable of inter-operating,

Which makes:
- Operations and trust difficult
- Configuration, management and monitoring harder
- Applying uniform security policies difficult.

Goal: Make CCIs highly available, secured against unauthorized access, highly adaptable to changes in context and policies even in the face of cyber attacks.

Technical Approach: We propose a middleware platform for providing confidential communications, privacy preserving access control, DoS resistance, anonymity, and dynamic loadbalancing for critical cyber infrastructures like smart buildings, and other large scale distributed computing environments.

Why Middleware?

Middleware offers an ideal infrastructure with which to:
- Integrate different security mechanisms
- Provide a set of primitives
- Provide common support for securing highly distributed heterogeneous systems.

Architectural Overview: The middleware partitions the network into two trust domains: an application domain network for clients and a protected services domain that consists of a network of Middleboxes and services.

The application domain provides users with:
- An abstraction of what services are available
- A set of interfaces to interact with the services
- Discovery and lookup services.

The services domain provides users and services with a set of security mechanisms through a network of Middleboxes.

A Middlebox is a node that contains some instantiation of security, privacy and/or load balancing mechanisms. The Middlebox network is a cluster of reconfigurable computing and communications nodes.

Middleboxes:
- Act as proxies or access points for critical services
- Mediate access to services by authenticating requesters and negotiating security requirements.