Autonomic GIG Management & Security Agent Technology

10th Annual

NDIA System Engineering Conference

October 22-25, 2007

Don P. Cox, Missile Systems

Youssif Al-Nashif, University of AZ

Salim Hariri, PhD, University of AZ

(520) 794-8186) dcox@raytheon.com

Abstract # 5386

NON-ITAR

Agenda

- The GIG
- Autonomia
- Attack Detection & Defense
- Conclusions

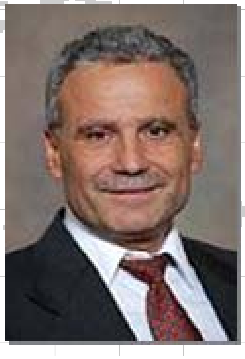
Thank you !

© Associated Press

H P D C

High Performance Distributed Computing Laboratory

Don Cox, MS.



Salim Hariri, Ph.D.

Youssif Al-Nashif, MS

NEW!

National Science Foundation

WHERE DISCOVERIES BEGIN

Center for Autonomic Computing

www.ece.arizona.edu

Introduction

- **Circa 2000 - F-18**
  - **Preflight status awareness**
  - **Tactical view integrated manually**
  - **Update via voice**
  - **Limited data security**
  - **Radar flight following**

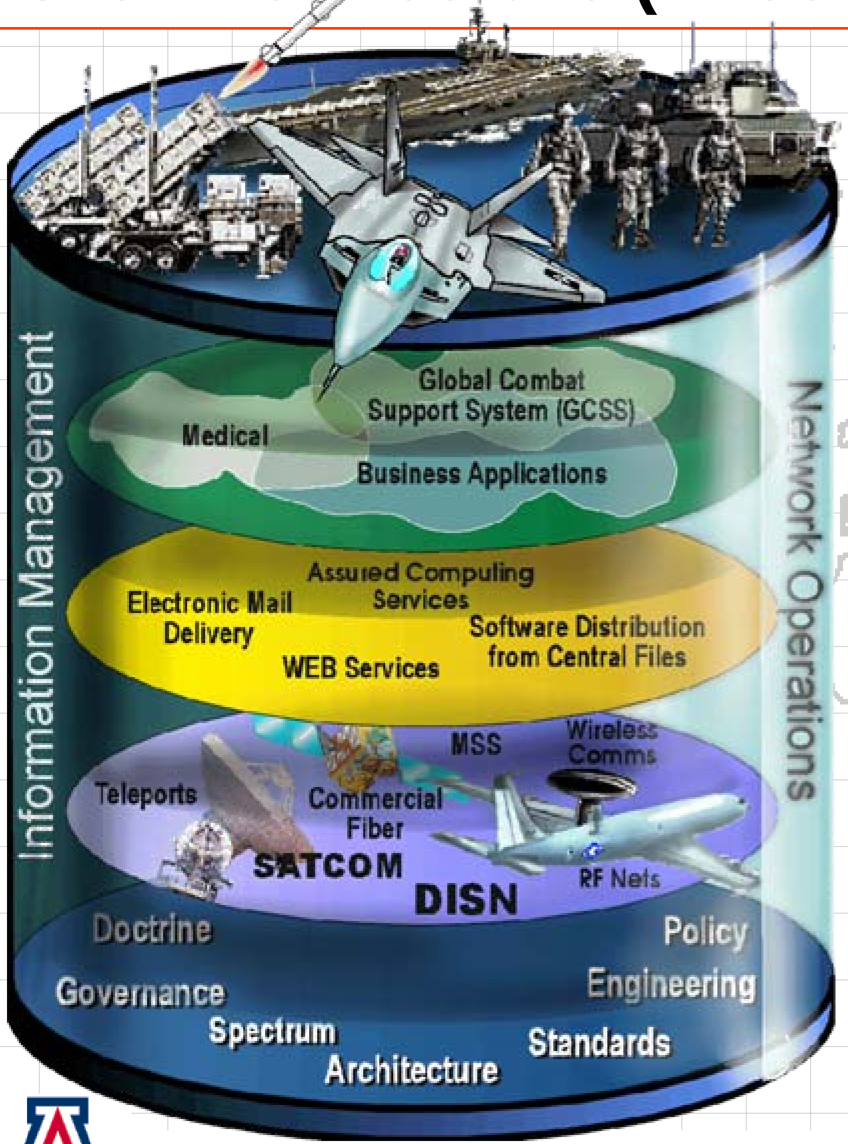
- **Circa 2015 – F-22**
  - **Integrated *Global Information Grid***
  - **Real-time data from forward C^{4}I center**
  - **Dynamic (In-flight) situation updates**
  - **Secure data-link (Intrusion aware)**
  - **C^2 AC mission capability awareness**

Difference? Data & Technology Management

GIG History

- The Clinger-Cohen Act, 1996
  - Information Technology Management Reform Act
- DoDCIO Memorandum “Global Information Grid,” (9/99)
  - Version 1.0 Approved by DoD CIO -- 8/01
  - Version 2.0 Approval by DoD CIO -- 8/03
- DoD Directive Number 8100.1 (11/03)
  - Global Information Grid (GIG) Overarching Policy

GIG Architecture ("Beer Barrel")



Warfighters (Joint Services)

Common set of information capabilities

- GIG Enterprise Services (GES)
- Core Enterprise Services (CES)
- Communities-of-Interest (COI)
- Service Oriented Architecture (SOA)

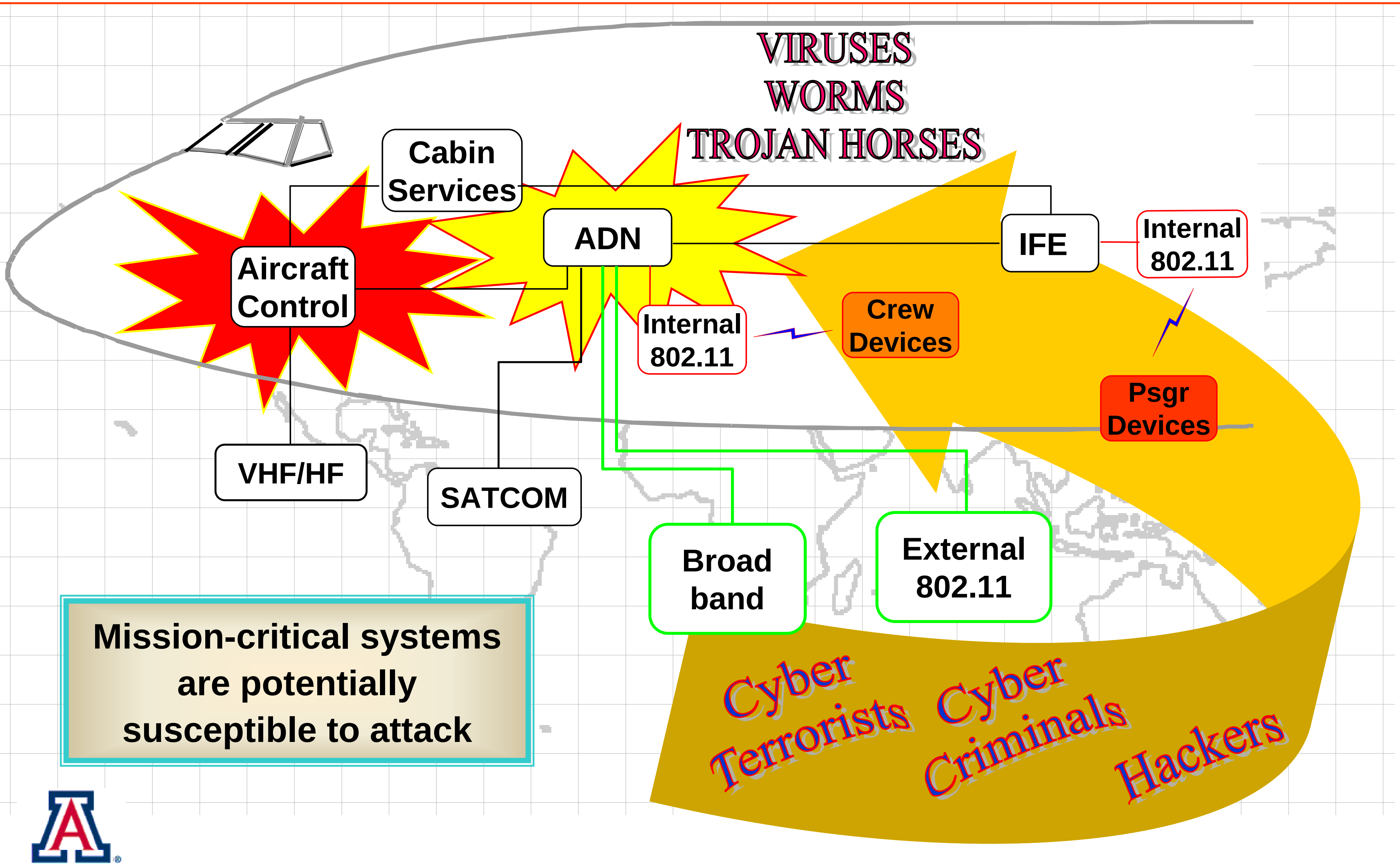
IT Infrastructure

DoD Foundation

- Policy/Doctrine/Governance
- Standards/Engineering/Architecture

Net Centric Aircraft?

GIG Security Challenges



Mission-critical systems are potentially susceptible to attack

Autonomic Computing

Self-Protecting Detect internal/external attacks and protect it’s resources from exploitation.

Self-Optimizing Detect sub-optimal behaviors and intelligently optimize resource performance.

Self-Healing Detect hardware/software failures and reconfigure to permit continued operations.

Self-Configuring Dynamically change resource configuration to maintain system & application requirements.

Autonomia **will ultimately provide all necessary tools for control and management of GIG networks and services.**

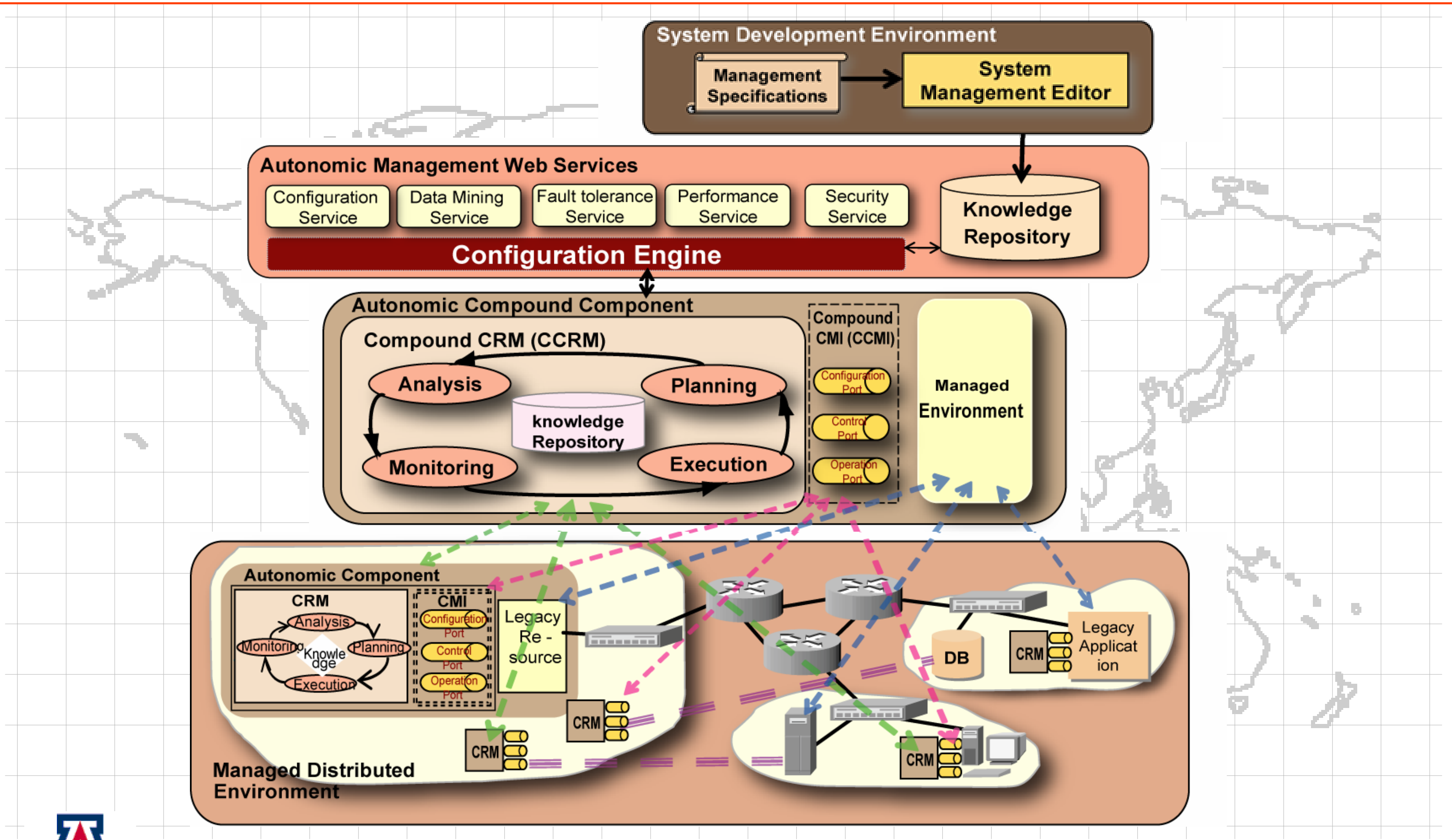
Autonomia Classification

- **Policy rule - Condition-action policy dictates the actions that should be taken whenever the system is in a given state.**

- **Optimization - Analytical techniques are used to model the overall system behavior and services through a utility function that is used to select the optimal adaptation strategy.**

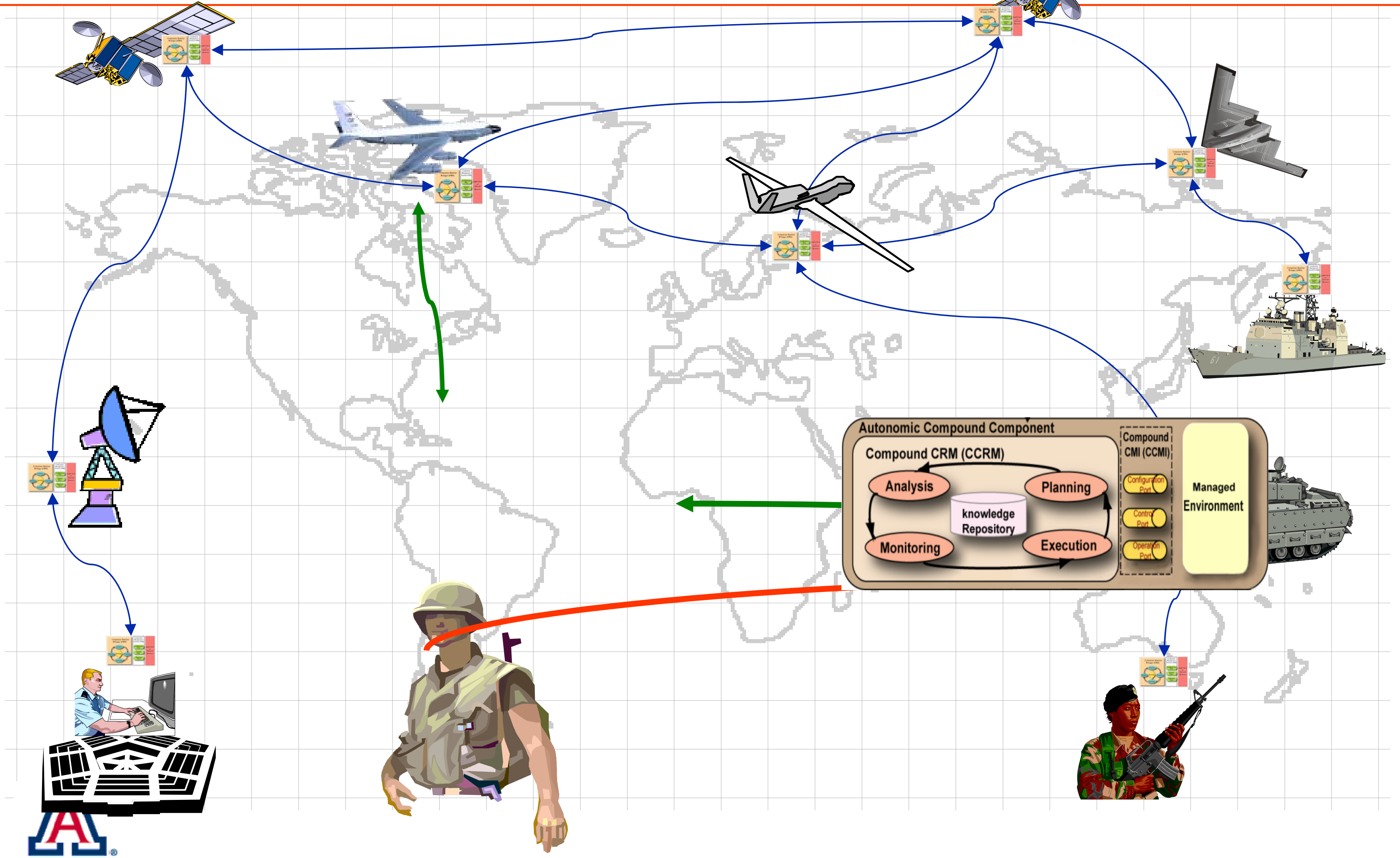
- **Artificial Intelligence - AI planning & learning techniques model system behavior by using data mining and statistical techniques.**

Autonomia Architecture

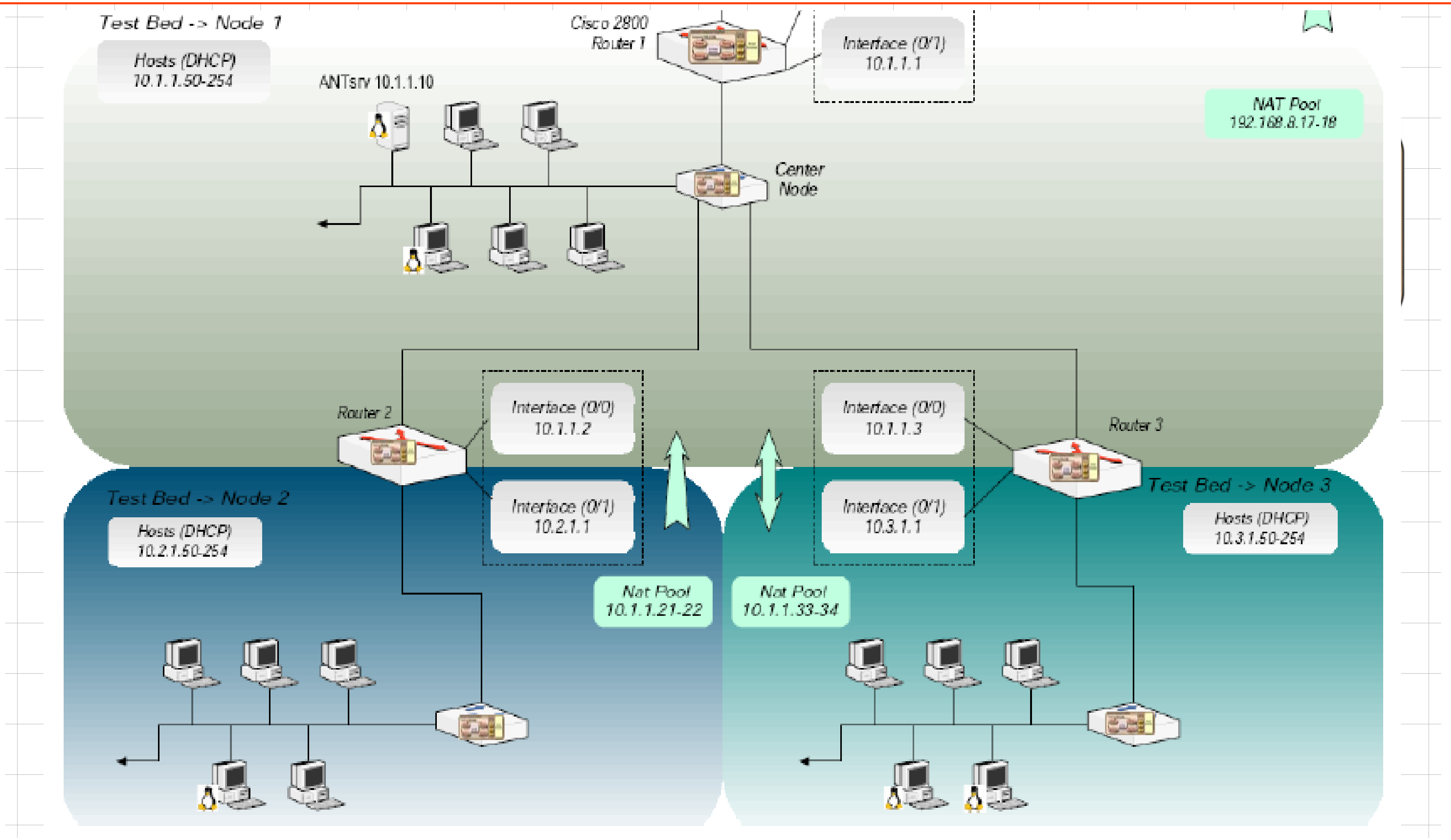


NON-ITAR

Autonomic Agent Approach



Autonomia Testbed



NON-ITAR

Test Results

USAF testing of Autonomia (Detection)

290,870 Netflow records – (70K normal + 220K abnormal)

Attack Category	*Attack Methods*	*Results*
Scanning	Xprobe2, APNET, Nikto, Traceroute, Nessus, SARA, NMAP , Queso	Detected
	Whisker, enum	Not detected
Passive Scanning	Ettercap	Not detected
Exploits	Ownstation, Snooqer, SMB/RPC Nuke, Jolt2, RPC DCOM, Octopus, Killthemessenger	Not detected
R2L	Netcat	Detected
DoS Attack	TCP SYN Flooding Attack, UDP flooding, ICMP flooding	Detected
Worm	theodin worm	Detected

False Alarms: 3

Feature Selection Validation

- USAF LAN (capture)
  - – DARPA Dataset KDD99 (Lincoln Labs)
  - – 9 Weeks raw TCP dump data.
  - – 5M connection records + 49K training records
  - – 41 features
  - – 22 different attack types

Class	UA Approach	Winner Entry using C5.0	CTree
Normal	98.45%	99.5%	92.78%
Dos	99.93%	97.1%	98.91%
U2R	92.55%	13.2%	88.13%
R2L	92.46%	8.4%	7.41%
PROBE	99.91%	83.3%	50.35%

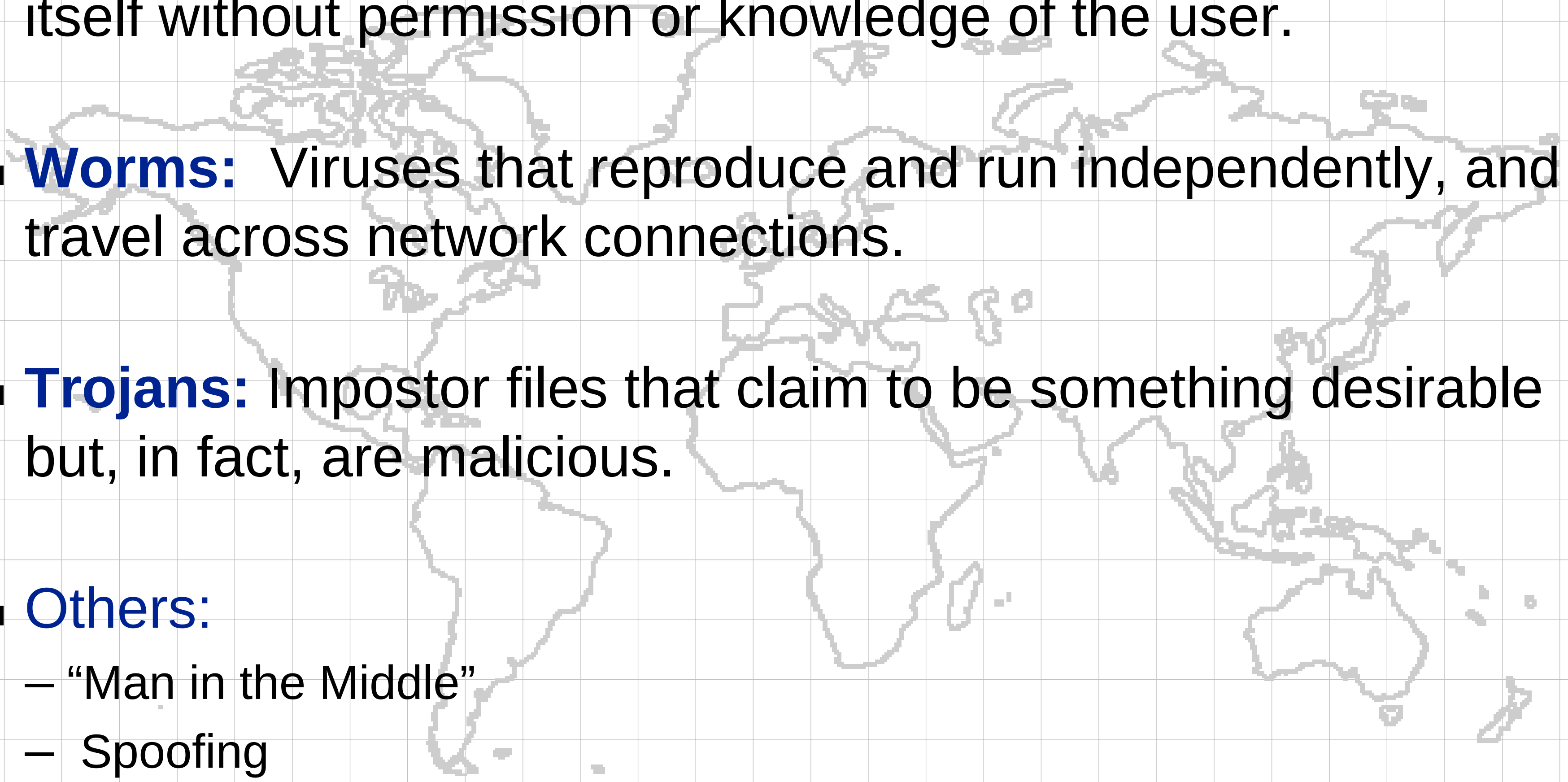
Conclusions

- Autonomia framework - autonomic computing systems and applications
- Supports “design-in” or legacy resources and software systems
- Initial Autonomia software modules to focus on self-protection (minimal)
- Existing Experimental Testbed (University of Arizona, Tucson)
- Effective in detecting and protecting the networks but immature
- Wide range of network attacks
- High detection rate accuracy + very low false alarms
- **Limits:**
  – Could not detect attacks that require payload monitoring or analysis
  – Internal or insider attacks (network monitors or ‘bad eggs’)

QUESTIONS?

Back-up Slides

Network Attack Technology



- **Viruses:** Computer program which distributes copies of itself without permission or knowledge of the user.
- **Worms:** Viruses that reproduce and run independently, and travel across network connections.
- **Trojans:** Impostor files that claim to be something desirable but, in fact, are malicious.
- Others:
  - "Man in the Middle"
  - Spoofing
  - Protocol (TCP) attacks

Additional Research

- **Payload monitoring and analysis**
  - **Current focus is on headers only**
- **Insider attack detection & defense**

- **Military MANET self-protect**
  - **Virtual Network Models**
    - **Network topology mapping targets**
      - **"Man-in-middle"**
      - **Spoofing**
- **Anti-tamper (captured weapons & personnel)**

References

- [Ananthanarayanan2005] R. Ananthanarayanan, M. Mohania, A. Gupta, *Management of Conflicting Obligations in Self-Protecting Policy-Based Systems*, The 2nd International Conference on Autonomic Computing, June 2005 Page(s):274 – 285

- [AutoAdmin] *The AutoAdmin project* http://research.microsoft.com/dmx/AutoAdmin

- [Bennani2005] M. Bennani, D. Menasce. *Resource Allocation for Autonomic Data Centers using Analytic Performance Models*. The 2nd International Conference on Autonomic Computing, June 2005 Page(s): 229- 240

- [Chen2004a] H. Chen, S. Hariri, B. Kim, M. Zhang, Y. Zhang, B. Khargharia, M. Parashar; *Self-Deployment and Self-Configuration of Network Centric Service*; The International Conference on Pervasive Computing, July 2004.

- [Chen2004b] M. Chen, A.X. Zheng, J. Lloyd, M. I. Jordan, E. Brewer, *Failure diagnosis using decision trees,* The 1st International Conference on Autonomic Computing, May 2004 Page(s): 36 – 43

- [Chen2006] H. Chen, S. Hariri, and F. Rasal, *An Innovative Self-Configuration Approach for Networked Systems and Applications* The 4th International Conference on Computer Systems and Applications (AICCSA-06)

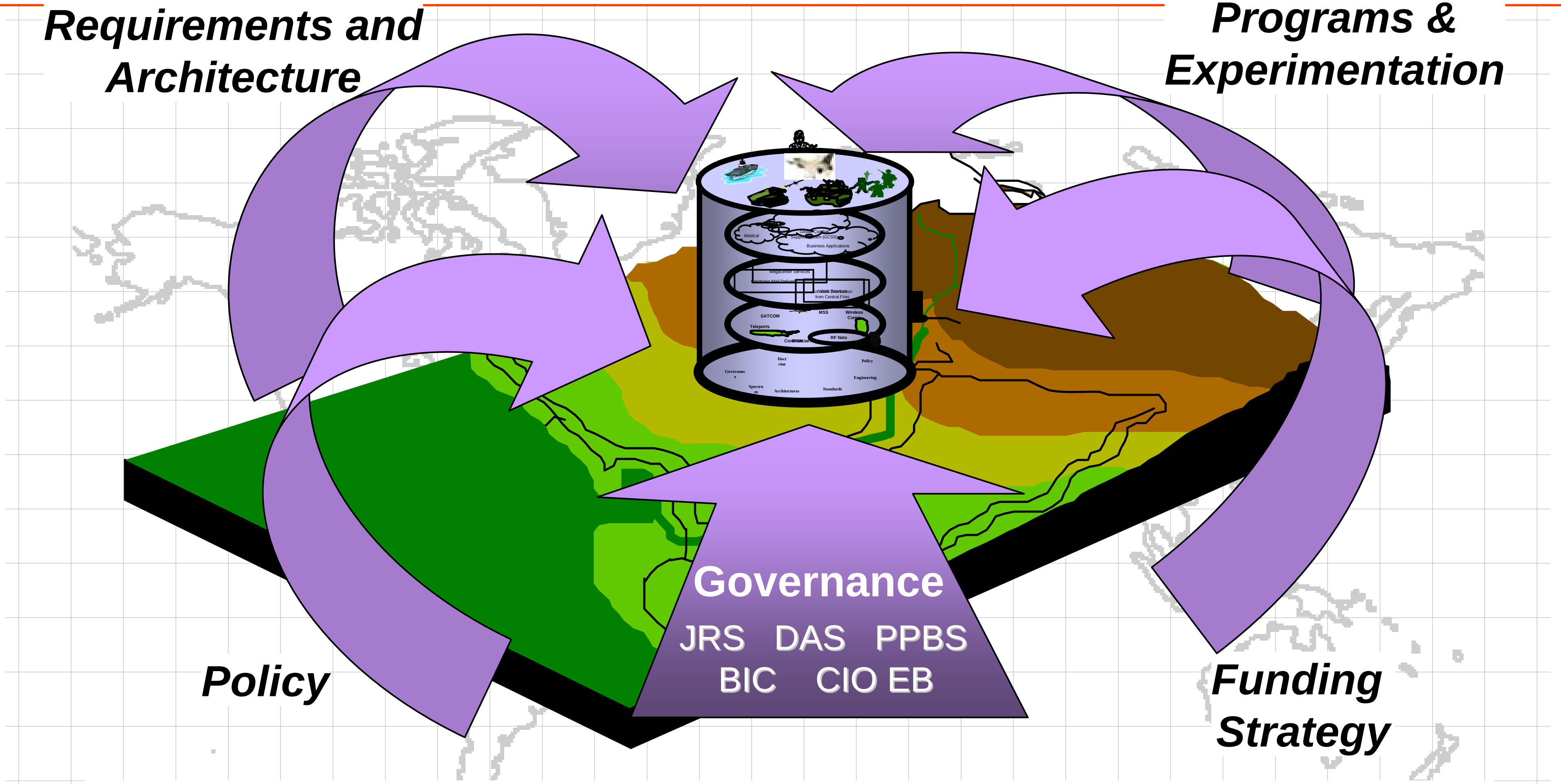
- [Chess2004] D. Chess, A. Segal, I. Whalley and S White, *Unity: experiences with a prototype autonomic computing system*, The 1st International Conference on Autonomic Computing, May 2004; Page(s): 140 – 147

- [CiscoACL2005] Access Control Lists and IP Fragments, http://www.cisco.com/warp/public/105/acl_wp.html, 2005

- [CiscoNetflow2006] Cisco IOS Netflow Introduction, http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html, 2006

- [Hariri2006] S. Hariri, B. Khargharia, H. Chen, Y. Zhang, B. Kim, H. Liu and M. Parashar, *The Autonomic Computing Paradigm,* Cluster Computing: The Journal of Networks, Software Tools and Applications, Special Issue on Autonomic Computing, Vol. 9, No. 2, 2006, Springer-Verlag.

GIG SCOPE



Requirements and Architecture

Programs & Experimentation

Policy

Funding Strategy

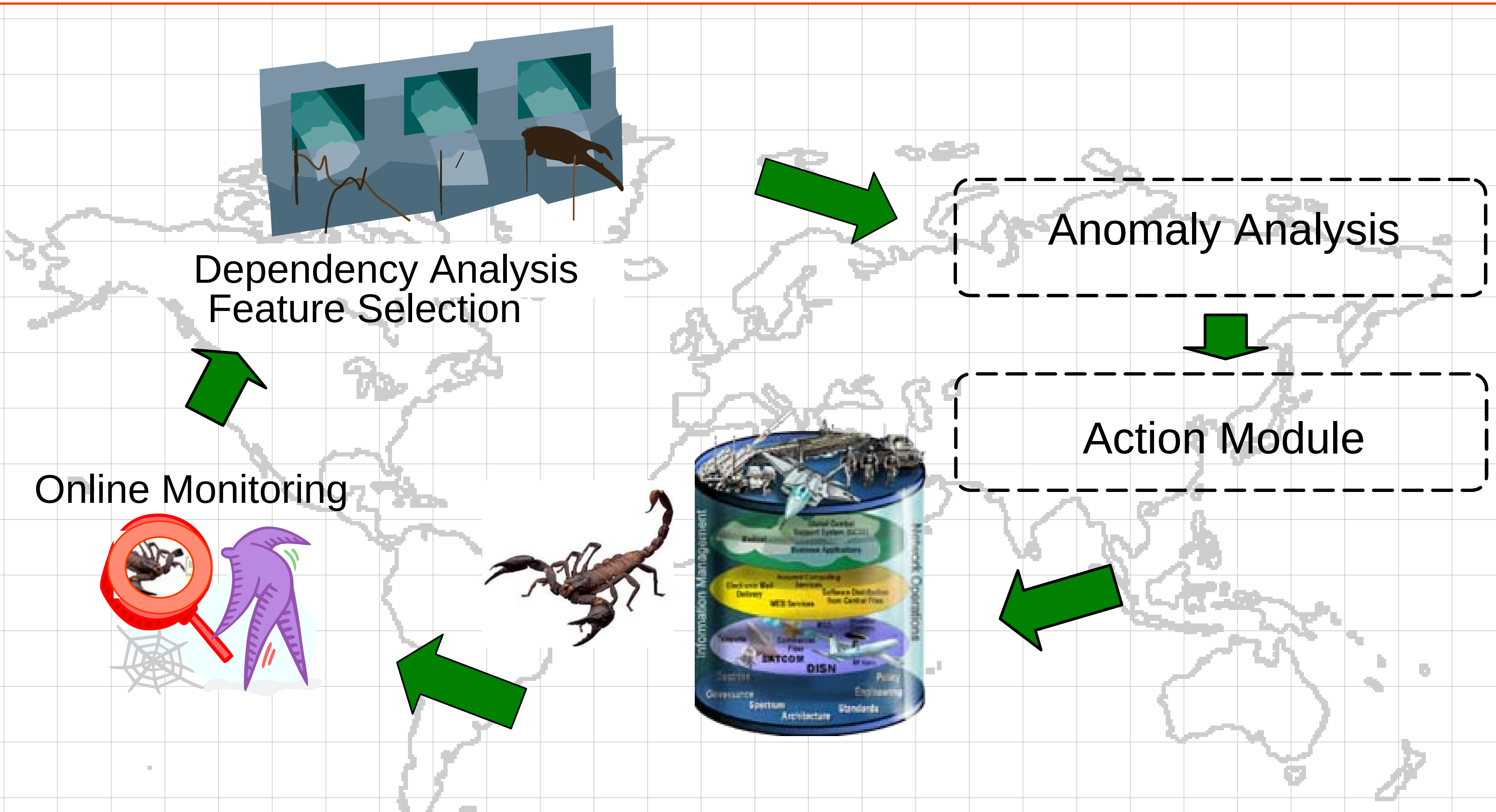
Governance

JRS DAS PPBS
BIC CIO EB

"Develop, maintain and facilitate the implementation of **a sound and integrated information technology architecture** for the executive agency."

(40 U.S.C. Section 1425)

Self-Protection Engine



Dependency Analysis
Feature Selection

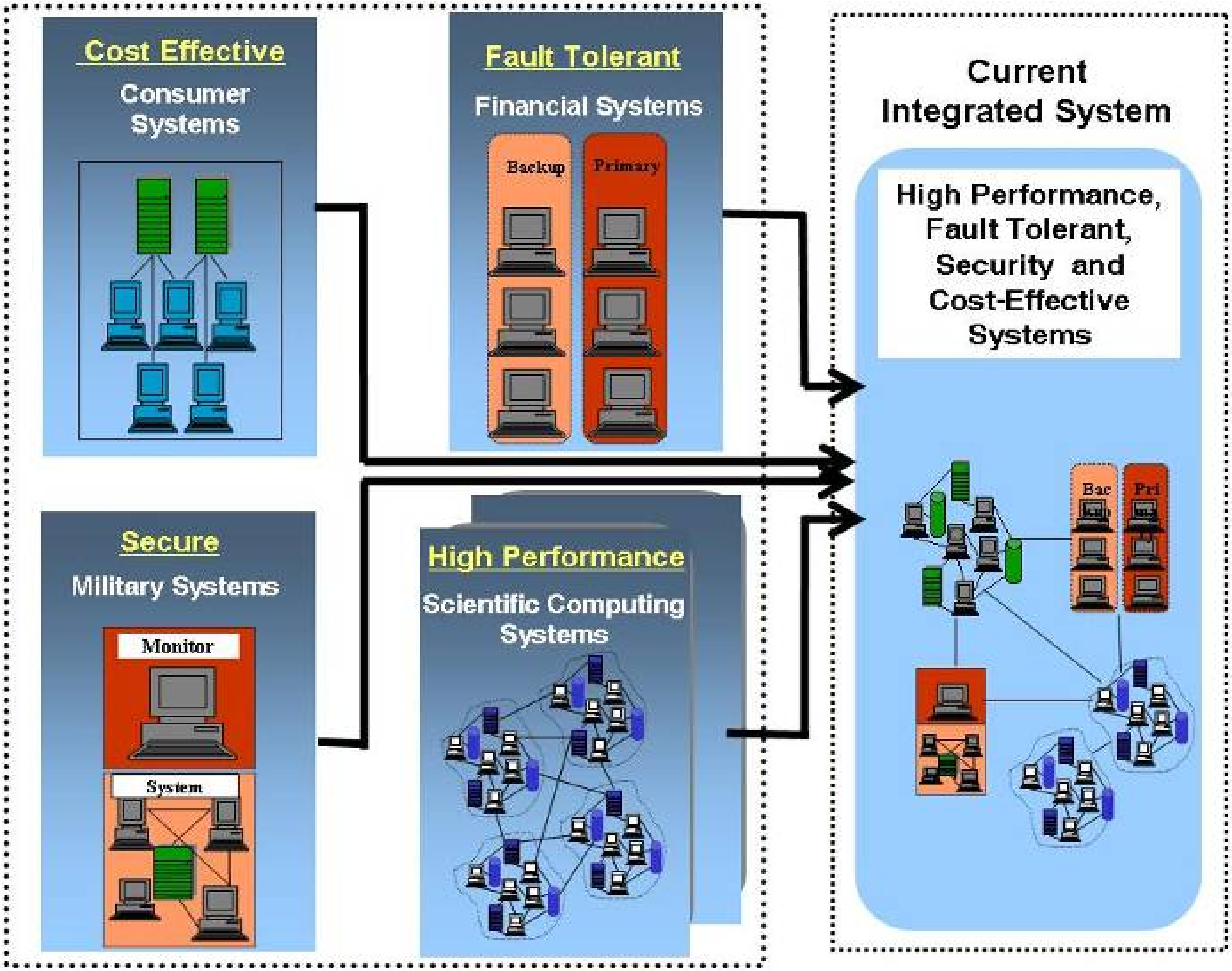
Anomaly Analysis

Action Module

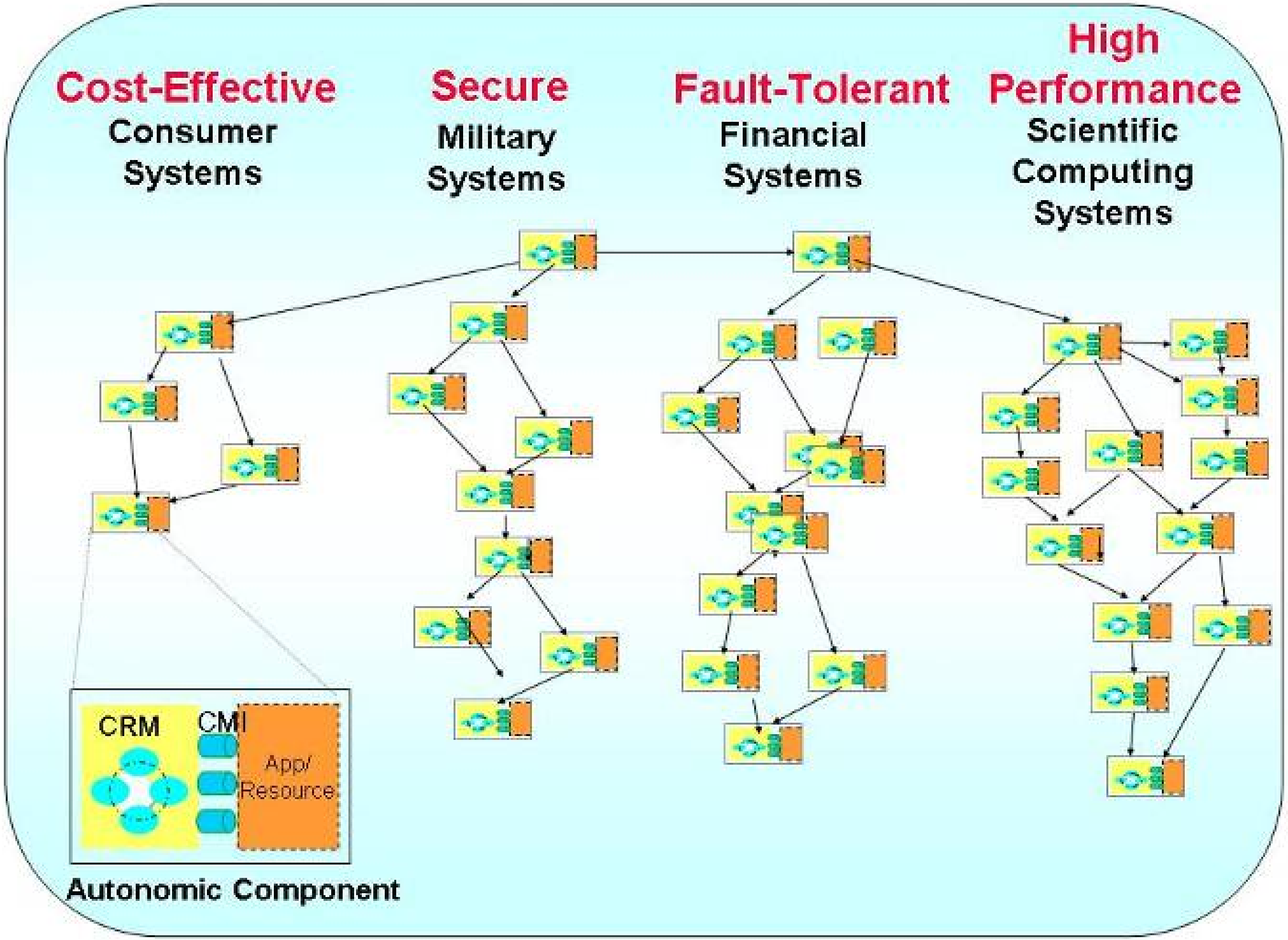
Online Monitoring

Primary goals: 1) Detect network attacks, known or unknown,
2) Proactively prevent or minimize impact on network operations and services.

Integration of isolated solutions

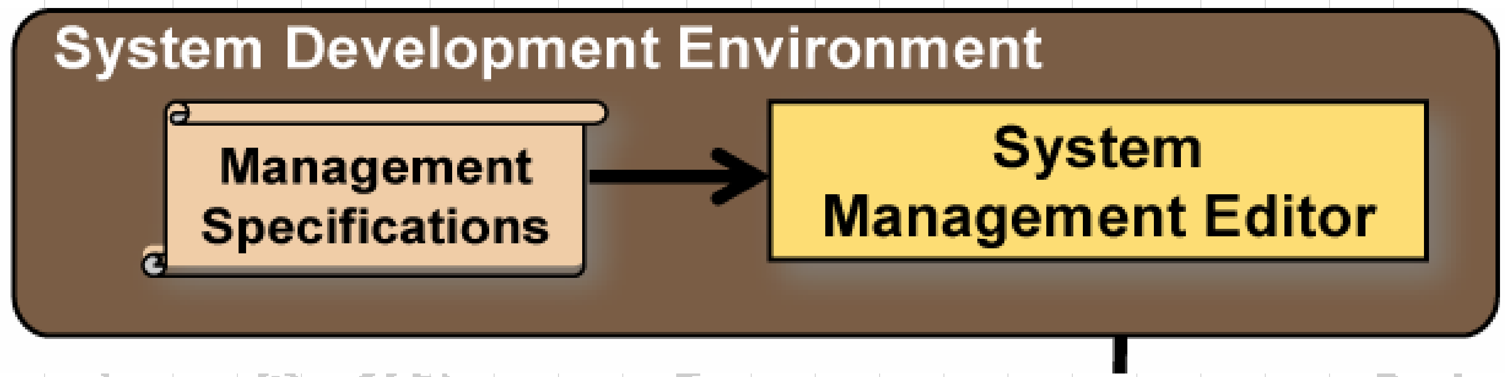


Holistic Approach to Autonomia



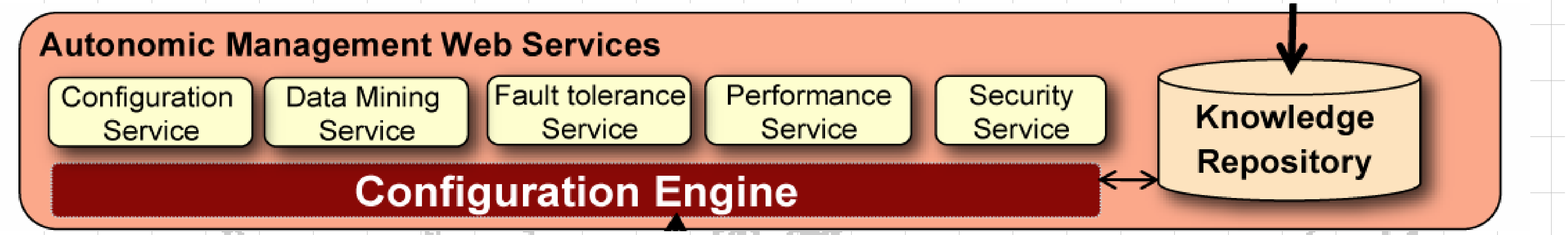
NON-ITAR

System Management Editor



Publishes component management policies according to the specified CMI schema.

Management Web Services



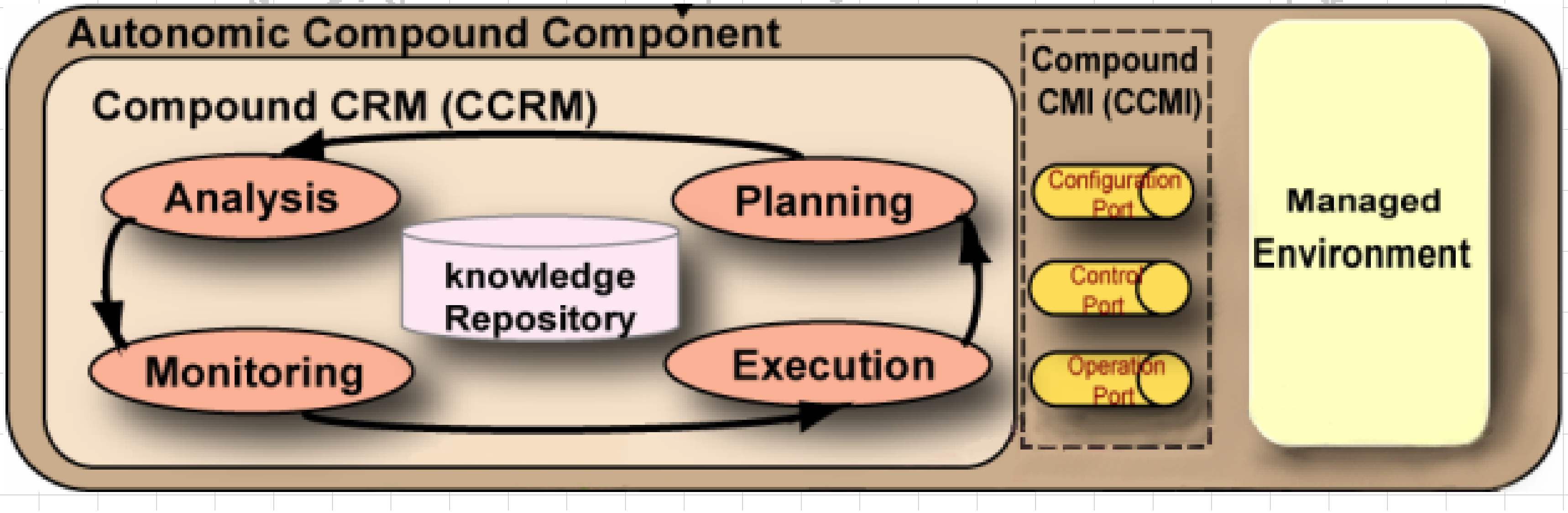
Provides algorithms & run time routines

- –Configuration services
- –Security
- –Fault tolerance
- –Performance

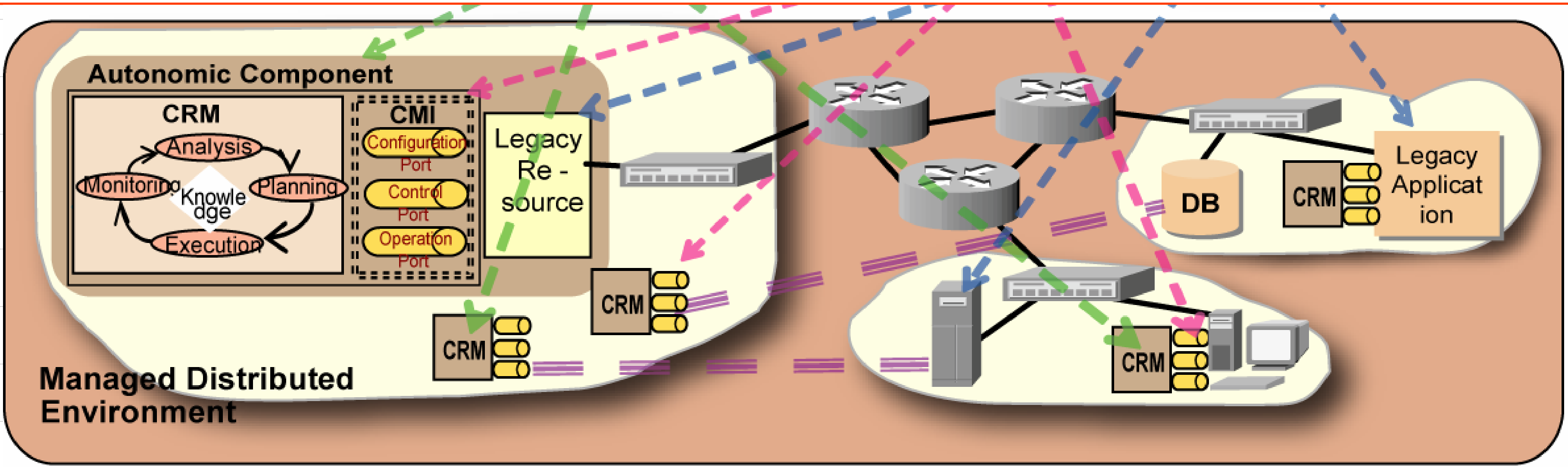
Compound CRM (CCRM)

- Manages Compound Components
  - Analysis
  - Monitoring
  - Planning
  - Execution

- CCMI Ports
  1. Configuration
  2. Control
  3. Operation

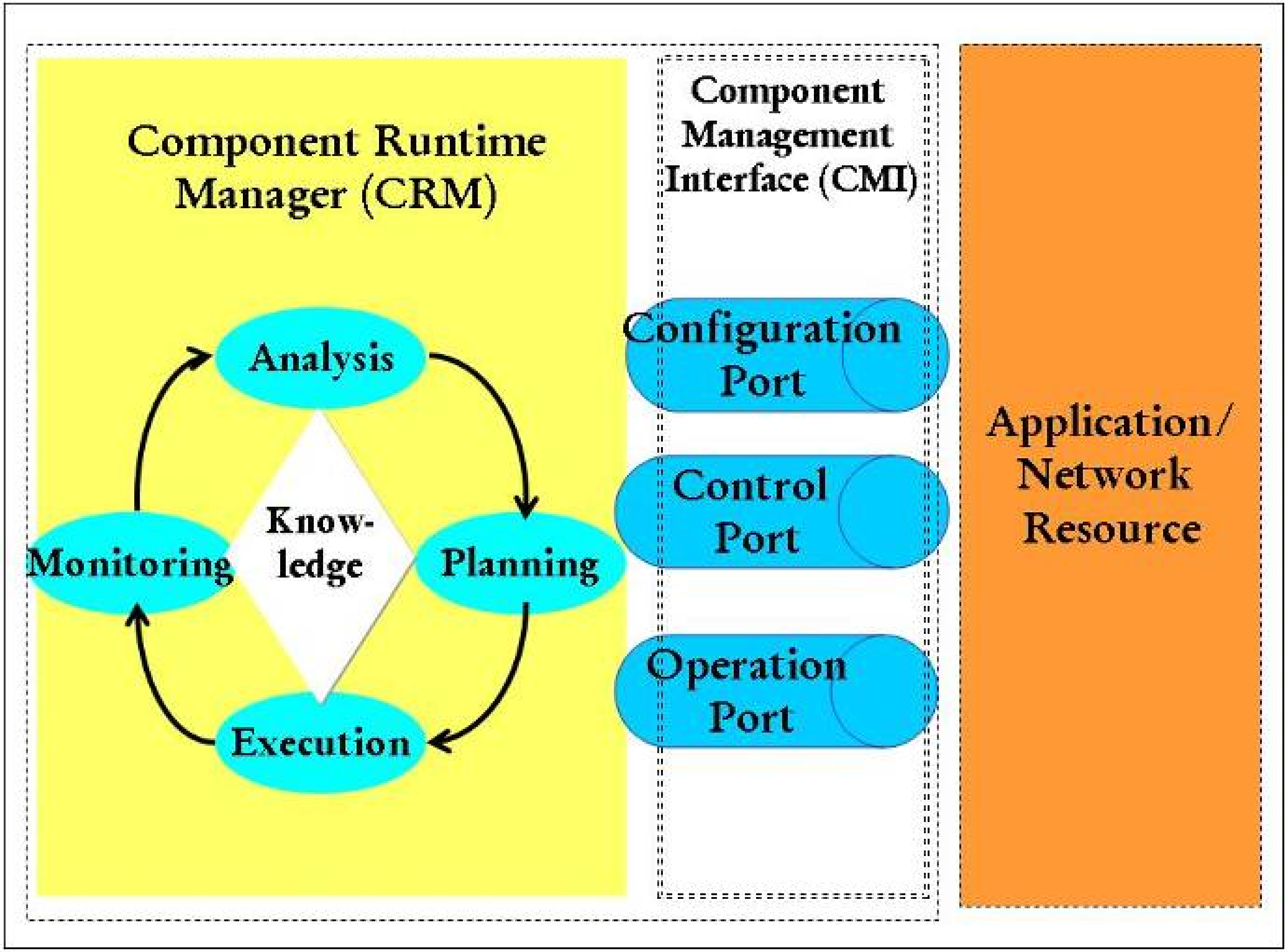


Managed GIG Environment



- **Larger autonomic systems**
  - **Hierarchical manner**
  - **Composed of many autonomic compound components**
  - **Deployed dynamically**
  - **Once deployed, becomes self-maintaining (“living”)**

CRM/CMI


Component Runtime Manager (CRM)
Component Management Interface (CMI)
Analysis
Monitoring
Know-ledge
Planning
Execution
Configuration Port
Control Port
Operation Port
Application/ Network Resource

NetFlow Data

Variable	Definition
Hid	Sequence id
Bytes	Number of bytes in this interval for a connection
Pkts	Number of packets in this interval for a connection
Input_snmp	related incoming/outgoing interface information
Output_snmp	
src_addr	IP source and destination address information
dst_addr	
Prot	Protocol number
L4_src/dst_port	Layer 4 port information
Next_hop	Next hop information
Src/dst_AS	Srouce/destination AS
Src/dst_mask	Mask of the src/dst IP
Tcp_flags	Bitwise OR of tcp flags
Src_tos	TOS of the connection

Feature Selection

FEATURE X	I(X; DOS)	I(X;DOS) / H(DOS)
count	0.647571	0.899405
dst_bytes	0.512438	0.711719
dst_host_same_src_port_rate	0.382541	0.531308
srv_count	0.338744	0.470478
dst_host_count	0.308133	0.427963
src_bytes	0.290684	0.403728
dst_host_srv_diff_host_rate	0.274275	0.380937
dst_host_srv_count	0.165472	0.229823
srv_diff_host_rate	0.165142	0.229364
dst_host_same_srv_rate	0.149499	0.207638
dst_host_diff_srv_rate	0.14109	0.195959
diff_srv_rate	0.084967	0.118009
dst_host_srv_serror_rate	0.081939	0.113804
same_srv_rate	0.080769	0.112179
dst_host_serror_rate	0.076816	0.106688

Intentionally Left Blank

(End Presentation)

NON-ITAR