



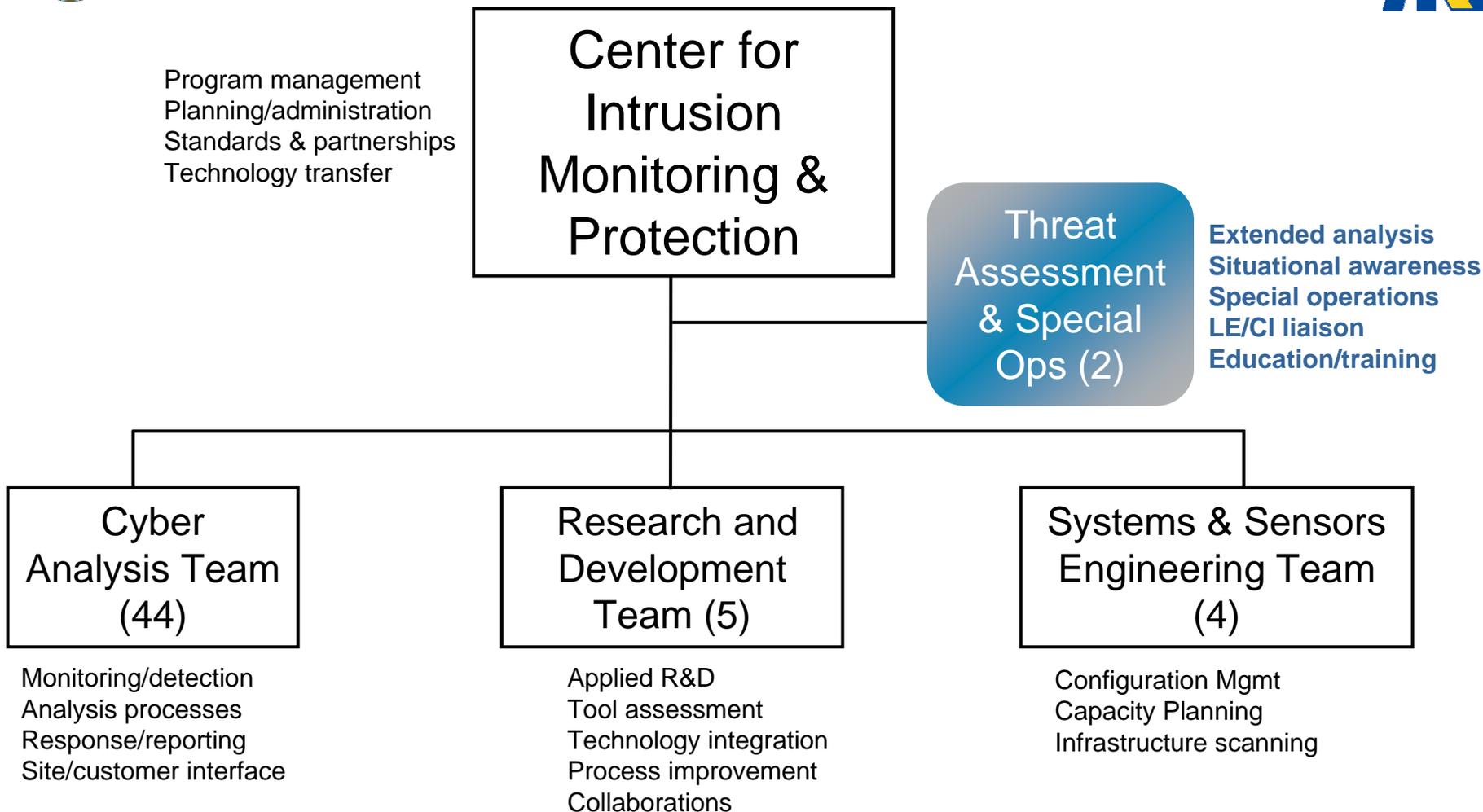
# Addressing the Intruder Detection Dilemma

## *ARL Center for Intrusion Monitoring and Protection*

**Kerry Long**  
Lead, Advanced Development  
Center for Intrusion Monitoring & Protection  
Computational & Information Sciences Directorate  
U.S. Army Research Laboratory  
301-394-2720  
klong@arl.army.mil



# What is the CIMP ?



The ARL Center for Intrusion Monitoring and Protection (CIMP) currently monitors and analyzes network data to detect intruders for multiple Army and DoD customers



# *Introduction-Our Assumptions*

---



- The number one threat to information confidentiality and integrity is the intruder who has gained access to a trusted cyber environment
- No matter what internal safeguards have been put in place, a successful intruder will ultimately undermine security goals
- There is currently no way to keep out a determined, savvy intruder from a publicly connected network



# *Introduction –Our Observations*



- Our nation's R&D infrastructure is a major target for sophisticated state sponsored attackers and cyber terrorists. Assets have been compromised, critical information has been exfiltrated, our technological advantage is at risk
- IA community is focused on developing tools and methods to prevent intrusions from occurring. Less resources are devoted to dealing with the situation once the intrusion has occurred
- Research and development in all IA related areas is largely decoupled from the implementers of IA



# Introduction –Our Objectives

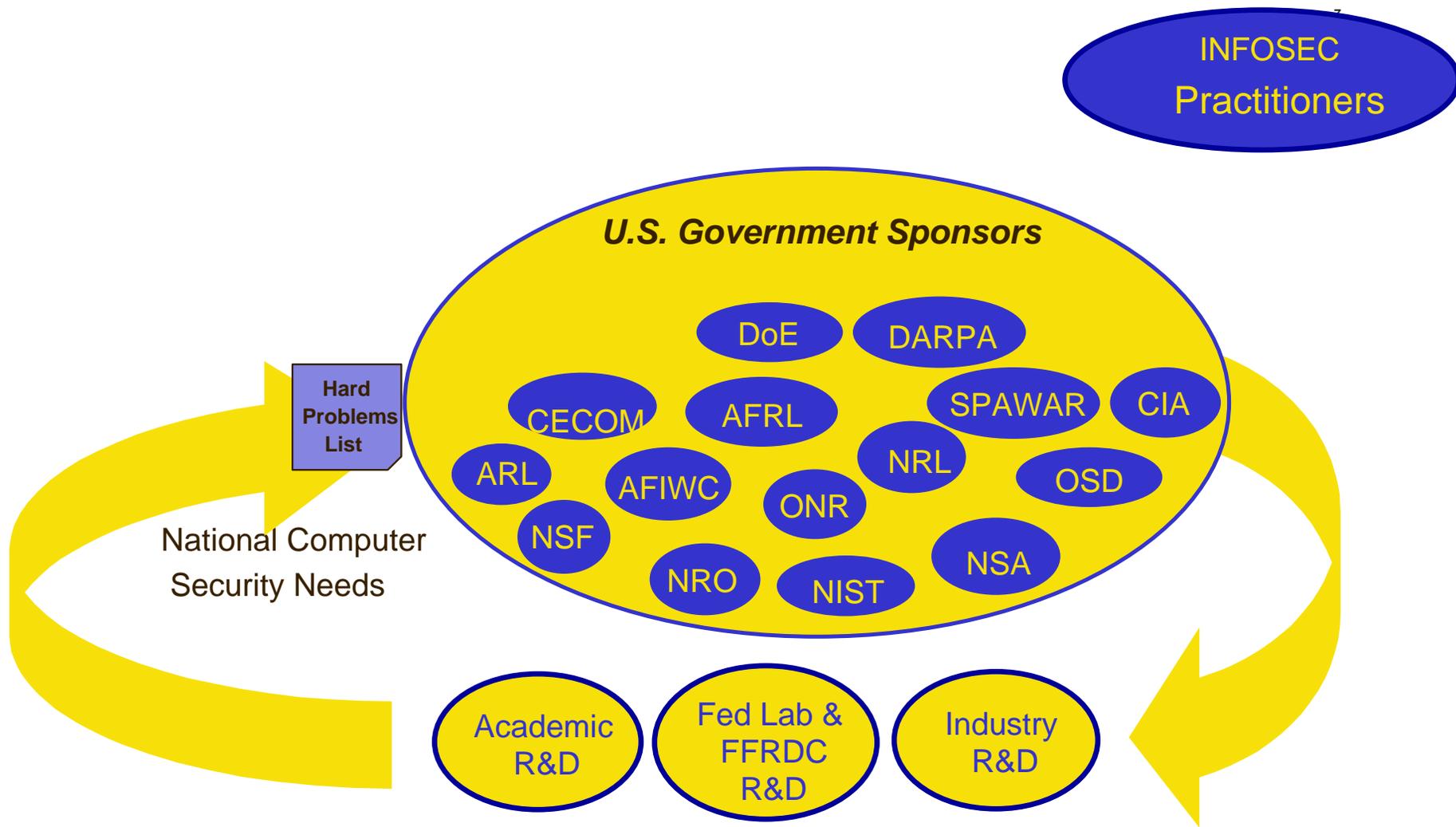
---



- To address the problem of the savvy intruder through detection rather than prevention. Plenty of others focused on prevention
- To develop better practical methods for detecting and dealing with intruders once they have penetrated a trusted network
- To couple our research and development with our operations into one constantly improving system



# How it's Currently Done





# *Why We're Different*

*Research and Development*

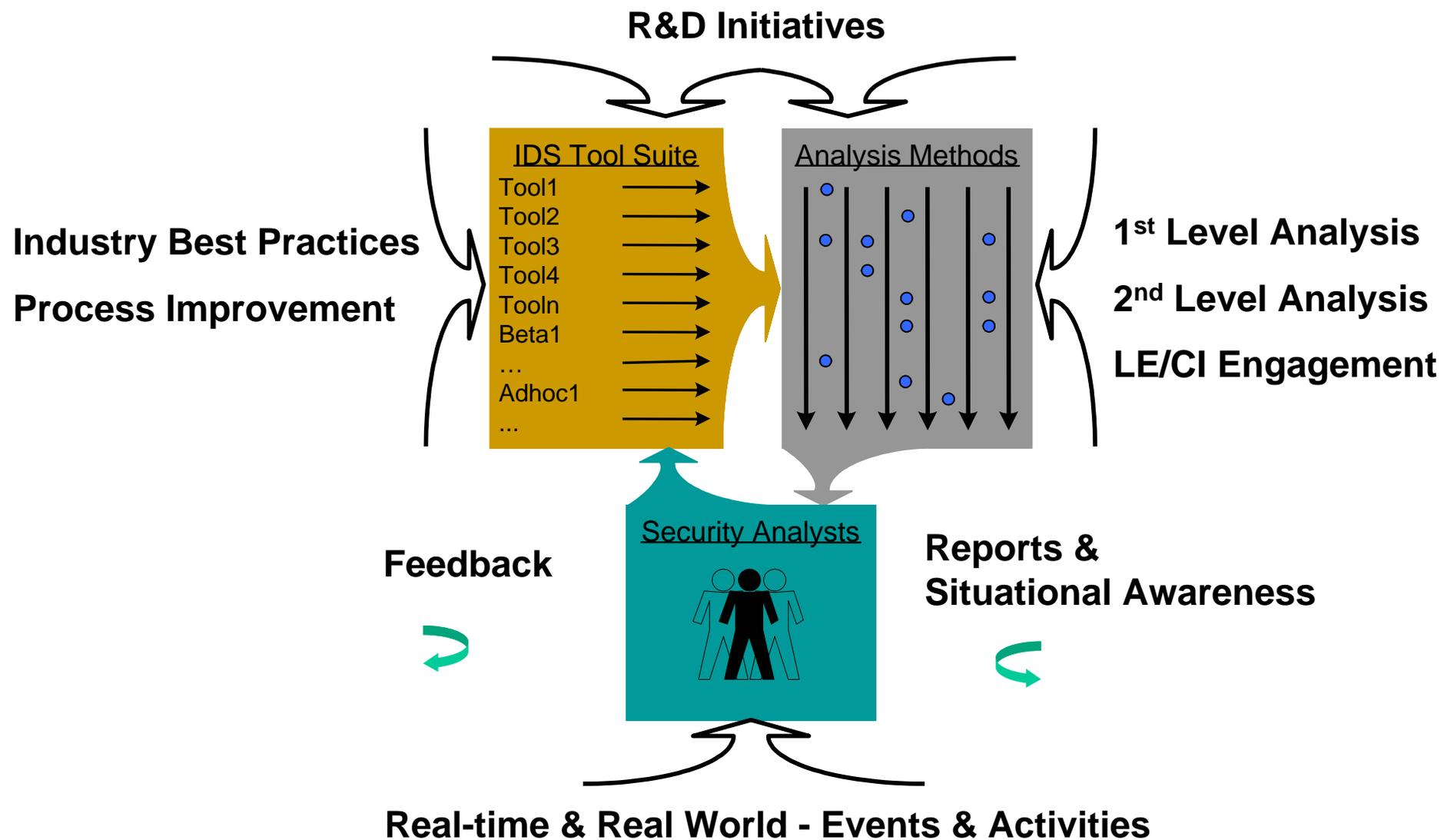
Network Raw Data  
Tool Assessment  
New Requirements

New IDS Tools  
Process Modifications  
New Methodology

*Security Analysts*

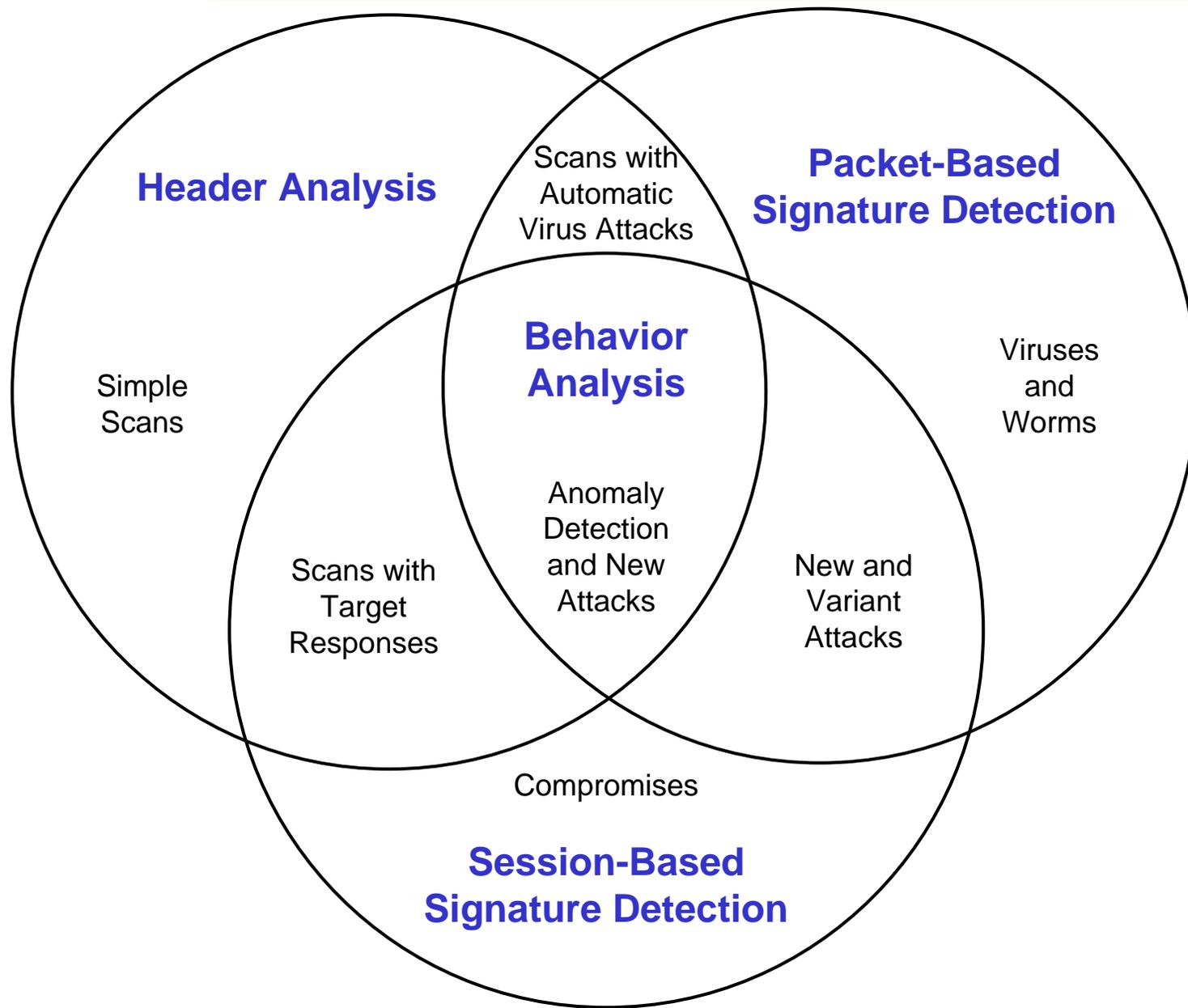


# Our IDS Model





# CIMP Toolset--Key to Success

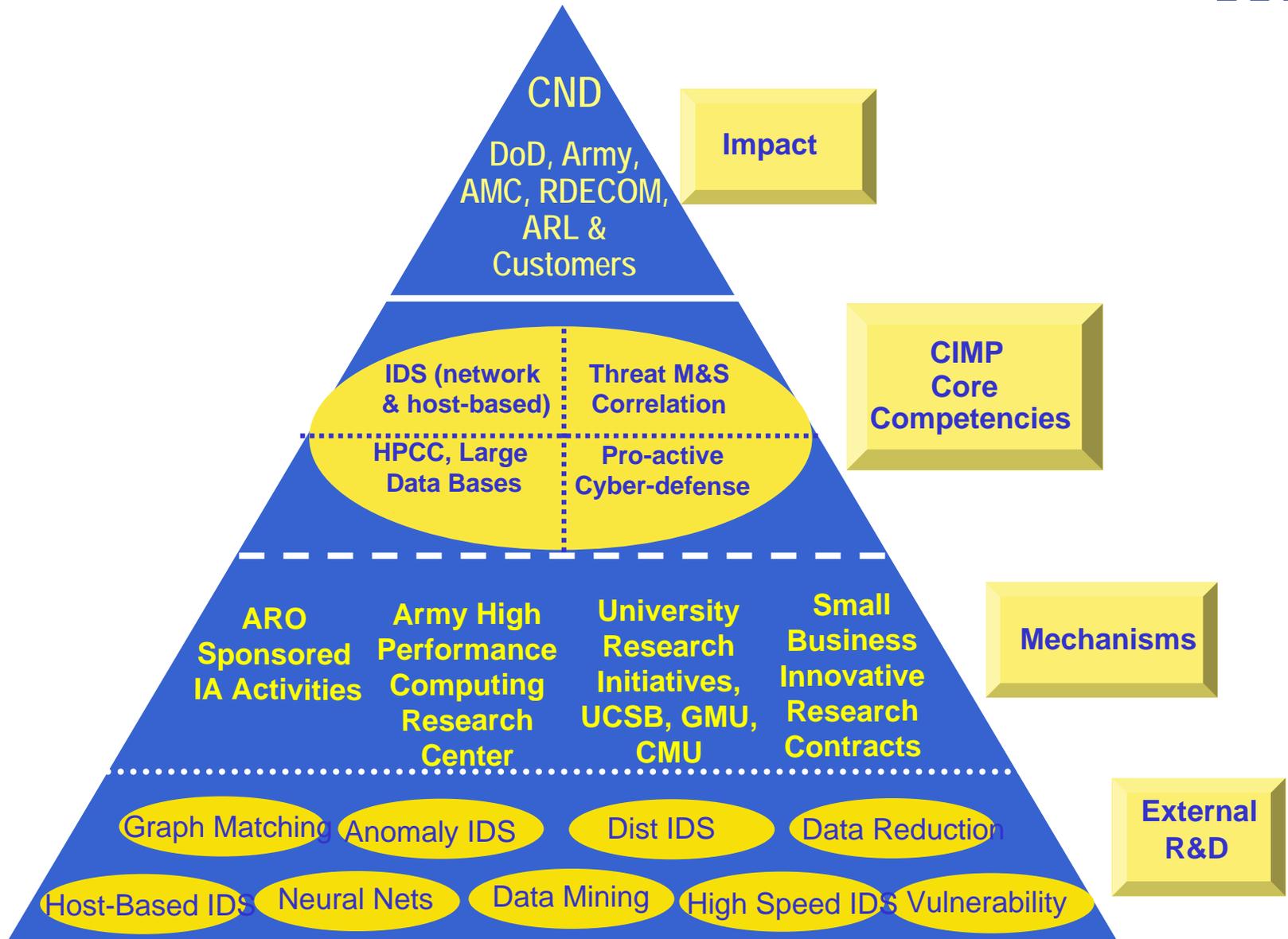




# R&D



## Computer Network Defense

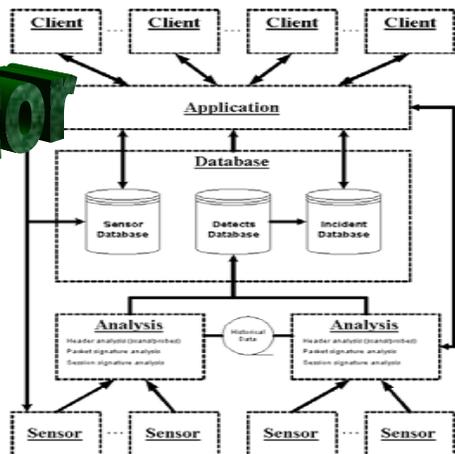




# Our current Research Initiative Interrogator



## Interrogator



## Objective

Development of a “near real-time” surveillance and analysis architecture that serves the needs of both researchers and analysts

## DoD capabilities enhanced by this project

Allows new detection methods to be thoroughly tested and prototyped without adversely affecting monitoring operations. Enables rich data mining operations and true retrospective analysis

## Scientific/technical approaches

- Sensors are easily configurable, inexpensive and are designed to be placed in hostile environment
- Enables advanced network security analysis over extended locations/periods of time
- Allows quick introduction of new tools and techniques in detecting attacks on networks
- Core idea: use analysts to test new IDS concepts as part of their everyday workflow

## Accomplishments

- Developed an integrated architecture that communicates securely and continuously between sensors and data repository
- Developed a distributed sensor monitoring and statistics tool
- 15 sensors currently in place operating in beta environment
- Designed and implemented an alerts database that allows a Network Security Officer to view and analyze alerts over multiple sites



# *What We're Striving For...*

---



- 
- effectively by other organizations or private sector
- Accelerate the integration of new methodology, technology and tools
- Establish an IA lab to be the mechanism for technology development and transfer

***We want to have an impact!***