



NAVAL  
POSTGRADUATE  
SCHOOL

***The Need for Distributed Intelligence  
Automation Implemented through Four  
Overlapping Approaches  
Intelligence Automation Software, Standardization for  
Interoperability, Network-Centric System of Systems  
Infrastructure (with Advanced Cloud Computing) and  
Advanced Sensors***

Presented by: Rachel Goshorn, Ph.D.

C4I Chair, Director Distributed GIG Intelligence Automation  
Systems Lab, Asst Prof, ECE Dept, Naval Postgraduate School

Monterey, California  
WWW.NPS.EDU





NAVAL  
POSTGRADUATE  
SCHOOL

# Four Goshorn Authors - Paper is the Result of 10+ Years of Goshorn Collaboration

**Dr. Lawrence  
Goshorn**

**Dr. Rachel  
Goshorn (me!)**

**Dr. Joshua Goshorn  
(Ph.D, 2011)**

**Dr. Deborah  
Goshorn**



\* **10+ Years of Collaboration in Intelligence Automation for Distributed Systems (+growing up w/ advanced technologies)**

\* **Invited Book Chapter:** Reference: Rachel E. Goshorn, Deborah E. Goshorn, Joshua L. Goshorn, and Lawrence A. Goshorn **"Behavior Modeling for Detection, Identification, Prediction, and Reaction (DIPR) in AI Systems Solutions"** Handbook of Ambient Intelligence and Smart Environments, Springer Handbook (<http://www.springerlink.com/content/n812r0064785g764/> )

WWW.NPS.EDU

\* **Invited Book on Tutorial Material Underway (majority of book material completed)**

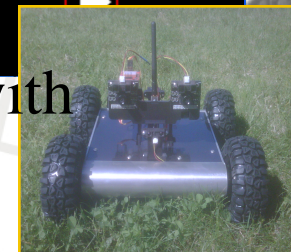
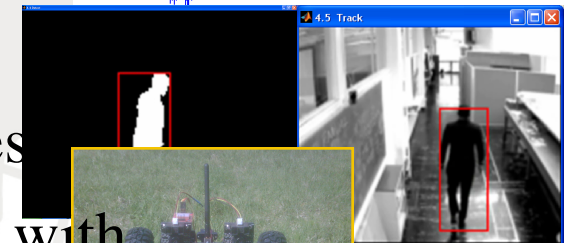
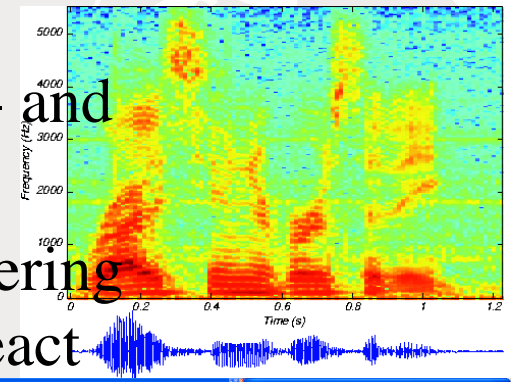




NAVAL  
POSTGRADUATE  
SCHOOL

# AI History of Events to Now ...

- 11-12 yrs ago: started intelligence automation
- 10 yrs ago: intelligence automation (looking for “bad behaviors” of people in the lab, cars on the freeway)
- 4-6 yrs ago: finding bad behaviors/jamming signals in the blue-comms spectrum and removing them
- 3-6 yrs ago: finding IED initiators (bad behaviors) - and selective jamming of IED initiators
- 1.5-3 yrs ago: AI Network-Centric Systems Engineering Lab with fixed sensors. Detect, Identify, Predict, React (DIPR)
- Now-1.5 yrs ago: mobile ground/airborne vehicles
- Now-1.5 yrs ago: NetCentric Operations/Warfare with automated unmanned vehicles
- Now-1 year ago: Concept Level - Intelligence Automation for Cyber Security/Warfare





# Need for Automation

**1. Predict & Prevent  
Terror/Crime  
(DoD, DHS, Everyday)**

**2. Current Economic  
Crisis  
(Crime/Terror ↑ + \$ ↓)**

*drives*

**Need for  
Automation**

*drives*

**1. Need for  
Intelligence  
Automation**

**2. Need for  
Standardization  
for  
Interoperability**

**3. Need for  
Network-Centric  
System of  
Systems**

**4. Need for New  
Sensors**

***Need for Intelligence Automation and Specialized Sensors at  
Multiple Levels of the GIG***





# Need for Automation

**Predict & Prevent  
Terror/Crime  
(DoD, DHS, Everyday)**

**Current Economic  
Crisis  
(Crime/Terror ↑ + \$ ↓)**

*drives*

**Need for  
Automation**

*drives*

## **1. Need for Intelligence Automation**

- 1. Detection
- 2. Identification
- 3. Prediction
- 4. Reaction
- + advanced fusion
- + advanced learning

## **2. Need for Standardization for Interoperability**

- 2a. Standard  
Interfaces
- 1. Intel  
Automation
  - 2. Comms
  - 3. Security

- 2b. Standard  
GIG Nodes
- 1. Dumb (pass  
raw data)
  - 2. Intelligent (some  
automation)
  - 3. Stand Alone (with  
rules of engagement)

## **3. Need for Network-Centric System of Systems**

- 1. Top-Down System  
(Enterprise/Collaboration/Cloud)
- 2. Bottom-Up System  
(Origination of Data: sensors,  
unmanned systems, etc)
- 3. Middle-Ware System  
(Smart push/smart pull)
- 4. Side-View System  
(Disadvantaged Users)  
+ NC Core (integrates SoS)  
(networks, comms, distributed  
processecing, real-time processing,  
cyber,...)
- + Where is the data?! (back-ups)

## **4. Need for New Sensors**

New threats  
require new  
sensors (comply  
with standards  
of #2)

***Need for Intelligence Automation and Specialized  
Sensors at Multiple Levels of the GIG***



# The Need

**Driver 1: Predict/Prevent Terror/Crime**

Driver 2: Current Economic Crisis



# Current/Future Warfare

- Terror threats are national, worldwide, and across the maritime domain (brown, green blue waters), and are the defining forces of the GWOT and Homeland Security.
- To mitigate these threats, we must automate detection, identification, prediction and reaction to nationally and globally distributed potential terror threats.
- The Global Information Grid (GIG), whether global or national, is the building block to bring information together.
- From information, comes intelligence.





# Current/Future Warfare (Cont.)



- GWOT and Homeland protection is made up of two elements: intelligence to determine a threat and the force to stop it.
- Intelligence is currently made up of mostly human intelligence, inputted manually into the GIG, and intelligence officers/analysts analyzing and predicting.
- With sensor numbers, and sensor types growing, there will never be enough: humans, intelligent centers, or bandwidth.
- Once GIG nodes are mobile, there will never be enough: bandwidth, power, or weight.
- The unmanned world has to be automated through intelligence automation.







# Network-Centric Warfare/Operations Implementation

- Mission
- Rules of Engagement
- GIG Technologies
- Situational Awareness
- Behavior Modeling
- Behavior Prediction— object and behavior tracking through the GIG
- Extraction of Key Features from Sensor Data
- Sensors to Collect Necessary Data
- Platforms for sensors





# Sensors: Collection of Information

- Sensors – Fixed



- Sensors – Mobile
- Unmanned Ground Vehicle (UGV)
- Unmanned Aerial Vehicle (UAV)
- Unmanned Surface Vehicle (USV)
- Unmanned Underwater Vehicle (UUV)

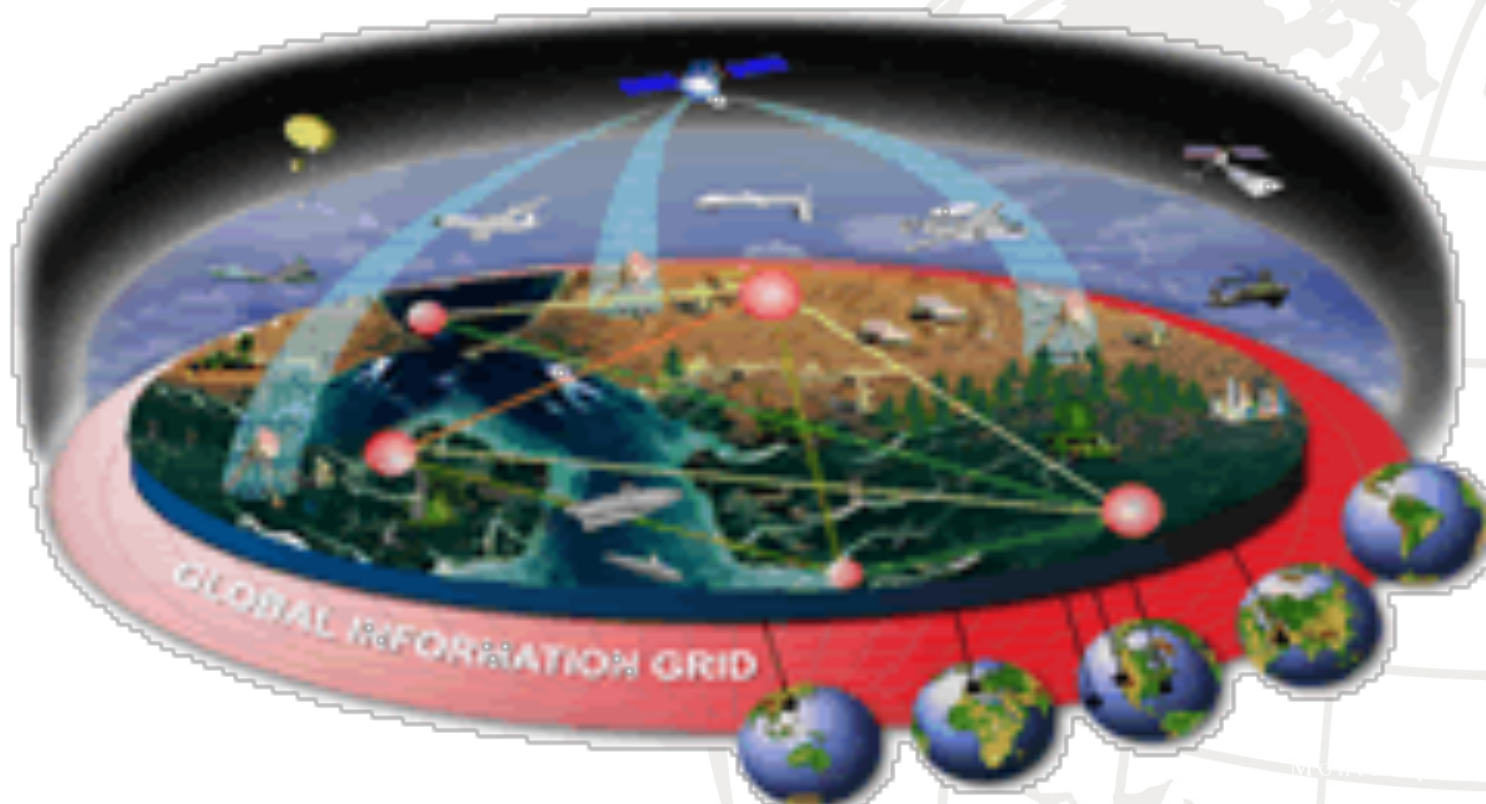






# The Global Information Grid (GIG)

- Big picture GIG
  - Inside and outside of the DoD
  - All information sources for C4ISR





# Where is the GIG Going?

Internet – everything is going to IP!

- What does this mean for the GIG?
- 4G (mobile comms) – all IP
  - Multi-media, virtual networks, VOIP, ...
  - Taking over from GSM ...
  - Once in IP world – never go through telephone switching
  - GIG will be - Parallel virtual networks
- Collaboration, service oriented architectures (SOA), enterprises, clouds, etc ...
- *Everything will be connected!!*
- NSA and the GIG: [http://www.nsa.gov/ia/programs/global\\_industry\\_grid/index.shtml](http://www.nsa.gov/ia/programs/global_industry_grid/index.shtml)



# Sensors = Too Much Data!

## Military Is Awash in Data From Drones

By CHRISTOPHER DREW  
Published: January 10, 2010

HAMPTON, Va. — As the military rushes to place more spy drones over Afghanistan, the remote-controlled planes are producing so much video intelligence that analysts are finding it more and more difficult to keep up.

 [Enlarge This Image](#)




Master Sgt. Demetrius Lester/U.S. Air Force, via EPA  
An MQ-1 Predator drone returned from a mission to Bagram Air Base in Afghanistan in 2008.

Air Force drones collected nearly three times as much video over Afghanistan and Iraq last year as in 2007 — about 24 years' worth if watched continuously. That volume is expected to multiply in the coming years as drones are added to the fleet and as some start using multiple cameras to shoot in many directions.

A group of young analysts already watches every second

☒ SIGN IN TO RECOMMEND

 TWITTER

 SIGN IN TO E-MAIL

 PRINT

 SINGLE PAGE

 REPRINTS

 SHARE

**CRAZY HEART**  
NOW PLAYING  
**3** ACADEMY AWARD  
NOMINATIONS

<http://www.nytimes.com/2010/01/11/business/11drone.html?pagewanted=1>





# Example

## *Bandwidth Required*

- 100 million keyboards, typing 10 characters a second, this is 1 billion bytes per second, all the keyboards in the world
- If you have a 20 megapixel camera, each pixel being 3 bytes, is 60 megabytes; if you're transmitting that at 30 frames/sec, that's 1.8 billion bytes per second
- Twice as many bytes as 100 million keyboards from one camera
- Therefore, there is a paradigm shift in network bandwidth required for all of these surveillance cameras
- With millions of these distributed, you will never have the humans, facilities, or bandwidth
- **Intelligence Automation (e.g. DIPR) is the ultimate bandwidth compression algorithm, facilities, and human savings**



## *Mobile/Satellite Bandwidth, Power, Weight*

- For every transmission, it takes a fixed amount of energy per bit – (energy per bit)
- If you transmit  $10^2$  bytes/sec versus  $10^7$  bytes/sec, you save  $10^5$  bytes/sec that don't have to be transmitted, and save  $10^4 - 10^5$  in power, thereby saving weight
- If 100 watts transmitting over  $10^8$  bits (one watt per million bits). If, only transmitting  $10^3$  bits, it's one milliwatt of power total for the same energy per bit
- Paradigm shift in bandwidth, power and weight requirements for mobile systems. Therefore, future will be the same for nano-satellites
- **Therefore, if bandwidth goes down, power goes down, weight goes down in mobile systems and future nano-satellites**
- **Intelligence Automation (e.g. DIPR) is the ultimate bandwidth, power and weight compression algorithm**



NAVAL  
POSTGRADUATE  
SCHOOL

# Network-Centric Warfare/Operations Implementation

*Planning*

- Mission
- Rules of Engagement
- GIG Technologies
- Situational Awareness
- Behavior Modeling
- Behavior Prediction— object and behavior tracking through the GIG
- Extraction of Key Features from Sensor Data
- Sensors to Collect Necessary Data
- Platforms for sensors

*Automation*

**1. Need for  
Intelligence  
Automation**

**2. Need for  
Standardization  
for  
Interoperability**

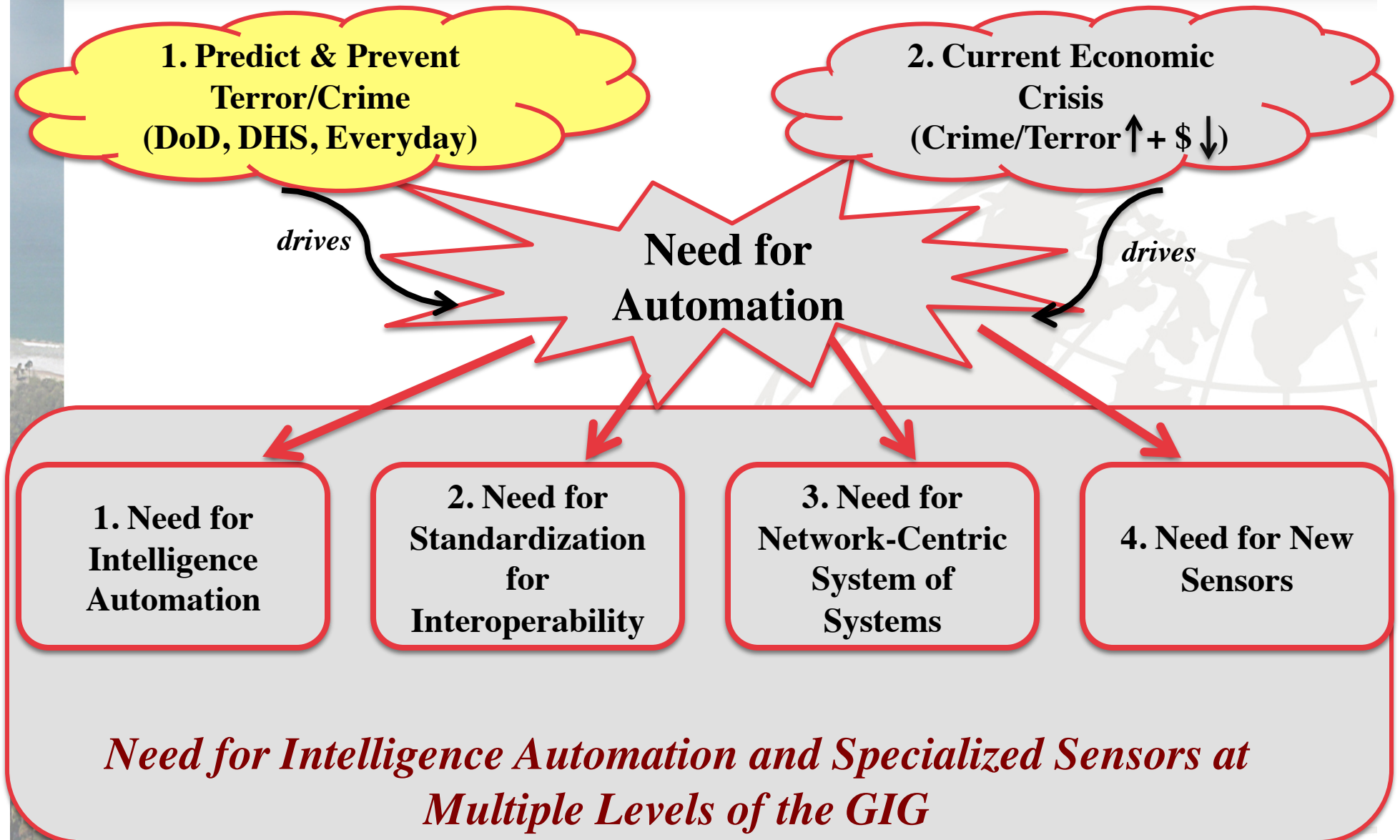
**3. Need for  
Network-Centric  
System of  
Systems**

**4. Need for New  
Sensors**





## Driver 2. Current Economic Crisis





# The Need

Driver 1: Predict/Prevent Terror/Crime

**Driver 2: Current Economic Crisis**



# Telephone Switching

## *Telephone Operators*



- 1920's – my Grandma worked as a telephone operator.
- 1920's - people projected a huge growth in the number of telephones.
- Based on the need – concluded they would need to *hire every high school girl graduate* as a telephone operator.

*Technology created – switching circuits  
(automated telephone operators)*





# Current Economic Crisis

***Terror/Crime Rates Are Going Up  
(Global, National, Local)***



***Requires increase in  
number of people***

***Budgets are Being Cut  
(DoD, HLS, Federal, State, Local)***



***Requires decrease in  
number of people***

***Forced to Automate***



## Example - Police

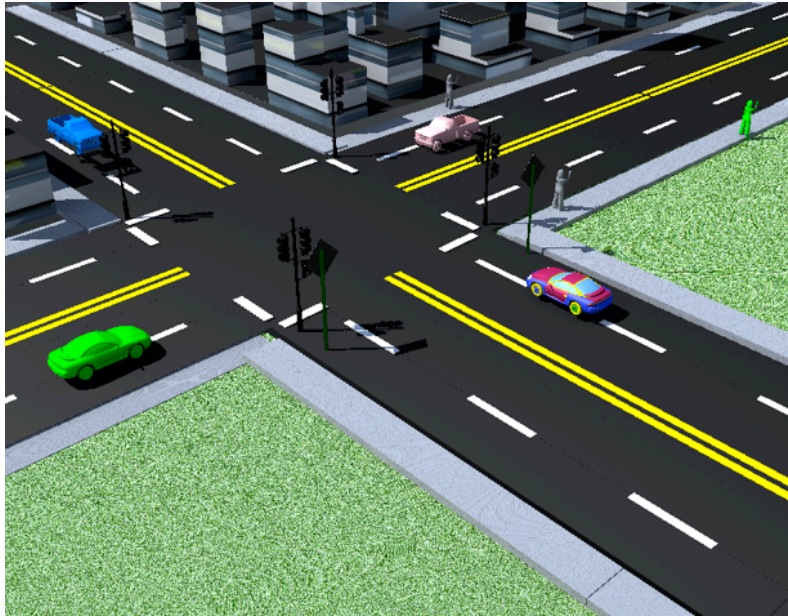
- Crime rate and terror threats require constant surveillance (24 hours a day, 7 days a week)



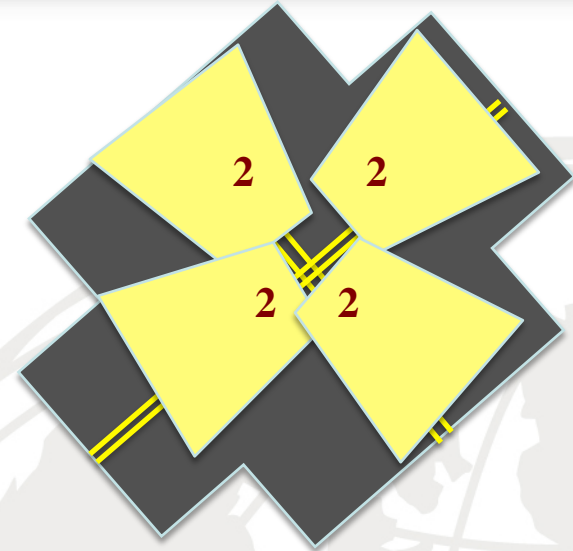




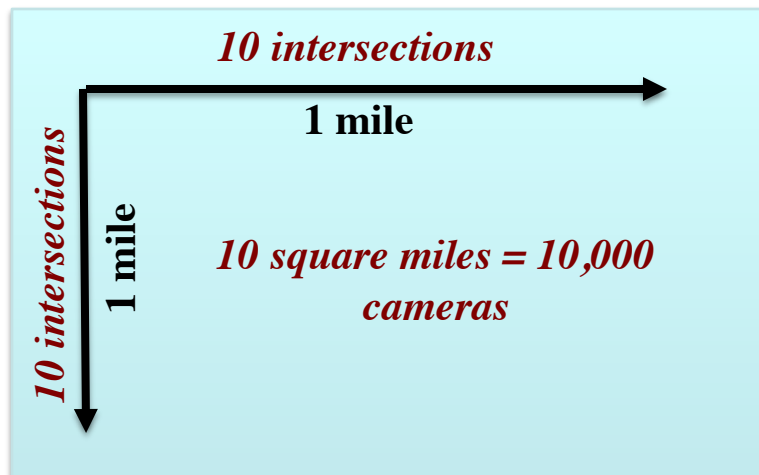
# Example - City



**Intersection – city block every 10<sup>th</sup> mile**



**10 cameras for one intersection (2 cameras looking down each street (day, night) + 2 extra)**



*10 intersections*

**1 mile**

*10 intersections*

**1 mile**

**10 square miles = 10,000 cameras**

**10,000 Displays**



**Good security system**





# Human Factors

**10 square mile = 10,000 Displays**



Visual inspection and ability to perform roles dramatically reduces within a few hours

- Assume one human can look on average 50 cameras (100 at night, 50 during the day)
- 10,000 cameras requires 200 policeman (10,000 = 200 x 50 cameras) constantly (24/7) to monitor **ten square miles** (and these are police not on the streets). Takes more police than patrolling by foot – *went in wrong direction!*

- Continue with automation on each camera – alerting abnormal behavior. Assume 1% of the time a camera may pick up abnormal behavior. Now, only need 2 policeman (24/7) per **10 square miles** (1% of 200 policeman), moderate activity (100 to 1 reduction in police)



# Cost is the Driving Factor!

- Today's world, turn-key system installed is \$20K per camera (without automation)
- When in mass production, with automation, project in future, \$4K per camera.  $10,000 \text{ cameras} \times \$4K = \$40M$
- Amortize over life of 20 years = \$2M/year
- Assume cost of one full-time policeman is \$330K/year (include overhead, department, etc)
- One police on 24/7 = 168 hours
- Assume one human puts in 28 effective hours per week (sick, vacation, holiday, admin, etc)
- $168/28 = 6 \times \$330K = \$1.98M$
- Amortize value of **10 square miles** of a fully automated system cost is equivalent to one 24/7 policeman fulltime



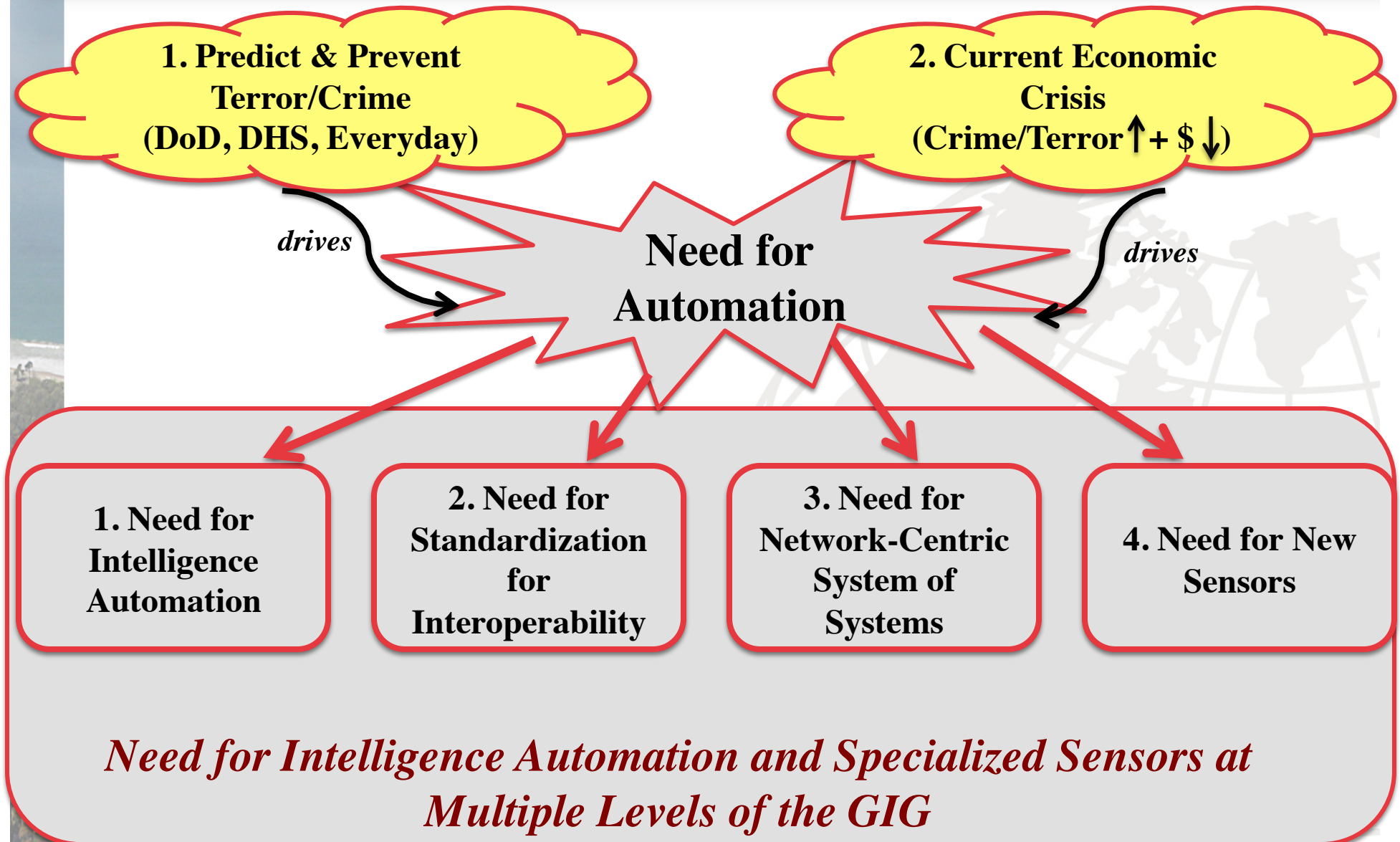
# Cost is the Driving Factor

- Therefore – benefits of having a system automated with full security + cost of one full time policeman
  - Could incorporate traffic and DMV violation automation (system would pay for itself)
- Scale this example to other applications
- For example: Soldiers – around \$1M/soldier in Iraq (include support per soldier)
  - Need for automation





# Need for Intelligence Automation





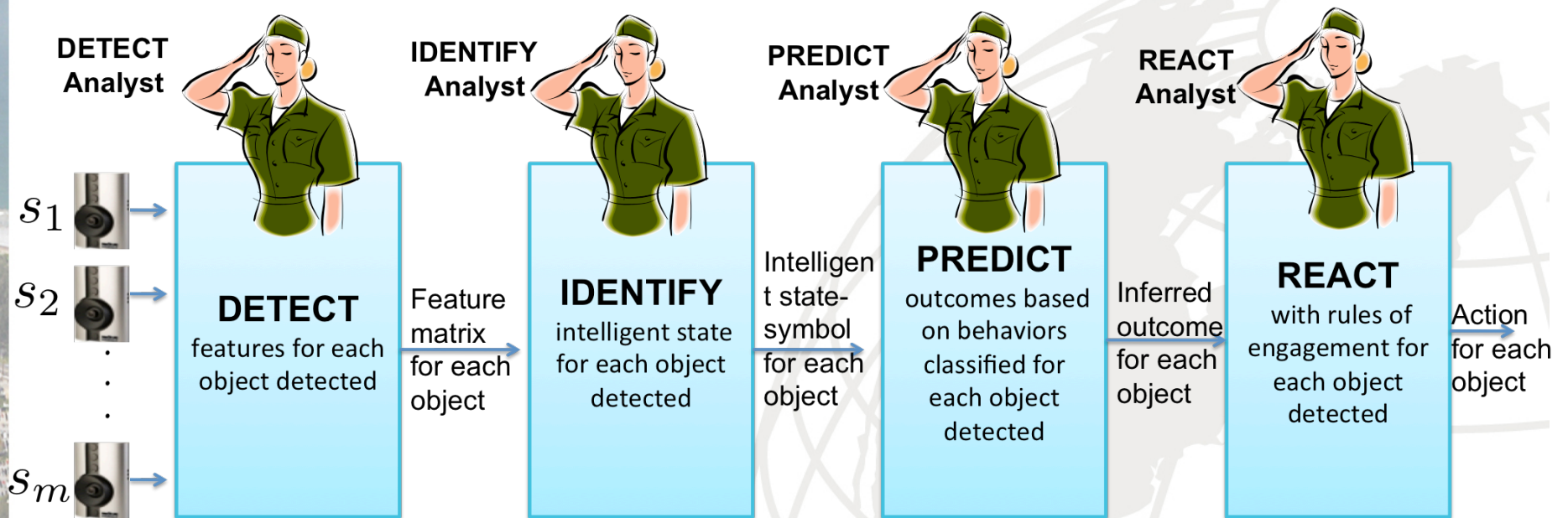
# Network-Centric Warfare/Operations Implementation

- Mission
- Rules of Engagement
- GIG Technologies
- Situational Awareness
- Behavior Modeling
- Behavior Prediction— object and behavior tracking through the GIG
- Extraction of Key Features from Sensor Data
- Sensors to Collect Necessary Data
- Platforms for sensors





# Intelligence Automation = Automating Intelligence Analysts

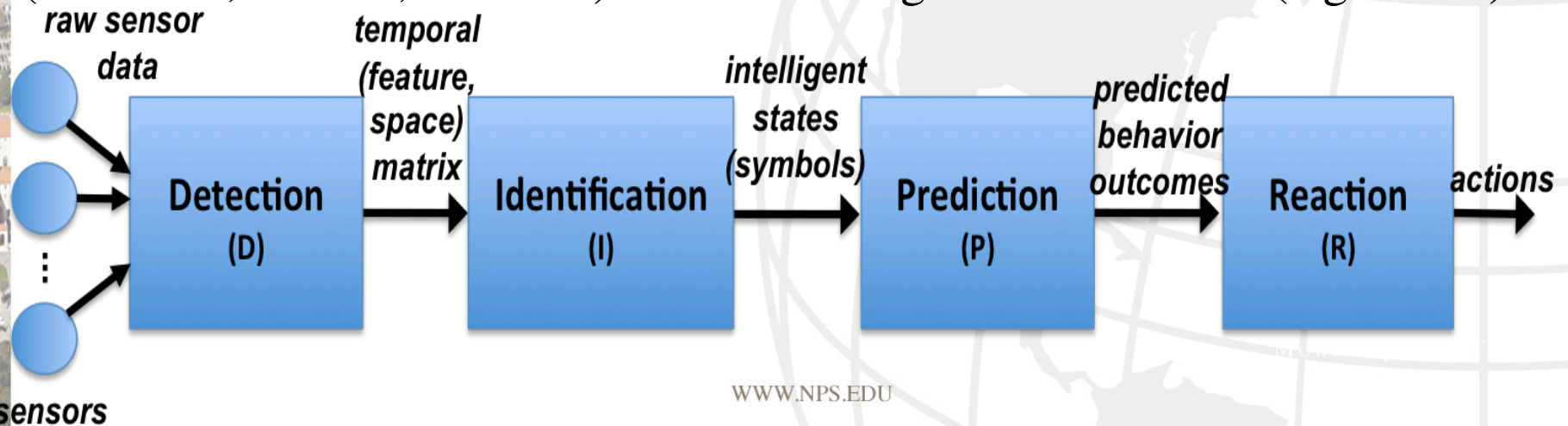


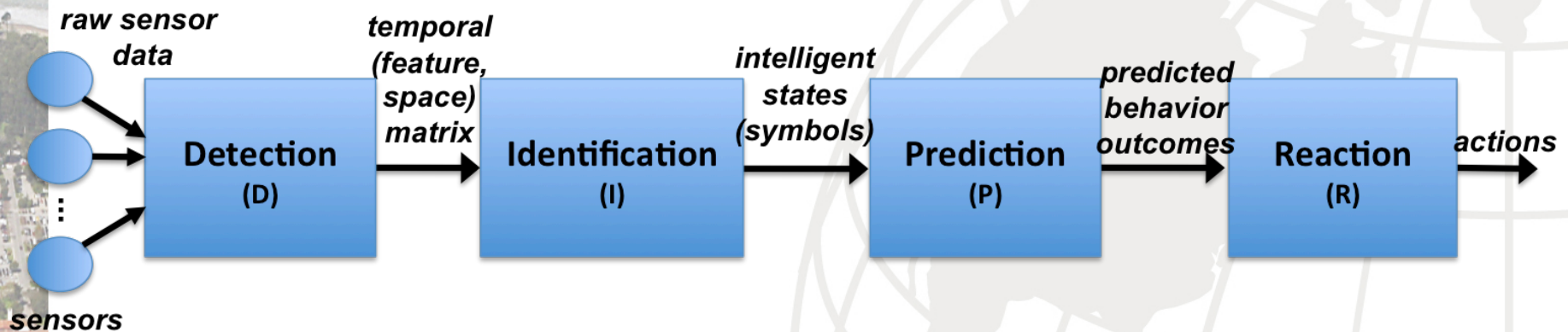




# System of Systems – AI Software using Detect, Identify, Predict, and React (DIPR)

- AI Software SoS is divided into different systems of technologies
- Detection System – objects or events in sensor data (e.g. extract features)
- Identification System – fusion of multiple features to form an intelligent entity
- Prediction System – entity tracking, behavior classification and prediction of events
- Reaction System – action outputs or rules of engagement
- DIPR can be distributed across a network, or loaded into one node of the network. Every sensor network system has two sides: the infrastructure (networks, comms, software) and the intelligence automation (e.g. DIPR)

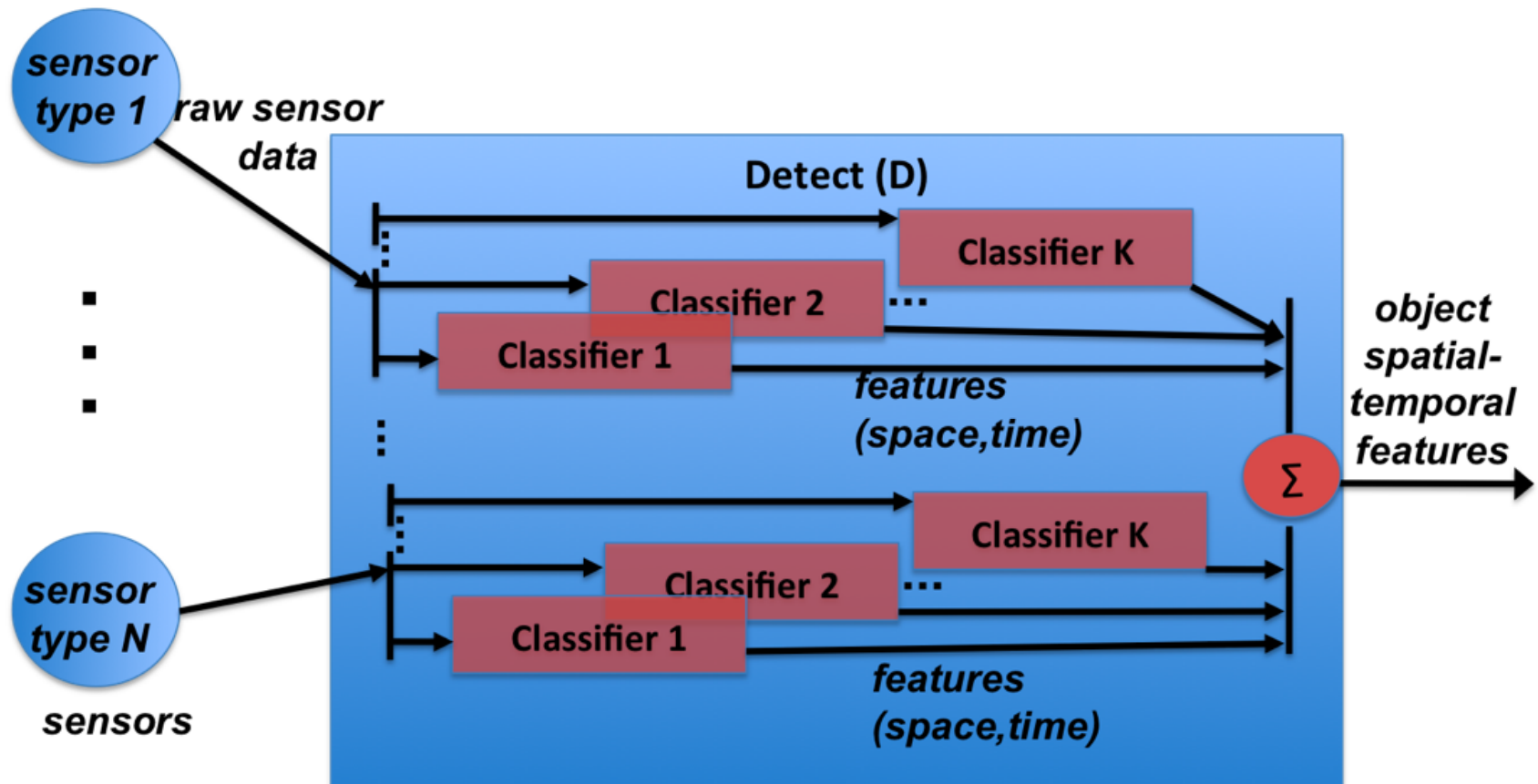




Reference: Rachel E. Goshorn, Deborah E. Goshorn, Joshua L. Goshorn, and Lawrence A. Goshorn  
"Behavior Modeling for Detection, Identification, Prediction, and Reaction (DIPR) in AI Systems Solutions"  
Handbook of Ambient Intelligence and Smart Environments, Springer Handbook (<http://www.springerlink.com/content/n812r0064785g764/>)



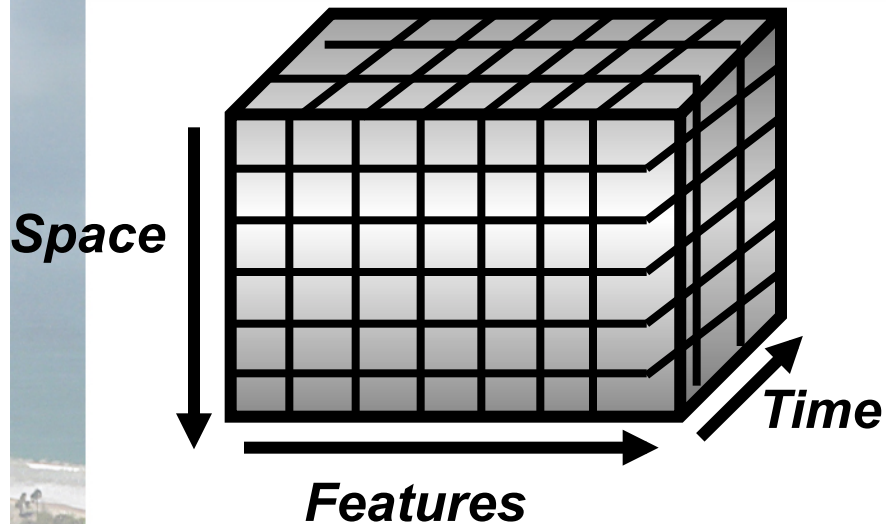
# Detect Subsystem







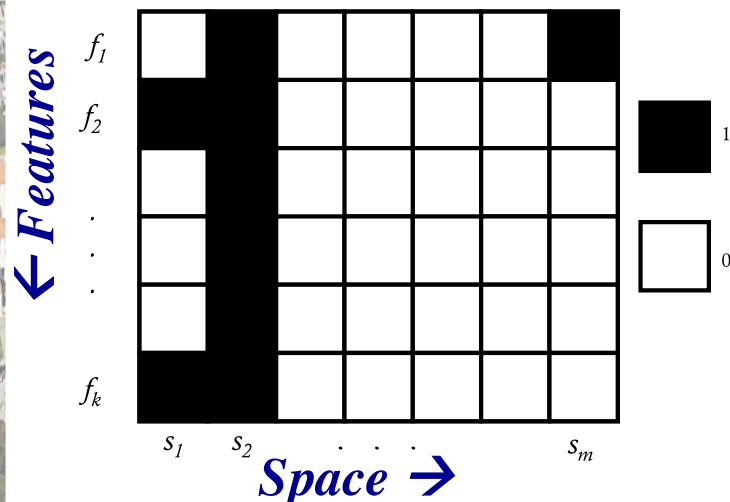
# Output of Detection System



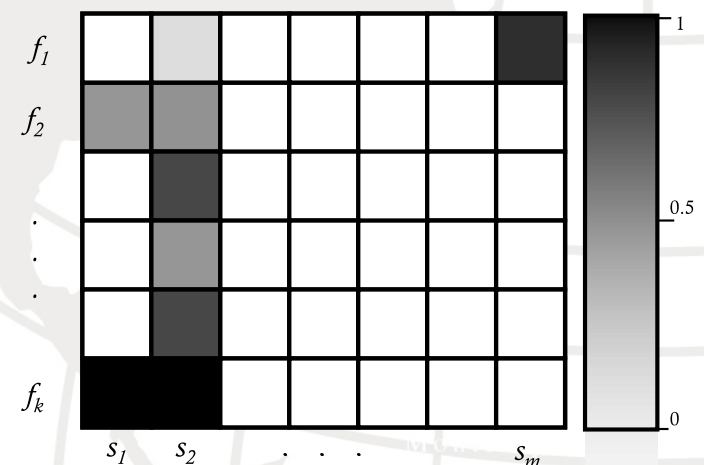
- Low-level classifiers - Output a certain feature, at a certain time, in a certain space
- Either analog or binary
- Used for fusion in Identification System

## *One Slice in Time*

### *Binary Detection Outputs*

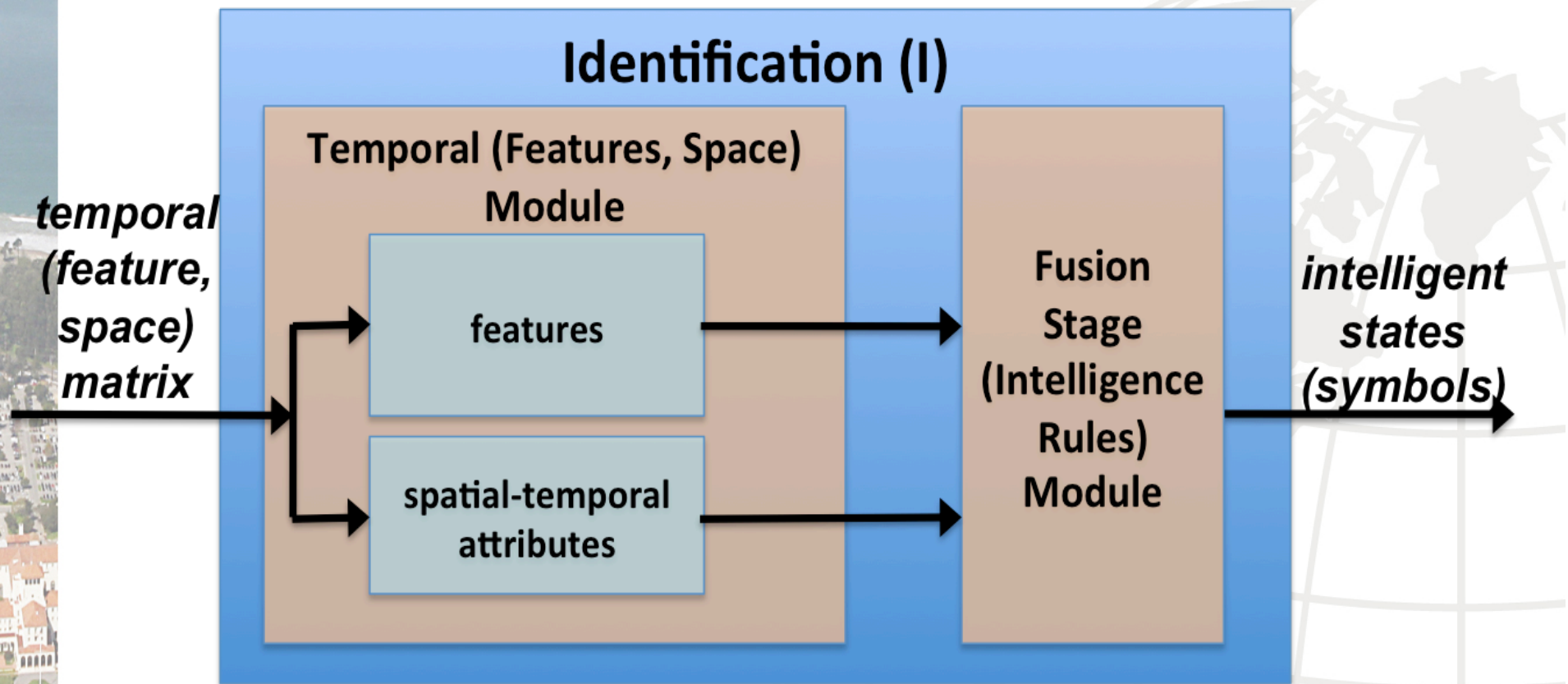


### *Analog Detection Outputs*



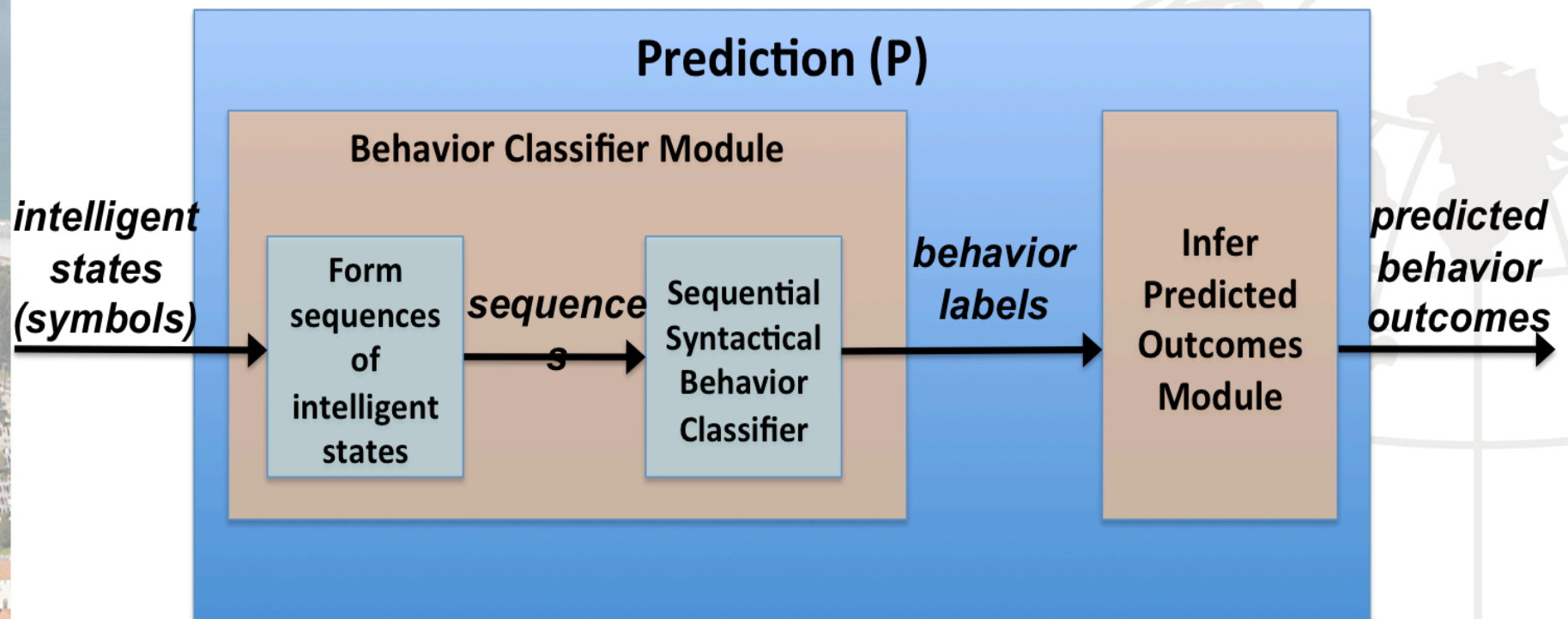


# Identification System



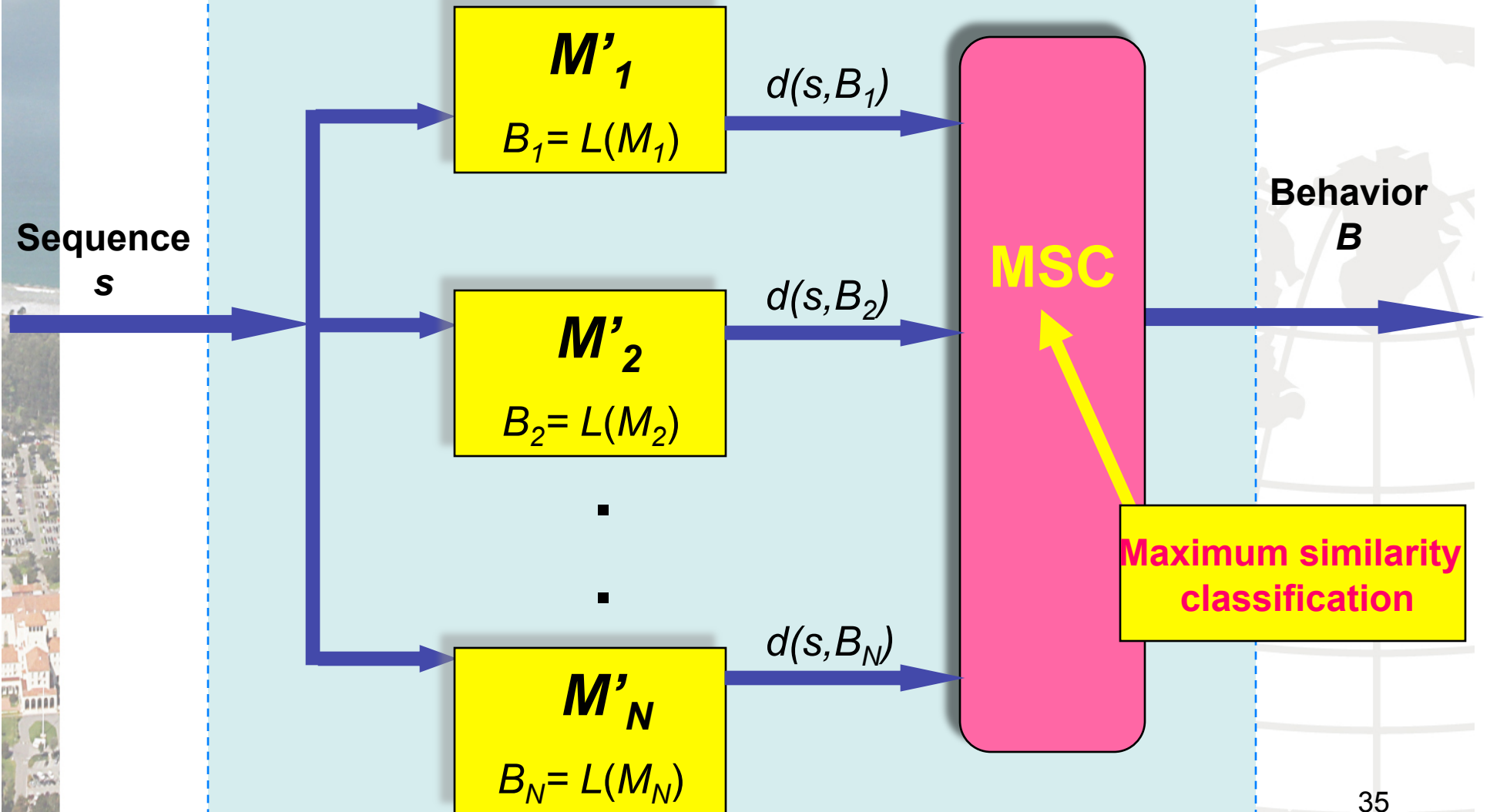


# Prediction System



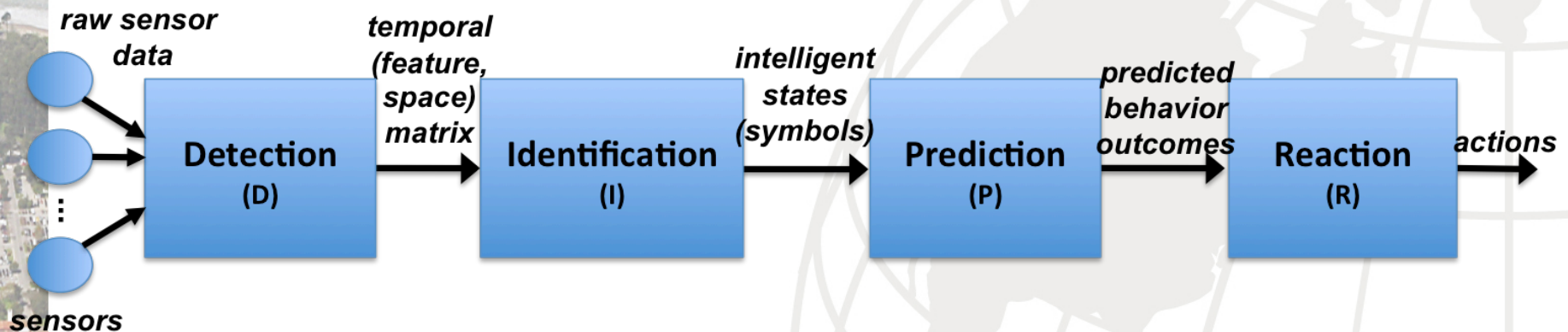


## Sequential-Syntactical Behavior Classifier





# DIPR and Reaction System



Reference: Rachel E. Goshorn, Deborah E. Goshorn, Joshua L. Goshorn, and Lawrence A. Goshorn  
“Behavior Modeling for Detection, Identification, Prediction, and Reaction (DIPR) in AI Systems Solutions”  
Handbook of Ambient Intelligence and Smart Environments, Springer Handbook (<http://www.springerlink.com/content/n812r0064785g764/>)



# Network-Centric Warfare/Operations Implementation

- Mission
- Rules of Engagement
- GIG Technologies
- Situational Awareness
- Behavior Modeling
- Behavior Prediction— object and behavior tracking through the GIG
- Extraction of Key Features from Sensor Data
- Sensors to Collect Necessary Data
- Platforms for sensors



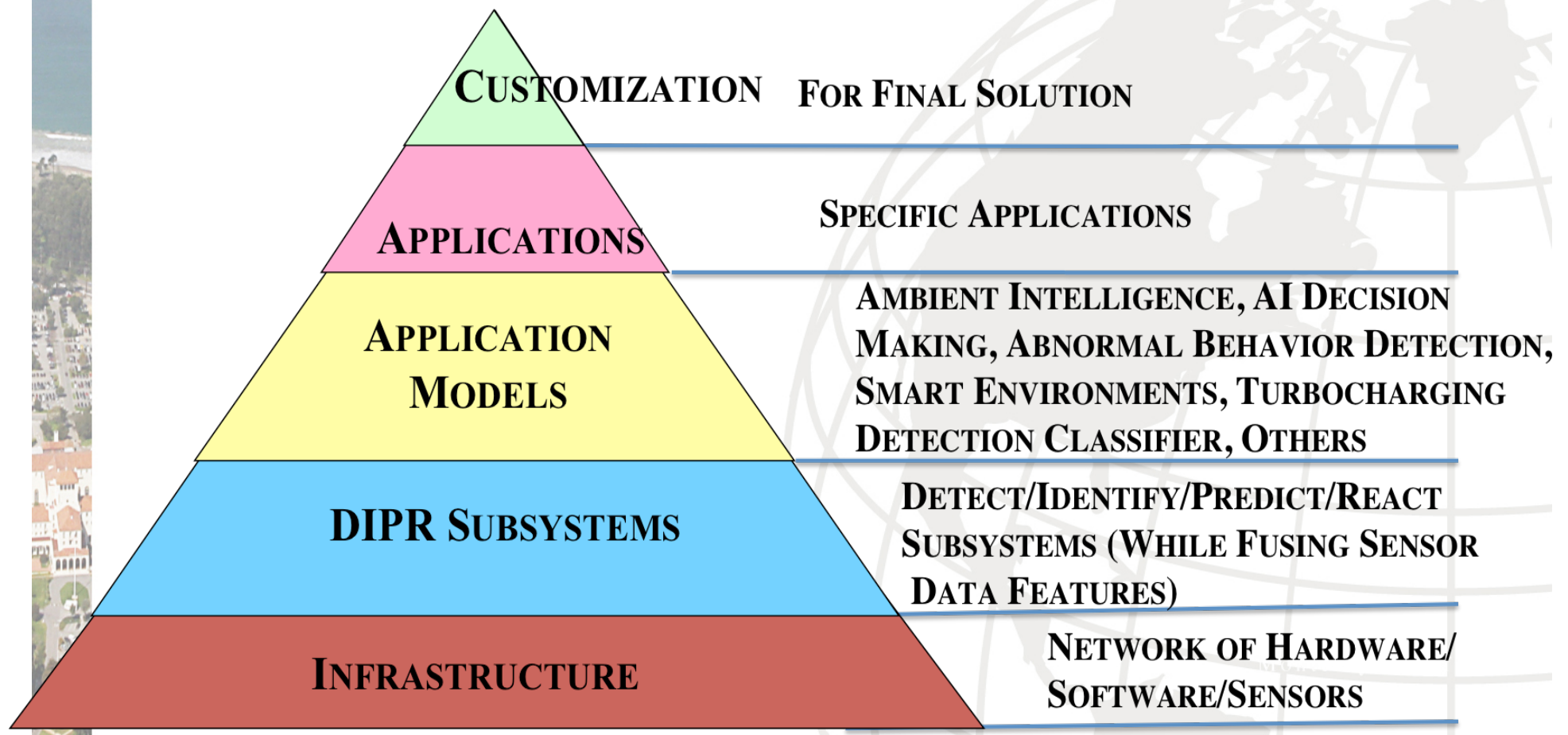




NAVAL  
POSTGRADUATE  
SCHOOL

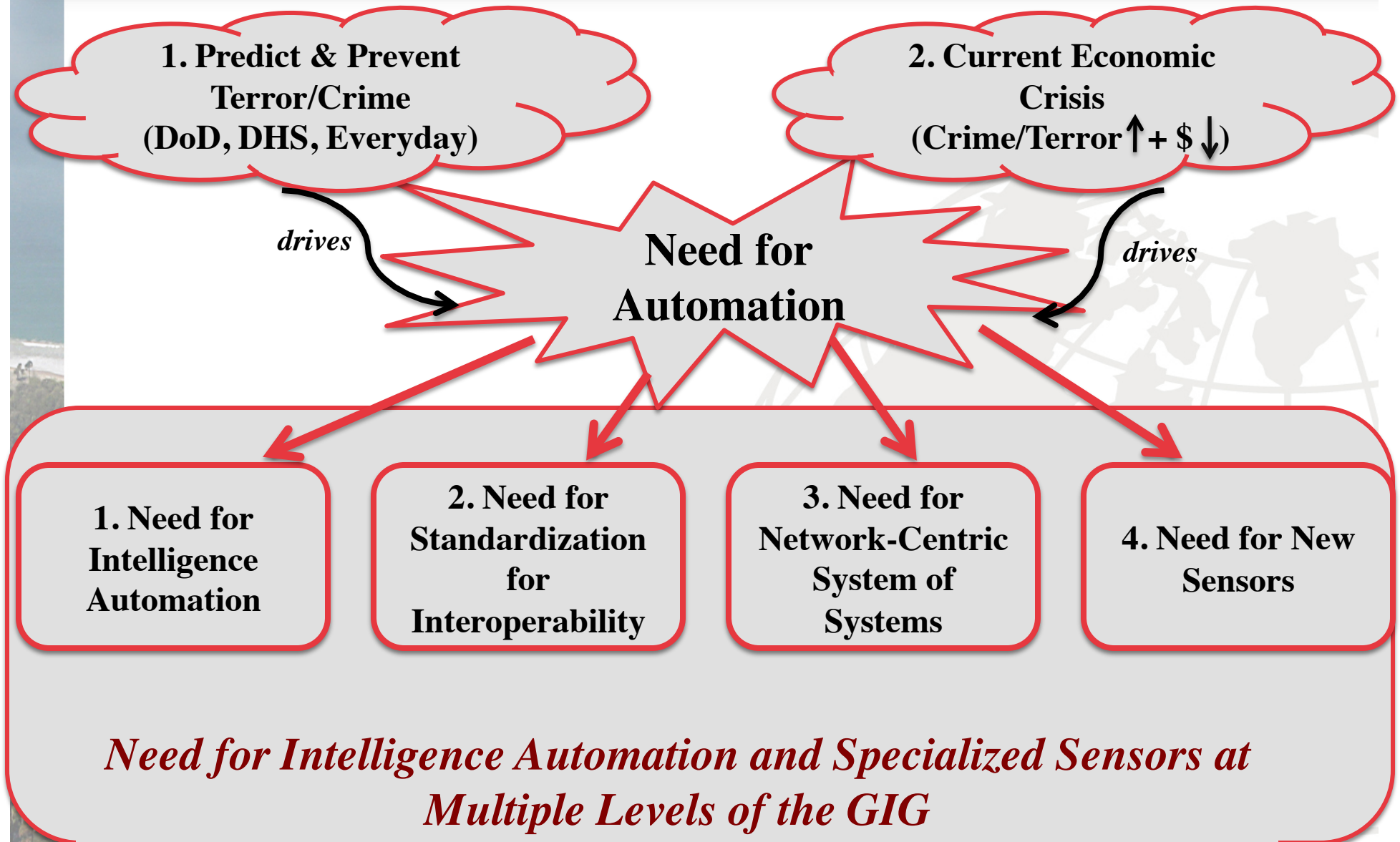
# A Generic Network-Centric SoS for Distributing Intelligence for Fixed and Mobile Nodes

- System of Systems (SoS) Hardware and Software Net-Centric Solution – (each level is a system of the entire Net-Centric Systems Solution)
- **System solution for ground is functionally the same as space**





# Need for Standardization for Interoperability





# Interoperability Standards are Required for Automation

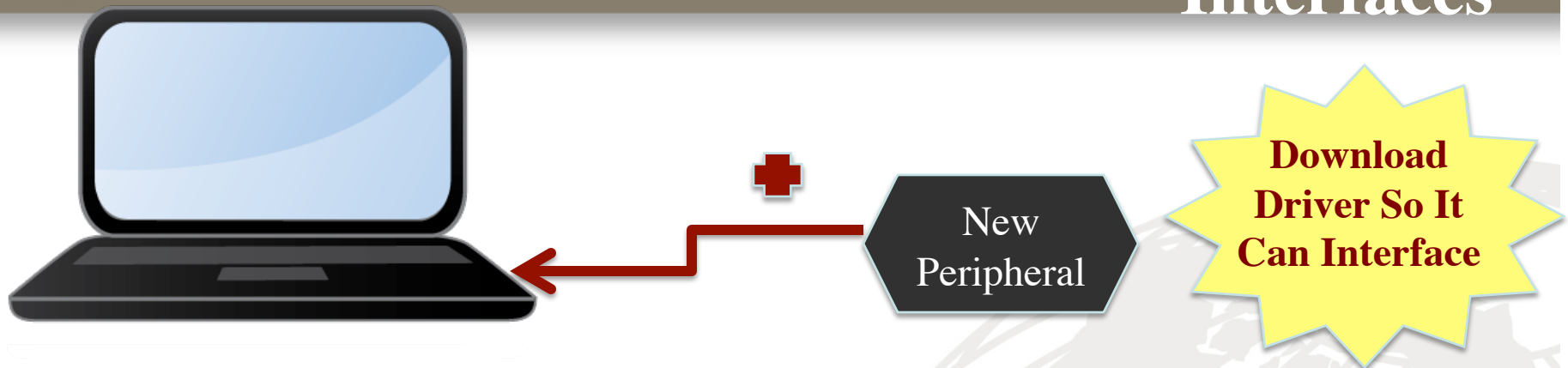
- *Interoperability must be standardized!*
- **Interoperability is broken into two areas:**
  - **Standard Interfaces**
  - **Standard GIG Nodes (Intelligence Automation)**



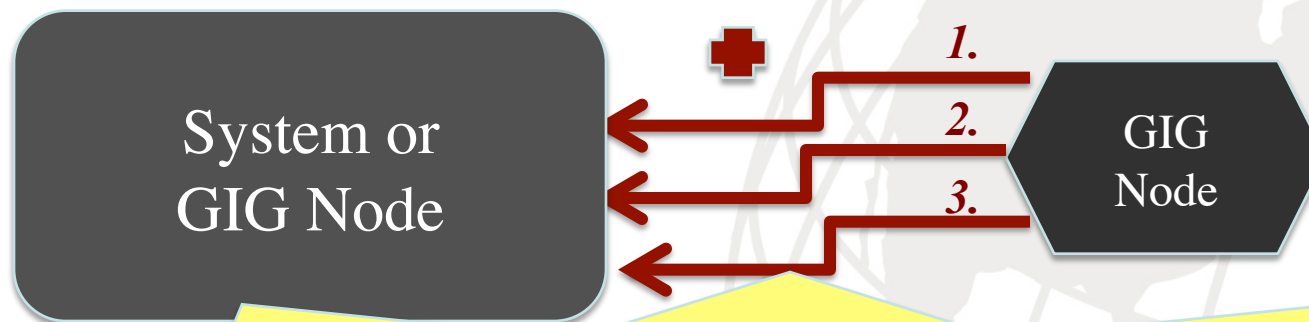


NAVAL  
POSTGRADUATE  
SCHOOL

# Interoperability Standardization of Interfaces



*What is the “driver” for a node, or system (GIG Node), so it can interface with another?*



## Standard Interfaces

1. Define the Intelligence Automation Standards (like outputs of DIPR)
2. Define What Communications Are Allowed
3. Define Allowed Security (Open, NIPRNET, SECRET, TOP-SECRET, etc)



# Intelligence Automation Interface Requirements

- Any interface must define the intelligence automation requirements
- Raw sensor data formats
- Detection Output: standard features (i.e. agreed vocabulary of features), standard temporal parameters, standard spatial parameters
- Identification Output (fused features): symbols (known text symbols)
- Prediction Output: known behavior predictions (library)
- Reaction Output: agreed upon rules of engagement (library)
- Could be in format: text files, XML, binary, etc ...



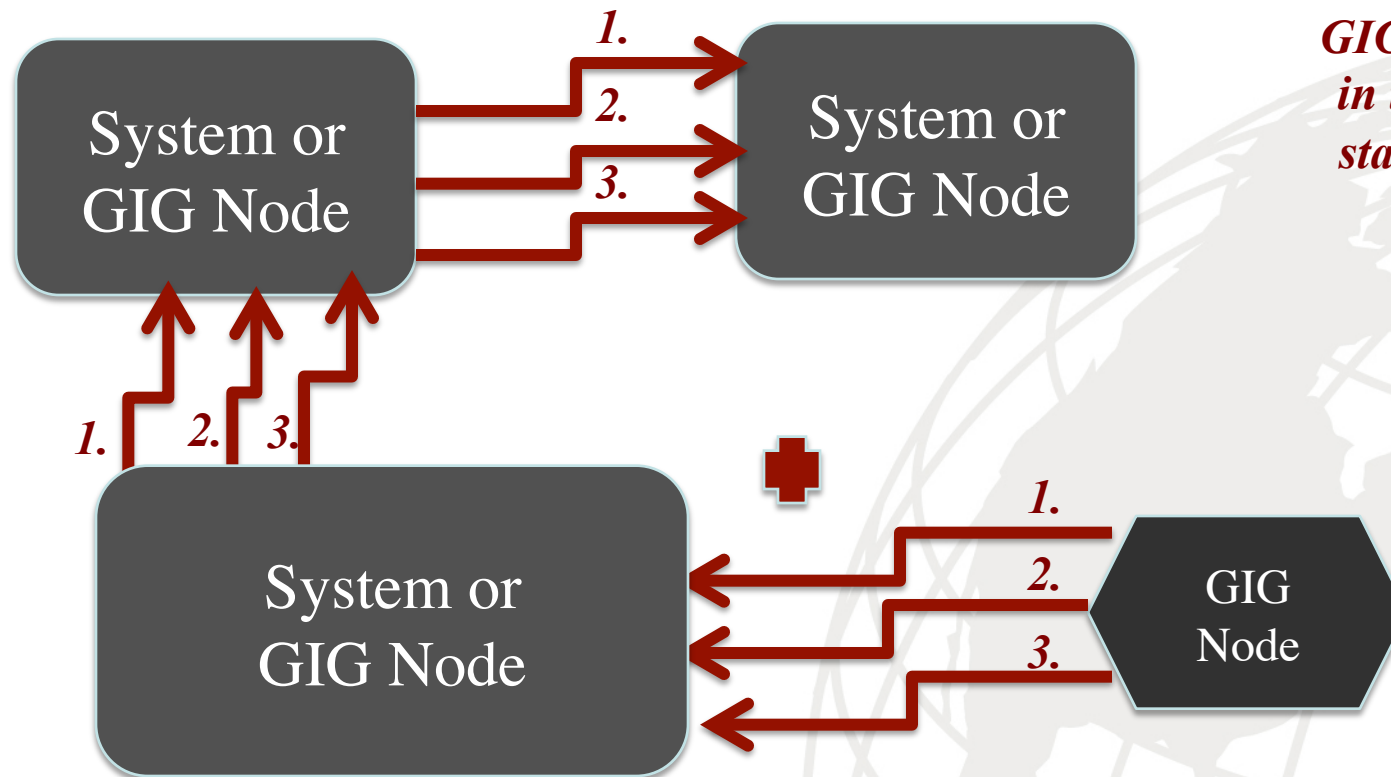
# Communications and Security Interface Requirements

- Agreed upon communication types allowed in the system (802.11, specific SATCOM, etc)
- Agreed upon security types allowed in the system (unclassified, secret, top-secret, etc ...)
- A GIG node can be plugged into the network anywhere, with standard data (DIPR outputs), standard comms, standard security. If the GIG node does not comply to the agreed standards, it will not be able to interface into the network.





# Interoperability Standardization of Interfaces



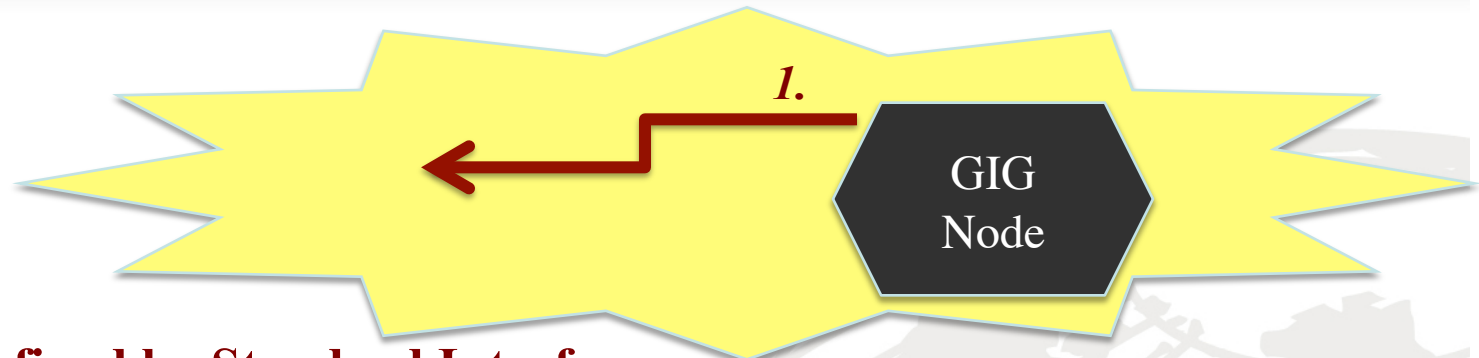
*Can plug and play  
GIG nodes anywhere  
in the network with  
standard interfaces  
defined*

## Standard Interfaces

1. Define the Intelligence Automation Standards (like outputs of DIPR)
2. Define What Communications Are Allowed
3. Define Allowed Security (Open, NIPRNET, SECRET, TOP-SECRET, etc)



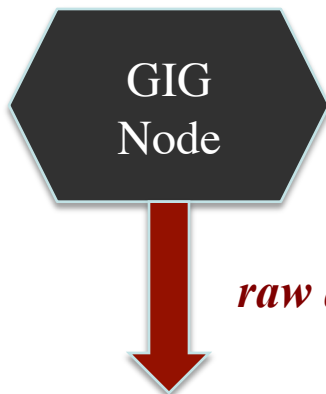
# Interoperability Standardization of Building Blocks – GIG Nodes



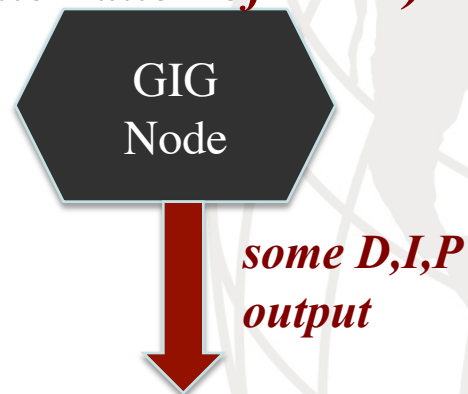
## GIG Node Defined by Standard Interface:

### 1. Define the Intelligence Automation Standards (outputs of DIPR)

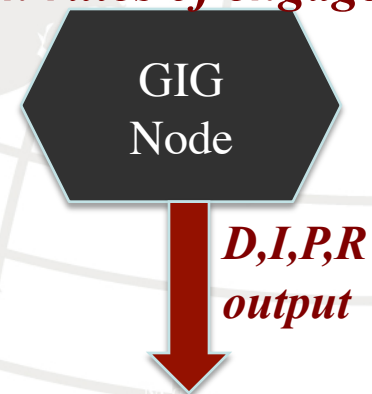
*Class 1: Dumb  
(pass raw data)*



*Class 2: Intelligent  
(some form of  
automation of DIPR)*



*Class 3: Stand Alone  
(with rules of engagement)*



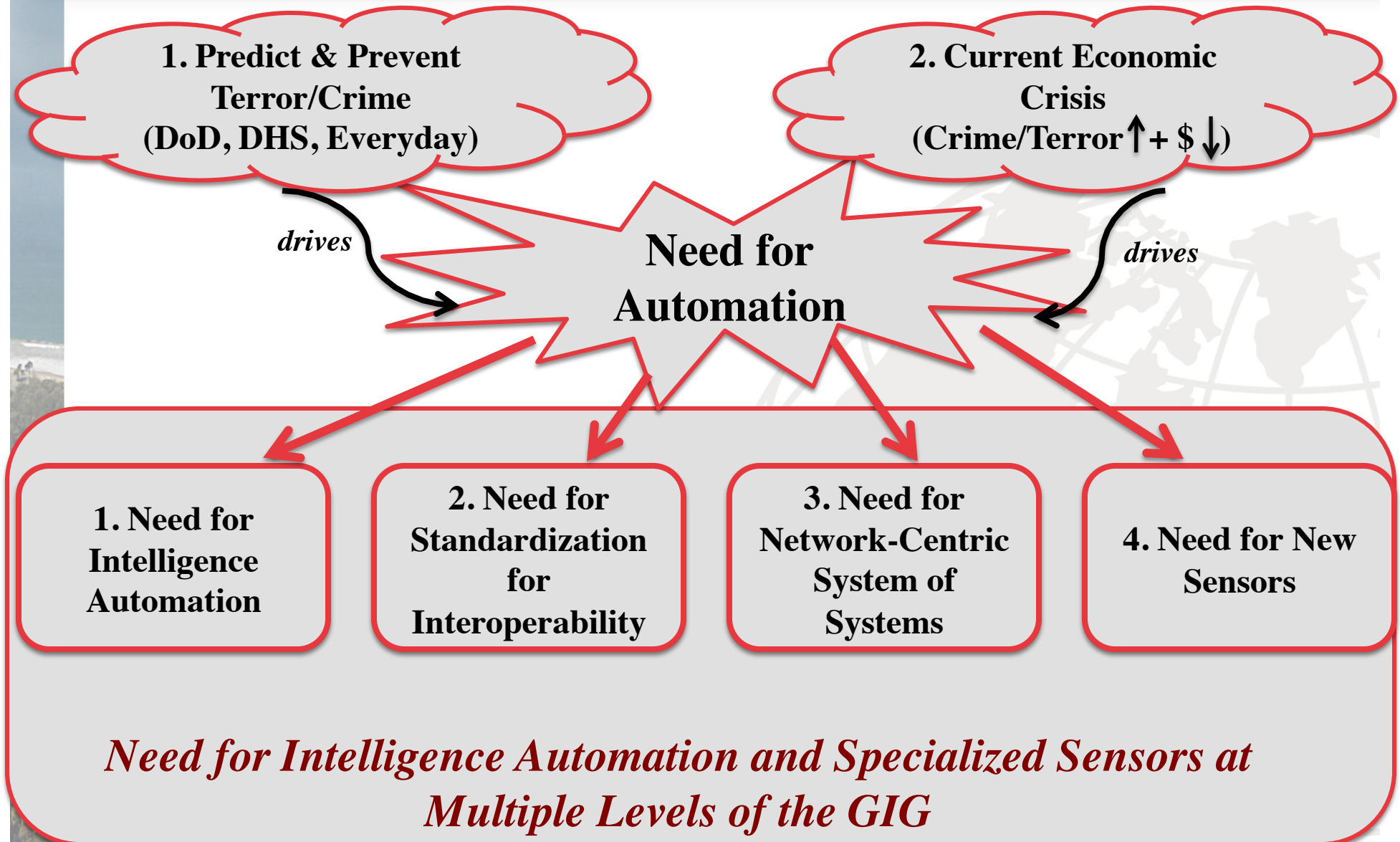


# Interoperability Standards are Required for Automation

- *Interoperability must be standardized!*
- **Interoperability is broken into two areas:**
  - **Standard Interfaces**
    - 1. Intelligence Automation
    - 2. Communications Requirements
    - 3. Security
  - **Standard GIG Nodes**
    - 1. Dumb (pass raw data)
    - 2. Intelligent (some form of automation)
    - 3. Stand Alone (with rules of engagement)



# Need for Network-Centric System of Systems Infrastructure







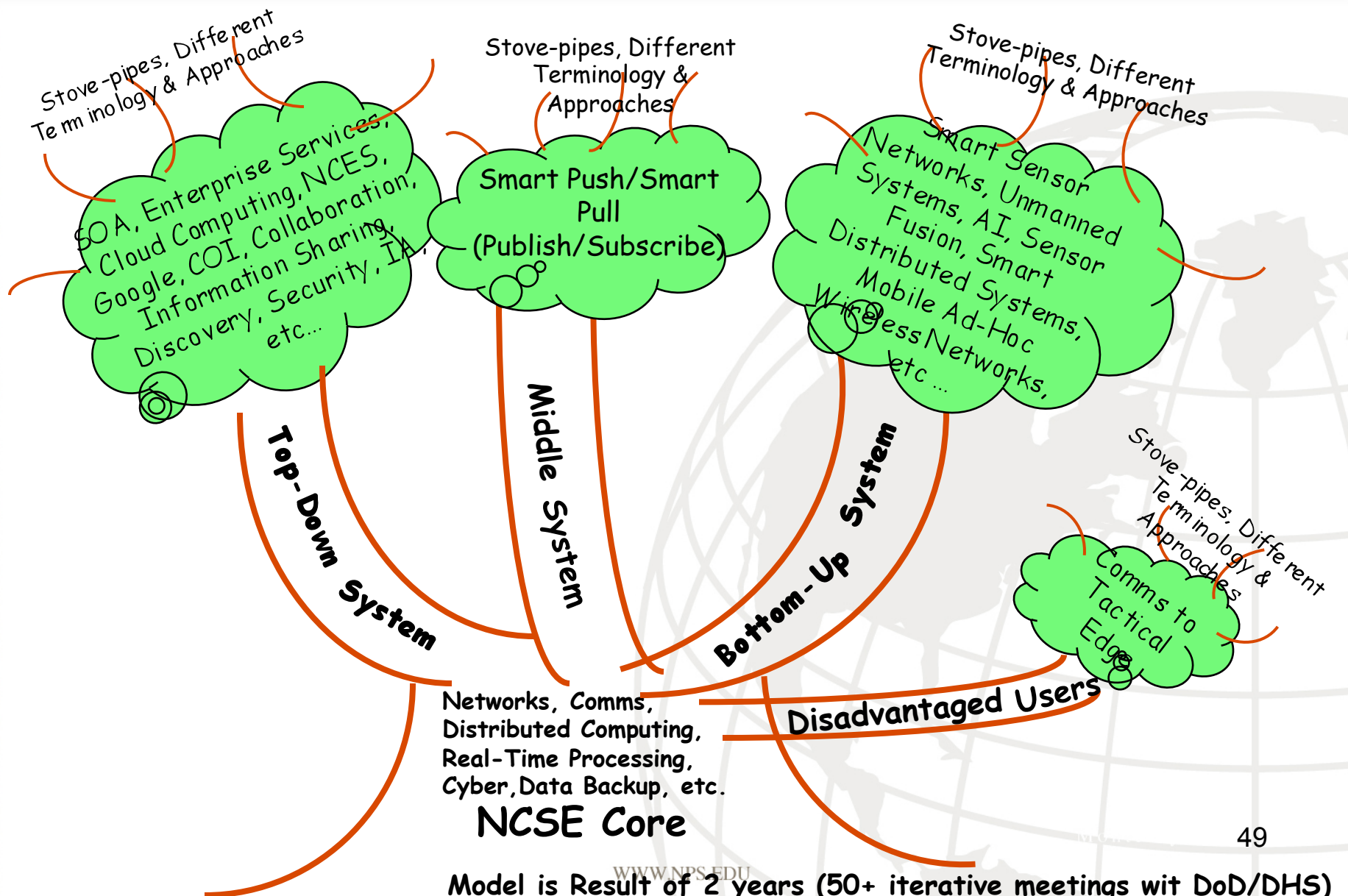
# Network-Centric Warfare/Operations Implementation

- Mission
- Rules of Engagement
- GIG Technologies
- Situational Awareness
- Behavior Modeling
- Behavior Prediction— object and behavior tracking through the GIG
- Extraction of Key Features from Sensor Data
- Sensors to Collect Necessary Data
- Platforms for sensors



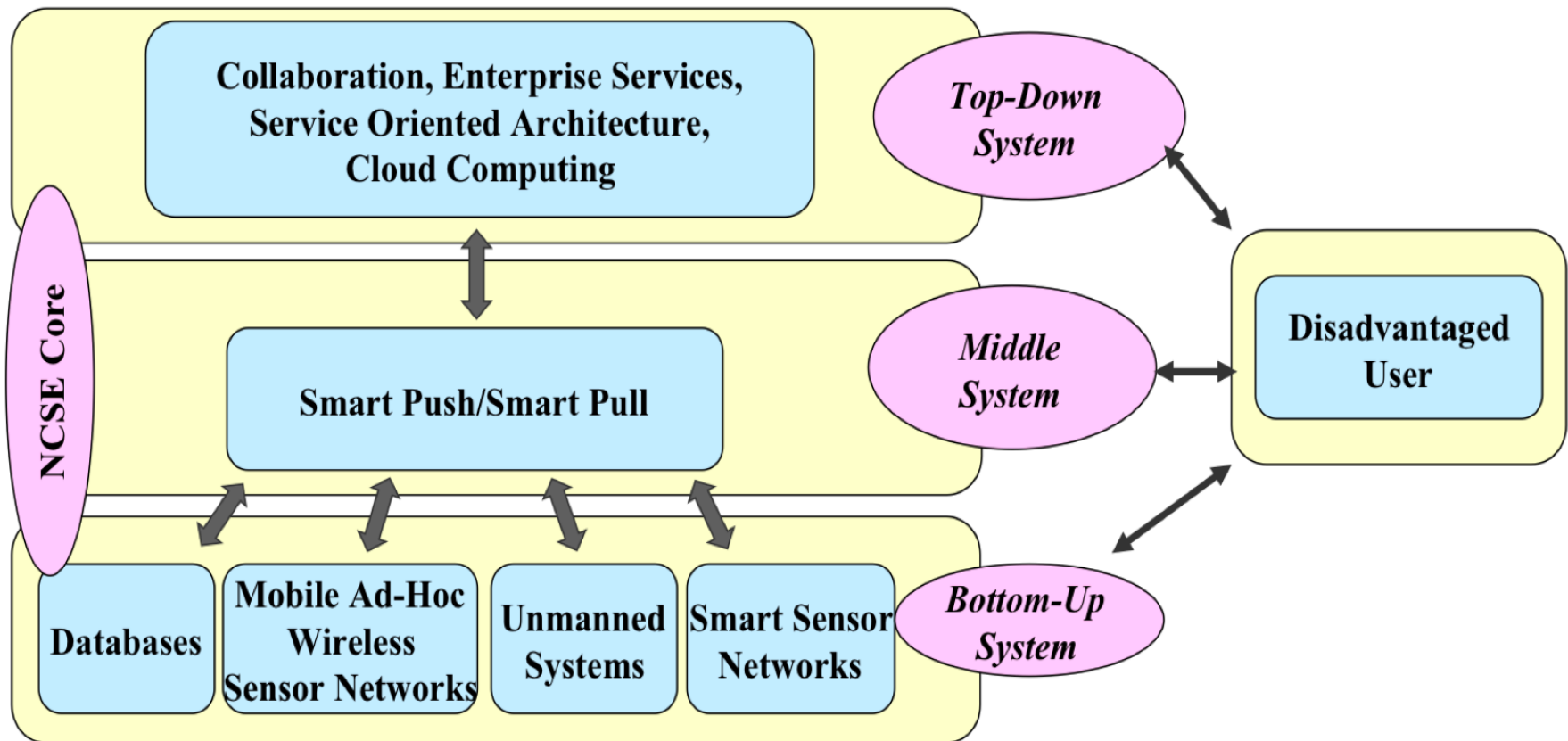


# Network-Centric Systems Engineering Generic Model





# Network-Centric Systems Engineering





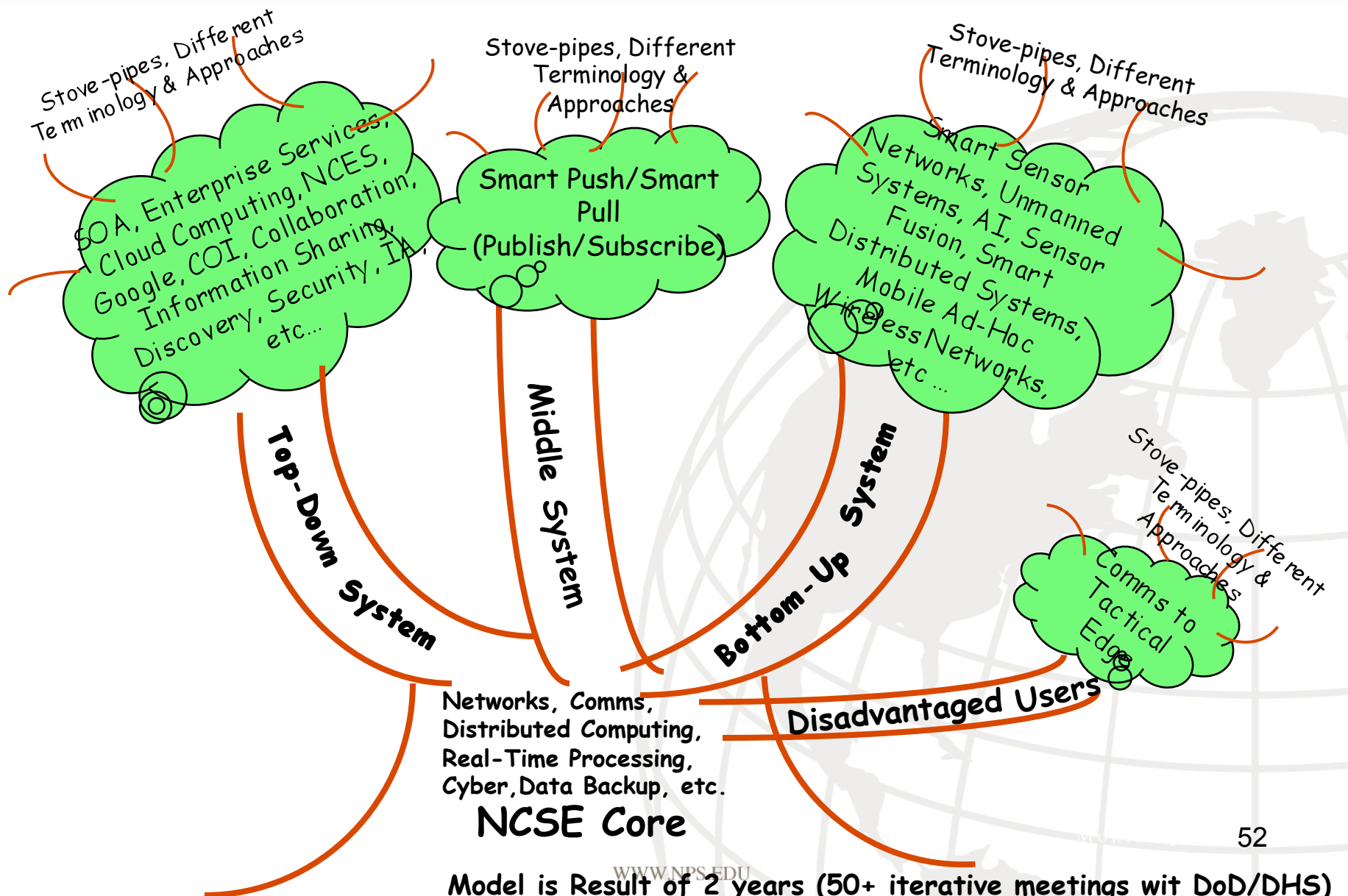
# Network-Centric System's Approach Required (Sharing Sensor Data)

- Bottom-Up System: origination of data
- All information needs to be shared (through a “smart push”) from a “bottom-up” approach (from sensors, humans, nodes, GIG Nodes, etc), to a top-down approach of collaboration (through a service oriented architecture with “smart push/smart pull”).
- Once sensors are selected, and formed into a GIG node, GIG nodes should be categorized into standard formats: dumb (passing information), intelligent (automation of some form), and stand alone with rules of engagement to take action.
- Interfaces need to be standardized – intelligence automation (DIPR)





# Network-Centric Systems Engineering Generic Model



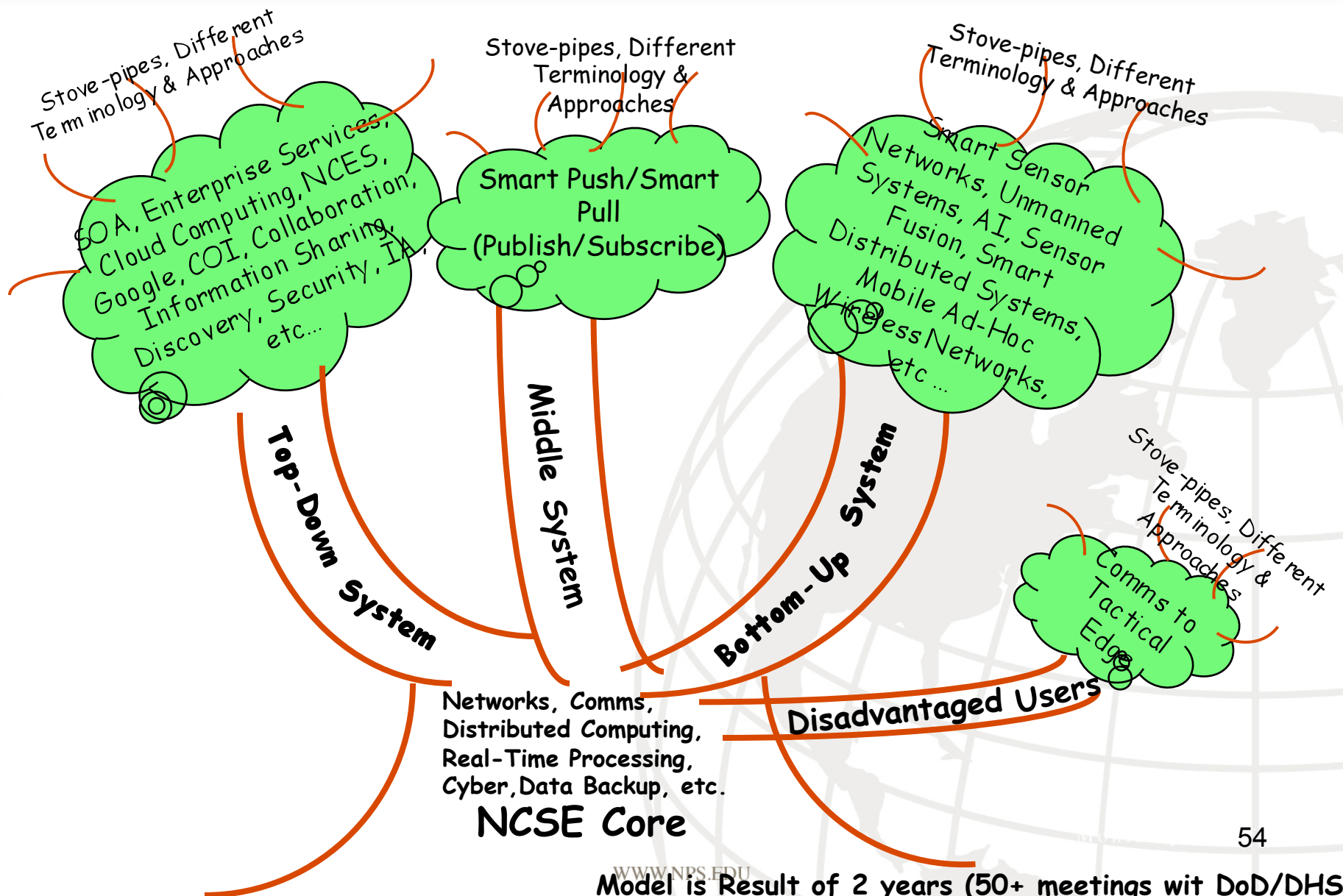


# Network-Centric System's Approach Required (Operator Interface to Intelligence)

- This enterprise and collaboration level must automate the information into the highest level of intelligence for the mission and user.
- The infrastructure of information sharing for threat predictions and preventions, must ride on a SOA/ Cloud infrastructure, where the analyst has control over the necessary intelligence (e.g. request behaviors, reactions, features, sensors from a “smart pull” and automate the “smart push” from the sensors, nodes, etc.), and must allow for potential “disadvantaged users” to “plug and play”.



# Network-Centric Systems Engineering Generic Model





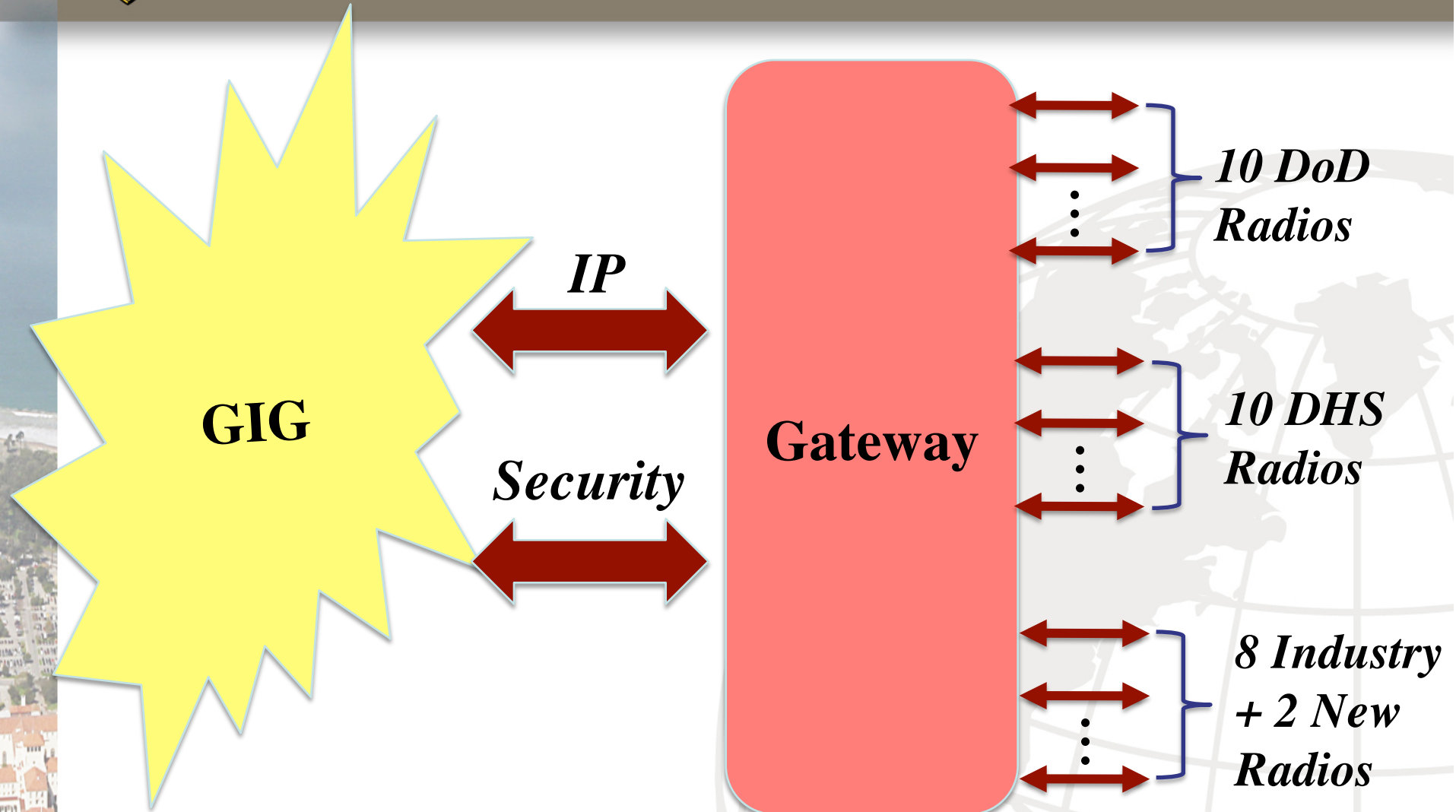
# Information from the “Tactical Edge”

- Additionally, in the GIG infrastructure, GIG nodes may be a “disadvantaged user”, a node with critical information to share, but a “disadvantaged” communications pipe (i.e. limited bandwidth/communications, limited security, stealth requirements, etc).
- Ensuring this information is pushed to the person/center of interest, is critical for GWOT and HLS threat prevention.
- Various communications architectures could be designed for “plug and play” for standardizing disadvantaged user interfaces.





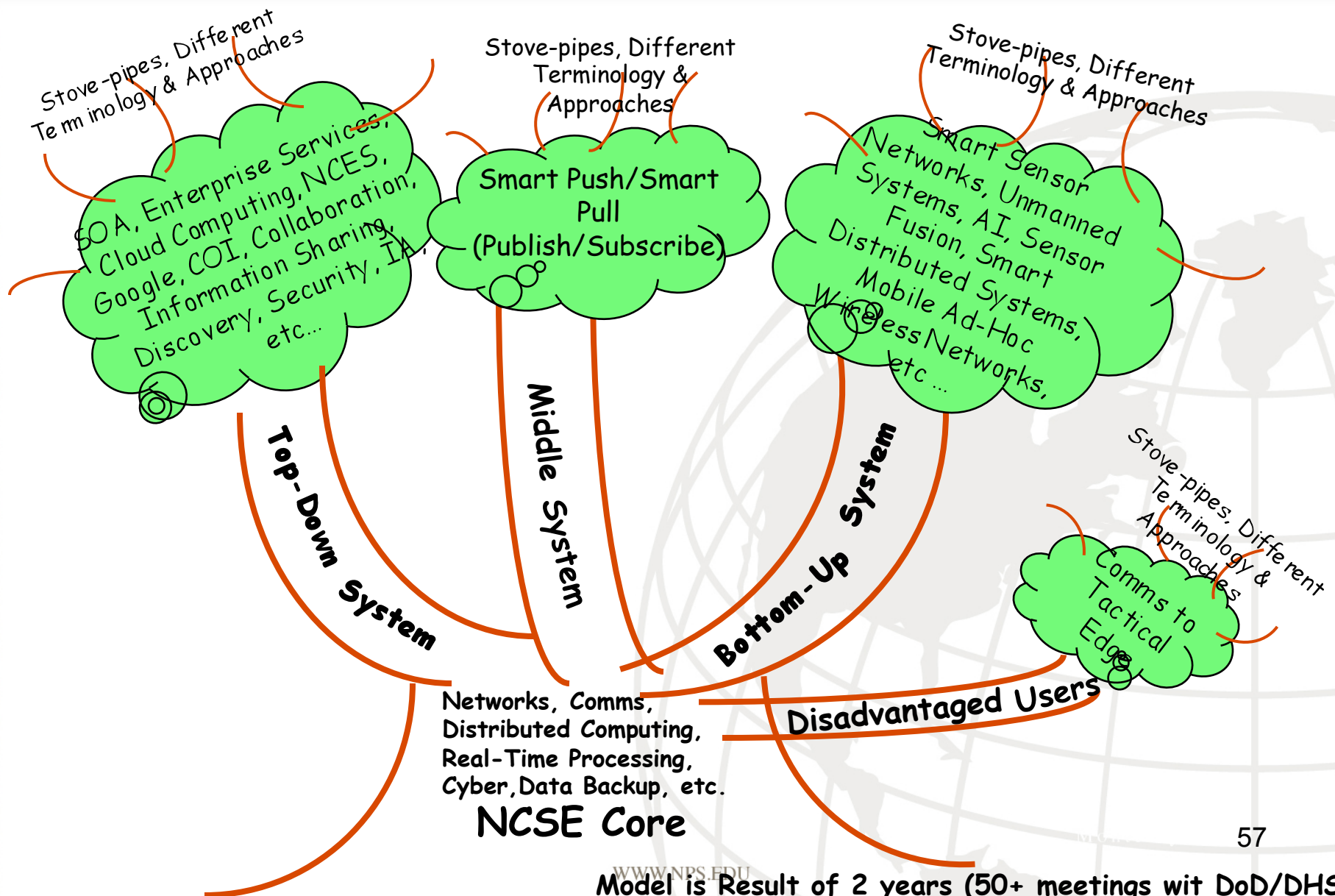
# Potential Disadvantaged User Solution



*Put gateways in area of operations to handle most disadvantaged users.  
Gateway transfer signals to/from IP and to/from security requirements.*



# Network-Centric Systems Engineering Generic Model

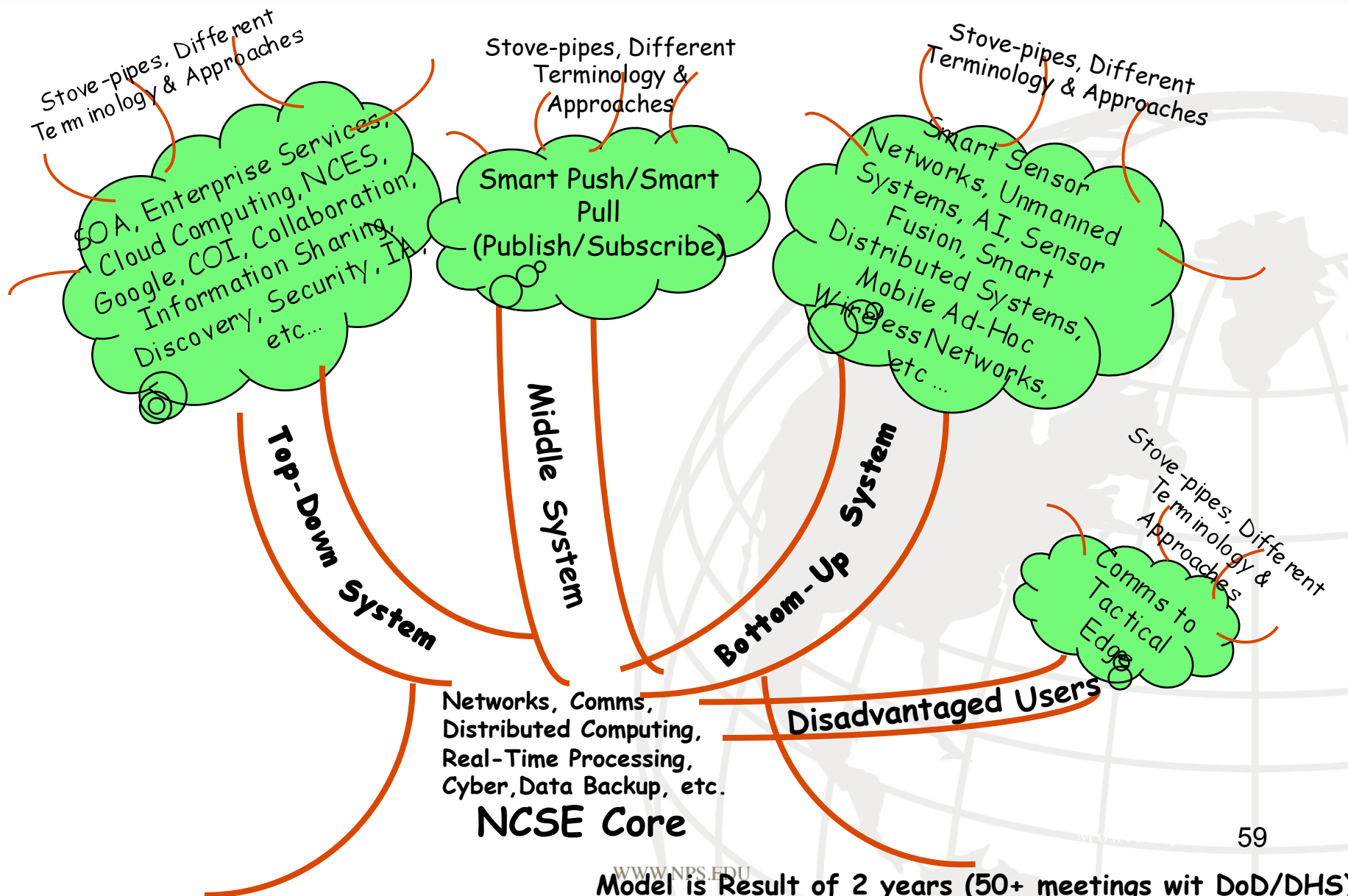




- NCSE CORE Integrates Four Systems (Top-Down, Middle, Bottom-Up, Disadvantaged Users)
  - Networks
  - Communications
  - Distributed Computing
  - Real-Time Processing
  - Cyber Security
  - Data Backup – Where is the data stored??
    - Need back-ups
  - etc.



# Network-Centric Systems Engineering Generic Model







Sensor networks, network-centric systems, existing networks (power grid), etc ...

## Cyber Security - Growing Threats!

Superimpose automated cyber security onto network-centric systems (e.g. using DIPR mindset – it has to be automated and go through the behavior prediction and reaction stages!)

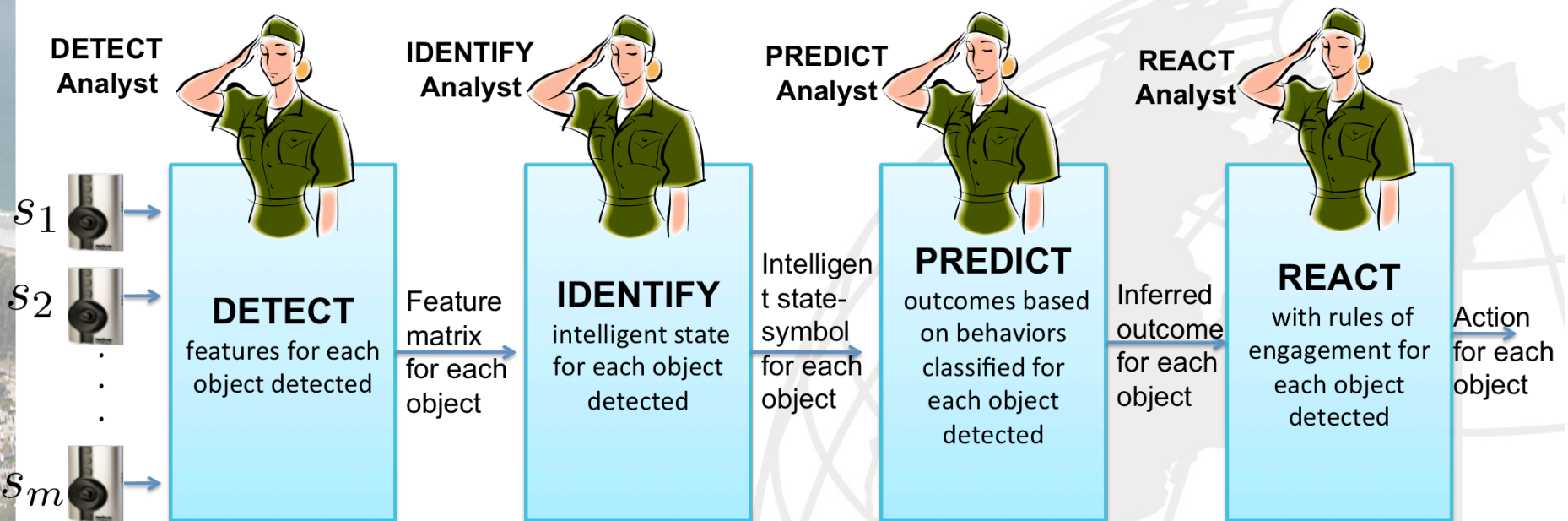


- Intelligence automation framework to automate “cybersecurity experts” to maintain a secure SoS and prevent potential cyber attacks.
- This intelligence automation framework can be used for securing a smart sensor network SoS, through automating feature extractions, fusions, classifying and predicting behaviors, and recommending and automating reactions.
- In addition, the same intelligence automation framework can be used to automate “cyber warfare experts” to infiltrate and take-down an enemy network SoS.

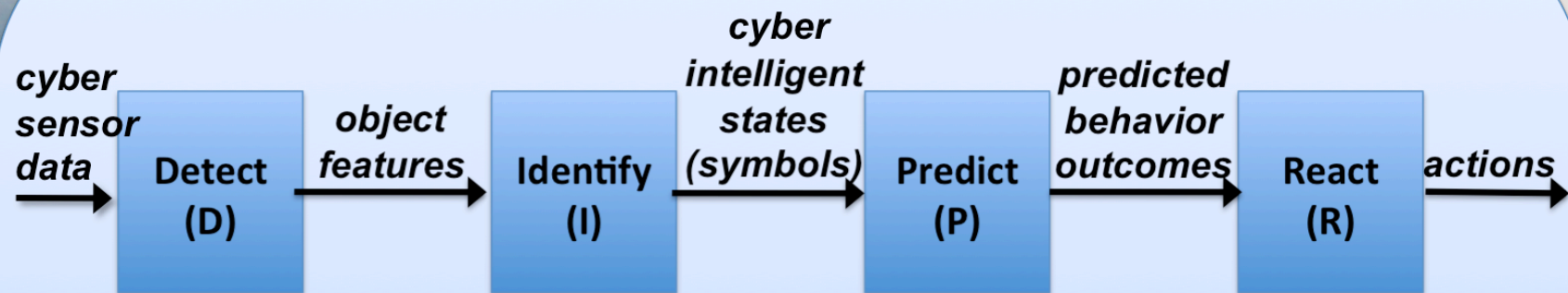


NAVAL  
POSTGRADUATE  
SCHOOL

# The Future of Cybersecurity and Cyber Warfare is Intelligence Automation, Automating Cyber Analysts.



Automating cyber analysts includes the automation of learning new enemy tactics, techniques, and procedures (TTPs).



- **Detect** - Detect features characteristic to cyber attacks, which involves assigning feature extraction algorithms to all possible sensors so that at any time unit, the presence (or absence of) of all desired features will be detected from the cyber sensor data.
- **Identify** – Identify the current intelligent cyber state of the network by fusing multiple detected cyber attack spatial-temporal features at one time.
- **Predict** – Predict an oncoming cyber attack using sequential syntactical behavior classifiers for classifying sequences of intelligent states of the cyber network into predefined cyber network behaviors, including abnormal cyber network behaviors.
- **React** – React by executing rules of engagement actions for preventing predicted cyber attack.

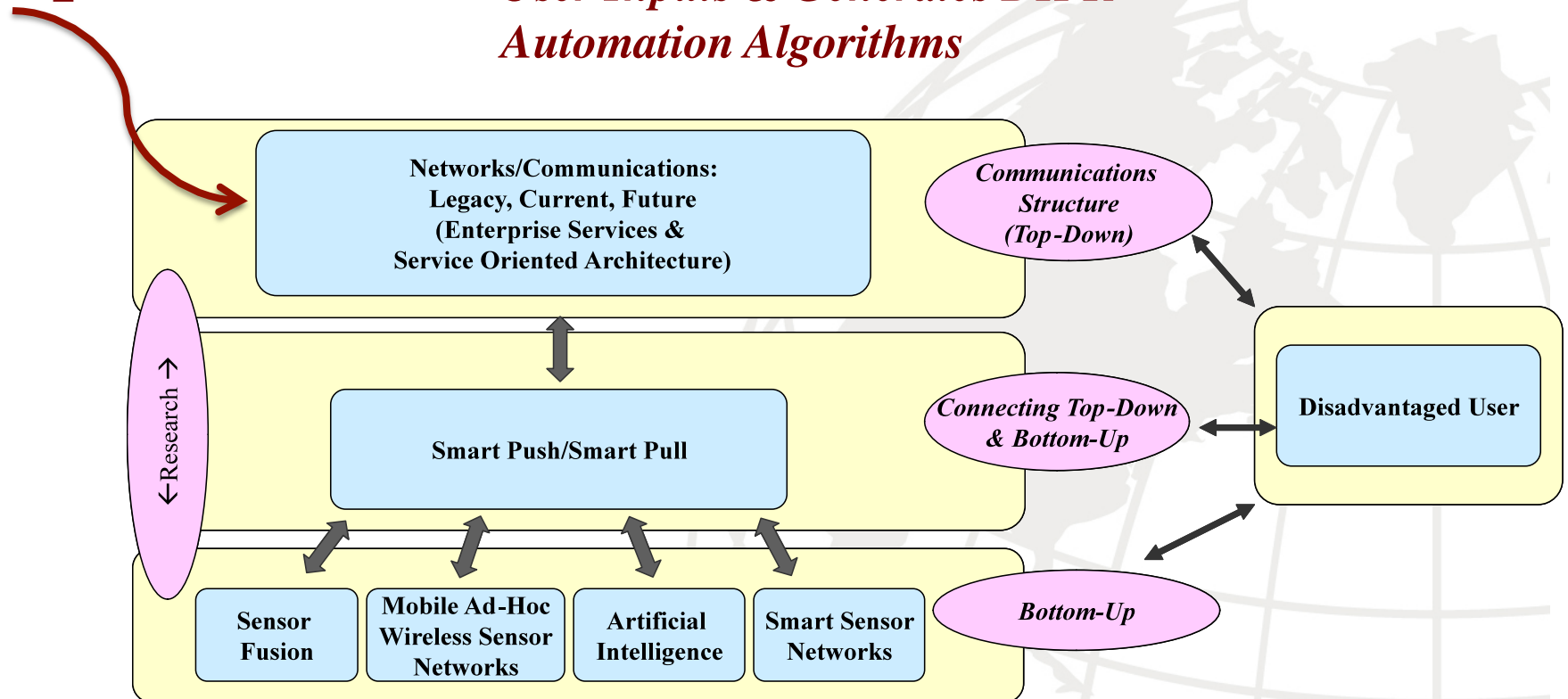




# **New Graphical User Interfaces (GUI's) Required at the Enterprise Level (Top-Down System)**

# New Graphical User Interfaces (GUI's) Required

*User Inputs & Generates DIPR  
Automation Algorithms*

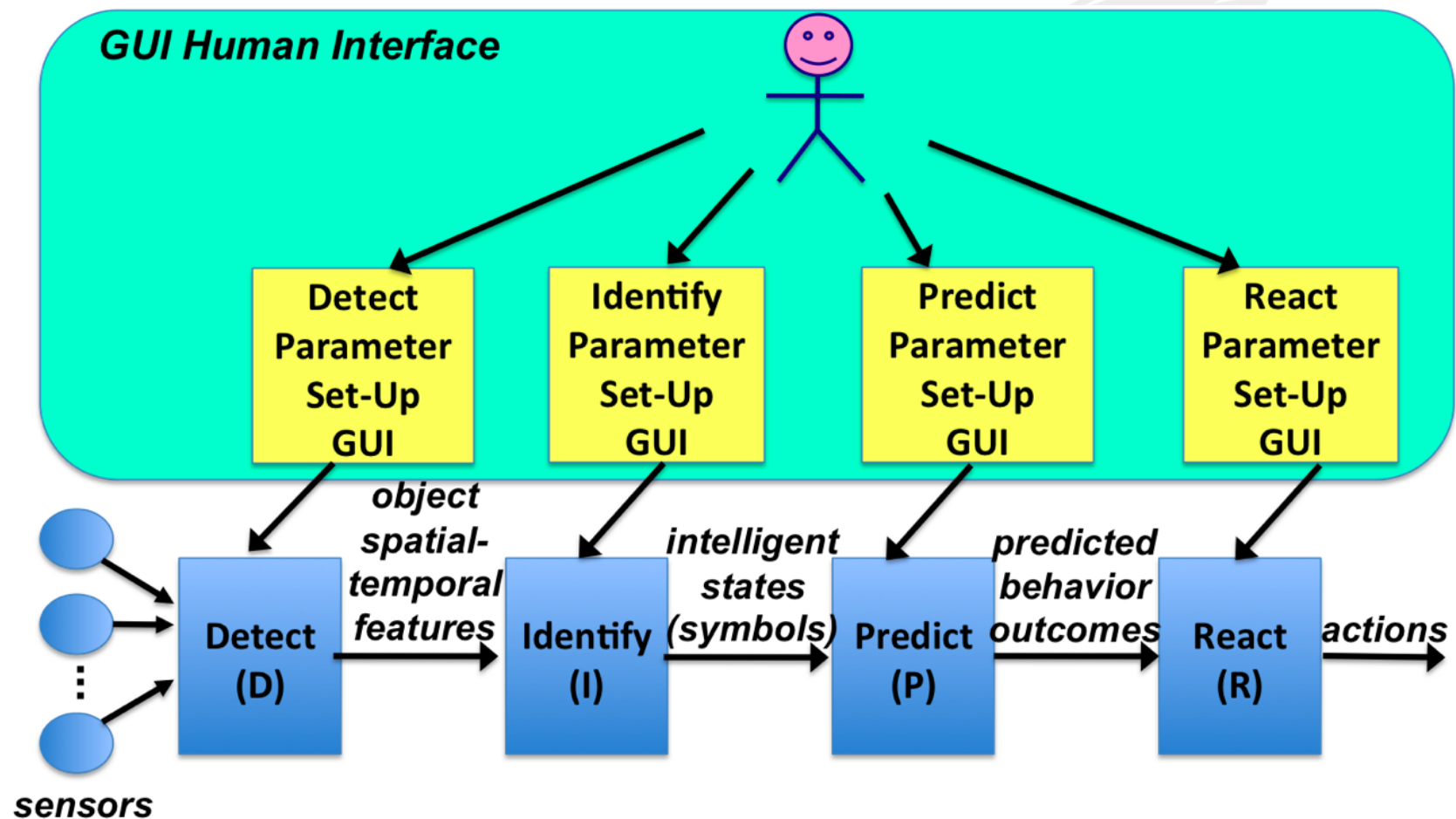




# Human Intel Operator Interface

- Information and the GIG are merging
- Intelligence automation also needs to be implementable through user friendly GUI's at various GIG nodes/servers, where analysts can input scenarios, high level rules of intelligence detection, prediction, reaction of interest; then, automation algorithms would be generated automatically and pushed down onto the appropriate nodes (i.e., in order to automate intelligence extraction at those nodes and pushing this intelligence, defined through the GUI, back to the analyst).
- These GUI's need to be simple and quick as new intelligence (i.e. potential threats) is discovered and needs to be implemented instantly. Automation will be discussed through four sciences of detection, identification, prediction, and reaction, with various applications (e.g. Land, Maritime, Border, etc.).

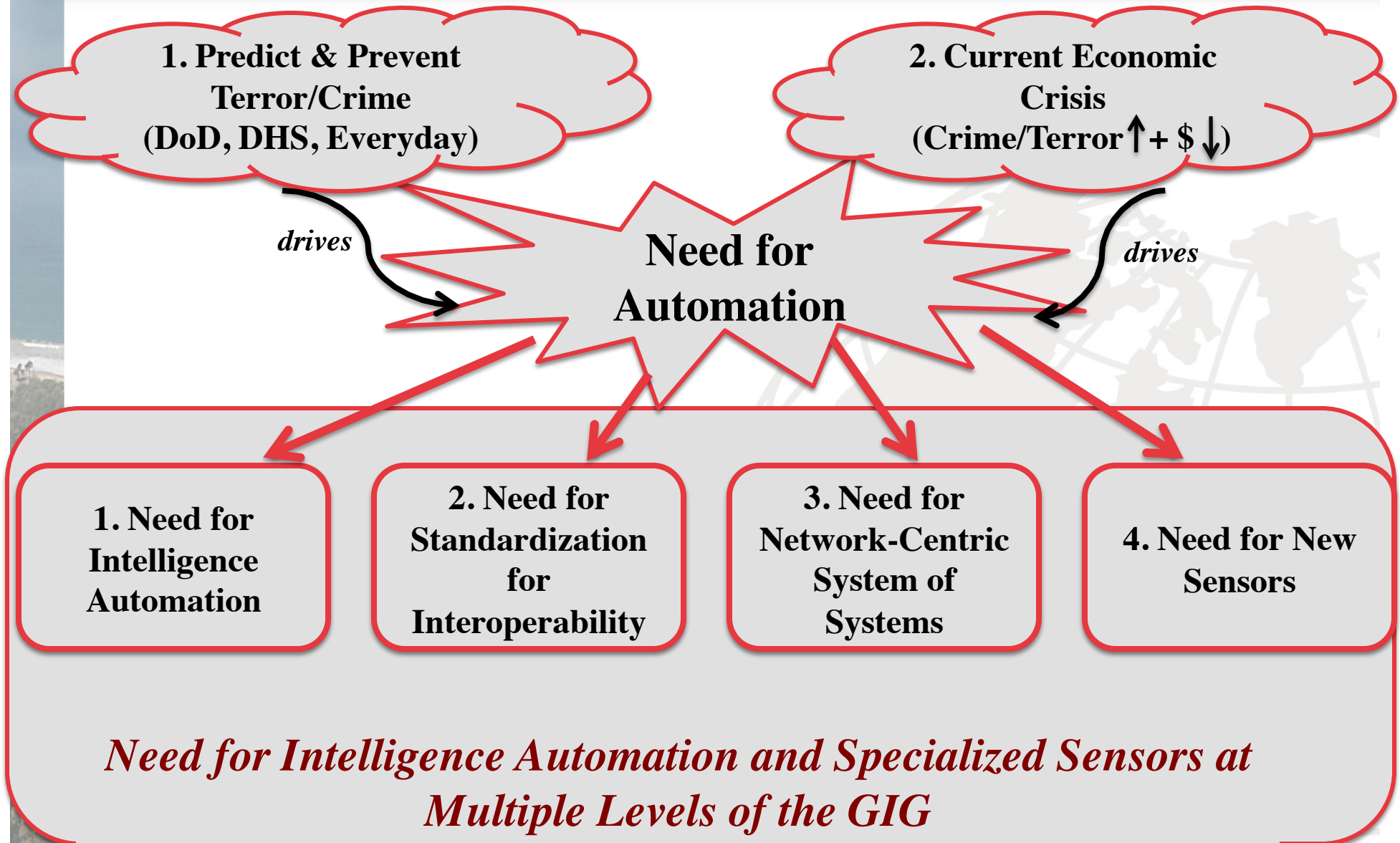
# *GUI Human Interface Superimposed On DIPR (Operators Input Rules of Engagement, Behaviors, Features, Select Sensors, etc .. Automation Algorithms are Generated)*





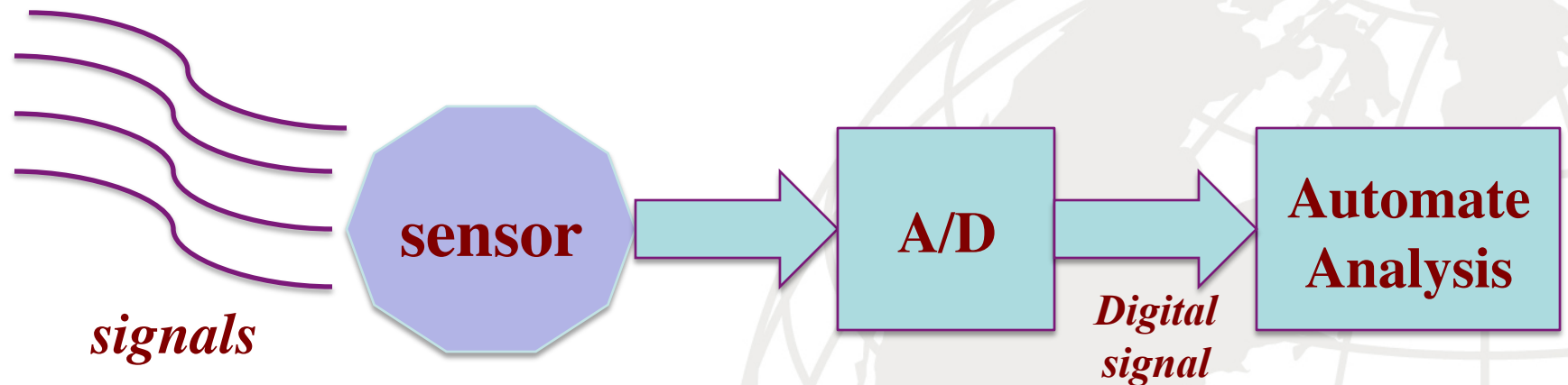


# Need for New Sensors





- What is a sensor?



*Can't analyze signals if the sensor does not exist to collect the signals of interest*



- Where are sensors going? And sensor networks?
- “eyes”, “ears”, “nose” – mimic human sensors
- Other – IR, magnetic, sonar, etc ...
- Cost, size, etc ...



- Where are sensors going?
- “eyes”, “ears”, “nose” – mimic human sensors
- Other – IR, magnetic, sonar, infrasonic, etc ...
- *New sensors – can you detect fear? Can you detect/predict evil? A new world of sensor developments will occur in order to collect information we need for intelligence to predict terror threats.*





# The Need for New Sensors

- Intelligence automation can be generalized, and then customized per application.
- If Maritime Domain Awareness (MDA) is an issue for blue, green, brown waters, the necessary sensors must be developed for threats that you can conceive and plan for in that environment.



- If threats could be in boats, planes, trains, autos, etc., then there must be sensors developed to detect what those vehicles are carrying.
- If it's human traffic and borders where the threat is, you must have sensors for detection of human and border barrier penetration



# Overwhelming Amount of Sensor Data

- Intelligence is currently made up of mostly human intelligence, inputted manually into the GIG, and intelligence officers/analysts analyzing and predicting.
- Once the sensors are there, it will become an overwhelming bottleneck of data, and require intelligence automation.
- Overall, the problem has to be broken into:
  - Sensors or Applications (or a matrix of those two).
  - Development can happen in those areas, and distribution around the GIG.





# Need for Automation

**Predict & Prevent  
Terror/Crime  
(DoD, DHS, Everyday)**

**Current Economic  
Crisis  
(Crime/Terror ↑ + \$ ↓)**

*drives*

**Need for  
Automation**

*drives*

## **1. Need for Intelligence Automation**

- 1. Detection
- 2. Identification
- 3. Prediction
- 4. Reaction
- + advanced fusion
- + advanced learning

## **2. Need for Standardization for Interoperability**

- 2a. Standard  
Interfaces
- 1. Intel  
Automation
  - 2. Comms
  - 3. Security

- 2b. Standard  
GIG Nodes
- 1. Dumb (pass  
raw data)
  - 2. Intelligent (some  
automation)
  - 3. Stand Alone (with  
rules of engagement)

## **3. Need for Network-Centric System of Systems**

- 1. Top-Down System  
(Enterprise/Collaboration/Cloud)
- 2. Bottom-Up System  
(Origination of Data: sensors,  
unmanned systems, etc)
- 3. Middle-Ware System  
(Smart push/smart pull)
- 4. Side-View System  
(Disadvantaged Users)  
+ NC Core (integrates SoS)  
(networks, comms, distributed  
processecing, real-time processing,  
cyber,...)
- + Where is the data?! (back-ups)

## **4. Need for New Sensors**

New threats  
require new  
sensors (comply  
with standards  
of #2)

***Need for Intelligence Automation and Specialized  
Sensors at Multiple Levels of the GIG***



# Examples of Now - Future Applications - NetCentric Operations/Warfare with Unmanned Vehicles and Automated Intelligence





# Applications



Launch an unmanned vehicle first for surveillance and reactions (automated intelligence and automated rules of engagement). E.g. react if the vehicle “sees” someone with an AKA-47.



NAVAL  
POSTGRADUATE  
SCHOOL

# Mobile Airborne Surveillance and Warfare ...



- Automate airborne human ISR and Rules of Engagement

WWW.NPS.EDU



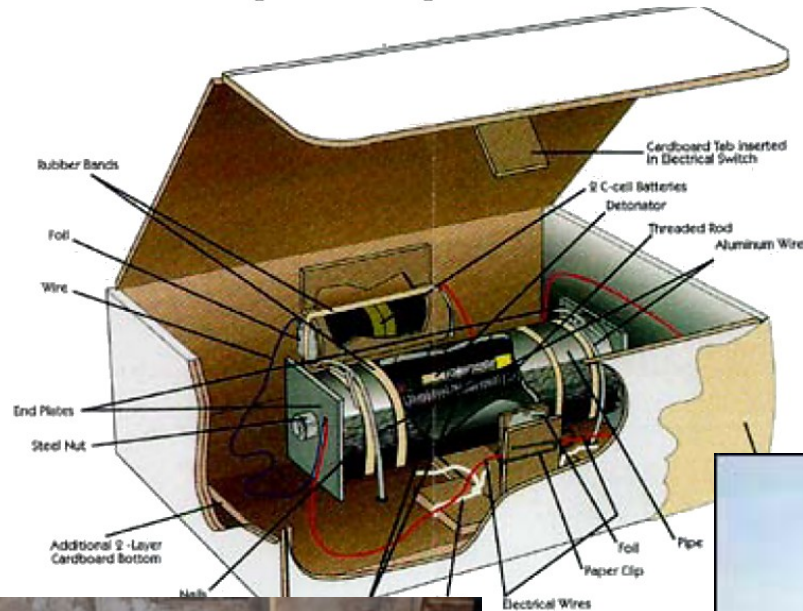




NAVAL  
POSTGRADUATE  
SCHOOL

# Automate Search and Destroy of IED's

Improvised Explosive Device







# Automate Search and Destroy of IED's (Movie "The Hurtlocker")



- Automate part of an Explosive Ordnance Disposal (EOD)'s job
- Automated unmanned ruggedized robots to search for IED's and automate rules of engagement (e.g. low-cost robots could be expendable and therefore destroy IED's)





# Sentry Duty



**Automate human intelligence – “sentry duty”**



# Network-Centric Warfare/Operations Implementation

- Mission
- Rules of Engagement
- GIG Technologies
- Situational Awareness
- Behavior Modeling
- Behavior Prediction— object and behavior tracking through the GIG
- Extraction of Key Features from Sensor Data
- Sensors to Collect Necessary Data
- Platforms for sensors





# Need for Automation

**Predict & Prevent  
Terror/Crime  
(DoD, DHS, Everyday)**

**Current Economic  
Crisis  
(Crime/Terror ↑ + \$ ↓)**

*drives*

**Need for  
Automation**

*drives*

## **1. Need for Intelligence Automation**

- 1. Detection
- 2. Identification
- 3. Prediction
- 4. Reaction
- + advanced fusion
- + advanced learning

## **2. Need for Standardization for Interoperability**

- 2a. Standard  
Interfaces
- 1. Intel  
Automation
  - 2. Comms
  - 3. Security

- 2b. Standard  
GIG Nodes
- 1. Dumb (pass  
raw data)
  - 2. Intelligent (some  
automation)
  - 3. Stand Alone (with  
rules of engagement)

## **3. Need for Network-Centric System of Systems**

- 1. Top-Down System  
(Enterprise/Collaboration/Cloud)
- 2. Bottom-Up System  
(Origination of Data: sensors,  
unmanned systems, etc)
- 3. Middle-Ware System  
(Smart push/smart pull)
- 4. Side-View System  
(Disadvantaged Users)  
+ NC Core (integrates SoS)  
(networks, comms, distributed  
processecing, real-time processing,  
cyber,...)
- + Where is the data?! (back-ups)

## **4. Need for New Sensors**

New threats  
require new  
sensors (comply  
with standards  
of #2)

***Need for Intelligence Automation and Specialized  
Sensors at Multiple Levels of the GIG***