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

Rachel E. Goshorn
Naval Postgraduate School: Electrical and Computer Engineering Department
Monterey, USA
goshorn@nps.edu

Deborah E. Goshorn
Naval Postgraduate School: Electrical and Computer Engineering Department
Monterey, USA
degoshor@nps.edu

Joshua L. Goshorn
University of California, San Diego: Electrical and Computer Engineering Department
San Diego, USA
joshua.goshorn@gmail.com

Lawrence A. Goshorn
Gantz-Mountain Intelligence Automation Systems
Pebble Beach, USA
larrygoshorn@gmail.com

***Abstract* – This paper describes the need for four approaches to automating intelligence from military, Homeland Security, economic crisis, and consumer points of view. Intelligence automation is one of the four approaches required in a complete solution. The four approaches presented in this paper are as follows: (1) intelligence automation through Detection/Identification/Prediction/Reaction (DIPR), (2) interoperability through standardization, (3) network-centric system of systems infrastructure (how to organize data and intelligence and actively "reprogram", through Service Oriented Architectures and smart cloud computing graphical user interfaces, the sensor systems connected to the cloud, as intelligence needs are updated), and (4) new/advanced sensors and architectures to support ongoing intelligence automating systems. The aim for this paper is to be a standalone educator and guide in attempt to solve the problem of augmenting and automating human intelligence in distributed sensor systems connected to the top-down system of smart cloud computing.**

Keywords- Distributed GIG Intelligence Automation Systems, Network-Centric Systems of Systems, Systems Engineering, Detect/Identify/Predict/React (DIPR) Systems, Behavior Prediction, Intelligence Standardization for Interoperability, Artificial Intelligence Systems, Distributed Systems, Intelligence Surveillance, Smart Robots, GWOT, Homeland Security

I. INTRODUCTION

This paper presents four approaches needed for solving the problem automating human intelligence within distributed sensor systems using the infrastructure of network-centric system of systems. Firstly, Section I introduces the need for intelligence automation, a background on the paper, and an overview of the four approaches required for automation. Section II presents the first approach needed, which is intelligence automation through the Detection/Identification/Prediction/Reaction (DIPR) framework. Section III presents the second approach of interoperability through standardization within a network-centric system of systems. Section IV presents the third approach of describing the infrastructure of a true network-centric system of systems, with smart cloud computing. Section V describes a brief overview of the need for new and advanced sensors and architectures that could be used in support of augmenting and automating human intelligence. Finally, Section VI concludes the paper.

A. The Need for Intelligence Automation

There is a critical need for distributed intelligence automation system of systems. This need is discussed from various perspectives, from the to need to predict and prevent terror and crime for the Global War on Terror (GWOT) and Homeland Security (HLS), to the lack of man-power due to budget cuts, to daily consumer needs. Today's world is driven by the need for actionable intelligence, whether for a warfighter, unmanned system, policeman, or consumer, etc.

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. The job of protecting this country, is obtaining the necessary intelligence to have homeland protection. 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.

In addition to the GWOT and HLS needs, because the terror and crime rates are going up, there is a requirement for more people; in parallel, budgets are being cut, which requires less people. Therefore, since more people are needed, and in parallel, the number of people are being reduced, automation is required. This paradigm shift, is analogous to the automation of telephone operators. In the 1920's, the Grandma of the first three authors (mother of the fourth author) worked as a telephone operator, Fig. 1. In the 1920's people projected a huge growth in the number of people who would own telephones. Based on the need, they concluded they would need to hire every high school girl graduate as a telephone operator, which was not possible. Therefore the technology of the switching circuit was developed to automate the telephone operator. It will be shown in the next subsection, that a system automated with full security is equivalent, to less than, a full time human.

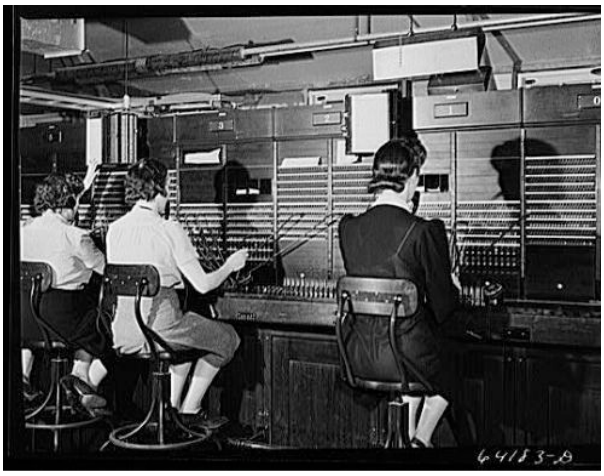


Figure 1. Need Drove Technology of Switching Circuits to Automate Telephone Operators.

In addition to the GWOT/HLS and the current economic crisis driving the automation need, daily consumer needs are driving this world to automation through intelligence automation. What does the consumer (whether a single user, home, organization, business, or city) want in the future? The consumer wants their world "synchronized and automated". The consumer wants more information, from multiple sources (devices, sensors, websites, social networking, etc); wants the information right now, and wants the information intelligently processed and automated to recommend "what to do" based on the consumer's preferences. In other words, the consumer has the desire for high-level intelligence of fused features, behaviors, and "what to do" recommendations or automated reactions, from various sources/devices in time and space. The author's proposed intelligence automation system for the consumer can be seen in Fig. 2.

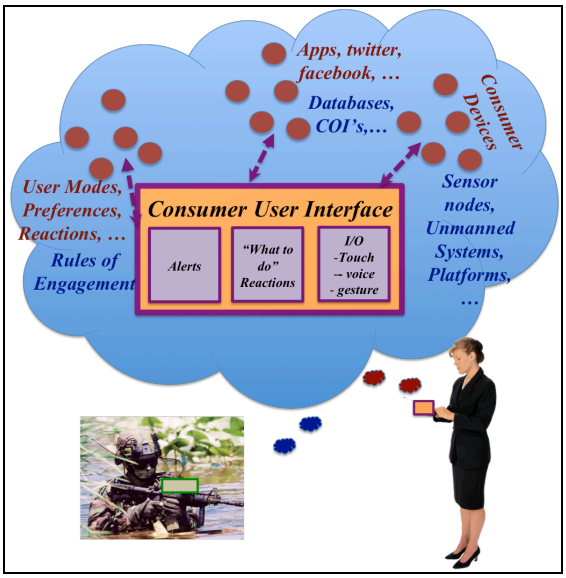


Figure 2. Consumer Intelligence System, "Synchronizing and Automating the Consumer's World", whether the consumer is a civilian or a warfighter. (Consumer referenced in red text, warfighter referenced in blue text in the Fig. bubble).

B. Examples Depicting the Need for Intelligence Automation

This subsection presents three different examples to show the need for intelligence automation. The first two examples present the paradigm shift requirement of compression through intelligence automation. First of all, there are not enough humans, facilities to monitor and analyze the sensor data. As highlighted in a recent *New York Times* article, one year's worth of missions from one drone would take about 24 man-years to analyze the data [19]. In addition, there is not enough bandwidth to communicate the sensors' data. The first example, generalizes a color camera transmission compared to one

hundred million people typing; the comparison is through the amount of information defined in bytes. The second example presents that there is not enough bandwidth, power, and weight in mobile sensor systems; therefore, compression of bandwidth, power, and weight is needed through intelligence automation at the mobile node. The third example deals with cost, since budgets are being cut and yet we need more manpower to monitor cities, borders, etc as crime has increased. This example demonstrates the cost of one fully automated system is less than one full-time police.

1. Bandwidth Required Example

Assume there are one hundred million keyboards in the world, which are typing, at the same time, at a rate of ten characters per second. This computes to be one billion bytes per second, for all the keyboards in the world. Assuming there is a 20 megapixel camera, where each pixel has three bytes (one byte for each: red, green, blue). This is 60 megabytes for one snapshot of the color camera. If the camera is transmitting at 30 frames per sec, it's transmitting 1.8 billion bytes per second. One color camera is transmitting about twice as many bytes as 100 million keyboards in one second. Therefore, there is a paradigm shift in network bandwidth required for all of these surveillance cameras, and sensors. With millions of these sensors distributed, you will never have the humans, facilities, or bandwidth to handle this much information. Intelligence Automation (e.g. DIPR; presented in the next section) is the ultimate bandwidth compression algorithm, facilities, and human savings.

2. Mobile/Satellite Bandwidth, Power, and Weight Example

For every information bit transmission, it takes a fixed amount of energy per bit. If you transmit 10^2 bytes per second versus 10^7 bytes per second, you save 10^5 bytes per second that do not have to be transmitted, and save 10^4 – 10^5 in power, thereby also saving weight (less power sources required). Assume 100 watts is transmitting over 10^8 bits; this therefore has a fixed energy per bit of one watt per million bits. If, you are now only transmitting 10^3 bits, it's one miliwatt of power total for the same energy per bit. There is a paradigm shift in bandwidth, power and weight requirements for mobile systems. Therefore, the future will be the same for nano-satellites. Therefore, processing with intelligence automation at the node, allows for bandwidth goes down, power goes down, weight goes down in mobile systems and future nano-satellites (as the number of sensors increase at the nano-satellite, with nano-satellites acting as mobile wireless ad-hoc nodes in space, will require compression at the node through intelligence automation). Intelligence Automation (e.g. DIPR) is the ultimate bandwidth, power and weight compression algorithm.

3. Cost of Fully Automated System vs. Manpower Example

This section presents the value of an automated system versus a fulltime policeman for constant surveillance in a standard ten square mile city. In addition a cost calculation for a sensor system, both with and without intelligence automation, is presented. Following are the assumptions for the environment of the example: (1) a standard city (i.e., no "sky risers"), with standard intersections and city blocks; (2) a surveillance example in a city, where the crime rate and terror threats require constant surveillance (24 hours a day, 7 days a week) with police. Most cities have one intersection, a city block, every 10^{th} of a mile. So, in one mile, there are ten intersections. For constant surveillance, cameras must be placed in these intersections in the four intersection directions. Assume ten cameras, two for each direction plus two extra (could be magnetic, etc). In ten square miles, there are ten thousand cameras. Therefore, there are ten thousand video displays for a good security system in a ten square mile city. (See Fig. 3).

With human factors' studies, it's known humans cannot monitor video constantly. So, visual inspection and the ability to perform roles dramatically reduces within a few hours. Assume one human can look on average at 50 cameras per day(100 at night, 50 during the day). Therefore, 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). In order to constantly monitor ten square miles, through surveillance systems, it takes more police than patrolling by foot. *This went in wrong direction!*

Assume there is automation on each camera, where each camera is alerting abnormal behavior. Assume one-percent of the time a camera may pick up abnormal behavior (standard city behavior; we are not analyzing a city like New York or Chicago). Now, two policeman (24/7) are only needed per ***10 square miles*** (1% of 200 policeman), for a city with moderate activity. This is a one hundred to one reduction in police (i.e., reduction in manpower through intelligence automation).

Cost is the driving factor. In today's world, a turn-key system could be installed for $20K (where $1K is $1,000) per camera, without automation. When in mass production, with automation, project in the future, $4K per camera. For ten square miles, 10,000 cameras x $4K = $40M (where $1M is one million dollars). Now, take this $40M and amortize over a life of 20 years, which equates to $2M/year. Now, let's compare to the cost of a policeman. Assume the cost of one full-time policeman is $330K/year (include overhead, department, etc). One police on full-time (24/7), equates to 168 hours. Now, assume one human puts in 28 effective hours per week (sick, vacation, holiday, admin, etc). So, 168 hours divided by 28 hours is six. Therefore, six policemen are required for one policeman fulltime. Six

police times $330K is $1.98M. Therefore, the amortize value of ***10 square miles*** of a fully automated system cost is equivalent to one 24/7 policeman fulltime. Therefore, the benefits of having a system automated with full security will assist in this current economic crisis. This system could also pay for itself: for example, incorporate traffic and DMV violation automation (monitor cars and ID them with license plate recognition). This example could be scaled to other applications. For example: soldiers costs around $1M/soldier in Iraq (include support per soldier); there is a definite need for automation due to cost and to protect our soldiers.

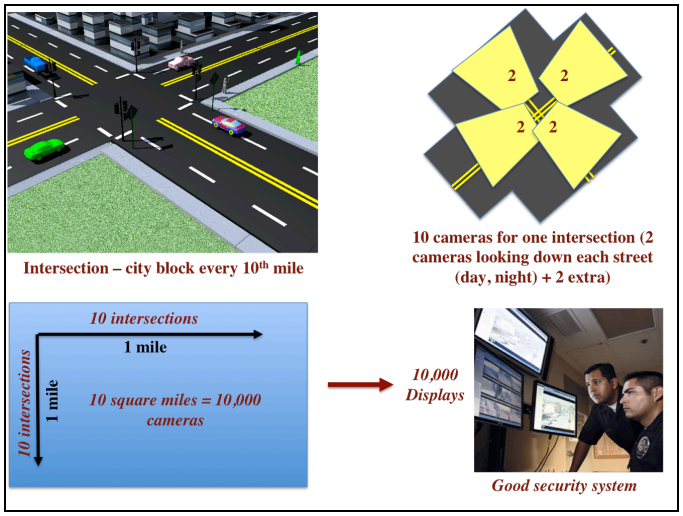


Figure 3. Example of a City Block and Ten Square Mile City with Constant Surveillance.

C. Authors and Paper Background

In order to show the criticalness of intelligence automation and the recommendations in this paper, a high-level background on the authors and paper is given. This paper is a result of over ten years of collaboration between the authors, in research in intelligence automation for distributed systems. The authors have over seventy years of experience in advanced systems design, specifically in the field of intelligence automation through behavior predictions and reactions. The authors have developed an intelligence automation standard, which is the basis of this paper, where separate technologies are combined through Detection, Identification, Prediction and Reaction (DIPR) and is presented in detail in an invited Springer Handbook for ambient intelligence and smart environments [2]. In addition, the material for this paper is a "survey" of the material for an invited book underway (a handful of leading technical publishers have invited the authors to write a book on this material). In addition, a list of references from the authors can be seen in REFERENCES Section [1-18]. In addition, several system implementations and proof of concept systems have been carried out on this subject with the authors.

Overall, this paper began by describing the need for intelligence automation from a military, Homeland Security, economic crisis, and consumer point of view. Intelligence automation software (DIPR) is one of the four approaches required in a complete solution for intelligence automation. This paper will give an explanation of the four approaches: intelligence automation (DIPR), interoperability through standardization, network-centric system of systems infrastructure (how to organize data and intelligence and actively "reprogram", through SOA/Cloud GUI's, systems as intelligence needs are updated), and new/advanced sensors and architectures. This paper is a stand alone educator and guide to solve the problem of automating human intelligence in distributed sensor systems.

D. Overview of Four Approaches Required for Intelligence Automation

As discussed in section I.A, there are three driving needs for automation, as seen in Fig. 4. Automation must be carried out through four approaches, also shown in Fig. 4. Additionally, Fig. 4 can be seen as an overview of this paper.

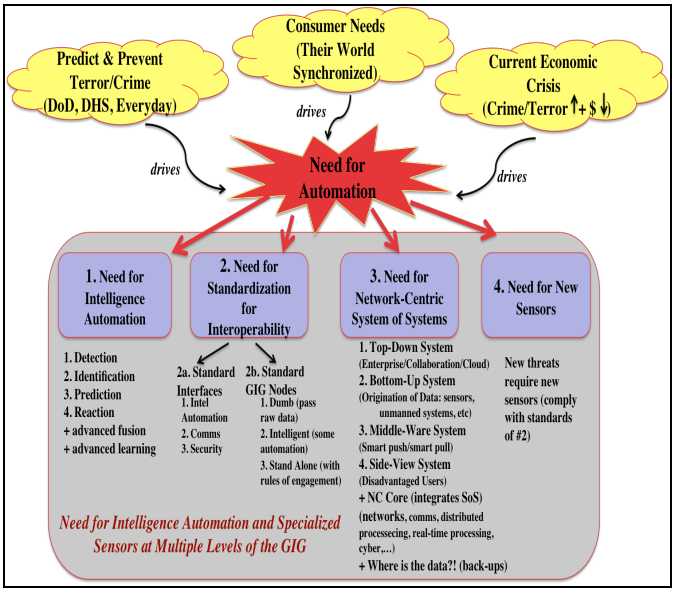


Figure 4. The Need for Intelligence Automation Systems, and the Four Approaches Required to Implement Automation (Paper Structure).

1. Approach 1: Intelligence Automation

First, once sensors are utilized, an overwhelming information bottleneck is created. Therefore, intelligence automation is necessary to remove the need for people and the reduction of potential bandwidth problems. If these GIG nodes are mobile, remote, and wireless, there may be packaging and power optimizations required in addition to intelligence automation. Intelligence automation should be broken into four sciences of DIPR (section II), as seen in

Fig. 4 (and the next section for more detail). Automation is required because of the combination of increasing the number of people needed due to the corresponding increase of terror and crime, while at the same time dealing with budget cuts.

2. Approach 2: Standardization for Interoperability

Secondly, there is the requirement to standardize for interoperability. Standardization is required in two areas: 2a. standard interfaces (intelligence automation, comms, security) and 2b. Standard GIG Nodes. Standardization for interoperability is presented in Section 3.

3. Approach 3: Infrastructure for Network-Centric System of Systems

Thirdly, information and systems need to be organized in a Network-Centric System of Systems approach. All information needs to be shared (through a "smart push") from a "bottom-up" system (from sensors, humans, unmanned systems, nodes, etc), to a top-down system of collaboration (through a service oriented architecture and cloud computing infrastructure with "smart push/smart pull"). 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 and cloud computing 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". Once sensors are selected, and formed into a GIG node, GIG nodes should categorize into standard formats: dumb (passing information), intelligent (automation of some form), and stand alone with rules of engagement to take action (which is discussed further in section III).

4. Approach 4: Bottom-Up Sensors

Fourthly, sensors need to be developed, whatever sensors are required to detect the information needed to obtain intelligence about whatever you're concerned about (*i.e.*, whether it's chemical, biological, detection of terrorist, etc …); there are sensors that can help automate gathering the information to predict threats, as presented in Section 5, along with a smart sensor node architecture allowing for vast parallel processing at the node.

II. Intelligence Automation

The first approach required for automating human intelligence in sensor systems entails both (1) the need for distributing intelligence into four levels (namely, Detect, Identify, Predict, and React (DIPR)) and (2) the need for a generalized solution of overlaying these four level of intelligence automation onto existing or new system infrastructure (hardware/software) for customization of solutions. The solution for the latter need is called an AI Systems Solution and is summarized in a hierarchy via the pyramid in Fig. 5, where each level is a system of the entire AI Systems Solution. This section first introductes the AI Systems Solution framework and is followed by a description of the four levels of intelligence automation DIPR are presented.

A. AI Systems Solution

The four levels, or technologies, of intelligence automation are typically different engineering or science fields, and not usually integrated together. The goal of DIPR is to implement hman analyst's experise, as seen in Fig. 6b. The total solution would require the Infrastructure of (first level of the pyramid) and the Application Models, which engineer DIPR subsystems to perform in a specific rather than generalized solution (third level of the pyramid). The complete solution begins with an actual Application (fourth level of the pyramid) to obtain knowledge required for the definitions of the Application Models and the DIPR subsystems. Once the Application Models and the DIPR subsystems are defined within the actual application, customization for the final solution is carried out (fifth level of the pyramid). More detail than Section II, can be seen in[2] and other author references in the References Section. A smart cloud computing approach is prsented in Section IV, where an analysist through a cloud computing/SOA Graphical User Interface (GUI) can input mission data (from an Application Model approach), select sensors and features, behaviors to track and rules of engagement (*i.e.*, the analyst selects the parameters for DIPR without programming and the algorithms are selected and generated behind the scenes).

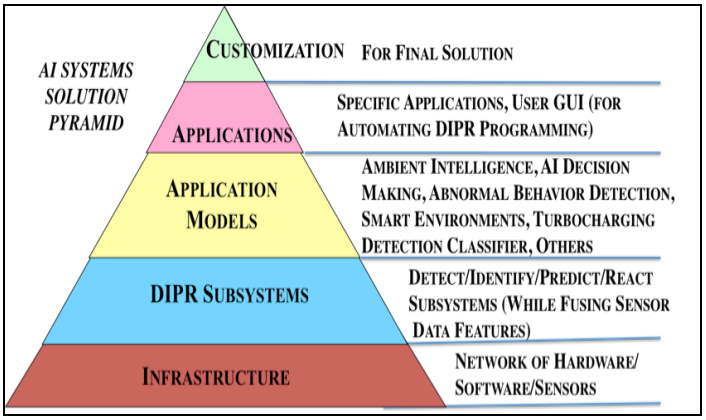
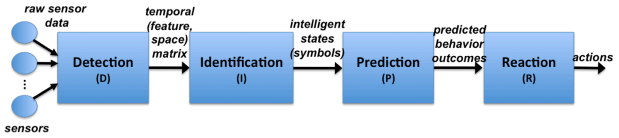


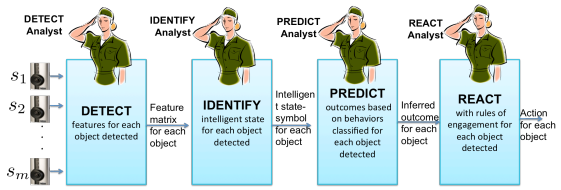
Figure 5. AI Systems Solution Pyramid, based on DIPR System

B. DIPR Description

The overall complex problem of starting with sensors and outputting intelligent reactions must be handled in this AI partition technology systems engineering approach, utilizing "Detection", "Identification", "Prediction" and "Reaction" (DIPR) technologies, as shown in Fig. 6a. The system is divided from the environment to raw sensor data, through stages of technologies, to Reactions. Each DIPR technology is a separate engineering, science, or math, discipline.



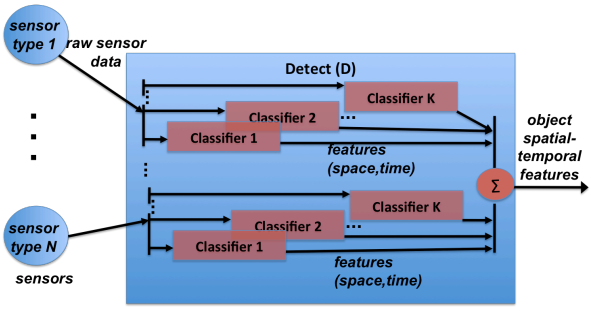
(a)



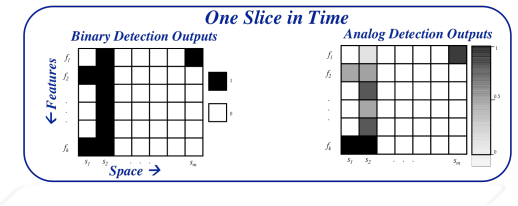
(b)

Figure 6. Detection, Identification, Prediction, and Reaction (DIPR) System (a). In (b), DIPR is analogous to automating analyst expertise.

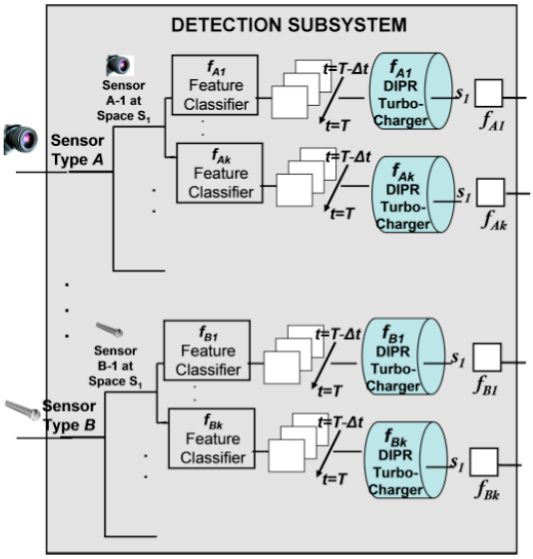
From the sensors comes the first subsystem of "Detection" (D = Detection), seen in Fig. 7a/b, which is defined here as extracted objects features, where features are low-level classifications extracted from raw sensor data. This also greatly reduces the bandwidth requirements since only extracted features are communicated upstream to the Identification subsystem. The Detection subsystem utilizes both new novel "turbocharger" and selected/refined/licensed/open source classifiers depending on the application.



(a)



(b)



(c)

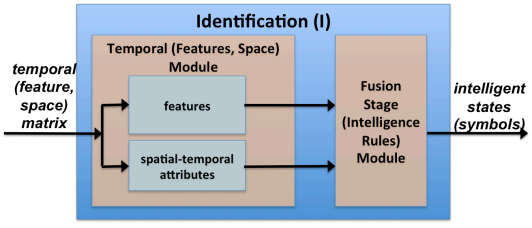
Figure 7. DIPR "Detection" Subsystem (a), "Detection" Subsystem Outputs (b), and (c) Optional DIPR Turbocharger.

Detection can be enhanced with a post-processing algorithm which "turbocharges" (enhances without redesigning) the performance of Detect classifiers, without reconfiguring the classifiers. The authors utilize the "DIPR turbocharger" [12], to perform this function. It is an advanced statistical enhancement filtering algorithm utilized to enhance general classifiers. Detecting features from raw data is the foundation of the "Detection" subsystem in the DIPR System. When such classifiers have mediocre

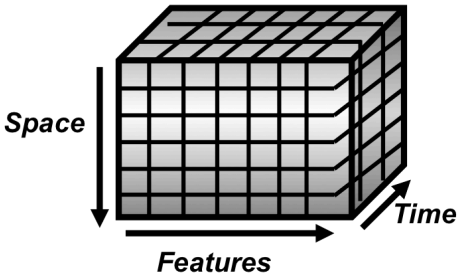
accuracy, there could be countless tunings until the feature classifier performs acceptably for the specific environment. Additionally, it is often the case that the sensors' environment changes, either by a dynamic environment or the sensor itself being physically moved to another location. In either case, the feature classifiers must be tuned again and often tediously retrained to achieve acceptable performance in the changed sensor environment. A novel approach was developed, and incorporated as a high-level classifier, to enhance the performance of the low-level classifier, and thus "turbocharging" the detection statistics of the feature classifier. This high-level classifier is called the DIPR Turbocharger, and has been shown to dramatically increase low-level classification errors, in some cases from 30% accuracy of the feature classifiers to 100% accuracy [12]. The DIPR Turbocharger is a paramount application to the DIPR system, and can be introduced into the Detection subsystem or any other DIPR subsystem, as seen in Fig. 7c.

The subsystem "Identification" (I = Identification) uses multiple object features (fusing) with space and time for low-level "Identifiers" outputs called intelligent states (symbols), seen in Fig. 8a. Symbols are created using features and spatial-temporal attributes (stored in "I", as seen in Fig. 8b) fused or combined by a priori low-level rules of intelligence. (These rules of intelligence are derived from knowledge of the application. A future system can be an Adaptable Learning System; see [2] for more details). The ability to fuse a wide array of sensor types is essential in describing any behavior.

The inputs to the subsystem "Prediction" (P=Prediction) are these intelligent states, with outputs of predicted behavior outcomes. Prediction is a high-level classifier; in this case, "P" uses a syntactical behavioral classifier (that is very generalized and scalable) that has been developed for over ten years by the authors, and continues to be upgraded [2]. "P" could also use various behavior classifiers. Intelligent states (symbols) are concatenated over time/space to form sequences (seen in Fig. 9). Then these sequences are classified into behaviors (behavior labels) through a statistical sequential syntactical behavior classifier. These behaviors are defined as known normal behaviors, known abnormal behaviors, and anything else (too far away) is an unknown behavior. These behavior classification labels are then inferred to predicted behavior outcomes (through defined inferred prediction outcome rules), as shown in Fig. 9.



(a)



(b)

Figure 8. DIPR "Identification" Subsystem (a) and temporal (feature, space) matrix history maintained (as a cube) in "Identification" Subsystem (b).

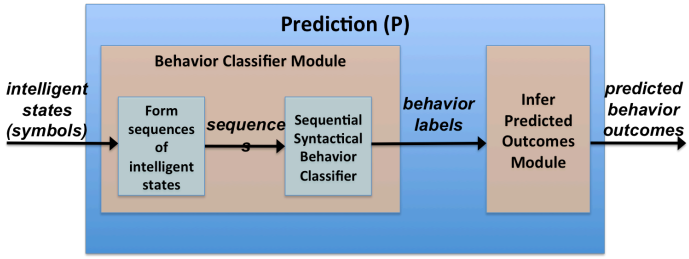


Figure 9. DIPR "Prediction" Subsystem.

The inputs to the subsystem "Reaction" (R=Reaction) are predicted behavior outcomes; outputs of Reaction are actions (could also be reports, alarms, or recommendations). The main function of Reaction subsystem is to create actions in response to the predicted behavior outcomes, and is application dependent; this is where rules of engagement come into play. These rules of engagement, or reporting, are implemented with "Rule-Base" AI Algorithms and look-up tables.

III. Interoperability

The second approach needed for enabling distributed, automated intelligent systems is the need for enforcing standards within a network-centric system of systems. Intelligence automation cannot occur if a system (composed of network nodes and data flow interfaces) is not interoperable. As missions change, areas of operation change, systems and sensors change, the network-centric system of systems needs to be able to be re-configured using pre-defined standards of interfaces and node types. Therefore, interoperability is a must in order to plug and play various sensors and systems, particularly in this word of system of systems. For interoperability, standardization must occur in two areas: one through standardizing interfaces and the other through standardizing the building blocks of a system (i.e., a system node; a node could be a human as well). Section III.A presents the need for standard interfaces and Section III.B presents the need for standardizing system node types.

A. Interoperability through Standard Interfaces

A network-centric system can be thought of as a system composed of nodes and node interfaces (more detail is presented in Section IV). Interfaces connect two nodes, whether a node is a computer system, sensor, or a human. In order to allow for network centric systems with open architectures that can scale, and allow intelligence automation, such a system must enforce standardization in both its node types and its node interface types. In other words, there must be a standard plug-in-play process for interfacing nodes. To provide an analogy, Fig. 10 provides an example of a system with one node expanding to two nodes: a PC Computer node and a newly added peripheral node. In order to plug in a new peripheral into the system, the system requires for one to download the peripheral driver onto the PC Computer node so the peripheral node can interface with the PC node in a standardized, pre-defined way.

Similarly, interfaces need to be standardized and pre-defined between nodes in a network-centric system of systems. Interfaces between network nodes should be standardized in three categories (see Fig. 10 below): intelligence automation, communications, and security, as described below.

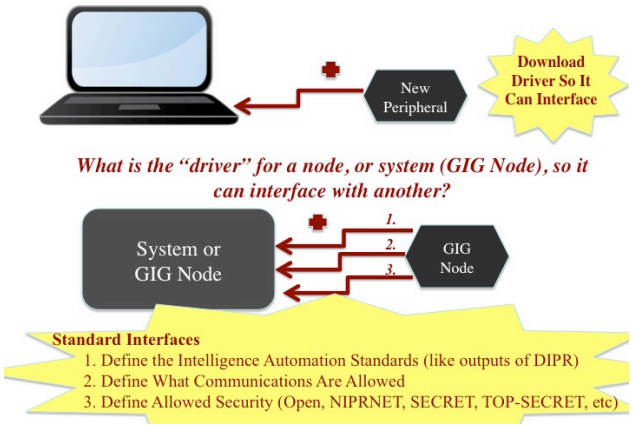


Figure 10. The need for standardization (each interface has three requirements for standardization).

1. Intelligence Automation Interface Standardization

The data type outputted from a node may be raw sensor data or may be some form of intelligence data product (as summarized in Section III.B under system node standardizations). For the network-centric system to understand the raw sensor data or intelligence product, the data product must be written in a standardized format. Various standards (STANAGs) exist for data already, but not in context to hierarchical intelligence automation (complexity). Additionally, for the system to continue its DIPR intelligence automation (automating object features, system states, object behavior predictions, and system reactions), the intelligence product must conform to one of the four levels of DIPR. Standards can be enforced in several methods/formats, such as text files, XML, binary files, etc.

To enable automation of complex behaviors, such files should be categorized into one of the four levels of intelligence: Detect stage, Identify Stage, Predict Stage, and React stage. This section overviews needed standardized interfaces for each stage.

Detection interfaces include raw sensor data formats, standards for outputting object features (i.e. agreed upon vocabulary of features), standards for temporal parameters on how often a node outputs features, standards for spatial parameters to include the resolution of sensor data for which to extract intelligence from. An example standardized message that exists today is the STANAG 4607, which are Ground Moving Target Indicator (GMTI) tracks, for tracking targets from raw sensor data such as video or radar.

Identification interfaces include an agreed upon vocabulary of system "intelligent states" or fused features. These were referred to as symbols (known text symbols).

Prediction interfaces include an agreed upon vocabulary of sequences of text symbols (e.g. DNA sequence) to represent a type of behavior. Behavior vocabularies need to be agreed upon. Finally, a library of predicted outcomes associated with each behavior need to be standardized.

Reaction Interfaces include a library of agreed upon rules of engagement associated with each behavior outcome.

2. Communications Interface Standardization

Communications standards are already a major area of interest in the military and in industry. The less stovepipe a system is in its data format, the better its success and future is. For example, military standards exist for communication links.

3. Security Interface Standardization

When a new node is going to be added to an existing network-centric system, it needs to be able to be prepared to enter on a particular official security classification (e.g. Coalition force friendly, For Official Use Only, Unclassified, Secret, Top Secret/SCI). A GIG node can be plugged into the network anywhere and its raw sensor data and generated intelligence product messages (as overviewed

in 3.1.1) of predefined standard data (DIPR outputs) will need to have predefined representation in each of the security classification. This will help messages transfer cross domain solutions (i.e. automatic message guards).

Overall, if a GIG node does not comply to the agreed standard interfaces, it will not be able to interface into the network. To summarize, every GIG Node or System, must comply to the three standard interfaces (as seen in Fig. 11 below). These interfaces are designed in detail for each mission/application or network-centric system of systems infrastructure. The goal is for any mission, be able to add a system or GIG Node as needed, and interoperate into the intelligence automation hierarchy.

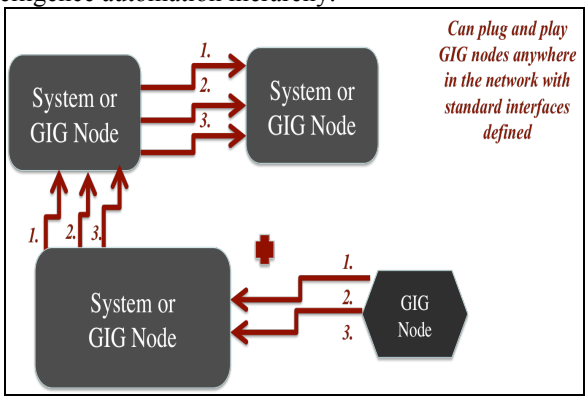


Figure 11. Plug-in Play a new GIG node into the network as long as the new GIG node meets 1. Intelligence Automation Message Standards, 2. Data Communications Standards and 3. Security Classification Standards in its interfaces.

B. *Interoperability through Standard GIG Nodes*

In addition, for interoperability, in order to develop a standardized architecture, the building blocks of the nodes, i.e. GIG Nodes, must be standardized. GIG nodes must be standardized in order plug and play. This is so that if we categorized GIG nodes into predefined standards, it is expected what high level of automation (if any) comes with the GIG node, just by knowing the level's class. Whenever a new GIG Node or system is developed, it must comply to a GIG Node standardization. In addition, "add-ons" may upgrade a legacy GIG Node or system into these standardizations.

Once sensors are selected, and formed into a GIG node, GIG nodes should categorize into standard formats. Recommended Classes of GIG nodes are explained below and depicted in corresponding Fig. 12 below.

1. *Class 1 GIG Nodes*

Class 1 GIG Node – This is the very basic node, with no intelligence (i.e., current legacy nodes on a platform, such as a sonar room with a human in the loop is a Class 1 GIG Node. Typically, a remote sensor converter is a Class 1 GIG Node). A Class 1 GIG Node is "dumb", simply passing raw data information.

2. *Class 2 GIG Nodes*

Class 2 GIG Node- This is in between Class 1 GIG Node and Class 3 GIG Node. A Class 2 GIG Node has the intelligence to push/pull features and information of interest, with various levels of automated and fused intelligence, but no reaction ("rules of engagement") is possible. A Class 2 GIG Node is intelligent, with some form of automation.

3. *Class 3 GIG Nodes*

Class 3 GIG Node - This is a stand-alone node and is the highest intelligent node that has Detection, Identification, Prediction and Reaction (DIPR). For example, a tomahawk missile could be a Class 3 GIG Node, which is standalone. It could detect features, identify intelligent information about the features, predict enemy behavior threats, and react by launching the missile at the desired target; or an IED node would detect and selectively jam within its "rules of engagement". Other actions/information communications are included as well. A Class 3 GIG Node is stand alone with rules of engagement to take action.

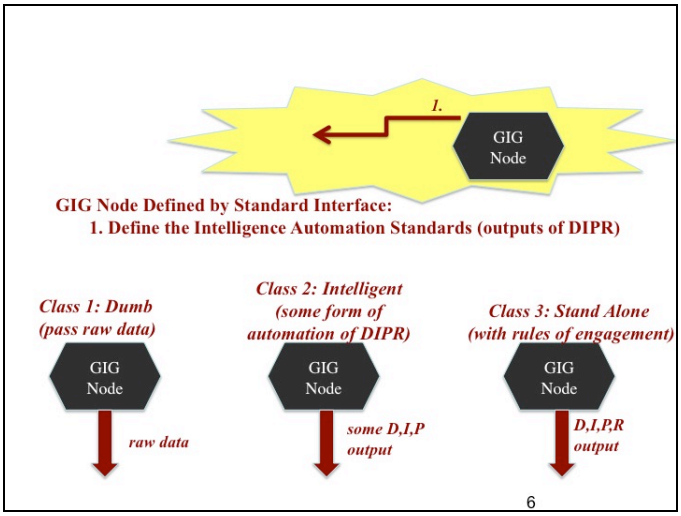


Figure 12. The need for standardization (GIG Nodes).

IV. NETWORK-CENTRIC SYSTEM OF SYSTEMS INFRASTRUCTURE

What do we do with the extracted intelligence and information? There is a need to organize information, data, intelligence, networks, sensors, systems, unmanned systems, etc. The third approach needed for enabling intelligent automation systems is the implementation of a network-centric system of systems infrastructure. The age in which we live, lead, and fight is evolving due to information sharing through Net-Centric Enterprise Systems and Services. The Global War on Terror and HLS are forcing us

to share information in order to make decisions more quickly and be able to predict and prevent potential terror, both abroad and at home. Overall, the DoD's operating environment has changed and will continue to change. Information needs to be organized through a Network-Centric System of Systems infrastructure.

A. Overview

Operators/analysts need to see the highest-level of intelligence and be able to "drill" down to the raw sensor data and "re-program" what sensors should be looking for, based on changes in mission. A network-centric system of systems infrastructure is therefore required. All information needs to be shared (through a "smart push") from a "bottom-up" approach (from sensors, humans, nodes, etc), to a top-down approach of collaboration (through a service oriented architecture (SOA) with "smart push/smart pull"). 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 and cloud computing 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". Once sensors are selected, and formed into a GIG node, GIG nodes should categorize into standard formats: dumb (passing information), intelligent (automation of some form), and stand alone with rules of engagement to take action. This section will present findings discovered by the authors over years of experience [2,10,18], beginning with modeling network-centric systems engineering education over two years time of over fifty iterative interactions with several DoD/DHS agencies, finding their needs for Network-Centric Systems Engineering (NCSE) education [18]. Since then, through the authors' collaboration, the model has been "fine-tuned". Overall, this has been and continues to be an iterative process.

B. Network-Centric System of Systems Infrastructure

The main problem found, in research in order to model network-centric systems, was that there are several different approaches, stove-pipe technologies, different terminologies in this network-centric world; it would be impossible to educate and model all approaches. This world can also be very ``smoky" and many can easily throw around ``buzz-words" without much meaning/depth. So, how can this world be educated and modeled? After researching and the several meetings, the various approaches and vocabularies were understood, that they were all attempting to carry out the same thing as another approach (they just used different words).

In modeling, it was discovered that this is a system of systems model. There are four core systems in this network-centric system of systems, that act and evolve, and it seems independent of each other. All four are critical to the whole network-centric world and must interact with each other, from a system of systems engineering approach, in order to implement this world. These systems branched out from these four core overlapping systems, as seen in Fig. 13.

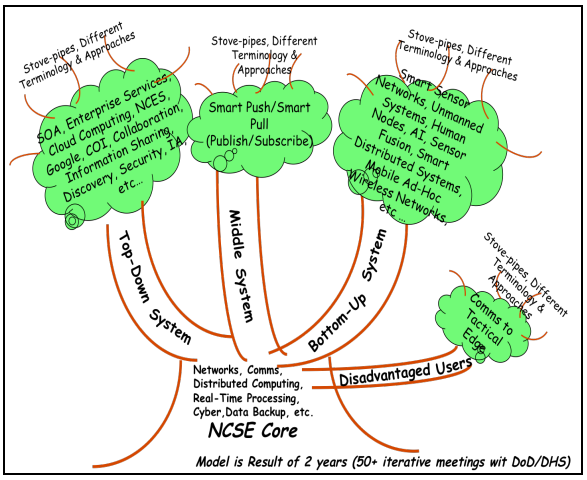


Figure 13. Network-Centric System of Systems, composed of four core overlapping systems, that extend out into the stove-pipe technologies and various terminologies, with an integrating NCSE Core (the "trunk").

The four overlapping systems which make up the Network-Centric System of Systems are the following:

1. Top-Down System – This is where the highest level of intelligence is for a mission and the ability to collaborate and share through service oriented architectures, cloud computing, enterprise architecture (SOA, Cloud Computing, Enterprise Services, DISA NCES, Google Apps, Collaboration, IA, Security, Data Discovery, T&E for Services- e.g. JITC testing, etc.).
2. Bottom-Up System – This is the origination of data, whether from a sensor, human node, database, unmanned system, etc. (Smart Sensor Networks, Human Nodes, Unmanned Systems, Smart Distributed Systems, AI, Sensor Fusion, Mobile Wireless Ad-Hoc Networks, etc.).
3. Middle System – This is the smart push/smart pull (connecting the top-down and bottom-up systems: from a top-down system understand how to intelligently pull information/data of interest and from a bottom-up system understand how to push information/data of interest).
4. Disadvantaged Users System – every Network-Centric System must be able to extend to and from a system that cannot "push/pull" because of the wrong communications, security, or because of

choice, i.e. stealth (extend to/from disadvantaged users for communications to the tactical edge).

In addition, in order to integrate these four overlapping systems, the Network-Centric Systems Engineering (NCSE) Core (the "trunk") is required. The NCSE Core is composed of: fundamentals of networking, communications, distributed computing, real-time processing, cyber security, data backup etc. This is the main problem discovered, the trunk (the NCSE Core) and all four systems, are often missing when you talk to various people in this world, but it's what is required to implement this network-centric world. Understanding this Network-Centric System of Systems Infrastructure (the four systems and the NCSE Core), one can scale out to as much detail as needed (e.g. into the branches and leaves). Interestingly, if you look at the tree (Fig. 13), and cover up the trunk of the tree (the core), it looks like each system is separate from each other; they each look like their own tree (not a part of each other); this is a "typical" problem in implementing Network-Centric Systems. If you talk to any one person, they usually live somewhere in the branches (or the leaves) of one approach. It is not that any one approach is wrong; they just need to be integrated together through a core systems approach. The core is what hooks them together.

Another view of the Network-Centric System of Systems "Tree" can be seen in Fig. 14. The bottom-up and top-down systems need to be connected through a middle system, the push and pull (also known as publish and subscribe or produce and consume). This middle system needs to be intelligent, hence the smart push/smart pull. A person usually comes from the smart push world (the bottom-up system) or the smart pull (top-down system), but one rarely is involved in both worlds; both worlds (systems) are required to implement a Network-Centric System of Systems, therefore, requiring the middle system and the NCSE Core. In order to implement this network-centric world, you must design and implement each of the four systems and this NCSE Core and then extend into the branches (and then leaves) for more detailed design and implementation. One should understand all four systems and the NCSE Core, and how they integrate together. In addition, one must be able to transpose any stove-pipe technology or terminology onto this model (these four overlapping systems and NCSE Core).

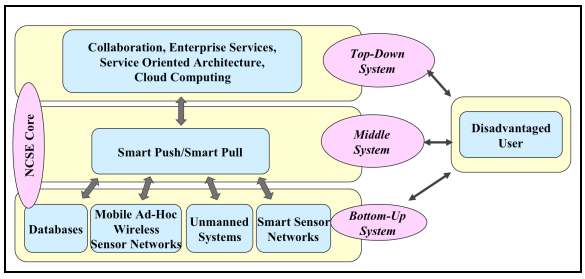


Figure 14. A Different View of Network-Centric System of Systems.

In addition, in any Network-Centric type of meeting or conference, there is the large concern for the disadvantaged user, the side-view. There will always be someone, or some GIG Node or system, on the tactical edge that needs to connect to this network-centric infrastructure, whether needing to share (push) information up, or get (pull) information down. Connecting to and from the disadvantaged user becomes a creative design process, and is a function of the requirements of the disadvantaged user and the capabilities the disadvantaged user has. A disadvantaged user could be disadvantaged for several reasons: limited communications, limited security, stealth missions, etc. In the figures above, the side-view of the disadvantage user system is also shown, needing to pull and/or push data/information of interest. Overall, 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 (i.e., the top-down system), is critical for GWOT and HLS threat prevention. Various communications architectures could be designed for "plug and play" for standardizing disadvantaged user interfaces, as seen in Fig. 15. The DoD and DHS should develop gateways that interface with common radios and convert the radio signals to and from IP (in order to interface with the GIG; as the GIG will most likely communicate through IP). The common radios could be the ten most common DoD radios, the ten most common DHS radios, the eight most common industry radios, plus develop two new ones. Gateways could be put in areas of operations, to handle most disadvantaged users. These gateways transfer signals to and from IP; once a signal is in IP, then it can communicate anywhere in the GIG.

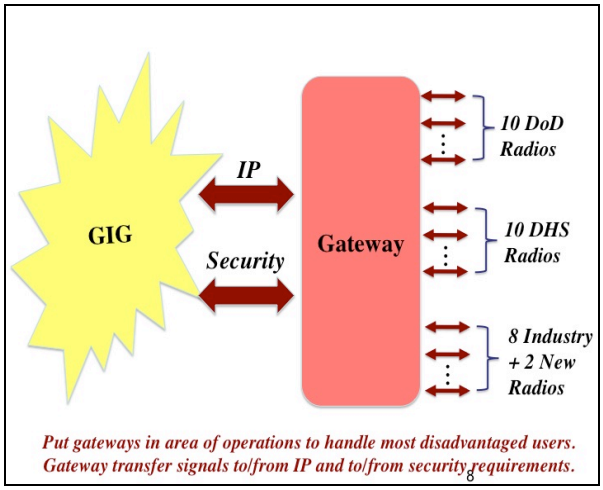


Figure 15. Disadvantaged user solutions. More gateway access increases the duration of communications with disadvantaged users when in communications, disadvantaged user nodes auto-synchronize data (push/pull)

C. Net-Centric Top-Down: Advanced Network-Centric System of Systems SOA/Cloud Infrastructure

In order for a network-centric system to be configured for each user group, mission, area of operation, sensor batch, and intelligence automation software, a set of Graphical User Interfaces (GUIs) are required at the top-down system, from SOA and Cloud Computing approach, seen in Figure 16. These GUI's will be defined and presented for intelligence automation applications. 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, identification, prediction, reaction of interest; then, automation algorithms would be generated automatically (behind the scenes; i.e., the operator does not program these) as seen in Fig. 17. These intelligence automation algorithms (of DIPR) are then pushed down onto the appropriate nodes. In other words, in order to automate intelligence extraction at those nodes and programming these nodes to push (from the bottom-up system) this intelligence, defined through the GUI, back to the analyst at the top-down system. These GUI's need to be simple and quick as new intelligence (i.e. potential threats) is discovered and needs to be implemented instantly. As missions change, an analysis needs to "drill" down and "re-program" to the bottom-up systems, what intelligence to look for.

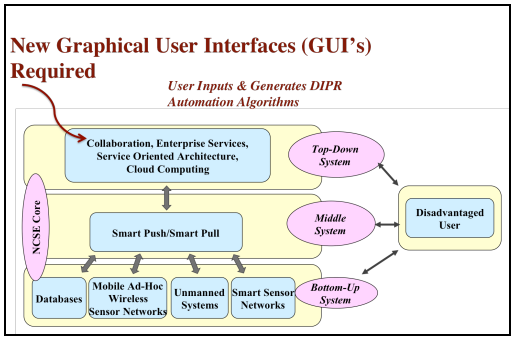


Figure 16. New Graphical User Interfaces (GUI's) Required at the Enterprise Level (Top-Down System).

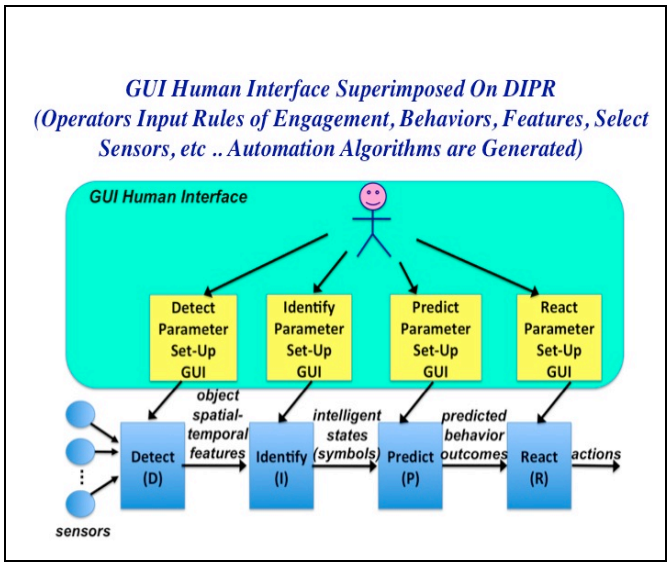


Figure 17. The need for GUI's for intel operators to input their missions, behaviors, rules of engagement and select sensors, which allows for intelligence automation behind the scenes.

D. Cyber Security and Warfare Required for Network-Centric System of Systems

A part of the infrastructure for a network-centric system of system is the need for cybsersecurity. As presented in Section IV.B, cyber security is part of the NCSE Core (Fig. 13). As cybersecurity behaviors are becoming more complex and dynamic in threat, it is recommended that automated cyber security be implemented through using the DIPR hierarchical intelligence automation mindset (presented in Section II). It should be automated and go through the behavior prediction and reaction stages. Intelligence automation framework of DIPR is used to automate "cybersecurity experts" to maintain a secure SoS and prevent potential cyber attacks (see Fig. 18 for DIPR automating cyber analysts). The Future of Cybersecurity and Cyber Warfare is Intelligence Automation, Automating Cyber Analysts, within network-centric smart sensor system of systems. Automating cyber analysts includes the automation of learning new enemy tactics, techniques, and procedures (TTPs).

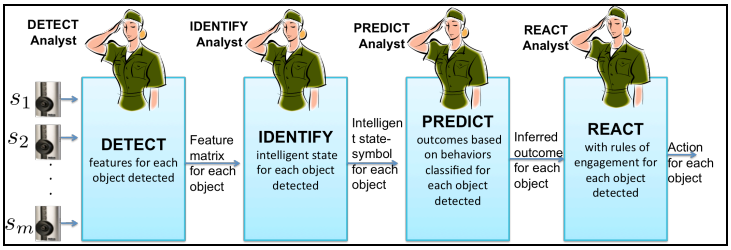


Figure 18. DIPR for Automating Cyber Analysts (for both cyber security and warfare).

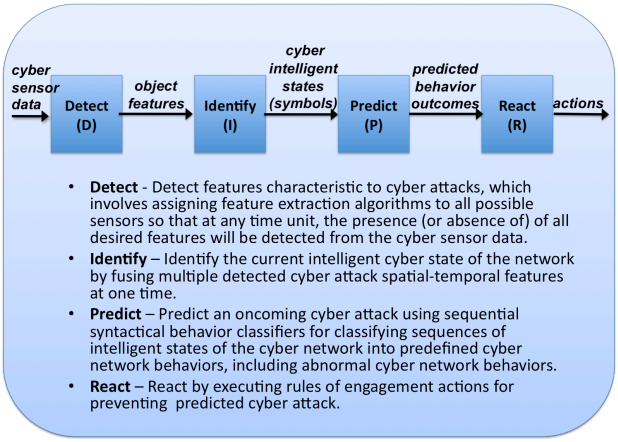


Figure 19. DIPR Example for Cyber Security.

In addition to modeling offensive cyber behaviors, the DIPR 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 order to detect threat within blue force networks. Figure 19 provides context of using DIPR for cyber security. In addition, the same intelligence automation framework can be used to automate "cyber warfare experts" to infiltrate and take-down an enemy network SoS. In this case, reactions would be part of the warfare tactics on enemy systems.

V. NEW AND ADVVANCED SENSORS AND ARCHITECTURES

The fourth approach necessary for automating intelligence systems requires the need for introducing advanced and innovative sensors and software that capture information and extract intelligences that humans usually sense and extract. Sensors are going down in cost and size and increasing in type. There are signals that could be detected, processed, characterized to assist in intelligence automation applications. Therefore, there is a need for new and advanced sensors for intelligence automation applications.

A. New and Advanced Sensors

If the sensor does not exist to collect signals that humans or animals analyze, automation for that intelligence extraction cannot occur (see Fig. 20). Therefore, sensors need to be developed, whatever sensors are required to detect the information needed to obtain intelligence about whatever you're concerned about (i.e., whether it's chemical, biological, detection of terrorist, etc …); there are sensors that can help automate gathering the information to predict threats. 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 pan 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. In each case, once the sensors are there, it will become an overwhelming bottleneck of data, and require intelligence automation.

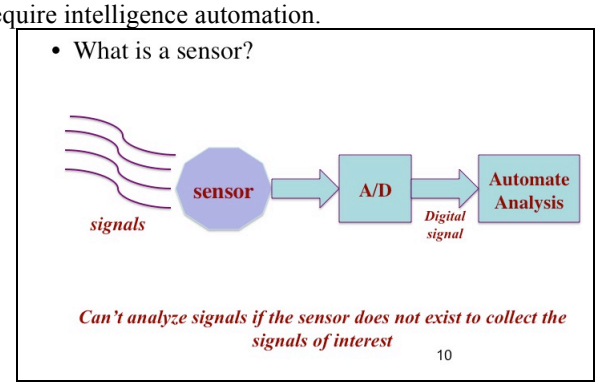


Figure 20. Need to develop signals in order to analyze the data.

Sensors are going down in cost and size and increasing in type. Various sensor platforms are to be used, from fixed to mobile. In fixed platforms, various sensor architectures exist. In addition, in mobile sensors, such as unmanned systems, robotics, various architecture exist. Additionally, humans may act as a sensor and output their intelligence products in standardized methods. Outputs of all type of said sensors relates back to the need for GIG node standardization and the presented DIPR intelligence automation infrastructure.

Sensors are still evolving. Typically, sensors mimic human sensors, such as "eyes" through cameras, "ears" through microphones, "nose" through smell sensors, etc. However, other irregular sensors exist, picking up signals that animals can sense, but humans cannot sense, such as infrared, magnetic, sonar, etc. Thus, new sensors need to be developed that can answer such questions as, "can you detect fear? can you detect/predict evil?" This is the ultimate goal in predicting and preventing terror in the GWOT and HLS and research is already underway. The world of "feeling" fear can be detected down in the infrasonic world, where animals communicate [20]. Sensors are being developed to collect signals at this frequency and then automation of feature extraction and intelligence can occur. A new world of sensor developments will occur in order to collect information we need for intelligence to predict terror threats.

Sensors need to be defined as new threats are being defined. Because the intelligence automation can be generalized into levels of intelligence and because of standardizations within a network-centric system of systems infrastructure, sensors can be customized per application/threat. For example, 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

Finally, with the increase in new sensors, comes the reminder of the need for automating intelligence from sensor data. Currently, intelligence is made up of mostly human intelligence, inputted manually into the GIG, and intelligence officers/analysts analyzing and predicting. Once the sensors are there, they must comply to the GIG Node standards, defined in Section III. 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.

B. Embedded Architecture Model for Intelligent Sensor Node with Applications Utilizing Multi-core DSP Platforms for DIPR Systems

With the increasing need of software for automating intelligence extraction from increasing number of new sensors, comes the requirement for a scalable hardware infrastructure. Fig. 21 suggests a scalable, embedded architecture to handle intelligence automation for a group of sensor nodes, including the need for an Intelligent Node Management System. The hardware for carrying the Intelligence Automation needs to be vast, distributed and independent of any particular computer architecture. Products can be organized around a network centric architecture, without any fixed need for any of its hardware/software products or systems to locate at a particular node in a net centric architecture. The computer organization in Fig. 21 could be implemented with an array of DSP computers, with or without, a selection of optional FPGA products to enhance the performance of the various algorithms that can run with various software or firmware performances. Additional load sharing/optimization node software could be used where varying load/overload handling requirements are needed.

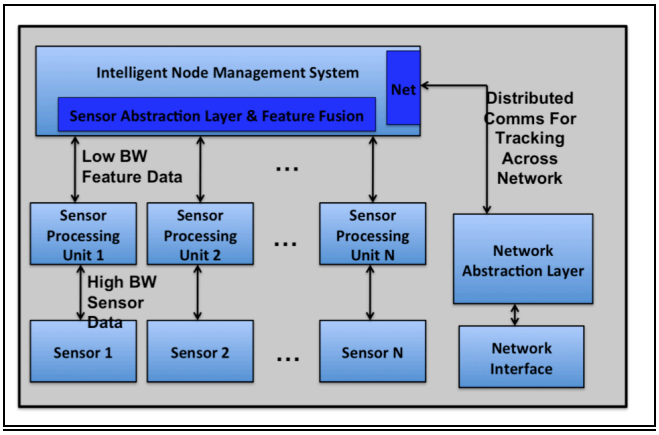


Figure 21. Intelligent Sensor Node Architecture.

VI. CONCLUSION

To conclude, this paper presents the need for intelligence automation, from the GWOT/HLS, economic crisis and consumer views. Automation must be carried, through four approaches. The four approaches presented in this paper were as follows: (1) DIPR; (2) interoperability through standardization; (3) network-centric system of systems infrastructure (how to organize data and intelligence and actively "reprogram", through Service Oriented Architectures and smart cloud computing graphical user interfaces, the sensor systems connected to the cloud, as intelligence needs are updated); and (4) new/advanced sensors and architectures to support ongoing intelligence automating systems.

The paper was to be a standalone educator and guide in attempt to solve the problem of augmenting and automating human intelligence in distributed sensor systems connected to the top-down system of smart cloud computing. In addition, future areas of intelligence automation that were not presented in this paper are to appear in the upcoming book. These areas continue to add awareness to the reader and help prepare the reader for future areas of intelligence automation.

REFERENCES

[1.] Deborah Goshorn, Rachel Goshorn, Joshua Goshorn, Lawrence Goshorn. "Abnormal Behavior Classification and Alerting through Detection, Identification, Prediction and Reaction (DIPR) System Applied to a Multi-Camera Network." German Conference on Artificial Intelligence, Workshop on Behavior Monitoring and Interpretation, September 2009.

[2.] R. E. Goshorn, D. E. Goshorn, J. L. Goshorn and L. A. Goshorn, "Behavior modeling for detection, identification, prediction, and reaction (DIPR) in AI systems solutions," Handbook of Ambient Intelligence and Smart Environments, H. Nakashima, Hamid Aghajan and J. C. Augusto, Eds., Springer, 2010. ISBN 978-0-387-93807-3

(Print) 978-0-387-93808-0 (Online). http://www.springerlink.com/content/n812r0064785g764/. (Book chapter written in 2008).

[3.] Rachel Goshorn, Deborah Goshorn, Joshua Goshorn, and Lawrence Goshorn. "Abnormal Behavior-Detection Using Sequential Syntactical Classification in a Network of Clustered." Workshop on Activity Monitoring by Multi-camera Surveillance Systems (AMMCSS), 2nd ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC-08), September 2008, Stanford, California.

[4.] D. E. Goshorn, R. E. Goshorn, J. L. Goshorn and L. A. Goshorn, "Abnormal Behavior Classification and Alerting through Detection, Identification, Prediction (DIPR) System Applied to a Multi-Camera Network," Behavior Monitoring and Interpretation – Well Being Workshop, 32nd German AI Conference, September 2009.

[5.] R. Goshorn, J. Goshorn, D. Goshorn, and H. Aghajan, "Architecture for Cluster-based Automated Surveillance Network for Detecting and Tracking Multiple Persons." IEEE/ACM 1st Int. Conf. on Distributed Smart Cameras (ICDSC), Sept. 2007, Vienna, Austria.

[6.] Rachel Goshorn, Deborah Goshorn, "Vision-Based Syntactical Classification of Hand Gestures to Enable Robust Human Computer Interaction," Special Session on Vision Based Reasoning, 3rd Workshop on Artificial Intelligence Technologies for Ambient Intelligence (AITAmI'08), collocated with the 18th European Conference on Artificial Intelligence (ECAI08), Patras, Greece.

[7.] Rachel Goshorn, Deborah Goshorn, and Mathias Kölsch, "The Enhancement of Low-Level Classifications for Ambient Assisted Living." 2nd Workshop on Behavior Monitoring and Interpretation, BMI'08, collocated with the German Conference on AI 2008, Kaiserslautern.

[8.] Rachel Goshorn, "Syntactical Classification of Extracted Sequential Spectral Features Adapted to Priming Selected Interference Cancelers", University of California San Diego, Electrical and Engineering Department (Intelligent Systems, Robotics, & Control), ECE Ph.D. Dissertation, UCSD, June 2005.

[9.] Rachel Goshorn, "Sequential Behavior Classification Using Augmented Grammars." ECE M.S. Thesis, UCSD, June 2001.

[10.] Deborah Goshorn, "The Systems Engineering of Network-Centric Distributed Intelligent System of Systems for Robust Human Behavior Classifications." Ph.D. Dissertation, UCSD, June 2010.

[11.] Deborah Goshorn, "Enhancing Low-Level Classifiers Including Parts-based Object Recognition Classifiers on Field Programmable Gate Arrays (FPGAs) for AI Systems Engineering." Computer Science C.Phil., UCSD. Spring 2009.

[12.] Deborah Goshorn, "The Enhancement of Low-Level Classifications in Sequential Syntactic High-Level Classifiers." Computer Science PhD Research Exam, UCSD. August 2008.

[13.] Deborah Goshorn, Shahnam Mirzaei, Junguk Cho, Ryan Kastner. Field Programmable Gate Array Implementation of Parts-based Object Detection for Real Time Video Applications International Conference on Field Programmable Logic and Applications. (FPL'10) Milano, Italy, Aug. 31st - Sep. 2nd, 2010.

[14.] Deborah Goshorn, Rachel Goshorn, "Cybersecurity in a Smart Environment Network-Centric System of Systems CyberSecurity," Workshop, Cyber Summit, Naval Postgraduate School October 2009.

[15.] Joshua Goshorn, "Distributed Framework for Object Tracking Applications Utilizing Wireless Multimedia Sensor Networks with Constrained Resources." Ph.D. Dissertation, UCSD, Summer 2011.

[16.] J.L. Goshorn, "Embedded Architecture Model for Intelligent Sensor Node with Applications to Vision Utilizing Multi-core DSP Platforms," International Conference on Distributed Smart Cameras (ICDSC-2009).

[17.] Joshua Goshorn, "Predictive Measurement-based Admission Control Algorithm." M.S. Thesis, UCSD, June 2005.

[18.] Rachel E. Goshorn, "FINDINGS FOR NETWORK-CENTRIC SYSTEMS ENGINEERING EDUCATION". MILCOM, November 2008: Net-Centric Enterprise Systems and Services Classified Sessions.

[19.] Drew, Christopher. "The Military is Awash with Data from Drones." New York Times. 10 JAN 2010. http://www.nytimes.com/2010/01/11/business/11drone.html?pagewanted=1.

[20.] "Infrasound." http://en.wikipedia.org/wiki/Infrasound.