Allocation of data mining resources: A system partitioning and hybrid control framework

John R. James
United States Military Academy
Department of Electrical Engineering and Computer Science
West Point, NY 10996

Abstract

This paper provides an approach for allocation of data mining resources. The ideas are an extension of earlier efforts to base analysis of information assurance for complex systems on system partitioning into a system of systems. Composition of components requires consideration of interaction of subsystems, especially when feedback loops are present. A model of Information Assurance (IA) processes consistent with this hybrid system model of complex processes is described. Information dominance is defined as superior situation understanding and superior support for making decisions under uncertainty. The approach is discussed in terms of modeling the information dominance problem of military systems as representative of modeling other complex systems. The information dominance model is then presented as an extension of the IA model. The paper provides a conjecture that more effective intrusion detection can be achieved by using the known purpose of an information system (e.g. achieving information dominance in support of an operation) to guide allocation of data mining resources.

1. INTRODUCTION

The phenomenal growth of networked information systems has created significant opportunities for increased efficiencies and associated opportunities for mischief. For military systems, this is reflected in the intent of the United States forces of the future to exploit increased knowledge of friendly and enemy forces (also known as information dominance) and the associated problem increased vulnerability of future forces to deliberate or inadvertent manipulation of friendly and enemy information. For medical systems this is reflected in the expanding capability for monitoring, diagnosing, and predicting patient or group status and associated concerns related to individual privacy or group discrimination. Similarly, for power, telecommunications, finance or other complex systems, there is an increasing reliance of these critical infrastructure systems processes on networked information systems and associated vulnerabilities to deliberate or inadvertent information systems failures. This paper presents a view of these complex systems as compositions of systems of systems and proposes a new model of information assurance processes associated with either discrete or continuous system components.

Previous Information Assurance (IA) models have ignored the continuous systems aspects of modeling complex systems. This paper presents a modeling approach that allows including continuous system models when appropriate.

In this paper we discuss explicit modeling of the reliability of information maintained on the state of complex systems. The approach discussed for modeling IA components of military systems rests upon the notion that the system at hand is intended to achieve some useful purpose and that a system of systems approach provides a feasible methodology for composing the system as an aggregation of sub-systems. The notions of purpose and system of systems lead to the need to understand the behaviors of the system and its component sub-systems, especially as those behaviors are modified via reactive control to continue meeting the system purpose while reacting to malicious IA activities. Thus, the modeling approach must support capturing process and sub-process behaviors. Maintaining trust of the information being presented is absolutely essential for military planning and re-planning processes and is impossible to achieve unless an effective approach for Information Assurance, including risk management is in place.

---

This work was partially supported by an endowment establishing the Adam Chair in Information Technology. The views expressed herein are those of the author and do not purport to reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense.
2. ORGANIZATION OF THE PAPER

The next section provides an overview of a modeling framework for analysis of military processes. Military operations depend upon reliable operation of many critical infrastructure processes and the framework discussed is consistent with modeling these infrastructure processes as well as the military processes that depend on their reliable operation. An enterprise architecture is considered to have several views: an operational view of the users, a systems view of the hardware and software implementation, and a technical view of the underlying standards and interoperability protocols. The section has four subsections:

- Operational Architecture
- Technical Architecture
- Systems Architecture
- Information Assurance modeling

Section four then extends the modeling framework of section three to consider Information Dominance. Section five discusses resource allocation for intrusion detection and section six summarizes the paper.

3. MODELING FRAMEWORK

The modeling framework described here applies the hybrid automaton ideas of hybrid control theory to model military operations. The approach features construction of agents to coordinate interactions of components that are composed to form the system of systems of a force structure planning and executing a military operation. This approach is general enough to capture the complexity of military operations as well as the interactions of military system components with supporting infrastructure processes. The framework also provides a rigorous way of restricting the set of hybrid trajectories to a collection of discrete and continuous variables. The general approach is mathematically rigorous and, at some point, may support automatic generation of system of systems solutions. However, current tools support the constructive assembly of components of known models into progressively more complex systems of systems and adaptive control of the (well-understood) composed system. This approach also supports development of verification and validation methods for a system-of-systems of autonomous enterprise agents since a necessary step in the composition process for composed systems is the satisfaction of independence of components constraints except where feedback loops are allowed. Thus the basic agent in a modeling and simulation framework is a hybrid automaton [2] that is a collection:

\[ H = (X, V, Init, f, Inv, R) \]

where

- \( X \) is a finite collection of state variables. We assume \( X = (X_D \cup X_C) \) with \( X_D \) countable and \( X_C \in \mathbb{R}^n \), an n-dimensional, real-number vector space;
- \( V \) is a finite collection of input variables. We assume \( V = (V_D \cup V_C) \) with \( V_D \) countable and \( V_C \in \mathbb{R}^n \);
- \( Init \subseteq X \) is a set of initial states;
- \( f : X \times V \rightarrow X_C \) is a vector field, assumed to be globally Lipschitz in \( X_C \) and continuous in \( V \);
- \( Inv \subseteq X \times V \) is an invariant set;
- \( R : X \times V \rightarrow 2^X \) is a reset relation.

We refer to \( x \in X \) as the state of \( H \) and to \( v \in V \) as the input of \( H \).

Associated with this model are rigorous definitions of continuous and discrete states and associated models of continuous behaviors and discrete behaviors and hybrid (combination of continuous and discrete) behaviors. These behaviors consist of continuous, discrete and hybrid trajectories from a set of initial states to a set of final states. The complete power of the hybrid modeling approach is not needed for each component. For some (maybe most) of the components, a discrete model is sufficient. Likewise, for some components, a continuous-system model is sufficient. The hybrid model is used when the composed system has both discrete and continuous components.

The hybrid automaton modeling approach has been developed within the control community for analysis, design and implementation of distributed control systems. The technology enables a more rigorous analysis of the middleware approach for distributed system development whereby applications use well-defined interfaces to access services from other local and distributed applications (the middleware) to provided their own functionality.

The development of military information systems is guided by interacting ideas of purpose and process. For military systems, the purpose is set in the Joint Vision 2020 declaration of achieving information superiority. The process is summarized in the view of the enterprise architecture as the view of a set of interacting
architectures described in the Army Enterprise Architecture (AEA) of Figure 1 [3].

Thus, we expect to observe in fielded implementation architectures (i.e. the hardware and software present in units vary according to System Architectures for specific units) a “normal” flow of information corresponding to the battlefield processes of a given unit (i.e. the input-output characteristics correspond to the Operational Architecture specified for the unit) which complies with the implementation standards required for the signal being observed (i.e. the transmission characteristics comply with the Technical Architecture of the unit being observed). The AEA provides the framework for life-cycle system management of Army information technology systems, including Army Command, Control, Communications, Computers, and Intelligence (C4I) systems and installation operations systems.

### 3.1. Operational Architecture

The Operational Architecture (Figure 2) captures the operational processes supporting the purpose that is captured in the mission statement for a given operation.

One way of viewing the elements of the operational architecture is to capture the relationships between the organizational partitioning of the force structure and the functional partitioning of the force structure. An example of this is the Conceptual Model of the Mission Space (CMMS) approach (see Figure 2) that has been developed by the Defense Modeling and Simulation Office (DMSO). The basic idea is to provide a crosswalk between the functional partitioning of tasks (functional entities) to be performed at each level in a hierarchical structure and the force structure components (physical entities) that take actions to accomplish the functional tasks. Our system state identification problem is then to filter the observed signals into appropriate sets of data for the unit being analyzed and to compare known patterns for separable components to patterns observed in the data being analyzed. Unit entities take actions to achieve behaviors needed to cause the current system state to move to a desired system state. Metrics are needed to determine closeness of observed patterns to expected patterns. Anomalous activity is then indicated (detected) when differences exceed some user-determined threshold.

### 3.2. Technical Architecture

The technical architecture provides the underlying standards and protocols from which the system components are constructed. One way of separating the technical architecture components is by focusing on those services that provide access to the computing platform and on those services that provide support to applications. The Department of Defense technical

---

**Figure 1.** Army Enterprise Architecture (AEA)

**Figure 2.** The Conceptual Model of the Mission Space (CMMS) view of an Operational Architecture
architecture takes this approach, which is similar to the layered approach taken by the Open Systems Interconnection (OSI) model for modeling distributed networked systems. The Army Technical Architecture for Information Management (TAFIM) Technical Reference Model (TRM) [4] is shown in figure 3. The TAFIM TRM organizes software into two entities, an Application Software Entity and an Application Platform Entity. The Application Software Entity communicates with the Application Platform Entity through an API. The Application Platform Entity communicates with the external environment through the External Environment Interface (EEI). The TAFIM TRM decomposes these entities into subcategories as shown in Figure 3. Currently, these ideas are expressed as a set of specifications for the Defense Information Infrastructure Common Operating Environment (DII–COE). The various mandates of the DII-COE establish the operating system and communication system constraints for interconnecting defense information systems.

3.3. Systems Architecture

A Systems Architecture (SA) is a description, including graphics, of the systems and interconnections providing for or supporting a warfighting function. The Army systems architecture for Force XXI envisions support for both installation applications and force structure applications. A high-level SA view is shown in Figure 4 and provides a summary of relationships between strategic, operational, and tactical information systems, including the links envisioned between installation (fixed) and tactical (mobile) networks.

Figure 3. The Technical Architecture

A low-level SA view in shown Figure 5 and provides an overview of administrative/logistics and command and control networks in an armor company. In Figure 5, the command and admin/log nets are voice, single-channel radio systems with limited range (i.e. they are frequency-modulated (FM), line-of-sight radios) with capability of limited data transmission. The Extended Position Location Reporting System (EPLRS) portion of the Future Battle Command, Brigade and Below (FBCB2) system provides situation awareness at company level through automatic dissemination of position information as well as automatic distribution of other selected information (e.g. selected activity and status information).

Figure 4. Command and Control Systems From Strategic Through Tactical Level

Figure 5. Administration/Logistics and Command/Control at the Company/Platoon Level
While armor companies do not have organic multichannel radio systems, Patriot batteries do have a Mobile Subscriber Equipment (MSE) Small Extension Node (SEN) multi-channel radio system. Major changes to current communication systems will occur when the Warfighter Information Network –Terrestrial (WIN-T) and Joint Tactical Radio System (JTRS) are fielded. WIN-T and JTRS will enable more flexible achievement (more widespread use) of tactical internets during joint force operations.

3.4. Information Assurance Modeling for Military Systems

Current ideas for reacting to malicious network activity apply fundamental ideas of control system science to consider the ideas of feedback loops and reactive control to compensate for anomalous events due to malicious activity. These ideas are based on the observation that a protection activity is often based on a sequence of sense, decide, act as a means of adapting to new circumstances. Adaptive network security is advocated by Internet Security Systems [5], a prominent provider of commercial products for network security, as a necessary approach for securing commercial enterprise networks against malicious attacks. ISS recommends a Detect, Monitor, Respond sequence for managing network attacks. Since military communication architectures are deliberately designed to change over time, degradation and enhancement of network information processing capability over time will be a characteristic of unit operations. Consistent with the discussion of the preceding paragraph, a unit’s ability to detect, monitor, and respond to IO attacks should be based on: a risk assessment of unit vulnerabilities, a deliberate decision concerning an acceptable level of risk [6], and methodologies to achieve that level of risk in unit information systems.

For example, a detect, monitor and respond capability is a necessary element of the Autonomic Information Assurance [7] project of the Defense Advanced Research Projects Agency (DARPA). The AIA project envisions a reactive capability to respond to an IO attack (see Figure 6) predicated on an ability to estimate the current state of the battlefield processes being monitored.

Given that military information systems are planned to evolve over time in synchrony with the changes of the force structure and the missions being executed, and also given the fact that the system itself is expected to change under attack, the Information Assurance Model must support this evolutionary process. The minimal capabilities include estimating (detecting) the current system state, comparing the current state to a desired state (monitoring), and selecting an appropriate response (reacting) when the system deviates “too far” from the desired state. A model that supports this set of modeling requirements is shown in Figure 7.
models change over time through a verification and validation process which explicitly supports changing the model in compliance with the constraints of the operational, technical, and systems architectures. As indicated in a recent paper in modeling Information Assurance, the original model of John McCumber [8] to capture Information security (INFOSEC) modeling requirements was later extended by him to accommodate the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC). The work of Maconachy et al. [9] extends McCumber’s work and addresses the problem that, in their words, “INFOSEC has evolved into Information Assurance (IA). This is more than a simple semantic change … In today’s information intensive environment, security professionals have expanded the scope, and thus the understanding of information and systems protection under an umbrella term referred to as IA.” The model of Maconachy et al. includes the Information States, Security Services, and Security Countermeasures of Figure 7 and also the notion that these entities change over time. This Information Assurance Model of Figure 7 is a modest extension of the work of Maconachy et al. to add the notion of Security Maintenance (the sense, decide, act idea of reactive control) and to explicitly consider some verification and validation mechanism to enable specification, analysis, design, implementation, test, and maintenance of Security Services in the context of system purpose which enables construction of some optimality criterion for use in deciding how to evolve the system.

4. INFORMATION DOMINANCE MODELING

Information dominance involves use of superior battlespace knowledge and superior decision-making capability to achieve the goal of consistently “getting inside the decision cycle” of opposing forces. Thus, we define Information Dominance in terms of three essential services to achieve this goal: situation-assessment support, military-decision-making-process support, and truth-maintenance support. Dominance in each of these services is needed in order to consistently and reliably “get inside the decision cycle” of adversaries. It should be noted that lack of dominance in any one of these three services may render dominance in the other two useless in terms of meeting the goal of enabling commanders to “see the battlespace” better than opponents and apply that knowledge to more effectively command friendly forces by making better decisions under uncertainty than opposing force commanders. Thus, a slight extension of figure 7 results in the model of information dominance processes represented in figure 8.

Note that the only addition to Figure 7 has been the notion of what constitutes Information Dominance for military operations. Thus, while Figure 7 is appropriate for estimating those elements of the state of an information system that are of interest for general enterprise processes, Figure 8 adds consideration of the situation-assessment, decision-making, and truth-maintenance processes which indicate that one military force dominates another in terms of information management processes.

5. A CONJECTURE FOR RESOURCE ALLOCATION

This section provides a conjecture that more effective intrusion detection can be achieved by using the known purpose of an information system (e.g. achieving information dominance in support of an operation) to guide allocation of intrusion detection resources.
5.1. Conjecture

The conjecture is stated in the form of cost-based allocation of intrusion detection resources to maintain acceptable levels of risk that enterprise knowledge has been compromised. The underlying assumption is that malicious activities will be deliberately concentrated in a manner reasoned to degrade achieving system purpose so that an effective use of available resources would be to focus detection activities upon those intrusion techniques that support that end.

The notion is that:
- There is a value chain of information based on support for enterprise processes,
- There is an associated increase in entity value in moving up the value chain from data to knowledge,
- Knowledge varies from enterprise to enterprise,
- Conjecture: Intrusion Detection will be more effective if explicit efforts are made to allocate Intrusion Detection Resources to support efforts to maintain acceptable levels of risk that enterprise knowledge has been compromised.

5.2. Military Example:

For the military, a value chain that has high-priority is the set of events that result in authorization to use deadly force:
- Deadly force is largely applied by officers in the Navy and Air Force and by units for the Army and Marines (i.e. officers make the decision to engage in the Air Force and Navy while soldiers in units make decisions to engage in the Army and Marines)
- Information Assurance resources (including Intrusion Detection resources) should be allocated to maintain an acceptable level of risk that application of deadly force to support meeting the commander’s intent has not been compromised.

Conjecture: Intrusion Detection resources will be more effectively used if they are allocated to support the priority of effort by phase to achieve the commander’s intent. This conjecture rests upon the assumption that a knowledgeable enemy will concentrate malicious activities upon those friendly assets most useful to meeting the commander’s intent that is the purpose for use of deadly force. Also, even in the absence of a knowledgeable enemy concentrating effort against the most critical assets, providing priority of effort to those information system elements critical to the task at hand will reduce the risk that those assets will be compromised.

Say there is some metric for determining degree of attainment of system purpose:
- Completely attained
- More than Adequately Attained
- Adequately Attained
- Less than Adequately Attained
- Minimally attained.

Then, to the degree that measures are available to indicate closeness to achieving system purpose and also that measures are available for estimating the relative contribution that elements in a knowledge value chain make to achieve the system purpose, then a cost-based allocation of resources can be made to protect, in priority, those assets which contribute the most to completion of enterprise purpose.

5.2.1. Military Example continued: Consider the value chain associated with applying deadly force to achieve the commander’s intent for the operation outlined in Figure 9.

Currently, an Army Brigade (about 4000 soldiers) is the level at which the information systems represented by Figures 4 and 5 are integrated. The companies (about 100 soldiers) of an Army Battalion (about 500 soldiers) use the communications equipment shown in Figure 5 to...
automatically share **situational awareness** data and to implement required analog and digital communication networks.

Figure 9 summarizes the Battalion Commander’s intent to seize objective Falkirk. The graphic constraints for this portion of the operation indicate that D Company of 3rd Battalion, 67th Armor will attack along Route purple, occupy Support By Fire Position 4D and provide covering fire for an element of A Company 588th Combat Engineers to make a single-lane breech of a minefield. Company D will then conduct a passage of lines of the engineer element and continue the assault along Route Purple to seize objective Falkirk. Not shown is a diversionary supporting attack by another Company of 3/67 Armor.

One top-level partitioning of information system components is into two sets: one set for those sub-systems associated with **administration and logistics** and one set for those sub-systems associated with **force-level control** (command and control).

5.2.2. Information value chains for different phases of an operation Prior to commencement of the attack, those Battalion-level systems that enable **administration and logistics** functions have a relatively high priority since the forces will not be ready to achieve the commander’s intent unless they are fully manned by trained and qualified personnel operating the required sets of equipment.

As the time for commencing the attack draws close, those Battalion-level information assets that allow commanders and staffs to understand the current locations and activities of friendly and enemy forces (i.e. the **intelligence estimation** assets of force-level control) will have a relatively high priority.

Once the attack begins, those Battalion-level information systems that enable **force level control** functions will have a relatively high priority. The force-level control functions are those that position the company (15 tanks) and platoon (four tanks) elements for application of deadly force as well as those systems that coordinate requests for supporting fire. Deadly force is applied by the combat-crew (tank) level and by supporting fire elements (mortars, artillery, aircraft, …). The Army uses a synchronization matrix to summarize the activities required by different force structure elements during different phases of an operation. The **synchronization matrix** provides a means for constructing metrics to estimate whether subordinate units of a given unit have met time and spatial constraints for achieving a **commander’s intent**. Thus, by phase and unit by echelon, we can estimate if goals are being: completely attained, more than adequately attained, adequately attained, less than adequately attained, or minimally attained.

The joint force information presented in different contexts to different individuals should address the needs of the user. This is particularly true in the case of engagement decisions where the different views of the common operational picture should reflect the fact that engagement decisions are made primarily by officers in the Air Force and Navy and primarily by combat weapons crews in the Army and Marine Corps. Estimates of the relative importance of different information system elements will require **on-line identification of system state** since the information system architecture (like the force structure it supports) will change as an operation proceeds. Changes will occur at the network level, at the middleware level, and at the application level. If we are to have automated assistance in estimating compliance of plan execution with plan formulation we need a modeling and simulation capability like that outlined in the next section.

5.2.3. Some specific variables to estimate system state Consider what would be needed to maintain an estimate of whether the operation summarized in figure 9 is “on track”. Suppose the commander has indicated that the time at which the occupation of the support by fire position occurs (T_{CO\text{-}SBF4D}) and the time at which the event “PLT-Breach” occurs (T_{PLT\text{-}Breach}). Using the Situational Awareness (SA) traffic to create such templates is the first step in being able to link sensed unit activities to the commander’s Concept of the Operation.

An information flow needed to build and apply such templates is:

\[ \Delta T_{Focus} = T_{PLT\text{-}Breach} - T_{SBF4D} \]

It should be noted that the time at which events occur, the location at which events occur, as well as the impacts events have on operational outcomes are not certain but have associated uncertainties. Thus, while an understanding of the temporal and spatial dynamics surrounding execution of operations by battlefield operating system (BOS) is needed to be able to determine the data mining priorities; the representation, analysis, and propagation of belief support for occurrence and impact of events is also needed.
(2) Determine the center of mass of the Team Dawg elements, by echelon (i.e. combat vehicle, platoon, task force), occupying SBF4D.

Declare the center of mass to be: $\text{Team } _{\text{DAWG}} \text{Center}$

(3) Determine when TF 588th Combat Engineers begins and completes the passage of lines through SBF4D by:

- Searching at time $T_{SBF4D}$ to identify the position of TF 588th Combat Engineers in the vicinity of SBF4D (i.e. within radius of the center of mass $\Delta_{\text{Vicinity}_{SBF4D}}$ of those Team Dawg elements occupying SBF4D, where $\Delta_{\text{Vicinity}_{SBF4D}}$ is a parameter to be determined.

Declare the center of mass to be: $T_{588} \text{Center}$

- Determining the incremental change in position of all 588th Combat Engineers vehicles identified in step a by searching through the appliqué messages, starting at $T_{SBF4D}$ and incrementally stepping

through time in $\Delta T_{Applique}$ increments, where $\Delta T_{Applique}$ is a parameter to be determined.

- Determining when the center of mass of the 588th Combat Engineers conducting the breach operation is outside of: $\text{Team } _{\text{DAWG}} \text{Center} + \Delta_{\text{Vicinity}_{SBF4D}}$

Declare that time to be: $T_{\text{TF588 } \text{Passage } \text{Complete}}$

Declare the set of centers of mass to be: $\{T_{588} \text{Center}_1, \ldots, T_{588} \text{Center}_k\}$

Where $T_{588} \text{Center}_1$ occurs at time

and $T_{588} \text{Center}_k$ occurs at time $T_{\text{TF588 } \text{Passage } \text{Complete}}$

(4) Determine indirect and direct fire coordinated by Team Dawg to suppress enemy fire on TF 588th Combat Engineers during the time when the breach operation is in progress by:

Searching through the time period between $T_{\text{TF588 } \text{Passage } \text{Complete}}$ and $T_{SBF4D} + \Delta T_{Focus}$ to identify all Team Dawg calls for indirect fire on objective Falkirk to suppress enemy fire on TF 588th Combat Engineers while the obstacle is being breached.

Declare these indirect fire Calls For Fire to be: $\{\text{CFF}_1, \ldots, \text{CFF}_m\}$

Searching through the time period between $T_{\text{TF588 } \text{Passage } \text{Complete}}$ and $T_{SBF4D} + \Delta T_{Focus}$ to identify all direct fire engagements conducted by Team Dawg to suppress enemy fire from Objective Falkirk on TF 588th Combat Engineers while the obstacle is being breached.

Declare these Direct Fires to be: $\{\text{DF}_1, \ldots, \text{DF}_n\}$

(5) Determine incremental position updates of TF 588th Combat Engineers for breach of the minefield by:

- Searching backward in time from $T_{\text{PLT-Breach}}$ to identify position of TF 588th Combat Engineers in the vicinity of PLT-Breach (i.e. within radius of the center of mass of the mine obstacle, where $\Delta_{\text{Vicinity}_{PLT-Breach}}$ is a parameter to be determined and a constraint is that, when the time is calculated, all members of the platoon that completed the passage of lines and have not subsequently been disabled are present for the center-of-mass calculation.

Declare the center of mass upon start to be: $T_{588} \text{Center-Breach-Start}$

and the time at which the breach started: $T_{\text{Breach-Start}}$

and the center-of-mass upon completion to be: $T_{\text{588 } \text{Center-PLT-Breach}}$

- Determining the incremental change in position of all 588th Combat Engineers vehicles identified in step 5a by searching through the appliqué messages, starting at $T_{\text{Breach-Start}}$
and incrementally stepping through time in increments,
\[ \Delta T_{\text{Applique}} \]
where \( \Delta T_{\text{Applique}} \) is a parameter to be determined.

Ending the calculations of position updates when time \( T_{\text{PLT-Breach}} \) has been reached.

Declare the set of centers of mass to be:
\[ \{TF588_{\text{Center}_1}, \ldots, TF588_{\text{Center}_p} \} \]

Where \( TF588_{\text{Center}_1} \) occurs at time \( T_{\text{Breach-Start}} \)

And \( TF588_{\text{Center}_p} \) occurs at time \( T_{\text{PLT-Breach}} \)

The activities described above provide a required few “first steps” for agents to access and interpret information flowing from scenarios implemented on force-on-force, attrition-based model of combat operations. Similarly, preliminary analysis of any operation is necessary to enable agent-based detection of operations activities that are anomalous to those expected to be present in executing the commander’s concept of the operation.

Additionally, analysis of the set of anomalous events to make an assessment of whether the status of the execution is normal (Green), somewhat abnormal (yellow), or definitely anomalous (red) will require the agents to have a deeper understanding of what range of deviation from “normal” is expected before the activity becomes “abnormal” or “anomalous”. For simulated activities, message delay or loss can be used to simulate IO attacks. Such results would be at the application layer level of the AEA Technical Architecture since this is the level at which message traffic occurs. To make the assessment of anomalous activity “real”, the simulated environment should be made as close as possible to the actual environment of the “system of systems” that makes up the Army XXI Systems Architecture.

6. SUMMARY

We have discussed modeling the information dominance problem of military systems as representative of modeling other complex systems. The approach discussed rests upon the notion that the system at hand is intended to achieve some useful purpose and that a system of systems approach provides a feasible methodology for composing the system as an aggregation of sub-systems. Many subsystem processes have continuous process models while higher system models are usually discrete. Composition of components requires consideration of interaction of subsystems, especially when feedback loops are present. A model of Information Assurance (IA) processes consistent with this hybrid system model of complex processes was described. Information dominance was then defined as superior capability in situation understanding and making decisions under uncertainty. The information dominance model was then presented as an extension of the IA model.

7. REFERENCES