# A Computational Framework for Modeling Targets as Complex Adaptive Systems

Eugene Santos Jr.[a], Eunice E. Santos[b], John Korah[b], Vairavan Murugappan[b] and Suresh Subramanian[b]
[a]Thayer School of Engineering, Dartmouth College, Hanover, NH, USA; [b]Department of Computer Science, Illinois Institute of Technology, Chicago, IL, USA

## ABSTRACT

Modeling large military targets is a challenge as they can be complex systems encompassing myriad combinations of human, technological, and social elements that interact, leading to complex behaviors. Moreover, such targets have multiple components and structures, extending across multiple spatial and temporal scales, and are in a state of change, either in response to events in the environment or changes within the system. Complex adaptive system (CAS) theory can help in capturing the dynamism, interactions, and more importantly various emergent behaviors, displayed by the targets. However, a key stumbling block is incorporating information from various intelligence, surveillance and reconnaissance (ISR) sources, while dealing with the inherent uncertainty, incompleteness and time criticality of real world information. To overcome these challenges, we present a probabilistic reasoning network based framework called complex adaptive Bayesian Knowledge Base (caBKB). caBKB is a rigorous, overarching and axiomatic framework that models two key processes, namely information aggregation and information composition. While information aggregation deals with the union, merger and concatenation of information and takes into account issues such as source reliability and information inconsistencies, information composition focuses on combining information components where such components may have well defined operations. Since caBKBs can explicitly model the relationships between information pieces at various scales, it provides unique capabilities such as the ability to de-aggregate and de-compose information for detailed analysis. Using a scenario from the Network Centric Operations (NCO) domain, we will describe how our framework can be used for modeling targets with a focus on methodologies for quantifying NCO performance metrics.

**Keywords:** target modeling, complex adaptive systems, bayesian knowledge bases, information aggregation, information composition, network centric operations, self-synchronization.

## 1. INTRODUCTION

Recent advances in sensor and network technologies have led to a revolution in military affairs (RMA) in the form of Network Centric Operations (NCO)[1]. NCO aims to support a paradigm shift in the way warfare is conducted through the use of various sources of intelligence including advanced Intelligence, Surveillance and Reconnaissance (ISR) assets to collect and share information at various levels of the command and control hierarchy. The key advantage of adopting this paradigm is to move away from the top-down information sharing which is prevalent in traditional military organizations, and support a more dynamic fighting force based on the availability of more accurate situational awareness throughout the organization, including the units on the ground. In short, the network becomes a weapon. As militaries around the world, adopt the NCO paradigm, it becomes essential for military planners to develop computational models that can adequately represent the intricacies of such organizations. One particular challenge is that human actors are an integral part of the decision making process in NCO organizations which introduces a certain level of uncertainty in the overall system behaviors. In the same vein, military planners are also interested in modeling events and organizations of national interest, such as modeling drug cartels in Mexico[2] and military conflicts in Syria and Iraq[3], which are complex and have multiple levels, with each level consisting of components, of varying autonomy, interacting with each other. Traditional target modeling techniques, as exemplified by the research in the target tracking domain[4], takes a simplistic approach wherein such organizations are considered to be monolithic and the underlying sub-systems and their interactions are either ignored or simplified. Although the traditional techniques have been effective when considering systems whose behaviors are well understood, such as modeling the trajectory of a missile, it starts to break down when considering complex systems where the interactions between its components or sub-systems can lead to new and unexpected behaviors.

There has been a growing trend in moving away from traditional target tracking models to methods that consider the targets to be complex adaptive systems. Complex adaptive systems (CAS) theory[5] models a system as a combination of autonomous components or units which interact with each other to generate complex behaviors. Adaptivity, emergence and self-organization are the key properties[5] exhibited by complex adaptive systems. Adaptivity refers to the ability to modify existing behaviors or learn new behaviors through interactions with other units in the system and with their environment. The interactions of the autonomous units and their inherent adaptivity can give rise to new and unexpected system behaviors as part of a phenomenon observed in CAS, called emergence. The interactions also can lead to groupings of the units in a process called self-organization, which is responsible for spontaneous generation of structures at various spatial and temporal scales. This property lends a multi-scalar and multi-level organizational structure to complex adaptive systems, which incorporate additional modeling challenges. Although CAS theory provides a path forward, any modeling framework proposed for this domain should also deal with other critical challenges, such as the inherent uncertainty in system behaviors involving human actors, the incompleteness of intelligence and ISR information about the target and the need to model components and structures at various spatial and temporal scales. Traditional methods, which have greater success when modeling systems with homogeneity in component behaviors and interactions, start to break down when the components can transform itself by learning new behaviors. Moreover, these methods typically represent the components of the models as black boxes that make end-to-end system analysis, while providing the underlying reasons and explanations, difficult.

In this paper, we present a framework called the Complex Adaptive Bayesian Knowledge Bases (caBKBs), for modeling real world targets as complex adaptive systems while overcoming the challenges of incorporating real-time information from various intelligence sources. caBKB is an extension and generalization of a well-known probabilistic reasoning network methodology called Bayesian Knowledge Bases (BKBs)[6]. BKBs have been utilized to model a number of real world scenario such as cross-border disease spread model[7] and nation stability models[8, 9]. The strength of BKBs is its ability to systematically represent complex behaviors in terms of more fundamental behaviors which can be combined by using a mathematically rigorous fusion algorithm[10]. BKBs represent these behaviors in terms of conditional probability rules (CPRs), which unlike Bayesian networks, can be built with an incomplete knowledge of the conditional probabilities. Moreover, a rich set of tools, such as Bayesian updating and revision[6], can be used with BKBs to provide analysis and predictions. caBKBs extends the BKB framework by allowing for the decomposition of a random variable into one or more BKBs, to represent underlying components. This allows caBKBs to support modeling and analysis of system processes at various scales, levels and entities. One of the key contributions made by caBKB is providing a rigorous mathematical framework for representing the two ways for incorporating information from ISR assets and other intelligence sources into a target model, namely information aggregation and information composition. Information aggregation refers to the process handled in most traditional data fusion and target modeling methodologies and is concerned with the incorporation of new pieces of information while handling inaccuracies and possible inconsistencies. On the other hand, information composition refers to the formulation of new components, along with well-defined operations. Although caBKB provides the framework to represent the multi-scale, multi-level and multi-entity behaviors of a system, other aspects such as the underlying networking infrastructure, sensor and weapons systems, that enable information sharing and other NCO capabilities need to be modeled. In previous work, we presented a framework for performance modeling and analysis of NCO environments, called the Network Centric Operations Performance and Prediction (N-COPP)[11–13]. N-COPP adopts a component based architecture that allows for the formulation of the mathematical representations of the underlying networks, network dynamism models, analysis tools and prediction techniques in separate components, which can then be used in a plug-and-play fashion. One of the contributions in the paper is to demonstrate how N-COPP can be used with caBKB to represent network specific properties and behaviors while providing the ability to define new performance metrics and to provide analysis.

To motivate the capabilities of the caBKB framework, we also provide some initial work in using it to model Somali pirates, operating along the coastline in the Horn of Africa (HOA). Piracy in Somali waters grew out of the prolonged inter-clan conflict in Somalia that followed the collapse of the central government in the 1990s. The pirate groups, which started off as an ad hoc enterprise, have grown into a paramilitary operation with sophisticated employment of technology, organization and tactics. A key challenge is that these groups are not well understood and information about their makeup, hierarchy and operational tactics are scarce. The Somali piracy scenario presents unique modeling challenges that distinguishes it from other military scenarios. In the following sections, we provide a background into some of the relevant state of the art methodologies in target modeling before going into the details of the caBKB framework. We focus on the capabilities of caBKB to support information aggregation, and its ability to leverage representations, performance metrics and analysis tools of the N-COPP framework to model targets with NCO capabilities. Using the Somali piracy scenario, we provide an initial demonstration of the capabilities of caBKB by using it to model an important NCO performance measure called self-synchronization[14].

## 2. BACKGROUND

Modeling military targets have been studied in various domains ranging from filtering approaches for refining sensor information to building complex models to analyze military operations. Earlier works on modeling targets focused on estimating the state of a simple target based on the information obtained from a sensor[4, 15] and subsequent works focused on fusing information from multiple sensors[16, 17]. The advances in information technology and the evolution of network-centric warfare military doctrine over the past few decades have progressively given rise to works that focus on modeling military targets of increasing complexity based on approaches such as complex adaptive systems[5, 18] and system of systems[19]. One of the prominent approaches used in estimation and prediction of a target's position is applying one or more variations of the Kalman filter[15]. However, the Kalman filter cannot be applied to problems where the linear Gaussian assumptions fail to hold[4]. Extended Kalman filter and unscented Kalman filter are two extensions of the Kalman filter that can be used for target estimation when the linear Gaussian assumptions fail to hold. Although the original Kalman filter focused on estimating the target state from a single sensor, later works addressed fusing information from multiple sensors[20, 21].

Another important issue in target tracking is that targets movement consists of both maneuvering and non-maneuvering motions[22]. This challenge is addressed in multiple model approaches by using a bank of filters. Each filter is matched with a different target motion and are run in parallel[23]. Generalized pseudo-Bayesian approach[24] and interacting multiple model (IMM)[25] are two of the commonly used multiple model approaches. Furthermore, IMM filters can be used in conjunction with other filters such as Joint Probabilistic Data Association (JPDA)[26] to track multiple targets. A more elaborate account of the evolution of various methods for target tracking is also discussed in Smith *et al.*[23] and Mazor *et al.*[27]. Although the accuracy of target estimation provided by a single sensor is crucial, actual military operational environments consist of networks of heterogeneous sensors. Many works in both military and nonmilitary domains have focused on information fusion in distributed sensors platforms[28, 29]. Some of the key challenges that need to be addressed when information is fused from multiple sensors are achieving consensus and cooperation among the sensors and addressing issues such as node and link failures. Various consensus filters and algorithms were proposed to efficiently fuse information from multiple sensors[16, 17, 28]. In addition, many works have also proposed information fusion methods that are robust to unreliable communication links[30] and sensor failures[31]. Although sensor based target tracking approaches are critical to model a certain class of military targets their utility is limited to processing information obtained from organic sensors (such as GPS, radars, sonars, infrareds, etc.). However, in current military environments information are not only obtained through organic sensors but also from various other sources such as human intelligence, expert opinions and other domain specific information sources. The target modeling approach presented in this work can leverage information obtained from sensor based target tracking methodologies along with other information sources. A key characteristic of current military operations is Network Centric Operations (NCO), where information from diverse mediums are integrated to provide an increased situational awareness[32]. Liang *et al.*[32] proposed a threat assessment framework called knowledge-based ubiquitous and persistent sensor network (KUPS) that combine information from multiple sources. Many works have also focused on building agent-based models and simulation frameworks to understand the interoperability[33] and communication performance[34] between different components of the NCO framework. These techniques can be applied to model network-centric aspects of the military units. However, these approaches are restricted to specific warfare environments and situations and are not generalizable to understand the overall effectiveness and performance across all NCO/NCW networks. As described in section 4.1, in this work we leverage the N-COPP network performance modeling framework that provides a generic methodology to represent, model and analyze NCO/NCW environments of the target system.

In addition to the network-centric components, modeling large military targets requires the ability to model the behaviors and interactions between complex systems comprising of various human and technological entities. The rise in computational capabilities over the past few decades has enabled researchers to model sophisticated military units and their interactions. Many works focus on modeling these complex military entities as complex adaptive systems (CAS)[5, 18]. Agent-based modeling is a popular approach to model such complex adaptive models. Map Aware Non-uniform Automata (MANA)[35] is an agent-based model where each agent in the model has a set of personality parameters that determines the movements of the agent[18]. MANA can be used to model agents and their interactions in scenarios such as maritime surveillance and coastal patrols[36]. Swarm[37] provides a multi-agent platform to simulate complex adaptive systems. In this model, each component can be modeled as a swarm that represents a collection of agents executing a schedule of actions. Cil *et al.*[38] proposed a multi-agent architecture to model military units as complex adaptive systems. This approach uses two layers of agents, the cognitive agents and the reactive agents. The cognitive agents build an operational plan based on the information obtained from various databases such as intelligence, environment, terrain, logistic and other relevant databases. The MANA simulation module is used to model the operational plan using reactive agents. System of systems (SoS) is another systems engineering approach to understand the overall behavior of a set of interlinked systems. Current military operations require multinational and interagency cooperation and interdependent joint command and control systems[39]. Many works have discussed the challenges involved and approaches that can be used to model military organizations as SoS[39–41]. One of the key issues in current agent-based modeling and SoS approaches is that they lack the ability to provide unambiguous and detailed explanations for the observed behavior. In addition, modeling complex targets require capturing the dynamism and emergent behaviors exhibited by the sub-components of the target systems. Furthermore, the real-world information available to model these targets are uncertain and incomplete. In the following section, we present our approaches to address these issues involved in modeling complex military targets.

## 3. COMPLEX ADAPTIVE BAYESIAN KNOWLEDGE BASES

In this paper, we propose the Complex Adaptive Bayesian Knowledge Bases (caBKBs) framework to model targets as complex adaptive systems. Targets of interest to military planners can vary in complexity, ranging from a single armored unit in the field to a complex, evolving political movement. caBKB provides a framework to model targets as CAS by rigorously representing behavioral information of the main actors/entities/components of a target at multiple scales and levels of granularity. Additionally, various factors and interactions, including the socio-cultural aspects, relevant to their behaviors, can be embedded in our model by representing them in the form of beliefs, goals and actions, as discussed later in this section. The probabilistic reasoning network framework deals with the uncertainty that is inherent in all or many of these behaviors. The uncertainty may be due to several reasons including gaps in our understanding of the target; inherent uncertainty in human decision making and behaviors; and insufficient intelligence information. Moreover, the observable target information generated by ISR sources generally correspond to its overall behavior, which makes it a challenge to make corrective changes in the sub-models of the underlying components. The goals of the caBKB are to be able to provide a rigorous, axiomatic methodology to incorporate information, from various intelligence sources including electronic intelligence (ELINT) and human intelligence (HUMINT) sources, in the target model, while providing a transparent end to end analysis. As such, we have generalized this into two main processes, namely information aggregation and information composition to distinguish between incorporating "pieces" and "parts", respectively. The critical difference between incorporating "pieces" and "parts" are that parts are information encapsulation with well-defined functions or operations. Information aggregation refers to incorporating "pieces" that updates existing components, behaviors and processes of the target. Using a source based fusion algorithm[42], described later in this section, caBKB is able to quickly aggregate new pieces of information, even competing information, in such a way so as to preserve the information and the source identity for future de-aggregation and analysis. On the other hand, information composition refers to a more fundamental change in the target model through the incorporation of "parts" that can lead to new components, interactions and behaviors.

caBKB is a generalization of the Bayesian Knowledge Bases (BKBs) frameworks. BKBs is a probabilistic reasoning network framework that has also been utilized to model complex social, cultural and behavioral characteristics of actors or entities in real world scenarios[43, 44]. caBKB builds on the theoretical foundations of BKBs and focuses on providing a rigorous framework for incorporating information in models, namely information aggregation and composition. Before going into details of the caBKB framework, we first provide a discussion of BKBs. BKBs are a generalization of Bayesian networks that can be used to represent these knowledge fragments as conditional probability rules (CPRs) linking random variables (rvs) in an "if-then" fashion[6]. However, unlike Bayesian networks, BKBs can handle incomplete information which is especially critical when modeling real-world scenarios. BKBs are graphically represented as directed graphs and consist of two types of nodes: instantiation nodes (I-nodes) and support nodes (S-nodes). The I-nodes represent various states of a random variable and the S-nodes represent the probabilistic values linking these random variables. BKBs can be formally represented as a tuple and is based on the correlation graph defined in Santos Jr. *et al.*[6].

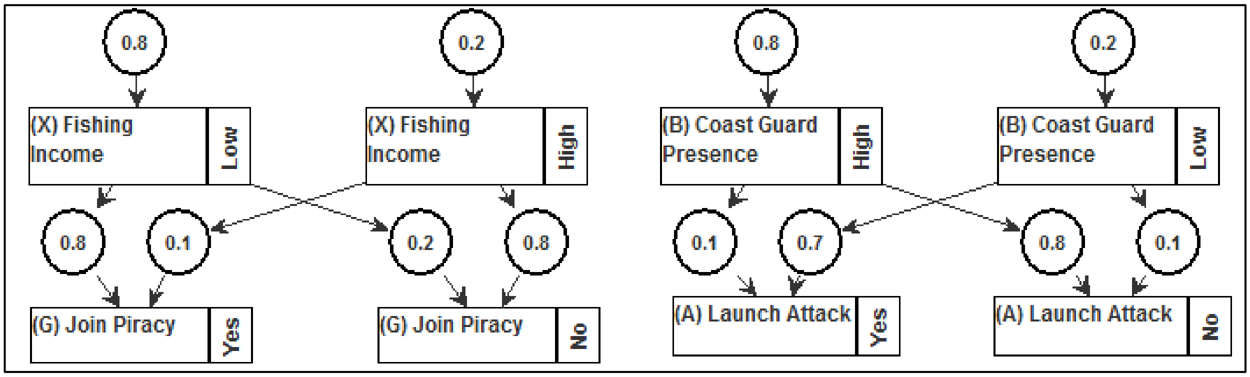

Figure 1. Example Bayesian Knowledge Bases (BKBs)

**Definition 1**[45]. A correlation-graph is a directed graph $G = (I \cup S, E)$ in which $I \cap S = \emptyset, E \subset \{I \times S\} \cup \{S \times I\}$, and $\forall q \in S$, there exists a unique $a \in I$ such that $(q, a) \in E$. If there is a link from $q \in S$ to $a \in I$, we say that $q$ supports $a$.

1. $Pred_G(q)$ represents the set of I-nodes pointing to $q$, i.e. $Pred_G(q) = \{a \in I | a \rightarrow q \in E\}$ where $q \in S$
2. $Desc_G(q)$ represents the I-node supported by $q$, such that $q \rightarrow a \in E$
3. I-nodes, $\alpha_1$ and $\alpha_2$ are said to be mutually exclusive if they are different instantiations of the same random variable

**Definition 2**[45]. A BKB is a tuple $K = (G, w)$ where $G = (I \cup S, E)$ is a correlation–graph, and $w : S \rightarrow [0,1]$ such that

1. $Pred_G(q)$ contains at most one instantiation of each random variable
2. $Pred_G(q_1)$ and $Pred_G(q_2)$ are mutually exclusive for distinct S-nodes $q_1, q_2$ that support the same I-node
3. Any complementary set of S-nodes $R \subseteq S$, $R$ is normalized: $\sum_{q \epsilon R} w(q) \leq 1$ where $w(q)$ is a weight function that represents the conditional probability $P(Desc_G(q) | Pred_G(q))$

```
BAYESIAN-KNOWLEDGE-FUSION $(K_1, K_2, \dots, K_n)$
Let $G' = (I', S', E')$ be an empty correlation graph and $w'$ a weight function
$I' \leftarrow \cup_{i=1}^{n} I_i$
$S' \leftarrow \cup_{i=1}^{n} S_i$
$E' \leftarrow \cup_{i=1}^{n} E_i$
for all fragments $K_i$ with $i \leftarrow 1$ to $n$
    for all S-nodes $q \in S_i$
        Let $\alpha \leftarrow Head_{G_i}(q)$
        Let the source I-node for $q$ be $s = (S_{R_\alpha} = \sigma_i$
        Add $s$ to $I'$ and add a new S-node $q_s$ to $S'$
        Add the edges $q_s \rightarrow s$ and $s \rightarrow q$ to $E'$
        Let $w'(q) \leftarrow w_i(q)$
for all source variables $S_{R_\alpha}$
Let $\Lambda = \{s \mid s\ is\ a\ source\ node\ which\ is\ a\ state\ of\ S_{R_\alpha}\}$
Let $\rho \leftarrow \sum_{s \in \Lambda} r(s)$
    for each $s \in \Lambda$, let $q_s$ be the S-node such that $q_s \rightarrow s \in E'$
        Let $w'(q_s) \leftarrow r(s)/\rho$
return $K' = (G', w')$
```

Figure 2. Bayesian knowledge fusion algorithm [42]

The behavioral and decision making characteristics of an entity/actor is based on its intent and knowledge possessed by it. Based on the adversarial intent inferencing (AII) model[46] we represent intent using four categories: 1) Axioms (X): represent the entity's beliefs about self, 2) Beliefs (B): represent the entity's belief about other entities, 3) Goals (G): represent the aims and goals of an entity and what it tries to achieve, and 4) Actions (A): represent the possible strategies or actions to pursue the goals. Figure 1 provides an example of a BKB related to a piracy scenario. If a fisherman possesses a self-belief (axiom) that his fishing income is low, then he will be highly likely to have a goal to join piracy related activities. Similarly, if a pirate believes that the coast guard presence is high then he or she will be less likely to pursue an attack on any merchant vessel in that region.

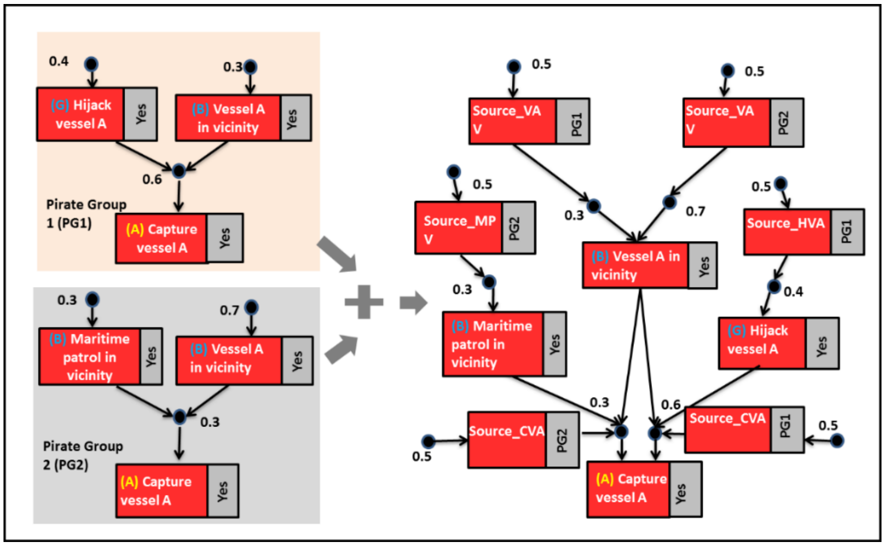

Figure 3. BKB fusion example

*Information Aggregation and Composition*: As mentioned before, caBKBs provide a framework to conduct information aggregation and composition. caBKB supports information aggregation, which deals with updating existing components and processes within the system, using the BKB fusion algorithm[42]. The BKB fusion algorithm (pseudocode provided in Figure 2) combines a set of $n$ BKB fragments $\{K_1, K_2, \dots, K_n\}$ where $K_i = (G_i, w_i, \sigma_i, r(\sigma_i))$ and $G_i = (I_i \cup S_i, E_i)$ and generates a new BKB, $K' = (G', w')$ with $G' = (I' \cup S', E')$. Fragments representing various attributes of an entity can be combined using the fusion algorithm to create an overall representation of that entity. Furthermore, BKB fusion can be used to capture the dynamism involved in real-world scenarios by fusing the BKB fragments representing an entity's beliefs with the fragments representing the events in a scenario. Figure 3 shows a simple BKB fusion example for a Somali piracy scenario. A detailed explanation of BKB fusion process can be found in our previous work[42]. Fused fragments can be analyzed using BKB reasoning algorithms. BKBs supports two form of reasoning algorithms, belief revision and belief updating. Belief revision algorithm can be used to determine the most probable outcome of the world that contains a given set of evidence. Belief updating computes the posterior probability of a target random variable state for a given evidence combination. A more detailed discussion on belief updating and belief revision can be found in Rosen *et al.*[47].

caBKB extends the BKB framework by providing the capability to decompose a random variable, in terms of underlying BKBs. In this manner, caBKBs model the hierarchy within a system where the overall systems may be decomposed into components, and components may be further decomposed into sub-components and so on. Consider a collection of finite discrete random variables (rvs), V where r(A) denotes the set of possible discrete values for random variable A in V. A conditional probability rule (CPR), R, defined using the BKB framework on V is of the form R: $If\ A_1 = a_1\ and\ A_2 = a_2\ \dots\ and\ A_n = a_n, then\ C = c$, where the rv $C = c$ is conditioned by the its antecedents $A_i = a_i$ for each $i$. Under caBKBs, the CPR R can be extended where C may be considered as a composition of subsystems $\beta_1$, $\beta_2$, …, $\beta_m$, where each are represented by random variables $B_1$, $B_2$, …, $B_m$, respectively, as long as the interactions of the rvs with C observe the mutual exclusivity principle. Moreover, each of the rvs $B_i$ may be further decomposed into rvs representing its subsystems and so on. In this manner, the caBKB framework provides a way to represent various levels within a complex adaptive system model while leveraging the strengths of the BKB reasoning algorithms. There are multiple ways to represent this decomposition in the caBKB framework. For example, consider the CPR R defined earlier. Here, the I-node C=c may be decomposed in terms of one or more BKBs constructed from a set of rvs that includes the antecedents of the I-node C=c. The value of the s-node leading to the I-node C=c may change based on the underlying BKBs. We have provided an example of decomposition from our Somali piracy scenario in Figure 6, where the mission objective of the group's central command, represented by the s-node *(G) Hijack vessel*, is affected by the mission objectives of the subordinate sea crews. The mission objectives of the sea crews may change due to the incorporation of new information from intelligence sources. Therefore the caBKB framework helps to model the ripple effects of the changing behaviors of the underlying sub-systems on the overall system behavior and vice versa.

Typically targets employ various technologies, including sensing, communication, and information processing/fusion technologies, that facilitate the interactions between system entities and components. This is apparent when modeling traditional military targets with ISR assets such as a navy flotilla. Other non-traditional targets such as political movements (e.g. the Arab spring movement[44]) have increasingly used sophisticated internet based technologies to share information, organize protests while allowing the participants to remain anonymous. In short, the underlying technical and social networks are critical for facilitating interactions between the system components and lead to the emergence of new behaviors. We will complement the capabilities of caBKBs by employing graph theoretic methods in the Network Centric Operations Performance and Prediction (N-COPP) framework to represent these interactions; mathematical functions to model dynamic changes in the system and its components; and define performance measures for the impact of these interactions on system behavior.

## 4. TECHNICAL BACKGROUND

In the previous section, we introduced caBKB, as a paradigm for modeling targets as complex adaptive systems. While caBKB provides a rigorous axiomatic framework for integrating and composing new information from various sources, modeling present day military targets requires the representation and analysis of the underlying technology including sensor networks, weapon systems, fusion and decision making algorithms, and even the social networks formed through the interactions between human actors within the organization. Modeling the underlying network of the target system is key towards identifying fusion points for information obtained from several sources. Furthermore, systematically modeling the dynamic network changes helps us to capture how the changes in behavior in one or more entities propagates throughout the entire target system. In order to provide these additional capabilities to the caBKB based target models, we will leverage our previous work in modeling network centric environments, and specifically our work in formulating a framework for network performance modeling and analysis called the Network Centric Operations Performance and Prediction (N-COPP) framework[11–13]. Below, we provide a brief description of the N-COPP framework, followed by a discussion on the integration of N-COPP with caBKB, in the next section.

### 4.1 Network Centric Operations Performance & Prediction (N-COPP)

N-COPP[11–13] is a theoretical framework to accurately model, predict the performance and identify optimization strategies for NCO/NCW networks. Robustness and reliability of a network infrastructure are critical especially in NCO/NCW networks since these networks need to continuously adapt to the changes in their environment. The N-COPP framework enables strategists and modelers to model the performance and also determine the robustness of a NCO/NCW networks by identifying the weaknesses in that network. The framework consists of four key components, network representation component (NRC), performance measures component (PMC), performance tool suite component (PTSC) and submodel interaction component (SIC).

The NRC component is used to formally represent the NCO/NCW network infrastructure. This component represents nodes and node interactions using graph-theoretic network representations. The nodes in the network represent various entities such as sensors, weapon systems, relay nodes, fusion nodes, etc. The links between the nodes represent connection properties such as link bandwidth, speed, connectivity, etc. Although the NRC model focus on the static snapshot of the network it should be able to represent network information that changes such as node mobility, network reconfiguration and fault propagation since the PMC component focus on analyzing network performance over time. Two important classes of metrics evaluated in the NRC component are labels and weights. The type a node or edge belongs to is represented by its label and the values of a metric at a given time is represented by the collection of weight at that time. As discussed earlier the NRC component provides the ability to analyze the network at a fixed time step. However, it is critical to analyze the network's performance over time and the PMC component provides the ability to accurately represent target structure for dynamic network analysis. PMC is represented as a collection of functions that can use the network variables (labels and weights) and predict the state of the network in a future time frame. The combination of NRC and PMC components provides the ability to obtain both current and future snapshots of the underlying network.

The PTSC component contains performance analysis tools and methodologies to measure the performance of the underlying network based on the metrics and measures provided by NRC and PMC components. The type of performance analysis provided by the PTSC component could be based on various factors and metrics, and therefore can be changed as required by the framework. For instance, network reliability can be evaluated using various methods such as analyzing the connectedness of the network, analyzing the signal strength and information drop rates. The performance of the current state of the network can be obtained using NRC and PTSC components. On the other hand, the performance of the future states of the network can be obtained by using NRC, PMC, and PTSC components. Moreover, NRC, PMC, and PTSC components can be used to obtain a quantitative analysis for a given set of metrics and measures of the network.

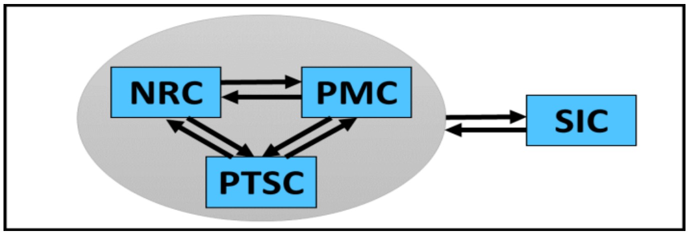

Figure 4. Network Centric Operations Performance and Prediction (N-COPP) Framework[11]

The first three components provide performance analysis for the NCO/NCW network. However, the quantitative performance measures need to be assessed to identify relevant modifications to handle any performance weaknesses. The SIC component contains methodologies to efficiently utilize the information obtained from NRC, PMC, and PTSC to detect performance bottlenecks and suggests subsequent modifications to resolve such issues. Various optimization techniques, learning algorithms and probabilistic modeling approaches can be employed to predict the quality of the network performance based on various performance criteria such as network reliability, efficiency, etc. Each component in the N-COPP framework addresses a specific aspect of the network performance. This modular approach provides a plug-and-play property to swiftly incorporate existing analysis methods and at the same time adapt to future changes in the technology. The utility of the N-COPP framework to model dynamic NCO/NCW networks was illustrated in Santos *et al.*[12]. A detailed explanation and applications of the N-COPP framework can be found in our previous works[11, 13].

## 5. INTEGRATION OF caBKB WITH N-COPP

For the target modeling work described in this paper, we integrate the capabilities of caBKB and N-COPP by focusing on two key groups or layers of components within the target, namely the network layer and the behavioral layer. The network layer encompasses the underlying technologies that support interactions between the components in the target. This may include ISR and weapon platforms used by the target, communication networks, information fusion systems, decision support systems, command hierarchies, and even the social networks that link human actors in the system. Recall that in the CAS based models, the target is considered to be a set of components of varying autonomy that interact with each other. The representations and methods of the network layer focus on modeling these interactions between the components. The behaviors of the components and the overall system, is the focus of the behavioral layer. In this work, caBKB has been used to model the behavioral layer while N-COPP focuses on the network layer. Specifically, the network representation component (NRC) of the N-COPP framework is used to represent the network using graph theoretic methods with the nodes representing the components/entities within the target and the edges represent the interactions between them. An important strength of the N-COPP is its flexibility, which allows for heterogeneous networks of various types and capabilities to be represented. The nodes have labels to represent relevant properties including the communication technology being used (e.g. wireless transmission) and weights to represent their respective metrics (e.g. communication range). Similarly, the edges in the network have labels and weights that may represent the characteristics of the communication link such as connectivity. Social networks, representing the interactions between human actors, within the system, are also represented in the NRC component. It is clear that interactions between the different networks may have an impact on the overall system behaviors. For example, the strength of ties in the social network is dependent on the opportunities for interaction, which in turn is facilitated by the underlying communications technologies.

Using our previous work on modeling actor intent[46], specific behaviors of the technological and human components of a target are modeled within caBKBs by breaking them down in terms of available information or beliefs, objectives or goals, feasible strategies or actions for achieving the goals and knowledge of its internal state or axioms. We have discussed how these elements relate to behaviors of human actors in section 3. The notion of intent can be extended to technology components, where axioms may represent its internal state, beliefs may include its knowledge of conditions in its environment and other components, goals may include its objective functions and actions may include possible modifications it can make to its internal state to achieve its objectives and respond to changes in the environment. Since the behaviors of a component undergo changes due to interactions with other components, there needs to be a careful integration of the N-COPP based representations and methods with those of caBKB. There are a number of ways to achieve this integration. In this work, we have utilized the NRC component as the lynchpin for the integration, with the nodes in the graph representations helping to map entities/components/actors to their behaviors encapsulated as caBKBs and the edges helping to direct the interactions between the components. Moreover, N-COPP helps to model the propagation of the changes to the caBKBs throughout the system.

One of our goals is to demonstrate the capability of caBKBs to deal effectively with information aggregation. As part of this effort, N-COPP can be used to identify fusion points for incoming information and to analyze how the effect of various changes propagate across the target system. The fusion points represent the entities in the organization to which the incoming information correspond to. We will also analyze the target by leveraging a commonly used metric from the NCO domain called self-synchronization[14], and study the link between aggregating intelligence of varying reliability and changes in self-synchronization.

## 5.1 Information Aggregation

The information available to model real-world complex military targets is usually obtained from multiple sources including electronic intelligence (ELINT), human intelligence (HUMINT), and subject matter experts. Various forms of information obtained from these diverse sources need to be effectively combined to analyze the targets. Additionally, the information obtained from various sources may have different reliabilities, and a piece of information could have varying levels of impact across multiple entities in the target system. Furthermore, changes encountered at a certain part of the target system could cause a subsequent ripple effect across multiple levels of the target system and could lead to an overall change in their behaviors. For instance, events such as a change in the leadership or failure in critical communication infrastructure can affect the goals and momentum of the overall system. Therefore, it is critical for our modeling framework to have the capability to efficiently handle these nuances involved in incorporating real-world information. Efficiently aggregating information from various sources is also essential to understand the target's level of situational awareness which is critical for modeling and measuring self-synchronization.

As mentioned in section 3, information aggregation is supported within caBKB by using the BKB fusion algorithm, which uses reliabilities of the sources to incorporate the new information. Analysis of N-COPP based network representations can provide insights on the appropriate fusion points in the model and estimates of their reliabilities. In some cases, information from ISR assets are tagged with location and time information, which may be used to determine the specific entity or component that the information is relevant to. In the absence of the tag information, graph representations within NRC can be used to determine the fusion points. In cases where the target is highly dynamic, the tag information may be outdated by the time it is incorporated into the model. The graph representations in the NRC along with the dynamism models in PMC can then be used to predict the fusion points. Similarly, N-COPP representations can be used to determine source reliabilities for the incoming information. For example, analysis of the social networks within the NRC component of N-COPP can be used to determine the level of trust for a HUMINT source, which can then be used to determine its reliability measure.

## 5.2 Self-Synchronization

In the NCO domain, self-synchronization is considered to be the main outcome of situational awareness and leads to better mission effectiveness. Various definitions for self-synchronization have been provided with emphases on the coordination of actions among groups, decentralized execution of commander's intent, individual decision making and common goals. As described by Araki[14], the underlying common theme in all these definitions is that self-synchronization is about "doing the right thing at the right time for the right reason without having to be told to do so"[48]. In self-synchronization, organizational goals are achieved by individuals proactively responding to actions of other teams based on a shared situational awareness. Although developing a quantitative measure for self-synchronization has been a challenging task, factors such as mission objective, situational awareness and trust have been identified as factors influencing self-synchronization. The BKB reasoning algorithms can be utilized with network based metrics, defined by N-COPP, to quantify these factors. For the modeling scenario, described in the next section, we will define a new quantitative measure for the effectiveness of self-synchronization, which will make use of the posterior probabilities of relevant random variables (rvs).

In the preceding sections, we described the caBKB and N-COPP framework and provided some initial ways for integrating them to model both the network and behavioral layers in the target. In the next section, we will develop an initial caBKB based target model for a fictional Somali pirate group and use the model to analyze the changes in self-synchronization, brought about by variations in its situational awareness, as simulated by the change in the reliability of the available information.

## 6. INITIAL SOMALI PIRACY SCENARIO AND MODEL

To demonstrate the effectiveness of our approach, we use a real-world scenario in the NCO domain that exhibits CAS characteristics, and have both technological and human elements. In particular, we chose the Somali piracy scenario[43, 49] to demonstrate our target modeling approach. The Somali pirate groups[50] are complex paramilitary organizations consisting of diverse units, of varying autonomy, that play different roles while seeking to achieve the organizational objectives.

### 6.1 Somali Piracy Scenario

Somalia piracy had its genesis in the early 1990s[43] and has continued up until now[51, 52] due to the effects of illegal fishing, illegal toxic waste dumping and 2004 Indian Ocean tsunami which threatened the livelihood of the fishing communities along the coastal regions of Somalia. The lack of other opportunities and enticements of financial gain made piracy a popular choice among youths in these communities. Even recently the Somali pirates have hijacked a Sri Lankan oil tanker[51] and an Indian cargo vessel[52] off the coast of Somalia. Although piracy in Somalia started as a crime of opportunity, the current level of planning involved in choosing and attacking targets, and the ensuing ransom negotiations show a vast improvement in their organizational capability. Somali pirate groups are commonly organized based on the functions and roles of the individuals. Based on the information obtained about the Somali pirate groups network and operational structure from various case studies[43, 49, 50, 53–56] we developed a representative organizational structure for a fictional pirate group (shown in Figure 5). While the attack and further negotiations are carried out under a leader, the pirate groups are funded through various sources including shareholders (local population, merchants, etc.), and in some cases by warlords. The pirate groups usually employ middlemen who are fluent in English to conduct hostage negotiations. The pirates also receive intelligence from both overseas sources at various international ports and from local spotters. The pirates may employ local fishermen as spotters to identify target merchant vessels and navy patrols in the vicinity. Based on the available reports about the pirates and their tactics, we have further divided the operational unit into land-based and sea-based crews. The sea-based crew uses the intelligence and other information from the spotters to track and attack the ship using a combination of mother ship and skiffs. The sea-based crew contains individuals with seafaring skills as navigators, military skills to handle the weapons and technology skills to utilize GPS, satellite phones and other devices to track the target and also to communicate with rest of the crew. Once the ship is captured, it is moved to a pirate-friendly port. The land-based crew is responsible for guarding the ship, providing food and water for the crew during the course of the negotiations. The negotiators are usually highly trusted middlemen with English speaking skills, hired to make contact and negotiate with the ship owners. In order to understand the overall behavior of such complex organizations it is essential to analyze and combine the behavior of the individual entities in the organization.

### 6.2 Initial Somali Piracy Model

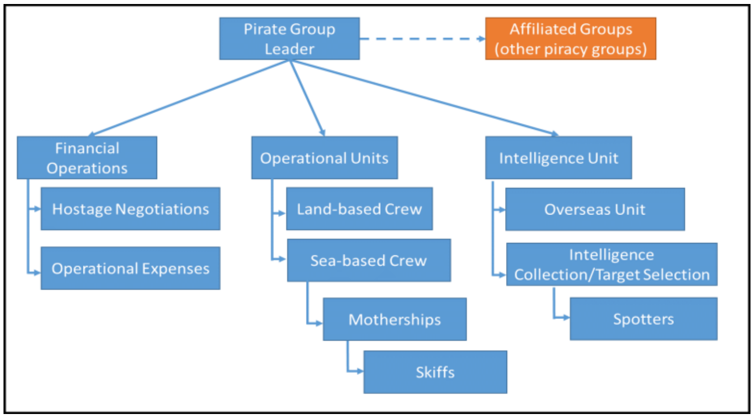

Figure 5. Representative organizational structure of a Somali pirate group

One key challenge when modeling real-world targets is that the information about the targets are continuously obtained from multiple sources and are often uncertain and incomplete. In order to utilize this diverse information, the target modeling framework should have the capability to dynamically aggregate information obtained from multiple sources. Another important aspect when modeling real-world targets as CAS is that these systems consist of several components that interact with each other at various scales to produce the overall system behaviors. The overall behaviors of these components are uncertain and can change based on factors such as changes in the environment, changes in the behavior of the neighboring components and a multitude of other factors. Hence the modeling framework should have the ability to represent the individual behaviors and interactions between these components at various scales. Moreover, the modeling framework should handle the inherent uncertainty, and incompleteness of information in real-world scenarios. Using the Somali piracy scenario, we will illustrate how the caBKB framework can be utilized to address these information aggregation challenges. A key performance metric that represents the overall effectiveness of a NCO based military target system is the level of self-synchronization[48]. Self-synchronization is based on the ability to the target system's entities to organize and adapt to achieve the overall mission objectives. By modeling the behavior of sea-based Somali pirate crews, we have analyzed how the effectiveness of self-synchronization changes as the events unfold in the scenario.

## Behavioral Layer Modeling

We used the information collected from various open source articles[50, 55, 56] and publications[43, 49, 53, 54] about the tactics used by Somali pirates during the hijacking and capturing of merchant vessels to construct the scenario. Here we focus on modeling the role of the sea based pirate crews within the group. Figure 6 illustrates how information aggregation and composition can be performed using caBKBs. In this example, the pirate group organization is delineated into a central command and sea-based crews. The central command's goal to hijack a merchant vessel is pursued by two sea crews and this process is captured by the interactions between the random variable "Hijack vessel A" present in each sub-group. Based on the information aggregated from different intelligence sources the sea crews adopt different strategies to hijack the target vessel and handle maritime security. Finally, the central command may alter its goal to hijack the target vessel based on the behaviors and actions of the sea crews. This illustrates the ability of the caBKB to model complex interactions between sub-components of a target system, and also across levels within the system. In this work, we focus on demonstrating the information aggregation procedure using caBKBs.

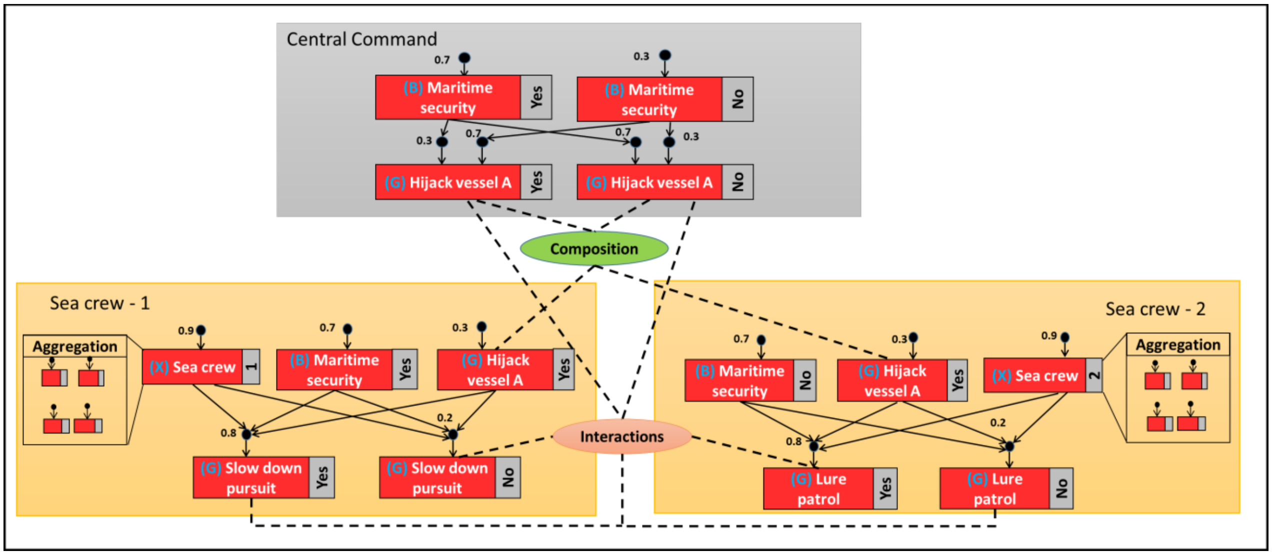

Figure 6. Example of a caBKB illustrating information aggregation and composition

## Network Layer Modeling

A key factor in launching a successful hijack is the availability of reliable and up-to-date situational awareness. Efficiently representing and modeling the underlying communication infrastructure of the pirates is essential to understand the quality and evolution of situational awareness. In this work, we leverage the Network Centric Operations Performance and Prediction (N-COPP) framework[11–13] to represent, model and analyze the social, communication and information sharing networks of the pirate groups. Recall that the N-COPP framework has a component based architecture with each component having the capability to handle the key challenges in modeling network-centric environments such as heterogeneity, network dynamism and network performance.

*Network Representation Component (NRC):* In our modeling methodology, the interactions among the individuals and groups in a Somali pirate group is represented using the NRC component. Two key aspects that are critical to understand the military targets are their underlying physical and social network structures[12]. Here we use the NRC to represent these two network structures. The social network can be represented as a graph $G_S(V_S, E_S)$, where the set of nodes $V_S$ represents the actors in the network and the set of edges $E_S$ represents their social ties. Each node $v_S \in V_S$ and edge $e_S \in E_S$ have a label and an associated weight to represent both qualitative and quantitative characteristics of the network elements. Using case studies[49–51, 53–56] we developed an initial social network structure of a sea-based pirate crew as shown in Figure 7. Each node represents an individual or a group of actors with specific roles within the organization. The navigators are the individuals with seafaring skills and the attackers are the individuals with military skills. The spotters are members of pirate group  and/or local fishermen who provide information about merchant vessels and patrol vessels. The leaders are the individuals involved in planning and decision making process at their appropriate chain of command. The edges represent social and communication ties between these actors.

The physical network can be represented as a graph $G_P(V_P, E_P)$. Here the set of nodes $V_P$ may represent the communication devices used to receive and transmit information, and the set of edges $E_P$ represents the information transmission between the nodes. Similar to the social network graph, node $v_P \in V_P$ and edge $e_P \in E_P$ has a label and an associated weight to represent the qualitative and quantitative characteristics of the network element. For instance, labels can represent features such as device type and network protocol used. The weights can represent network properties including network bandwidth, packet drop rate, etc. Based on their role in the organizational hierarchy and the nature of the mission, the pirates may use different modes of communication. For instance, the pirate leaders could have access to different communication devices such as devices connected to the internet, cell phones, satellite phones and intelligence from local military and foreign spies at the ports. The sea-based crews could have access to satellite phones, cell phones, marine very high frequency (VHF) radios, GPS, radar and other equipment onboard in their mothership and skiffs. Figure 8 shows a physical network example for the pirate group and the hierarchy based on the social network in Figure 7. The labels show both the devices used and the actors that use these devices. The edges represent the direction of information transmission.

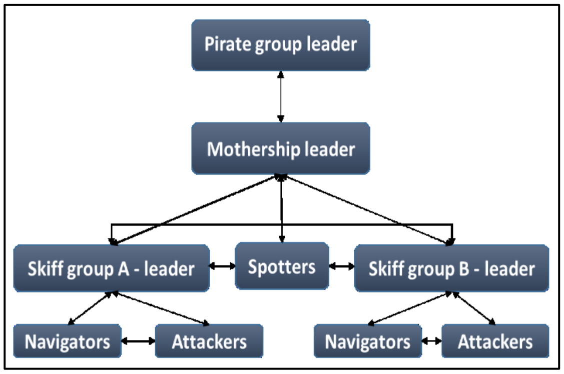

Figure 7. Example of a social network of a sea-based pirate crew

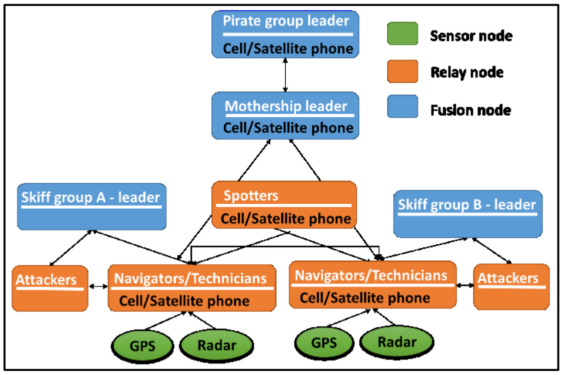

Figure 8. Example of a physical (communication) network of a sea-based pirate crew

Based on our previous work, nodes in the physical network can be broadly classified into three types[13]: 1) Sensor Nodes: Nodes such as radars and GPS that monitor the environment, 2) Relay Nodes: Nodes that collect and transmit the information obtained from the sensors, and 3) Fusion Nodes: Nodes that assimilate information obtained from the relay nodes and therefore possess a broader view of the environment. Decomposing the overall interaction network of the pirate groups into a social and a physical network enables us to capture the intricacies in the human ties and at the same time efficiently model the technical characteristics of the underlying physical network. Furthermore, information available to model these targets in real-world scenarios are obtained from multiple sources and are often incomplete and may focus on describing only limited aspects of the target system. Decomposing the target system's networks to a reasonable granularity of detail enables us to efficiently incorporate the partial real-world information within the appropriate parts of the network.

*Performance Measures Component (PMC):* The NRC component represents the state of the network at a fixed time step. However, the network structures in a dynamic environment adapt continuously based on node mobility, unfolding events and changes in the environment. The PMC component of the N-COPP framework uses prediction strategies to estimate the future state of the network. Furthermore, as mentioned earlier, the information available to model these targets are usually incomplete and partial. The PMC component can use the available information and estimate how the network evolves in future time steps. The communication behavior of the pirate groups at future time steps can be estimated by simulating the dynamic changes in the pirates' physical network using methods such as discrete event simulation tools and agent-based modeling techniques[12]. Based on factors such as node position, network hierarchy, number of communication links, signal strength, information drop rates and other relevant characteristics, we can estimate how the network conditions change with time. The changes in the strength of social ties at future time steps can be estimated by analyzing changes in the intent of pirates over time, brought about by new information being incorporated using BKB fusion[42].

*Performance Tool Suite Component (PTSC):* In this work, we measure the effectiveness of self-synchronization by analyzing how the probability of achieving the overall goal (mission objective) of the organization changes when entities within the organization proactively adopt tactics based on the situational awareness. In particular, by modeling the behavioral aspects of various entities in the organization using caBKBs, we measure self-synchronization by analyzing how the actions performed by the entities affect the probability of achieving the mission objective. Let $P_t(MO_S)$ be the probability that the mission objective can be accomplished at time step $t$ and conversely, $P_t(MO_F)$ be the probability that the mission objective cannot be accomplished. Then, the effectiveness of self-synchronization is given by the odds ratio, $\frac{P_t(MO_S)}{P_t(MO_F)}$ and its change between two time steps is given by $\frac{P_t(MO_S)}{P_t(MO_F)} - \frac{P_{t-1}(MO_S)}{P_{t-1}(MO_F)}$. Entities that share beliefs or intent with the organization towards achieving the final objective can perform actions that will increase the degree of self-synchronization, i.e., $\frac{P_t(MO_S)}{P_t(MO_F)} - \frac{P_{t-1}(MO_S)}{P_{t-1}(MO_F)} > 0$. On the other hand, entities that share different beliefs with the organization towards achieving the final objective can perform actions that will lead to lower self-synchronization, i.e. $\frac{P_t(MO_S)}{P_t(MO_F)} - \frac{P_{t-1}(MO_S)}{P_{t-1}(MO_F)} < 0$.

### 6.3 Initial Analysis

Table 1. Description of events in the scenario

<table>
<tr><td colspan="4"><b>Pirates:</b> Central command, sea crew 1 (SC1) and sea crew 2 (SC2)<br><b>Other entities:</b> Merchant vessels A and B, and a maritime patrol vessel<br><b>Objective:</b> Hijack the merchant vessel A</td></tr>
<tr><th>Event</th><th>Sub-scenario 1 (without intelligence sharing)</th><th colspan="2">Sub-scenario 2 (with intelligence sharing)</th></tr>
<tr><td>1</td><td>Central command orders Sea crew 1 (SC1) and Sea Crew 2 (SC2) to hijack vessel A (Baseline).</td><td colspan="2">Central command orders SC1 and SC2 to hijack vessel A (Baseline).</td></tr>
<tr><td>2</td><td>Both SC1 and SC2 using skiffs sails towards vessel A.</td><td colspan="2">Both SC1 and SC2 using skiffs sails towards vessel A.</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">The sea crews are spotted by a nearby maritime patrol vessel and are attacked.</td><td><b>Sub-scenario 2.1</b></td><td><b>Sub-scenario 2.2</b></td></tr>
<tr><td>Sea crew receives information about a maritime patrol vessel in the vicinity of the merchant vessel A.<br>SC1: slows down their pursuit.<br>SC2: stages a decoy raid by approaching another merchant vessel B that is far away from the merchant vessel A and thereby lures the maritime patrol away from vessel A.</td><td>Sea crew receives information about a maritime patrol vessel in the vicinity of the merchant vessel A.<br>Both SC1 and SC2 expedites their attack on Vessel A to avoid interception with the patrol vessel.</td></tr>
<tr><td>4</td><td>Both sea crews are overwhelmed by the maritime patrol and they surrender.</td><td>As the patrol vessel approaches the merchant vessel B, SC2 evades and retreats. SC1 attacks and captures the vessel A.</td><td>Both SC1 and SC2 attacks and captures the vessel A.</td></tr>
</table>

Here we model how the actions of the two sea crews (SC1 and SC2) changes the likelihood of hijacking a merchant vessel. SC1 is the lead attack group and SC2 is the secondary attack group. To emphasize the importance of information sharing, situational awareness and autonomous decision making we designed three sub-scenarios. Table 1 shows the events in our synthetic scenario developed based on the case studies[43, 49, 50, 53–56]. We used the BKBs to model the belief, goals and actions of the pirate groups.

### Sub-scenario 1

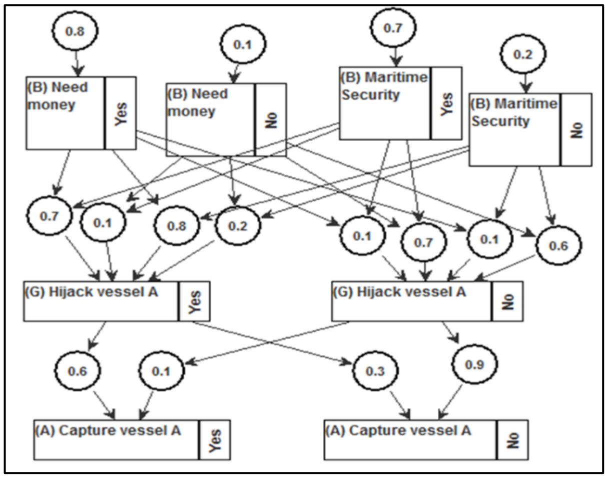

Figure 9a. BKB fragment for central command's intent

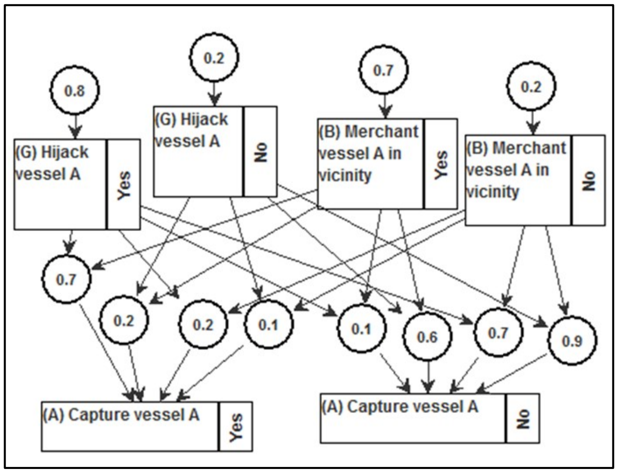

Figure 9b. BKB fragment for sea crews baseline

In sub-scenario 1, we model how the absence of intelligence information could adversely affect the sea crews in achieving the organizational objective, and thereby their self-synchronization behavior. Figure 9a shows the BKB fragment representing the beliefs and goals of a pirate organization described in event 1. In particular, we model how the need for money and the presence of maritime security influences the pirate organization's objective to hijack a certain merchant vessel. In this scenario, two groups of pirates equipped with skiffs and weapons carry out the hijack. The baseline behavior of sea crew is shown in Figure 9b. By fusing these two fragments, we model how the pirate organization's goal drives the sea crews' behavior to capture the merchant vessel A. In sub-scenario 1, the sea crews do not receive any real-time intelligence regarding nearby movements of maritime patrol vessels. Once they encounter the maritime patrol they are overwhelmed and eventually surrender as described in events 4 and 5 (Figure 10). This sub-scenario clearly illustrates how the lack of intelligence sharing could hinder entities attempting to accomplish organizational objectives in a real-world military scenario. In subsequent scenarios, we will illustrate the alternate case when real-time information could enable entities to efficiently self-synchronize.

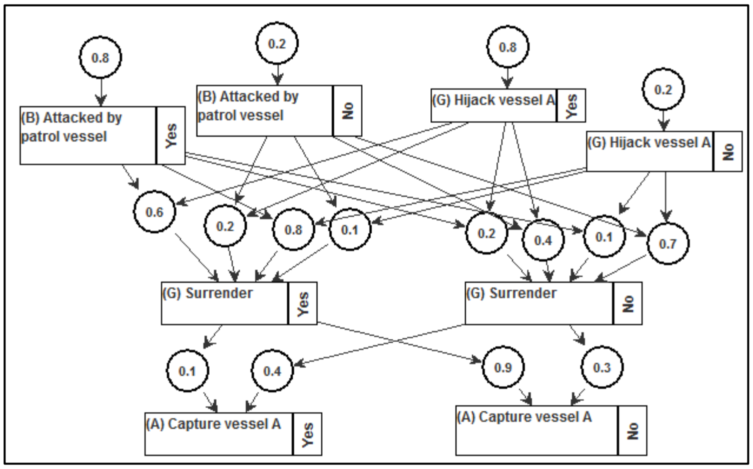

Figure 10. BKB event fragment for sea crews being approached by patrol

### Sub-scenario 2.1 & 2.2

In sub-scenario 2.1 and 2.2 both groups, SC1 and SC2, receive information about an approaching maritime military security patrol and change their tactics to achieve the mission objective. Events in sub-scenario 2.1 diverges from sub-scenario 2.2 starting at event 3 when both sea crews SC1 and SC2 receive information about a maritime patrol vessel in the vicinity of the target merchant vessel A. While SC1 slows down its pursuit of the vessel (see BKB in Figure 11) in sub-scenario 2.1, SC2 proactively engages in a decoy tactic (Figure 12) and lures the maritime patrol away from the target vessel A. SC1 is able to hijack the target vessel A and achieve the overall mission objective. As in sub-scenario 2.1, both SC1 and SC2 receive information about the maritime patrol vessel in sub-scenario 2.2. SC1 and SC2 adopt a different tactic where they expedite their plan to hijack vessel A before the patrol vessel arrives (see BKB in Figure 13).

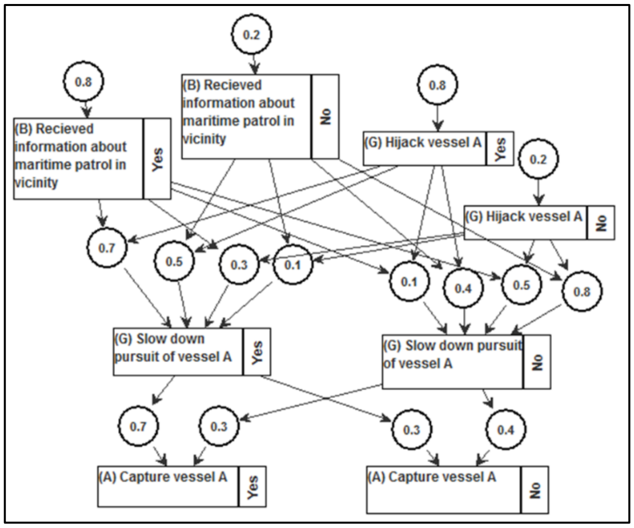
0.2
0.8
(B) Recieved information about maritime patrol in vicinity
No
0.8
(G) Hijack vessel A
Yes
(B) Recieved information about maritime patrol in vicinity
Yes
0.2
(G) Hijack vessel A
No
0.7
0.5
0.3
0.1
0.1
0.4
0.5
0.8
(G) Slow down pursuit of vessel A
Yes
(G) Slow down pursuit of vessel A
No
0.7
0.3
0.3
0.4
(A) Capture vessel A
Yes
(A) Capture vessel A
No

Figure 11. BKB fragment for SC1's behavior based on intel update

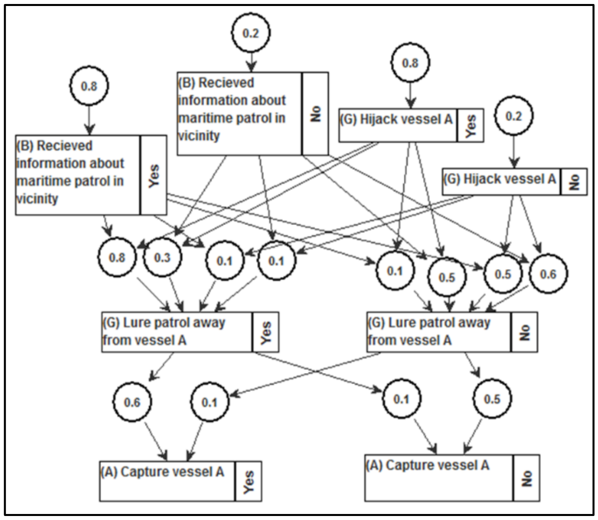
0.2
0.8
(B) Recieved information about maritime patrol in vicinity
No
0.8
(G) Hijack vessel A
Yes
0.2
(B) Recieved information about maritime patrol in vicinity
Yes
(G) Hijack vessel A
No
0.8
0.3
0.1
0.1
0.1
0.5
0.5
0.6
(G) Lure patrol away from vessel A
Yes
(G) Lure patrol away from vessel A
No
0.6
0.1
0.1
0.5
(A) Capture vessel A
Yes
(A) Capture vessel A
No

Figure 12. BKB fragment for SC2's behavior based on intel update

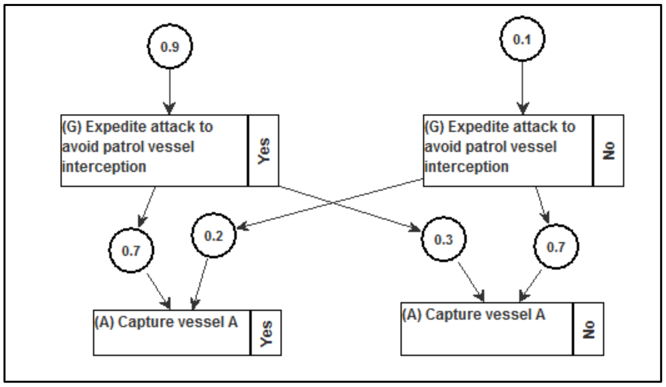
0.9
0.1
(G) Expedite attack to avoid patrol vessel interception
Yes
(G) Expedite attack to avoid patrol vessel interception
No
0.7
0.2
0.3
0.7
(A) Capture vessel A
Yes
(A) Capture vessel A
No

Figure 13. BKB fragment for SC1 and SC2's behavior to expedite their pursuit

### Initial Experimental Results and Analysis

In this preliminary set of results, first we focus on analyzing the changes in the level of self-synchronization with respect to the events in the scenario and the actions performed by the sea-based crew. We measure self-synchronization by computing the success to failure ratio of the mission objective using the posterior probability of the random variable "*(A) Capture vessel A*". In addition, the reliability values of the information can affect the actions performed by the sea crews. Here Figure 14a and Figure 14b shows the level of self-synchronization across the three scenarios for low and high information reliability values, where the incoming intelligence information are fused with source reliability values of 0.2 and 0.95, respectively.

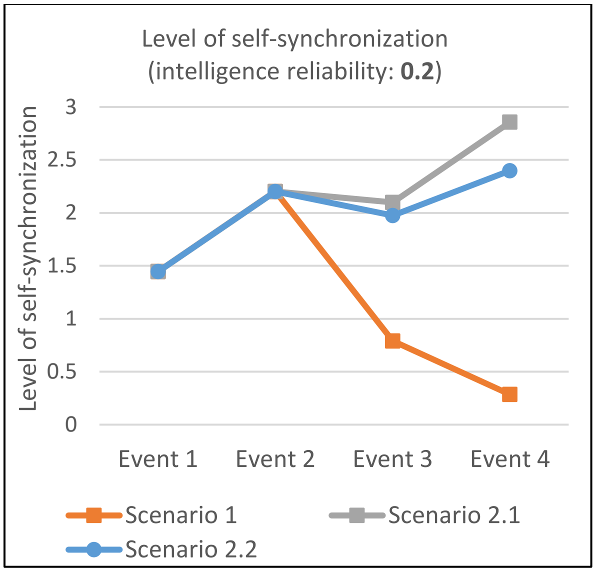

Figure 14a. Level of self-synchronization for low reliability value of intelligence information source

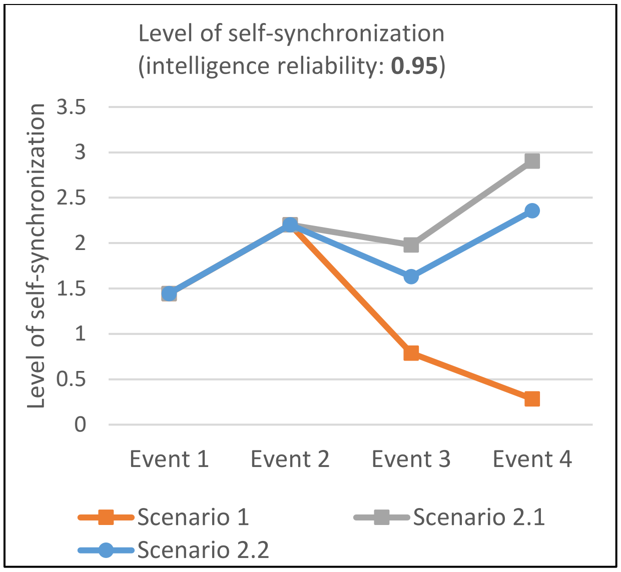

Figure 14b. Level of self-synchronization for high reliability value of intelligence information source

In our scenario, during the first two events, the central command issues an order to SC1 and SC2 to capture a specific merchant vessel. Since these two events are similar across the three scenarios, the models should exhibit similar level of self-synchronization. Since the sea crews in scenario 1 do not receive real-time intelligence information, they fail to adopt new strategies to handle the maritime patrol presence in event 3 and surrender in event 4. This explains the drop in self-synchronization levels in scenario 1, following event 2. Both sub-scenarios 2.1 and 2.2 demonstrate how enhanced situational awareness provides skiff groups the opportunity to dynamically change tactics when faced with unforeseen challenges. We can observe from the BKBs (Figure 11 and Figure 12) that the tactic adopted by the sea crews in sub-scenario 2.1 can improve the probability of mission success since the patrol vessel is lured by the SC2 and therefore provides sufficient time for SC1 to capture the merchant vessel. On the other hand, in sub-scenario 2.2, there is a higher likelihood of the pirates being intercepted during their attack. This explains the higher self-synchronization levels achieved in scenario 2.1 when compared to scenario 2.2. Thus, by evaluating the posterior probability of achieving the mission objective we can explain the variations in the self-synchronization levels observed across different scenarios. Furthermore, the effects of change in the reliability values of intelligence information can be observed by comparing the level of self-synchronization in Figure 14a and Figure 14b. We fuse the intelligence information for sub-scenarios 2.1 and 2.2 at event 3. When the intelligence information about maritime patrol presence is given a higher reliability of 0.95 as shown in Figure 14b, it increases the credibility of the intelligence information. This results in an overall decrease in the likelihood of mission success on both sub-scenarios 2.1 and 2.2 when compared to Figure 14a, where the intelligence information is given a lower reliability (0.2).

During the course of a scenario/simulation the level of self-synchronization can vary significantly, therefore it is critical to analyze the change in the level of self-synchronization with respect to the current state to understand the effects of each individual event. Figure 15a and Figure 15b shows the change in the effectiveness of self-synchronization (as described in section 6.3) between consecutive events for different intelligence information reliability values. Here positive and negative values correspond to increase and decrease in the level of self-synchronization between current and previous event. The level of self-synchronization increases from event 1 to event 2 in all three scenarios. This can be attributed to the fact that in event 2 both sea crews start pursuing the order received from the central command in event 1 and the first two events are similar across all the scenarios. However, in event 3, the appearance of maritime patrol obstructs the sea crews' initial plan to hijack the merchant vessel and therefore affects their previous level of self-synchronization. In particular, the sea crews in scenario 1 do not receive any intelligence information about the maritime patrol whereas in sub-scenarios 2.1 and 2.2 the sea crews receive intelligence information which increases their situational awareness. Therefore, the decrease in the level of self-synchronization is substantially higher in scenario 1 when compared to sub-scenarios 2.1 and 2.2. Although the sea crews in both sub-scenarios receive the same intelligence information, the tactics adopted by them affects the level of self-synchronization. For instance, the crews in sub-scenario 2.1 adopt a decoy strategy and crews in sub-scenario 2.2 attempts to expedite their attack before the maritime patrol could reach the target merchant vessel. However, expediting the attack increases their likelihood of facing the maritime patrol when compared to luring the maritime patrol away as in sub-scenario 2.1. In event 4, the sea crews in scenario 1 surrender to the maritime patrol and results in a decrease in the level of self-synchronization. However, in sub-scenario 2.1 and 2.2 the sea crews successfully capture the target vessel and this increase the level of self-synchronization when compared to the previous event. Similar to the previous results (Figure 14a and Figure 14b), increase in the reliability of intelligence information about maritime patrol presence decreases the likelihood of mission success and consequently reduces the level of self-synchronization. Therefore, the drop in the level of self-synchronization at event 3 for sub-scenario 2.1 and 2.2 is higher when the intelligence information has a higher reliability value (Figure 15b).

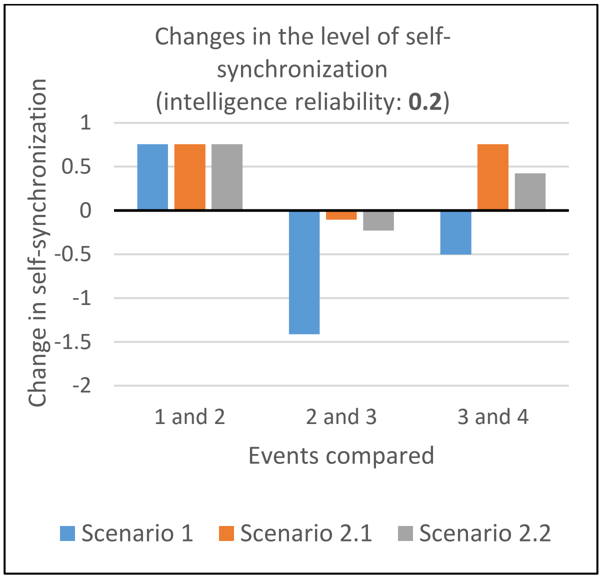

Figure 15a. Changes in the level of self-synchronization for intelligence reliability value of 0.2

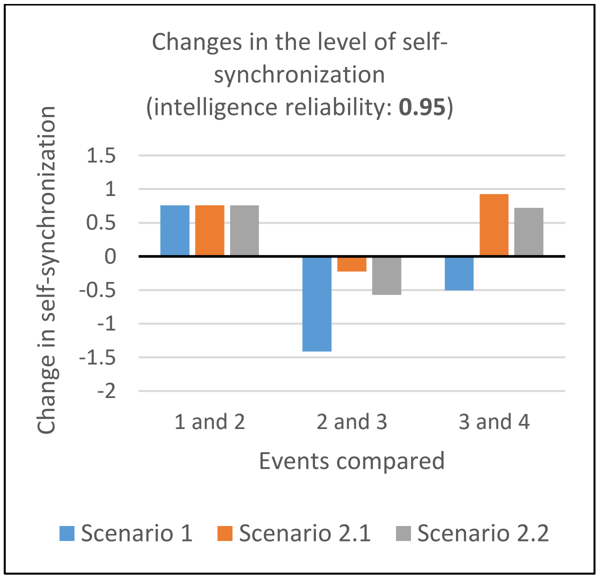

Figure 15b. Changes in the level of self-synchronization for intelligence reliability value of 0.95

In this work, we have demonstrated how information about the sea-based crews' behaviors can be systematically aggregated using the caBKB framework and can subsequently be used to measure the changes in the level of self-synchronization in the target system. In addition, this preliminary scenario shows the capability of our framework to aggregate information from multiple sources with different levels of information reliability. In our future work, we plan to extend this scenario by incorporating factors such as the speed and the response time of the patrol vessel, speed of the skiffs, distance to the coast and other relevant factors that will enable us to realistically analyze the overall effectiveness of the strategies adopted by the sea crews. The Somali scenario discussed here illustrates the significance of situational awareness and communication capabilities in military environments to enable entities to self-synchronize and autonomously undertake actions to enable overall mission effectiveness.

## 7. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we introduced caBKBs as a rigorous, overarching and axiomatic framework for modeling complex military targets. We described the challenges involved in modeling the behavior of target system that exhibits CAS characteristics. Furthermore, we presented two key processes, information aggregation and information composition that are crucial to model the behavior of such complex targets. In particular, methodologies for incorporating information from multiple intelligent sources with varying reliabilities were described. The significance of modeling the NCO capabilities of the target system and ability of caBKBs to leverage the N-COPP framework for efficient network representation and network performance analysis were also presented. We developed an initial measure to analyze the level of self-synchronization in real-world based military target systems. We designed a Somali piracy based target modeling scenario, modeled their physical (communication) and social network structure and illustrated the information aggregation process using caBKBs. In particular, we analyzed how events, actions, situational awareness and intelligence information reliability influence the level of self-synchronization between the Somali pirate crews.

As future work, we plan to study the interaction between network dynamism and information aggregation. We will investigate how to efficiently perform information aggregation when the underlying network structure of the target system is continuously evolving. We are also interested in developing a systematic procedure to identify conditions that can induce substantial change in the behavior of the system and its components, and applying information composition process to model the effects of such radical changes. In addition, we will extend the Somali piracy scenario by explicitly modeling the pirate groups underlying network infrastructures and modeling interactions among other entities such as foreign navies, neighboring pirate crews and other stakeholders.

## ACKNOWLEDGEMENT

This work was supported in part by the Naval Postgraduate School, under grant No. N00244-15-1-0046.

## REFERENCES

[1] Cebrowski, A. k, Garstka, J.J., "Network-centric warfare: Its origin and future," US Nav. Inst. Proc. **124**(1), 28–35 (1998).

[2] Shirk, D., Wallman, J., "Understanding Mexico's Drug Violence," J. Conflict Resolut. **59**(8), 1348–1376 (2015).

[3] Bakker, E., Singleton, M., "Foreign Fighters in the Syria and Iraq Conflict: Statistics and Characteristics of a Rapidly Growing Phenomenon," [Foreign Fighters under International Law and Beyond], A. de Guttry, F. Capone, and C. Paulussen, Eds., T.M.C. Asser Press, The Hague, 9–25 (2016).

[4] Stone, L.D., Corwin, T.L., Barlow, C.A., [Bayesian Multiple Target Tracking], Artech House (1999).

[5] Holland, J., "Studying complex adaptive systems," J. Syst. Sci. Complex. **19**, 1–8 (2006).

[6] Santos Jr., E., Santos, E.S., "A Framework for Building Knowledge-Bases Under Uncertainty," J. Exp. Theor. Artif. Intell. **11**, 265–286 (1999).

[7] Santos, E.E., Santos Jr., E., Korah, J., Thompson, J.E., Gu, Q., Kim, K.J., Li, D., Russell, J., Subramanian, S., et al., "Modeling emergent border-crossing behaviors during pandemics," SPIE Defense, Secur. Sens., E. M. Carapezza, Ed., International Society for Optics and Photonics (2013).

[8] Santos, E.E., Santos Jr., E., Wilkinson, J.T., Korah, J., Kim, K., Li, D., Yu, F., "Modeling complex social scenarios using culturally infused social networks," Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern., 3009–3016, Anchorage, AK (2011).

[9] Santos, E.E., Santos Jr., E., Korah, J., George, R.M., Gu, Q., Jurmain, J., Kim, K., Li, D., Russell, J., et al., "Incorporating Social Theories in Computational Behavioral Models," Proc. Seventh Int. Conf. Soc. Comput. Model. Predict., 341–349 (2014).

[10] Santos Jr., E., Wilkinson, J.T., Santos, E.E., "Bayesian Knowledge Fusion," Proc. Twenty-Second Int. Florida Artif. Intell. Res. Soc. Conf. (2009).

[11] Santos, E.E., "A framework for assessing and predicting network loads and performance for network-centric operations and warfare," Proc. SPIE **6578**, R. Suresh, Ed., International Society for Optics and Photonics (2007).

[12] Santos, E.E., Santos Jr., E., Korah, J., George, R., Gu, Q., Kim, K., Li, D., Russell, J., Subramanian, S., "Modeling Socio-Cultural Processes in Network Centric Environments," SPIE Defense, Secur. Sens., R. Suresh, Ed., 84050A–84050A–14, International Society for Optics and Photonics (2012).

[13] Santos, E.E., Ojha, A., Korah, J., "Modeling situational awareness in network centric systems," Proc. SPIE **7350**, R. Suresh, Ed., International Society for Optics and Photonics (2009).

[14] Araki, L.M., "Self-Synchronization: What is it, How is it Created, and is it Needed," Newport, RI: Naval War College (1999).

[15] Kalman, R.E., "A New Approach to Linear Filtering and Prediction Problems," J. Basic Eng. **82**(1), 35 (1960).

[16] Olfati-Saber, R., "Distributed Kalman filter with embedded consensus filters," Proc. 44th IEEE Conf. Decis. Control. Eur. Control Conf. CDC-ECC '05 **2005**, 8179–8184 (2005).

[17] Olfati-Saber, R., Shamma, J.S., "Consensus Filters for Sensor Networks and Distributed Sensor Fusion," Proc. 44th IEEE Conf. Decis. Control(0), 6698–6703 (2005).

[18] Moffat, J., Bathe, M., Frewer, L., "The Hybrid War Model: a complex adaptive model of complex urban conflict," J. Simul. **5**(1), 58–68 (2010).

[19] Office of the Deputy Under Secretary of Defense for Acquisition and Technology, "Systems and Software

Engineering. Systems Engineering Guide for Systems of Systems, Version 1.0," Washington, D.C. (2008).

[20] Willner, D., Chang, C., Dunn, K., "Kalman filter algorithms for a multi-sensor system," 1976 IEEE Conf. Decis. Control Incl. 15th Symp. Adapt. Process., 570–574, IEEE (1976).

[21] Rao, B.S., Durrant-Whyte, H.F., "Fully decentralised algorithm for multisensor Kalman filtering," IEE Proc. D Control Theory Appl. **138**(5), 413 (1991).

[22] Li, X.R., Jilkov, V.P., "Survey of Maneuvering Target Tracking. Part I: Dynamic Models," IEEE Trans. Aerosp. Electron. Syst. **39**(4), 1333–1364 (2003).

[23] Smith, D., Singh, S., "Approaches to multisensor data fusion in target tracking: A survey," IEEE Trans. Knowl. Data Eng. **18**(12), 1696–1710 (2006).

[24] Ackerson, G.A., Fu, K.S., "On State Estimation in Switching Environments," IEEE Trans. Automat. Contr. **AC-15**(1), 10–17 (1970).

[25] Bar-Shalom, Y., "Interacting multiple model algorithm for systems with Markovian switching coefficients.," IEEE Trans. Automat. Contr. **33**(8), 780–783 (1988).

[26] Chen, B., Tugnait, J.K., "Tracking of multiple maneuvering targets in clutter using IMM/JPDA filtering and fixed-lag smoothing," Automatica **37**(2), 239–249 (2001).

[27] Mazor, E., Averbuch, A., Bar-Shalom, Y., Dayan, J., "Interacting multiple model methods in target tracking: A survey," IEEE Trans. Aerosp. Electron. Syst. **34**(1), 103–123 (1998).

[28] Li, W., Wang, Z., Wei, G., Ma, L., Hu, J., Ding, D., "A Survey on Multisensor Fusion and Consensus Filtering for Sensor Networks," Discret. Dyn. Nat. Soc. **2015** (2015).

[29] Olfati-Saber, R., Fax, J.A., Murray, R.M., "Consensus and cooperation in networked multi-agent systems," Proc. IEEE **95**(1), 215–233 (2007).

[30] Boyd, S., Lall, S., "A scheme for robust distributed sensor fusion based on average consensus," IPSN 2005. Fourth Int. Symp. Inf. Process. Sens. Networks, 2005., 63–70 (2005).

[31] Gupta, G., Younis, M., "Fault-tolerant clustering of wireless sensor networks," Proc. IEEE WCNC **3**(C), 1 (2003).

[32] Liang, Q., Cheng, X., "KUPS: Knowledge-based ubiquitous and persistent sensor networks for threat assessment," IEEE Trans. Aerosp. Electron. Syst. **44**(3), 1060–1069 (2008).

[33] Ge, Y., Qiu, X., Huang, K., "Conceptual interoperability model of NCW simulation," Proc. 2010 IEEE Int. Conf. Inf. Theory Inf. Secur. ICITIS 2010, 911–914 (2010).

[34] Shin, K., Nam, H., Lee, T., "Communication modeling for a combat simulation in a network centric warfare environment," Proc. 2013 Winter Simul. Conf. - Simul. Mak. Decis. a Complex World, WSC 2013, 1503–1514 (2013).

[35] Lauren, M., Stephen, R., "Map-aware non-uniform automata (MANA)-A New Zealand approach to scenario modelling," J. Battlef. Technol. **5**(1) (2002).

[36] Ross, J.L., "A Comparative Study of Simulation Software for Modeling Stability Operations," Proc. 2012 Symp. Mil. Model. Simul. (2012).

[37] Minar, N., Burkhart, R., Langton, C., Askenazi, M., "The Swarm Simulation System : A Toolkit for Building Multi-agent Simulations," Simulation, 1–11 (1996).

[38] Cil, I., Mala, M., "A multi-agent architecture for modelling and simulation of small military unit combat in asymmetric warfare," Expert Syst. Appl. **37**(2), 1331–1343 (2010).

[39] DiMario, M.J., "System of Systems Interoperability Types and Characteristics in Joint Command and Control," 2006 IEEE/SMC Int. Conf. Syst. Syst. Eng., 222–227, IEEE (2006).

[40] Meilich, A., "System of Systems (SoS) Engineering & Architecture Challenges in a Net Centric Environment," 2006 IEEE/SMC Int. Conf. Syst. Syst. Eng., 1–5 (2006).

[41] Neema, S., Bapty, T., Koutsoukos, X., Neema, H., Sztipanovits, J., Karsai, G., "Model Based Integration and Experimentation of Information Fusion and C2 Systems," Fusion 2009 12Th Int. Conf. Inf. Fusion, Vols 1-4, 1958–1965 (2009).

[42] Santos Jr., E., Wilkinson, J.T., Santos, E.E., "Fusing multiple Bayesian knowledge sources," Int. J. Approx. Reason. **52**(7), 935–947 (2011).

[43] Percy, S., Shortland, A., "The Business of Piracy in Somalia," J. Strateg. Stud. **36**(4), 541–578 (2013).

[44] Anderson, L., "Demystifying the Arab spring: Parsing the Differences Between Tunisia, Egypt, and Libya," Foreign Aff. **90**(3), 2–7 (2011).

[45] Santos, E.E., Santos Jr., E., Korah, J., Thompson, J.E., Kim, K., George, R., Gu, Q., Jurmain, J., Subramanian, S., et al., "Intent-Driven Behavioral Modeling during Cross-Border Epidemics," Privacy, Secur. Risk Trust 2011 IEEE Third Inernational Conf. Soc. Comput. (SocialCom), 2011 IEEE Third Int. Conf., 748–755 (2011).

[46] Santos Jr., E., Zhao, Q., "Adversarial Models for Opponent Intent Inferencing," [Adversarial Reasoning: Computational Approaches to Reading the Opponents Mind], A. Kott and W. McEneaney, Eds., Chapman & Hall/CRC, Boca Raton, 1–22 (2006).

[47] Rosen, T., Shimony, S.E., Santos Jr., E., "Reasoning with BKBs – Algorithms and Complexity," Ann. Math. Artif. Intell. **40**(3/4), 403–425 (2004).

[48] van Bezooije, B., Essens, P., Vogelaar, A., "Military self-synchronization: An exploration of the concept," Proc. 11th Int. Command Control Res. Technol. Symp. (2006).

[49] Ploch, L., Blanchard, C.M., O'Rourke, R., Mason, R.C., King, R.O., "Piracy off the horn of Africa," Econ. Polit. Soc. Issues Africa, 180–208 (2011).

[50] Beatriz Binkley, Laura Smith, "Somali Pirates: The Anatomy of Attacks," <http://research.ridgway.pitt.edu/blog/2010/09/28/pirate-attacks/> (1 January 2017 ).

[51] Gardner, F., "Somalia ship hijack: Maritime piracy threatens to return," BBC News, 2017, <http://www.bbc.com/news/world-africa-39283911> (4 July 2017 ).

[52] "Somalia piracy: India ship hijacked in new attack," BBC News, 2017, <http://www.bbc.com/news/world-africa-39478457> (4 July 2017 ).

[53] Hallwood, P., Miceli, T.J., "An Economic Analysis of Maritime Piracy and its Control," Scott. J. Polit. Econ. **60**(4), 343–359 (2013).

[54] Mejia Jr., M.Q., Cariou, P., Wolff, F.-C., "Is maritime piracy random?," Appl. Econ. Lett. **16**(9), 891–895 (2009).

[55] Hallwood, C., Miceli, T., [Maritime Piracy and Its Control: An Economic Analysis], Springer (2014).

[56] Williams, R.L., "Somalia Piracy: Challenges and Solutions," ARMY WAR COLLEGE CARLISLE BARRACKS PA (2013).