

16th ICCRTS
“Collective C2 in Multinational Civil-Military Operations”

Distributed Threat Evaluation in Naval Tactical Battle Management

Topics:

Topic 8: Architectures, Technologies, and Tools
Topic 10: C2, Management, and Governance in Civil-Military Operations

Authors:

Hengameh Irandoust, Abder Benaskeur, Philippe Bellefeuille,
and Froduald Kabanza

Point of Contact:

Hengameh Irandoust
Decision Support Systems for C2 Section,
Defence R&D Canada – Valcartier
2459 blvd. Pie XI North, Québec, QC, G3J 1X5, Canada
Telephone +1 (418) 844-4000 x4193
hengameh.irandoust@drdc-rddc.gc.ca

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUN 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Distributed Threat Evaluation in Naval Tactical Battle Management			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defence R&D Center - Valcartier, Decision Support Systems for C2 Section, 2459 blvd. Pie XI North, Quebec, QC, G3J 1X5, Canada,			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.					
14. ABSTRACT Threat evaluation is a critical function in naval battle management command and control. It involves taking into account a large number of variables and requires making complex inferences under time and uncertainty constraints. Collaborative threat evaluation within a multi-unit and geographically dispersed force can reduce the uncertainty factor by bringing additional information sources and computational power and providing more capability and robustness. However, it also introduces many communication and coordination challenges. This paper presents an automated and adaptive capability that performs threat evaluation for a naval task force. The proposed capability supports different coordination methods, each enforcing a different approach to collaborative threat evaluation in the distributed context of force operations. Moreover, it adapts its coordination method to changes in the tactical situation, whether dictated by the status of the communication links or as the consequence of the choice of a specific command structure by the force command team. Besides the coordination layer, the capability includes a set of threat evaluation algorithms that determine the level and the ranking of threats. A modeling and simulation environment has been developed to allow the evaluation and demonstration of the force-level threat evaluation capability.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 43	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Distributed Threat Evaluation in Naval Tactical Battle Management

H. Irandoust, A. Benaskeur, P. Bellefeuille, F. Kabanza

ABSTRACT

Threat evaluation is a critical function in naval battle management command and control. It involves taking into account a large number of variables and requires making complex inferences under time and uncertainty constraints. Collaborative threat evaluation within a multi-unit and geographically dispersed force can reduce the uncertainty factor by bringing additional information sources and computational power and providing more capability and robustness. However, it also introduces many communication and coordination challenges. This paper presents an automated and adaptive capability that performs threat evaluation for a naval task force. The proposed capability supports different coordination methods, each enforcing a different approach to collaborative threat evaluation in the distributed context of force operations. Moreover, it adapts its coordination method to changes in the tactical situation, whether dictated by the status of the communication links or as the consequence of the choice of a specific command structure by the force command team. Besides the coordination layer, the capability includes a set of threat evaluation algorithms that determine the level and the ranking of threats. A modeling and simulation environment has been developed to allow the evaluation and demonstration of the force-level threat evaluation capability.

1. INTRODUCTION

Threat evaluation is a critical function in naval battle management Command and Control (C2). It consists in determining the level of threat and the level of priority associated with entities within a certain area of interest. Threat evaluation is a complex task that involves the consideration of a large number of variables and requires making complex inferences under time and uncertainty constraints. This complexity is further increased in the context of force operations, where multiple units interact and operate conjointly to perform C2 activities and achieve the mission objectives. The geographical dispersal of the units improves information superiority by multiplying the information sources and may provide more capability and robustness to the force. However, distribution also introduces many additional challenges.

This paper presents an automated and adaptive capability that addresses two of the main challenges in force-level threat evaluation, that is, information exchange and activity coordination. There exists a large spectrum of coordination patterns along which a multi-unit force can cooperate and exchange information. The proposed capability supports three main coordination methods, each enforcing a different approach to collaborative threat evaluation. Furthermore, it adapts to dynamic changes in the tactical situation, whether dictated by the

status of the communication channels or as the consequence of the choice of a specific command structure by the force command authority.

Section 2 introduces the problem of threat evaluation from a naval C2 perspective. Threat evaluation is viewed as based on the determination of an object's intent, capability and opportunity to inflict harm. The problem of distributed threat evaluation is discussed in Section 3, as a particular case of distributed systems with its advantages and issues. The proposed capability is presented in Section 4, including an overview of the system, the modeling and simulation environment that enables the evaluation and demonstration of the force-level threat evaluation capability, the threat evaluation algorithms, as well as a brief survey of the body of existing work on threat evaluation. Section 5 presents the coordination approaches the capability can address. Finally, the scenario used to test the proposed capability is briefly described in Section 6.

2. THREAT EVALUATION PROCESS

C2 is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

The C2 process, in the context of naval battle management, can be decomposed into a set of generally accepted functions that must be executed within some reasonable delays to ensure mission success (Figure 1). These functions generally include: Picture Compilation; Threat evaluation; Engageability Assessment; and Combat Power Management¹.

The process of all actions and activities aimed at maintaining tracks of all surface, air, and subsurface entities with a certain volume of interest is referred to as *Picture Compilation*. It includes several sub-processes, the most important being *object localization* (or tracking) and *object recognition and identification*. *Threat Evaluation* establishes the likelihood that certain entities within that volume of interest will cause harm to a defending force or its interests. The output of threat evaluation along with that of the engageability assessment process, which determines the defending force options against the threat, is used by the combat power management process to generate a response plan.

It is generally accepted that three concepts are central to the notion of threat. To constitute a threat, an entity must possess the intent or be intended to cause harm, and have the capability and opportunity to achieve this intent [16][17][19].

¹ Also often referred to as Weapons Assignment, although we argue [2][3] that the latter does not consider all the problems related to Combat Power Management.

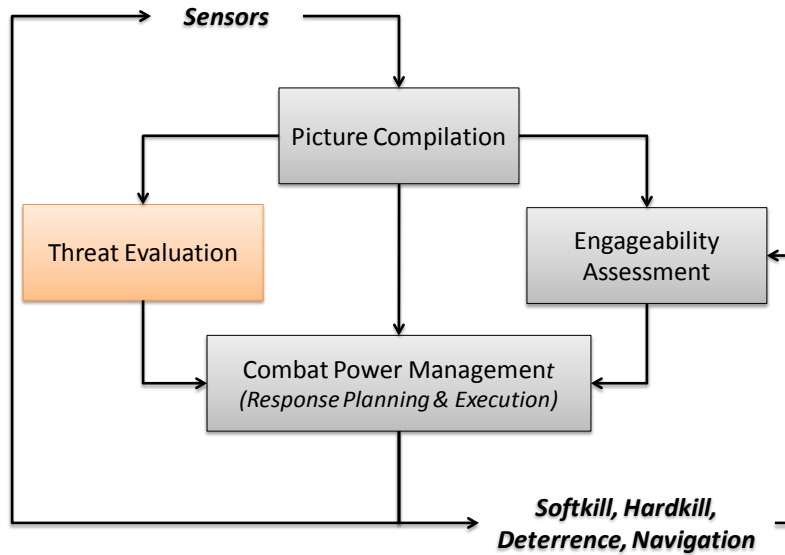


Figure 1: Naval C2 Processes

- Intent is defined as the goal of the threat. Intent assessment determines (using all available evidences) whether the object of interest intends to cause harm.
- Capability is defined as the ability of an object to achieve its goal and/or plan (or part thereof) as determined by the intent.
- Opportunity is defined as the existence in the environment of the required preconditions for the threat's goal/plan to succeed.

In operational environments, such as the naval military setting, threat evaluation is often defined as the problem of determining the level of threat of entities in a volume of interest and the level of priority associated to those threats [7]. The level of threat indicates to what extent an entity is threatening. The level of priority indicates how much attention an observer should devote to that entity. Threat evaluation is conducted based on a priori knowledge (e.g., intelligence, operational constraints and restraints, evaluation criteria, etc.), dynamically acquired and inferred information (e.g., kinematics and identification of entities in a given volume of interest, as well as various indicators), and data received from complementary sources in relation to the mission objectives. The outcome of the threat evaluation process is a prioritized list of threats that should be engaged using some kind of combat power, contingent the availability of engagement solutions.

3. COLLABORATIVE THREAT EVALUATION

In dispersed force operations, own and friendly units operate conjointly to achieve the mission objectives. This configuration involves distributed teams on air, surface and subsurface

units cooperatively interacting to perform C2 activities (Figure 1). The geographical dispersal of the units improves information superiority by multiplying the information sources; however, distribution introduces additional challenges. One major challenge is the coordination of units for information exchange.

In effect, when operating as a force, the different units must achieve a certain level of shared situation awareness through information sharing. Ultimately, they have to come up with a consistent (conflict-free) threat list to act upon. This requires a certain level of coordination which can be performed in different ways.

The remainder of this section discusses some of the advantages of distributed threat evaluation and some of its operational hurdles. The different coordination methods that can be used in collaborative threat evaluation are then presented.

3.1. Advantages of Distributed Threat Evaluation

Distributed threat evaluation inherently offers the following advantages of distributed systems:

- **Functional separation:** Distributed threat evaluation spatially distributes entities that perform different tasks based on their capability and purpose. This function specialization simplifies the design of the system, as the latter is split into entities, each of which implementing part of the global functionality and communicating with the other entities.
- **Information superiority:** The main advantage of a distributed system is its ability to allow the sharing of information and resources. Information and knowledge provided by other sources and their fusion into a common picture, enhances the quality of the assessment and supports informed decision making.
- **Enhanced real-time response:** Increased responsiveness is one of the major requirements of threat evaluation. This can be achieved through distribution by deploying observers and processors close to the threat. In a networked environment, this has the potential of improving the flow of real-time information directly to decision makers, providing means of rapidly assessing changing situations.
- **Robustness and resilience:** Distributed threat evaluation has a *partial-failure* property in that, even if some agents (including human, software and hardware) fail, others can still achieve the task (at least partly). Such failure would only degrade, not disable, the whole evaluation outcome. If the distributed system has self-organization capabilities, it can also dynamically re-organize the way in which the individual entities are deployed. This feature makes the system highly tolerant to the failure and bias of individual entities.

3.2. Communication and Coordination

The above advantages require that the components of the system performing threat evaluation be able to exchange information clearly and in a timely manner. The lack of the following requirements can sometimes be an impediment to effective communication in a distributed context:

- **Interoperability:** This is the ability of two or more agents, systems or components to exchange information and to use the information that has been exchanged. Distributed threat evaluation can encompass a heterogeneous set of individuals and computational entities that must be able to communicate and cooperate despite differences in language, context, format or content.
- **Connectivity:** Establishment of communications can be troublesome by itself. Provision of remote connectivity between the nodes in distributed threat evaluation is a major technical challenge which cannot be understated. Maintaining a communication channel is not guaranteed and, when it is, its quality can be degraded due to multiple environmental factors. Communications can also be hampered in an attempt by different units to use certain communication frequencies while remaining covert to minimize the detection, localization, and recognition by the opposing forces through the electromagnetic emissions [1]. Kopp [10] listed security of transmission, robustness of transmission, transmission capacity, message, and signal routing and signal format and communications protocol compatibility as the main challenges of communication media in military domain, although most of them apply also to non-military domains.
- **Security:** Threat evaluation represents a specific domain of interest that highly correlates with information system security. Although the use of multiple distributed sources of information and analyzers can improve situational awareness, it can make the system more vulnerable to unauthorized access, use, disclosure, disruption, modification or destruction.

3.3. Threat Evaluation Coordination Methods

In a task force, each unit receives from its sensors information about its local operational environment that may differ from the other units. Yet, to coordinate actions properly, it is important that all units reach the same conclusion on which objects/events pose a threat to the force or to its mission.

There is a large spectrum of coordination methods along which a multi-unit force can cooperate. Furthermore, for threat evaluation, the coordination can be done along two axes: picture compilation and threat evaluation. The system presented in this paper supports three different coordination methods. Although they do not cover the whole spectrum of possible

coordination mechanisms, they show how the system can adapt to different coordination requirements and even adapt its coordination approach to the evolving situation.

The three different coordination methods currently used by the system are:

- **Centralized Picture Compilation and Centralized Threat Evaluation (CC):** In this coordination method, a single central unit (*e.g.*, a command ship) compiles the tactical picture using information provided by the other units in the task force. This tactical picture combines the track information from every unit in a single conflict-free tactical picture. The central unit then uses this tactical picture to produce, centrally, a force-level threat evaluation list.
- **Decentralized Picture Compilation and Centralized Threat Evaluation (DC):** In this coordination method, the units de-conflict their tactical pictures in a decentralized way. Each unit will have its own tactical picture that is coherent with the tactical picture of other units in the force. These pictures may represent only partial views of the global situation. Each unit then produces a local threat evaluation based on its own tactical picture, and shares the result with a central unit. The central unit combines those partial threat evaluations to produce, centrally, a single force-level threat evaluation list.
- **Decentralized Picture Compilation and Decentralized Threat Evaluation (DD):** In this coordination method, tactical pictures are produced in much the same way as in the DC coordination method. However, the units collaborate together to produce the force-level threat evaluation list. Rather than sharing the whole threat evaluation information, they share the minimum information required to insure a consistent force-level threat evaluation amongst all units.

Naval operations take place in dynamic situations and the units may have to switch from one configuration to another. For example, units may have to accommodate degradation in the communication links, or even loss of communication, as well as modifications to the force composition (*e.g.*, units leaving or joining the force).

4. OVERVIEW OF THE SYSTEM

This section gives an overview of the main components of the proposed solution and the modelling and simulation environment used to test and demonstrate it.

The system (Figure 2) is comprised of a simulation testbed (Layers 1 & 2); threat evaluation algorithms (Layer 3); and an advisory system (Layer 4). Scenarios related to naval Anti-Air Warfare (AAW) operations are generated, simulated, and visualized in the testbed. In Section 4.1, emphasis is put on this component that allows simulation of force-level threat evaluation and the application of the different coordination methods. The threat evaluation algorithms are briefly described in Section 4.2. They allow for identification and evaluation of air threats.

Currently, a rule-based algorithm and a probabilistic plan recognition algorithm are implemented. The Advisory Capability manages the interactions between the operator and the automation and the information provided through the Operator-Machine Interfaces (OMI). The features of the advisory system are presented in [8] and are not discussed in this paper.

4.1. Testbed

To run the threat evaluation system, we use a testbed that simulates the environment and entities around the task force as well as the behaviour of the ships' sensors. The testbed uses three Commercial off the Shelf (COTS) applications which are connected together to provide realistic simulation of threatening situations: Stage Scenario from Preagis, Ship Air Defence Model from BAE Systems, and SIMDIS developed by the Naval Research Lab.

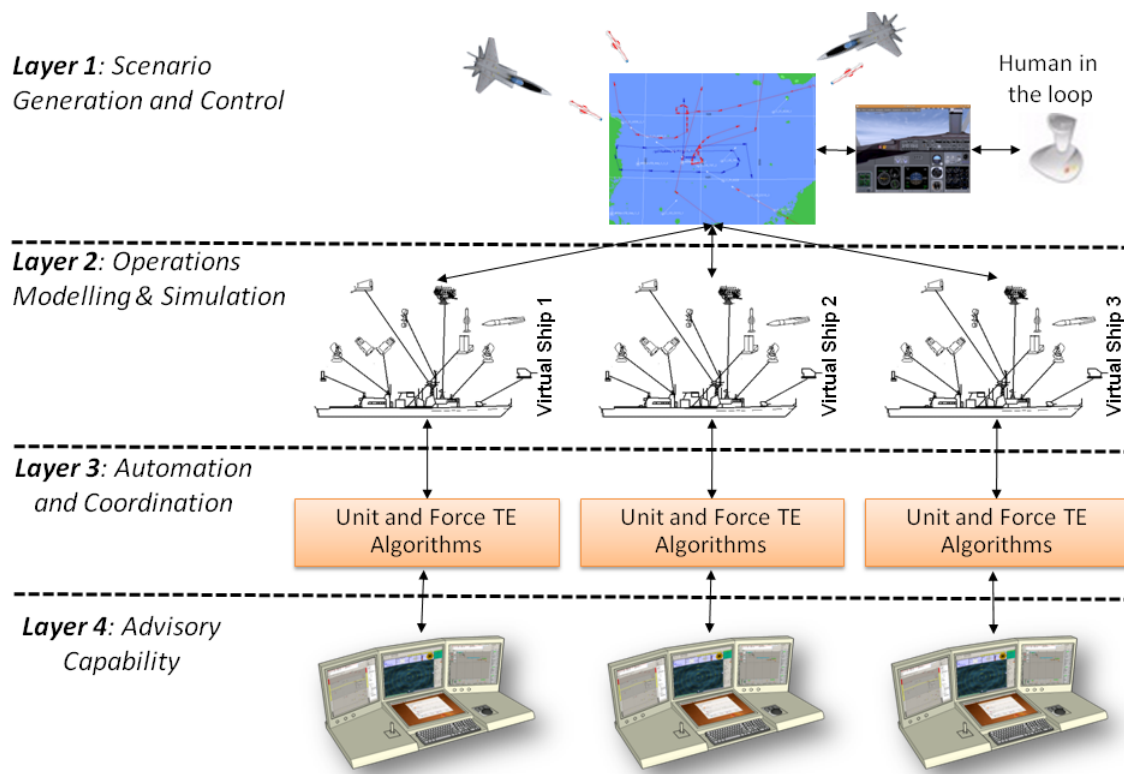


Figure 2: Force-Level Testbed

Stage, as part of Layer 1, simulates the ground truth by controlling the opposing force entities as well as the civilian traffic. It allows creating complex scenarios and scripting advanced behaviours for the different entities in the simulation. SADM, as the main component of Layer 2, provides realistic modelling and simulation of the ships' sensors and weapons systems. When an entity in Stage or a ship in the task force launches a missile, SADM takes control of that missile in order to simulate realistic high-fidelity engagements. Two instances of SIMDIS can run on the testbed. One is used to provide 3D visualization of the ground truth

while the other presents a comprehensive tactical picture, as generated by the sensors in SADM. Table 1 provides a summary of the components of the testbed.

Table 1: The Modeling and Simulation Environment Components

Component	Role
SADM	Simulates ownship (sensors, weapons) Simulates threats (seekers, weapons) Generates system track data Processes commands from C2 application
STAGE	Used as scenario generator Simulates blue, red, and neutral entities Entity information provided to SADM
SIMDIS	Provides 3D view of scenario (ground truth) Provides 2D physical display (tactical picture)
Open Splice DDS	Middleware for data distribution
Data Router	Handles communication between various components in the tested

4.2. Threat Evaluation Algorithms

The system evaluates threats posed to the task force and its mission. It evaluates threats along three axes: intent, capability, and opportunity, as discussed previously. The system attempts to answer the following questions through observation of the environment and dynamic inference:

- **Intent:** Does the track intend to harm members of the task force or hinder the task force's mission?
- **Capability:** Does the track possess the necessary equipment and abilities to harm members of the task force or hinder the mission?
- **Opportunity:** Is the track, or will the track be, in a position to harm a member of the task force or hinder the mission?

Some of the threat indicators can be directly observed (*e.g.*, bearing, range, speed, etc.), while others need simple calculations (*e.g.*, Closest Point of Approach – CPA, flight profile) or advanced calculations (*e.g.*, third party targeting), and still others could require knowledge-based inference. Indicators are derived from track characteristics, tactical data, background

geopolitical situation, geography, intelligence reports, and other data. The indicators observed may be relative to any of the three key ingredients.

Using the indicators and a set of rules of the following form:

IF indicator₁ AND indicator₂ AND AND indicator_n THEN intent / capability / opportunity true

The system evaluates the intent, capability and/or opportunity of the tracks in the force's volume of interest. It then classifies each track in three classes: High Threat, Medium Threat and Low Threat. To do so, the system uses a decision tree (Figure 3), where each leaf node corresponds to a threat level. Although not shown here, each leaf node, in addition to having a threat level, also has a unique value (called node weight) that allows the system to quickly compare the threats and rank the threat within the same level. For instance, the leaf node reached when a track has both capability and opportunity but not intent has a higher node weight than the one reached when the track has intent, but neither capability nor opportunity. As such, everything else being equal, a track reaching the former will be ranked higher than a track reaching the latter, even though both are medium level threats.

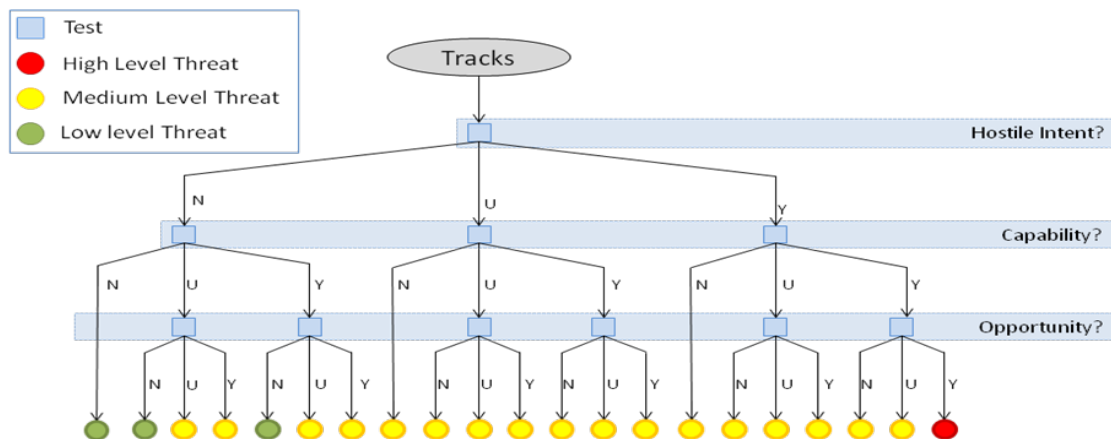


Figure 3: Threat Evaluation Decision Tree

The threat evaluation system outputs a ranked list of threats. The rules used for the ranking are as follows:

1. Rank the threats by threat level;
2. For threats with the same threat level, rank them according to the priority of the asset they threaten;
3. For threats that are still equal, rank them according to their node weight;
4. For threats that are still equal, rank them according to their lethality;
5. For threats that are still equal, rank them by track number (lower number gets higher ranking).

The threat evaluation solution, implemented in Layer 3 of the system shown in Figure 2, combines the above described rule-based reasoning with a plan recognition algorithm based on PHATT [4]. By allowing the rules to be evaluated on both simple cues from the tactical picture and cues derived from the plan recognition results, the proposed solution greatly reduces the number of rules that need to be specified while still providing very advanced reasoning. For instance, our system allows rules such as:

IF attackPlan(aircraft) THEN intent(aircraft),

where “attackPlan” is derived from the output of the plan recognition algorithm. In order to emulate this simple rule, a rule-based system with no plan recognition capability would need a large number of rules to represent all the possible plans that lead to an attack.

4.2.1. Related Work

Multiple approaches to threat evaluation have been explored in the literature. Among them, the more common ones are case-based reasoning [12], rule-based reasoning [20], fuzzy logics [11], and probabilistic inference [9][13][14][15], sometimes for plan recognition [4][5][6][18]. Although many of these approaches do not address warfare applications specifically, their algorithmic theoretic foundations are related to threat evaluation problem as discussed herein.

The uncertainty characterizing data and inferences in threat evaluation has led many authors to use probabilistic approaches, and more particularly Bayesian networks. Johansson and Falkman [9] used a Bayesian network to evaluate the threat level of an aircraft as a function of many parameters such as the speed, distance, weapon range and type of the aircraft. Heinze et al. [6] use Bayesian networks to recognize manoeuvres of air threats from raw trajectories using a spatial reasoning system. Santos and Zhao [18] also use Bayesian networks for plan recognition where the goals are the assets targeted by the threats. The main difficulty in probabilistic approaches lies in finding the correct a priori and conditional probabilities. This is especially true for a domain as complex as the naval warfare, as there are few reference cases on which one can base the probability estimates.

Geib and Goldman [4] use Hidden Markov Models (HMM) for plan recognition. Their Probabilistic Hostile Agent Task Tracker (PHATT) compares the sequence of observed actions from the observed agent to plans in a plan library and to the actions in the set of actions which are enabled by previous steps, in order to: (i) generate hypotheses on the agent’s goals; (ii) compute the probability of each hypothesis; and (iii) calculate the next pending set. In PHATT, plans are represented as Hierarchical Task Networks (HTN) and the algorithm must maintain copies of the tree structures in memory for the different hypotheses. Yet Another Probabilistic Plan Recognizer (Yappr) [5] improves on this by using probabilistic grammars and string re-writing.

5. COORDINATION METHODS

This section illustrates three coordination methods implemented by the system. These are only three possibilities in a large spectrum of possible methods, but are the most realistic and are different enough from each other to illustrate the adaptive nature of the proposed system. Each coordination method is described in its default operational mode and in situations where it recovers from a loss of communication with a unit in the force. It is then shown how the system switches between the different coordination methods to adapt to degradation of communications.

5.1. Centralized Picture Compilation and Centralized Threat Evaluation (CC)

In this coordination approach (Figure 4), one unit (the central command ship) is responsible for compiling the common tactical picture, performing force-level threat evaluation, and sending the results of picture compilation and threat evaluation to all units. All other units only have the responsibility to send the tactical information they have gathered to the central unit. They do not perform force-level threat evaluation.

This coordination approach is the easiest one from an algorithmic perspective because the central unit has access to all the information and, because it is the only one to produce the output, there are no conflicts to be resolved. On the downside, it is the most demanding approach on a communication level since it requires all the subordinate units to send constant updates of their bulk local tactical picture at a high update rate.

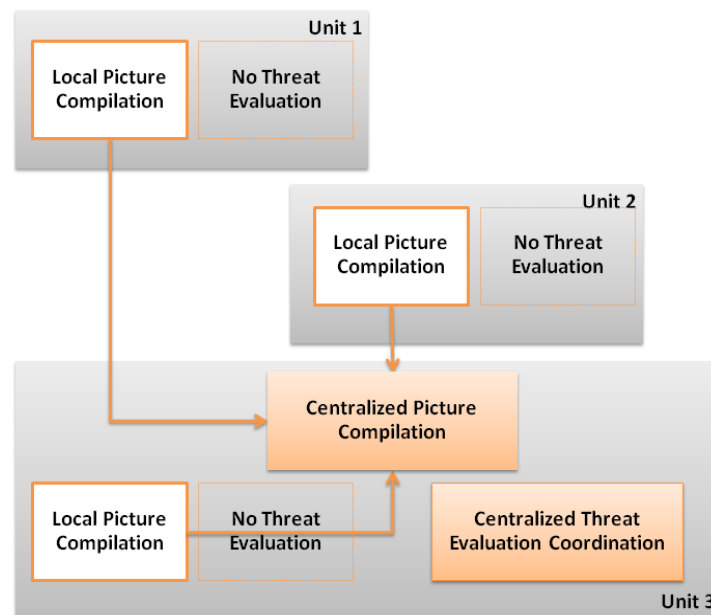


Figure 4: Centralized Picture Compilation and Centralized Threat Evaluation

5.2. Decentralized Picture Compilation and Centralized Threat Evaluation (DC)

In this coordination approach (Figure 5), force-level threat evaluation is performed independently on each unit using a coherent, but partial tactical picture. Each unit uses an identical threat evaluation algorithm and the same criteria. This results in each unit having a partial force-level threat evaluation. One unit is therefore tasked to gather those partial evaluations in order to merge and de-conflict them. The result is then sent back to each unit so that the whole force uses the same threat evaluation list.

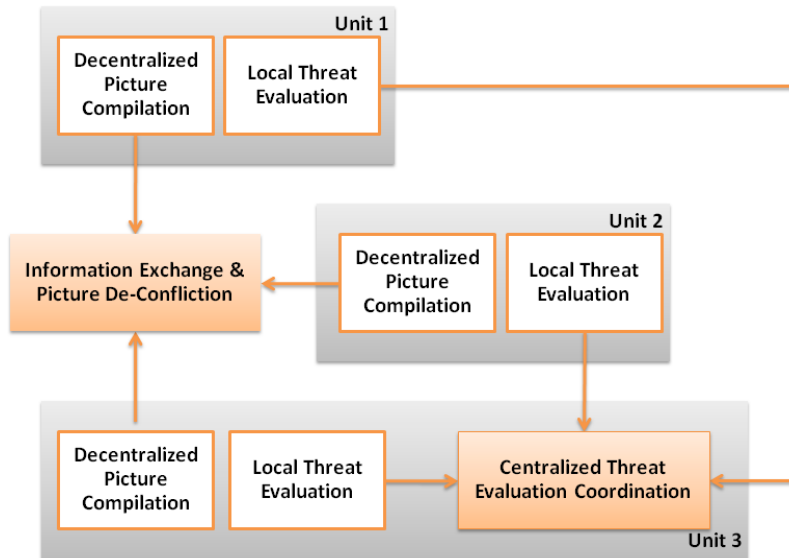


Figure 5: Decentralized Picture Compilation and Centralized Threat Evaluation

This coordination approach requires a more elaborate solution from the algorithmic perspective, as the central coordinating unit needs to resolve conflicts that may arise between evaluations from the different units (they each have a partial view of the situation that may differ from one another). On the flip side, this puts less stress on the communications because the rate at which the updates are sent to the central unit is much lower. Indeed, threat evaluation changes at a much slower pace than the tactical picture, and requires a smaller amount of data to be exchanged.

5.3. Decentralized Tactical Picture and Decentralized Threat Evaluation (DD)

In this coordination approach (Figure 6), each unit produces its partial threat evaluation in much the same way as they do in the previous (DC) approach. However, unlike the DC approach, the de-conflicting and merging is also done in a decentralized way here. Initially, each unit shares its local threat evaluation with the other units. Each unit then merges and de-conflicts locally all the received partial evaluations. Since all the units use the same set of algorithms and input data, the result is expected to be the same, at least in theory. As each unit does the merging and de-confliction, it takes note of the objects that are missing from, or are in

conflict with, its own evaluation, as well as the unit that sent the corresponding tracks. Those are the objects for which updates will be needed. The unit notifies each of the other units about the updates it needs. The updates will only be sent for requested or for newly acquired tracks (and only once per new track unless further requests are made for the same track). The complete threat evaluation is broadcast periodically to insure that no new conflicts have been detected.

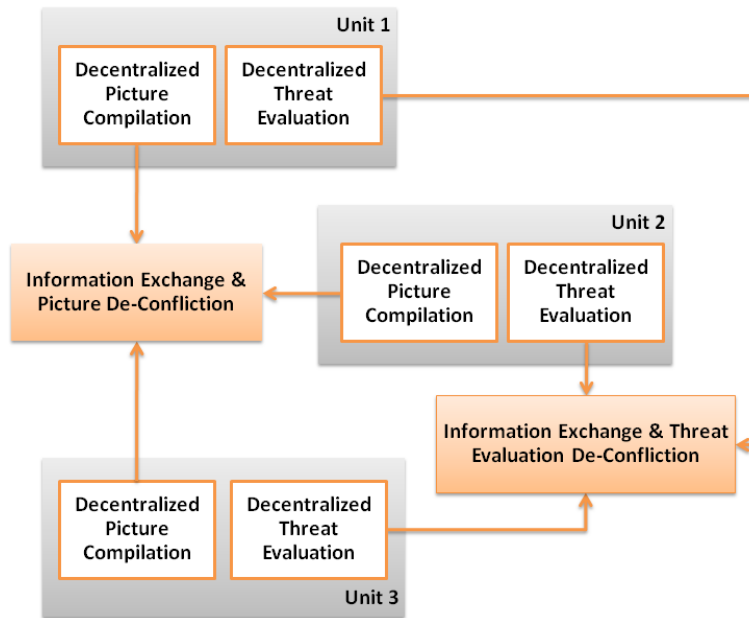


Figure 6: Decentralized Tactical Picture and Decentralized Threat Evaluation

To illustrate, let us assume the following scenario: three ships A, B and C and four tracks, 1001, 1002, 1003 and 1004 (Figure 7). The initial threat evaluation produced by each ship is shown in Table 2.

Let us first consider the point of view of Ship B. When merging the lists from A and C with its own, B will realize that track 1001 (maintained by A) is missing from its picture. It will further notice that track 1002 is in conflict, since at least one list (from the other ships) has it as high and at least one has it as medium. Again, the evaluation that conflicts with that of B comes from A. There is no conflict for track 1003, which is already on the list of B. Track 1004 is both missing from B's list and is in conflict (between A and C). In this situation, B will need to request track 1001 and 1002 from A. Since A and C reach different results regarding track 1004, B will need to request this track from both A and C. A will have to request track 1004 from C. To resolve the conflict on track 1002, A can request the track from either B or C as they both have the same results. The situation is the same for track 1003.

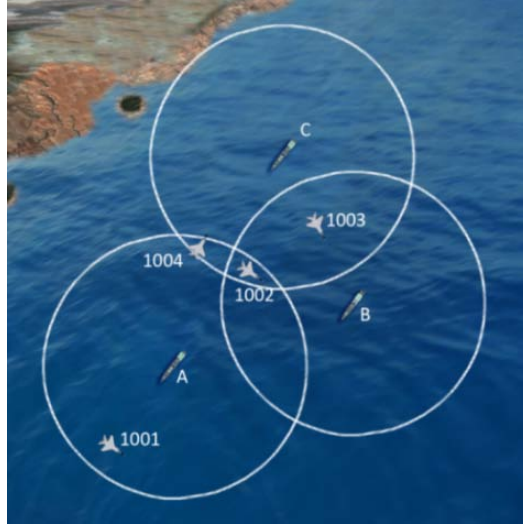


Figure 7: Illustration for Decentralized Threat Evaluation

Table 2: Initial Threat Evaluation Results for Each Ship

Track\Ship	A	B	C
1001	Low	---	---
1002	Medium	High	High
1003	---	Medium	Medium
1004	Low	---	Medium

This coordination approach is much more complex than the previous two (i.e., CC and DC) as it requires information exchange and de-confliction between the units to insure that they maintain a consistent force-level threat evaluation. However, since only a small part of the threat evaluation is exchanged, it typically requires a smaller bandwidth than the other two approaches. Nevertheless, in the worst case, where none of the units holds common tracks, they will need to exchange their complete threat evaluation each time. Such a case boils down to the centralized picture compilation/decentralized threat evaluation coordination mode.

5.4. Loss of Communication

Sometimes the force may lose communication with one of its units because of hardware failure or damage, loss of electrical power, opposing force jamming operations, etc.

Dealing with this situation depends on the adopted coordination approach and the unit with which communication is lost. In the case of CC and that of DC coordination approaches, losing communication with a unit other than the central one does not affect the ability of the rest of

the force to operate. It certainly affects the quality of the assessment because the central unit receives less information, but the force continues to function almost normally.

If communication with the central unit is lost, the whole coordination mechanism falls apart if nothing is done. In such a situation, two recovery methods are possible. The system can switch to the DD coordination approach until communication with the central unit is restored. If centralized coordination is absolutely required, then the system must transfer coordination responsibility to a new unit. To make this process simple and efficient, each unit has an ordered list of all units in the task force. If communication with the current central unit is lost, then the central responsibility is transferred to the next available unit on the list. Since all units in the task force have the same list, reconfiguration should occur seamlessly.

In the case of DD coordination, if communication with a unit is lost, it follows that some units will no longer receive updates on the tracks they had requested from that unit. Yet, it is possible for some other units in the task force to hold that track. In the example introduced earlier, if ship A requests track 1003 from ship B, and then communication with ship B is lost, ship A will no longer receive updates on ship 1003, even though ship C could provide them. To prevent such a problem, when communication with a unit is lost, all units broadcast their complete threat evaluation.

In case a unit loses communication with the whole task force, it will be on its own and will have to operate with its local tactical picture and partial threat evaluation.

5.5. Communication Degradation

In force operations, the network may become unable to support the amount of communication required for intra-unit coordination, whether because there are too many units, there are too many tracks in the area, some other process is putting strain on the network, or some technical difficulties have arisen. In order to maintain the real time aspect of the threat evaluation process, it is important to reduce the amount of communication required to a point where the network can support it without excessive delays.

As mentioned above, the amount of data transfer required for CC coordination is larger than the amount of data required for DC coordination, and much larger than that required for DD coordination. As such, in the case where the units are in CC coordination mode, a first solution would be to switch to the DC mode. If this is not enough, the system can then switch to the DD mode. Finally, if that is still not sufficient, the system can restrain the nature of data to be exchanged, by only allowing sharing of information on most threatening tracks. This solution will reduce the quality of the evaluation for low threats, but will keep the evaluation of the most important (and therefore most relevant) threats up-to-date (Figure 8). If the network reaches a point where even the coordination method that requires the least amount of

bandwidth is still unaffordable, then the system will consider itself to be in a situation of total loss of communication with all units.

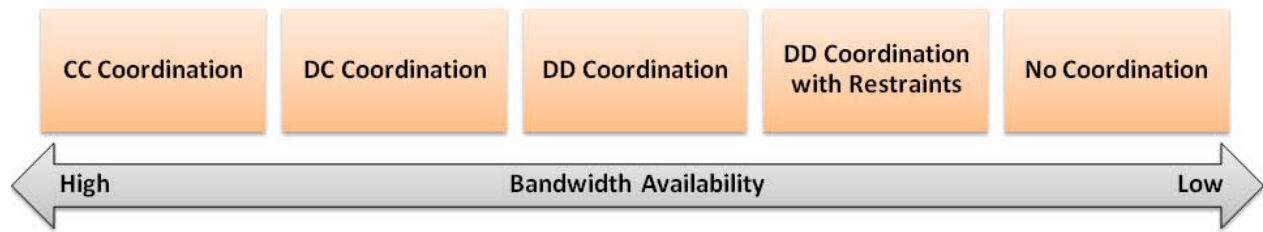


Figure 8: Coordination Mode vs. Bandwidth Availability

When the bandwidth capacity is restored, the system will gradually step back to the coordination mode it was using.

6. SCENARIO

The capability has been tested with a fictitious, yet realistic, naval warfare scenario (Figure 9) between a Naval Task Group (NTG) and the opposing force nation of *Orangeland* in the proximity of the neutral nation of *Blueland*.



Figure 9: Scenario

The scenario, set in the littoral where there is a high density of shipping and inshore fishing vessel traffic, describes a high tempo situation illustrating some of the challenges the

commander of the NTG may face during the conduct of operations with a focus on threat evaluation processes.

A base scenario was created presenting an NTG comprised of two frigates, a destroyer and a replenishment ship on route to enforce a UN Security Council Resolution (UNSCR) designed to prevent the shipment of goods into *Orangeland* ports. *Orangeland* has been uncooperative, but has not shown sign of hostility yet. Harassment from the fighter jets at the nearby airbase is to be expected, but an attack would be unlikely. *Orangeland's* harassment mission eventually escalates into an unexpected attack by one of the aircraft. From this scenario, various vignettes were derived to highlight coordination challenges in force threat evaluation system.

This scenario was used to characterize, from both operational and technological perspectives, the threat evaluation problem in naval force operations and to test the evaluation and coordination algorithms of the developed capability.

To test the adaptation mechanisms implemented, a communication channel has been modeled and different delays and limitations on the availability of the bandwidth have been simulated. To avoid frequent changes in the coordination mode, a hysteresis-based filter was added to the adaptation logics. Although exhaustive tests and performance evaluation are still to be conducted, preliminary results, obtained so far, have showed the ability of the proposed coordination approach to handle steady and transient limitations on the communications channels.

7. CONCLUSION

The conduct of threat evaluation has been increasingly challenging in modern complex environments. This paper presented an adaptive capability that supports threat evaluation coordination in the context of naval force operations. The capability not only offers different coordination modes, but allows coordination to cope with changes in the tactical situation, whether these changes are dictated by the status of the communication links or as the consequence of the choice of command structure by the force command team.

Threat evaluation presents the blue force analysis of the situation by considering the red perspective (i.e., behaviour of the opposing force). Work is currently in progress to build coordination mechanisms for the blue perspective. The latter, referred to as engageability assessment, is aimed at establishing the feasibility of response options for the blue force to counter the red force. Coordination modes, similar to those applied to threat evaluation, are being adapted to the distributed engageability assessment problem. The combined result of threat evaluation and engageability assessment capabilities will provide the force command team with all the information they need for the planning and execution of response actions, as part of combat power management.

REFERENCES

- [1] Athans, M. (1987) Command and Control (C2) Theory: A Challenge to Control Science, IEEE Transactions on Automatic Control, Vol. AC-32, No. 4.
- [2] Benaskeur, A. and F. Kabanza (2009), Combat Power Management for INCOMMANDS TDP: Integration of CORALS into the Command Decision Support Capability. DRDC Valcartier TR 2009-083, UNCLASSIFIED
- [3] Benaskeur, A., Kabanza, F., Beaudry, E., and Beaudoin, M. (2008). A probabilistic planner for the combat power management problem. In Proc. of International Conference on Automated Planning and Scheduling (ICAPS). 12-19.
- [4] Geib, C. and R. Goldman (2003), Recognizing Plan/Goal Abandonment, in Proceedings of International Joint Conferences on Artificial Intelligence.
- [5] Geib, C., J. Maraist, and R. Goldman (2008), A New Probabilistic Plan Recognition Algorithm Based on String Rewriting, in Proceedings of the Int. Conference on Automated Planning and Scheduling.
- [6] Heinze, C., S. Goss, and A. Pearce (1999), Plan Recognition in Military Simulation: Incorporating Machine Learning with Intelligent Agents, in Proceedings of IJCAI-99 Workshop on Team Behaviour and Plan Recognition.
- [7] Irandoust, H., A. Benaskeur, K. Baker, and S. Banbury, *Naval Force-Level Tactical Command & Control: and Problem Characterization*, DRDC TR 2009-199, UNCLASSIFIED.
- [8] Irandoust, H., A. Benaskeur, F. Kabanza, P. Bellefeuille (2010) A Mixed-Initiative Advisory System for Threat Evaluation. Proceedings of the 15th International Command and Control Research and Technology Symposium, Santa Monica, USA, June 2010.
- [9] Johansson, F. and G. Falkman (2008), A Bayesian Network Approach to Threat Evaluation, in Proceedings of Int. Conference on Information Fusion.
- [10] Kopp, C. (2009) NCW101: An Introduction to Network Centric Warfare, 9780980550603 (pdf), AirPower Australia.
- [11] Liang, Y. (2007), An Approximate Reasoning Model for Situation and Threat Assessment, in Proceedings of the 4th Int. Conference on Fuzzy Systems and Knowledge Discovery.
- [12] Liebhaber, M. and B. Feher (2002), Air Threat Assessment: Research, Model, and Display Guildines, in Proceedings of the CCRTS, Naval Postgraduate School, Monterey, CA.
- [13] Mirmoeini, F. and V. Krishnamurthy (2005), Reconfigurable Bayesian Networks for Hierarchical Multi-Stage Situation Assessment in Battlespace, in Conference Record of the Thirty-Ninth Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA.
- [14] Noh, S. and P. Gmytrasiewicz (1998), Rational Communicative Behavior in Anti-Air Defense, in Proceedings of Int. Conference on Multi Agent Systems, Paris, France.
- [15] Okello, N. and G. Thoms (2003), Threat Assessment using Bayesian Networks, in Proceedings of International Conference on Information Fusion.
- [16] Paradis, S., A. Benaskeur, M. Oxenham, P. Cutler (2005), Threat Evaluation and Weapons Allocation in Network-Centric Warfare, Proceedings of Fusion 2005, Philadelphia, PA.
- [17] Roy, J. (2011) A View on Threat Analysis Concepts, Models and Estimation Techniques, DRDC Valcartier Technical Memorandum TM 2008-382.

- [18] Santos, E. and Q. Zhao (2006), Adversarial Models for Opponent Intent Inferencing, in Adversarial Reasoning: Computational Approaches to Reading the Opponents Mind, A. Kott and W. McEneaney, Eds., Boca Raton, Florida: Chapman & Hall, pp. 1-22.
- [19] Steinberg, A. (2005), An Approach to Threat Assessment, Proceedings of Fusion 2005, Philadelphia, PA.
- [20] Tamble, M. et al. (1995), Intelligent Agents for Interactive Simulation Environments, AI Magazine, vol. 16, no. 1, pp. 15-39.

Distributed Threat Evaluation in Naval Tactical Battle Management

Dr. H. Irandoust

Decision Support Systems for C2 Section
DRDC Valcartier



- Threat Evaluation in the context of Naval Tactical BM
- Collaborative Threat Evaluation
- Overview of the System
 - Automation
 - Testbed
 - Advisory Capability
- Coordination Modes
- Future Work

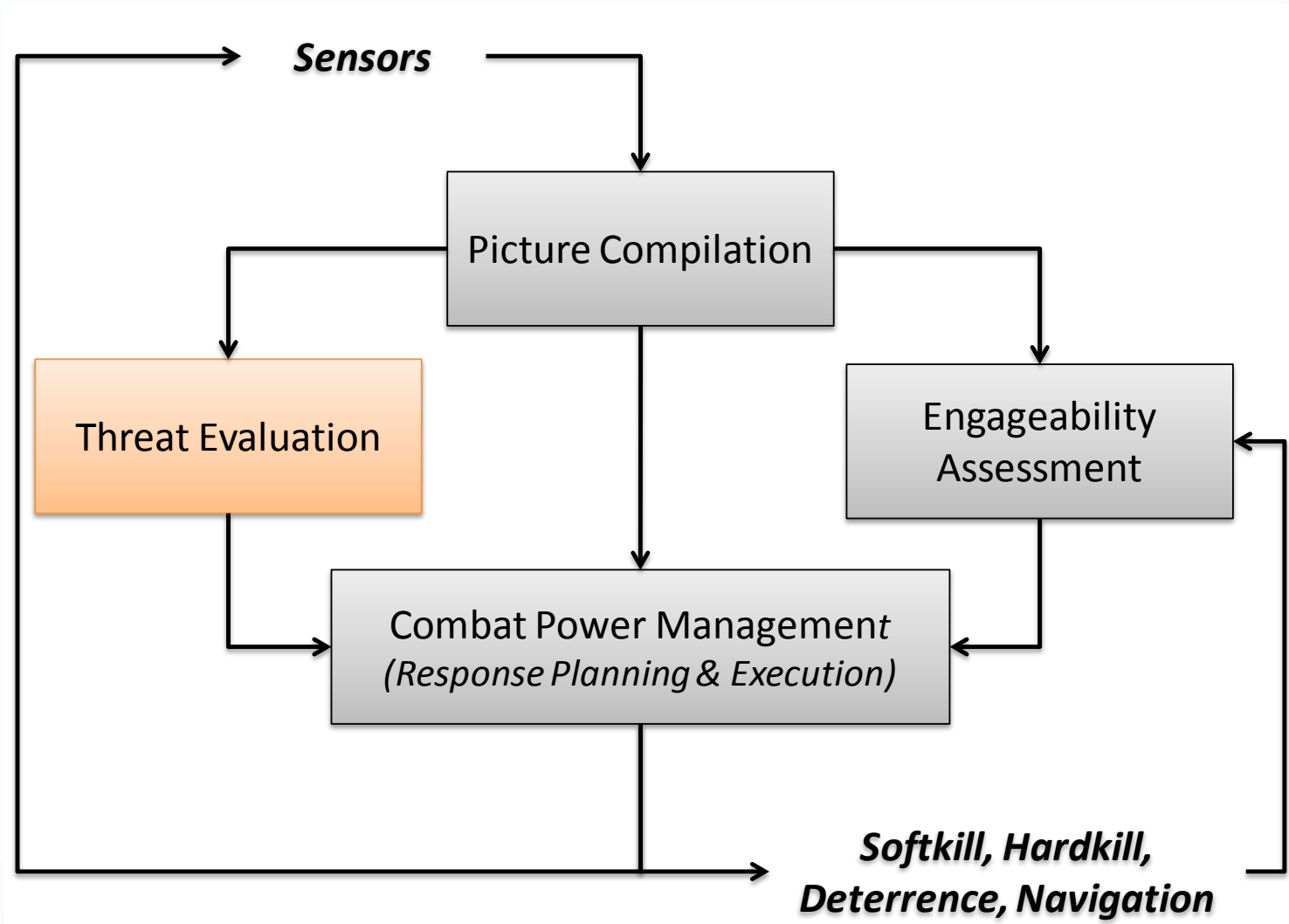
Context

- Wide range of sophisticated threats with different modes/guidance systems (cruise missiles, bombs, shoulder-launched rockets, etc.)
- Threats may originate from the sea, land or air, or a combination thereof

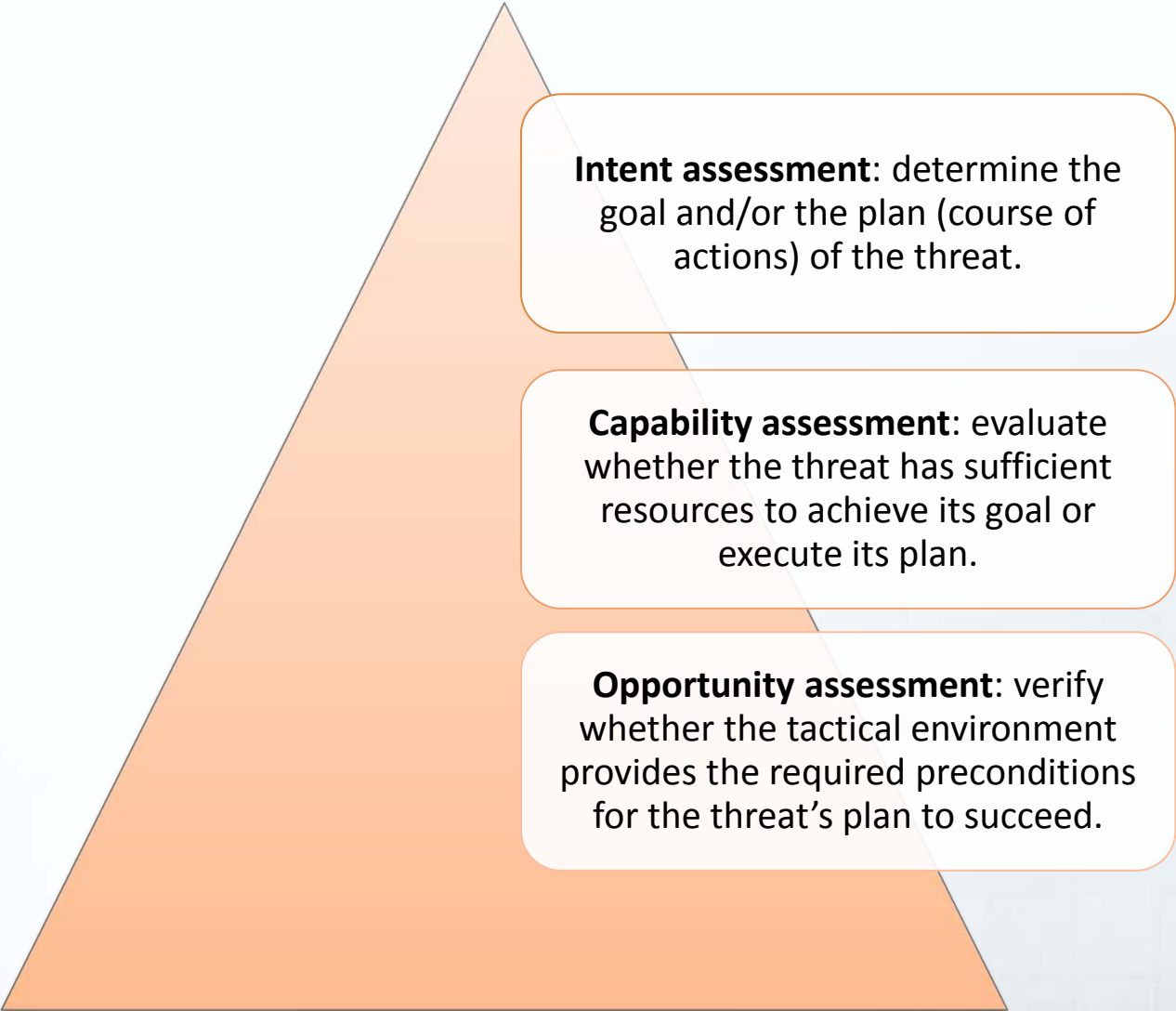


- Requirement to operate in littorals, jointly and in coalitions, has increased the complexity of operations and introduced additional challenges to the Navy

Threat Evaluation and C2 Functions



Threat Evaluation: Definition



Intent assessment: determine the goal and/or the plan (course of actions) of the threat.

Capability assessment: evaluate whether the threat has sufficient resources to achieve its goal or execute its plan.

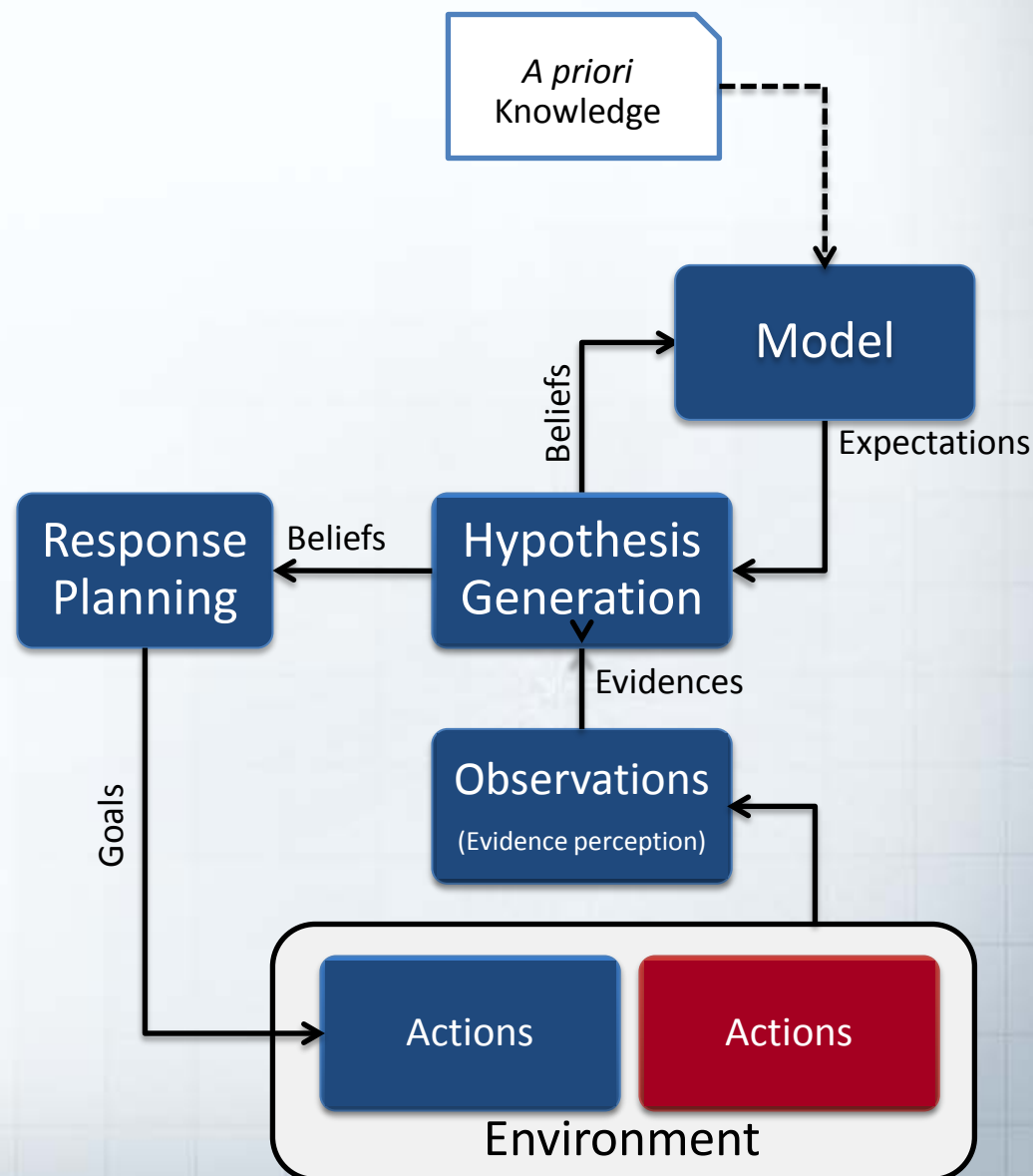
Opportunity assessment: verify whether the tactical environment provides the required preconditions for the threat's plan to succeed.

Output:

- Threat List
- Classification
- Ranking

Threat Evaluation Inference Model

- A priori knowledge (*e.g.*, intelligence, operational constraints and restraints, evaluation criteria, etc.)
- Dynamically acquired and inferred information (based on various indicators observed/obtained from various sources)



Threat Evaluation Challenges

Overload

Large amount of data

Time pressure

Information gathering & processing vs.
Decision/action

Situation Analysis

Uncertainty

- Imperfection of information sources
- Ambiguity in human behaviour

Dynamic environment

- Validity of information

Distributed TE: Advantages

- Information superiority (multiplying the information sources)
- Enhanced real-time response (deploying observers and processors close to the threat)
- Functional separation
- Robustness and resilience (tolerant to failure and bias of individual entities)



Distributed TE: Challenges

Overload

Data overload

Time pressure

Coordination overhead

Double-hatting

Situation Analysis

Red force

- Uncertainty
- Dynamic environment

Blue force

- Reference point different than own ship
- Awareness of other units' capabilities & limitations

Collaborative Decision Making

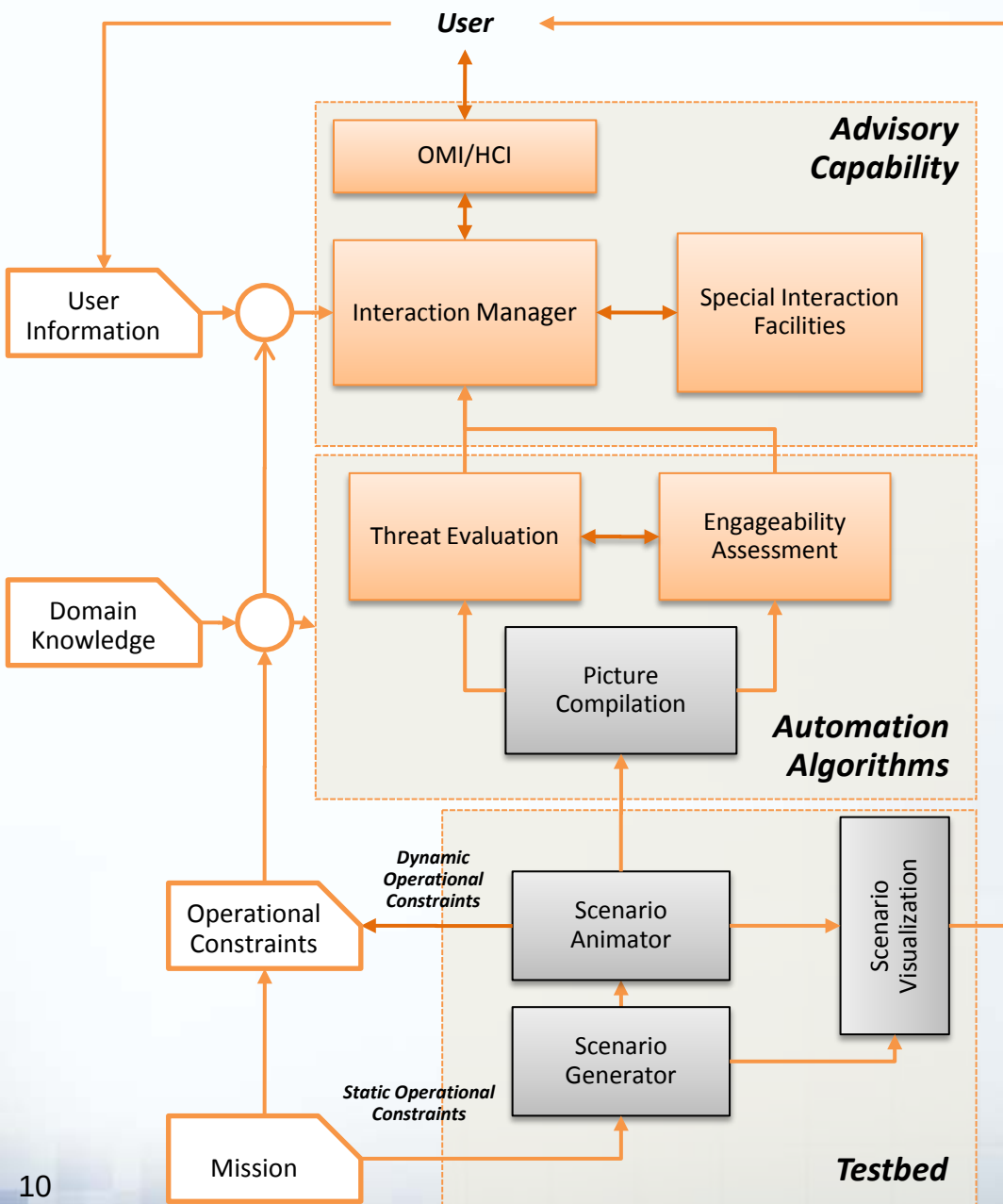
Information exchange, sensemaking

- Interoperability
- Connectivity - Security
- Remote communication
- Multiple (conflicting) decision nodes

Coordination

- Synchronization of activities
- Resource planning

FLEET Decision Support System



- **Testbed**

- Simulates the world

- **Automation Algorithms**

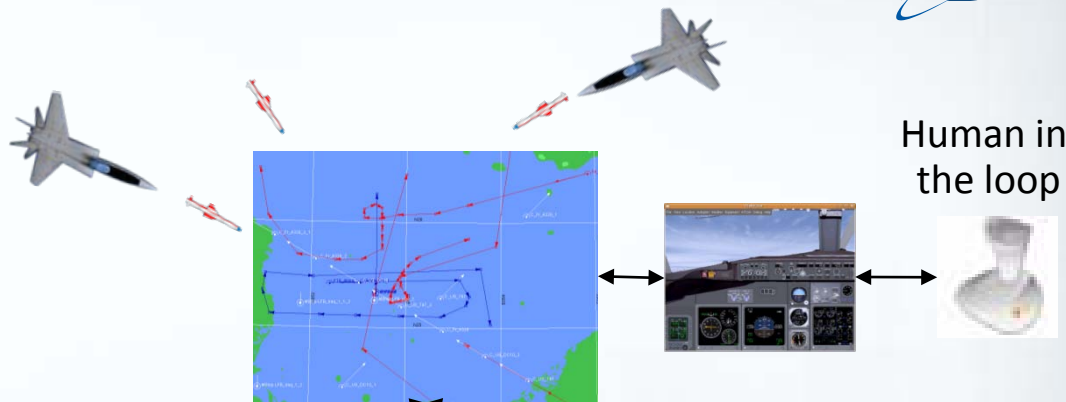
- Threat Evaluation
 - o Classifies threats (H, M, L)
 - o Ranks threats in each class
- Engageability Assessment
 - o Generates feasible actions

- **Advisory Capability**

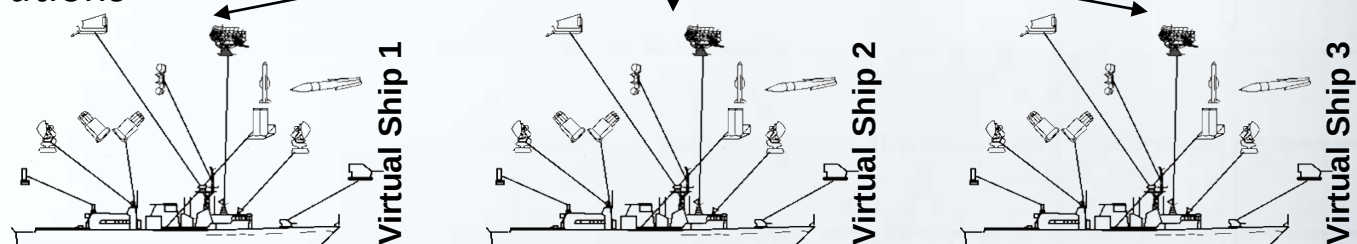
- Displays automation algorithms results
- Supports mixed-initiative interaction

FLEET Architecture

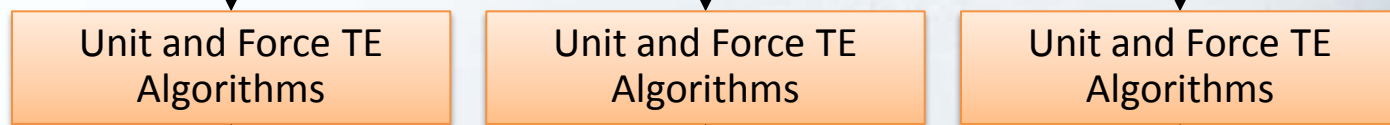
Layer 1: Scenario Generation and Control



Layer 2: Task Group Operations Modelling & Simulation



Layer 3: Automation and Coordination

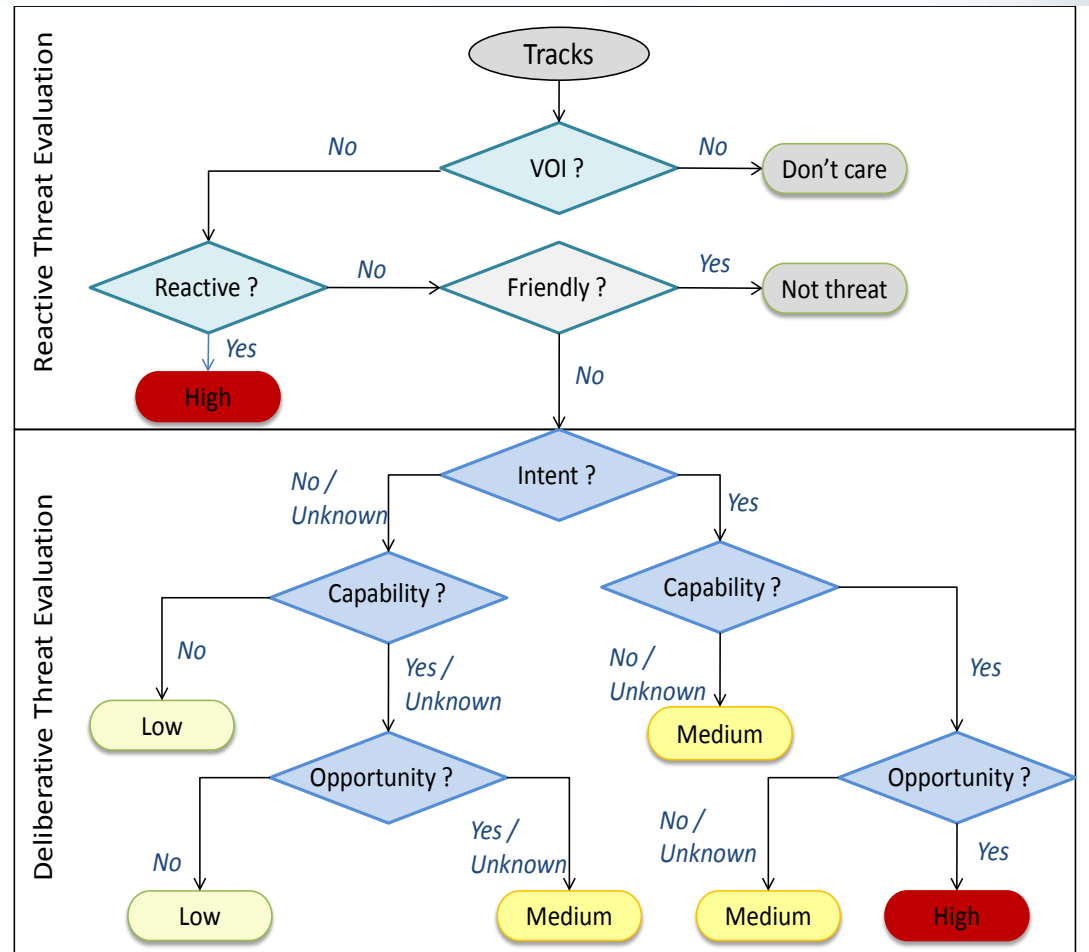


Layer 4: Decision Aids and Collaboration



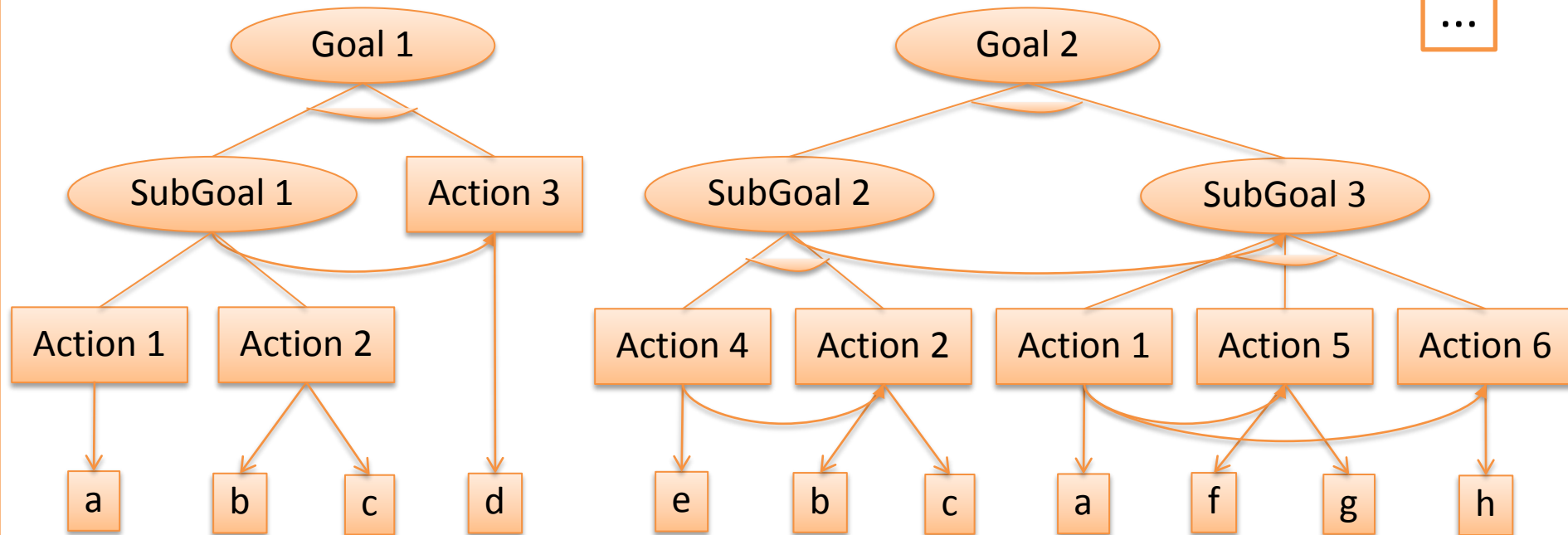
Automation: Rules

- Speed
- IFF
- Identity
- CPA
- Conformance to civilian airlines
- Manoeuvres
- Coordinated threats
- Deceptive behaviour



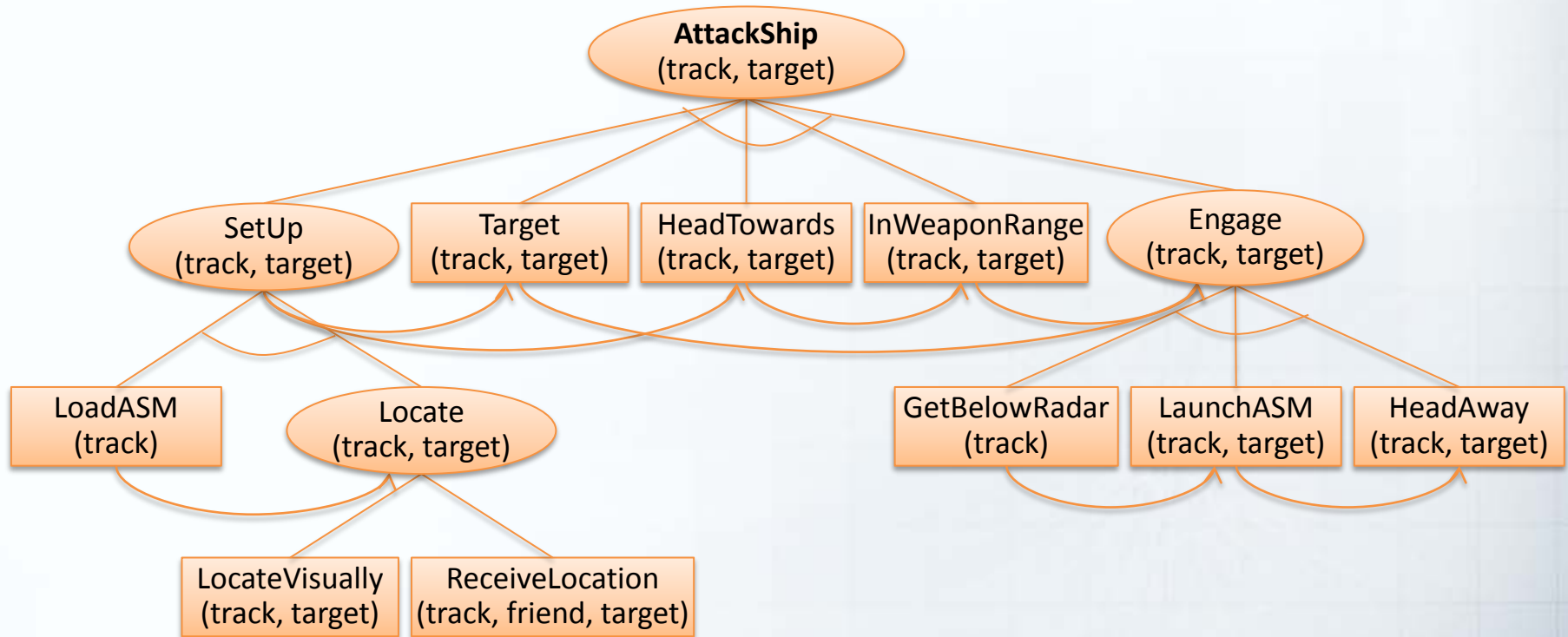
Automation: Plan Recognition

Plan Library

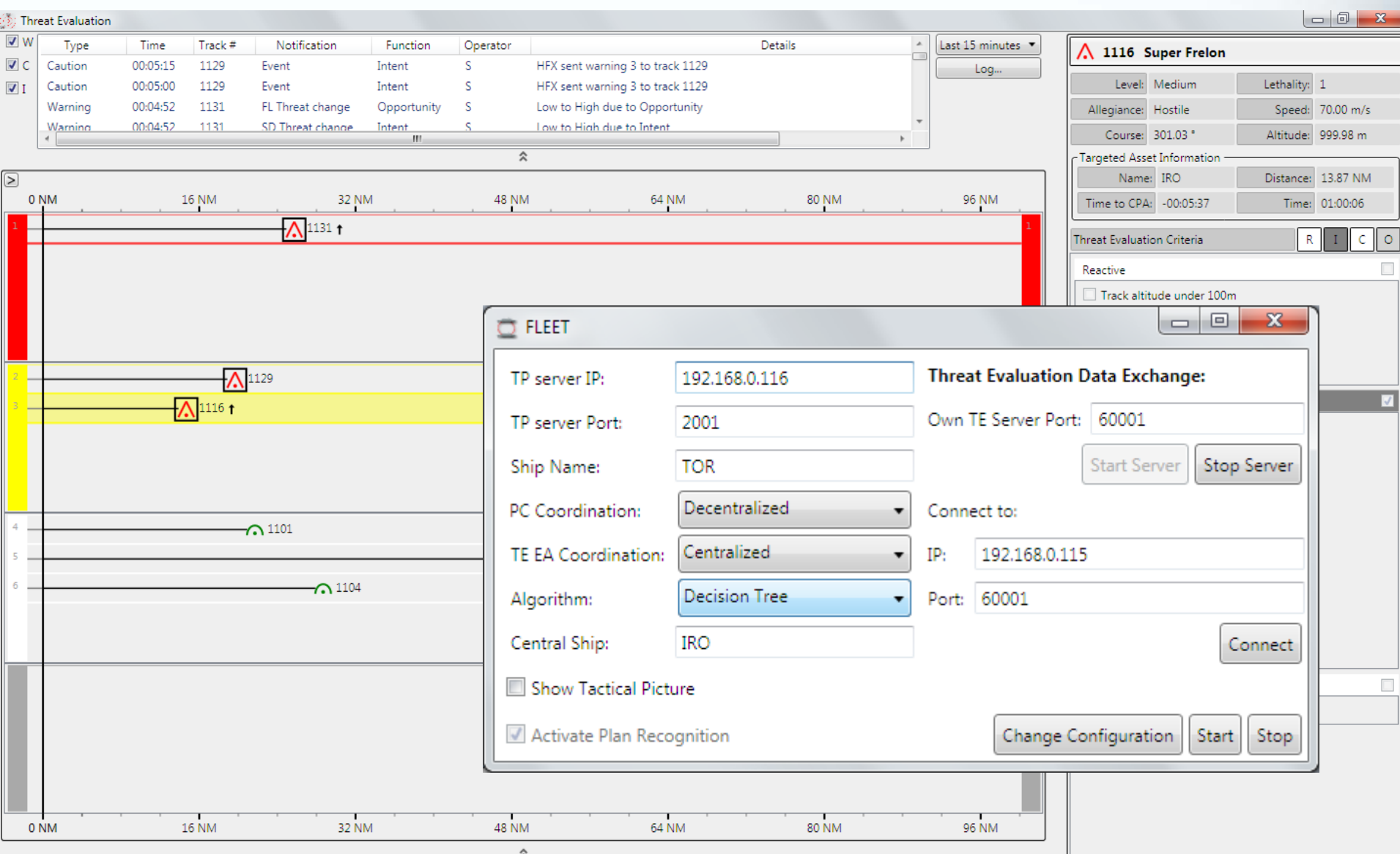


- a, b, c... are observations from which actions of the observed agent are inferred.
- A plan specification also includes (not shown in the figure):
 - Observation probabilities : $p(\text{observation} | \text{actions})$
 - Subgoal selection/decomposition probabilities
 - A priori goal selection probabilities.

Example of a Plan: Attacking an asset



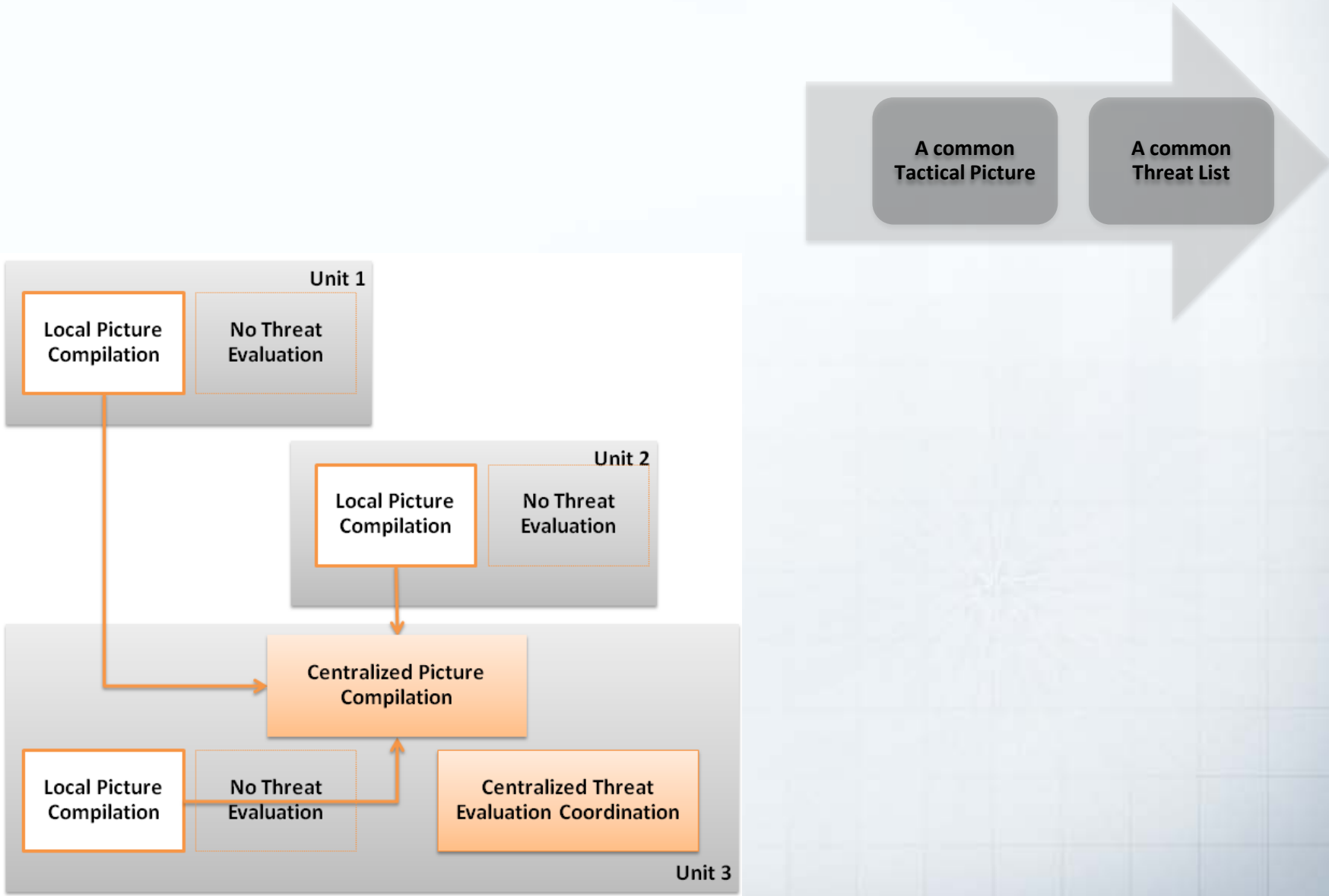
Advisory Capability



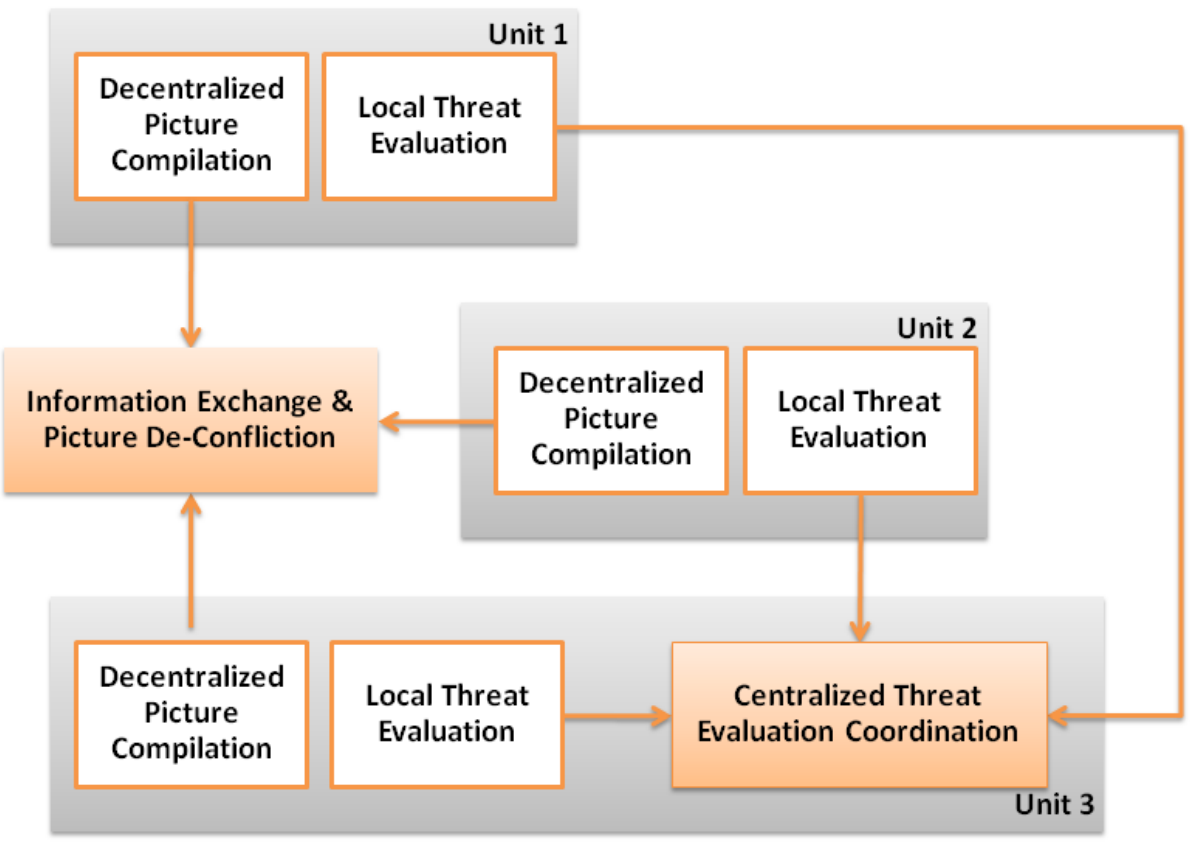
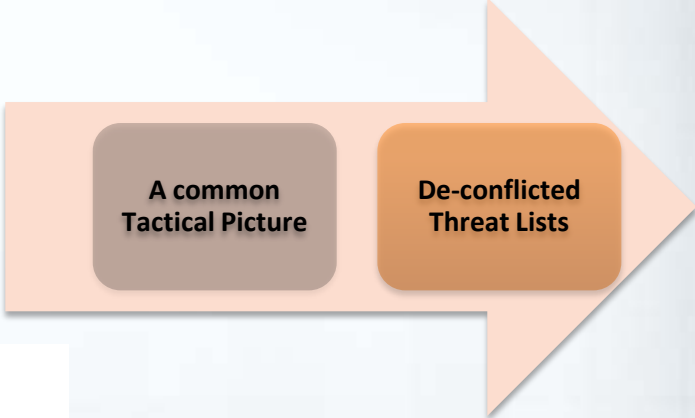
Coordination Modes

- Spectrum of coordination modes
- Can be performed along 2 axes: PC and TE
 - CC: Centralized PC / Centralized TE
 - DC: Decentralized PC / Centralized TE
 - DD: Decentralized PC / Decentralized TE
- Adapt to requirements (command structure) or evolving situation (degradation/loss of communication; changes to force composition)

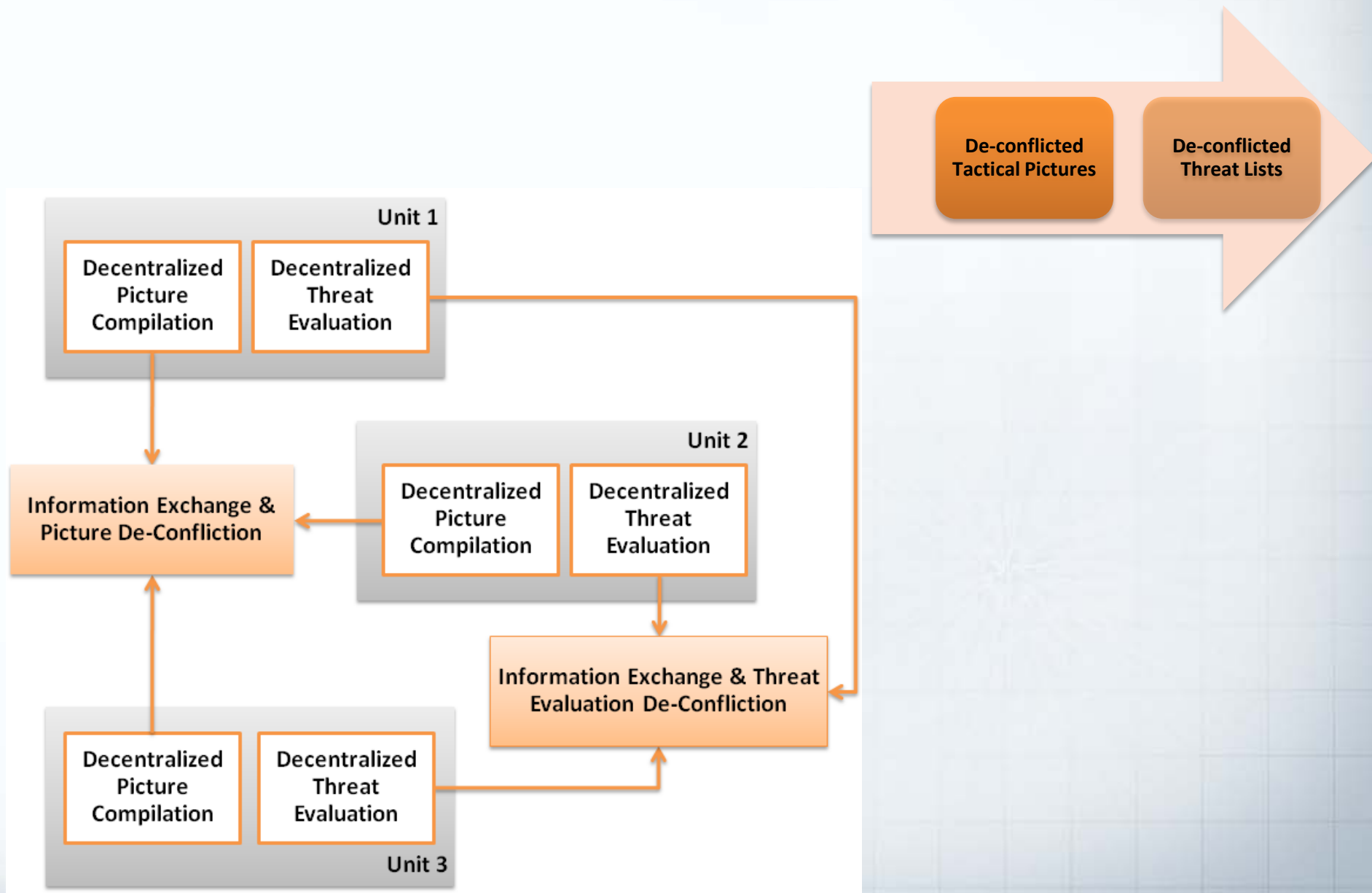
Coordination: Mode 1 (CC)



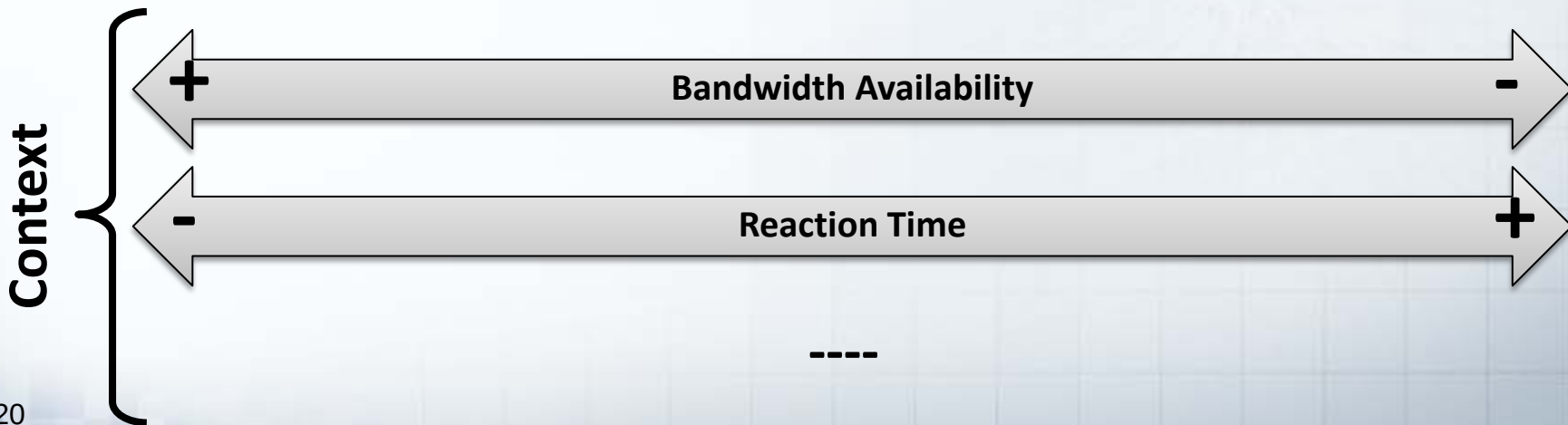
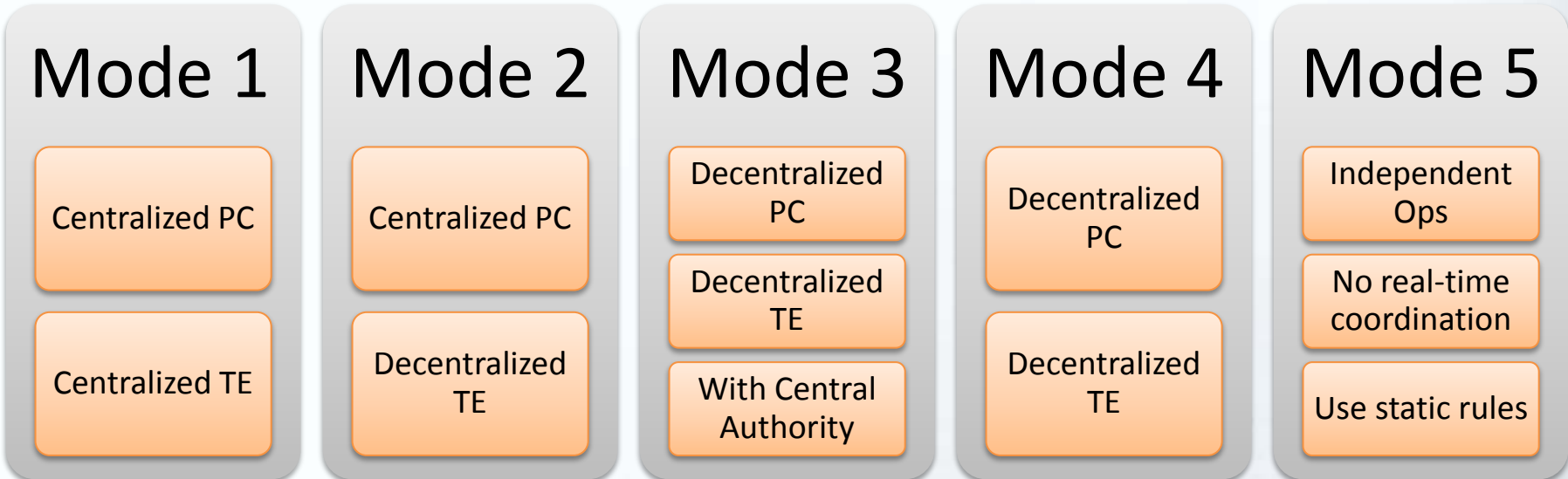
Coordination: Mode 2 (DC)



Coordination: Mode 3 (DD)



Adaptive/Robust Coordination Approach

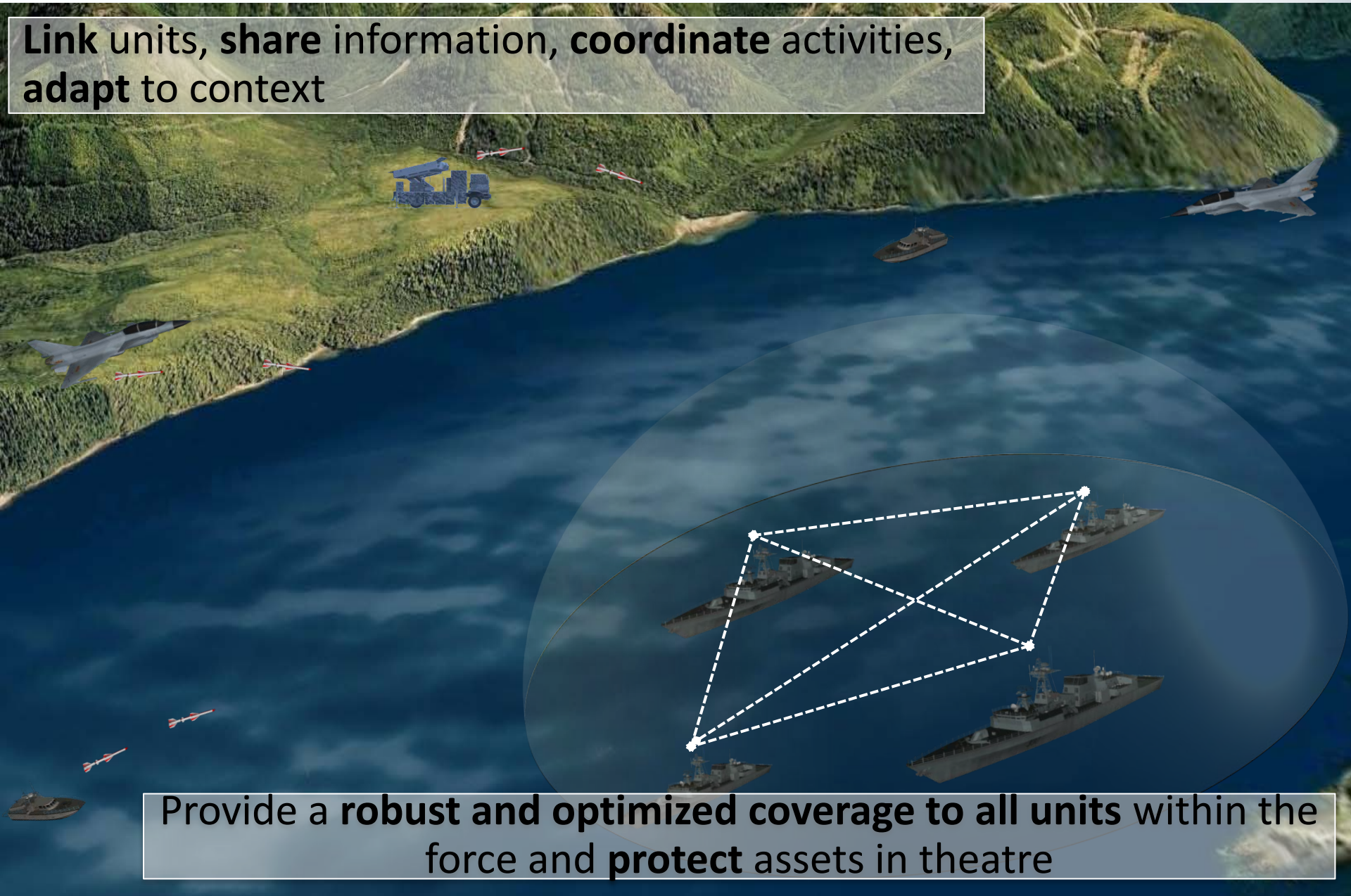


DEFENCE DÉFENSE



Future: Adaptive/Robust AAD Capability

Link units, share information, coordinate activities, adapt to context



Provide a **robust and optimized coverage** to all units within the force and **protect** assets in theatre

