Towards Characterizing Maritime Piracy Problem and Solution Spaces: Preliminary Results from Study Group Discussions

Éloi BOSSÉ[1], Elisa SHAHBAZIAN[2], Jesús García HERRERO[3], Galina ROGOVA[4] and Alan STEINBERG[5]

[1]Université Laval, Québec, QC, Canada
Director of NATO HSD.MD.ASI.984016
[2]President OODA Technologies Inc., Montréal, QC, Canada
[3]University Carlos III of Madrid, Madrid, Spain
[4]Encompass Consulting, NY, USA
[5]Georgia Tech Research Institute, VA, USA

Abstract. The main objective of the NATO HSD.MD.ASI.984016 on **Prediction and Recognition of Piracy Efforts Using Collaborative Human-Centric Information Systems** is to provide discussions on prediction, recognition and deterrence of maritime piracy through the use of collaborative human-centric information support systems. A group of more than 70 specialists and students gathered in Salamanca, Spain during the period of 19-30 September 2011 to examine maritime piracy problems and possible solutions. The ASI involved both technology and domain experts who exchanged their knowledge through lectures, plenary and brainstorming breakout study sessions in smaller interdisciplinary groups. They certainly improved their mutual awareness of the requirements, issues, policy as well as technology capable of helping to predict, recognize and deter maritime piracy. This paper presents the results of the discussions of the four interdisciplinary groups formed to study the various aspects of the maritime piracy problem.

Keywords. Maritime piracy, decision support, situation analysis, information fusion, cognitive engineering

Introduction

The members of the organizing committee previously organized a number ([1], [2], [6], [7], [8], [9]) of NATO Advanced Research Workshops (ARW) and Advanced Study Institutes (ASIs), symposia and Research Task Groups that discussed applications of decision support technologies to various security problems. A significant observation obtained during these meetings was that the domain experts (e.g., personnel from various organizations responsible for maritime security) have little understanding of the wide variety of technology solutions available, and how these solutions can enhance the performance of decision makers. Similarly, although technology experts have a general understanding of the various security system requirements, they do not have sufficient knowledge of antipiracy operations including constraints and a variety of factors (policy, geopolitical, legal, personnel, training, etc.) to overcome this problem. this ASI gathered both technology and domain experts to provide an opportunity for them to improve their mutual understanding of the specific requirements, issues, and policies of the antipiracy domain, as well as of technology capable to predict, recognize and deter maritime piracy. The ASI comprised lectures, plenary sessions and brainstorming study sessions in smaller interdisciplinary groups. We have been fortunate to have lecturers comprising many leading scientists and very knowledgeable maritime piracy domain experts. We also had students from various countries whose research topics were precisely maritime piracy. The results of the study group discussions presented here are preliminary, and focus mostly on identifying various aspects of concern for both the problem space and the solution space of maritime piracy. Finally, an ASI is not usually structured to have intensive or extensive working sessions to conduct in depth analysis of these aspects, but at least, by conducting these brainstorming sessions, this ASI was able to deliver a list of issues or topics on which future ARWs can be proposed.

1. Piracy Threat Management Framework

Before the study groups could start their assessments, a framework to help structure the analyses to be performed by the groups was developed in a plenary session. This framework leveraged the participants' background, as well as past publications, presentations and conclusions from previous NATO-funded meetings organized by the members of the organizing committee ([4], [5]) and other scientific events on crisis and emergency response, harbour protection and other defence and security problems.

A detailed analysis of these contributions is beyond the scope of this paper, but would certainly deserve to be considered in the context of maritime piracy. Note that all contributions including the companion contributions to past publications focus on a wide variety of information systems ranging from sensing, to making sense, to decision making that is behind the model of the piracy threat management framework

1.1. An analysis Framework

In a previous ASI entitled *Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management*, held in Albena, Bulgaria, 2005, a triadic model [3] was proposed to characterise interactions between the task, the technology and the people.

As illustrated in Figure 1, three elements compose the triad: the task, the technology and the human. In the command and control context, the OODA (Observe-Orient-Decide-Act) loop represents the task to be accomplished. Systems designers are introduced via the technology element.

Their main axis of interest is the link between the technology and the task. The general question related to this link is: "What systems must be designed to accomplish the task?" Systems designers are also considering the human. Their secondary axis of interest is thus the link between the technology and the human. The main question of this link is: "How to design the system so it is suitable for the human?" However, systems designers have also a hidden axis of interest, namely, the axis between the human and the task is usually not covered by their expertise. From the analyses of the axis, technological possibilities and limitations are identified. However, all environmental constraints may not be covered by the technological possibilities. These uncovered constraints, named thereafter deficiencies, are then addressed as statements of requirements to the human factor community.

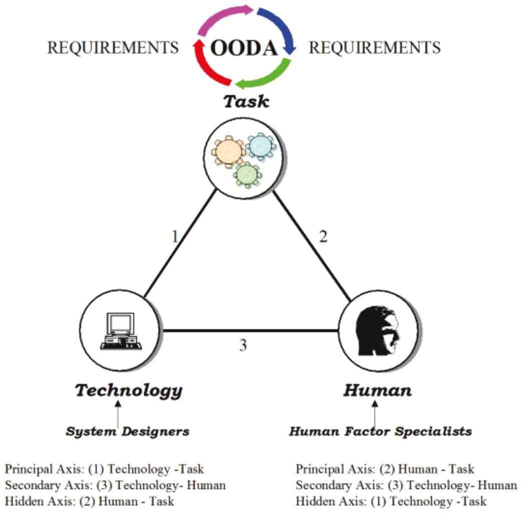

REQUIREMENTS
OODA
REQUIREMENTS
Task
1
2
3
Technology
Human
System Designers
Human Factor Specialists
Principal Axis: (1) Technology -Task
Secondary Axis: (3) Technology- Human
Hidden Axis: (2) Human - Task
Principal Axis: (2) Human - Task
Secondary Axis: (3) Technology- Human
Hidden Axis: (1) Technology -Task

Figure 1. Task/Human/Technology Triad Model

These requirements lead to better training programs, the reorganisation of work and the roles for leadership, team communication, etc. This very high level framework has been used to structure our discussions on maritime piracy.

1.2. Understanding Complex Situations

The prediction and recognition of piracy enterprises, hereafter referred to as "Piracy Threat Management," is an extremely complex problem, spanning many operational phases and involving many participating organizations. The analysis of the decision support requirements for such a large and complex application is envisaged to have many dimensions. It was agreed to structure the analysis framework into five dimensions, corresponding to the five operational phases of a piracy situation evolution shown in **Figure 2**.

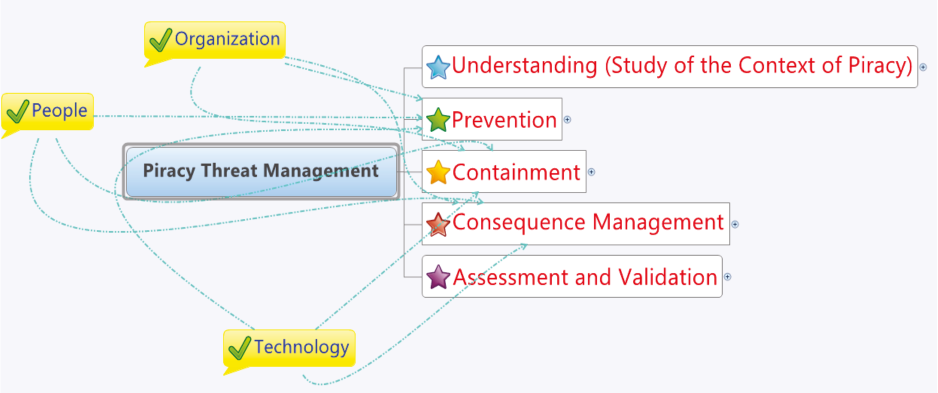


Figure 2. Five (5) dimensions of the analysis framework

For each Piracy Threat Management dimension, analysis topics (activities, factors, relationships, dependencies, technologies, organizations, issues, etc.) were identified and detailed in some cases into more than one level. The resulting "trees" of mapping the Piracy Threat Management dimensions into analysis topics have been included in Annex A of this paper, hereafter referred to as the Management Framework. It is clear that the presented framework does not cover the complete problem space and subsequent analyses are required. Subsequent analyses need to examine the currently identified topics as well as identify other analysis topics to mature and complete the framework. However considering the scope of the ASI, the strategy for the problem of Piracy Threat Management has been structured into an initial set of numerous smaller topics which can be easier to analyse.

2. Study Sessions Analyses

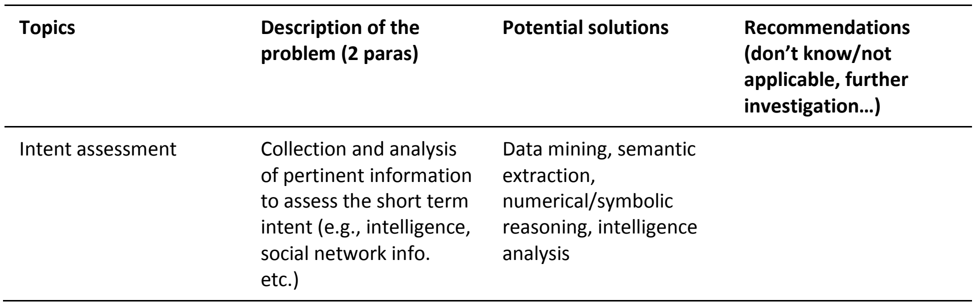
The study teams used the Management Framework as a starting point for their discussions aimed at identifying technologies which could enable enhanced decision making for the overall piracy threat management. Different topics of each dimension of the analysis framework were examined to establish the degree to which they could help in the decision making process, or identify important factors to also be taken into account. However, fully recognizing that within the scope of the ASI it is not feasible to cover a significant part of the problem space, the team leaders were given freedom to select a subset of the topics (accordingly to the experience and expertise of the group members) as well as the methodology for their analysis. While two teams followed the sequential path of taking the analysis topics one at a time and discussing technological solutions, two others chose alternate paths. One of these two teams concentrated on classifying topics by the type of solution that will make the biggest impact on the performance of decision makers, and grouping them into families: operational, political, legal or technological. The second of these two teams looked at the overall problem of prediction and recognition of piracy attacks by decomposing the process of prediction and recognition of attacks (the mission) into a set of technical issues (i.e., needed capabilities that technology might help provide) and analysing the technological solutions.

Considering the time available for the study sessions, the main output represented preliminary methodologies for each of the paths taken by the teams.

A short description of these methodologies is presented below.

2.1. The Methodology of "Sequential Path"

Figure 3 illustrates the analysis methodology proposed at the plenary session. As an example, it shows how the topic "intent assessment," within block "Containment," could be examined.



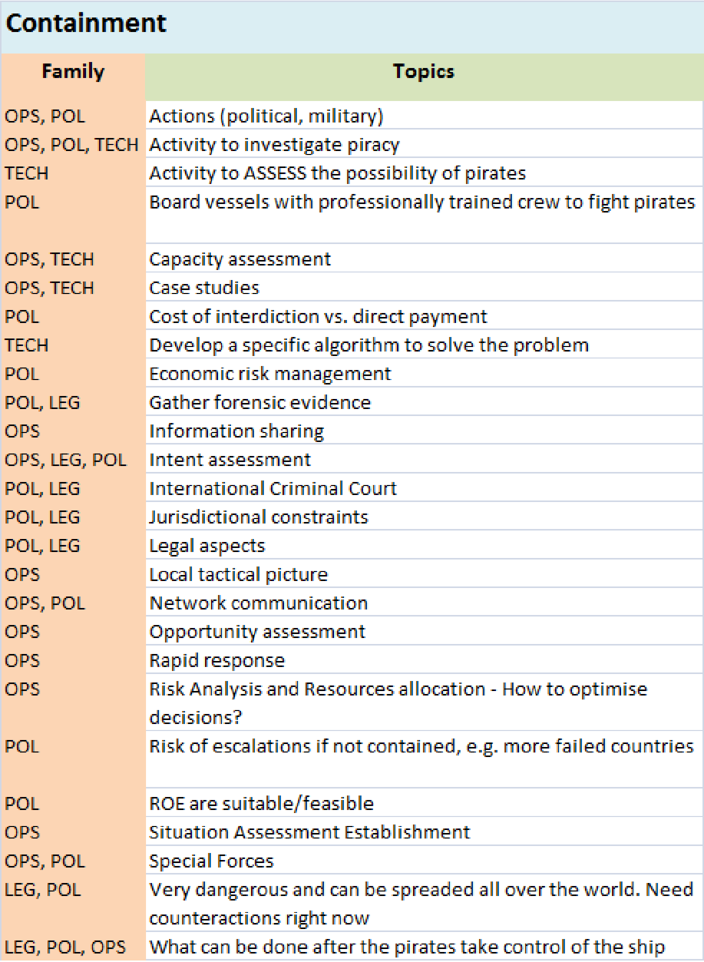
Topics	Description of the problem (2 paras)	Potential solutions	Recommendations (don't know/not applicable, further investigation…)
Intent assessment	Collection and analysis of pertinent information to assess the short term intent (e.g., intelligence, social network info. etc.)	Data mining, semantic extraction, numerical/symbolic reasoning, intelligence analysis	

Figure 3. Sequential path methodology for topic analysis (example)

2.2. The Topic Classification Methodology

As mentioned above, one of the study teams decided to first classify the analysis topics by what type of change or solution would make the biggest impact in enhancing performance, grouping them into families: operational, political, legal or technological. **Figure 4** presents an initial classification into families of the topics of the "Containment" dimension (the shorter of the dimensions).

The members of this study group observed that the technological solutions would be very much dependent on the specific political, operational and legal context of how all participating countries and jurisdictions addressed piracy situations. Only a small number of topics have been classified in the TECH family; however it is apparent that in fact there will be very few topics for which no technological solutions will be required. Specifically, the experts in this study groups debated whether all topics in the OPS family should be also in the TECH family, as operations will require technology enabled decision support, while specific technological solutions will be operations and doctrine dependent.



Containment	
Family	**Topics**
OPS, POL	Actions (political, military)
OPS, POL, TECH	Activity to investigate piracy
TECH	Activity to ASSESS the possibility of pirates
POL	Board vessels with professionally trained crew to fight pirates
OPS, TECH	Capacity assessment
OPS, TECH	Case studies
POL	Cost of interdiction vs. direct payment
TECH	Develop a specific algorithm to solve the problem
POL	Economic risk management
POL, LEG	Gather forensic evidence
OPS	Information sharing
OPS, LEG, POL	Intent assessment
POL, LEG	International Criminal Court
POL, LEG	Jurisdictional constraints
POL, LEG	Legal aspects
OPS	Local tactical picture
OPS, POL	Network communication
OPS	Opportunity assessment
OPS	Rapid response
OPS	Risk Analysis and Resources allocation - How to optimise decisions?
POL	Risk of escalations if not contained, e.g. more failed countries
POL	ROE are suitable/feasible
OPS	Situation Assessment Establishment
OPS, POL	Special Forces
LEG, POL	Very dangerous and can be spreaded all over the world. Need counteractions right now
LEG, POL, OPS	What can be done after the pirates take control of the ship

Figure 4. Classification of topics

The abbreviations in the family names are: OPS – operational; POL – political; LEG – legal; and TECH – technological.

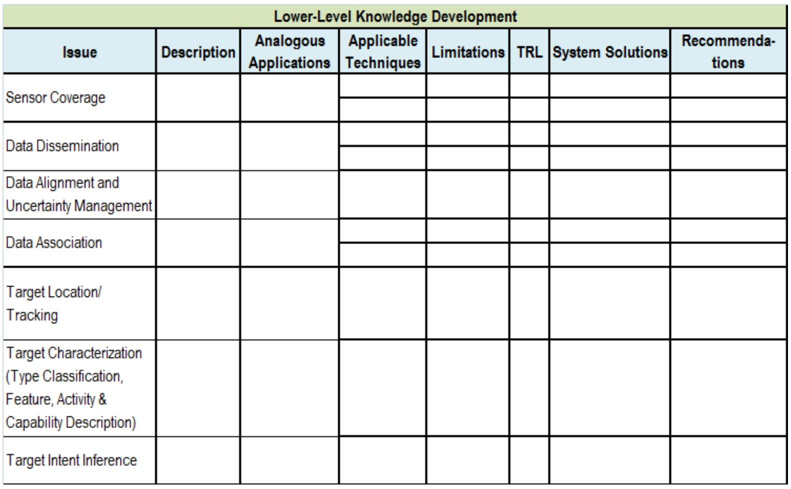
2.3. The Technology Centred Methodology

The approach adopted by this study group was to:

- Decompose the process of predicting and characterizing piracy attacks (the mission) into a set of technical issues (i.e., needed capabilities which technology might help provide).
- For each such issue, list potential technical solutions in terms of their maturity and potential effectiveness in resolving the issue.

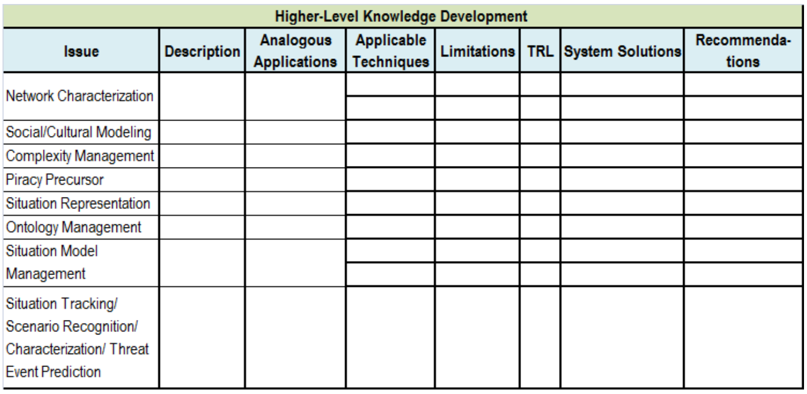
Figure 5-7 present the decompositions, while preliminary findings performed by this study team are included in Annex B. While for Figures 5 and 6 potential technical

solutions for some identified technical issues have been developed and included in the annex, the issues for Figure 7 are still awaiting possible technical solutions.



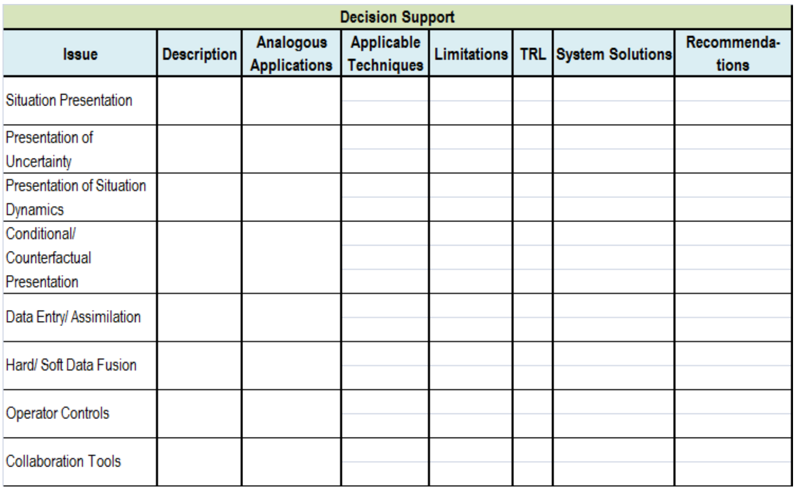
Lower-Level Knowledge Development							
Issue	Description	Analogous Applications	Applicable Techniques	Limitations	TRL	System Solutions	Recommenda-tions
Sensor Coverage							
Data Dissemination							
Data Alignment and Uncertainty Management							
Data Association							
Target Location/ Tracking							
Target Characterization (Type Classification, Feature, Activity & Capability Description)							
Target Intent Inference							

Figure 5. Lower-level knowledge development



Higher-Level Knowledge Development							
Issue	Description	Analogous Applications	Applicable Techniques	Limitations	TRL	System Solutions	Recommenda-tions
Network Characterization							
Social/Cultural Modeling							
Complexity Management							
Piracy Precursor							
Situation Representation							
Ontology Management							
Situation Model Management							
Situation Tracking/ Scenario Recognition/ Characterization/ Threat Event Prediction							

Figure 6. Higher-level knowledge development

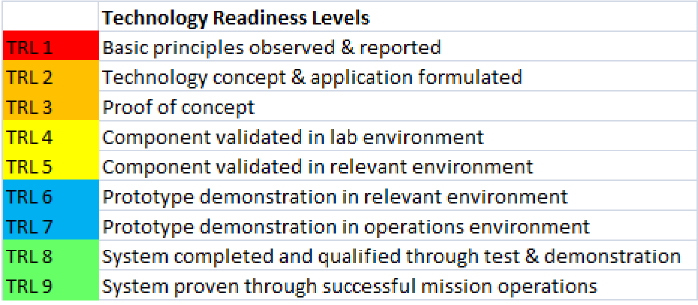


Decision Support							
Issue	Description	Analogous Applications	Applicable Techniques	Limitations	TRL	System Solutions	Recommenda-tions
Situation Presentation							
Presentation of Uncertainty							
Presentation of Situation Dynamics							
Conditional/ Counterfactual Presentation							
Data Entry/ Assimilation							
Hard/ Soft Data Fusion							
Operator Controls							
Collaboration Tools							

Figure 7. Decision Support

Definitions and Metrics in these tables are defined as follows:

- Mission Capability: The ability to predict and recognize piracy efforts sufficiently to support effective responses: Prevention, Containment, and Consequence Management.
- Issues: A problem relevant to achieving the mission capability.
- Analogous Applications: Other mission capabilities that involve related technical issues.
- Applicable Techniques: Technologies or designs that might be used to solve the given issue.
- Limitations: Technical, operational or other factors that limit the capability of the given technique to provide a complete solution to the given problem.
- Maturity: The technology readiness level (TRL) of the given technique (presented in Figure 8).
- System Solutions: Candidate approaches to addressing given issues.
- Recommendations: Suggested actions for NATO or NATO members to solve the given issues.



	Technology Readiness Levels
TRL 1	Basic principles observed & reported
TRL 2	Technology concept & application formulated
TRL 3	Proof of concept
TRL 4	Component validated in lab environment
TRL 5	Component validated in relevant environment
TRL 6	Prototype demonstration in relevant environment
TRL 7	Prototype demonstration in operations environment
TRL 8	System completed and qualified through test & demonstration
TRL 9	System proven through successful mission operations

Figure 8. Technology readiness levels

Again, there was not sufficient time to complete the tables analysing the technologies further. Additional discussion on this approach would be beneficial.

3. Conclusion

This paper presents a high-level discussion on the potential support of collaborative information support systems to improve the ability to predict and prevent the occurrence of piracy incidents or rapidly recognize its nature and extent for effective collective response. The problem of maritime piracy is quite complex, and substantial research efforts are required to effectively design or adapt information systems to support the three actions of the *Partnership and Action Plan* presented in the introduction.

References

[1] É. Bossé, Chair of *NATO RTO-IST-086, C3I for Crisis, Emergency and Consequence Management*, NATO symposium, Bucharest, Romania, 11-12 May 2009. NATO report RTO-MP-IST-086, May 2009.

[2] É. Bossé, Ed., *Modelling of organisations and decision architectures*, Final report of RTO/IST-019/TG006, Dec. 2004, 249 pages.

[3] É. Bossé, S. Paradis, R. Breton, Decision Support in Command and Control: A Balanced Human-Technological Perspective, in *Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management*, 16-27 May 2005, 205-222.

[4] É. Bossé, J. Roy and S. Wark*, Concepts, Models, and Tools for Information Fusion,* Artech House, Norwood, 2007, 352 pages.

[5] A. Guitouni, A Time Sensitive Decision Support System for Crisis and Emergency Management, *NATO RTO-IST-086, C3I for Crisis, Emergency and Consequence Management,* paper 13, Bucharest, Romania, 11-12 May 2009.

[6] E. Lefebvre, Ed., *Advances and Challenges in Multisensor Data and Information Processing*, NATO Sciences Series, IOS Press, The Netherlands, 2007.

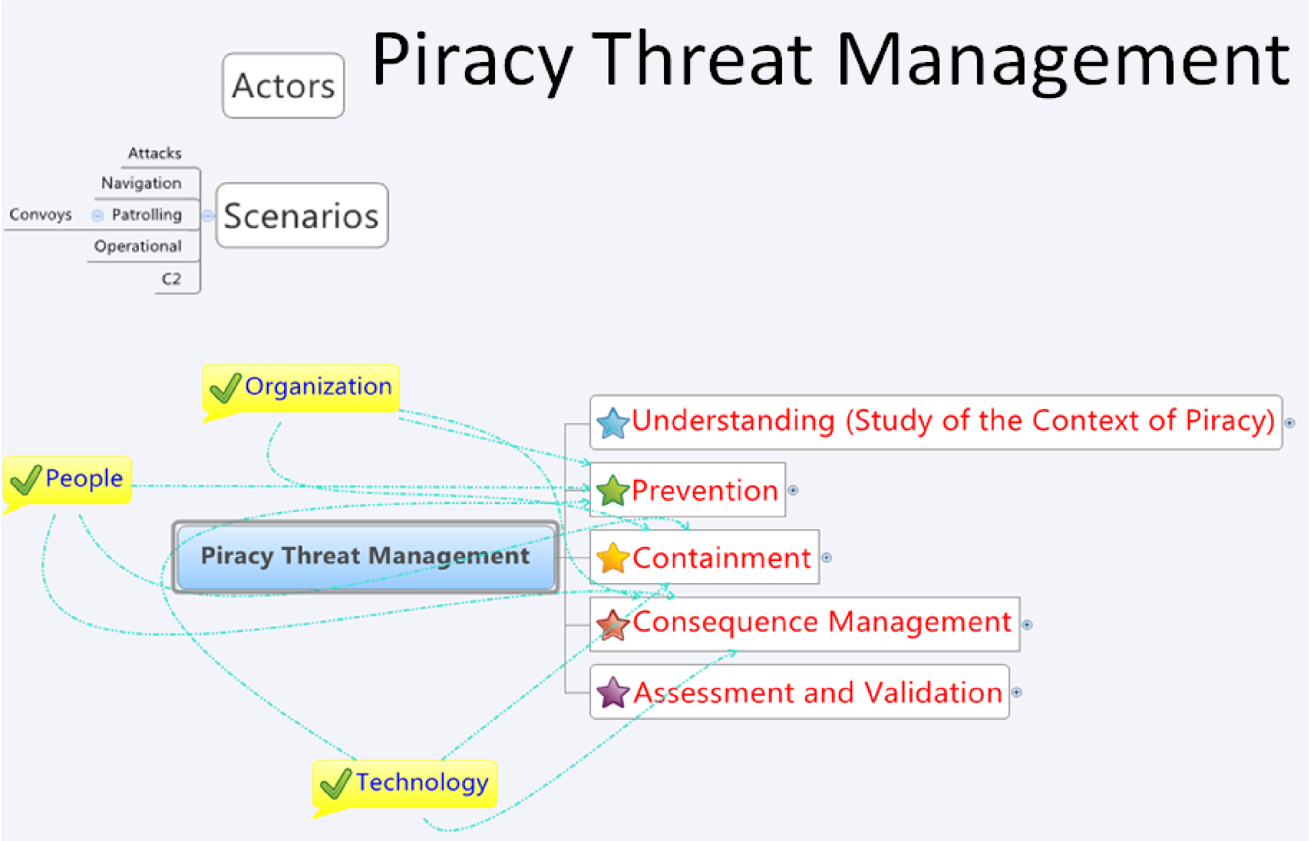
[7] E. Shahbazian, G. Rogova, Eds., *Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security,* NATO Sciences for Peace and Security Series D: Information and Communication Security-Vol 28, IOS Press, ISSN 1874-6268, The Netherlands, 2010.

[8] E. Shahbazian, G. Rogova, M.J. de Weert, Eds., *Harbour Protection Through Data Fusion Technologies,* NATO Sciences Series, Springer, The Netherlands, 2009.

[9] E. Shahbazian, G. Rogova, P. Valin, Eds.*, Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management,* NATO Sciences Series, IOS Press, The Netherlands, 2005.

Annex A

Piracy Threat Management Framework



Piracy Threat Management

Actors

Scenarios

Attacks

Navigation

Patrolling

Convoys

Operational

C2

Piracy Threat Management

Understanding (Study of the Context of Piracy)

Prevention

Containment

Consequence Management

Assessment and Validation

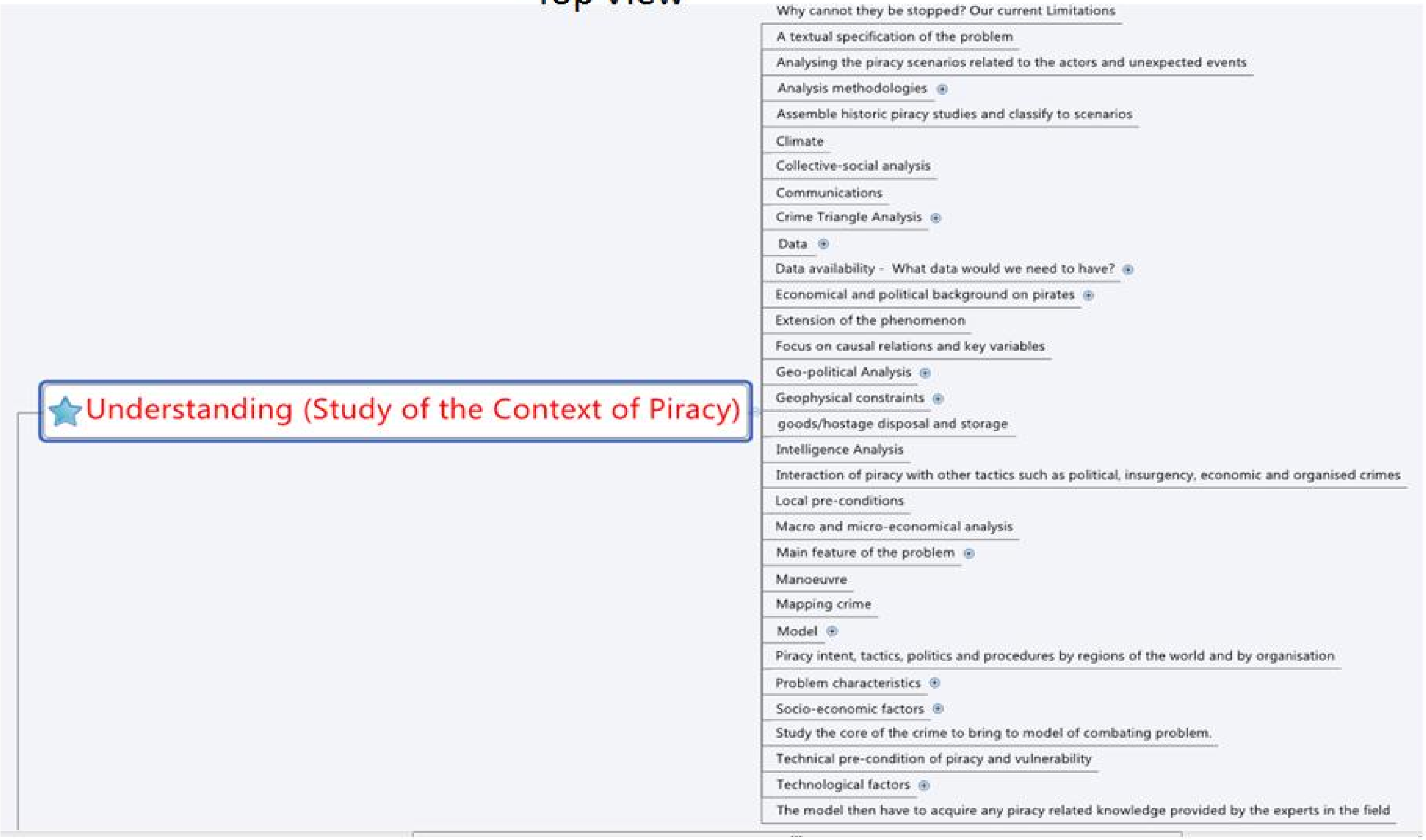
Organization

People

Technology

Understanding

Top View

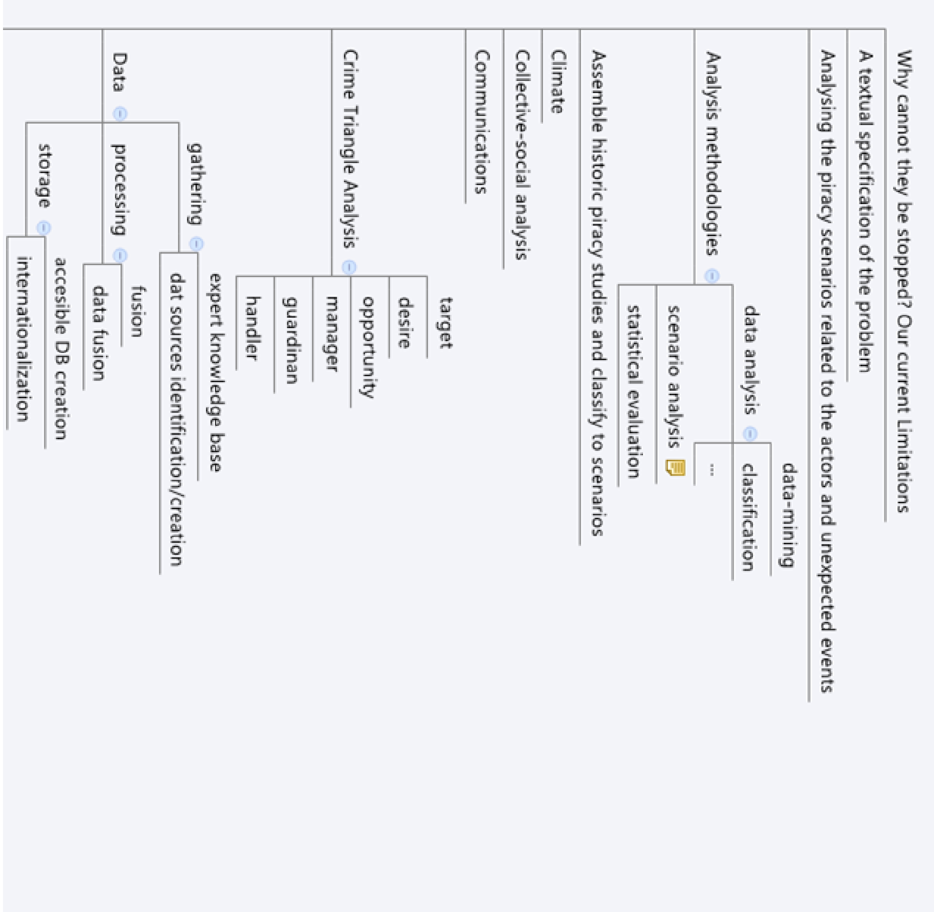


Understanding (Study of the Context of Piracy)

- Why cannot they be stopped? Our current Limitations
- A textual specification of the problem
- Analysing the piracy scenarios related to the actors and unexpected events
- Analysis methodologies ⊕
- Assemble historic piracy studies and classify to scenarios
- Climate
- Collective-social analysis
- Communications
- Crime Triangle Analysis ⊕
- Data ⊕
- Data availability - What data would we need to have? ⊕
- Economical and political background on pirates ⊕
- Extension of the phenomenon
- Focus on causal relations and key variables
- Geo-political Analysis ⊕
- Geophysical constraints ⊕
- goods/hostage disposal and storage
- Intelligence Analysis
- Interaction of piracy with other tactics such as political, insurgency, economic and organised crimes
- Local pre-conditions
- Macro and micro-economical analysis
- Main feature of the problem ⊕
- Manoeuvre
- Mapping crime
- Model ⊕
- Piracy intent, tactics, politics and procedures by regions of the world and by organisation
- Problem characteristics ⊕
- Socio-economic factors ⊕
- Study the core of the crime to bring to model of combating problem.
- Technical pre-condition of piracy and vulnerability
- Technological factors ⊕
- The model then have to acquire any piracy related knowledge provided by the experts in the field

Understanding

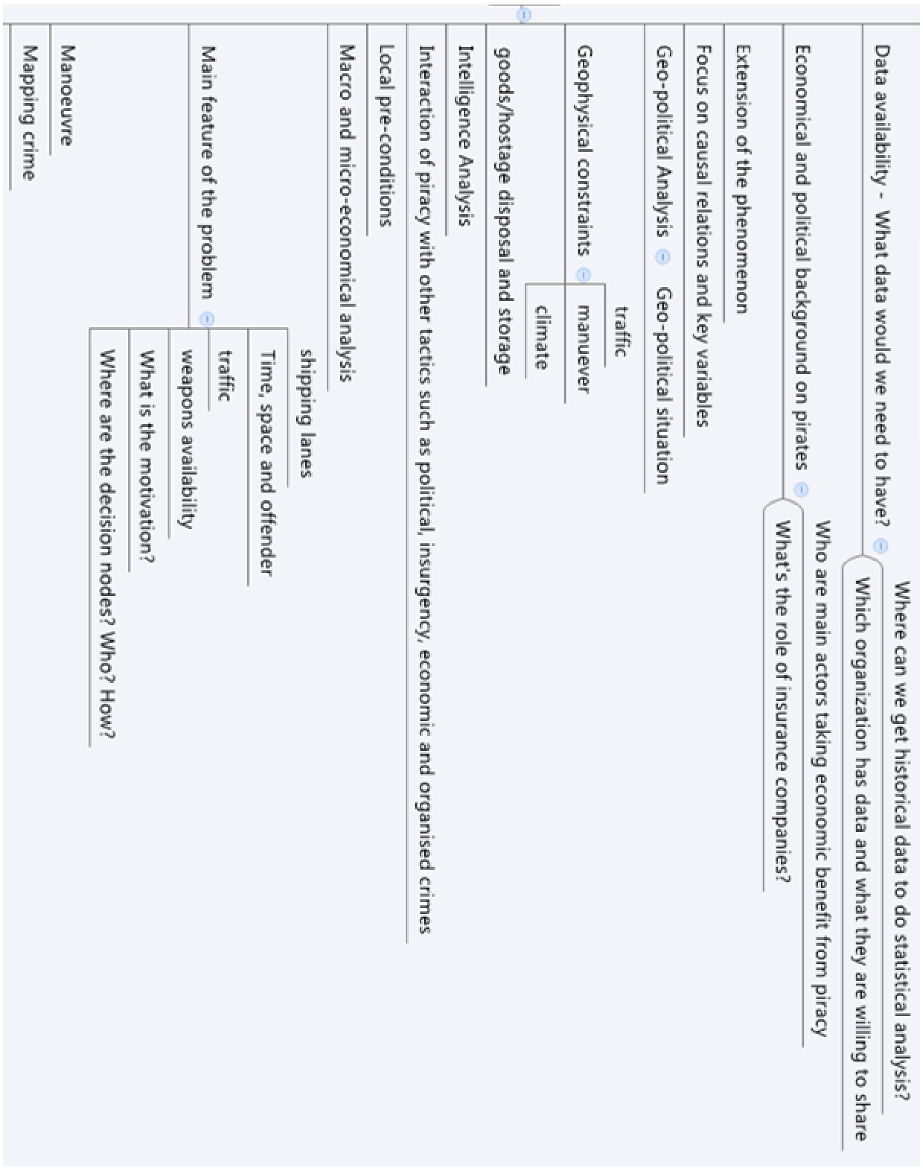
Detail_P1



- Why cannot they be stopped? Our current Limitations
- A textual specification of the problem
- Analysing the piracy scenarios related to the actors and unexpected events
- Analysis methodologies
  - data analysis
    - data-mining
    - classification
  - scenario analysis
    - ...
  - statistical evaluation
- Assemble historic piracy studies and classify to scenarios
- Climate
- Collective-social analysis
- Communications
- Crime Triangle Analysis
  - target
  - desire
  - opportunity
  - manager
  - guardinan
  - handler
- Data
  - gathering
    - expert knowledge base
    - dat sources identification/creation
  - processing
    - fusion
    - data fusion
  - storage
    - accesible DB creation
    - internationalization

Understanding

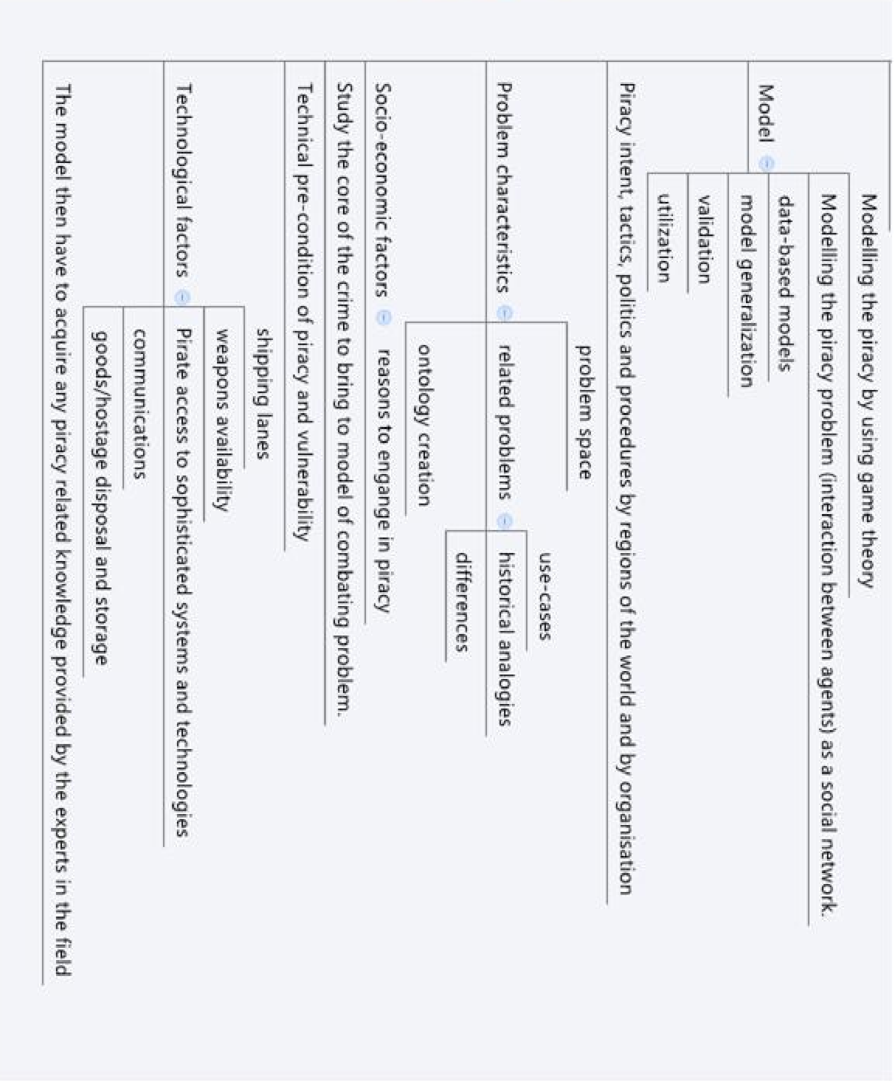
Detail_P2



- Data availability - What data would we need to have?
  - Where can we get historical data to do statistical analysis?
  - Which organization has data and what they are willing to share
- Economical and political background on pirates
  - Who are main actors taking economic benefit from piracy
  - What's the role of insurance companies?
- Extension of the phenomenon
- Focus on causal relations and key variables
- Geo-political Analysis
  - Geo-political situation
- Geophysical constraints
  - traffic
  - manuever
  - climate
- goods/hostage disposal and storage
- Intelligence Analysis
- Interaction of piracy with other tactics such as political, insurgency, economic and organised crimes
- Local pre-conditions
- Macro and micro-economical analysis
- Main feature of the problem
  - shipping lanes
  - Time, space and offender
  - traffic
  - weapons availability
  - What is the motivation?
  - Where are the decision nodes? Who? How?
- Manoeuvre
- Mapping crime

Understanding

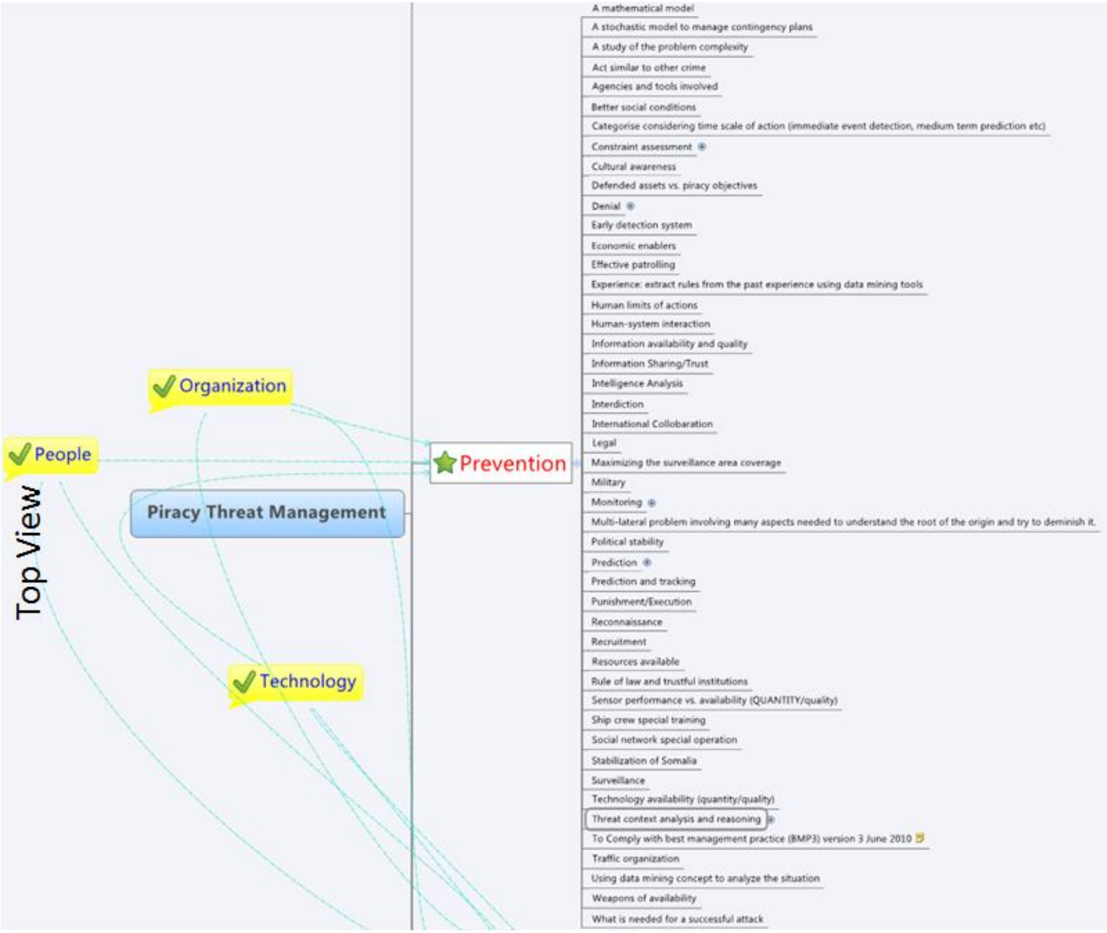
Detail_P3



- Model
  - Modelling the piracy by using game theory
  - Modelling the piracy problem (interaction between agents) as a social network.
  - data-based models
  - model generalization
  - validation
  - utilization
- Piracy intent, tactics, politics and procedures by regions of the world and by organisation
- Problem characteristics
  - problem space
  - related problems
    - use-cases
    - historical analogies
    - differences
  - ontology creation
- Socio-economic factors
  - reasons to engange in piracy
- Study the core of the crime to bring to model of combating problem.
- Technical pre-condition of piracy and vulnerability
- Technological factors
  - shipping lanes
  - weapons availability
  - Pirate access to sophisticated systems and technologies
  - communications
  - goods/hostage disposal and storage
- The model then have to acquire any piracy related knowledge provided by the experts in the field

Prevention

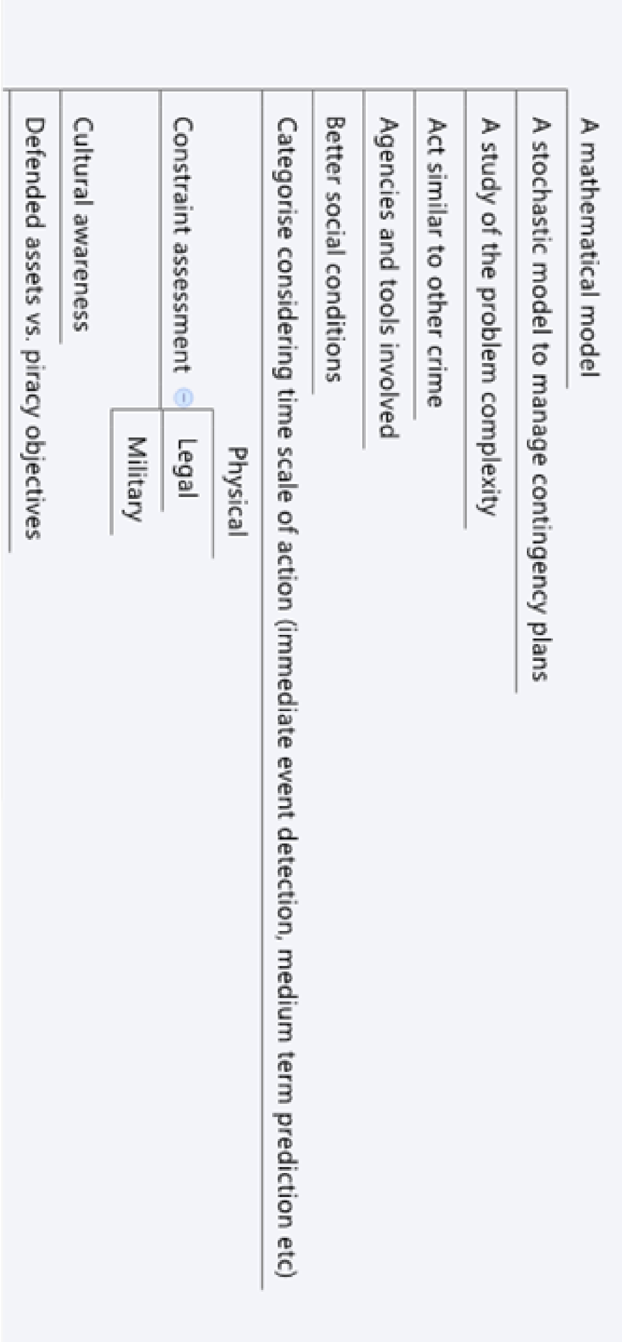
Top View



- A mathematical model
- A stochastic model to manage contingency plans
- A study of the problem complexity
- Act similar to other crime
- Agencies and tools involved
- Better social conditions
- Categorise considering time scale of action (immediate event detection, medium term prediction etc)
- Constraint assessment
- Cultural awareness
- Defended assets vs. piracy objectives
- Denial
- Early detection system
- Economic enablers
- Effective patrolling
- Experience: extract rules from the past experience using data mining tools
- Human limits of actions
- Human-system interaction
- Information availability and quality
- Information Sharing/Trust
- Intelligence Analysis
- Interdiction
- International Collobaration
- Legal
- Maximizing the surveillance area coverage
- Military
- Monitoring
- Multi-lateral problem involving many aspects needed to understand the root of the origin and try to deminish it.
- Political stability
- Prediction
- Prediction and tracking
- Punishment/Execution
- Reconnaissance
- Recruitment
- Resources available
- Rule of law and trustful institutions
- Sensor performance vs. availability (QUANTITY/quality)
- Ship crew special training
- Social network special operation
- Stabilization of Somalia
- Surveillance
- Technology availability (quantity/quality)
- Threat context analysis and reasoning
- To Comply with best management practice (BMP3) version 3 June 2010
- Traffic organization
- Using data mining concept to analyze the situation
- Weapons of availability
- What is needed for a successful attack

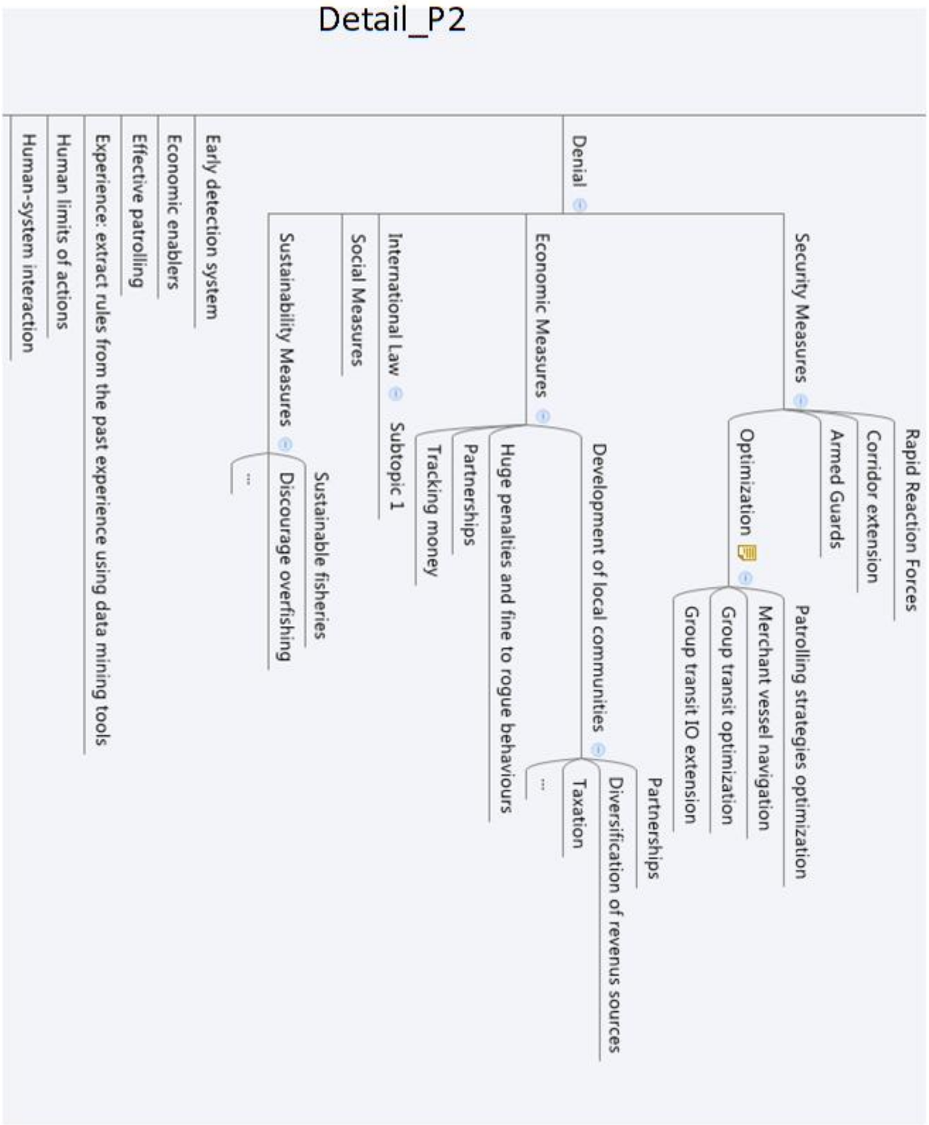
Prevention

Detail_P1



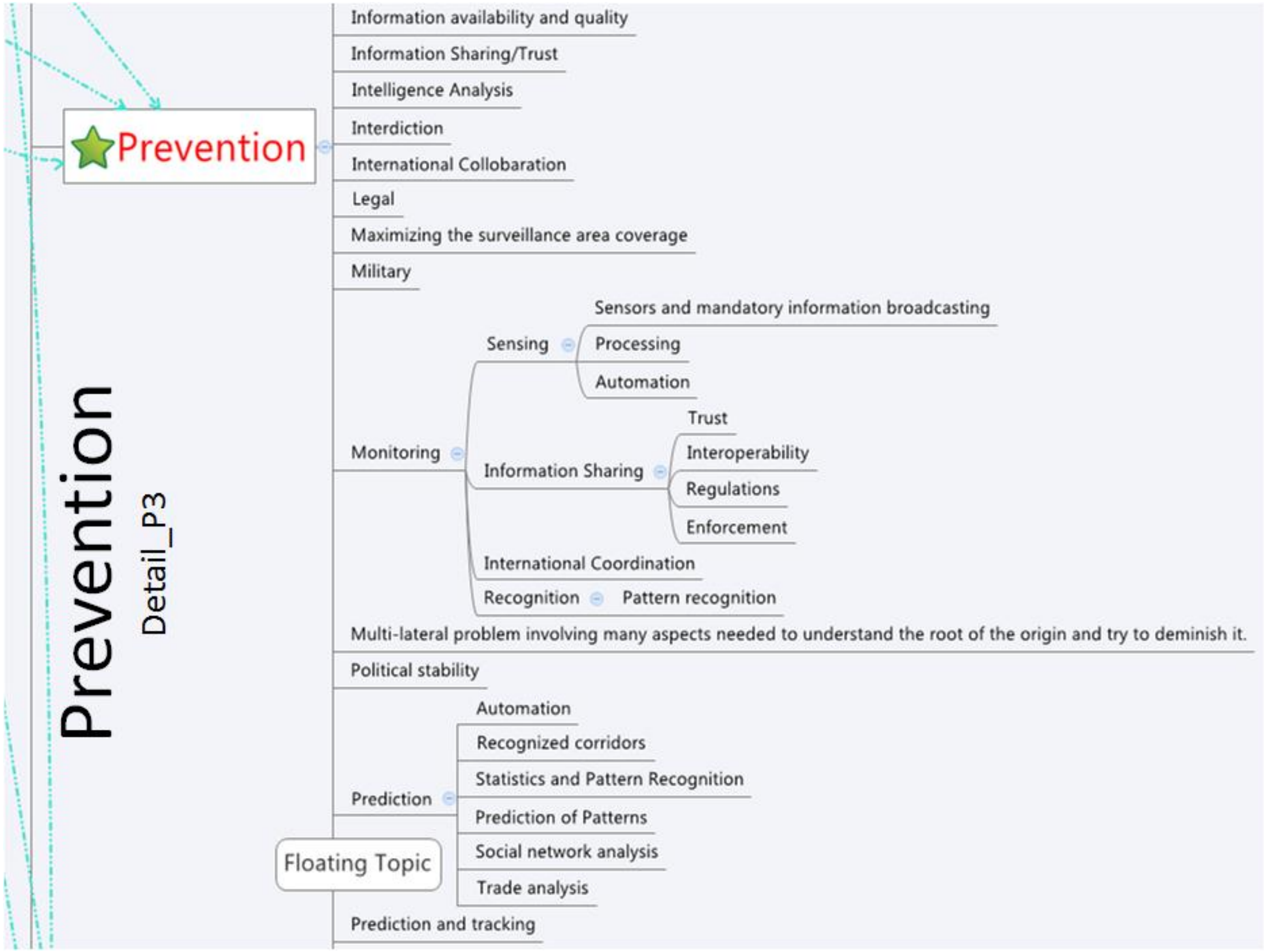
- A mathematical model
- A stochastic model to manage contingency plans
- A study of the problem complexity
- Act similar to other crime
- Agencies and tools involved
- Better social conditions
- Categorise considering time scale of action (immediate event detection, medium term prediction etc)
- Constraint assessment
  - Physical
  - Legal
  - Military
- Cultural awareness
- Defended assets vs. piracy objectives

Prevention



Detail_P2

- Denial
  - Security Measures
    - Rapid Reaction Forces
    - Corridor extension
    - Armed Guards
    - Optimization
      - Patrolling strategies optimization
      - Merchant vessel navigation
      - Group transit optimization
      - Group transit IO extension
  - Economic Measures
    - Development of local communities
      - Partnerships
      - Diversification of revenus sources
      - Taxation
      - ...
    - Huge penalties and fine to rogue behaviours
    - Partnerships
    - Tracking money
  - International Law
    - Subtopic 1
  - Social Measures
  - Sustainability Measures
    - Sustainable fisheries
    - Discourage overfishing
    - ...
- Early detection system
- Economic enablers
- Effective patrolling
- Experience: extract rules from the past experience using data mining tools
- Human limits of actions
- Human-system interaction



Prevention

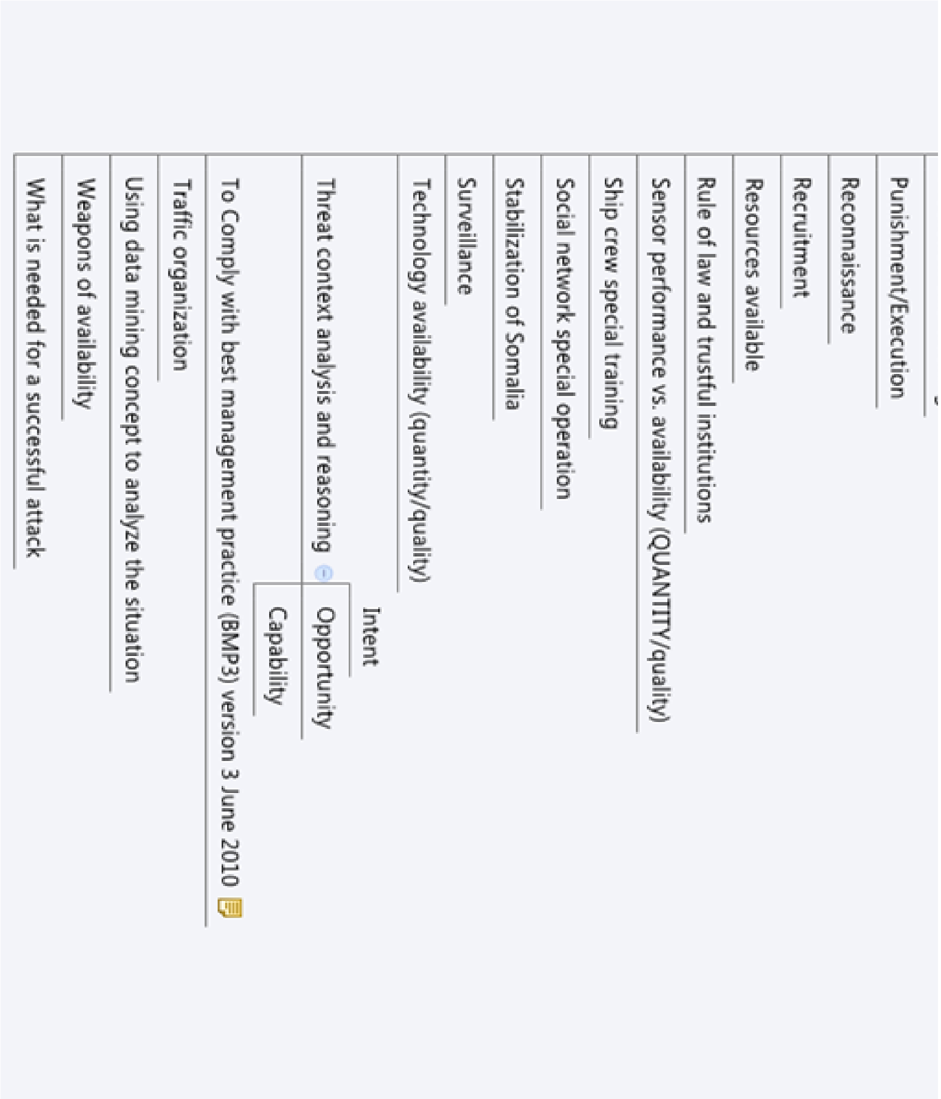
Detail_P3

- Prevention
  - Information availability and quality
  - Information Sharing/Trust
  - Intelligence Analysis
  - Interdiction
  - International Collobaration
  - Legal
  - Maximizing the surveillance area coverage
  - Military
  - Monitoring
    - Sensing
      - Sensors and mandatory information broadcasting
      - Processing
      - Automation
    - Information Sharing
      - Trust
      - Interoperability
      - Regulations
      - Enforcement
    - International Coordination
    - Recognition
      - Pattern recognition
  - Multi-lateral problem involving many aspects needed to understand the root of the origin and try to deminish it.
  - Political stability
  - Prediction
    - Automation
    - Recognized corridors
    - Statistics and Pattern Recognition
    - Prediction of Patterns
    - Social network analysis
    - Trade analysis
  - Prediction and tracking

Floating Topic

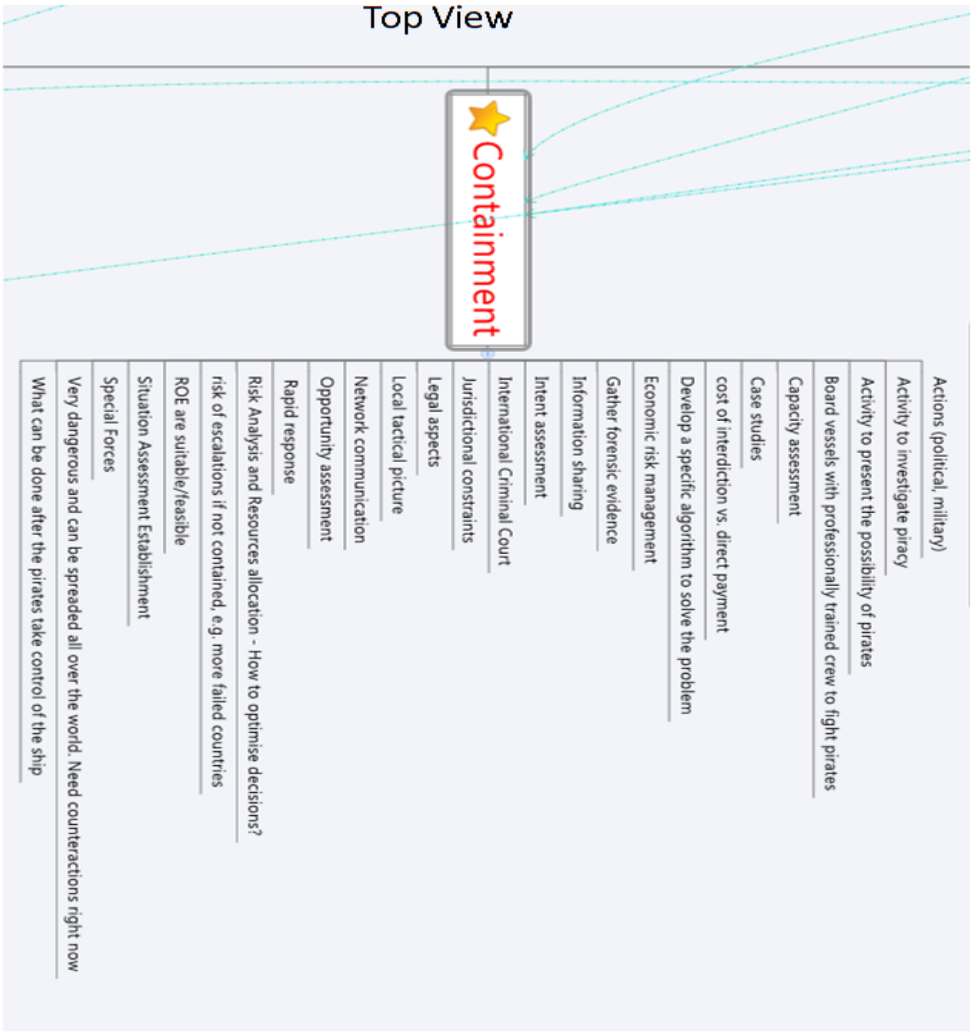
Prevention

Detail_P4



- Punishment/Execution
- Reconnaissance
- Recruitment
- Resources available
- Rule of law and trustful institutions
- Sensor performance vs. availability (QUANTITY/quality)
- Ship crew special training
- Social network special operation
- Stabilization of Somalia
- Surveillance
- Technology availability (quantity/quality)
- Threat context analysis and reasoning
  - Intent
  - Opportunity
  - Capability
- To Comply with best management practice (BMP3) version 3 June 2010
- Traffic organization
- Using data mining concept to analyze the situation
- Weapons of availability
- What is needed for a successful attack

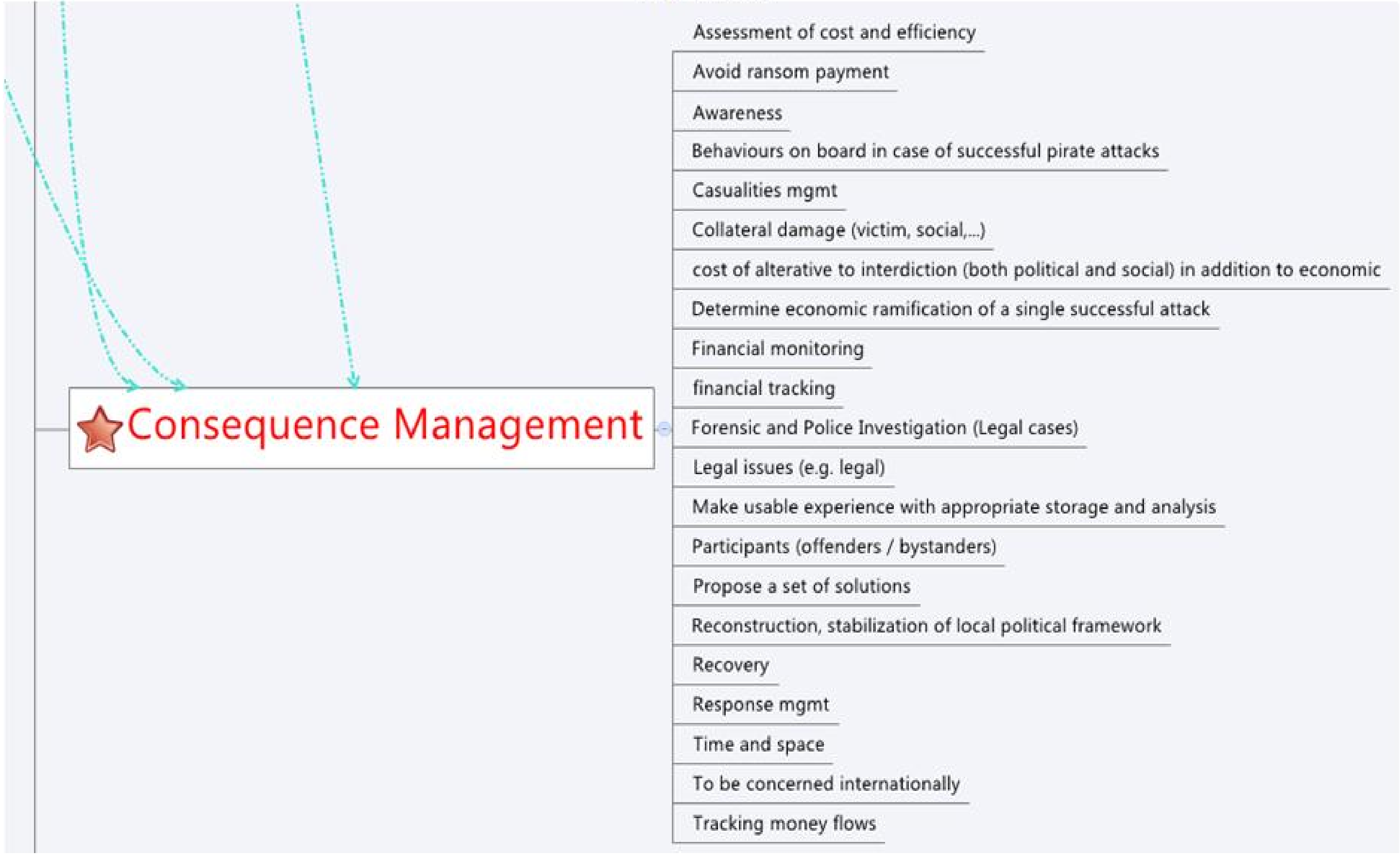
Containment



- Actions (political, military)
- Activity to investigate piracy
- Activity to present the possibility of pirates
- Board vessels with professionally trained crew to fight pirates
- Capacity assessment
- Case studies
- cost of interdiction vs. direct payment
- Develop a specific algorithm to solve the problem
- Economic risk management
- Gather forensic evidence
- Information sharing
- Intent assessment
- International Criminal Court
- Jurisdictional constraints
- Legal aspects
- Local tactical picture
- Network communication
- Opportunity assessment
- Rapid response
- Risk Analysis and Resources allocation - How to optimise decisions?
- risk of escalations if not contained, e.g. more failed countries
- ROE are suitable/feasible
- Situation Assessment Establishment
- Special Forces
- Very dangerous and can be spreaded all over the world. Need counteractions right now
- What can be done after the pirates take control of the ship

Consequence Management

Top View

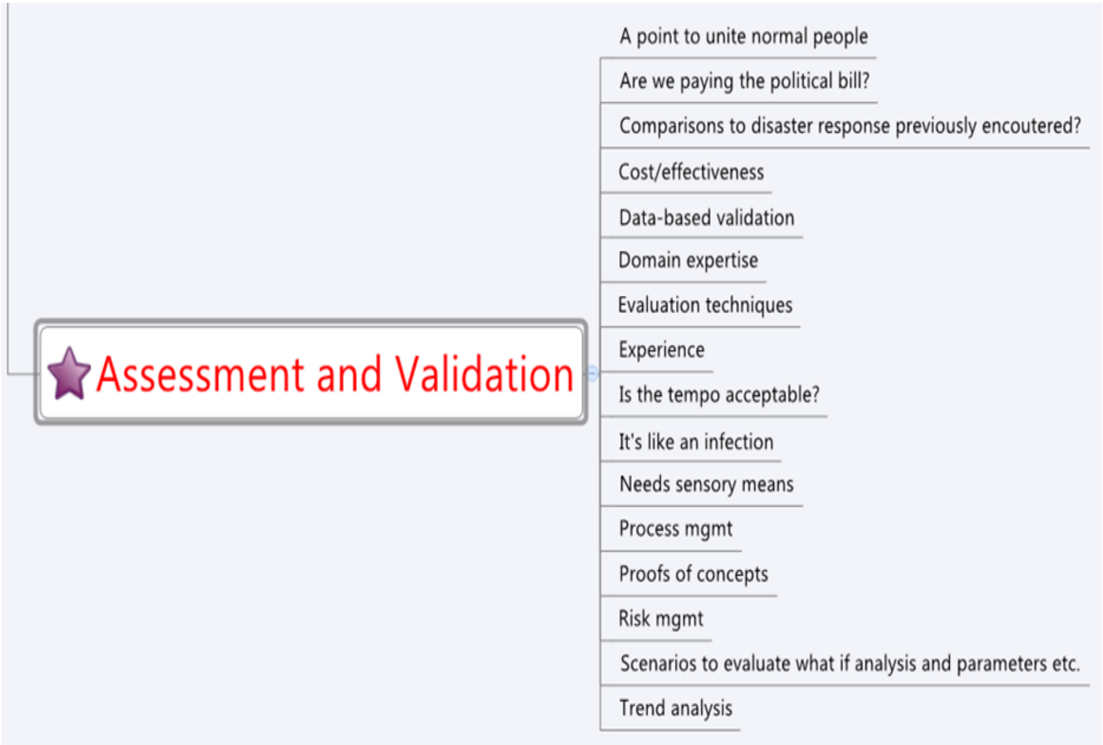


Consequence Management

- Assessment of cost and efficiency
- Avoid ransom payment
- Awareness
- Behaviours on board in case of successful pirate attacks
- Casualities mgmt
- Collateral damage (victim, social,...)
- cost of alterative to interdiction (both political and social) in addition to economic
- Determine economic ramification of a single successful attack
- Financial monitoring
- financial tracking
- Forensic and Police Investigation (Legal cases)
- Legal issues (e.g. legal)
- Make usable experience with appropriate storage and analysis
- Participants (offenders / bystanders)
- Propose a set of solutions
- Reconstruction, stabilization of local political framework
- Recovery
- Response mgmt
- Time and space
- To be concerned internationally
- Tracking money flows

Assessment and Validation

Top View



Assessment and Validation

A point to unite normal people

Are we paying the political bill?

Comparisons to disaster response previously encoutered?

Cost/effectiveness

Data-based validation

Domain expertise

Evaluation techniques

Experience

Is the tempo acceptable?

It's like an infection

Needs sensory means

Process mgmt

Proofs of concepts

Risk mgmt

Scenarios to evaluate what if analysis and parameters etc.

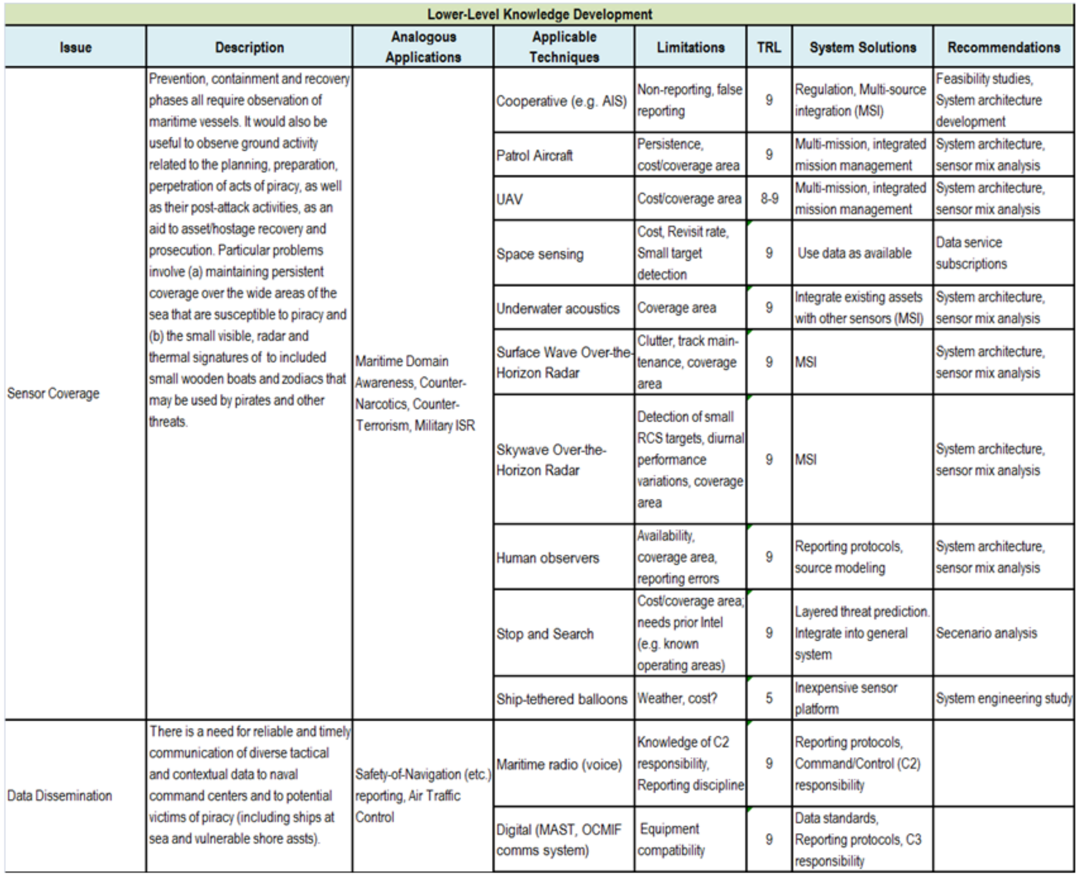
Trend analysis

Annex B

Technology Applicability

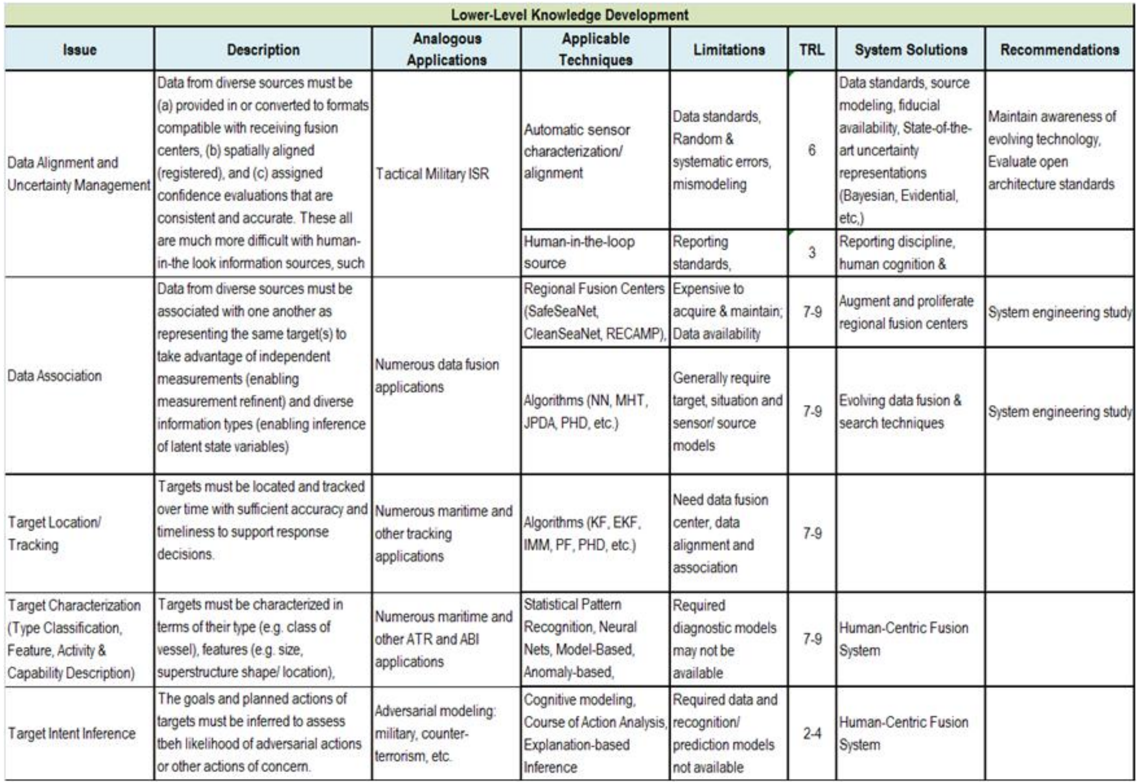
\

Lower-Level Knowledge Development



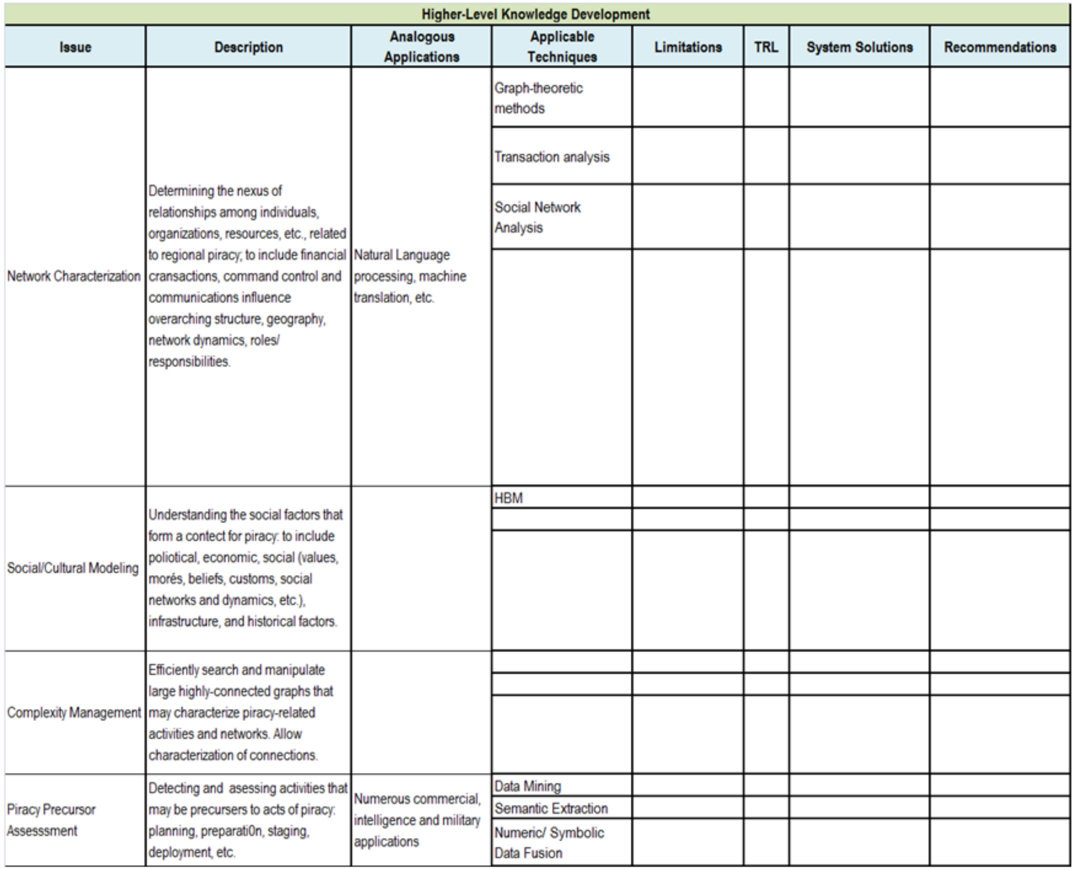
Lower-Level Knowledge Development							
Issue	**Description**	**Analogous Applications**	**Applicable Techniques**	**Limitations**	**TRL**	**System Solutions**	**Recommendations**
Sensor Coverage	Prevention, containment and recovery phases all require observation of maritime vessels. It would also be useful to observe ground activity related to the planning, preparation, perpetration of acts of piracy, as well as their post-attack activities, as an aid to asset/hostage recovery and prosecution. Particular problems involve (a) maintaining persistent coverage over the wide areas of the sea that are susceptible to piracy and (b) the small visible, radar and thermal signatures of to included small wooden boats and zodiacs that may be used by pirates and other threats.	Maritime Domain Awareness, Counter-Narcotics, Counter-Terrorism, Military ISR	Cooperative (e.g. AIS)	Non-reporting, false reporting	9	Regulation, Multi-source integration (MSI)	Feasibility studies, System architecture development
			Patrol Aircraft	Persistence, cost/coverage area	9	Multi-mission, integrated mission management	System architecture, sensor mix analysis
			UAV	Cost/coverage area	8-9	Multi-mission, integrated mission management	System architecture, sensor mix analysis
			Space sensing	Cost, Revisit rate, Small target detection	9	Use data as available	Data service subscriptions
			Underwater acoustics	Coverage area	9	Integrate existing assets with other sensors (MSI)	System architecture, sensor mix analysis
			Surface Wave Over-the-Horizon Radar	Clutter, track main-tenance, coverage area	9	MSI	System architecture, sensor mix analysis
			Skywave Over-the-Horizon Radar	Detection of small RCS targets, diurnal performance variations, coverage area	9	MSI	System architecture, sensor mix analysis
			Human observers	Availability, coverage area, reporting errors	9	Reporting protocols, source modeling	System architecture, sensor mix analysis
			Stop and Search	Cost/coverage area; needs prior Intel (e.g. known operating areas)	9	Layered threat prediction. Integrate into general system	Secenario analysis
			Ship-tethered balloons	Weather, cost?	5	Inexpensive sensor platform	System engineering study
Data Dissemination	There is a need for reliable and timely communication of diverse tactical and contextual data to naval command centers and to potential victims of piracy (including ships at sea and vulnerable shore assts).	Safety-of-Navigation (etc.) reporting, Air Traffic Control	Maritime radio (voice)	Knowledge of C2 responsibility, Reporting discipline	9	Reporting protocols, Command/Control (C2) responsibility	
			Digital (MAST, OCMIF comms system)	Equipment compatibility	9	Data standards, Reporting protocols, C3 responsibility	

Lower-Level Knowledge Development, cont'd



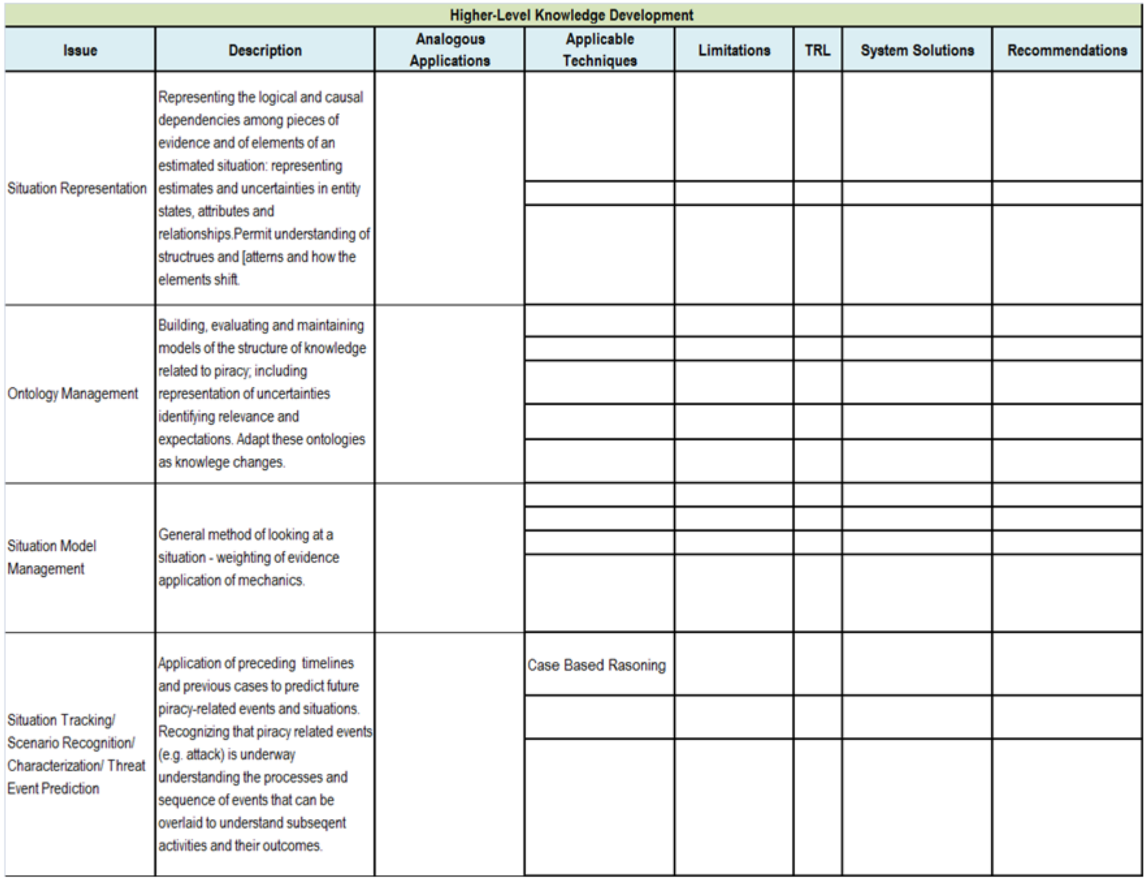
Lower-Level Knowledge Development							
Issue	**Description**	**Analogous Applications**	**Applicable Techniques**	**Limitations**	**TRL**	**System Solutions**	**Recommendations**
Data Alignment and Uncertainty Management	Data from diverse sources must be (a) provided in or converted to formats compatible with receiving fusion centers, (b) spatially aligned (registered), and (c) assigned confidence evaluations that are consistent and accurate. These all are much more difficult with human-in-the look information sources, such	Tactical Military ISR	Automatic sensor characterization/ alignment	Data standards, Random & systematic errors, mismodeling	6	Data standards, source modeling, fiducial availability, State-of-the-art uncertainty representations (Bayesian, Evidential, etc,)	Maintain awareness of evolving technology, Evaluate open architecture standards
			Human-in-the-loop source	Reporting standards,	3	Reporting discipline, human cognition &	
Data Association	Data from diverse sources must be associated with one another as representing the same target(s) to take advantage of independent measurements (enabling measurement refinent) and diverse information types (enabling inference of latent state variables)	Numerous data fusion applications	Regional Fusion Centers (SafeSeaNet, CleanSeaNet, RECAMP),	Expensive to acquire & maintain; Data availability	7-9	Augment and proliferate regional fusion centers	System engineering study
			Algorithms (NN, MHT, JPDA, PHD, etc.)	Generally require target, situation and sensor/ source models	7-9	Evolving data fusion & search techniques	System engineering study
Target Location/ Tracking	Targets must be located and tracked over time with sufficient accuracy and timeliness to support response decisions.	Numerous maritime and other tracking applications	Algorithms (KF, EKF, IMM, PF, PHD, etc.)	Need data fusion center, data alignment and association	7-9		
Target Characterization (Type Classification, Feature, Activity & Capability Description)	Targets must be characterized in terms of their type (e.g. class of vessel), features (e.g. size, superstructure shape/ location),	Numerous maritime and other ATR and ABI applications	Statistical Pattern Recognition, Neural Nets, Model-Based, Anomaly-based,	Required diagnostic models may not be available	7-9	Human-Centric Fusion System	
Target Intent Inference	The goals and planned actions of targets must be inferred to assess tbeh likelihood of adversarial actions or other actions of concern.	Adversarial modeling: military, counter-terrorism, etc.	Cognitive modeling, Course of Action Analysis, Explanation-based Inference	Required data and recognition/ prediction models not available	2-4	Human-Centric Fusion System	

Higher-Level Knowledge Development



Higher-Level Knowledge Development							
Issue	Description	Analogous Applications	Applicable Techniques	Limitations	TRL	System Solutions	Recommendations
Network Characterization	Determining the nexus of relationships among individuals, organizations, resources, etc., related to regional piracy; to include financial cransactions, command control and communications influence overarching structure, geography, network dynamics, roles/ responsibilities.	Natural Language processing, machine translation, etc.	Graph-theoretic methods				
			Transaction analysis				
			Social Network Analysis				
Social/Cultural Modeling	Understanding the social factors that form a contect for piracy: to include poliotical, economic, social (values, morés, beliefs, customs, social networks and dynamics, etc.), infrastructure, and historical factors.		HBM				
Complexity Management	Efficiently search and manipulate large highly-connected graphs that may characterize piracy-related activities and networks. Allow characterization of connections.						
Piracy Precursor Assesssment	Detecting and asessing activities that may be precursers to acts of piracy: planning, preparati0n, staging, deployment, etc.	Numerous commercial, intelligence and military applications	Data Mining				
			Semantic Extraction				
			Numeric/ Symbolic Data Fusion				

Higher-Level Knowledge Development, cont’d



Higher-Level Knowledge Development							
Issue	Description	Analogous Applications	Applicable Techniques	Limitations	TRL	System Solutions	Recommendations
Situation Representation	Representing the logical and causal dependencies among pieces of evidence and of elements of an estimated situation: representing estimates and uncertainties in entity states, attributes and relationships.Permit understanding of structrues and [atterns and how the elements shift.						
Ontology Management	Building, evaluating and maintaining models of the structure of knowledge related to piracy; including representation of uncertainties identifying relevance and expectations. Adapt these ontologies as knowlege changes.						
Situation Model Management	General method of looking at a situation - weighting of evidence application of mechanics.						
Situation Tracking/ Scenario Recognition/ Characterization/ Threat Event Prediction	Application of preceding timelines and previous cases to predict future piracy-related events and situations. Recognizing that piracy related events (e.g. attack) is underway understanding the processes and sequence of events that can be overlaid to understand subseqent activities and their outcomes.		Case Based Rasoning				