



HAL
open science

Evaluation de situations multi-agents à partir d'observations partielles et hétérogènes

Kilian Vasnier

► **To cite this version:**

Kilian Vasnier. Evaluation de situations multi-agents à partir d'observations partielles et hétérogènes. Système multi-agents [cs.MA]. Normandie Université, 2020. Français. NNT : 2020NORMC207 . tel-03103332

HAL Id: tel-03103332

<https://theses.hal.science/tel-03103332v1>

Submitted on 8 Jan 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Normandie Université

THÈSE

Pour obtenir le diplôme de doctorat

Spécialité INFORMATIQUE

Préparée au sein de l'Université de Caen Normandie

Evaluation de situations multi-agents à partir d'observations partielles et hétérogènes

**Présentée et soutenue par
Kilian VASNIER**

**Thèse soutenue publiquement le 06/07/2020
devant le jury composé de**

Mme ZAHIA GUESSOUM	Maître de conférences HDR, Université Reims Champagne Ardenne	Rapporteur du jury
M. RENE MANDIAU	Professeur des universités, Université polytechnique Hauts de France	Rapporteur du jury
Mme MAROUA BOUZID	Professeur des universités, Université Caen Normandie	Président du jury
Mme AMAL EL FALLAH SEGHRUCHNI	Professeur des universités, Université Paris 6 Pierre et Marie Curie	Membre du jury
M. ABDEL ILLAH MOUADDIB	Professeur des universités, Université Caen Normandie	Directeur de thèse

Thèse dirigée par ABDEL ILLAH MOUADDIB, Groupe de recherche en informatique, image, automatique et instrumentation



UNIVERSITÉ
CAEN
NORMANDIE



Notice

Cette thèse est en partie financée par la DGA (Direction Générale de l'Armement) à travers le dispositif Cifre-Défense via le contrat n° 005/2016/DGA.

Ce document et son contenu sont la copropriété de AIRBUS DEFENCE AND SPACE SAS et du GREYC de l'Université de Normandie et ne doit pas être copié ni diffusé sans autorisation. Toute utilisation en dehors de l'objet expressément prévu est interdite.

Il est strictement interdit de reproduire, distribuer et utiliser le contenu de ce document sans l'autorisation préalable de l'auteur. Les contrefacteurs seront jugés responsables pour le paiement des dommages. Tous droits réservés y compris pour les brevets, modèles d'utilité, dessins et modèles enregistrés.

Copyright ©2019 - AIRBUS DEFENCE AND SPACE SAS - GREYC, Université de Normandie - Tous droits réservés.



Remerciements

Résumé

Dans cette thèse, nous considérons le problème d'évaluation de situations dans le cadre plus spécifique des situations de crise. Dans le cadre de ces situations de crise, nous nous intéressons plus particulièrement au problème de l'évaluation de la menace dans un environnement topologique formalisé sous forme de graphe.

Les systèmes d'évaluation de situations proposent actuellement une récupération souvent passive de l'information et sont confrontés à deux problématiques majeures : l'hétérogénéité des informations décrivant l'environnement qui amène à un problème de représentation de la connaissance et une forte complexité temporelle due au volume important de ces informations alors que cette dimension est critique dans le cas des situations de crise.

Nous proposons un système d'évaluation de situations automatisé (le système ASAAP) cherchant à pallier ces deux problèmes. Nous y présentons une modélisation dynamique de l'environnement permettant une analyse des variables d'états utiles à l'évaluation de la situation afin de réduire le champ des possibles et maximiser le gain d'informations. Dans le cadre des situations de crise, nous proposons également une application du système à l'évaluation de menace. Cette contribution permet d'analyser et définir la menace à laquelle sont exposées différentes zones tout en définissant la stratégie de l'ennemi. Enfin, nous proposons une approche préliminaire sur l'optimisation de l'utilisation des capteurs pour couvrir les variables d'états utiles dans l'optique de maximisation du gain d'informations.

Nous avons généré des scénarios inspirés de situations réelles afin d'évaluer nos approches dans les domaines maritime et militaire. Les résultats du système ASAAP montrent une amélioration de l'évaluation de situation en terme de complexité ainsi que la capacité de décrire la stratégie de l'ennemi dans un temps raisonnable.

Mots-clefs : Évaluation de situations, Situation de crise, Modélisation d'environnement dynamique, Évaluation de menace, Représentation de la connaissance.



Abstract

In this thesis, we consider the problem of situation awareness, and more specifically, in crisis situation. In the crisis situation field, we are interested primarily in threat assessment in a topographical environment with a graph representation.

Situation awareness systems propose mostly a passive acquisition of information and they face two major problematics. Firstly, the heterogeneity of information which describes the environment brings a knowledge representation problem. The second problem is a high temporal complexity due to the large amount of information while this dimension is crucial in crisis situation assessment.

We propose an automated situation awareness system (ASAAP system) which tries to mitigate these problems. We present a dynamic environment modelling allowing an analysis of most valuable variables for situation assessment in order to reduce the field of possibilities and maximise the information gain. In the crisis situation field, we also propose to apply our system on a more specific domain, the threat assessment. This contribution allows to define and analyse the threat level of each exposed zones with the capacity of understanding the enemy's strategy by both representing its targets and the path to reach them. Finally, we present a preliminary approach about the optimisation of the coverage of most valuable variables by the sensors to maximise the information gain.

We generated scenarios inspired from real situations to evaluate ours approaches in maritime and military field. The ASAAP system results show an improvement in situation awareness in its complexity and by its capacity to describes the enemy's strategy in reasonable time.

Mots-clefs : Situation awareness, Crisis situation, Dynamic environment modelling, Threat assessment, Knowledge representation.



Table des matières

Table des matières	ix
Liste des figures	xv
Liste des tableaux	xix
1 Introduction	1
I État de l’art	7
2 Évaluation de situations	9
2.1 L’origine des modèles d’évaluation de situations	10
2.1.1 L’intuition des modèles d’évaluation de situations à travers l’histoire	10
2.1.2 Les modèles mentaux	11
2.2 Cycle OODA et cycle du renseignement	12
2.2.1 Cycle du renseignement	12
2.2.2 Le cycle OODA et ses évolutions	13
2.3 Définition de l’évaluation de situations	18
2.3.1 Le modèle d’Ensley	18
2.3.2 Un modèle holistique de SA	20
2.4 Évolution des modèles d’évaluation de situation	22
2.4.1 Modèle de Fusion d’Informations JDL DF	22
2.4.2 Exemple de modélisation de SA pour le C2	23
2.4.3 Révision du modèle JDL DF par DFIG	26
2.5 La Fusion d’Informations Haut-Niveau	28
2.5.1 La Fusion d’Informations	28

2.5.2	La Fusion d'Informations Haut-Niveau	30
2.6	La Perception Active	37
2.6.1	Les problématiques de la Perception Active	37
2.6.2	La perception active dans les systèmes multi-agents	38
2.7	Conclusion	40
3	La représentation de la connaissance	43
3.1	Qu'est-ce que la représentation de connaissances ?	44
3.1.1	La représentation de connaissances	44
3.1.2	Le triangle sémiotique	45
3.1.3	Données, informations et connaissances	46
3.1.4	Premières applications	47
3.1.5	Les ontologies	48
3.2	La représentation de l'incertitude	52
3.2.1	Représenter l'incertitude	52
3.2.2	Les mesures de probabilités	53
3.2.3	Réseaux bayésiens dynamiques	54
3.2.4	La théorie Dempster-Shafer	58
3.3	La théorie de l'information de Shannon	59
3.3.1	La théorie de l'information	59
3.3.2	L'entropie de Shannon	60
3.4	Conclusion	61
4	L'évaluation de la menace	63
4.1	L'évaluation de menace	64
4.1.1	Les principes de l'évaluation de menace	64
4.1.2	Une tâche de prédiction	65
4.2	Le modèle COI pour la menace	68
4.3	La propagation de la menace	71
4.3.1	La menace, une propagation incertaine	71
4.3.2	La propagation de croyances de Pearl	71
4.3.3	Propagation de croyances et complexité	73
4.4	Considération de la menace selon la doctrine militaire	74
4.4.1	Définition de l'environnement et de la menace	74
4.4.2	L'UBR, une unité multicapteurs	75
4.4.3	Fiabilité et véracité de l'information	76
4.5	Conclusion	77
II	Contributions théoriques	79
5	Un nouveau système d'évaluation de situations	81

5.1	Le système ASAAP	81
5.1.1	Brique de Fusion d'Informations	83
5.1.2	Brique d'analyses des variables	83
5.1.3	Brique d'optimisation des capteurs	84
5.2	Conclusion	85
6	L'analyse des variables utiles	87
6.1	La fusion d'informations avec les Réseaux Bayésiens Dynamiques	88
6.2	Modélisation de l'environnement via les DBN	89
6.3	L'analyse des variables les plus utiles	91
6.3.1	Une variable utile	92
6.3.2	Processus d'analyse au sein d'un DBN	93
6.4	Conclusion	96
7	Propagation de menace	97
7.1	Introduction	97
7.2	Modélisation du problème à travers un graphe topologique	98
7.2.1	Définition de l'environnement	98
7.2.2	Définition de la menace	100
7.3	Un système de propagation de menace automatisé	100
7.3.1	Une approche pessimiste	100
7.3.2	Définition formelle du modèle	101
7.3.3	Processus algorithmiques	104
7.4	La menace à horizon défini	105
7.5	Généralisation	107
7.6	Conclusion	108
8	Optimisation association capteurs / variables via le <i>Scored Maximum Flow</i>	109
8.1	Introduction	109
8.2	Modélisation de l'environnement via un graphe biparti	110
8.3	Notations	110
8.4	Poids et capacité	111
8.4.1	Le problème du Flot Maximal	112
8.4.2	Score	114
8.5	Processus de perception active	116
8.5.1	Première étape : variables utiles	116
8.5.2	Deuxième étape : ensemble des variables observables	119
8.5.3	Conclusion	120

III	Évaluation du système	121
9	Cas d’usage maritime	123
9.1	Définition du cas d’usage	123
9.1.1	Les capteurs	124
9.1.2	Les hypothèses à monitorer	125
9.2	Résultats des expérimentations	126
9.2.1	Contraintes de l’expérimentation	126
9.2.2	Déroulement du scénario	126
9.3	Conclusion	130
10	Cas d’usage OPEX	131
10.1	Modélisation de l’environnement	131
10.2	Présentation des trois scénarios	134
10.2.1	Premier scénario - preuve du concept	134
10.2.2	Second scénario - l’attaque multi-objectifs	136
10.2.3	Troisième scénario - une stratégie de feinte	140
10.3	Conclusion	142
11	Résultats préliminaire sur l’optimisation des capteurs	145
11.1	Un problème de complexité combinatoire	145
11.2	Exemple scénario	145
11.2.1	Première étape	146
11.2.2	Deuxième étape	148
11.3	Premières expérimentations :	149
11.3.1	Test sur le premier scénario	149
11.3.2	Test sur le second scénario	150
11.4	Conclusion	152
IV	Conclusion et perspectives	153
12	Synthèse	155
12.1	Un système d’évaluation de situation automatisé	155
12.2	Champs d’applications possibles	156
12.3	Liste des publications réalisées au sein de la thèse	157
13	Perspectives	159
13.1	Perspectives à court terme	159
13.2	Perspectives à moyen terme	159
13.3	Perspective à long terme	160

V	Annexes	I
A	Liste des publications	III
	Bibliographie	V

Liste des figures

1.1	Exemple de domaines de situation de crise	2
2.1	De l'utilité de l'évaluation de situations	9
2.2	Cycle du renseignement	12
2.3	Cycle OODA	14
2.4	Modèle du cycle OODA étendu	15
2.5	Cycle dynamique OODA	17
2.6	Modèle de SA de Endsley	19
2.7	Modèle holistique de Lundberg	21
2.8	Modèle JDL DF	23
2.9	Modèle de SA pour le C2 [Wallenius, 2004]	25
2.10	Modèle JDF DL révisé	26
2.11	Principales différences et exemples d'informations <i>Hard & Soft</i>	30
2.12	Bas-Niveau et Haut-Niveau de fusion d'information (de [Blasch et al., 2012])	31
2.13	Illustration d'espaces conceptuels pour des fruits (de [Dietze and Domingue, 2009])	33
2.14	Framework de fusion d'information du projet MURI (de [Dietze and Domingue, 2009])	34
2.15	Exemple d'ontologie (de [Bellenger, 2013])	35
2.16	Modèle de perception active (de [Weyns et al., 2004])	40
3.1	Comment rendre compréhensible la connaissance pour un or- dinateur ? ¹	44
3.2	Le triangle sémiotique (adapté de [Bellenger, 2013])	46
3.3	Hierarchie des Données-Informations-Connaissances (de [Bel- lenger, 2013])	47
3.4	Le triangle sémiotique (adapté de [Bellenger, 2013])	49

3.5	Ontologie militaire (de [Yoo et al., 2014])	49
3.6	Ontologie Wookie (de [Serrano, 2014])	51
3.7	Les trois types d’incertitude et leurs origines (de [Bellenger, 2013])	52
3.8	Un réseau bayésien avec 5 variables (de [Van Harmelen et al., 2008])	55
3.9	Exemple de représentation de réseau bayésien dynamique . . .	57
3.10	Exemple de représentation de réseau bayésien dynamique . . .	61
4.1	Une bonne évaluation de la menace permet de trouver la bonne contre-mesure	63
4.2	Relation d’inclusion entre l’évaluation de situation, d’impact et de menace (de [Le Guillaume, 2016])	66
4.3	Illustration de l’évaluation de la menace (adapté de [Le Guillaume, 2016])	68
4.4	Le modèle COI (adapté de [Le Guillaume, 2016])	69
4.5	Représentation des facteurs de l’intentions (de [Roy et al., 2007])	70
4.6	Propagation de messages dans un réseau bayésien (de [Ajroud et al., 2012])	72
5.1	Système ASAAP	82
6.1	DBN representation	88
6.2	Représentation de l’environnement via DBN.	90
6.3	Hypothèse θ_i décrite par son DBN	91
6.4	Exempmlle de processus d’analyse des MVV.	95
7.1	Exemple de graphe topologique	99
7.2	Exemple de propagation de menafe sur une carte de chaleur de menace.	103
7.3	Illustration de zone atteignable par une compagnie selon $Vel(c)$. 106	
7.4	Exemple à $t = 1$ avec une compagnie dans z_1	107
8.1	Système ASAAP	109
8.2	Exemple de représentation d’un environnement par un graphe 110	
8.3	Graphe avec les nœuds de la source et du puits	112
8.4	Première étape : application du processus sur les variables utiles 117	
8.5	Deuxième étape : application du processus sur toutes les variables	120
9.1	Hypothèse θ_i décrite par son DBN	126
9.2	Analyses des MVV à l’étape de temps t_1	127

9.3	Résultats de l'analyse des MVV à t_2 et t_3	129
10.1	Graphe topologique des scénarios de l'expérimentation	132
10.2	Exemple d'une carte de chaleur de menace du scénario 1 (à t_2)	134
10.3	Résultats des stratégies <i>5-best</i> pour le scénario 1	136
10.4	Horizon des évènements de la stratégie <i>1-best</i> à t_2 pour le scénario 1	137
10.5	Résultats des stratégies <i>5-best</i> pour le scénario 1	138
10.6	Horizon des évènements de la stratégie <i>1-best</i> à t_3 pour le scénario 2	138
10.7	Résultats des stratégies <i>5-best</i> pour le scénario 3	140
10.8	Horizon des évènements de la stratégie <i>5-best</i> à t_3 pour le scénario 3	142
11.1	Schéma du scénario	146
11.2	Combinaisons possibles	147
11.3	Résultats de l'étape 2	148
11.4	Premier scénario : combinaisons étape 1	149
11.5	Premier scénario : résultats étape 2	150
11.6	Deuxième scénario : quelques exemples de l'étape 1	151
11.7	Second scénario : résultats étape 2	151

Liste des tableaux

2.1	Schéma de partitionnement de Fusion d'Informations (adapté de [Steinberg and Bowman, 2004])	24
2.2	Exemple d'attributs observables par des capteurs <i>Hard</i> et/ou <i>Soft</i> (de [Pravia et al., 2009])	31
4.1	cotation de la fiabilité et véracité d'une source d'information .	77
9.1	Niveau de confusion normalisé des capteurs ϵ	124
9.2	Score de confiance de θ_2 et θ_3 durant les trois étapes de temps du scénario	128
9.3	Attribution des capteurs pour observer les MVV à t_1 et t_2 . . .	128
10.1	TS(c)	132
10.2	Cr(c)	132
10.3	Scenarios	133
10.4	Score de menace des points d'attaque (AP) - Scénario 1	135
10.5	Score de menace des points d'attaque (AP) - Scénario 2	139
10.6	Score de menace des points d'attaque (AP) - Scénario 3	141

CHAPITRE 1

Introduction

Les travaux présentés dans cette thèse s'intéressent à de nombreux domaines transverses rassemblés autour d'un champ de recherche qui est l'évaluation de situations.

Avec les progrès de l'informatique et de l'intelligence artificielle, l'univers scientifique se penche depuis plusieurs décennies sur l'évaluation de situations. Cette tâche, souvent réservée à l'homme dans le monde applicatif, nécessite la capacité de représenter et comprendre un très grand nombre d'informations. Certaines sont simples et directement observables, mais d'autres sont complexes et composées de plusieurs autres informations nécessitant d'inférer leur état. Cette complexité est de plus en plus grandissante du fait que les capteurs permettant de récupérer ces informations sur une situation à évaluer sont de plus en plus nombreux et divers. Et l'analyse des informations brutes est souvent complexe pour être gérée par l'homme en un temps satisfaisant. D'où le besoin de réussir à automatiser le plus possible certaines tâches afin d'agglomérer ces informations et d'en permettre une représentation lisible et analysable humainement tout en étant cependant le plus proche possible de la réalité. En effet, les informations sont souvent bruitées et peuvent parfois être inexactes. C'est d'autant plus vrai pour des informations inférées à partir de plusieurs autres. L'enjeu est donc de permettre d'avoir une représentation la plus exhaustive possible de la situation à évaluer, tout en étant le plus proche possible de l'état actuel de la situation.

Dans le cadre de ces travaux, nous nous sommes focalisés sur un domaine spécifique de l'évaluation de situation, celui des situations de crise. Une situation de crise amène deux contraintes fortes. La première est que le temps est une ressource précieuse et le but est d'acquérir une connaissance opti-

male sur la situation satisfaisante le plus rapidement possible. En effet, dans le cas d'une situation de crise, nous voulons avoir la possibilité de mettre en place une contre-mesure à la situation que l'on cherche à résoudre. La deuxième contrainte (souvent liée à celle du temps) est que les ressources d'observations sont limitées et empêchent une observation omnivoyante de la situation. Il faut donc composer avec les ressources disponibles et optimiser au mieux leur utilisation de sorte à ce qu'elles permettent d'apporter le maximum d'information pour combler ce manque.

Beaucoup de domaines s'intéressent à l'évaluation de situations et plus spécifiquement aux situations de crise. Le domaine de la défense et du renseignement en premier lieu pour notamment l'analyse des champs de bataille pour optimiser ses défenses ou ses troupes ou encore l'appréhension de personnes armées lors d'attaques terroristes. Mais aussi le domaine des secours lors de catastrophes naturelles par exemple pour l'optimisation des moyens de sauvetage en fonction de l'évolution de la catastrophe. Certains domaines médicaux, comme l'épidémiologie, peuvent aussi chercher à réaliser des simulations de crises avec la propagation de maladies et les moyens de mettre en place une procédure d'urgence pour endiguer la diffusion d'agents pathogènes.



FIGURE 1.1 – Exemple de domaines de situation de crise

Le premier domaine transverse de l'évaluation d'évaluation correspond à l'acquisition de données via des sources hétérogènes. En effet, les capteurs permettant d'obtenir de l'information sont de plus en plus nombreux et diversifiés. Cela amène à un véritable défi scientifique sur la façon de traiter un tel flux d'informations qui peuvent être tout autant physiques (caméra, micro, radar, ...), que linguistiques (rapport, observateur humain, réseaux sociaux, ...). Cette hétérogénéité amène à une autre grande problématique, celle de la fusion d'informations que la littérature scientifique cherche à résoudre depuis de nombreuses années. La question est de réussir à comprendre lorsque plusieurs capteurs différents apportent de l'information s'ils parlent d'un même

objet ou de plusieurs. L'étape de fusion d'informations est une étape cruciale et critique pour permettre une représentation correcte de la situation à un instant donné. De nombreux outils existent pour permettre cette fusion entre certains types de données, mais pour gérer l'ensemble des informations ; les solutions manquent encore de maturité pour permettre à un système automatisé de le réaliser.

Outre les problèmes de fusion, la modélisation est une autre grande difficulté que l'évaluation de situation rencontre. Ce que nous appelons la représentation de connaissances est un sujet étudié depuis plus d'une soixantaine d'années. Il est question ici d'être en mesure de modéliser et définir l'environnement que nous devons évaluer pour qu'une machine soit en mesure de réaliser des calculs et en représenter les résultats nécessaires à la bonne analyse de la situation. De nombreux modèles existent, avec chacun leurs avantages et inconvénients, et il faut ici faire un travail approfondi de conception pour savoir à terme ce qu'il faudra être en mesure de faire sur les données permettant de décrire notre environnement.

La représentation de connaissances est donc intimement liée à la façon d'analyser et d'inférer les états des objets de l'environnement à évaluer. C'est ici le troisième grand domaine de l'évaluation de situations. Pour permettre à un système d'analyser de façon automatisée une situation, il doit être en mesure de comprendre grâce à la modélisation de l'information ce qui se passe dans l'environnement. Pour cela, le modèle doit permettre la représentation potentielle des états des objets de l'environnement et de se représenter lequel ou lesquels sont les plus probables. Cela nécessite d'être en mesure de réfléchir via un historique d'informations tout en prenant en compte des contraintes liées à la situation à analyser. Cela demande un travail de compréhension *à priori* sur ce que nous voulons analyser dans la situation et quelles informations doivent être comprises et connues afin de résoudre cette situation. Cependant, cette étape amène un degré supplémentaire d'incertitude quant à l'état réel des objets de l'environnement de par cette inférence. Cette incertitude doit être prise en compte dans la confiance que l'on porte à l'image de la situation que l'on obtient.

Enfin, la finalité de l'évaluation de situation doit composer avec les problématiques et les difficultés liées au domaine de la prise de décision et d'aide à la décision. Le facteur de décision se trouve dans le cas de l'évaluation de situation à deux moments clefs. Le premier lors de l'analyse en elle-même de la situation afin d'avoir une image la plus proche possible de la réalité. À ce moment donné, la décision concerne la façon d'orienter ses capteurs pour essayer d'obtenir le maximum d'informations et de la meilleure qualité possible. Cette décision est en continu à chaque cycle de temps pendant la période d'acquisition de l'information afin d'affiner sa connaissance sur

cette dernière. La seconde phase de la décision est lorsque la situation est considérée comme suffisamment connue, c'est à dire le moment où le preneur de décision a suffisamment d'éléments pour prendre une décision sur ce qu'il doit faire afin de résoudre la situation. Dans ce deuxième cas, on parle presque systématiquement d'aide à la décision dans le sens où la décision automatisée n'est pas ou rarement en mesure de prendre des décisions aussi critiques. L'aide à la décision est un domaine où l'outil automatique est présent pour appuyer un opérateur humain dans sa prise de décision en facilitant son accès à l'information.

Une autre notion importante dans le monde de l'évaluation de situations est celui de la perception. La majeure partie de ce qui a été proposé dans la littérature scientifique pour les systèmes d'évaluation de situations propose une perception dite passive. Où le but est simplement de capter le maximum d'informations possibles en maximisant l'utilisation des capteurs. Cependant, une notion relativement récente nous intéresse, celle de la perception active. Dans ce deuxième cas, nous cherchons à déterminer quelles informations pourraient nous permettre de comprendre plus rapidement et plus efficacement la situation.

Les travaux présentés dans ce manuscrit font état dans un premier temps d'une veille scientifique traitant l'intégralité des domaines présentés ci-dessus. Les contributions proposées dans cette thèse se focalisent sur l'analyse de l'environnement et proposent une aide à la décision en améliorant la connaissance de la situation à évaluer et en apportant une lisibilité sur la confiance estimée de l'analyse automatisée. Pour cela, un système "expert" de perception active est proposé dans son fonctionnement global où l'idée est de comprendre quelles seront les variables les plus utiles à la prochaine itération d'observation afin de maximiser le gain d'information. Les contributions se concentrent, au sein de ce système, sur l'analyse des variables de l'environnement ainsi que sur des travaux préliminaires, sur l'optimisation de l'utilisation des capteurs d'observation suite à cette analyse.

Ce manuscrit est organisé en quatre parties. La première concerne la veille scientifique réalisée sur le sujet et divisée en trois chapitres décrivant le concept d'évaluation de situation, puis les problématiques de la représentation de la connaissance liées à la section précédente et enfin l'évaluation de la menace qui est un domaine spécialisé de l'évaluation de situation. La seconde partie décrit les contributions de la thèse. Le premier chapitre décrit le système d'évaluation de situations proposé dans nos travaux. Le second chapitre présente l'algorithme d'analyse des variables dites utiles au sein de notre système. Un troisième chapitre définit le système de propagation de menace mis en place comme cas spécifique de l'évaluation de situation. Et enfin le quatrième chapitre propose des travaux préliminaires sur l'optimisa-

tion de l'utilisation de capteurs pour observer des variables via un algorithme de flot maximum. La troisième partie expose les différents cas d'usages et d'applications réalisés pour évaluer le système proposé. Le premier chapitre présente le cas d'usage maritime concernant la modélisation du système afin d'y appliquer l'algorithme d'analyse des variables utiles. Un deuxième chapitre introduit le cas d'usage OPEX (Opérations Extérieures) qui présente des résultats concernant la propagation de menace. Enfin un troisième chapitre propose les résultats préliminaires sur l'optimisation des capteurs pour observer les variables. Pour finir, la quatrième partie se divise en deux chapitres pour proposer d'abord une synthèse des travaux réalisés, puis les perspectives de cette thèse.

Première partie
État de l'art

CHAPITRE 2

Évaluation de situations

L'évaluation de situation (*Situation Awareness* ou *Situational Awareness* qui sera notée SA à l'avenir) est un domaine de recherche qui ne cesse d'attirer de plus en plus l'intérêt depuis ces quatre dernières décennies. L'idée derrière ce concept est d'être en mesure de décrire les états d'une situation réelle de la façon la plus précise et complète possible au vu des informations à disposition pour un utilisateur humain. Un tel outil a pour but d'aider ces opérateurs à prendre une décision dans des problèmes où la complexité de la situation rend son analyse difficile.

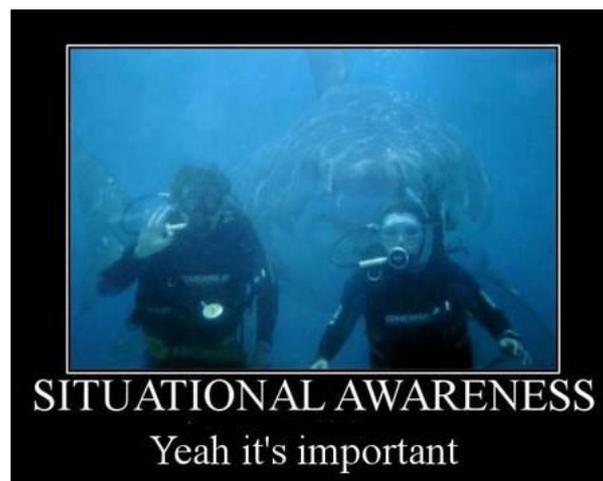


FIGURE 2.1 – De l'utilité de l'évaluation de situations

Le besoin d'être en mesure de connaître et comprendre une situation afin d'anticiper ses conséquences et ne pas se faire surprendre s'exprime dans de nombreux domaines.

À titre d'exemple, dans le domaine des secours en cas de catastrophe naturelle, il est indispensable d'évaluer les risques d'une réplique d'un tremblement de terre pendant un sauvetage et de connaître les zones les plus à risque. Tout comme il est nécessaire de savoir combien et où se trouvent les personnes à secourir afin de savoir comment répartir les différentes équipes et de prioriser les zones. Dans le domaine militaire, l'intérêt de comprendre qui est l'ennemi, les troupes engagées et leurs intentions précises sont des facteurs vitaux pour mettre en place une contre-mesure efficace et planifier les actions de leurs unités.

La difficulté devant l'évaluation de situations tient autant de la capacité à représenter et modéliser les problèmes et les concepts définissant une situation que dans l'automatisation de l'aide à la décision via des systèmes afin de répondre à cette situation.

2.1 L'origine des modèles d'évaluation de situations

2.1.1 L'intuition des modèles d'évaluation de situations à travers l'histoire

L'évaluation de situations prend ses racines dans l'histoire de la théorie militaire. Le terme SA est relativement récent et a été défini au cours des quarante dernières années dans la communauté scientifique.

Il est possible de remonter tôt dans l'histoire sur les premières nécessités d'évaluer des situations dans le domaine militaire avec notamment l'œuvre de Sun Tzu *l'art de la guerre* [Tzu, 2019], rédigée vers 512 avant notre ère, où la formalisation du conflit militaire prenait en compte le contexte d'un conflit autrement que par la simple quantité de troupes à affronter. Le résultat de l'évaluation de situation aide à prendre une décision pour réagir à cette dernière.

Plus récemment, la première utilisation du terme SA a pris place dans la formalisation d'une mesure de l'évaluation d'une situation dans le domaine de recherche des facteurs humains. Plusieurs travaux se sont concentrés sur l'étude des phénomènes contingents dans le domaine de l'aéronautique [Dawson and Biferno, 1973] [Biferno and Dawson, 1977].

Cependant, le domaine du SA prend réellement pied dans les années 90 où les recherches ont commencé à proliférer dans de nombreux domaines (militaires, aéronautiques, sécurité civile, services de secours, catastrophes naturelles...). La formalisation de ces problématiques, bien que dans des contextes

différents, cherche à définir les étapes nécessaires à la résolution pour y adapter la modélisation adéquate.

2.1.2 Les modèles mentaux

Les modèles de SA se sont inspirés des modèles mentaux qui décrivent la façon de penser d'une personne à travers un processus afin de comprendre comment le monde réel fonctionne.

Formellement, un modèle mental est défini tel que [Forrester, 1971] :

Définition 1. L'image du monde autour de nous, que nous construisons mentalement, est juste un modèle. Personne dans sa tête n'imagine tous les mondes, gouvernements ou pays. On ne sélectionne que des concepts, des relations entre eux et on les utilise pour représenter le système réel.

On comprend suite à cette définition qu'il n'est pas nécessaire de représenter toutes les informations d'un environnement, mais seulement les concepts, objets et relations nécessaires à comprendre le système qui nous intéresse. L'intérêt ici est de pouvoir monitorer uniquement les éléments nécessaires à la compréhension d'une situation afin de gagner en clarté et en efficacité.

Cette représentation de l'environnement permet ensuite de définir des algorithmes pour comprendre un comportement (d'une personne ou d'un objet) au sein de ce dernier. Les relations entre concepts ou leurs actions dans l'environnement permettent de comprendre leurs buts ou leur stratégie au sein d'un système fermé et défini pour répondre à une problématique spécifique. L'idée est d'imiter l'intuition d'un opérateur humain qui observe une situation afin d'en dresser une image et de comprendre quels sont les enjeux en cours.

Les modèles mentaux se décrivent par une série d'axiomes et de règles pour comprendre et décrire un environnement. Chaque modèle décrit une possibilité d'évolution d'un environnement avec l'évolution de ses concepts ou objets le composant ainsi que leurs relations. Les modèles sont basés sur le principe de vérité, ce qui implique qu'ils décrivent uniquement ce qui est vrai dans la possibilité de la situation présentée par rapport aux choses observées et les axiomes du système [Johnson-Laird, 2006].

Les opérateurs considèrent qu'une situation est plausible lorsqu'elle est valide dans tous les modèles décrivant la situation. Le principe est d'utiliser le contre-exemple comme moyen d'invalidier une inférence d'un modèle [Schroyens et al., 2003].

Les environnements opérationnels, à décrire, étant complexes et nécessitant l'observation de nombreux éléments, il est difficile de prendre une dé-

cision sur les mesures à percevoir. Les modèles mentaux correspondent à la perception et à la compréhension de l'environnement, puis l'opérateur doit en inférer les états possibles et futurs pour comprendre ce qu'il va se passer afin d'être en mesure de prendre une décision [Serfaty et al., 1997].

Cependant, les modèles mentaux ne permettent pas une formalisation suffisamment complète pour permettre de définir un modèle d'aide à la décision pour l'évaluation de situations.

2.2 Cycle OODA et cycle du renseignement

Le domaine de l'évaluation de situations a trouvé ses premiers cas d'application dans le domaine militaire et celui du renseignement. Les premières formalisations de modèles ont donc cherché à décrire les besoins et les étapes nécessaires à l'évaluation de situations dans des processus d'analyse, de planification et d'action sur l'environnement.

2.2.1 Cycle du renseignement

Dans les années 80, le concept du cycle de renseignement a été mis en avant dans des problématiques de fusion d'informations pour l'aide à la décision.

The Intelligence Cycle

Facilitates well-informed business and security decisions about risks to your brand, reputation, people, infrastructure, and partners.

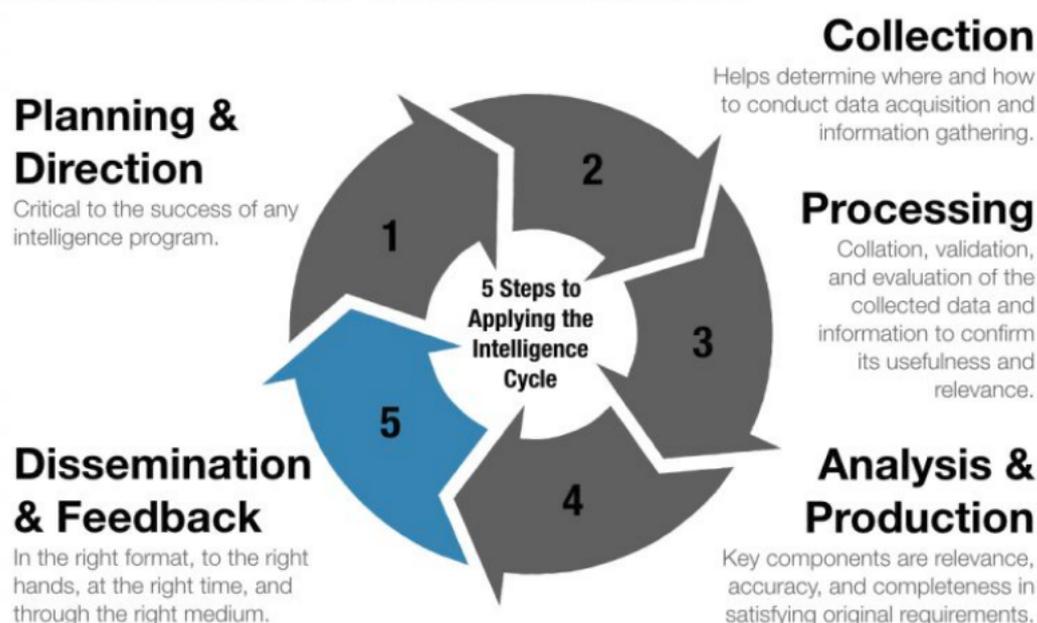


FIGURE 2.2 – Cycle du renseignement

La Figure 2.2¹ présente ce cycle décrit en 5 phases :

- **Planification et direction** : Compréhension de ce qui doit être achevé dans le cadre de la mission et sur comment parvenir à la prise d'informations pour être en mesure de prendre les bonnes décisions. Cette première étape est la plus cruciale dans le cycle du renseignement. Une fois cette étape réalisée, les équipes de renseignement comprennent le problème et savent quoi et où chercher pour le résoudre. C'est notamment durant cette étape que les sources d'informations sont définies pour permettre une collecte efficace et pertinente.
- **Collecte d'informations** : Déploiement de moyens tels que des capteurs physiques ou des sources humaines pour obtenir des informations brutes généralement présentées sous forme de rapport de renseignements avec un haut niveau d'abstraction.
- **Évaluation des données** : Analyse, comparaison et corrélation des rapports générés par l'étape précédente. Les données collectées sont ainsi évaluées afin de vérifier leur utilité et leur pertinence.
- **Analyse et production de rapports** : Fusion des informations collectées et analysées lors de la phase précédente. Cette fusion permet la génération de rapports de renseignements complets de façon lisible et synthétique par un opérateur humain. Le but est de rapporter les informations pertinentes de la façon la plus complète et précise possible.
- **Dissémination et retours** : Distributions de ces informations fusionnées aux opérateurs humains en mesure d'utiliser ces informations pour la prise de décision. Une fois le retour de ces opérateurs effectué, la tâche est considérée comme complétée et la prise de décision sur la mission est alors rendue possible.

Le cycle du renseignement, même si conçu initialement pour le domaine militaire et de la défense, est aussi employé dans de nombreux autres domaines comme celui de l'entreprise, du management ou de l'étude de projet et client par exemple.

2.2.2 Le cycle OODA et ses évolutions

2.2.2.1 Le cycle OODA

Le cycle OODA (Observer-Orienter-Décider-Agir) (aussi appelé *Boyd Control Loop*) a été développé par le Colonel John Boyd de l'*United States*

1. Image provenant de <https://www.groupsense.io/intelligence-cycle/>

Air Force (USAF) en 1987 [Boyd, 1987]. Ce modèle a été créé pour le Commandement et Contrôle (*Command and Control* noté C2) qui est "un ensemble organisationnel et technique qui se sert d'opérateurs humains, de capteurs physiques et de ressources d'informations afin de résoudre des problèmes et accomplir des missions" [Pigeau and McCann, 2002] [Claverie and Desclaux, 2016].

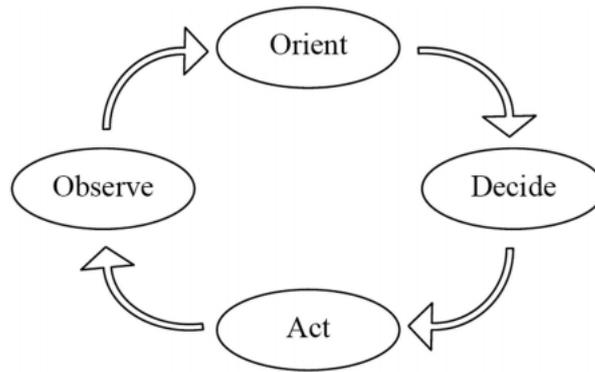


FIGURE 2.3 – Cycle OODA

La Figure 2.3 montre le cycle OODA qui est composé de 4 phases :

- **Observer** : Récupérer des informations sur l'environnement.
- **Orienter** : Évaluer et comprendre la situation à partir des informations récupérées pour comprendre la menace.
- **Décider** : Répondre à la situation et réfléchir sur les prochaines actions à entreprendre.
- **Agir** : Planifier et exécuter les actions pour solutionner la situation

Le cycle OODA, bien que simpliste, permet de refléter au mieux les besoins du C2 et a été abondamment utilisé dans les problématiques de fusion d'informations dans ces domaines [Hall and McMullen, 2004] [Nilsson, 2007] [Niklasson et al., 2008].

2.2.2.2 Le cycle OODA étendu

Ce modèle a rapidement été étendu suite aux critiques du premier modèle considéré comme trop simpliste. La Figure 2.4 montre l'évolution du modèle OODA après sa généralisation par Boyd qui a permis d'étendre son utilisation à d'autres formes de combat que celle du combat un contre un. Dans les principales modifications, l'intérêt de ce modèle étendu est la présence de nombreuses boucles de retours (*feedbacks*) aussi bien au moment de la décision qu'au moment de l'action (les deux dernières phases). En effet, les hypothèses définies lors de la phase de décision peuvent nécessiter de nouvelles observations pour être validées ou invalidées avant d'agir. De même,

la phase d'action peut nécessiter la confirmation de l'effet attendu si cette dernière se prolonge sur une longue durée. Enfin, une action, comme dans le modèle précédent, amène à une modification de l'environnement et nécessite donc de nouvelles approches d'observation pour vérifier ses conséquences.

La phase d'orientation a elle aussi été enrichie. L'orientation était initialement considérée comme la recherche, l'évaluation et la compréhension de composantes physiques (positions d'un ennemi, direction, ...). Cette fois, le modèle prend aussi en considération des composantes psychologiques (comme les traditions culturelles ou les expériences passées) afin de mieux représenter l'objectif ou le comportement observé de l'ennemi. Cela introduit donc des concepts plus abstraits et de haut-niveau pour le preneur de décision afin de mieux l'orienter dans ses choix.

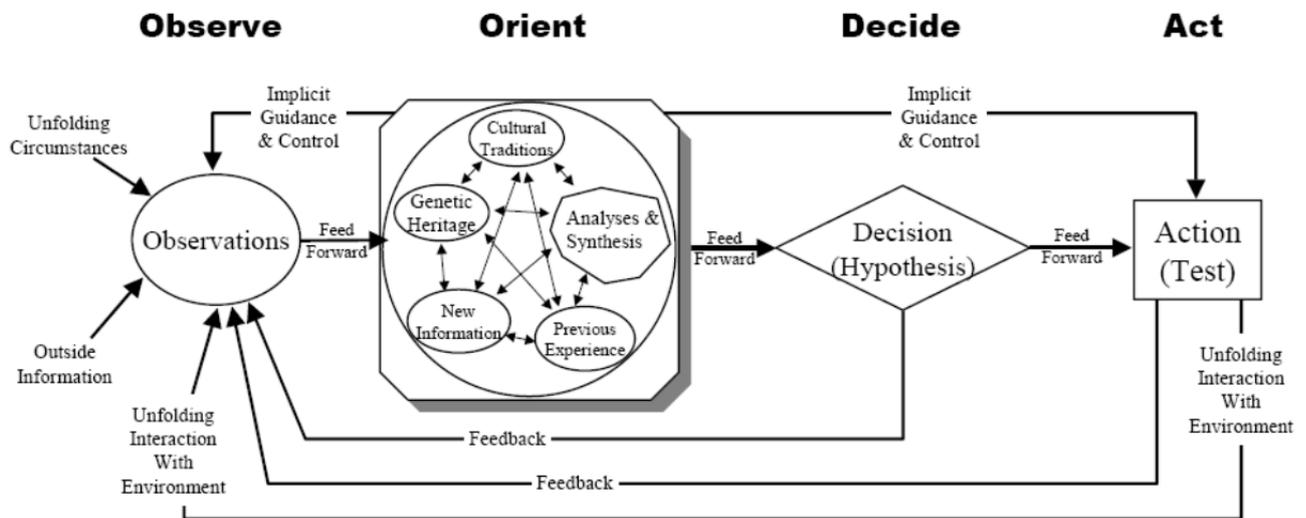


FIGURE 2.4 – Modèle du cycle OODA étendu

Cependant, ce modèle continue de subir trois principales critiques. La première est qu'il n'arrive toujours pas à généraliser suffisamment la modélisation pour qu'elle fonctionne dans tous les domaines. Mais elle n'est pas non plus assez précise pour le domaine militaire. La seconde est que ce modèle ne s'applique qu'à un combattant dans les situations d'action et ne peut pas fonctionner pour une armée ou des théâtres d'opération. Enfin la troisième critique reproche que le cycle OODA ne permet que de capturer une image statique de la prise de décision.

2.2.2.3 Le cycle OODA dynamique

Pour pallier ce manque de prise en compte dynamique dans la prise de décision, [Brehmer, 2005] propose le cycle OODA dynamique (ou D-OODA), soit un modèle générique pour le C2, qui est une adaptation du cycle OODA

de Boyd et qui a été réalisé pour fonctionner avec les modèles cybernétiques du C2.

Pour réaliser ce modèle, Brehmer s'est demandé quelles fonctions devaient être satisfaites pour permettre à un commandant de réaliser sa mission au sein du C2. Pour cela, le livre *Command in war* [Van Creveld, 1985] a formalisé ce qui caractérise les missions du C2 en huit fonctions telles que :

- Recueillir les informations des ses propres forces, celles des forces ennemies, du temps météorologique et du terrain.
- Trouver des moyens de stocker, collecter, filtrer, classifier, distribuer, et afficher les informations.
- Évaluer la situation.
- Fixer des objectifs et élaborer des moyens alternatifs pour les atteindre.
- Décider de ce qu'il faut faire.
- Planifier.
- Écrire les ordres et les transmettre en vérifiant qu'ils ont été reçus et correctement compris par leurs récepteurs.
- Surveiller leur exécution au moyen de retours d'informations (*feedbacks*) au cours desquels le processus se répète.

Le modèle, en se basant sur ces huit propositions, s'est divisé en différentes fonctions (collecte d'informations, recherche de sens, concept de commandement, planification, décision/ordre, activité militaire, effets) telles que représentées dans la Figure 2.5. Ces fonctions sont les suivantes :

- **Le concept de commandement** : un concept global de conduite de l'opération. C'est le concept le plus important du modèle.
- **La recherche de sens** : le *sensemaking* se réfère à la compréhension de la situation actuelle et ce qui peut être fait à ce moment. Le résultat de cette fonction est une décision collective du commandant et de son État-Major afin de viser une action à réaliser. Cependant, il faut souligner qu'il ne faut pas confondre *sensemaking* avec évaluation de la situation.
- **Effet** : la décision a un effet explicite et significatif dans l'environnement qui l'entoure.
- **les flèches du schéma** : elles déterminent le flux et les boucles de retour entre les différentes fonctions. Cependant la possibilité de chevauchement de fonctions (*overlaps*) est un problème connu.

Malgré la reconnaissance de ce modèle dans le domaine de la prise de décisions naturelles (*Natural Decision Making*), il n'a pas été accepté par la

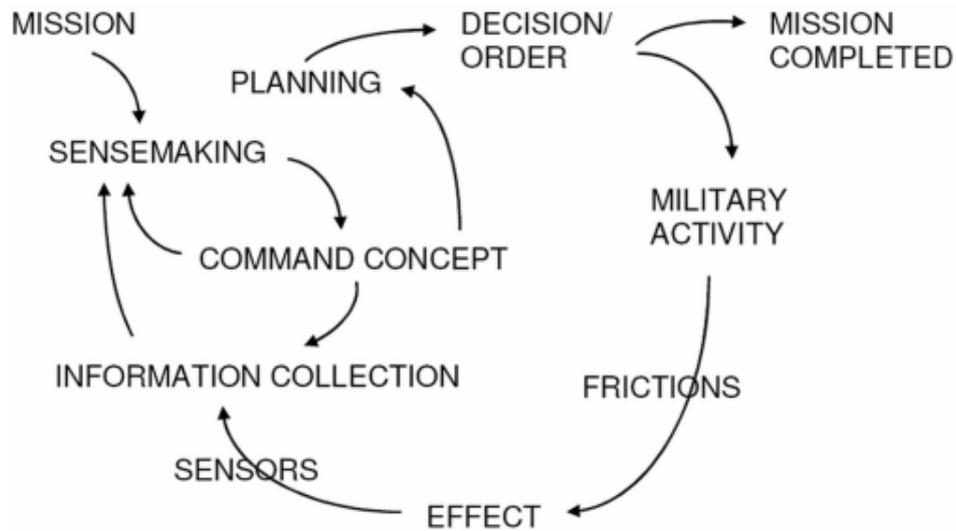


FIGURE 2.5 – Cycle dynamique OODA

communauté de fusion d'informations en tant que processus de Commandement et Contrôle (C2). Les experts ont aujourd'hui tendance à développer des modèles *ad-hoc* internes plutôt que les modélisations plus génériques comme le cycle OODA et ses dérivés bien qu'ils s'en inspirent.

2.3 Définition de l'évaluation de situations

L'évaluation de situation a dû attendre la fin des années 80 voire le début des années 90 avant de pouvoir trouver une définition plus généralisée et adaptable à tous les domaines.

2.3.1 Le modèle d'Ensley

L'évaluation de situations est un concept défini comme étant la perception d'éléments et d'évènements au sein d'un environnement spatialisé et temporel. Plus formellement, la définition retenue est la suivante [Ensley, 1987] [Ensley, 1988b] :

Définition 2. Le SA est la perception des éléments dans un environnement à travers le temps et l'espace, leurs significations et la projection de leurs statuts dans un futur proche.

Le point important dans cette définition (en plus de ce que sont les modèles mentaux) est de permettre la projection de l'état des éléments de l'environnement dans le futur. Cela permet de pouvoir anticiper les prochains états de la situation pour essayer de comprendre les conséquences de celle-ci. La perception et la compréhension à chaque instant d'une situation permet donc de mettre à jour ce que l'on croit possible dans son évolution potentielle.

La Figure 2.6 décrit le modèle développé par Ensley [Ensley, 1988a] [Ensley, 1995] qui est la première référence de modèle de SA à partir duquel de nombreux autres ont découlé. Ce modèle décrit une boucle à chaque étape de temps d'une situation. Le système se trouve à un instant donné dans un certain état. La première étape est celle du SA décrit en trois niveaux que sont la perception, la compréhension et la projection. Suite à cela, il est possible de prendre une décision sur la situation actuelle et une fois la décision prise, on réalise les actions (contres-mesures) afin de régler le problème présenté. Cela engendre un nouvel état du système qui amène à devoir de nouveau appliquer le modèle de SA et ainsi de suite. Chacune de ces étapes nécessite une connaissance experte des buts potentiels des éléments présents dans l'environnement et d'avoir un moyen de représenter toutes ces informations.

Les trois étapes du SA sont définies par Ensley [Ensley, 1987] tel que :

- **(Niveau 1) Perception** : "La première étape à réaliser dans un système de SA est de percevoir les statuts, les attributs et la dynamique des éléments pertinents de l'environnement". Le Niveau 1 consiste donc à la surveillance des différents éléments observables concernant la situation

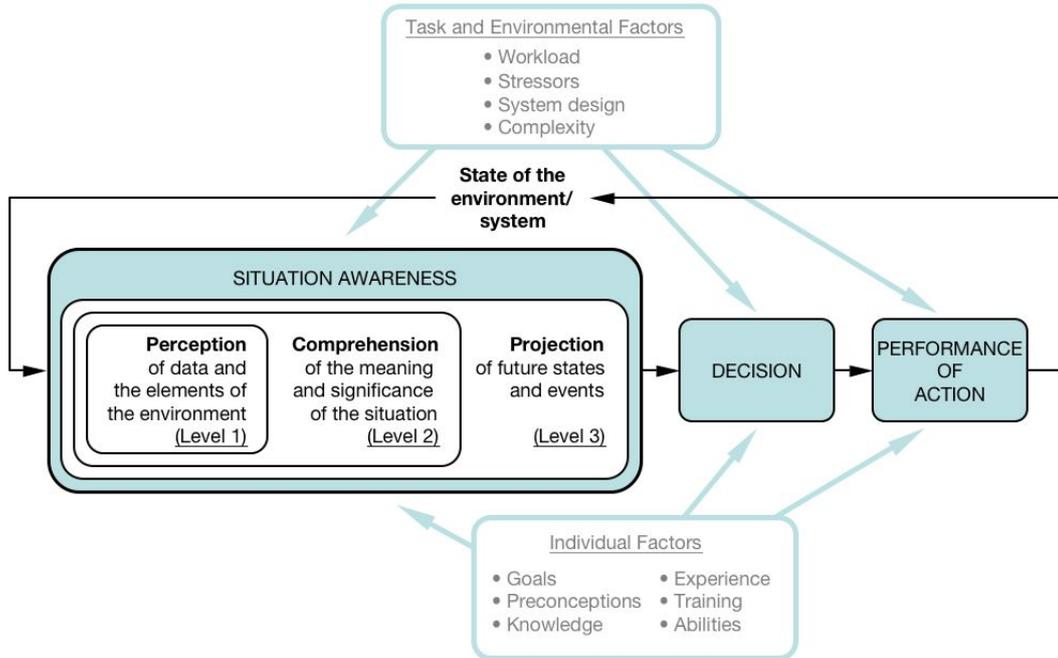


FIGURE 2.6 – Modèle de SA de Endsley

à évaluer ainsi que les évènements la décrivant. Par exemple, un général sur un théâtre d'opération doit avoir une idée des troupes qui ont été repérées (nombre d'unités, localisation, type, capacité, ...).

- **(Niveau 2) Compréhension** : "La compréhension de la situation est basée sur la synthèse des éléments disjoints du Niveau 1". Ici, l'idée et de réussir à comprendre l'impact de la présence des éléments observés dans la première étape selon leur état courant à l'aide de reconnaissance de "patterns", d'interprétations et d'évaluations. Suite à cette étape, un opérateur est capable de décrire une image holistique de la situation à l'instant présent. Par exemple, comprendre que la présence de troupes ennemies à proximité d'un point sensible peut représenter une tentative d'attaque de ce dernier.
- **(Niveau 3) Projection** : "La capacité à projeter les actions futures des éléments présents dans l'environnement - au moins à court terme - compose le troisième et plus haut niveau de SA". Ce dernier niveau nécessite la compréhension de la situation des deux niveaux précédents et de la dynamique des éléments observés. Riche de cette connaissance, la projection a pour but d'extrapoler ces informations afin d'estimer la suite la plus crédible et plausible des évènements. Par exemple, une fois des troupes ennemies détectées dans une zone, il peut être possible d'envisager le chemin le plus probable que ces dernières comptent emprunter, voire d'estimer la stratégie que l'ennemi compte appliquer.

Ce premier modèle est la référence en termes de SA pour globaliser la

méthode, peu importe le contexte ou le domaine auxquels il s'applique. Il décrit les grandes étapes nécessaires à la formalisation de la prise de décision naturelle dans des environnements dynamiques où un opérateur doit observer et analyser l'évolution des acteurs de la situation à analyser.

Ces premiers travaux ont pu donc servir de base à toutes les recherches futures qui ont par la suite complété le modèle en y ajoutant ou précisant certaines étapes d'évaluations.

2.3.2 Un modèle holistique de SA

D'autres modèles ont vu le jour plus récemment tel le modèle holistique [Lundberg, 2015] où les états, le système ainsi que les processus descriptifs sont considérés comme interdépendants.

Ce dernier formalise les modèles de SA via quatre concepts (contrairement aux trois de Endley) :

- **Objet** (De quoi parle-t-on ?) : Les objets sont les éléments observés dans l'environnement ainsi que les attributs les décrivant. Ces informations sont mises à jour continuellement pour maintenir la connaissance sur leur état.
- **Trame** (*frame*) (i.e. Que se passe-t-il ?) : La trame représente la compréhension et la délibération sur ce qui se passe au sens large. La capacité à reconnaître une situation peut s'élaborer grâce à la multitude de trames décrites par le système (à savoir que des trames contradictoires peuvent exister).
- **Implication** (i.e. Qu'elle est la situation ?) : L'implication correspond à l'interprétation des objets au sein des trames. C'est ce qui permet l'interprétation d'une trame par l'état des objets pour pouvoir en tirer des conclusions. Les implications font référence au lien entre l'objet et la trame en terme de temps et d'espace. Par exemple, la possibilité de savoir la capacité d'une unité à atteindre un point en un certain temps donné par rapport à un objectif donné.
- **Horizon des évènements** : Cet horizon représente l'évaluation de l'incertitude en terme de temps et d'espace vis-à-vis des évènements ainsi que leur cohérence dans la stratégie globale de la situation observée. L'évaluation doit tenir compte à la fois de la situation courante mais aussi des potentiels futurs états ou évènements (pronostic et propagation) et des évènements passés (diagnostic). L'horizon permet également de représenter différentes alternatives dans le futur de la situation.

Ce processus de SA est dirigé par ces quatre aspects comme le montre la Figure 2.7. Les objets servent de signaux en évaluant continuellement leur

état et en fonction de cette évolution, les trames dans lesquelles ces objets sont impliqués sont elles aussi mises à jour.

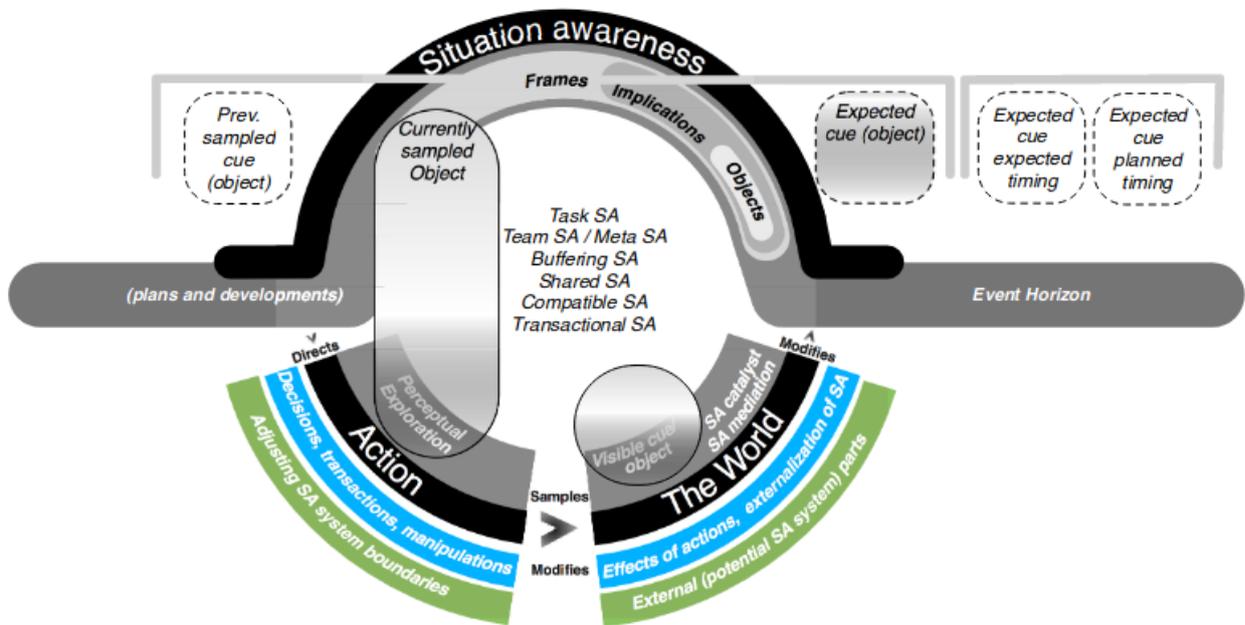


FIGURE 2.7 – Modèle holistique de Lundberg

La connaissance ainsi générée permet de définir l’horizon des évènements et de comprendre quelles sont les prochaines étapes à réaliser en termes d’évaluation, ou de comprendre quels objets doivent être observés par la suite pour comprendre les possibles évolutions de la situation.

Par exemple, le fait de voir qu’une unité se dirige vers un point sensible à défendre dans le cas d’une invasion, permet de comprendre que la zone risque d’être la cible d’une attaque dans un futur plus ou moins proche. Il faut donc concentrer ses forces de défenses vers cette zone et chercher à prendre l’information autour de cette dernière.

Les modèles de SA holistiques ont continué d’émerger des modèles causaux [McAnally et al., 2018]. Ces modèles conceptuels décrivent les mécanismes de causalité d’un système (causes et conséquences des évènements) et sont la réponse logique aux besoins des systèmes d’aide à la décision naturelle [Klein, 2008].

Ces modèles ont commencé à poser la question de la représentation de la connaissance pour un système informatique ce qui sera discuté dans le chapitre suivant.

2.4 Évolution des modèles d'évaluation de situation

2.4.1 Modèle de Fusion d'Informations JDL DF

Le modèle de IF JDL DF a été créé par le JDL Data Fusion Group dans le département de la défense des États-Unis [Hall and Llinas, 1997]. Le but de ce modèle est de faciliter les communications, la compréhension, la coordination et la coopération à travers les différentes communautés de Fusion d'Informations afin d'identifier les problèmes auxquels la fusion de données peut être appliquée. Ce premier modèle a été le plus représenté dans la IF et une étude détaillée peut être trouvée dans les travaux de [Foo and Ng, 2013]. Une première révision du modèle a été réalisée dans [Steinberg et al., 1999] où une définition plus précise et moins restrictive de la Fusion d'Informations apparaît comme étant :

Définition 3. Le processus de combinaison de données ou d'informations pour estimer et prédire l'état d'une entité.

La Figure 2.8 décrit le modèle révisé et recommandé par Steinberg et Bowman [Steinberg and Bowman, 2004]. Ce modèle révisé décrit cinq niveaux fonctionnels de fusion et se focalise sur les entités d'intérêt pour l'utilisateur du système afin d'estimer ou prédire la situation. Ses niveaux sont les suivants :

- **Niveau 0** Évaluation du signal / de l'élément : estimation et prédiction des états des signaux ou des éléments de la situation. Cela correspond aux motifs inférés depuis les observations et les mesures.
- **Niveau 1** Évaluation des entités : estimation et prédiction des états paramétriques et attributifs des entités (en tant qu'individu). Cela comprend l'estimation du type de l'entité, sa position, son activité et tout autre attribut discret ou continu.
- **Niveau 2** Évaluation de situations : estimation et prédiction sur les relations entre entités et états situationnels des entités. Contrairement au Niveau 1, les entités ici sont considérées comme une agrégation d'éléments définissant une situation (comment participent-ils à la situation ?).
- **Niveau 3** Évaluation de l'impact : estimation et prédiction des effets, des états, des entités et des situations fusionnés en rapport avec leurs objectifs. L'idée est de prédire l'utilité et le coût de l'état d'une entité ou d'une situation en considérant les états futurs potentiels qui pourraient découler de la situation actuelle.

- **Niveau 4** Évaluation de la performance : estimation et prédiction des mesures de performance du système en fonction des états désirés et des mesures d'efficacité. Ce dernier niveau interagit avec tous les autres niveaux.

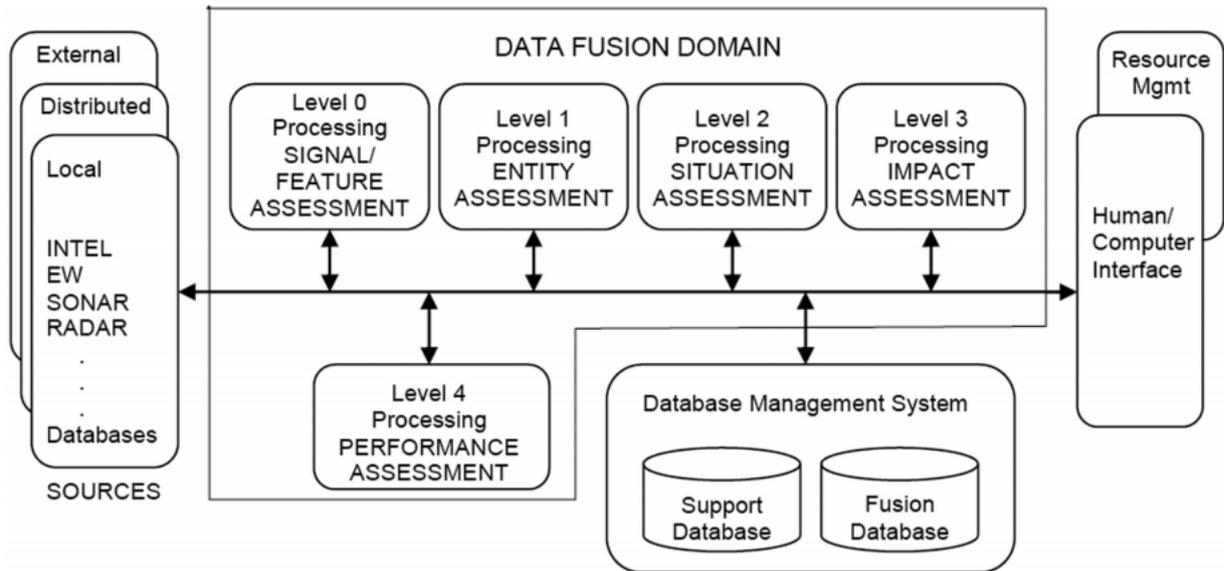


FIGURE 2.8 – Modèle JDL DF

Il est important de préciser que les niveaux de fusion ne sont pas nécessairement réalisés de façon séquentielle dans ce modèle. Comme le montre la Figure 2.8 les processus peuvent être réalisés en parallèle bien que généralement, il y ait besoin - du moins au début - de les réaliser dans l'ordre. Le processus est explicité dans la Table 2.1. Le Niveau 3 de l'évaluation de l'impact est dépendant de la modélisation du problème de SA dans le sens où les actions des entités suivent un objectif qui doit être défini dans le modèle, afin de comprendre l'utilité d'une action et de pouvoir projeter les futurs états des entités et des relations.

2.4.2 Exemple de modélisation de SA pour le C2

À titre d'exemple, la Figure 2.9 montre justement une modélisation de SA pour le C2 à travers le modèle JDL DF [Wallenius, 2004].

Comme dit précédemment, le SA permet dans un premier temps d'avoir un avantage stratégique certain sur les théâtres d'opération. En effet, les stratégies militaires en mesure de prendre et d'analyser la situation plus rapidement prennent le dessus sur leur adversaire en étant capables de mettre en place la contre-mesure adaptée [Roy et al., 2007]. [Wallenius, 2004] précise dans ses travaux un modèle complet de SA dans le contexte du C2 tel que :

Niveau d'évaluation	Association	Estimation	Résultat
N.0 - Signal	Capteurs → signaux	Extraction d'éléments	États des signaux/éléments estimés et la confiance associée
N.1 - Entités	Signaux → entités	Estimation des états attributifs des entités	États des entités estimés et la confiance associée
N.2 - Situations	Entité → entité, entité vers relation ou relation vers relation	Estimation des états relationnels	Estimation des relations (et groupe de relations) et la confiance associée
N.3 - Impact	Actions du système → leur utilité	Analyse coût/bénéfice des actions	Estimation / projection des états des entités et de la future utilité et confiance associée
N.4 - Performance	État du système → les buts et les estimations/projections	Analyses des performances	Estimations des mesures de performance, d'efficacité et de confiance

TABLEAU 2.1 – Schéma de partitionnement de Fusion d'Informations (adapté de [Steinberg and Bowman, 2004])

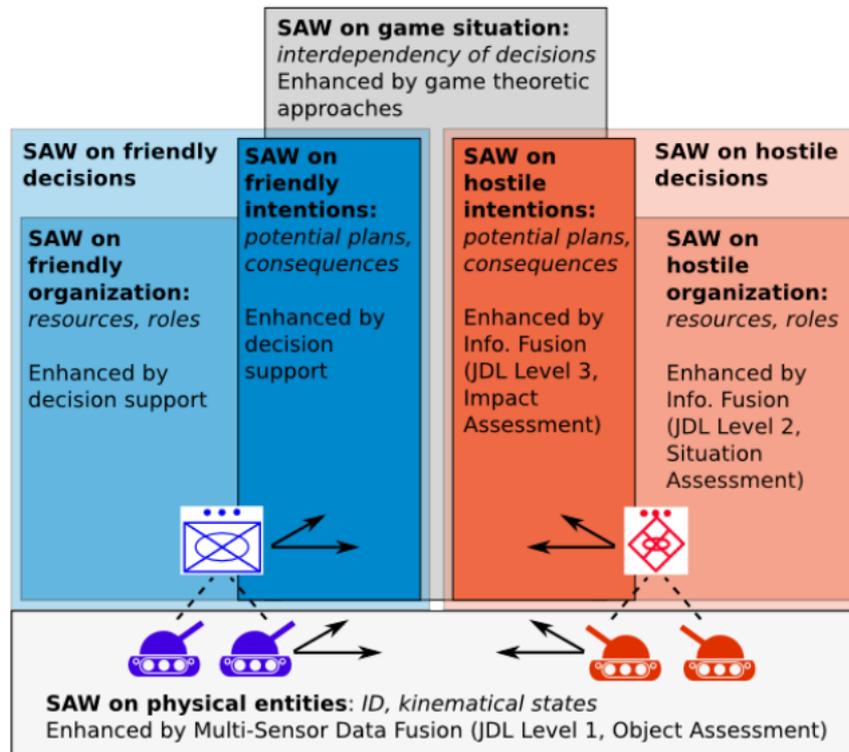


FIGURE 2.9 – Modèle de SA pour le C2 [Wallenius, 2004]

1. **SA pour les entités physiques** : comprenant la perception des entités physiques (véhicules, soldats, armes, capteurs, ...) et l'estimation de l'état de ces ressources.
2. **SA pour les décisions alliées** : cela englobe le SA à la fois sur les organisations alliées (compagnies, bataillons, régiments, ...) ainsi que le SA de leurs intentions (leur plan d'action de leurs ressources). Ces informations sont obtenues par le partage d'informations entre alliés.
3. **SA pour les décisions ennemies** : de même que pour les décisions alliées, cela comprend à la fois les organisations ennemies et leur plan d'action. Les organisations ennemies peuvent (dans le cas d'organisations militaires étatiques connues par les services de renseignement) être connues ou non (dans le cas de milices ou d'organisations terroristes), ce qui amène à plus d'incertitude que pour les alliés. Les informations sont obtenues grâce au ressources de captation d'informations.
4. **SA pour la théorie des jeux** : l'évaluation à la fois des alliés et des ennemis amène a une situation qui peut être décrite par la théorie des jeux notamment dans la compréhension des intentions des différents agents.

Cette description explicite le lien entre les modèles de fusion d'informations inhérents aux besoins des modèles de SA.

2.4.3 Révision du modèle JDL DF par DFIG

Une autre amélioration / révision du modèle JDL DF a été proposée par le DFIG [Blasch and Plano, 2003] [Blasch and Plano, 2005] présenté dans la Figure 2.10.

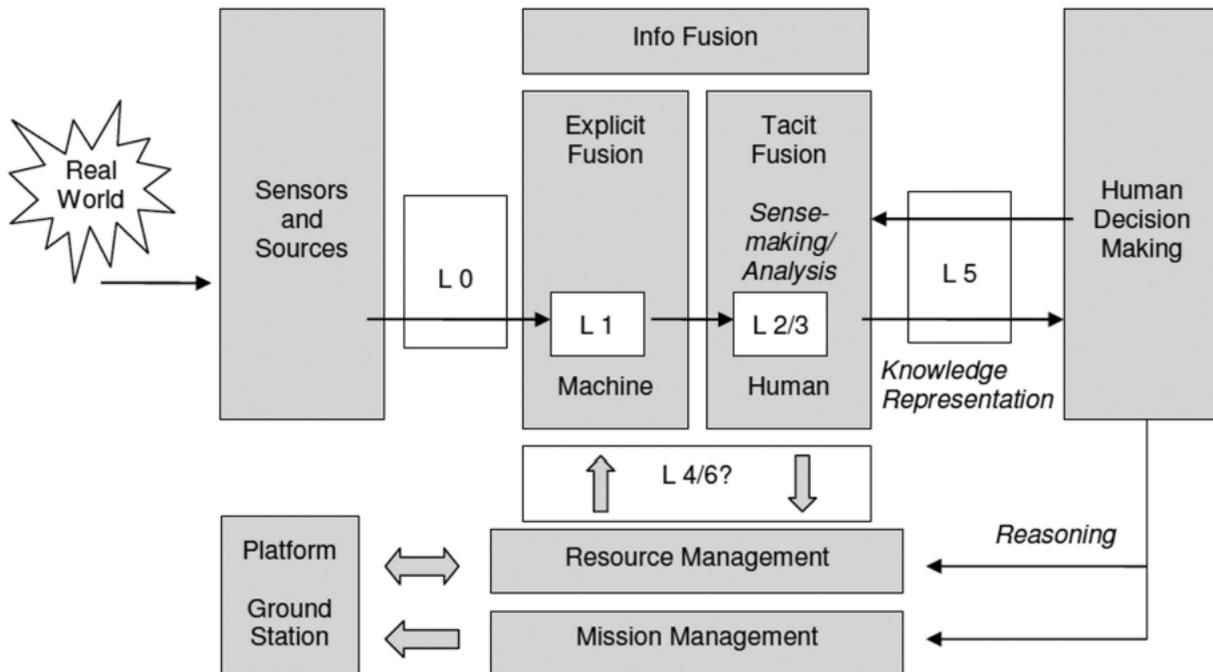


FIGURE 2.10 – Modèle JDL DF révisé

L'idée était de séparer la fusion d'informations de la gestion des fonctions. Une explication détaillée est présentée dans [Blasch, 2006] où trois fonctions de contrôle sont distinguées, les fonctions spatiales, temporelles et du spectre (*spectrum*).

Les besoins des fonctions du spectre sont basés sur le type de capteurs nécessaires pour obtenir une certaine information. Les fonctions temporelles correspondent au besoin de l'opérateur humain d'obtenir des informations suivant une ligne temporelle pour comprendre l'ordre des actions observées / projetées. Enfin, les besoins spatiaux sont reliés aux buts de la mission.

Ce modèle se découpe en 7 niveaux :

- **Niveau 0** Évaluation des données : estimation et prédiction des états observables des objets et signaux via les systèmes de collecte d'informations.
- **Niveau 1** Évaluation des objets : estimation et prédiction des états des entités grâce à l'association de données, ainsi que l'estimation des états discrets et continus de ces dernières (i.e. traitement des données).

- **Niveau 2** Évaluation de la situation : estimation et prédiction des relations entre entités afin d'inclure les structures de forces et de relations, communications, etc (i.e. traitement de l'information).
- **Niveau 3** Évaluation de l'impact : estimation et prédiction des effets de la situation analysée ou des actions estimées/projetées des entités (i.e. évaluer les actions de menace par rapport aux buts de la mission).
- **Niveau 4** Affinage par le processus : (gestion de ressources) adaptation de l'acquisition de la donnée et des supports de traitements (i.e. gestion de capteurs et dissémination de l'information).
- **Niveau 5** Affinage par l'utilisateur : (gestion de connaissances) adaptation à qui demande l'information et qui a accès à l'information et adaptation de la récupération des données et de leur affichage vers un support cognitif d'aide à la décision (i.e. interface homme-machine).
- **Niveau 6** Gestion de la mission : (gestion de plate-forme) adaptation des ressources de contrôle spatio-temporelles, de la planification de parcours/trajectoires et de la détermination des buts afin d'aider l'équipe de prise de décision avec des contraintes sociales, économiques et politiques (comme c'est nécessaire dans les théâtres d'opérations).

Il est intéressant de souligner que le Niveau 0 et le Niveau 1 différencient les états directement observables par des capteurs, et les états qui sont inférés par une analyse des données et donc qui ne sont pas directement observables. Cette distinction sera vue plus en détail dans la Section 2.6.

L'autre intérêt de cette amélioration du modèle se retrouve dans les trois derniers niveaux de fusion. Le Niveau 4 prend en considération le besoin d'optimiser et d'adapter les sources d'acquisition de l'information en fonction de ce qui est utile à observer à un moment donné. Ce concept sera lui aussi développé plus en détail dans la Section 2.6. Le Niveau 5 est sûrement l'un des plus intéressants car il met l'opérateur explicitement au cœur du système afin qu'il puisse corriger en temps réel les observations réalisées et les projections qui en découlent. Il est important de considérer cela, car les modèles d'aide à la décision restent imparfaits dûs à l'incertitude de l'information récupérée et traitée. Le fait de pouvoir corriger cela via un expert humain est un point primordial. Enfin, le Niveau 6 est un niveau qui permet de généraliser et globaliser l'approche en y apportant une couche de connaissances et de facteurs extérieurs à la situation pour la contextualiser dans des couches plus abstraites.

2.5 La Fusion d'Informations Haut-Niveau

De nombreux domaines s'intéressent à la Fusion d'Informations. Ces communautés trouvent leurs racines dans différentes applications comme dans le domaine médical, l'environnement, le contrôle du trafic aérien, le domaine de la sécurité et le domaine militaire pour ne citer que ceux-là.

Le point commun de toutes ces disciplines réside sur le fait qu'elles doivent modéliser des systèmes dynamiques en temps réel (ou quasi temps réel) avec un grand nombre de données qui doivent être synthétisées en une seule "image" opérationnelle afin de permettre une meilleure compréhension de ce qui se passe (i.e. l'évaluation de situation).

2.5.1 La Fusion d'Informations

La définition de la Fusion d'Informations est la suivante [Pek and Gee, 2013] :

Définition 4. La Fusion d'Informations et de Données (*Data and Information Fusion* noté DIF) comprend un processus de combinaison de données provenant de multiples sources (depuis une ou plusieurs sources telles que les capteurs ou les rapports textuels). Le but est d'obtenir une information plus riche (plus utile et pleine de sens) que ce qui peut être obtenu à partir de chaque source individuellement (autrement dit, sans fusion).

La DIF permet donc une meilleure compréhension des données en fusionnant les informations provenant de multiples sources et permet notamment :

- d'**améliorer la précision et la connaissance sur les informations** obtenues en réduisant notamment l'incertitude et l'ambiguïté entre les données.
- de **réduire le nombre global d'informations à traiter** en évitant les doublons et les informations récurrentes tout en complétant les données, les informations provenant de diverses sources concernant une même entité.
- une **meilleure compréhension de la situation** ce qui, dans le cas de l'évaluation de situations, améliore de façon substantielle le résultat du niveau 2 des modèles de SA (voir Section 2.3) et permet donc une meilleure prise de décision à terme.

La DIF comprend plusieurs étapes condensées en deux principales. La première est celle du calcul de la distance de similarité entre deux objets pour exprimer à quel point ces deux derniers sont similaires ou "dissimilaires"

(sachant qu'il existe la possibilité qu'on ne soit pas en mesure de décider). La seconde est celle de l'association de données qui demande une optimisation sur le choix des données et de comparer pour décider d'une fusion ou non. La première étape fournit le score permettant la réalisation de la seconde et ce sont deux problèmes bien distincts.

2.5.1.1 Les informations dites *Hard & Soft*

Le premier problème est de trouver un moyen de représenter des données très hétérogènes. Cela est dû à la grande variété des différents capteurs disponibles aujourd'hui pour extraire l'information. Les informations sont considérées comme étant de deux types ; dures (*Hard*) et douces (*Soft*) [Pravia et al., 2009].

Informations *Hard*

Les informations dites *Hard* représentent l'ensemble des informations collectées via des capteurs physiques (radar, caméra, micro, ...) qui permettent un traitement algorithmique et mathématique et procurent une information quantitative. La Fusion des informations *Hard* est généralement considérée comme maîtrisée et mature et les quelques articles dans la littérature qui continuent de parler du sujet sont généralement sur de l'optimisation computationnelle ou de fusion entre capteurs différents.

Informations *Soft*

Les informations dites *Soft* sont des informations de types linguistiques produites par des humains. Les sources peuvent aller des rapports d'experts ou d'observateurs humains à l'extraction d'informations sur les réseaux sociaux ou différents sites internet ou encore les traitements voix-texte (*speech-to-text*). Les informations *Soft* proposent une information qualitative complémentaire aux informations *Hard* en apportant une dimension sémantique à l'information. Bien que les informations *Hard* peuvent elles aussi apporter des informations de types relationnels, les informations *Soft* permettent de lier des entités à des évènements ou des intentions (comme renseigner si une personne est victime ou acteur d'une attaque).

La Fusion d'Informations *Soft* reste un problème très complexe et on trouve plusieurs solutions dans la littérature qui restent, souvent, perfectibles. Cela est souvent dû à une plus forte incertitude mais surtout à une incomplétude des données renseignées. De fait, la comparaison de deux objets avec des informations sur des attributs différents rend souvent le calcul de distance de similarité complexe et incertain.



FIGURE 2.11 – Principales différences et exemples d'informations *Hard & Soft*

D'autres exemples de données fournies par des capteurs d'origines *Hard* ou *Soft* sont présentés dans la Table 2.2. On remarque que beaucoup d'informations sont accessibles via les deux sources d'informations et cela montre assez logiquement l'intérêt d'être capable de compléter les informations de ces deux sources complémentaires.

2.5.2 La Fusion d'Informations Haut-Niveau

La littérature distingue deux niveaux de Fusion d'Informations ; le Bas-Niveau (*Low-Level Information Fusion*, noté LLIF) et le Haut-Niveau (*High-Level Information Fusion*, noté HLIF) qui ont été introduits par Waltz et Llinas [Waltz et al., 1990]. Les principales différences entre les deux niveaux sont représentées dans la Figure 2.12.

Le Bas-Niveau de Fusion d'Informations, aussi appelé fusion de données multi-capteurs, correspond aux niveaux 0 et 1 du modèle JDL DF (voir Section 2.4.3) et gère des données numériques sur les données des entités qui sont mesurables et prédictibles (position, tracking, identification, etc...). Selon [Foo and Ng, 2013], ce domaine est considéré depuis de nombreuses années comme étant mature et les recherches se portent maintenant essentiellement sur le domaine de fusion de données Haut-Niveau qui présentent encore de nombreux défis dont le plus important est sa dimension sémantique, son ambiguïté et son incertitude.

Le HLIF correspond quant à lui aux niveaux 2 à 4 du modèle JDL DF ; ... en se focalisant sur le raisonnement symbolique et en traitant à la fois des données physiques (comme celles du LLIF) et des données plus abstraites (comme l'intention, la menace, la stratégie, ...). Le traitement de ces données comporte de nombreuses difficultés. Premièrement, essayer d'estimer

Attribut	Description	Hard	Soft
Temps	Temps de la détection ou de l'occurrence de l'évènement	✓	✓
Position	Point géo-spatial où la détection ou l'occurrence de l'évènement se sont produites	✓	✓
Piste	Série temporelle de positions	✓	✓
Couleur	Spectre de lumière visible	✓	✓
Volume	Volume qu'occupe un objet	✓	✓
Type	Type de l'objet observé	✓	✓
Relation	Relation entre deux objets	✓	✓
Nom de l'entité	Nom d'une personne, groupes ou d'organisation		✓
Description	Description factuelle, biographique ou lié à un évènement		✓
Évaluation	Opinion ou estimation de la situation, menace...		✓

TABLEAU 2.2 – Exemple d'attributs observables par des capteurs *Hard* et/ou *Soft* (de [Pravia et al., 2009])

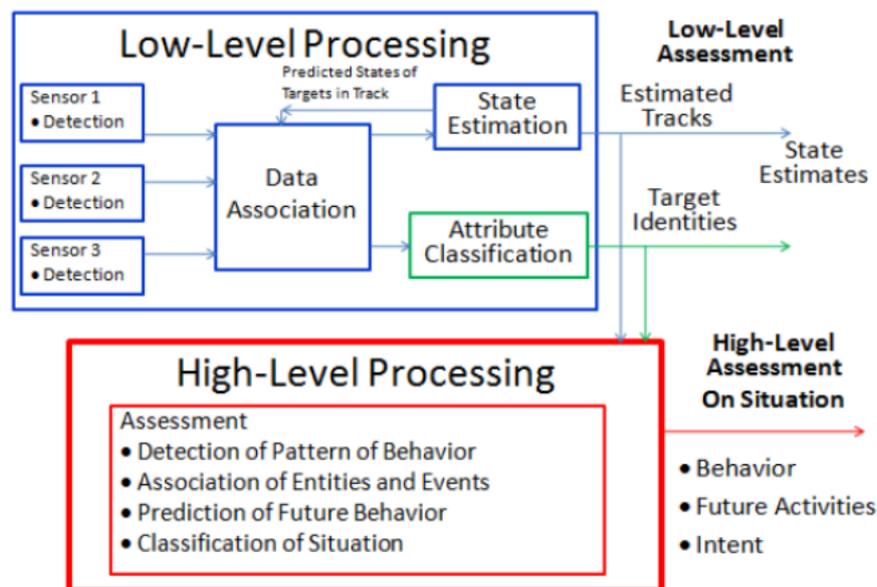


FIGURE 2.12 – Bas-Niveau et Haut-Niveau de fusion d'information (de [Blasch et al., 2012])

la stratégie d'un ennemi et quelle cible il décidera d'attaquer représente une grande complexité (voir Section 3.2.3.1) et les modèles existant pour définir le comportement ou le but d'un agent sont bien moins avancés que les modèles physiques permettant par exemple d'estimer la prochaine position d'un bateau [Steinberg, 2009].

On comprend donc que le HLIF va reposer sur des problématiques de fusion d'informations *Hard & Soft*. La fusion *Soft* "contamine" naturellement la fusion *Hard* par sa complexité et demande donc d'utiliser les procédés correspondant à cette dernière.

Différents outils ont été présentés dans les dix dernières années pour apporter des début de réponses à cette problématique. Le souci majeur dans ce domaine est de trouver comment réaliser une distance de similarité qui permettrait l'association de données connaissant la diversité et l'incomplétude des données collectées. Ce problème reste actuellement un grand défi scientifique à relever.

2.5.2.1 Des premières solutions pour la fusion d'information Haut-Niveau

Espace conceptuel

Un espace conceptuel (*Conceptual Space*, noté CS) [Dietze and Domingue, 2009] est une structure géométrique. Cette structure représente un nombre de dimensions qualitatives qui décrivent des caractéristiques avec lesquelles les objets et les concepts peuvent être comparés tels que le poids, la couleur, la température et les trois dimensions spatiales (x,y et z). Dans un CS les points représentent les objets et les régions les concepts.

Grâce à cela, on peut facilement imaginer une mesure de similarité entre deux objets via la distance entre deux points à travers ces différents espaces. Les objets proches les uns des autres font partie, par définition des espaces conceptuels, d'un même concept et donc, sont proches sémantiquement et devraient représenter le même objet.

Par exemple, la Figure 2.13 représente des fruits qui sont placés dans un CS de trois dimensions : teinte/couleur (*hue*), douceur (*sweetness*) et rondeur (*roundness*). Dans cette Figure, on peut facilement voir la similarité entre le concept d'une pomme et celui d'une Granny Smith - ce dernier représentant une sous-catégorie du premier. Mais on peut aussi voir qu'une pomme est plus proche d'une poire que d'une banane alors qu'en parallèle, il y a une forte distance entre une orange et un citron (bien qu'il soit tous les deux des agrumes). Cela démontre que le choix des dimensions dans les CS peut complètement changer les résultats de mesure de similarité.

Bien qu'élégante, cette solution nécessite un travail préparatoire important à partir de connaissances expertes pour produire correctement le CS afin

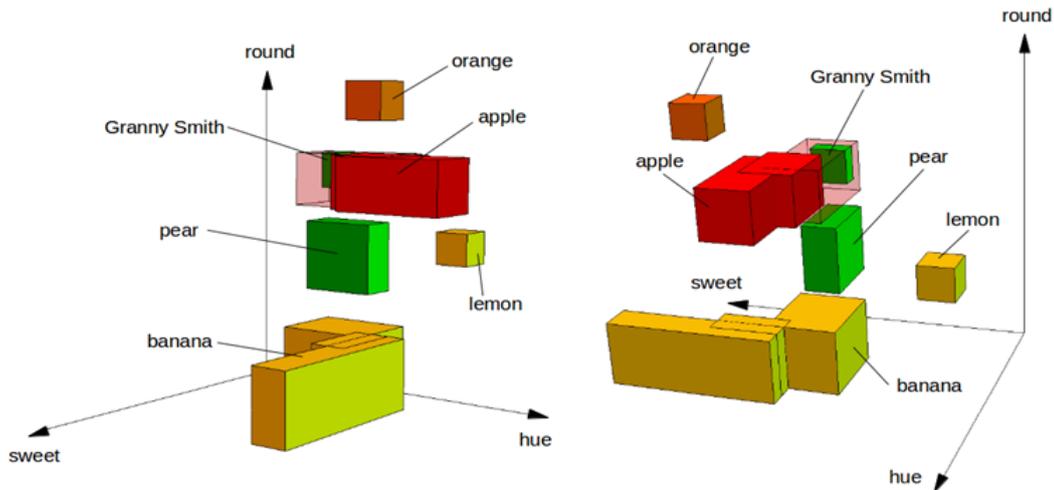


FIGURE 2.13 – Illustration d’espaces conceptuels pour des fruits (de [Dietze and Domingue, 2009])

qu’il produise une mesure de similarité cohérente pour permettre à terme une bonne fusion.

L’autre grande limite d’une telle solution est que les CS permettent de gérer des informations linéaires (continues ou discrètes) mais pas des informations telles qu’un nom que l’on ne peut pas représenter dans une dimension linéaire et donc ne peuvent pas être gérés via un tel outil.

Fusion à partir d’une structure de réseaux

Le projet *Multi-disciplinary University Research Initiative* (MURI) titré *Unified Research on Network-based Hard & Soft Information Fusion* a développé un framework de recherche intégrant des composants de Fusion d’Informations Haut-Niveau (*Hard & Soft*) [Gross et al., 2014].

La Figure 2.14 décrit ce système à travers lequel des données brutes *Hard & Soft* sont traitées ; dans un premier temps à travers des algorithmes de fusion de capteurs physiques (*hard*) et en parallèle dans des processus de Traitement Automatique des Langues (*Soft*). S’ensuivent des processus de référencement, d’alignement et d’association d’entités entre les deux sources d’informations pour être envoyés à un processus de SA.

La fonction de mesure de similarité propose une distance qui est positive lorsque deux entités sont similaires et négatives lorsqu’elles sont dissimilaires. Cependant, ce système ne définit nulle part cette fonction de calcul de similarité et semble être réalisée sur des données simulées pour permettre d’appliquer leurs algorithmes de fusion d’informations. Donc cet outil ne répond qu’à la deuxième moitié de la question : l’association de données.

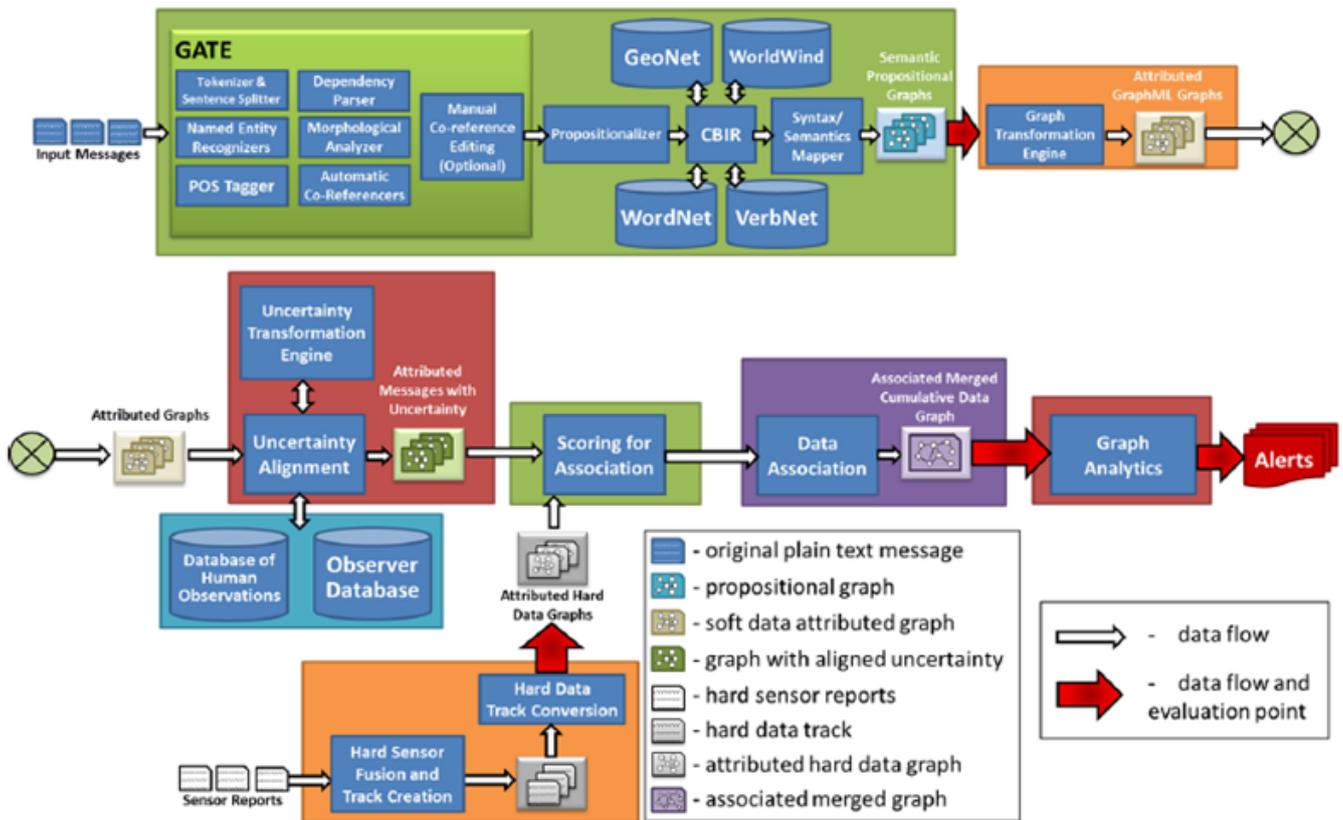


FIGURE 2.14 – Framework de fusion d’information du projet MURI (de [Dietze and Domingue, 2009])

Distance de similarité sémantique agrégée

Dans les travaux d'A. Bellenger [Bellenger, 2013], une première distance sémantique a été proposée en travaillant sur les ontologies qui permettent de facilement travailler avec des données hétérogènes (*Hard & Soft*) et incomplètes (voir Chapitre 3 Section 3.1.5).

La mesure retourne une valeur entre 0 et 1 où plus le score est proche de 1 plus les deux objets comparés sont similaires. Pour calculer ce score de similarité, les travaux d'A. Bellenger combinent plusieurs facteurs depuis la terminologie de l'ontologie en une seule valeur. La similarité entre deux objets est notée $sim(I_j, I_k)$ où I_j et I_k sont deux objets instanciés de l'ontologie. La fonction de similarité prend en compte la comparaison structurelle des deux instances (relatif à la terminologie a priori de l'ontologie), mais aussi la comparaison entre les attributs en commun entre les deux instances et les valeurs instanciées de ces attributs (propriétés ou relations). La Figure 2.15 servira d'exemple d'ontologie pour illustrer les différentes formules.

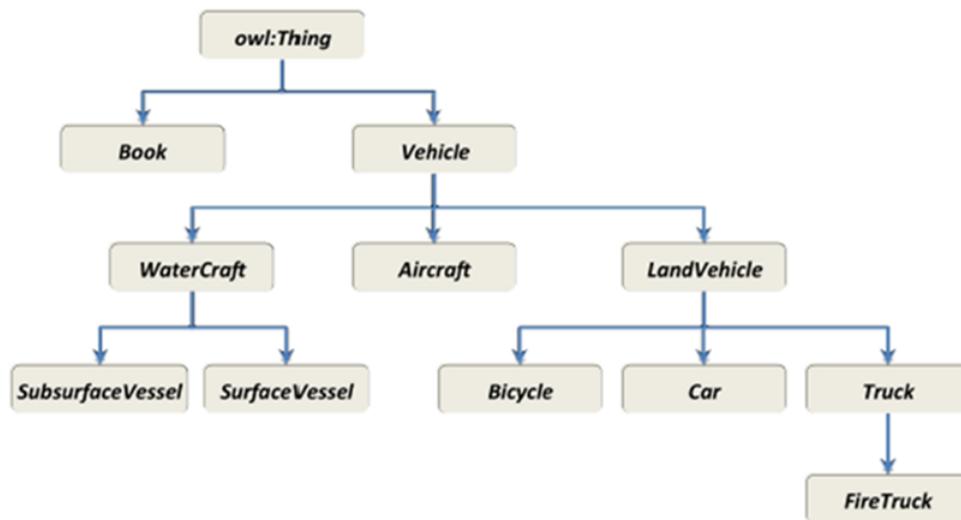


FIGURE 2.15 – Exemple d'ontologie (de [Bellenger, 2013])

La première distance concerne donc la position des classes des deux objets instanciés dans l'ontologie. Du fait de la structure d'une ontologie, le concept de hiérarchie de classe peut être vu comme le calcul dans un graphe de la distance entre deux nœuds. Cette première distance correspond donc au plus court chemin entre deux concepts de la taxonomie (soit le nombre d'arcs du graphe à traverser entre les deux nœuds). Cela correspond à pouvoir dire que la classe *Car* et la classe *LandVehicule* par exemple se ressemblent plus que *Car* et *Aircraft*. L'Équation 2.1 décrit cette formule avec C_j la classe de l'objet instancié I_j , $depth_C(C_j)$ la profondeur de la classe C_j dans l'ontologie et de même pour C_k pour I_k . Enfin, $depth(C)$ représente la plus grande

profondeur commune entre les classes C_j et C_k (dans notre exemple entre *Aircraft* et *Car*, la classe commune la plus profonde est *Vehicule*).

$$sim_{Taxonomy}(I_j, I_k) = \frac{2 \cdot depth(C)}{depth_C(C_j) + depth_C(C_k)} \quad (2.1)$$

La seconde distance compare le nombre d'attributs communs entre les deux classes, nombre normalisé via le nombre total d'attributs de chaque classe. La terminologie d'une ontologie n'est pas uniquement déterminée par sa structure hiérarchique mais aussi par le type des propriétés, leur domaine et leur intervalle de valeurs. L'Équation 2.2 permet de prendre en compte ce facteur dans la distance de similarité. Par exemple, les classes *Car* et *Truck* partagent l'attribut *HasNumberOfDriveWheels* que ne partage pas la classe *Bicycle* ce qui amène les deux premières classe à avoir une proximité sémantique un peu plus forte qu'avec *Bicycle*. La notation $ObjectPropDomain(C_j)$ représente l'ensemble des propriétés de la classe C_j (qui est la classe de l'objet instancié I_j) et de même pour C_k et I_k . La notation $|ObjectPropDomain(C_j)|$ représente la cardinalité de l'ensemble de propriétés et donc $|ObjectPropDomain(C_j) \cap ObjectPropDomain(C_k)|$ correspond au nombre de propriétés communes entre la classe C_j et C_k .

$$sim_{ObjectPropDomain}(I_j, I_k) = \frac{2 \cdot |ObjectPropDomain(C_j) \cap ObjectPropDomain(C_k)|}{|ObjectPropDomain(C_j)| + |ObjectPropDomain(C_k)|} \quad (2.2)$$

Enfin, la troisième formule compare elle aussi les propriétés (attributs ou relations) des deux classes mais cette fois-ci, la comparaison concerne les valeurs que prennent ces propriétés pour les objets instanciés I_j et I_k . Cette formule compte le nombre de propriétés identiques entre les deux objets instanciés par rapport au nombre total de propriétés communes. Par exemple, un objet de classe *Car* comparé à un *Truck* partageant comme propriété *mainColor = red* sera plus proche qu'un autre objet *Car* avec *mainColor = blue*. La notation $|ObjectProp(I_j) \cap ObjectProp(I_k)|$ correspond ici au nombre de propriétés communes ayant la même valeur entre l'objet I_j et I_k .

$$sim_{ObjectProp}(I_j, I_k) = \frac{2 \cdot |ObjectProp(I_j) \cap ObjectProp(I_k)|}{|ObjectProp(I_j)| + |ObjectProp(I_k)|} \quad (2.3)$$

La formule agrégée de cette distance de similarité est ensuite calculée telle que (achant que $\sum_i w_i = 1$) :

$$sim(I_j, I_k) = \begin{cases} w_1 \cdot sim_{Taxonomy}(I_j, I_k) \\ + w_2 \cdot sim_{ObjectPropDomain}(I_j, I_k) \\ + w_3 \cdot sim_{ObjectProp}(I_j, I_k) \end{cases} \quad (2.4)$$

Cette solution, bien que l'une des meilleures existantes, est trop rigide et empêche une corrélation réaliste et cohérente entre les informations collectées. De plus, elle ne prend pas en compte la dimension dynamique et temporelle de l'évolution des attributs dans le temps.

Modèles d'évolution

Des travaux ont été réalisés en parallèle de cette thèse sur une amélioration de la distance sémantique présentée précédemment avec l'apport des modèles d'évolution (*Models of Evolution*) [Vasnier et al., 2019]. L'idée est de modifier la 3^{ème} distance de similarité sémantique agrégée pour prendre en compte l'incertitude liée à l'évolution temporelle de chaque attribut (entre 2 observations).

Le deuxième point concerne l'apport de l'incertitude portée par les capteurs ayant récupéré l'information sur chaque attribut. Ces deux premières contributions ont été démontrées à travers différents modèles et formules et ajoutées dans le méta-modèle de l'ontologie.

Le dernier apport est d'avoir normalisé les distances telles que $\delta = [-1, 1]$ avec un score de -1 correspondant à une dissimilarité certaine, 1 une similarité certaine et 0 une incertitude totale. Cette normalisation permet de faciliter les travaux sur l'association de données et de mieux gérer la notion d'incertitude.

Le brevet étant en court de validation, il n'est pour le moment pas possible d'en parler plus.

2.6 La Perception Active

Les environnements dans le domaine du SA sont de plus en plus complexes à observer et la quantité d'informations à obtenir est souvent trop grande pour permettre de couvrir l'ensemble des objets. Dans les problématiques d'évaluation de situations, et notamment dans la gestion de crise, le nombre de ressources d'acquisition d'information est limité et le besoin de comprendre la situation rapidement est une contrainte forte. Il est donc nécessaire de trouver un moyen de comprendre comment optimiser l'observation de l'environnement pour utiliser au mieux ces ressources afin de maximiser le gain d'informations sur la situation.

2.6.1 Les problématiques de la Perception Active

La perception active a été définie par Bajcsy telle que [Bajcsy, 1988] :

Définition 5. Le problème d'optimisation des stratégies appliquées au processus d'acquisition des données, qui dépendent de l'état actuel de l'interprétation des données et de l'objectif ou de la tâche du processus.

Il est donc question de comprendre et trouver comment optimiser l'acquisition d'information sur la situation actuelle en prenant en compte ce qui est déjà connu afin d'optimiser la connaissance sur la situation lors de la prochaine itération d'observation. L'adjectif "actif" signifie qu'il y a une recherche d'optimisation dans l'utilisation de l'agent (capteur) et non dans ce qu'il représente en tant que tel.

Cela fait de la perception active un problème complexe car il est très dépendant des critères multi-objectifs par rapport au gain d'informations ou encore au coût des actions ou de l'acquisition des informations. De plus, une autre difficulté est celle de l'incertitude liée à la fois par l'imprécision de chaque agent dans leur prise d'information ainsi que par rapport au fait que l'environnement soit partiellement observable. Ces notions d'incertitude sont développées plus en détail dans le Chapitre 3 Section 3.2.1.

La perception active propose de nombreux challenges [Mihaylova et al., 2002] :

1. Les modèles des agents et des capteurs ne sont pas linéaires, et quand bien même certains peuvent être linéarisés, tous les problèmes ne peuvent pas être gérés de cette façon.
2. La solution d'une tâche dépend d'un critère optimal qui est une fonction multi-objectifs pondérant le gain d'information en fonction de l'utilité et des coûts. Les fonctions d'optimisation multi-objectifs amènent en général à une explosion de complexité en terme de temps et du nombre de calculs.
3. Il faut prendre en compte l'incertitude due au modèle des agents, de l'environnement et des capteurs.
4. Le système est (presque) systématiquement partiellement observable, donc les capteurs ne donnent des informations que sur certaines variables mais pas toutes.

De plus, l'hétérogénéité des capteurs (ici nos agents) pour récupérer l'information peut les rendre complémentaires ou augmente la complexité de l'optimisation de leur utilisation.

2.6.2 La perception active dans les systèmes multi-agents

La perception active, d'un point de vue multi-agents, a été étudiée dans différents cas de figures dont principalement :

- l'exploration de carte : l'environnement topologique est inconnu et les agents doivent l'explorer pour construire la carte.
- le cas antagoniste : les agents sont confrontés à des ennemis et connaissent l'environnement topologique. Ce qui est exploré ici est le comportement des ennemis pour comprendre les événements qui se déroulent. On peut comprendre ici la stratégie de l'ennemi grâce à l'exploration des événements observés.

Dans cette thèse, nous nous intéressons essentiellement au deuxième cas, le cas antagoniste. Dans un cas d'évaluation de situation sur un champ de bataille, on peut considérer les capteurs d'acquisition d'informations (radar, drone, observateur humain) comme des agents et donc, la perception active revient à une problématique d'optimisation de ces agents pour observer l'environnement et chercher à maximiser le gain d'information.

D'autres modèles ont été présentés comme celui de Weyns qui propose un modèle de perception active pour des applications multi-agents (représenté dans la Figure 2.16). Ce modèle divise la perception active en trois étapes :

La perception (*sensing*) :

La perception permet la représentation de l'état de l'environnement. Cette perception suit la représentation d'ensemble de symboles structurés qui réfèrent à des objets présents dans l'environnement. La représentation des états dépend de deux facteurs. Le premier est le choix de l'agent sur un ensemble de **focus**. Chacun de ces focus possède une sensibilité différente ainsi que d'autres paramètres telle que la capacité de l'agent d'acquérir de l'information sur ce focus. C'est en définitive ce qui permet de prioriser le choix d'observer une information par rapport à une autre. Par exemple, un agent peut être en mesure d'obtenir des informations visuelles, tandis qu'un autre, des informations olfactives.

Le second facteur se caractérise par un ensemble de **lois perceptuelles**. Ces lois correspondent aux contraintes de perceptions par rapport à comment sont modélisés les objets en termes de représentation. Par exemple, cela peut correspondre à l'ajout de bruit si un certain agent observe un objet dans certaines conditions, ou encore définir ce qui peut être hors d'atteinte d'un agent en terme d'observation car derrière un mur.

L'interprétation (*interpating*) :

L'interprétation correspond à une représentation d'une image mentale. Afin d'interpréter une représentation, un agent utilise une description. Ces

images mentales sont structurées de sorte à ce que les agents arrivent à comprendre ce que représentent les objets à un plus haut niveau (comme les relations entre ces objets). C'est ce qui permet par exemple de considérer des objets différents comme un groupe d'objets agissant de la même façon (tel un cluster).

le filtrage (*filtering*) :

Le filtrage se base sur un critère de sélection qui permet aux agents de choisir quelles informations ils vont vouloir observer. Par exemple, un agent qui veut se focaliser sur des informations visuelles et ne veut s'intéresser qu'aux objets qui se trouvent dans son champ de vision, le filtre permettra de respecter ces contraintes afin qu'il ne se concentre que sur les objets dans son entourage.

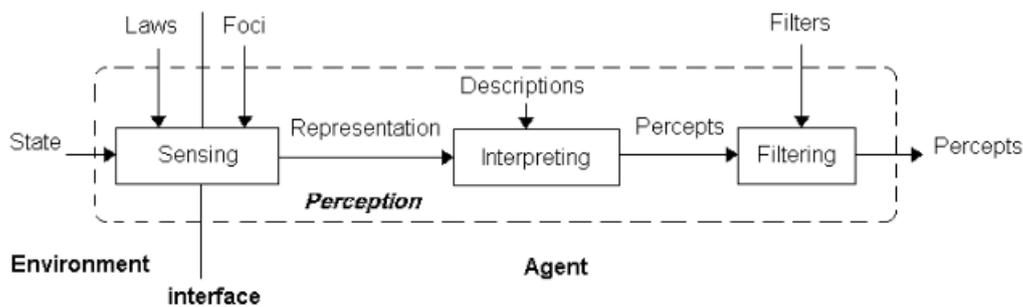


FIGURE 2.16 – Modèle de perception active (de [Weyns et al., 2004])

D'autres modèles ont vu le jour suivant ces concepts avec des représentations se basant sur les réseaux bayésien dynamiques pour générer un ensemble de règles et contraintes sur les capacités d'observation des agents [Zhang and Ji, 2006].

Cependant, les modèles utilisant ce genre d'approche restent actuellement trop simplistes et nécessitent d'être améliorés pour réussir à représenter des scénarios complexes et suffisamment proches de la réalité. De plus, les modèles existants se basent sur des problématiques de fusion d'information Bas-Niveau (voir Section 2.5.2) et ne prennent donc pas en compte toutes les informations disponibles dans la plupart des cas d'utilisation.

2.7 Conclusion

Ce chapitre nous a permis de :

- Définir ce qu'est l'évaluation de situations (SA), ses origines, ses problématiques
- Introduire le concept des cycles du renseignement et le cycle OODA et ses améliorations
- Décrire et présenter le modèle d'Ensley qui a servi de base à tous les modèles suivants de SA
- Définir les différents types d'informations (*Hard & Soft*) et leur complémentarité
- Présenter le domaine de la fusion d'informations dites Haut-Niveau qui expose un problème majeur sur comment représenter une information hétérogène et incomplète mais aussi comment décider d'une association
- Présenter quelques outils actuels apportant une première réponse sur le calcul de distance de similarité et d'association de données.
- Parler du concept de perception active qui est nécessaire dans le cas de l'évaluation de situation du fait du nombre de ressources limitées pour obtenir des informations dans un environnement partiellement observable.

L'évaluation de situations amène à des problèmes complexes de représentations de l'information afin de réaliser la mission d'évaluation. L'hétérogénéité de ces informations et leur volume important impose de réfléchir à la façon de représenter cette connaissance sur l'environnement. La question qui se pose est comment représenter une information provenant de sources aussi différentes de façon unifiée ? De plus, l'incomplétude, la concurrence des informations, ainsi que le potentiel manquant de précision sur l'acquisition des ces informations amènent à devoir traiter le problème de l'incertitude sur les données récupérées.

Pour cela, nous allons présenter dans le chapitre suivant une veille sur les problèmes de représentation de la connaissance et la gestion de l'incertitude sur cette dernière.

CHAPITRE 3

La représentation de la connaissance

Les systèmes de SA sont très dépendants des domaines et des cas d'usages dans lesquels ils sont utilisés du fait que chaque situation nécessite la compréhension d'informations différentes pour aider un opérateur à décider de la stratégie à mettre en place. Un pilote d'avion n'a pas besoin de connaître et d'estimer les mêmes choses qu'un officier de l'armée de terre. Cependant, le concept reste commun à chacun des domaines ce qui a permis de mettre en place une méthodologie globale.

Cette dimension *ad-hoc* des domaines et même des problématiques du SA pose la question de comment réussir à représenter les connaissances expertes permettant de comprendre une situation. Le but étant d'automatiser les processus d'aide à la décision, cette question est cruciale pour permettre à un système de comprendre et d'analyser les informations qu'il reçoit. Tout comme réussir à les représenter à un opérateur humain afin de faciliter sa compréhension et sa prise de décision.

Il existe divers outils pour représenter la connaissance tels que les réseaux sémantiques [Sowa, 2014], les cadres (*frames*) [Minsky, 1974], les systèmes à base de règles ou encore les ontologies [Guarino, 1995] comme nous le verrons dans ce chapitre. Ces différentes représentations de la connaissance ont servi dans un premier temps à des systèmes de raisonnement automatique tels que les systèmes d'inférence, les démonstrateurs automatiques de théorèmes et les classificateurs. Mais ils ont vite été adaptés pour répondre aux problématiques de SA présentées dans le chapitre précédent.

1. Image provenant de <http://www.lisperati.com/tellstuff/>

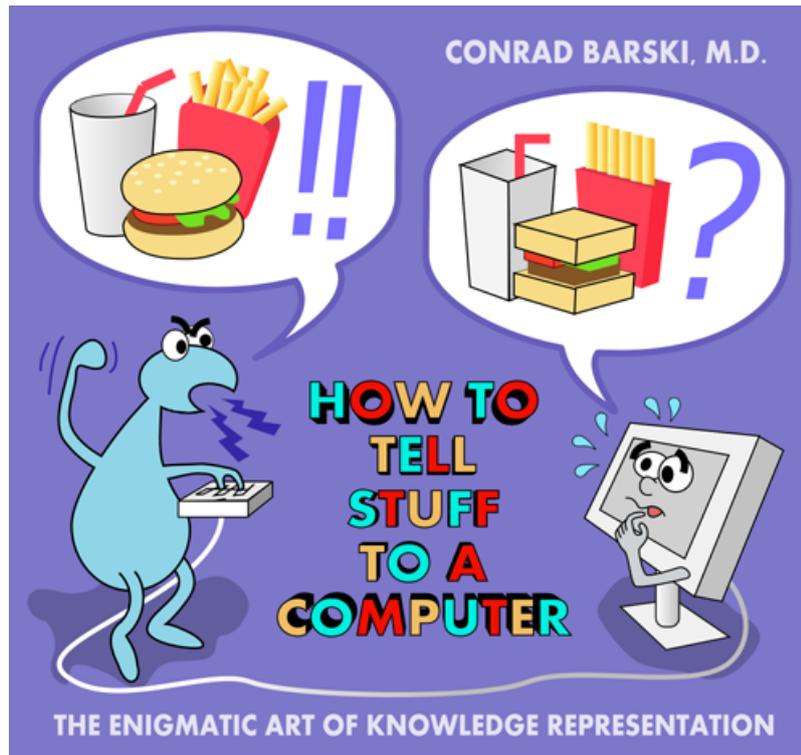


FIGURE 3.1 – Comment rendre compréhensible la connaissance pour un ordinateur ?¹

3.1 Qu'est-ce que la représentation de connaissances ?

La représentation de la connaissance (*Knowledge Representation* notée KR) est un domaine de recherche intrinsèquement lié à celui du SA. Le but étant de pouvoir formaliser l'évaluation de situations afin d'en automatiser au mieux le processus, il faut donc pouvoir représenter les informations de sorte à ce qu'un système informatique puisse les comprendre et les utiliser pour fournir des analyses et des diagnostics.

3.1.1 La représentation de connaissances

Ce domaine prend ses racines dans la psychologie où des travaux ont décrit comment l'homme cherche à solutionner des problèmes et comment il représente l'information et la connaissance [Schank and Abelson, 2013]. Un tel formalisme a pour but de permettre le développement de système pour raisonner à partir de règles logiques ou sémantiques afin de pouvoir tirer des conclusions ou trouver des solutions.

La représentation de connaissances a été définie la première fois par [Smith, 1985] comme :

Définition 6. Tout processus intelligent mécaniquement intégré est composé

d'ingrédients structurels que : a) nous, observateurs externes, prenons naturellement pour représenter un compte propositionnel de la connaissance que le processus global présente, et b) indépendamment de cette attribution sémantique externe, jouent un rôle formel mais essentiel pour engendrer le comportement qui manifeste cette connaissance.

Plus tard, [Davis et al., 1993] explicite cinq rôles majeurs du KR :

- La représentation de connaissances est fondamentalement un **substitut de l'action**, utilisé pour permettre à une entité de déterminer les conséquences en pensant plutôt qu'en agissant.
- C'est un ensemble d'engagements ontologiques, c'est-à-dire une réponse à la question : en quels termes devrais-je penser le monde ? Sur quoi dois-je me concentrer pour réfléchir et penser le monde ?
- C'est une théorie fragmentée du raisonnement intelligent, exprimée en 3 composants : (1) la conception fondamentale de la représentation de la déduction intelligente, (2) l'ensemble des inférences que la représentation pénalise, (3) l'ensemble des inférences qu'elle recommande.
- C'est un support pour un calcul pragmatique et efficace grâce à la façon dont la représentation de connaissances permet d'organiser l'information et de ne considérer que ce qui est important pour l'inférence.
- C'est un support pour l'expression humaine, c'est à dire un langage qui permet de dire à la machine comment nous percevons le monde.

3.1.2 Le triangle sémiotique

On comprend que la représentation de connaissances a pour but de rendre la connaissance la plus explicite possible. En effet, les connaissances sont des informations implicites [García González et al., 2005], c'est à dire des informations obtenues par un agent via des observations de son environnement selon sa propre représentation et ses propres croyances.

Le concept du triangle sémiotique permet de mieux comprendre la distinction entre informations explicites et implicites. Le triangle sémiotique a été formalisé par [Bestman, 1995] and [Sølvberg, 1999] (voir Figure 3.2).

Tout part d'un objet que l'on appelle ici référent. Le référent est un objet qui existe par lui-même. Par exemple le référent peut être un tank observé par une compagnie de reconnaissance. Ces observateurs ont naturellement conceptualisé d'une certaine manière ce référent, ici le tank. Mais le besoin de partager l'information nécessite que le référent soit représenté par des symboles (ici "tank") afin que lorsque des agents communiquent, l'observateur

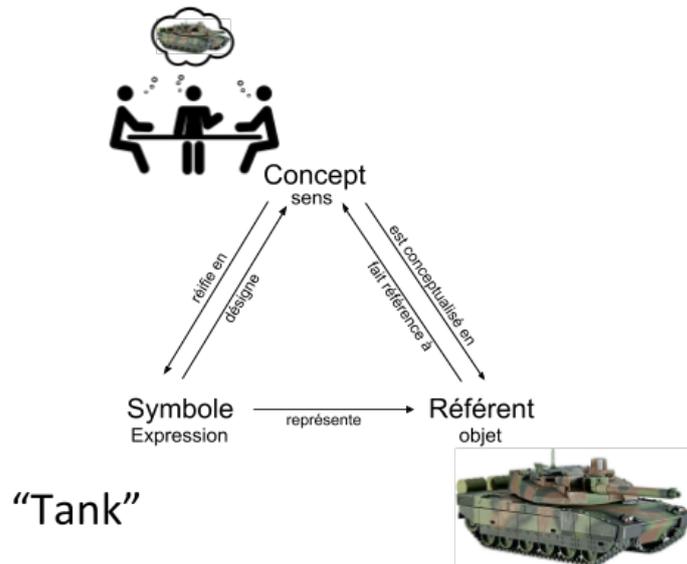


FIGURE 3.2 – Le triangle sémiotique (adapté de [Bellenger, 2013])

puisse être en mesure d’expliquer ce qu’il a vu par un vocabulaire commun à l’agent avec lequel il partage ce qu’il a vu.

La représentation de connaissances est donc ce qui permet de représenter symboliquement un objet qui existe afin de pouvoir partager l’information de sorte que tout le monde soit en mesure de comprendre quel est cet objet.

3.1.3 Données, informations et connaissances

La différenciation entre les données, les informations et les connaissances a été développée dans plusieurs travaux ([Aamodt and Nygård, 1995] [Bellenger et al., 2004] [Boisot and Canals, 2004]). La Figure 3.3 représente la pyramide de la connaissance (*Knowledge Pyramid* ou encore *Knowledge/Information Hierarchy*). Plus un concept est haut dans le graphe, plus il contient de sens et nécessite plus de mécaniques de raisonnement et de compréhension.

Dans [Dretske, 1981], l’auteur propose une définition qui éclaire cette problématique :

Définition 7. L’information est le produit permettant de produire de la connaissance et de dire quelles sont les informations qu’un signal transporte et ce que nous pouvons en apprendre. La connaissance est identifiée avec la croyance produite via l’information, mais l’information qu’une personne reçoit est relative à ce qu’elle sait déjà à propos des possibilités de la source.

Pour résumer et appliquer cela à l’évaluation de situations, la donnée correspond aux signaux bruts observés sans traitement autre que leur stockage. Les informations elles correspondent à la structuration et l’agrégation des

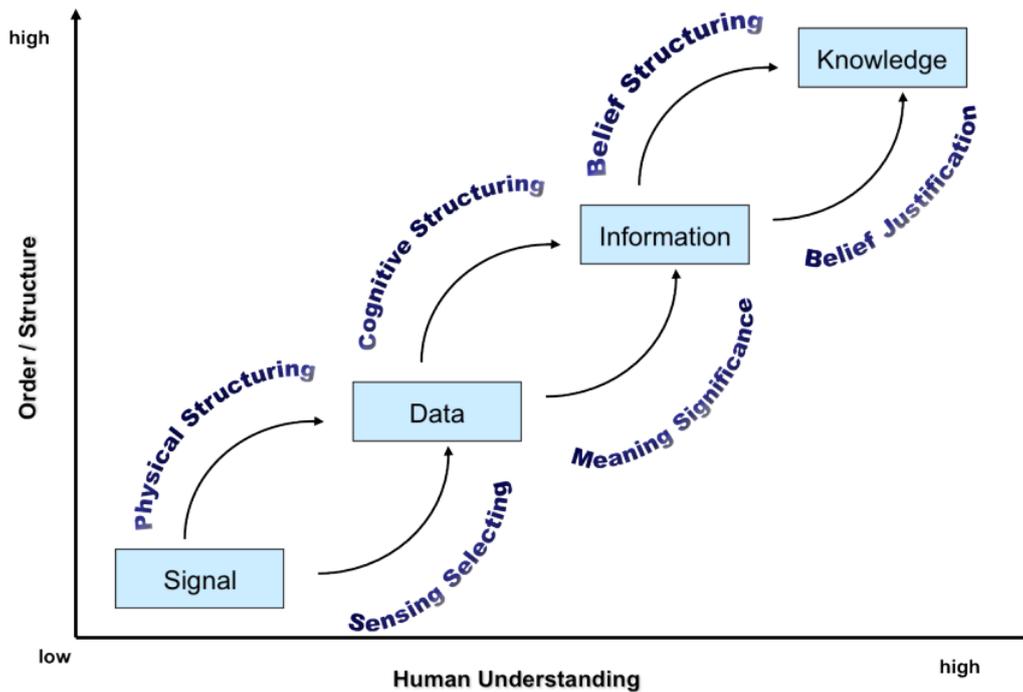


FIGURE 3.3 – Hiérarchie des Données-Informations-Connaissances (de [Bellenger, 2013])

données pour comprendre des patterns ou des relations entre les données et l'état des entités observées. Enfin les connaissances sont le système de croyances qui permet d'inférer l'état complexe des entités et le but qu'elles cherchent à atteindre. Ceci se fait en prenant en compte le contexte de ces entités dans leur environnement et leurs relations entre elles afin de permettre un processus de décision.

3.1.4 Premières applications

Comme le présente J. Renoux dans sa thèse [Renoux, 2015], les premières applications du KR ont été développées dans le domaine de la logique propositionnelle. Cette logique permet de manipuler des atomes (le vocabulaire de la logique) et des formules composées d'atomes et d'opérateurs. L'avantage de la logique est que l'on peut représenter des concepts via les formules où les réponses sont "*vrai*" ou "*faux*". S'en est suivie la logique des prédicats avec les quantifieurs (\forall "pour tout" et \exists "il existe"), la logique modale avec les opérateurs tels que \diamond "il est possible" et \square "il est nécessaire" et la logique épistémique ajoutant les opérateurs B "je crois que" et K "je sais que".

D'autres outils théoriques sont arrivés par la suite pour représenter la connaissance et permettent même l'inférence et la révision de croyances telles que les réseaux bayésiens (comme développés dans la suite du chapitre).

3.1.5 Les ontologies

De nombreux systèmes ont émergé pour représenter l'information dans l'Intelligence Artificielle (IA). Pour n'en citer que certains, les réseaux sémantiques (*semantic nets*), les systèmes à base de règles ou encore les ontologies.

Dans le cas de l'évaluation de situations, le modèle qui a le plus retenu l'attention est celui de l'ontologie. Celle-ci a la capacité de représenter n'importe quel type d'informations (informations *Hard & Soft*, Section 2.5.1.1). Peu importe sa provenance, sa qualité ou sa complétude, les ontologies permettent de représenter la connaissance et de raisonner à partir de ce modèle.

Initialement, le terme d'ontologie est apparu dans le domaine de la philosophie, plus spécifiquement, celui de la métaphysique qui cherche à définir la nature de la réalité. Les ontologies tentent donc d'expliquer ce qui existe dans le monde et comment les objets qui composent le monde sont organisés les uns par rapport aux autres.

En Intelligence Artificielle, la définition retenue a été celle décrite par Borst [Borst, 1999] étant une définition affinée de Gruber [Gruber, 1993] :

Définition 8. Une ontologie est une spécification formelle et explicite d'une conceptualisation partagée.

Cette définition met en avant deux concepts importants. Le premier est celui de la *conceptualisation* qui correspond à ce que l'ontologie essaie de représenter. Dans la Figure 3.4 (adapté de la Figure 3.2), cela correspond à ce que le concept représente philosophiquement. La *conceptualisation* est composée de concepts identifiés, d'objets et de toutes les entités existants dans le monde que l'on tente de décrire ainsi que leurs relations. Le second concept est celui de la *spécification* (correspondant au symbole dans la Figure 3.4) qui représente une définition non-ambigüe des différents concepts et de leurs relations. C'est à la fois une définition admise de tous à travers un consensus d'experts travaillant sur la problématique (*partagée*), mais aussi une définition compréhensible d'un point de vue informatique (*explicite*) et respectant un ensemble de règles sur la représentation de la connaissance (*formelle*).

À titre d'exemple, la Figure 3.5 montre un exemple d'ontologie militaire décrivant la hiérarchie des classes dans le domaine de l'information [Yoo et al., 2014]. On peut voir le concept de dépendance de classes avec par exemple le "type d'ennemi" (*type of Enemy*) qui comprend trois sous-classes "forces terrestres" (*ELF*), "forces navales" (*ENF*) et "forces aériennes" (*EAFF*) et dans les entités de type *ELF* on retrouve les armes employées (*Weapon of ELF*), les types de troupes dans l'organisation de l'armée (*Type of ELF*) avec des informations telles que les types de troupes, de divisions ou de compagnies qui composent les forces ennemies terrestres.

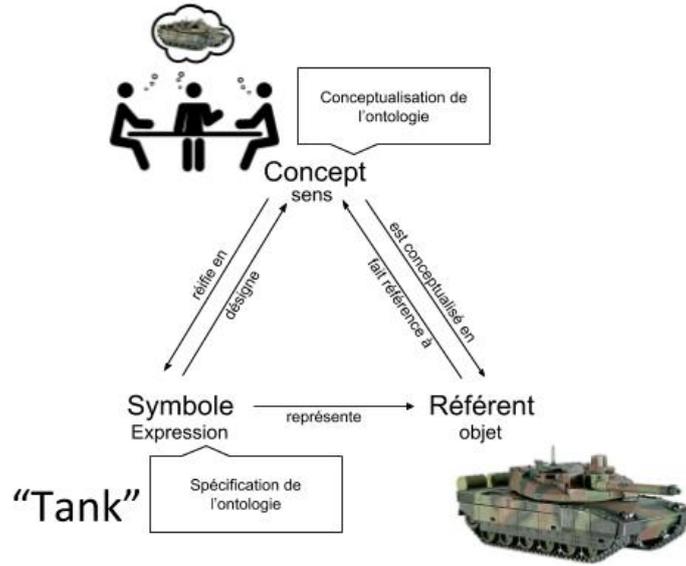


FIGURE 3.4 – Le triangle sémiotique (adapté de [Bellenger, 2013])

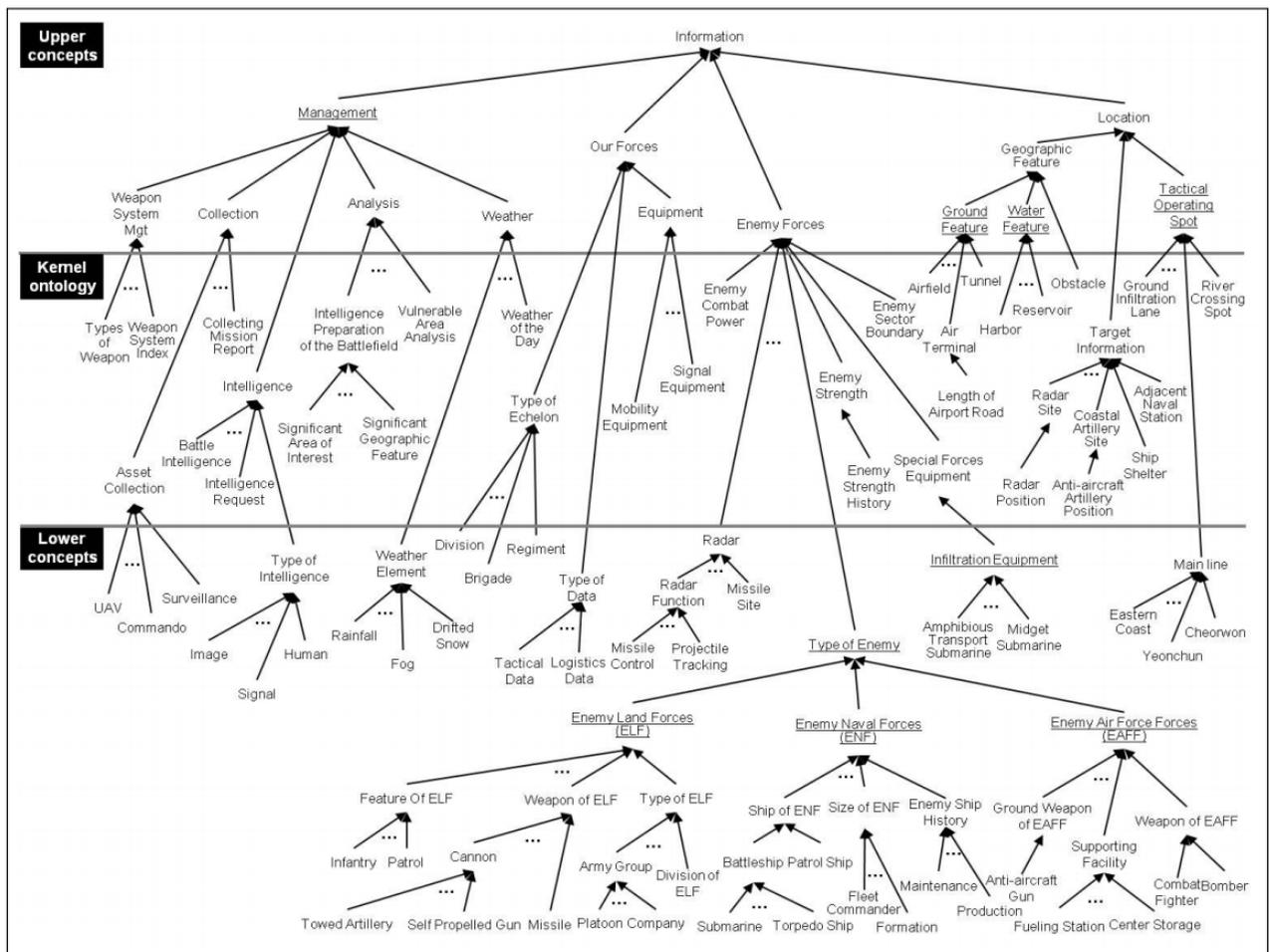


FIGURE 3.5 – Ontologie militaire (de [Yoo et al., 2014])

Un autre exemple d'ontologie est celle développée dans les travaux de L. Serrano sur l'ontologie Wookie [Serrano, 2014] qui décrit la notion d'évènements et de relations comme le montre la Figure 3.6. On peut voir que les évènements sont séparés en catégorie dans la Figure 3.6a. Cela permet de donner un sens sémantique à l'évènement qui, lorsqu'il est instantié dans une classe, permet de remonter à toutes les classes dont il hérite. Par exemple, une opération de maintien de la paix va être instantiée en tant que *PeaceKeepingOperation* qui est un évènement de type *MilitaryOperation* dans la catégorie *MilitaryEvent*. Enfin, la Figure 3.6b montre des relations possibles entre entités telles que "implique" (*involve*) qui, lorsqu'il est lié par exemple à un évènement, permet de mettre en relation avec des entités de type "personne" (*person*) afin de définir que l'évènement implique les entités personnes rattachées via cette relation. De même que la relation "est causée par" (*isCausedBy*) montre qui ou quoi est acteur de l'évènement en fonction de l'entité reliée.

Les ontologies permettent donc à la fois de gérer, formaliser et structurer des concepts pour une meilleure compréhension humaine, mais aussi de permettre à des outils informatiques de lire et d'utiliser ces données afin de les traiter de façon uniforme et prédictible.

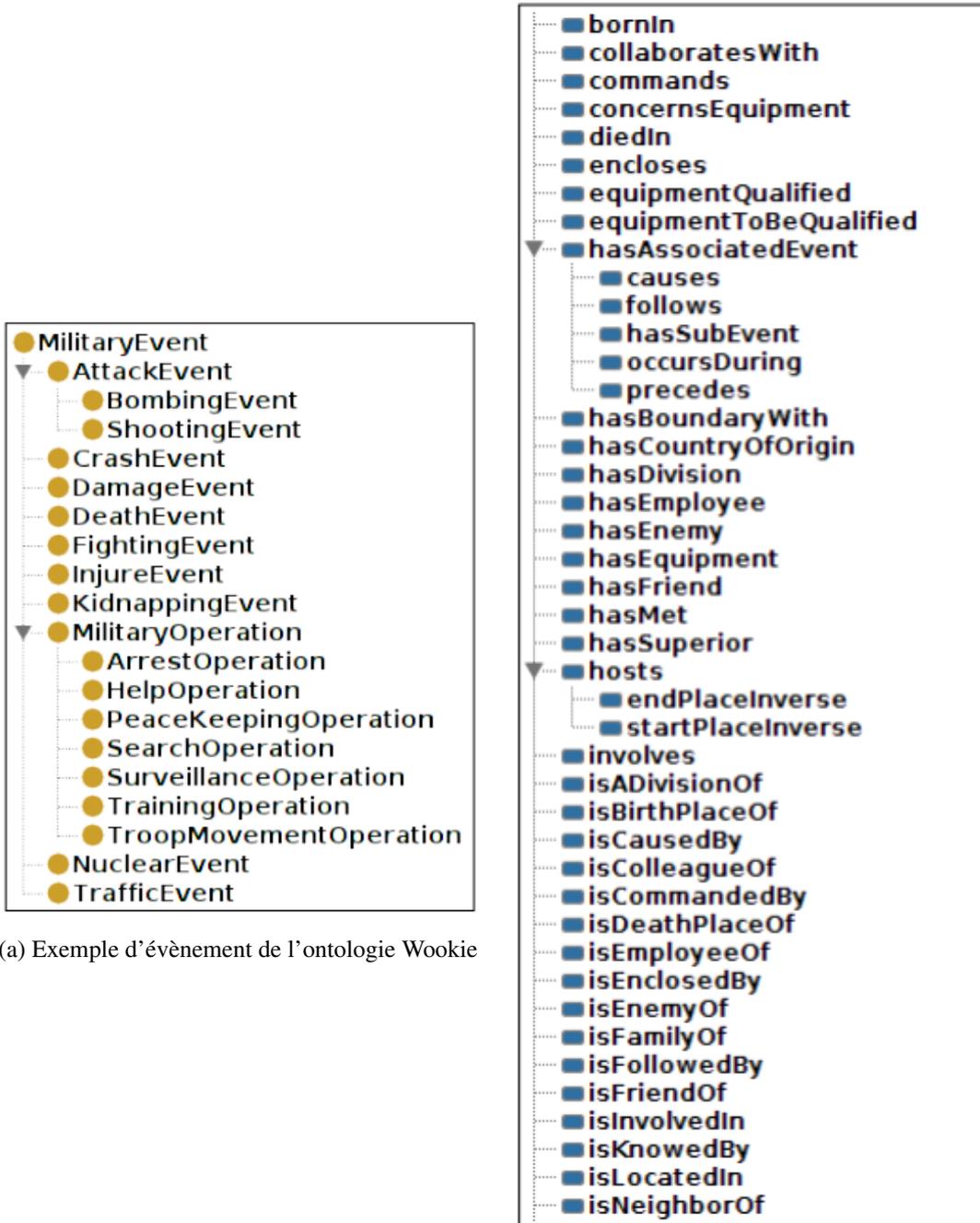


FIGURE 3.6 – Ontologie Wookie (de [Serrano, 2014])

3.2 La représentation de l’incertitude

La représentation de l’incertitude est une problématique intrinsèque au domaine du SA. Les observations peuvent être bruitées, l’inférence des états peut être faussée, ou simplement les informations peuvent être trop incomplètes pour être en mesure d’être efficaces dans la compréhension d’une situation. Cette section a été réalisée en grande partie grâce aux travaux de [Bellenger, 2013] et [Renoux, 2015].

3.2.1 Représenter l’incertitude

Dans [Dubois, 2007], l’auteur définit trois types d’incertitudes ayant trois origines différentes : l’incertitude aléatoire, l’incertitude épistémique et l’incertitude inconsistante (voir Figure 3.7).

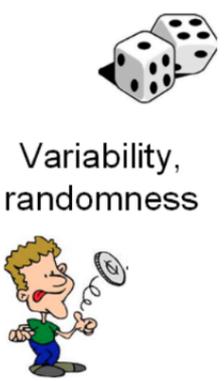
Type of Uncertainty	Aleatory Uncertainty	Epistemic Uncertainty	Inconsistent Uncertainty
Origins	 <p>Variability, randomness</p>	<p>Ignorance, Incompleteness</p> 	<p>Conflict between sources</p> 

FIGURE 3.7 – Les trois types d’incertitude et leurs origines (de [Bellenger, 2013])

L’incertitude aléatoire provient de l’aléatoire des expérimentations, comme jeter un dé. Cette incertitude peut être mesurée ou estimée via les données statistiques et la connaissance du bruit apporté par les capteurs dans leurs observations. L’incertitude épistémique est quant à elle due au manque de connaissance, c’est à dire à l’incomplétude de la connaissance sur ce qu’on observe. Cette fois, il n’y a pas moyen de mesurer via des modèles statistiques cette incertitude. Enfin, l’incertitude inconsistante correspond à l’incertitude générée par la provenance d’informations contradictoires de plusieurs sources. La question est de savoir quelle source croire sur ce qui est le plus proche de la réalité ou non.

Afin d'être en mesure de gérer l'incertitude, les agents ont besoin de représentations formelles. La quasi intégralité des modèles se base sur les *mondes possibles*. Chaque agent génère un ou plusieurs mondes possibles en fonction des informations et de la connaissance qu'il a de l'environnement qu'il observe. Cette connaissance permet de générer ces différents mondes possibles, et plus il y a de mondes possibles, plus l'incertitude est grande. Le but est donc de réussir à réduire le plus possible le nombre de mondes possibles et d'estimer à quel point ils sont possibles pour pouvoir prendre une décision.

Différentes approches permettent de représenter l'incertitude. La suite de cette section va parler des mesures de probabilités puis se focaliser sur l'approche choisie avec les réseaux bayésiens dynamiques et la façon de mesurer le niveau d'incertitude.

3.2.2 Les mesures de probabilités

Considérant un jeu de mondes possibles $W = w_1, \dots, w_n$. Pour chaque monde $w_i \in W$, on associe une probabilité $P(w_i)$ qui décrit la probabilité que ce monde soit le monde réel. Cette mesure de probabilité respecte les règles suivantes :

$$\forall w_i \in W, P(w_i) \in [0, 1] \quad (3.1)$$

$$\forall w_i, w_j \in W, w_i \neq w_j, P(w_i \cup w_j) = P(w_i) + P(w_j) \quad (3.2)$$

$$\sum_{w_i \in W} P(w_i) = 1 \quad (3.3)$$

Plus la probabilité d'un monde est proche de 1, plus le monde lié à cette probabilité est potentiellement l'état du monde actuel et moins les probabilités des autres mondes sont possibles du fait de l'Équation 3.3. Inversement, un monde avec une probabilité à 0 sous-entend que le monde est impossible.

Selon le *principe d'indifférence*, en l'absence d'information, on considère chaque monde dans W avec la même probabilité d'être le monde actuel, tel que $\forall w_i \in W, P(w_i) = \frac{1}{n}$ avec n le nombre de mondes possibles dans W .

On appelle état de croyances la mesure de probabilité liée à l'ensemble des mondes $w_i \in W$. Cette état de croyances doit être mis à jour à chaque fois que de nouvelles informations arrivent. La méthode la plus utilisée pour cela est le théorème de Bayes [Bayes, 1763] :

$$P(w_i|E) = \frac{P(E|w_i) \cdot P(w_i)}{P(E)} \quad (3.4)$$

Ou :

- w_i : le monde possible considéré.
- E : l'évidence qui considère quelles informations et comment ces dernières affectent la probabilité d'un monde possible.
- $P(w_i)$: la probabilité *a priori* que le monde w_i soit le monde actuel (avant que E soit observé).
- $P(w_i|E)$: la probabilité *a posteriori* que le monde w_i soit le monde actuel (sachant E).
- $P(E|w_i)$: est fonction de la vraisemblance de E (la probabilité *a posteriori* de E sachant w_i).
- $P(E)$: est la probabilité marginale de E (ou probabilité *a priori*).

Le souci avec cette règle de mise à jour de l'état de croyances est que dans le cas où un des mondes possibles atteindrait une probabilité associée égale à 0, il n'est dès lors plus possible à cause de l'impossibilité de la division par 0. Dans ce cas, $P(w_i|E)$ n'est pas défini.

Théoriquement, du fait de l'état initial des mondes possibles selon le *principe d'indifférence*, la distribution de probabilité est une distribution uniforme. Selon l'application du théorème de Bayes, la valeur exacte des probabilités ne peut jamais atteindre 0. Mais à cause des besoins des discrétisations des états et de leur approximation, ce cas peut malgré tout survenir. Il faut donc un outil permettant de gérer ces cas.

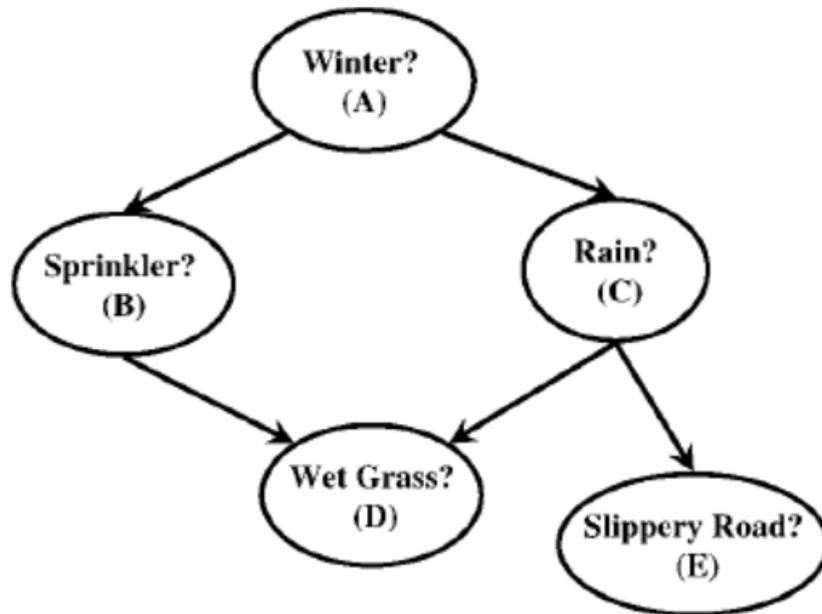
3.2.3 Réseaux bayésiens dynamiques

3.2.3.1 Les réseaux bayésiens

Les réseaux bayésiens (*Bayesian Network* noté BN) ont été introduits par Pearl dans [Pearl, 1988] and Neapolitan [Neapolitan, 1990] et permettent de représenter les dépendances causales entre différentes variables aléatoires. Un réseau bayésien est un graphe acyclique dirigé (*Directed Acycle Graph* noté DAG) où les nœuds sont des variables aléatoires et où les arêtes sont les dépendances causales entre deux variables aléatoires.

À titre d'exemple, les travaux de Harmelen [Van Harmelen et al., 2008] présentent un réseau bayésien simple où deux évènements sont considérés comme responsables que l'herbe soit mouillée : la pluie ou l'utilisation d'un arroseur automatique. Il est aussi considéré que la pluie puisse être responsable du fait que les routes soient glissantes. La Figure 3.8 montre la modélisation de cet exemple via un réseau bayésien.

Chacun des nœuds de la figure représente les différentes variables aléatoires de la situation et les arêtes leur dépendances causales. Chaque variable



A	Θ_A
true	0.6
false	0.4

A	B	$\Theta_{B A}$
true	true	0.2
true	false	0.8
false	true	0.75
false	false	0.25

A	C	$\Theta_{C A}$
true	true	0.8
true	false	0.2
false	true	0.1
false	false	0.9

B	C	D	$\Theta_{D B,C}$
true	true	true	0.95
true	true	false	0.05
true	false	true	0.9
true	false	false	0.1
false	true	true	0.8
false	true	false	0.2
false	false	true	0
false	false	false	1

C	E	$\Theta_{E C}$
true	true	0.7
true	false	0.3
false	true	0
false	false	1

FIGURE 3.8 – Un réseau bayésien avec 5 variables (de [Van Harmelen et al., 2008])

a deux valeurs possibles : *vrai* ou *faux*. Un tableau représente les dépendances et les valeurs des probabilités associées de chaque nœud par rapport à ses parents. On peut par exemple voir que lorsque que la variable *Hiver* (A) est *vraie*, la probabilité que l'utilisation d'un arroseur automatique (B) est vraie avec une probabilité de $P(B|A) = 0,2$ alors que la probabilité qu'il ne soit pas utilisé est à $P(B|A) = 0,8$.

La mise à jour de la distribution de probabilités de chaque variable aléatoire X dans l'ensemble de variables V de taille n du modèle est réalisée telle que selon [Pearl, 1988] :

$$P(X_i) = \prod_{i=1}^n P(X_i|\pi(X_i)) \quad (3.5)$$

Avec $\pi(X_i)$ l'ensemble des parents de X_i instantiés dans un état.

Forts de cela, les réseaux bayésiens permettent de réaliser une inférence sur les états des variables et de répondre à deux requêtes fondamentales :

- **Explication la plus probable** (*Most Probable Explanation* notée MPE) :
- **Probabilité de l'évidence** (*Probability of Evidence* notée PE) : Quelle est la probabilité de l'évidence $P(E)$?

Ces problèmes sont considérés respectivement comme *NP-Hard* [Cooper, 1990] et *PP-Hard* [Littman et al., 2001] et différents algorithmes ont été développés afin de répondre à ces questions de façon exacte ou approximative.

Les algorithmes exacts sont basés sur les réseaux topologiques et utilisent l'élimination de variables [Dechter, 1999], les arbres joints (joint trees) [Shenoy and Shafer, 1986] [Lauritzen and Spiegelhalter, 1988] [Jensen, 1990], ou encore les conditions récursives [Darwiche, 2001]. L'idée est de travailler sur la structure du réseau et sur ses paramètres afin d'affiner les résultats d'inférences. Cela peut se faire en adoptant des représentations non-tabulaires des probabilités conditionnelles (comme dans [Poole and Zhang, 2003] [Larkin and Dechter, 2003]) ou en travaillant sur des structures locales du réseaux (comme dans [Allen and Darwiche, 2002] [Chavira and Darwiche, 2005]).

Les algorithmes approximatifs eux se sont construits sur l'idée que le calcul du meilleur résultat peut être trop compliqué à réaliser et qu'une *bonne* réponse peut être suffisante. Les principales méthodes des algorithmes approximatifs sont les échantillons stochastiques (*stochastic sampling*) [Shachter and Peot, 1990] [Cheng and Druzdzel, 2000], la propagation de croyances [Yedidia et al., 2005], les principes variationnels (*variational methods*) [Jordan et al., 1999]. Ces algorithmes ont généralement des erreurs bornées.

Les réseaux bayésiens sont des outils complets très intéressants pour l'évaluation de situations et la représentation de la connaissance, mais le souci est qu'ils ne permettent de travailler que sur une image à un instant donné. La

notion dynamique et temporelle d'une situation par exemple n'est pas prise en compte.

3.2.3.2 Les réseaux bayésiens dynamiques

Les réseaux bayésiens dynamiques (*Dynamic Bayesian Network* notés DBN) sont une extension des réseaux bayésiens permettant de représenter l'évolution des variables aléatoires par rapport à une séquence discrète, qui la plupart du temps est temporelle (comme des pas de temps) [Dean and Kanazawa, 1989]. Les DBN respectent la même structure de réseau que les BN, mais le réseau est dupliqué à travers une séquence discrète avec une influence de chaque variable sur elle-même et d'autres à travers la séquence (par exemple, une variable va avoir une dépendance causale sur elle-même de t vers $t + 1$).

Les DBN représentent naturellement la dimension spatio-temporelle des environnements dynamiques. La dimension temporelle est représentée par des intervalles de temps où chaque intervalle est un réseau bayésien. De ce fait, la fonction d'inférence change et devient une distribution jointe telle que :

$$P(X_{1:T}) = \prod_{t=1}^T \prod_{i=1}^n P(X_i^t | \pi(X_i^t), X_i^{t-1}) \quad (3.6)$$

Où X_i^t est la $i^{\text{ème}}$ variable aléatoire au pas de temps t et $\pi(X_i^t)$ les parents de cette variable aléatoire à t ainsi que la variable elle-même à $t - 1$. La Figure 3.9 montre un exemple de DBN avec sa représentation graphique de ces dépendances avec notamment un arc entre la variable elle-même au pas de temps précédent.

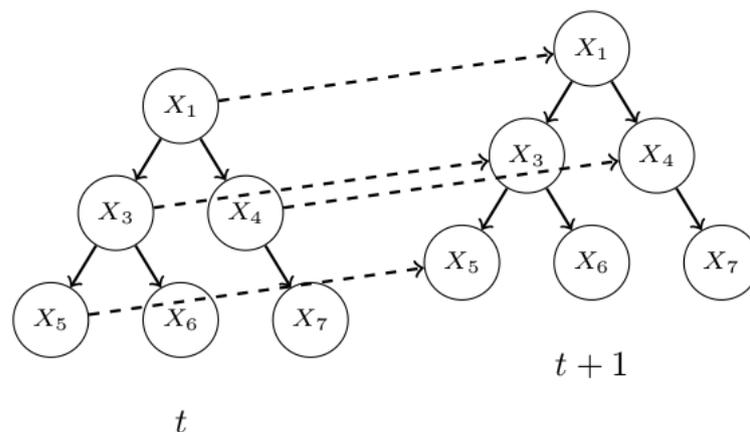


FIGURE 3.9 – Exemple de représentation de réseau bayésien dynamique

D'autres modèles existent et sont utilisés pour la représentation d'environnement dynamique tel que les Filtres de Kalman (*Kalman Filter Model*

noté KFM) et les modèles de Markov cachés (*Hidden Markov Model* noté HMM) pour ne citer que les deux plus utilisés. Mais comme le montrent les travaux de Murphy [Murphy, 2002], les DBN sont malgré tout préférés à ces modèles. Les KFM ont besoin que la densité de probabilités conditionnelles (*Conditional Probability Densities* notée CDP) soit une gaussienne linéaire alors que les DBN permettent de modéliser des CDP non-linéaires et sont donc plus polyvalents. D'autant plus que dans l'évaluation de situation, certaines informations à traiter ne peuvent pas être représentées par des fonctions gaussiennes linéaires. Pour ce qui est des HMM, ils ne modélisent qu'une seule variable aléatoire alors que les modèles via DBN modélisent un ensemble de variables aléatoires. Et même si les HMM factorisés permettent de représenter plusieurs variables aléatoires, les DBN sont plus efficaces en terme de complexité de calcul grâce à leur représentation compacte.

Les DBN représentent donc un avantage certain pour l'évaluation de situations car ils ont en plus l'avantage d'être une représentation proche de ce que présentent les ontologies et permettent naturellement de modéliser le problème en s'inspirant de ces dernières comme le montre [Town, 2004] [Fenz et al., 2009]. Mais en plus, ils permettent de représenter le caractère dynamique de l'environnement et d'inférer l'état des variables aléatoires. C'est pour toutes ces raisons que ce modèle a été retenu pour les travaux qui seront présentés dans la partie contribution.

3.2.4 La théorie Dempster-Shafer

La théorie de Dempster-Shafer a été proposée par Shafer en 1975 ([Shafer, 1976]) à partir des travaux d'Arthur P. Dempster. Cette théorie est aussi connue sous le nom de théorie de l'évidence (*Evidential theory*) et la théorie de fonction de croyances (*theory of belief functions*).

Le concept de la théorie Dempster-Shafer est de permettre de combiner les évidences obtenues par différentes sources afin de calculer une croyance globale pour une hypothèse donnée. Chaque événement est décrit par un niveau de croyances (la crédibilité) et un degré de plausibilité plutôt qu'un seul degré de probabilité.

L'une des principales différences de la théorie de Dempster-Shafer sur la théorie des probabilités est donc de permettre de spécifier un degré d'ignorance dans une situation au lieu d'être obligé de fournir des probabilités *a priori*. Cela permet de travailler directement sur des hypothèses composées plutôt que des hypothèses simples. Enfin, contrairement à la théorie des probabilités, il n'y a pas de relation entre l'existence d'un événement ou non (car il n'y a pas besoin que la somme des croyances valent 1). La croyance est associée à une classe sans influencer les autres classes.

Dans le cas de nos travaux, nous avons malgré tout préféré nous focaliser sur les DBN plutôt que la théorie de Dempster-Shafer pour deux raisons. La première est que nous préférons nous concentrer sur la modélisation se concentrant sur l'inférence des informations dans la représentation de la connaissance en définissant des hypothèses avec des liens causaux entre elles. Alors que la théorie Dempster-Shafer, bien que pouvant permettre cela, est plus intuitivement liée à la notion de fusion par sources d'informations et est moins expressive que les DBN pour nos cas d'usage. Le deuxième point est que nous avons une plus grande maîtrise et connaissance des DBN que de la théorie Dempster-Shafer. Mais cette théorie pourrait être une autre façon de faire tout aussi intéressante.

3.3 La théorie de l'information de Shannon

3.3.1 La théorie de l'information

Historiquement, le concept de *théorie de l'information* a été décrite par C. Shannon [Shannon, 1948]. En réalité, il s'agissait ici d'une théorie de la communication de l'information telle que Shannon et Weaver l'ont appelée dans leurs travaux, mais le terme théorie de l'information a été retenu par l'usage. Dans ses travaux, Shannon décrit l'information comme un ensemble de messages possibles, où le but est d'envoyer ces messages à travers un canal bruité, puis de demander au récepteur de reconstruire le message avec une faible probabilité d'erreur, malgré le bruit de canal. Le but originel était donc de transmettre une information le plus rapidement possible avec un maximum de sécurité dans les domaines de la télécommunication.

La théorie de l'information est utilisée dans de nombreux domaines à commencer par la physique mais aussi l'informatique, la biologie, le traitement du langage et bien d'autres. Ce qui nous intéresse ici est sa vision à travers la théorie des probabilités et les statistiques.

Selon Shannon, une information est un évènement aléatoire. Naturellement, elle est décrite via une variable aléatoire avec une distribution de probabilités sur les valeurs possibles de cette dernière. La considération de l'information comme évènement aléatoire amène le concept d'incertitude, et Shannon va définir l'information uniquement sur la probabilité de l'évènement avec $I = -\log p$. Cette définition de l'information correspond à une mesure d'incertitude. A partir de là, on peut considérer que plus une information est incertaine plus elle est intéressante.

Ce dernier point sera intéressant dans le développement de la contribution Section 2.3.

3.3.2 L'entropie de Shannon

En théorie le concept de base de l'information est donc que lorsque l'on reçoit un message contenant une nouvelle valeur, l'intérêt est de savoir si cette valeur est vraiment celle attendue et à quel point. Selon Shannon, si un évènement est extrêmement probable, ce n'est donc pas une surprise et il n'est pas intéressant. Alors qu'un évènement peu probable contient plus d'informations à apprendre qu'un évènement attendu.

L'entropie de Shannon [Shannon, 1948] est une mesure sur la quantité d'informations sur un message, ou dans notre cas, sur la connaissance de la distribution de probabilités d'une variable aléatoire. Mais elle peut aussi définir à quel point un état peut être prédictible ou non (ce qui correspond plus à la lecture dont nous avons besoin pour l'évaluation de situations).

L'entropie d'une variable aléatoire X est donc définie comme suit :

$$H(X) = - \sum_{i=1}^n P(x_i) \log_b P(x_i) \quad (3.7)$$

Avec n le nombre de valeurs possibles pour la variable X et $P(x_i)$ la probabilité que la variable X prenne la valeur x_i .

La Figure 3.10² illustre le concept de l'entropie. Dans le premier bac, il y a 4 balles rouges. Dans ce cas, l'entropie est faible (en l'occurrence elle vaut 0) car la connaissance sur la couleur de la balle que l'on va tirer au sort est sûre ; on tirera obligatoirement une balle rouge, soit $P(X = \text{rouge}) = 1$. Dans le second cas, il y a une faible chance de tirer une balle bleue plutôt qu'une rouge, $P(X = \text{rouge}) = 0.75$, et $P(X = \text{bleu}) = 0.25$ et donc l'entropie sera raisonnablement plus élevée. Enfin, le dernier bac représente le pire cas où les probabilités sont équiprobables (correspond au *principe d'indifférence* - Section 3.2.2) avec $P(X = \text{rouge}) = 0.5$ et $P(X = \text{bleu}) = 0.5$. Ici l'entropie sera très élevée car le niveau d'incertitude est maximal.

On voit donc bien que plus l'information est considérée comme certaine, plus l'entropie est basse (jusqu'à la valeur 0 où la probabilité est maximale donc 1).

L'intuition derrière est de pouvoir utiliser l'entropie de Shannon pour définir quel est le niveau de connaissance sur une variable aléatoire, et donc, de savoir à quel point la probabilité de ces états représente la situation actuelle.

2. Image provenant de la vidéo de Luis Serrano sur l'entropie et le gain d'information <https://www.youtube.com/watch?v=9r7FIXEAGvs>

What ball will we pick?

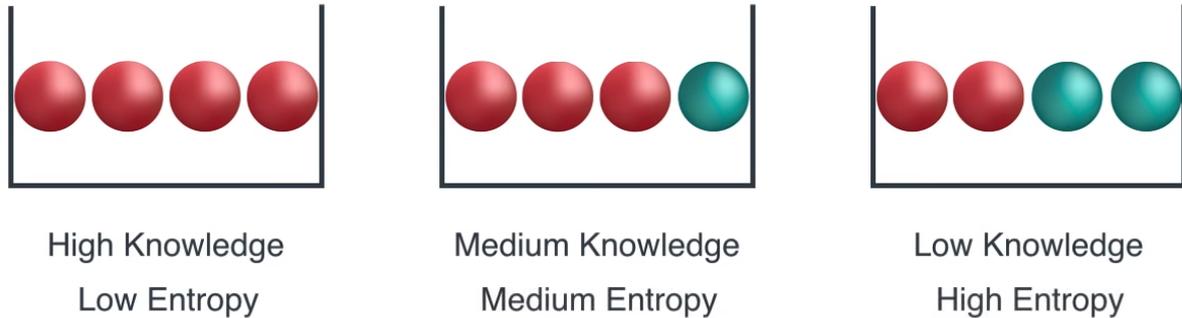


FIGURE 3.10 – Exemple de représentation de réseau bayésien dynamique

3.4 Conclusion

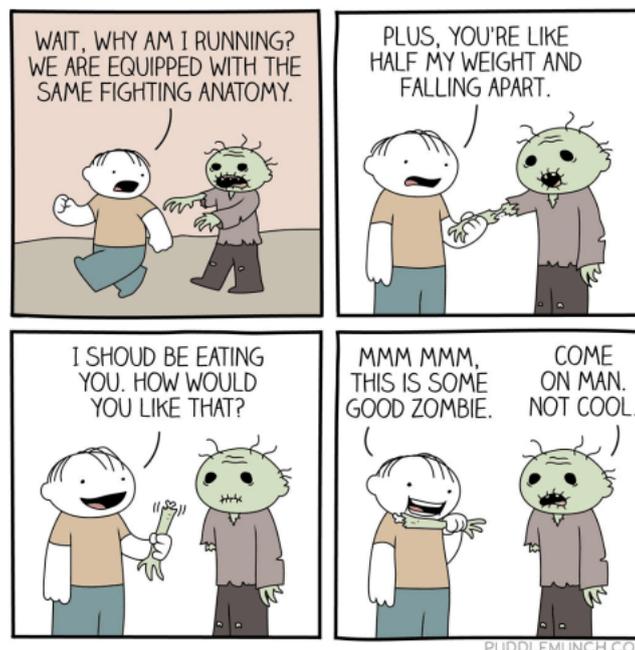
Ce chapitre nous a permis de :

- Définir ce qu'est la représentation de connaissances (KR)
 - D'expliquer la différence et la hiérarchie des Données-Informations-Connaissances
 - Parler des outils et premières applications pour le KR
 - Définir le concept d'ontologie qui est l'outil le plus représentatif en KR
- Introduire et définir le concept d'incertitude et de sa représentation
- Présenter les outils permettant de travailler avec l'incertitude
- Introduire les réseaux bayésiens dynamiques et permettre l'inférence de variables aléatoires
- Introduire l'entropie de Shannon à travers la théorie de l'information afin d'être utilisée comme mesure de gain d'information

CHAPITRE 4

L'évaluation de la menace

L'évaluation de menace (*Threat Assessment*, notée TA) est une spécialisation de l'évaluation de situations. Dans de nombreuses problématiques, elle fait d'ailleurs partie du SA dans l'analyse de l'impact (voir le modèle JDL DF Chapitre 2 Section 2.4.3).



Zombie threat assessment

FIGURE 4.1 – Une bonne évaluation de la menace permet de trouver la bonne contre-mesure

Le TA a pour objectif soit de prévenir un évènement néfaste (et dans ce cas on parle souvent d'évaluation de risque (*risk assessment*) afin de réduire

voire endiguer ce risque, soit d'évaluer la menace lors d'un évènement en cours et dans ce cas trouver le meilleur moyen de contrer la menace.

La menace peut revêtir différentes formes en fonction du domaine applicatif. Dans le cas de catastrophes naturelles, elle se définirait par les risques de répliques d'un séisme ou les risques d'effondrement d'un bâtiment après une catastrophe par exemple. Lors d'une attaque terroriste, la menace est représentée par le ou les sujets impliqués dans l'attaque, et notamment leur position, leurs équipements et leur attitude. Lors d'une opération militaire ou sur un théâtre d'opération, la menace est représentée par la stratégie de l'adversaire, ses déplacements et ses objectifs.

Ce chapitre va permettre de définir ce qu'est la menace dans la littérature, pour la définir plus spécifiquement dans le domaine militaire via la doctrine militaire.

4.1 L'évaluation de menace

4.1.1 Les principes de l'évaluation de menace

Il existe trois principes fondamentaux dans l'évaluation de menace [Fein and Vossekuil, 1998]. Le premier est que la violence ciblée est le résultat d'un processus de pensée et de comportement compréhensibles et discernables. Les actes de violence ciblés ne sont ni spontanés ni impulsifs car ils nécessitent la mise en place d'une stratégie, ce qui prend un certain temps. Une personne cherchant à lancer une attaque ciblée va identifier et choisir sa cible, collecter des informations et planifier les actions nécessaires pour réussir l'attaque.

Le second principe définit la violence comme résultant d'interactions entre l'attaquant, les évènements passés, la situation actuelle et la cible. En effet, la recherche dans ce domaine se concentre maintenant plus sur le contexte et la compréhension de la situation et du risque plutôt que sur l'individu susceptible de commettre une action violente comme c'était le cas par le passé (via le profilage psychologique). Il est question ici de savoir comment le sujet est susceptible de réagir face à des situations passées (rejet social, humiliation, échec, ...).

Enfin, le troisième principe est l'une des clefs de l'investigation et de la résolution de l'évaluation de menace ; l'identification des comportements du sujet liés à l'attaque. Ceux qui se lancent dans une attaque ciblée arborent souvent un comportement discret lorsqu'ils sont dans la planification et la préparation logistique de cette dernière. Connaître ces facteurs est important pour l'appréciation de la gestion du risque.

Ces recherches se concentrent plus sur des attaques avec un sujet ou un petit groupe de sujets qui agissent suite à un traumatisme ou par idéologie (tueur de masse, attaque terroriste, ...). Le cas d'application le plus répandu aux USA est d'ailleurs celui des tueurs de masse en école comme à Columbine [O'Toole, 2000] [Reddy et al., 2001]. Cette vision de l'évaluation de menace aussi appelée dans ce cas évaluation de risque (*risk assessment*) est d'ailleurs souvent employée à des fins de prévention [Fein et al., 1995].

Les concepts présentés ici sont intéressants pour voir la globalité des facteurs pris en compte pour définir la menace. Cependant, les travaux de cette thèse se concentrent plus sur l'évaluation de la menace lors d'une situation néfaste en cours (théâtre d'opération militaire) et non la prévention de la menace (comme pour l'évaluation de risque).

4.1.2 Une tâche de prédiction

Une définition générale de l'évaluation de menace a été introduite par Steinberg [Steinberg, 2009] :

Définition 9. L'évaluation de menace implique d'évaluer la situation afin de déterminer si oui ou non un évènement néfaste est susceptible de se produire.

Cette définition correspond au Niveau 3 du modèle JDL DF (Chapitre 2 Section 2.4.3) qui originellement était défini comme une étape d'évaluation de menace plutôt qu'une évaluation d'impact (du fait du contexte militaire de la création de ce modèle). Dans cette formalisation, le système s'intéresse à mesurer une fonction de coût / utilité des sujets générant la menace afin d'essayer d'estimer les prochaines actions possibles. Dans le cas où plusieurs sujets attaquent (par exemple lors d'une attaque sur un front de guerre), les interactions entre eux deviennent très importantes pour estimer les objectifs communs avec la multitude d'actions possibles (communes ou indépendantes) afin de mesurer le coût / utilité permettant d'essayer d'estimer quelle stratégie ou suite d'action est la plus susceptible de se produire.

Initialement, [Lambert, 2001] et [Salerno, 2008] ont distingué l'évaluation de l'impact (cest à dire celle de la menace) de l'évaluation de situation en les séparant des concepts temporels et ontologiques (sémantiques) respectivement. Mais Steinberg propose une vision où l'évaluation de situation permet l'évaluation de l'impact en générant les différents mondes possibles via l'inférence des scénarios possibles à partir des observations collectées à l'instant présent [Steinberg, 2009]. De fait, l'évaluation de menace se base plus sur l'évaluation de la situation actuelle mais sur des situations projetées dans les futurs possibles. Le TA est donc une tâche de prédiction alors que l'évaluation d'impact correspond de façon plus générale à une tâche de

projection. Comme présenté par [Le Guillarme, 2016], il y a une relation inclusive entre l'évaluation de situation, d'impact et de menace en terme d'interprétation épistémique (montré dans la Figure 4.2). Le TA vu comme une tâche de prédiction correspond donc au plus Haut-Niveau d'évaluation de situation (Niveau 3 du modèle d'Ensley - voir Chapitre 2 Section 2.3.1).

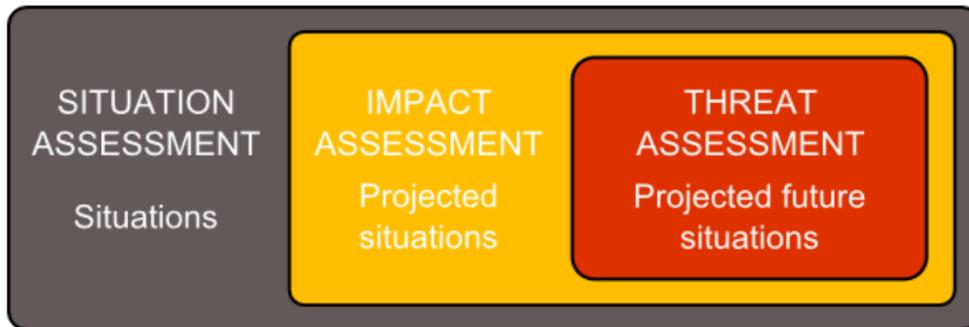


FIGURE 4.2 – Relation d'inclusion entre l'évaluation de situation, d'impact et de menace (de [Le Guillarme, 2016])

Comme dans les travaux de Leguillarme [Le Guillarme, 2016], nous nous concentrerons sur l'évaluation de la menace telle que des événements menaçants intentionnels aussi appelés **attaques** comme définis par Steinberg [Steinberg, 2009]. L'évaluation de ces événements intentionnels nécessite de prédire et caractériser une situation où des agents cherchent à faire le mal en produisant des dommages. C'est d'ailleurs comme cela que Roy caractérise la menace : "une expression de l'intention de faire le mal, provoquer des blessures ou des dommages" [Roy et al., 2007]. L'intention est donc une notion clef de la menace dans ce contexte. Il faut donc essayer de prédire quelles sont les actions futures les plus probables qu'un agent nocif va tenter de réaliser afin d'estimer l'impact négatif que ces actions auront sur les différentes cibles de l'attaque. Steinberg donne d'ailleurs une définition plus générale [Steinberg, 2009] telle que :

Définition 10. Nous avons besoin de reconnaître l'évaluation de menace comme l'aspect d'un problème plus général qui est l'évaluation de l'intention et la caractérisation, la reconnaissance et la prédiction d'un acte intentionnel en général.

Pour être en mesure de prédire la menace, il est nécessaire d'avoir des modèles prédictifs de comportements humains comprenant notamment la perception, le raisonnement et la planification. Ces modèles sont complexes et difficiles à produire ce qui rend la tâche d'évaluation ardue. Différentes tentatives ont été développées à travers la théorie des jeux dans une approche de gestion de conflit [Roger, 1991]. Les premières approches consistaient à

étudier les stratégies d'agents compétitifs devant atteindre des objectifs incompatibles dans un environnement partagé. Puis les travaux plus récents ont travaillé sur la reconnaissance d'intention de l'adversaire (notamment dans le jeu d'échecs [Plaat et al., 1996] and [Baxter et al., 1999] en décrivant l'environnement à travers des structures de graphe en arbre de décision). Cependant, l'intention n'est pas le seul facteur à prendre en compte pour ce qui est de l'évaluation de menace : il faut aussi savoir si un agent hostile a la capacité et l'opportunité de réaliser son attaque (correspondant au modèle COI défini dans la section suivante 4.2. Ces trois facteurs permettent en effet d'inférer et de prioriser des scénarios d'attaque en terme de priorité pour un opérateur qui doit prendre une décision.

La littérature ne propose que peu de tentatives de formalisation de l'évaluation de menace. Cela se justifie par le fait que la tâche est complexe car elle tente de répondre à de nombreuses questions telles que : qui/quoi (entités menaçantes, entités menacées), pourquoi (intentions, objectifs), où/quand/comment (capacité, opportunité, déroulement de l'action), quelles conséquences (bilan, coût/utilité). La littérature fournit cependant une définition de l'évaluation de menace comme un problème plus spécifique [Paradis et al., 2005] :

Définition 11. La partie de l'analyse de la menace qui concerne le processus en cours pour déterminer si une entité a l'intention d'infliger du mal, des blessures ou des dommages aux forces en défense et à ses intérêts, ainsi que le classement de ces entités en fonction du niveau de menace qu'elles représentent.

Soit $D = D_1, \dots, D_m$ un ensemble de points d'intérêt à défendre et $E = E_1, \dots, E_n$ un ensemble d'ennemis détectés dans la zone de surveillance cherchant à attaquer les points D . Selon [Johansson and Falkman, 2008], le problème d'évaluation de menace considère des paires (E_i, D_j) avec $E_i \in E$ et $D_j \in D$ auxquelles est associée une valeur de menace $T_{ij} \in [0, 1]$ représentant le niveau de menace que E_i génère sur D_j . Plus la menace est probable, plus elle se rapproche de 1, et moins elle l'est, plus elle se rapproche de 0. La priorité de la menace est donc ordonnée via ces valeurs de menace comme le montre la Figure 4.3 où D_2 semble être la cible la plus probable de l'ennemi E_1 .

Cependant, on ne représente ici que la probabilité de la cible attaquée par chaque ennemi détecté. Il manque ici la notion de stratégie de l'ennemi (présentée plus en détail dans la Section 4.4) pour connaître son plan d'action, les chemins empruntés pour réaliser son attaque, les dommages potentiels sur chaque cible en fonction du type d'ennemi, etc.

Cette vision de l'évaluation de menace comme tâche prédictive plutôt que comme prévention d'une attaque est celle retenue pour les travaux de cette

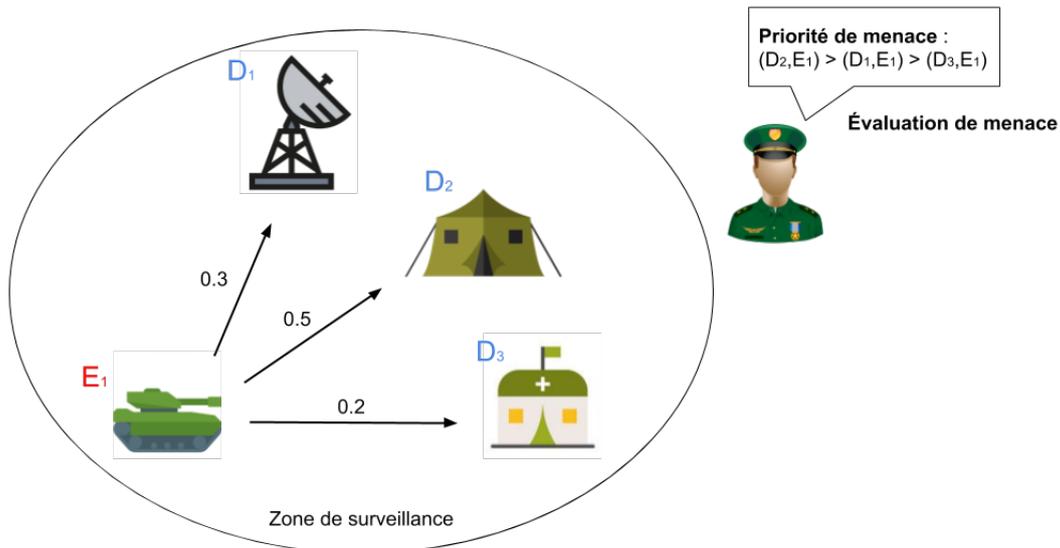


FIGURE 4.3 – Illustration de l'évaluation de la menace (adapté de [Le Guillaume, 2016])

thèse. En effet, nous nous concentrerons sur une attaque en cours pour évaluer le niveau de menace et la force déployée de l'ennemi afin d'en comprendre la stratégie et d'être capable de proposer à un opérateur humain une image la plus représentative de la situation afin d'adapter de la façon la plus efficace et rapide la contre-mesure adéquate.

4.2 Le modèle COI pour la menace

Le modèle Capacité-Opportunité-Intention (noté COI) a été proposé par Little et Rogova à travers leur ontologie sur la menace [Little and Rogova, 2006]. Le concept de ce modèle est d'être en mesure d'estimer ces trois facteurs afin d'estimer si les conditions nécessaires sont suffisantes pour générer une menace et lui permettre d'exister (voir Figure 4.4). Ce modèle a été étendu par Steinberg par la suite pour la prédiction d'acte intentionnel [Steinberg, 2007] ce qui est devenu le modèle de référence de la plupart des travaux d'évaluation de menace.

Capacité

La capacité comprend un agent physique cherchant à produire une action. Little et Rogova définissent la capacité comme :

Définition 12. Le type d'objets (i.e. armes), les attributs de l'objet (i.e. projectile ou explosif) ou le comportement (i.e. capacité de mouvement, de perception) qui peuvent infliger un certain niveau de dommage, de perturbation

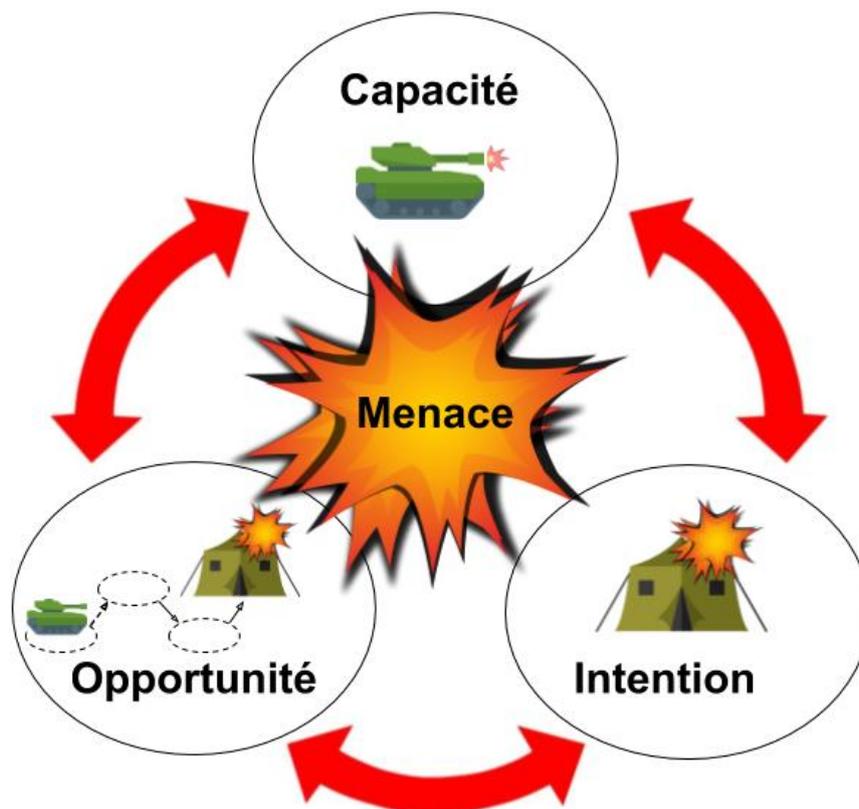


FIGURE 4.4 – Le modèle COI (adapté de [Le Guillarme, 2016])

ou de létalité à une cible (telle qu'identifiée par une intention et rendue possible par des opportunités).

Le concept de capacité est donc directement relié à la faisabilité d'une action par les capacités d'un agent. Les capacités de ce dernier lui permettent ou non de réaliser une action. La capacité est donc considérée comme un composant individuel de la menace.

Opportunité

L'opportunité quant à elle considère des facteurs extérieurs conduits par l'environnement qui rend possible ou non la réalisation d'actions en fonction des capacités des agents. Steinberg définit l'opportunité comme :

Définition 13. La présence d'un environnement d'exploitation dans lequel des cibles potentielles d'une action sont présentes et sont susceptibles de faire l'objet de mesures.

L'opportunité est définie ici comme un facteur spatio-temporel entre l'agent et l'environnement dans lequel il se trouve. C'est à dire la relation d'un agent avec son environnement. Par exemple, la position d'un agent par rapport à sa cible en rapport à sa portée de tir. Si la portée de tir de l'agent est inférieure

à sa distance avec sa cible, il ne peut donc lui nuire. Cette notion peut aussi prendre en compte l'exposition d'une cible en fonction de l'absence ou non de protection ou de système de défense [Roy and Guyard, 2012]. Si la cible est plus vulnérable et que l'agent a les capacités de l'attaquer, alors l'opportunité de l'attaquer augmente.

Intention

Dans le cadre de l'évaluation de menace avec des agents hostiles, l'intention correspond à la détermination d'une entité d'infliger des dégâts à des zones défendues ou à leurs défenses [Roy and Guyard, 2012]. L'intention représente donc la volonté d'un agent d'agir d'une certaine façon afin d'atteindre son but, en d'autres termes, la motivation de l'agent. Ce facteur ne peut pas être directement observé et nécessite d'inférer à partir des éléments observables pour le comprendre (correspond au Haut-Niveau des modèles de Fusion d'Informations pour l'évaluation de situation). Pour cela, plusieurs facteurs sont pris en compte comme montré dans la Figure 4.5. où l'on voit que l'intention intègre les intérêts (buts Haut-Niveaux), les capacités, les opportunités et la vulnérabilité [Roy et al., 2007].

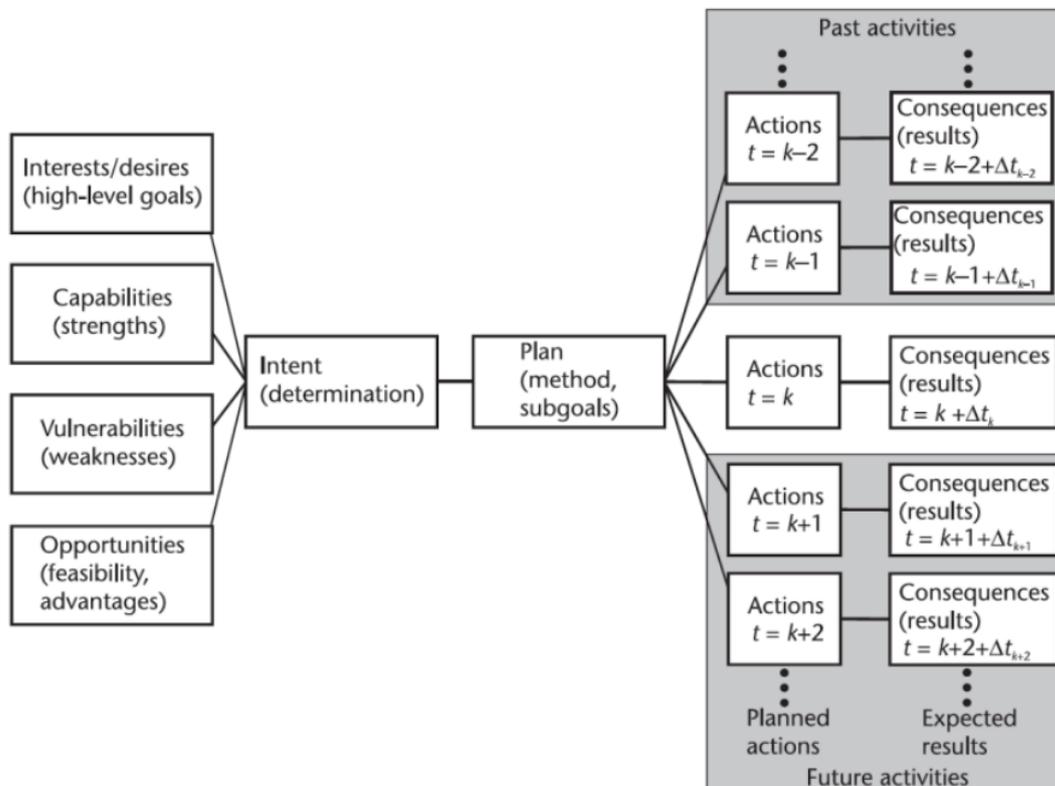


FIGURE 4.5 – Représentation des facteurs de l'intentions (de [Roy et al., 2007])

4.3 La propagation de la menace

4.3.1 La menace, une propagation incertaine

Le but de l'évaluation de menace est d'être en mesure d'identifier toutes les menaces potentielles, c'est à dire qui n'existent pas encore mais sont en devenir. Le défi est de réussir à les identifier le plus rapidement possible afin de permettre au preneur de décisions de réagir le plus rapidement et le plus efficacement possible.

Pour cela, on génère différents mondes possibles avec des scénarios différents de menace. Mais pour comprendre rapidement ce qui se passe, il faut être en mesure de prédire les menaces potentielles alors que les agents hostiles ne sont pas encore suffisamment proches de leurs cibles pour être en mesure de comprendre leur intention.

Comme vu à travers le concept d'opportunité (voir Section 4.2), la menace se trouve définie à travers un environnement spatio-temporel avec des agents physiques pouvant se déplacer en fonction de leur capacité et de leur intention. De fait, la menace se propage de façon spatio-temporelle à travers cet environnement en fonction des mouvements des agents et du modèle COI.

Les différents scénarios de menace étant incertains, ils représentent chacun un monde possible (voir Section 3.2.1). Cette incertitude vient du fait qu'on ne sait pas exactement quel parcours/chemin un agent va emprunter ne sachant pas exactement quelle cible il compte attaquer. Chacun de ces mondes possibles représente une façon possible dont la menace peut se propager en fonction des potentiels futurs déplacements des agents hostiles.

Toutes les modélisations présentées dans la Section 3.2.1 ont pu être utilisées dans l'évaluation de menace, mais le modèle ayant le plus retenu l'attention dans la littérature est celui des Réseaux Bayésiens (BN), puis des Réseaux Bayésiens Dynamiques (DBN) (voir Section 3.2.3). En effet, un tel environnement peut être assez naturellement représenté par un graphe, et les DBN permettent de représenter les rapports de causalité spatiaux et temporels.

4.3.2 La propagation de croyances de Pearl

La propagation de menace peut être perçue comme une propagation de croyances sur l'état des agents hostiles et de leurs intentions futures. On définit le terme **croyance** (*belief*) tel qu'une information possible et imparfaite concernant l'environnement [Dastani et al., 2005]. C'est une connaissance mais qui n'est pas nécessairement vraie (du fait de l'imperfection) et qui nous ramène à la notion d'incertitude. La **propagation de croyances** (Belief

Propagation) a été introduite et développée par Pearl et permet de propager une information à travers des réseaux bayésiens ou des modèles de Markov aléatoires [Pearl, 1982]. Pour cela, Pearl a présenté un algorithme de propagation d'inférence dans des poly-arbres (*polytrees*) qui sont définis par [Pearl, 1988] tel qu'un graphe acyclique dirigé avec la propriété qu'en ignorant les directions sur les arêtes, on obtient un graphe sans cycles non orientés. Les poly-arbres permettent grâce aux algorithmes de Pearl une inférence rapide et exacte (en temps linéaire alors que les BN sont en temps NP-Hard) ce qui les a mis en avant dans la communauté scientifique pour des problèmes d'évaluation de situation.

La Figure 4.6 représente le cas général d'un nœud X qui est une variable aléatoire avec une distribution de probabilité. Les variables $U = \{U_1, \dots, U_m\}$ représentent les parents de X et les variables $Y = \{Y_1, \dots, Y_n\}$ les enfants de X .

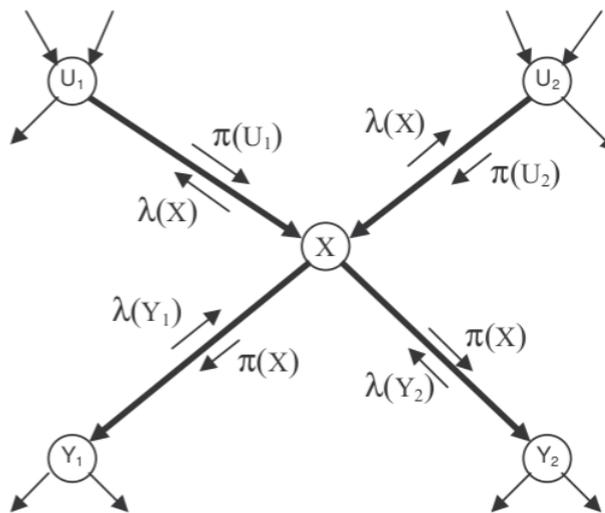


FIGURE 4.6 – Propagation de messages dans un réseau bayésien (de [Ajroud et al., 2012])

On définit comme les **évidences** W les variables aléatoires du réseau bayésien (qui est un poly-arbre) qui ont pu être observées et dont on considère connaître la valeur de façon sûre. Les évidences "au-dessus" de X (qui sont ses parents ou les parents de ses parents) sont notées W_X^+ et celles "en-dessous" sont notées W_X^- .

De là, la connaissance sur ces variables peut se propager du haut du réseau vers le bas (des parents vers les enfants, et inversement (des enfants vers les parents)). Les π -messages sont les messages partant d'un parent $u_i \in U$ vers la variable X et les λ -messages sont ceux partant des enfants $y_i \in Y$ vers X .

Pour toutes les valeurs x_i que X peut prendre, les π -messages et λ -messages sont définis tels que :

$$\pi(x_i) = P(x_i|W_X^+) \tag{4.1}$$

$$\lambda(x_i) = \begin{cases} P(W_X^- | x_i) & \text{if } X \notin W \\ 1 & \text{if } X \in W \wedge X = x_i \\ 0 & \text{if } X \in W \wedge X \neq x_i \end{cases} \quad (4.2)$$

Les messages sont propagés depuis les évidences dans tout le réseau jusqu'à ce que toutes les probabilités soient mises à jour. Une fois tous les π -messages et λ -messages calculés, la probabilité que la variable X prenne la valeur x_i est calculée telle que :

$$P(X = x_i) = \alpha \pi(x_i) \lambda(x_i) \quad (4.3)$$

Avec α un facteur de normalisation sur les valeurs possibles de X .

4.3.3 Propagation de croyances et complexité

L'algorithme de propagation de croyances est de complexité polynomiale en fonction du nombre de nœuds et converge dans un temps proportionnel à la largeur du réseau [Pearl, 1988]. De plus, la complexité du calcul de probabilité d'un nœud est fonction de la taille de sa table de probabilités conditionnelles. Le souci étant que la majorité des réseaux bayésiens ne sont pas des poly-arbres et dans le cas de BN avec des cycles, il a été prouvé que l'algorithme de Pearl ne donne pas de résultats corrects notamment sur les distributions de probabilités *a posteriori*.

Pour pallier ces problèmes, différents algorithmes d'inférence exacte ont été proposés à commencer par la méthode dite *loop cutset conditioning* présentée aussi par [Pearl, 1986] qui modifie les connexions d'un réseau à connexions multiples pour le transformer en réseau à connexion unique. Cependant, la complexité de cette méthode augmente exponentiellement avec la taille du *loop cutset* et la minimisation du *loop cutset* dans un réseaux à connexions multiples est aussi un problème NP-Hard.

Une autre solution est celle de la propagation via des cliques d'arbres (*clique-tree propagation*) [Lauritzen and Spiegelhalter, 1988] qui transforme le réseau en plusieurs cliques d'arbres. Mais ce dernier modèle peut être très lent car sa complexité est exponentielle en fonction de la plus large clique du réseau transformé.

Les algorithmes d'inférence approximative restent donc à favoriser quand les réseaux deviennent trop complexes d'autant plus que l'inférence exacte dans un réseau bayésien est considérée NP-Hard [Cooper, 1990].

4.4 Considération de la menace selon la doctrine militaire

Dans cette section, nous allons présenter la doctrine militaire selon laquelle nos travaux se sont appuyés pour générer un scénario crédible et un modèle adapté aux méthodes du renseignement et de la planification. Ce qui est présenté ici est basé sur deux documents de la doctrine militaire, le manuel de l'Unité de Brigade de Renseignement (UBR) [PFT RENS, 2016] et le manuel d'emploi du sous-groupement recherche multicapteurs [RENS, 2016].

La présentation de cette doctrine se fait par le biais du scénario (défini dans le Chapitre 10) où deux camps sont considérés, celui de l'attaquant (l'ennemi) et celui du défenseur (l'allié). Le but est de défendre des zones spécifiques et de comprendre laquelle ou lesquelles seront attaquées.

4.4.1 Définition de l'environnement et de la menace

Les services de renseignement lors d'un théâtre d'opération définissent différents éléments permettant de représenter une situation (de crise) à partir de laquelle les observateurs humains (le centre de commandement) vont réaliser les étapes nécessaires à l'évaluation de situation et en l'occurrence, l'évaluation de la menace de l'ennemi qui est affronté.

La première chose définie par ces services sont les Zones d'Informations Prioritaires (notées ZIP) sur le champ de bataille. Ces zones correspondent aux zones à observer pour être en mesure de comprendre l'intention de l'ennemi, ses déplacements, autrement dit sa stratégie. Le but pour les troupes alliées est d'observer ces ZIP pour réussir à comprendre quels sont les objectifs et les cibles de l'adversaire et comment il compte mener l'assaut.

On considère dans ce cadre la stratégie de l'ennemi comme comprendre comment il compte conduire ses opérations, c'est à dire :

- Connaître le(s) objectif(s) de l'ennemi
- Connaître la(es) cible(s) que l'ennemi souhaite attaquer
- Comprendre les moyens déployés par l'attaquant et leur force de destruction
- Comprendre les déplacements de l'ennemi dans la zone et identifier les groupes d'assaut

Le but des forces opposantes étant l'assaut de point stratégique, les renseignements définissent également des Points d'Attaque (notés PA) que les alliés doivent défendre. Le preneur de décision doit rapidement comprendre quels sont les AP les plus exposés et donc susceptibles d'être attaqués afin

d'adapter sa stratégie en conséquence et de disposer ses troupes pour optimiser les défenses en réponse à l'attaque.

Afin d'évaluer le plan d'attaque de l'adversaire, le commandement doit détecter les manœuvres ennemies et décrire la situation de la menace durant chaque phase de l'attaque en temps réel (ou quasi-réel). La menace ici est considérée par la façon dont l'ennemi déplace ses compagnies. Une compagnie est un groupe d'unités militaires avec un rôle spécifique et une force de destruction associée. Plus la compagnie possède une force de destruction conséquente, plus la menace de cette dernière est élevée.

Mais il est aussi nécessaire de prendre en compte la capacité de l'unité (portée de tir, capacité de mouvement, résilience, ...) comme vu dans le modèle COI. Vue au travers du modèle COI, la **capacité** représente les caractéristiques de chaque type de compagnies engagées, l'**opportunité** est caractérisée par la topologie du terrain, la capacité de déplacement des troupes, et le chemin emprunté pour atteindre son objectif et l'**intention** est dirigée par la stratégie globale de l'ennemi (soit une intention multi-agents centralisée par une intention globale).

4.4.2 L'UBR, une unité multicateurs

L'UBR est une brigade de renseignement déployée sur le terrain pour acquérir l'information lors d'une situation de crise (un théâtre d'opération militaire). Elle est composée d'un ensemble de capteurs hétérogènes composé de 4 sources de renseignement afin d'observer les ZIP.

RORAD

Le Renseignement d'Origine Radar (RORAD) correspond aux détections radar. Les radars permettent d'identifier la taille ou la masse de l'objet détecté pouvant faire la différence entre des véhicules lourds blindés ou une troupe d'infanterie. Cependant, l'identification précise du type nécessite souvent de corrélérer l'information avec d'autres sources.

Le Radar d'Acquisition et de Surveillance Terrestre (RASIT) est un radar Doppler. Il permet de détecter des piétons (14km), des hélicoptères et avions légers (25km) et tout autre type de véhicules (40km). Ce radar est installé sur des véhicules de reconnaissance (P4 ou VBL). Sa précision souffre des replis de terrain et nécessite un point haut pour être déployé.

Il est à noter qu'un facteur risque existe sur l'utilisation de ce dernier du fait du temps d'émission et de prise d'information du radar qui, une fois en marche, peut être à son tour détecté. Cela amène à une utilisation courte nécessitant un déplacement à la fin de la prise d'information.

ROEM

Le Renseignement d'Origine ÉlectroMagnétique (ROEM), à l'instar du radar, la détection électromagnétique nécessite un temps d'observation court suivi d'un déplacement en situation réelle. Le Groupe Léger de Guerre Électronique (GLGE) est une unité qui renseigne sur les activités radioélectriques dans le milieu environnant (hors téléphonie satellitaire et cellulaire). Elle alerte sur la détection et localisation de réseaux menaçants.

ROIM

Le Renseignement d'Origine Image est la collecte et l'analyse d'information visuelle. Dans notre cas, ces informations sont fournies par tout appareil permettant d'utiliser la photographie aérienne¹. Mais l'un des outils principaux pour le ROIM est la DRAC, soit une troupe au sol pouvant déployer un drone pour assurer une prise d'information visuelle durant 1H afin de combler les lacunes des connaissances sur la zone.

SAER

La Solution d'Aide à l'Exploitation du Renseignement (SAER) utilise une SGBDR (Système de Gestion de Base de Données Relationnelle) afin de permettre des requêtes pour aider à l'identification de troupes. Cet outil est dépendant des autres capteurs dans le sens où il faut au préalable un certain nombre d'informations afin de pouvoir réaliser une requête et compléter l'information grâce aux résultats fournis par le SAER.

4.4.3 Fiabilité et véracité de l'information

La doctrine militaire qualifie la fiabilité et la véracité de l'information collectée en 6 niveaux pour chacune des deux notions (représentées dans la Table 4.1).

La fiabilité correspond au niveau de confiance de l'information collectée par un capteur en fonction de sa capacité à analyser correctement cette information. Par exemple, un soldat reportant une information se voit attribuer une fiabilité par rapport à son expertise sur l'information envoyée et aussi son ancienneté ou son expérience.

La véracité définit la confiance sur la corrélation des informations retournées pour être sûr que l'information collectée soit vraie ou non. Une informa-

1. Les satellites ne sont pas pris en compte car l'intervalle temporel pour obtenir une information est trop grand pour être utilisable durant une situation de crise

tion corrélée par plusieurs sources a plus de chance d'être vraie que par une seule source.

Ces deux notations permettent d'avoir un indice global de confiance sur l'information reçue afin de savoir si oui ou non il est possible de travailler à partir de cette dernière. Cela permet de gérer la probabilité qu'un élément observé soit correctement qualifié et permet de travailler avec un niveau de confiance plus ou moins élevé pour réaliser l'évaluation de la menace.

TABLEAU 4.1 – cotation de la fiabilité et véracité d'une source d'information

Fiabilité de la source	Véracité de l'information
A - totalement fiable	1 - corroborée par d'autres moyens
B - habituellement fiable	2 - probablement vraie
C - assez fiable	3 - peut-être vraie
D - rarement fiable	4 - douteuse
E - non fiable	5 - improbable
F - la fiabilité ne peut être estimée	6 - la véracité ne peut être estimée

4.5 Conclusion

Dans ce chapitre nous avons pu :

- Voir que la définition de la menace était initialement vue dans un but de prévention en prenant en compte une dimension psychologique et comportementale des potentiels acteurs de la future menace.
- Envisager la menace comme une tâche de prédiction qui, contrairement au point précédent, permet de gérer la menace en fonction de l'intention d'un ennemi lors d'une attaque en cours.
- Développer les concepts du COI (Capacité, Opportunité et intention) qui sont trois principes clefs dans la modélisation de la menace.
- Introduire l'idée de propagation de menace - notamment dans un environnement topographique - basée sur la propagation de croyances.
- Définir la menace dans un cadre plus applicatif qui est celui de la doctrine militaire en rapport avec les expérimentations de cette thèse

Comme ce chapitre le présente, des premières solutions ont été proposées dans la littérature pour être en mesure de prédire la menace. Cependant, les problèmes de complexité combinatoire rendent la tâche laborieuse voire impossible du moins dans des problématiques en temps quasi-réel. De plus, les outils proposent généralement une vision trop simpliste concernant l'exposition d'une zone à une menace. Il n'est pas possible de définir la stratégie mise en place par l'ennemi de sorte à pouvoir anticiper le plus tôt possible sur les contre-mesures à prendre en place.

Ce sont ces deux problèmes majeurs que les contributions proposées vont tenter de traiter. L'optimisation du système d'évaluation de situation (et plus précisément de menace) de sorte à s'approcher d'une capacité d'analyser en temps quasi-réel, l'optimisation de l'utilisation des capteurs pour évaluer la situation et la capacité de définir la stratégie mise en place par l'ennemi.

Deuxième partie
Contributions théoriques

Un nouveau système d'évaluation de situations

De nombreux systèmes d'évaluation de situations (*Situation Awareness*, notés SA) ont vu le jour depuis les quarante dernières années. Chaque évolution apporte de nouveaux concepts sur la méthodologie nécessaire à la bonne réalisation d'une évaluation de situations. Cependant, les systèmes autonomes d'évaluation automatique de situations n'ont pas encore pu aboutir. Pour cela, la redéfinition ou spécification des modèles de SA doit encore avancer pour permettre la mise en place de l'ensemble des briques logicielles nécessaires à l'automatisation de cette tâche complexe.

5.1 Le système ASAAP

Suite à la veille sur le domaine de l'évaluation de situations (SA, 2), aucune solution logicielle ne permet l'automatisation de tâches d'évaluation de façon satisfaisante. Cette première contribution a donc été le résultat d'une réflexion sur les besoins et les manques pour mettre en place un tel système.

Le système ASAAP (*Automated Situation Awareness for Active Perception*), représenté dans la Figure 5.1, est composé de trois briques logicielles qui se succèdent de sorte à ce que la sortie (*output*) d'une brique soit l'entrée (*input*) de la suivante en terme architectural et algorithmique.

La majorité des systèmes vont chercher à savoir ce qu'ils veulent connaître pour savoir ce qu'ils veulent observer. C'est une approche experte classique où le choix des objets à observer se fait passivement par des fonctions classiques d'optimisations coût/utilité (perception passive).

L'originalité de ce système se trouve dans l'approche dite *bottom-up* de l'analyse de la situation. Ici, le système propose une approche inverse de per-

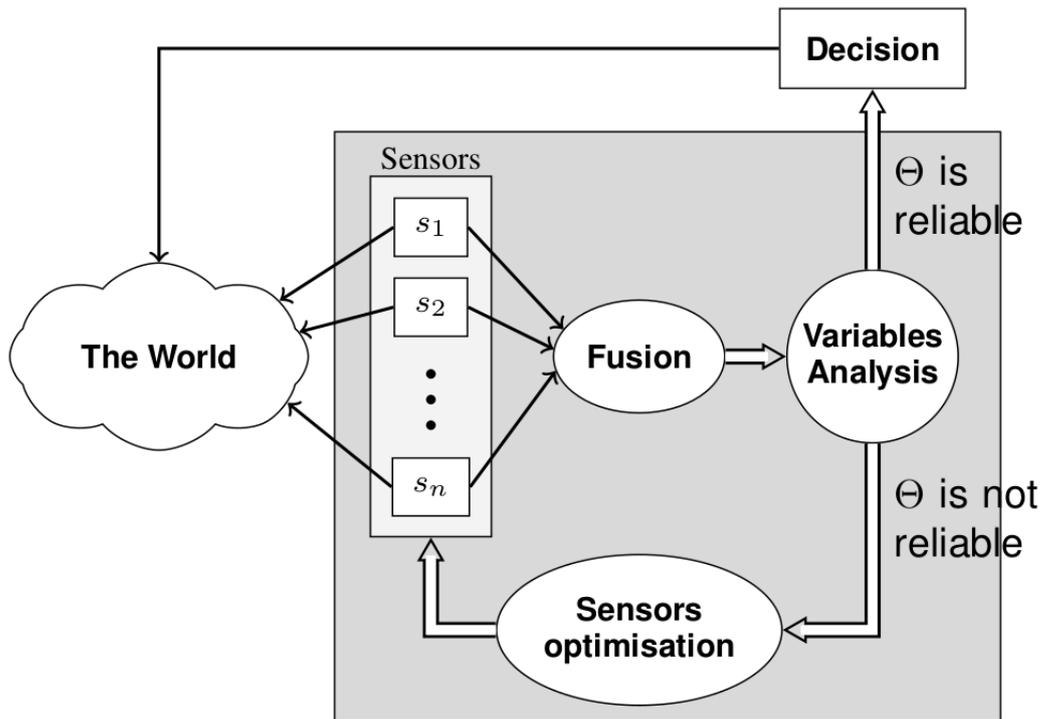


FIGURE 5.1 – Système ASAAP

ception active où les variables vont être analysées pour comprendre ce qu'il faut observer afin de maximiser le gain d'informations sur les hypothèses que l'on cherche à valider ou non pour l'évaluation de la situation.

De plus, le système ASAAP est un système qui permet à la fois d'évaluer la situation de façon automatisée mais aussi d'optimiser la gestion des capteurs pour savoir à chaque itération de temps quelle action doit réaliser chaque capteur.

La contribution de cette thèse repose sur la proposition du système ASAAP ainsi que les contributions réalisées dans les différentes briques afin de permettre à terme un système complet permettant l'évaluation de situation de façon automatisée.

La finalité de ce système est de permettre d'inférer une situation à évaluer tout au long de son déroulement et de fournir une image la plus précise et complète possible en temps quasi-réel. Le système permet également d'informer le preneur de décision (un opérateur humain) au moment où la situation est considérée comme connue avec suffisamment de confiance sur l'inférence réalisée afin que ce dernier comprenne qu'il peut travailler à partir des informations fournies par le système.

5.1.1 Brique de Fusion d'Informations

La brique de Fusion d'Informations est la première des trois briques du système ASAAP. L'objectif de cette dernière est de fusionner les informations reçues par l'ensemble des capteurs afin de mettre à jour les connaissances sur l'environnement.

Pour se faire, elle reçoit donc comme *input* les données de tous les capteurs (*Hard & Soft*) à disposition qui observent l'environnement où se déroule la situation à évaluer. La première étape consiste en la fusion des informations correspondant à l'étape de temps courante pour savoir si les entités observées par différents capteurs sont les mêmes ou non. Par exemple, si un tank est observé par un capteur s_i et un autre tank est observé par un autre capteur s_j , il est question de savoir si c'est le même ou un tank différent.

Pour cela, il existe tout un ensemble de fonctions de fusion décrites dans la partie état de l'art (Partie I). Cependant, il existe encore de nombreuses limites pour la fusion dite *Hard & Soft*.

Ensuite, vient la mise à jour des connaissances et l'inférence des états (en l'occurrence du réseau bayésien dynamique, noté DBN, représentant la situation). Cette étape consiste en une mise à jour classique des informations obtenues depuis t_0 à t_{i-1} en fonction des états observés à t_i .

L'*output* est une vision la plus complète possible de l'environnement tel qu'il est possible de le représenter via la succession d'observations depuis le début de la situation. Cet *output* est un DBN dans notre cas.

Cette partie n'a pas été développée au sein des travaux de cette thèse. Cependant, j'ai pu réaliser des travaux au sein d'Airbus Defense & Space qui ont mené à une contribution dans le domaine de la Fusion Hard & Soft [Vasnier et al., 2019]. Ces travaux pourront à terme être intégrés à la suite du processus de Fusion nécessaire au bon fonctionnement de cette brique.

5.1.2 Brique d'analyses des variables

L'analyse des variables de l'environnement correspond à la deuxième étape majeure du système ASAAP. Cette brique possède deux rôles : Celui de savoir lorsque les informations observées ou inférées permettent la prise de décision pour la situation à évaluer et celui d'être en mesure de définir un ensemble de variables prioritaires à observer pour améliorer la confiance sur la connaissance de la situation afin d'arriver plus vite à la capacité de décider. Elle prend pour *input* l'*output* de la brique précédente qui est un DBN.

La première étape de cette brique est donc de vérifier si la situation à évaluer est considérée comme suffisamment connue et sans ambiguïté pour que le preneur de décision (un opérateur humain) puisse être en mesure de

décider et agir sur l'environnement.

Deux cas de figure se présentent alors, le premier est lorsque la situation est considérée comme connue avec suffisamment de confiance sur les informations critiques et nécessaires à la prise de décision. Dans ce cas, le système s'arrête et annonce au décideur qu'il peut travailler avec la connaissance de la situation actuelle. Dans le second cas, la connaissance sur la situation est trop faible (ambiguë) et nécessite une nouvelle itération d'observations pour mieux l'évaluer (désambiguïser). S'ensuit une analyse des variables du DBN que nous avons choisi pour décrire la situation et pour savoir quelles seront les variables permettant d'obtenir le plus d'informations à la prochaine itération. Cela permet de prioriser l'information à observer, ce qui est crucial du fait des ressources limitées ne permettant pas l'observation de l'intégralité de l'environnement.

L'*output* généré est un ensemble de variables prioritaires considérées comme plus utiles que les autres au sein du DBN.

C'est sur cette brique que les travaux présentés dans cette thèse se sont focalisés. Ils sont présentés dans les chapitres suivants (Chapitre 6 et Chapitre 7).

5.1.3 Brique d'optimisation des capteurs

La brique d'optimisation des capteurs va utiliser l'*output* de la brique d'analyse des variables qui correspond à un ensemble de variables prioritaires à observer comme *input*. Le but va être d'optimiser l'utilisation des capteurs pour obtenir la plus grande quantité et la meilleure qualité d'information possible sur les variables les plus utiles.

L'*output* de cette brique est un ensemble d'associations de capteurs à des variables qu'ils devront observer à la prochaine étape de temps. Le choix des actions sur les capteurs est donc lui aussi automatisé pour permettre une utilisation optimale.

Dans un premier temps, la maximisation de l'utilisation des capteurs est réalisée sur uniquement les variables utiles. Et dans le cas où des capteurs resteraient disponibles après l'association de ces derniers aux variables les plus utiles, le même procédé peut être appliqué pour les utiliser sur les autres variables.

Des travaux ont été réalisés sur cette étape mais n'ont pas été menés à maturation pour être présentés comme contribution. L'idée est de représenter les capteurs et les variables dans un graphe d'association bipartite et d'y adapter le problème du Flot Maximal [Ford Jr, 1956] afin de maximiser différents paramètres. Les paramètres pris en compte sont la qualité de l'information par rapport à la précision d'un capteur sur le type d'observation qu'il

peut réaliser, la quantité et diversité d'informations qu'il peut obtenir pour une variable et si oui ou non il est en mesure d'observer une variable par le biais d'une action. Les premiers tests ont permis d'automatiser l'association capteurs/variables mais uniquement en prenant en compte une fonction d'utilité/coût à horizon $t + 1$. Ce travail fera l'objet de poursuites de la thèse.

5.2 Conclusion

Le système ASAAP est donc un système complet dans lequel nous avons focalisé nos recherches sur la deuxième brique d'analyse des variables. Cependant, d'autres travaux en parallèle avec Airbus Defense & Space ont été réalisés pour la brique Fusion et des travaux préliminaires ont été menés pour la brique d'optimisation des capteurs.

Des travaux sont encore nécessaires pour permettre à ce système d'être employé intégralement dans des premiers tests. Cependant, l'architecture globale a été définie et la veille scientifique pour chacune des briques a été réalisée.

CHAPITRE 6

L'analyse des variables utiles

L'analyse des variables utiles se base sur une approche d'approximation pour les réseaux bayésiens dynamiques (Chapitre 3 Section 3.2.3). Les mondes possibles et les possibilités combinatoires liées à une situation à évaluer étant explosifs en terme de complexité, le but est de travailler sur une structure locale du graphe afin de réduire le nombre de calculs nécessaires à l'évaluation.

Étant dans une problématique de ressources limitées (vis-à-vis des variables à observer) il est impératif d'être en mesure de définir quels sont les objets (e.g. entités ou zones) de l'environnement prioritaires à observer pour obtenir la meilleure information possible sur la situation. On parle de maximiser le gain d'information.

Pour cela, nous avons développé un outil qui précède la phase d'optimisation de l'utilisation des capteurs en identifiant quelles seront ces variables les plus informatives (i.e. variables les plus utiles) au sein de notre modélisation de l'environnement via les DBN.

En résumé, l'intuition derrière l'analyse des variables utiles est d'être en mesure à l'instant $t + 1$ de dire quelles seront les variables les plus informatives sur la situation pour la prochaine inférence afin de travailler sur un réseau local et de faciliter l'optimisation de l'utilisation des capteurs.

6.1 La fusion d'informations avec les Réseaux Bayésiens Dynamiques

Comme présentés dans l'état de l'art, les réseaux bayésiens dynamiques (DBN) représentent un outil idéal pour permettre l'évaluation de situation dans une problématique de représentation de la connaissance et l'inférence inhérente à cette dernière (Chapitre 3 Section 3.2.3).

En effet, l'héritage des modèles causaux permet de mettre en avant les dépendances causales entre entités dans l'environnement et les besoins d'inférence sur les croyances par rapport à l'état d'un monde partiellement observable [McAnally et al., 2018].

L'intérêt principal, et pour rappel, les DBN permettent une modélisation via une dimension temporelle. Cette dimension est représentée par des tranches temporelles discrétisées qui sont modélisées chacune par des réseaux bayésiens (notés BN). Chaque nœud représente une variable aléatoire et chacun des arcs représente la dépendance causale d'une variable envers une autre. De fait, l'inférence d'un DBN diffère de celle des BN et représente une distribution jointe telle que :

$$P(X_{1:T}) = \prod_{t=1}^T \prod_{i=1}^n P(X_i^t | \pi(X_i^t)) \quad (6.1)$$

où X_i^t est la $i^{\text{ème}}$ variable aléatoire à l'étape de temps t et $\pi(X_i^t)$ sont les parents de la $i^{\text{ème}}$ variable aléatoire à l'étape de temps t représentant l'état de ses parents à $t - 1$ comprenant lui-même.

La Figure 6.1 montre un exemple de DBN avec la représentation en graphe des dépendances entre variables aléatoires avec les arcs (dont celui de la variable elle-même à l'étape de temps précédente).

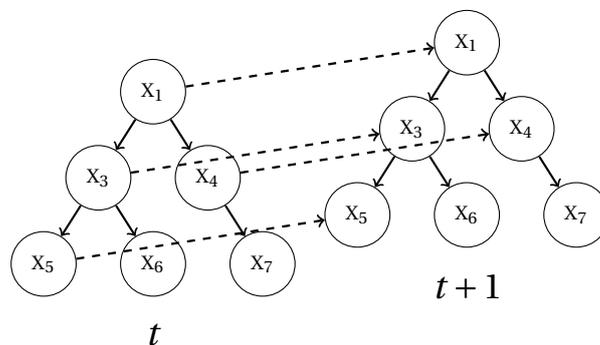


FIGURE 6.1 – DBN representation

Cette inférence est basée sur l'observation des variables à l'instant t qui permet de connaître l'état des variables observées et de propager la croyance sur chacune des variables.

6.2 Modélisation de l'environnement via les DBN

L'évaluation de situation (SA) comprend un ensemble d'hypothèses qui doivent être connues.

Définition 14. Une hypothèse correspond à un élément à monitorer pour la bonne compréhension d'une évaluation de situation. Cet élément est considéré comme étant une instance Haut-Niveau (voir Chapitre 2 Section 2.5.2) défini par un ensemble de variables et de relations entre-elles.

Par exemple, dans le cadre de l'évaluation de la menace de navires, une hypothèse correspond au niveau de menace d'un bateau. Il y a donc une hypothèse par bateau à observer. Dans le cas d'une catastrophe naturelle, les hypothèses pourraient être les risques de répliques d'un séisme, les zones endommagées, le nombre d'habitations à secourir, etc...

La SA est représentée par Θ qui correspond à un ensemble d'hypothèses tel que $\Theta = \langle \theta_1, \dots, \theta_k \rangle$ où θ_i qui décrit les éléments qui doivent être connus pour comprendre la situation évaluée. La Figure 6.2a décrit la représentation graphique de l'état de croyance sur la situation.

Chaque hypothèse θ_i est décrite par deux ensembles de variables. Le premier correspond aux variables observables $\mathcal{S} = \langle I_1, \dots, I_m \rangle$ qui peuvent être directement observées par les capteurs. Le second est celui des variables inférables $\mathcal{X} = \langle X_1, \dots, X_n \rangle$ qui ne peuvent pas être observées mais inférées à partir des variables observables dans \mathcal{S} qui décrivent la variable X_i . Chaque variable $X_i \in \mathcal{X}$ est décrite soit par une ou plusieurs variables dans \mathcal{X} , soit par une ou plusieurs variables dans \mathcal{S} . La Figure 6.2b représente ces dépendances permettant de décrire une hypothèse θ_i .

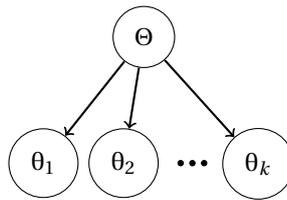
Par exemple, une hypothèse concernant la menace d'un navire peut être décrite par plusieurs variables aléatoires comme son chemin tel que $X_{path} \in \mathcal{X}$ décrite elle-même par la position, la vitesse et la direction qui sont trois variables dans \mathcal{S} .

Enfin, la modélisation comprend également un ensemble de capteurs $\mathcal{S} = \langle S_1, \dots, S_p \rangle$ décrits comme des variables aléatoires afin de représenter leur capacité à observer les variables dans \mathcal{S} . Un capteur possède un ensemble d'actions possibles représentées par $S_i^{\mathcal{A}} = \langle A_1, \dots, A_q \rangle$ et une action $S_i^{A_k}$ correspond à l'ensemble des variables observables que permet d'observer l'action A_k pour le capteur S_i .

Comme le montre la Figure 6.2b, un arc lie une variable observable I_j et un capteur S_i si et seulement si $I_j \in S_i^{A_k}$. Une action correspond par exemple à un mouvement physique (comme déplacer une caméra, orienter un radar, ...) ou à l'application d'un traitement algorithmique sur des données (reconnaissance d'objet, suivi d'objet, détection de groupe, ...).

Situation à évaluer

Éléments monitorés



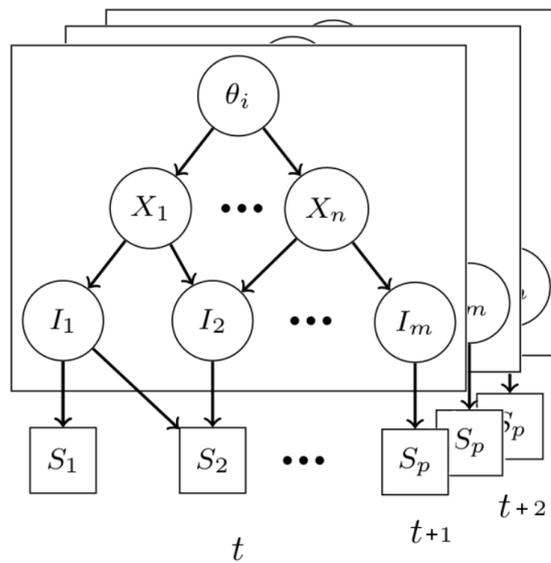
(a) Représentation de la situation à évaluer en graphe.

Hypothèses

Variables inférables

Variables observables

Capteurs



(b) Représentation d'une hypothèse via un graphe.

FIGURE 6.2 – Représentation de l'environnement via DBN.

La Figure 6.3 représente un exemple appliqué d'une hypothèse décrivant la menace d'un navire avec ses variables inférables et observables, ainsi qu'un ensemble de capteurs. Cet exemple est défini dans le cas d'usage maritime (9).

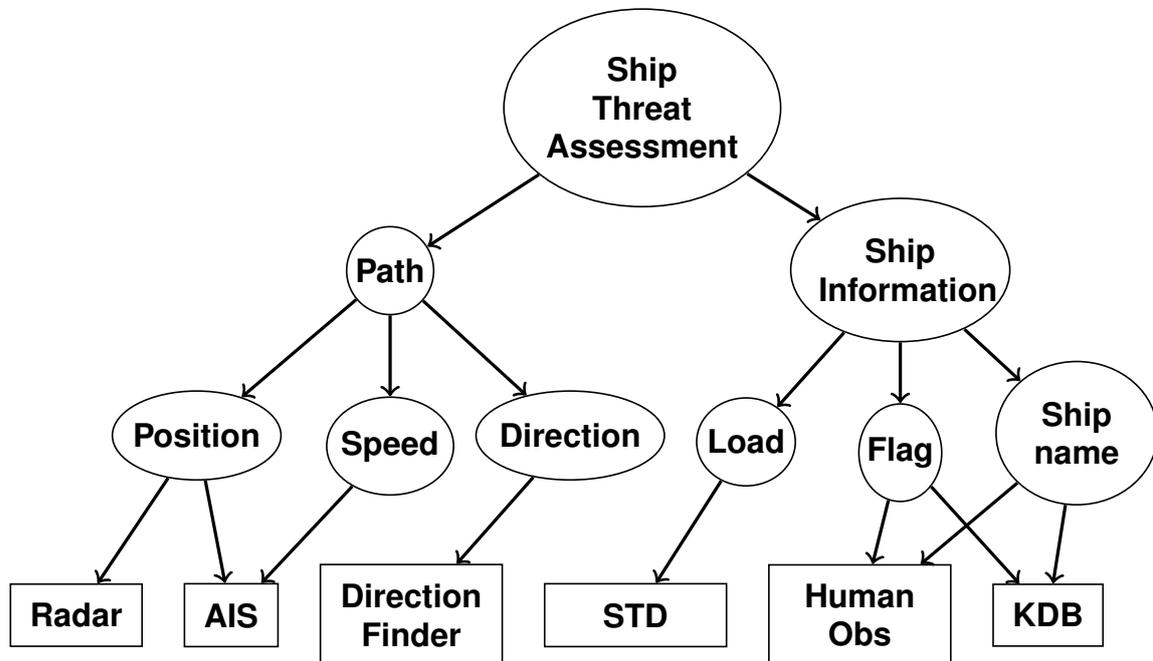


FIGURE 6.3 – Hypothèse θ_i décrite par son DBN

6.3 L'analyse des variables les plus utiles

L'environnement d'une situation à évaluer est décrit par un certain nombre de variables aléatoires comme montré précédemment. Les ressources d'acquisition, d'observation étant limitées, il n'est pas possible d'observer l'intégralité de ces variables. De plus, il n'est parfois pas utile de toutes les observer. L'objectif est de définir un sous-ensemble de variables prioritaires à observer pour améliorer la connaissance sur la situation de façon plus efficace.

L'analyse des variables les plus utiles se base sur l'étude des variables qu'il faudrait observer afin de maximiser le gain d'informations et faciliter ensuite l'optimisation de l'utilisation des capteurs à la prochaine étape de temps.

Plutôt que de simplement travailler sur les capteurs afin d'optimiser leurs observations comme les systèmes existants le proposent, l'analyse des variables va permettre de définir quelles variables sont les plus utiles à observer. Ce procédé cherche donc à mettre en place une mesure permettant de définir de telles variables.

6.3.1 Une variable utile

L'idée est de réussir à définir quelles sont les variables apportant une information de meilleure qualité si elle est observée à nouveau. Cela sous-entend de prédire l'utilité de l'observation d'une variable dans le futur. Pour cela, on définit des variables dites utiles en se basant sur ce que l'on espère obtenir à travers sa future observation.

Une variable utile (*Most Valuable Variable*, MVV) est donc définie telle que :

Définition 15. Une variable est considérée comme utile si elle est en mesure de fournir une plus grande quantité d'informations que les autres par le fait de réduire de façon plus conséquente l'incertitude sur les hypothèses de la situation à évaluer.

Sachant que dans un DBN les relations causales entre les variables sont connues, nous sommes en mesure d'estimer quel sera l'impact d'une meilleure connaissance de telle ou telle variable vis-à-vis de l'ensemble du DBN (et donc sur les hypothèses). L'intuition derrière ce procédé est de chercher quels nœuds fils du DBN sont en mesure de donner la meilleure qualité d'information en réduisant l'incertitude sur la croyance des états plutôt que de simplement appliquer l'inférence passivement sur le réseau.

On peut donc résumer l'objectif du processus par le fait d'obtenir une confiance suffisante sur chaque hypothèse θ_i de la situation Θ . La première étape consiste donc à déterminer si la situation est connue ou représentée avec une confiance suffisamment élevée pour travailler à partir des connaissances acquises.

Pour cela, le système utilise un seuil de confiance global à partir duquel une variable aléatoire est considérée comme ayant une croyance sur ses états avec une confiance suffisante. Chaque variable possède alors un score de confiance. Pour savoir si la connaissance sur la situation est suffisante, il faut donc que ce score pour chaque hypothèse de la situation dépasse ce seuil de confiance. Si toutes les hypothèses remplissent cette condition, il est alors légitime de considérer que le preneur de décision est en mesure de travailler avec les informations fournies par le système pour agir sur la situation.

Considérons Γ comme le seuil de confiance global, et $\gamma(X)$ le score de confiance de la variable aléatoire X (et $\gamma(\theta)$ celui d'une hypothèse). Du fait qu'un DBN soit intégralement constitué de variables aléatoires, l'entropie de Shannon est toute indiquée pour mesurer la quantité d'informations et donc de connaissances sur la distribution de probabilités en tant que mesure d'incertitude. L'entropie de Shannon est définie telle que :

$$H(X) = - \sum_{i=1}^n P(x_i) \log P(x_i) \quad (6.2)$$

Où x_i est une valeur possible de la distribution $X = \{x_1, \dots, x_m\}$ et $P(x_i)$ est la probabilité que la variable X soit dans l'état x_i . L'entropie $H(X)$ correspond donc à notre score de confiance $\gamma(X)$. Ce score représente le "désordre" de l'information sur la variable X qui augmente au plus la distribution de probabilités de X s'approche de l'équiprobabilité. Dans le cas où la valeur de X est sûre (une valeur de la distribution valant 1 et toutes les autres à 0), le score vaut alors 0. L'objectif est de réduire ce désordre et de discriminer les probabilités des états de X . Si le score diminue, la confiance sur la connaissance de l'information augmente.

Les variables utiles seront donc l'ensemble des variables avec un score de confiance supérieur au seuil de confiance global tel que $\gamma(X) > \Gamma$.

Du fait que le concept de perception active cherche à optimiser l'utilisation des capteurs, il n'est nécessaire de considérer comme MVV uniquement les variables observables car ce sont les seules variables avec lesquelles peuvent interagir les capteurs.

Formellement, considérons $\mathcal{U} = \{U_1, \dots, U_l\}$ comme l'ensemble des MVV. Une variable observable devient une variable utile si elle respecte les propriétés suivantes :

Propriété 1. $\mathcal{U} \neq \emptyset$ si et seulement si $\exists \theta_i \in \Theta, \gamma(\theta_i) \leq \Gamma$.

Propriété 2. L'ensemble \mathcal{U} est défini tel que $\mathcal{U} \subseteq \mathcal{I}$.

Propriété 3. $I_j \in \mathcal{U}$ si et seulement si il existe au moins un chemin causal depuis une hypothèse $\theta_i \in \Theta, \gamma(\theta_i) > \Gamma$ vers la feuille du DBN I_j où $\forall X \in X_{path}, \gamma(X) > \Gamma$ avec X_{path} représentant l'ensemble des variables inférables par lesquelles passe le chemin.

Propriété 4. $I_j \in \mathcal{U}$ si et seulement si $\gamma(I_j) > \Gamma$.

6.3.2 Processus d'analyse au sein d'un DBN

Comme dit précédemment, si $\forall \theta_i \in \Theta$ et $\gamma(\theta_i) \leq \Gamma$ alors la situation à évaluer est considérée comme connue avec une confiance suffisante pour prendre une décision et le système le notifie à l'agent humain. Dans ce cas, le système n'analyse aucune autre variable. Dans le cas contraire, le système lance une analyse sur les variables pour trouver les MVV.

Dans un premier temps, le processus va d'abord calculer le score de chaque variable $X_i \in \mathcal{X}$ correspondant aux variables inférables. Dans le cas où $\gamma(X_i) \leq \Gamma$, il n'est alors pas nécessaire d'observer ses nœuds fils (jusqu'aux variables observables) donc l'algorithme s'arrête afin de ne pas calculer leur

score de confiance inutilement. Mais si le score de confiance n'est pas suffisant, alors le système va vérifier celui de tous les nœuds fils de la variable X_i et ainsi de suite. Si le dernier nœud fils (c'est à dire une feuille du DBN) est atteint et que l'incertitude sur son état est trop forte, alors la variable $I_j \in \mathcal{I}$ devient une variable utile.

L'Algorithme 1 décrit cette analyse des MVV. Cette fonction récursive prend une hypothèse en entrée et un ensemble vide qui correspondra aux MVV du DBN pour paramètres. Si la fonction atteint un noeud qui n'a pas de fils et dont le score de confiance est supérieur au seuil, alors il l'ajoute à l'ensemble de MVV.

Algorithm 1 MVV analysis algorithm

```

1: procedure RECURSIVEMVVANALYSIS(node,  $\mathcal{V}$ ,  $\Gamma$ )
2:   if hasNoChild(c) and  $\gamma(c) < \Gamma$  then
3:      $\mathcal{V} \leftarrow \mathcal{V} + \{node\}$ 
4:   else
5:     if  $\gamma(node) < \Gamma$  then
6:       for each child  $c \in childrenOf(node)$  do
7:         recursiveMVVAnalysis(c,  $\mathcal{V}$ )
8:       end for
9:     else
10:      return
11:    end if
12:  end if
13:  return
14: end procedure

```

La Figure 6.4 illustre le procédé à travers un exemple théorique. Dans cet exemple, la variable inférable X_3 est considérée comme fiable grâce à son score γ . Donc la variable I_1 n'est pas intéressante à observer car elle ne permet d'inférer que X_3 qui n'a pas besoin de plus de connaissances sur son état. Cependant, la variable I_2 reste utile car même si elle décrit X_3 , elle décrit aussi X_4 qui reste suffisamment incertaine pour devoir encore être inférée à partir de sa variable observable. De même pour I_3 qui décrit X_2 . Ici, l'ensemble de MVV est donc $\mathcal{U} = \{I_2, I_3\}$.

Une fois l'ensemble de MVV défini, les capteurs sont orientés de sorte à obtenir la meilleure couverture sur ses variables. Ici, les variables qui ne sont pas dans \mathcal{V} sont considérées comme ne valant pas la peine d'être observées. Ce focus sur les MVV permet d'économiser l'utilisation des ressources tout en maximisant le gain d'informations lors de l'observation à la prochaine étape de temps

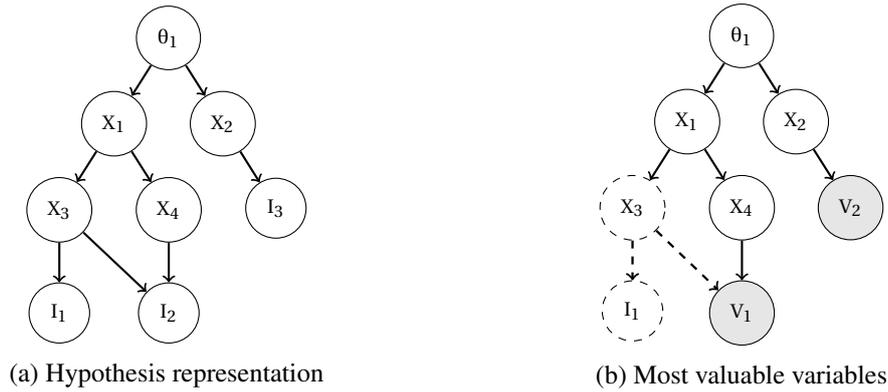


FIGURE 6.4 – Exempmlle de processus d'analyse des MVV.

Afin de maximiser le gain d'informations, le concept naïf choisi ici est de choisir les variables où la confiance est la plus basse comme les plus prioritaires à observer. Considérons $X_i^{\mathcal{S}}$ comme l'ensemble des capteurs pouvant observer X_i . Sachant que $\epsilon(S_i^{\mathcal{A}_k})$ correspond au niveau de confusion normalisé¹ du capteur via ses actions \mathcal{A}_k . Pour toute variable $v \in \mathcal{V}$, le capteur choisi pour observer v est $\operatorname{argmin}_{s \in X_i^{\mathcal{S}}, a \in s^{\mathcal{A}}} \epsilon(s^a)$. Le processus d'attribution des capteurs continue jusqu'à ce que tous les capteurs soient associés à une MVV. L'Algorithme 2 décrit ce procédé. L'ensemble des MVV étant trié par ordre ascendant sur le score de confiance permettant ainsi de gérer les MVV avec le score du plus bas au plus haut.

Algorithm 2 Variables attribution to sensors

```

1:  $\mathcal{V} \leftarrow$  set of MVV from Algorithm 1
2:  $\mathcal{V} \leftarrow \operatorname{sortScoreAscendingOrder}(\mathcal{V})$ 
3:  $\mathcal{SV} \leftarrow$  set of mapping between  $v \in \mathcal{V}$  and  $s \in \mathcal{S}$ 
4: for each variable  $v \in \mathcal{V}$  do
5:    $\operatorname{bestSensor} \leftarrow$  first sensor of  $\mathcal{S}$ 
6:   for each sensor  $s \in v^{\mathcal{S}}$  do
7:     for each action  $a \in s^{\mathcal{A}}$  do
8:       if  $\epsilon(s) < \epsilon(\operatorname{bestSensor})$  then
9:          $\operatorname{bestSensor} \leftarrow s$ 
10:      end if
11:    end for
12:  end for
13:   $\operatorname{SV} \leftarrow \operatorname{SV} + \operatorname{pair}(v, \operatorname{bestSensor})$ 
14: end for
15: return  $\operatorname{SV}$ 
    
```

1. Le niveau de confusion normalisé correspond à l'imprécision du capteur.

Dans le cas où $|\mathcal{S}| < |\mathcal{V}|$, toutes les MVV ne pourront pas être observées, mais la maximisation du gain d'informations permettra malgré tout de prioriser les MVV entre-elles. Dans le cas où $|\mathcal{S}| > |\mathcal{V}|$, les capteurs restants pourront observer des variables $X \notin \mathcal{V}$ avec la même priorité sur le score de confiance.

Enfin, il est important de noter qu'à l'initialisation d'un cas d'usage SA, toutes les variables observables sont considérées comme des MVV. Dans ce cas, l'utilisation des capteurs sera optimisée en fonction des variables qui sont atteignables par les capteurs et via une fonction d'utilité/coût par rapport à la précision et la capacité du capteur à observer une variable. Les associations capteurs/variables obtenant le meilleur score utilité/coût sont choisies en priorité jusqu'à ce que chaque capteur soit associé à une variable de la même façon qu'expliqué précédemment pour l'Algorithme 2.

Cette fonction peut prendre notamment en compte pour l'utilité sa précision sur l'observation de la variable et la quantité d'informations qu'il peut obtenir s'il observe cette variable. Le coût lui peut être représenté par la capacité d'un capteur à observer la variable à $t + 1$, ou encore par le coût (de déplacement ou d'activation) nécessaire pour l'observation de la variable s'il peut l'observer.

6.4 Conclusion

L'analyse des MVV procède de l'école des algorithmes exacts (voir 3 Section 3.2.3.1) en terme d'inférence. Cette analyse permet de travailler sur un sous ensemble du DBN afin de réduire la complexité de l'exploration du graphe pour trouver quelles seront les variables les plus utiles à observer à $t + 1$. Il est donc ici question d'une prédiction sur l'utilité d'une variable à horizon $H = 1$.

Cependant, il reste à travailler l'optimisation des capteurs qui peut être vue comme un problème d'association de graphes bipartis. Des premières expérimentations ont été réalisées sur l'idée de la maximisation des flots à travers un graphe, mais ces derniers méritent d'être approfondis et étudiés dans le futur.

CHAPITRE 7

Propagation de menace

7.1 Introduction

Cette autre contribution sur les travaux de cette thèse se focalise sur la propagation de menace. Comme présentée dans l'état de l'art, l'évaluation de situation (SA) est un problème complexe et le cas des situations de crise apporte des contraintes fortes aussi bien temporelles que de ressources (d'observations). Un opérateur humain doit, dans ce cadre, prendre des décisions critiques rapidement malgré un nombre de ressources d'acquisition d'informations limité. Il faut donc proposer un système de représentation des informations fiables.

Cette contribution s'est focalisée sur le SA à travers le domaine du renseignement dans des situations de crise telles que les théâtres d'opération. Une étude dans un workshop [Hamilton et al., 2002] résume bien les défis et les problématiques qui nécessitent d'être traitées dans ce domaine.

Ces travaux se sont basés sur la doctrine militaire ([PFT RENS, 2016] et [RENS, 2016]) pour proposer un système expert de représentation de la connaissance (KR) sur lequel il est possible d'appliquer une propagation de menace afin de définir l'objectif et la stratégie de l'adversaire.

Différents travaux ont proposé des approches via la théorie des jeux mais la problématique du SA à travers l'évaluation de la menace est très peu ou mal abordé [Le Guillarme, 2016]. Il n'existe à vrai dire pas encore de systèmes satisfaisants permettant de prédire la menace.

L'idée à travers ces travaux est de proposer une modélisation propre aux système de SA dans le cadre militaire avec un système de propagation de menace permettant de prédire les zones qui seront menacées en fonction des

informations récupérées sur l'ennemi.

7.2 Modélisation du problème à travers un graphe topologique

Le SA à travers les théâtres d'opérations militaires cherche à obtenir des informations sur les troupes ennemies et leurs déplacements. Le but dans le cadre d'une attaque est d'être en mesure d'anticiper quelles seront les zones que l'ennemi va attaquer. Pour cela, il faut être en mesure d'observer au mieux les déplacements de ses troupes afin de comprendre la stratégie que ce dernier cherche à mettre en place.

L'environnement considéré est donc un environnement topologique dans lequel des troupes vont se déplacer pour chercher à atteindre un ou plusieurs points spécifiques. Le but est donc de proposer une modélisation générique de l'environnement correspondant aux besoins opérationnels permettant de jouer des scénarios à la fois plausibles et crédibles.

7.2.1 Définition de l'environnement

Pour décrire l'environnement à modéliser, nous nous plaçons dans le cadre d'une attaque d'un pays A vers un pays B. L'attaquant cherche à pénétrer la frontière du défenseur en utilisant différents chemins possibles pour arriver aux différentes zones d'attaques.

Les services de renseignement définissent des Zones d'Informations Prioritaires (notées HPIZ pour *High Priority Information Zone*) sur le champ de bataille correspondant aux zones de bifurcations possibles pour les troupes ennemies (c'est à dire les croisements). Les capteurs disponibles du défenseur doivent collecter les informations sur ces différentes zones afin de comprendre quels chemins et *a fortiori* stratégie l'ennemi compte adopter pour réussir son assaut.

Ici, comprendre la stratégie de l'ennemi consiste à trouver quelle(s) zone(s) il compte attaquer et pour cela, quel(s) chemin(s) il compte emprunter. Les zones d'attaques (AP pour *Attack Point*) doivent être protégées et le preneur de décision doit rapidement comprendre comment disposer ses troupes pour optimiser sa défense.

Afin d'évaluer le plan d'attaque de l'ennemi, le système "expert" doit détecter et décrire l'évolution de la menace durant les différentes phases de l'attaque. La menace correspond à la façon dont les troupes ennemies vont être déplacées et donc à quel point les différentes AP sont menacées en fonction du chemin emprunté. Une compagnie est définie comme un ensemble

d'unités militaires avec un rôle et une force de destruction spécifiques. Plus la force de la compagnie est élevée, plus sa menace est forte.

L'environnement est donc défini par des zones que traversent des chemins et des routes. Conséquemment, la meilleure représentation de cela est un graphe. Nous considérons donc un Graphe Dirigé Acyclique (DAG) $G = \{V, E\}$ avec V l'ensemble des nœuds et E l'ensemble des arcs, qui représentent conjointement un graphe topologique (comme le montre la Figure 7.1).

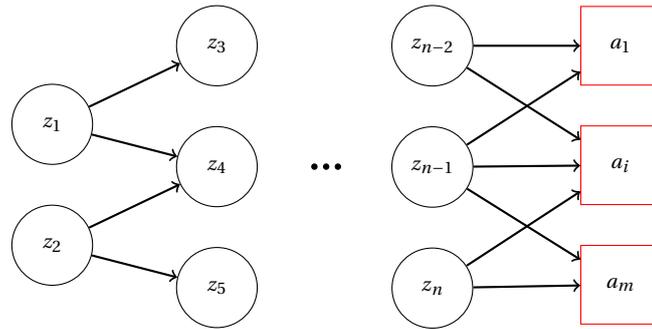


FIGURE 7.1 – Exemple de graphe topologique

Soit $Z = \{z_1, \dots, z_n\}$ l'ensemble des HPIZ tel que $Z \subseteq V$ et $\forall z \in Z, \pi(z) \neq \emptyset$ avec $\pi(z)$ les nœuds fils z représentant l'ensemble des zones accessibles depuis z .

Soit $A = \{a_1, \dots, a_m\}$ l'ensemble des AP tel que $A = V \setminus Z$ et $\forall a \in A, \pi(a) = \emptyset$, étant donné que les AP représentent les feuilles du graphe en les zones finales que l'ennemi compte atteindre.

Étant donné E l'ensemble des arcs tel que $\forall e \in E, e^{(u \rightarrow v)}$ est le chemin entre les nœuds $u, v \in V$ décrivant la possibilité pour des troupes d'aller de u vers v . Chaque arc e possède un poids noté $w_e = [0, 1] \in \mathbb{R}$ correspondant à la probabilité qu'une compagnie prenne ce chemin. La somme de tous ces arcs sortants depuis le nœud v , noté $w_{e^{z^+}}$ vaut 1.

Chaque arc possède également un type T_e caractérisant la difficulté de le traverser. Cela peut correspondre par exemple à une forêt, une route, une montagne ou une rivière par exemple (étant plus ou moins difficiles à traverser en fonction de la capacité de la compagnie).

Les phases de l'attaque sont définies comme suit : $P = \{p_1, \dots, p_k\}$ un ensemble de phases avec p défini tel que $p \subseteq V$ sachant $\forall p \in P \setminus p_k \subseteq Z$. La phase p_1 correspond à tous les nœuds racines tels que $\forall z \in Z, u(z) = \emptyset$ avec $u(z)$ les parents du nœuds z . Les phases p_2 jusqu'à p_{k-1} sont définies par $p_i = \bigcup_{z \in p_{i-1}} \pi^*(z)$ avec $\pi^*(z) = \pi(z) \setminus z \in p_{i-1}$. Et enfin, $p_k = \{A\}$ contient toutes les AP.

Les troupes ennemies sont décrites telles que $C = \{c_1, \dots, c_q\}$ un ensemble de compagnies. Chaque compagnie est décrite par un type T_c (infanterie, tanks, artillerie, ...). Le type d'une compagnie comprend tout d'abord un

score de menace spécifique $TS(c) \in \mathbb{N}$ représentant son rôle et sa force de destruction, et deuxièmement, un index de traversabilité, $Cr(c) = [0, 1] \in \mathbb{R}$ dépendant du type de chemin T_e emprunté. Un indice de traversabilité valant 0 représente l'impossibilité pour la compagnie de traverser le chemin.

7.2.2 Définition de la menace

A travers ce réseau topologique et après avoir décrit formellement ce qui le compose, la menace peut être définie elle aussi formellement.

Toutes les compagnies présentes dans une HPIZ z à un instant t sont notées C_z^t , qui est un ensemble vide si aucune compagnie ne s'y trouve. Le score de menace à l'instant t de la zone est alors défini tel que :

$$M(z_i)^t = \sum_{c_k \in C_{z_i}^t} TS(c_k) \quad (7.1)$$

La fonction de transition d'une zone z_i vers une zone z_j est donnée par la matrice de transition $T(c_k \in C_{z_i}^t, \pi(z_i))$ qui retourne toutes les probabilités de transition, notées $P(c^{z_i \rightarrow z_j})$, depuis z_i vers un de ses enfants $z_j \in \pi(z_i)$. La probabilité de la transition est définie par :

$$P(c^{z_i \rightarrow z_j}) = w_e^{(z_i \rightarrow z_j)} \cdot Cr(c) \cdot TS(c) \quad (7.2)$$

Ceci correspond à une première définition de ce qu'est la menace en fonction des troupes ennemies repérées.

7.3 Un système de propagation de menace automatisé

Nous allons maintenant voir comment le système "expert" développé à travers ces travaux va permettre d'automatiser la propagation de menace au fur et à mesure de l'évaluation de la situation afin de montrer la stratégie que l'ennemi va appliquer et quelles seront la ou les zone(s) attaquée(s).

7.3.1 Une approche pessimiste

La propagation de menace considérée ici se base sur une approche pessimiste. Cette méthode admet le pire des cas lors d'une attaque, c'est à dire un scénario où l'ennemi va chercher à se comporter de façon optimale en cherchant à générer les plus gros dommages possibles au défenseur (telle qu'une approche min/max dans un jeu).

L'hypothèse subséquente est de considérer que l'ennemi va constamment chercher à aller de l'avant et se déplacer vers les AP sans chercher à revenir en arrière. Et il va chercher également à emprunter le chemin le plus optimal en fonction des zones qu'il compte attaquer afin de réaliser une attaque éclair.

L'idée est donc de calculer la menace générée par chacune des compagnies selon tous les chemins qu'elles peuvent prendre et propager cette menace. Un **monde possible** est alors généré depuis la combinatoire de chaque **mouvement non-concurrent** des compagnies observées. Un monde possible est une représentation de l'environnement (tel que défini précédemment) à $t + 1$ considérant donc le mouvement possible des compagnies au pas de temps suivant avec la propagation de la menace correspondant sur chaque zone (HPIZ et AP).

Un mouvement non-concurrent représente toutes les combinaisons possibles de chaque compagnie chaque fois qu'une compagnie est présente dans une et une seule zone qui lui est accessible.

Ensuite, le système compare la menace globale (menace totale sur chaque AP) de chacun de ces mondes possibles et les plus hauts scores de menace représentent les scénarios futurs les plus plausibles que l'ennemi pourra adopter.

7.3.2 Définition formelle du modèle

La propagation de menace commence par les nœuds racines tels que $\forall z \in Z$ sachant que $u(z) = \emptyset$. La propagation va ensuite vers leurs enfants $\pi(z)$ et ainsi de suite pour chaque phase jusqu'aux AP.

La propagation de menace est calculée après avoir pris en compte tous les mouvements potentiels pour chaque compagnie à $t + 1$ afin d'estimer la plus haute menace qu'elles peuvent générer. Mais étant donné qu'une compagnie ne se comporte pas forcément de la façon la plus rationnelle (i.e. pas la plus optimale possible) ou qu'il peut y avoir des informations cachées à l'observateur, le modèle propose un ensemble de stratégies appelées les **k-best stratégies** afin d'évaluer plusieurs possibilités avec chacune une forte probabilité.

La propagation est donc réalisée à $t + 1$ et la propagation de menace résultante depuis une HPIZ z_i vers une autre zone (HPIZ ou AP) z_j , notée $Prop(z_i)^{t+1}$, est alors calculée comme il suit :

$$Prop(z_i)^{t+1} = P(z_i \rightarrow z_j) \cdot \overline{Cr(C_{z_i}^{t+1})} \quad (7.3)$$

Avec $P(z_i \rightarrow z_j)$ la probabilité de prendre le chemin depuis z_i vers z_j . Donc le score de menace total résultant de z_j à l'étape de temps $t + 1$ est calculé comme :

$$M(z_j)^{t+1} = \text{prop}(z_i)^{t+1} + M(z_j)^t \quad (7.4)$$

Qui représente les mouvements des compagnies de z_j avec $M(z_j)^t$ le score actuel à t de z_j . La menace prend en compte la probabilité des compagnies d'aller d'une zone à l'autre et aussi la moyenne de l'index de traversabilité de toutes les compagnies incluses dans le mouvement pris en compte dans ce monde possible (ainsi que le score global de menace) tel que :

$$\overline{Cr(C_{z_i}^{t+1})} = \frac{\sum_{c_k \in C_{z_i}^{t+1} \cup Cz \dots \rightarrow z_i^{t+1}} (TS(c_k) \cdot Cr(c_k))}{|C_{z_i}^{t+1} \cup Cz \dots \rightarrow z_i^{t+1}|} \quad (7.5)$$

Avec $Cz \dots \rightarrow z_i^{t+1}$ toutes les compagnies dans tous les nœuds après le mouvement qui peuvent atteindre z_i depuis la racine. Cela inclut donc toutes les troupes pouvant atteindre z_i depuis ses parents $\dagger(z_i)$ et leurs parents jusqu'aux nœuds racines.

Formellement, la propagation de menace est représentée par la formule suivante :

$$M(c_k, z_j) = TS(c_k) * P(z_c \rightarrow z_j) * Cr(c_k^{z_c \rightarrow z_j}) \quad (7.6)$$

Dans laquelle z_c est la HPIZ où la compagnie se trouve à $t + 1$ et $z_c \rightarrow z_j$ représente toutes les HPIZ traversée depuis z_c jusqu'à z_j . Ce score est calculé pour chaque compagnie et pour chaque zone qu'elle peut atteindre.

Pour éviter tout comportement irrationnel potentiel de compagnies, la propagation considère une pénibilité (ou un score de fatigue) d'avoir traverser un chemin de t à $t + 1$. Si ce paramètre n'est pas pris en compte à travers le modèle, les compagnies ont tendance à traverser des terrains vraiment difficiles sans aucune pénalité vu que la récompense pour traverser un environnement peut permettre d'obtenir un meilleur score de menace sur les AP si le coût de la traversée après t n'est pas prise en compte. Donc le score de menace d'une compagnie à $t + 1$ est représenté par :

$$M(c_k^{t+1}) = TS(c_k) * Cr(z_i^t \rightarrow z_i^{t+1}) \quad (7.7)$$

Avec z_i la position de c_k à t et z_i^{t+1} sa position à $t + 1$. Il est important de noter que cet ajout n'empêche pas une compagnie de prendre un chemin laborieux si cela améliore la menace potentielle et représente un mouvement plus rationnel.

Chaque combinaison de ces mouvements potentiels est ensuite propagée pour chaque compagnie et pour chaque mouvement non-concurrent de toutes les compagnies, un monde possible Φ à l'étape de temps $t + 1$ est généré où la menace globale de ce monde est calculée telle que :

$$M(\Phi) = \sum_{a_i \in \Phi} M(a_i) \tag{7.8}$$

Il en résulte un score qui permet de comparer pour chaque monde Φ le plus haut score de menace possible tel qu'on l'imagine au moment de l'attaque sur les AP (comme le montre la figure 7.2). Depuis ces mondes possibles, le système est en mesure d'évaluer quelle est la stratégie la plus susceptible d'être appliquée par l'ennemi et de proposer les k-best stratégies.

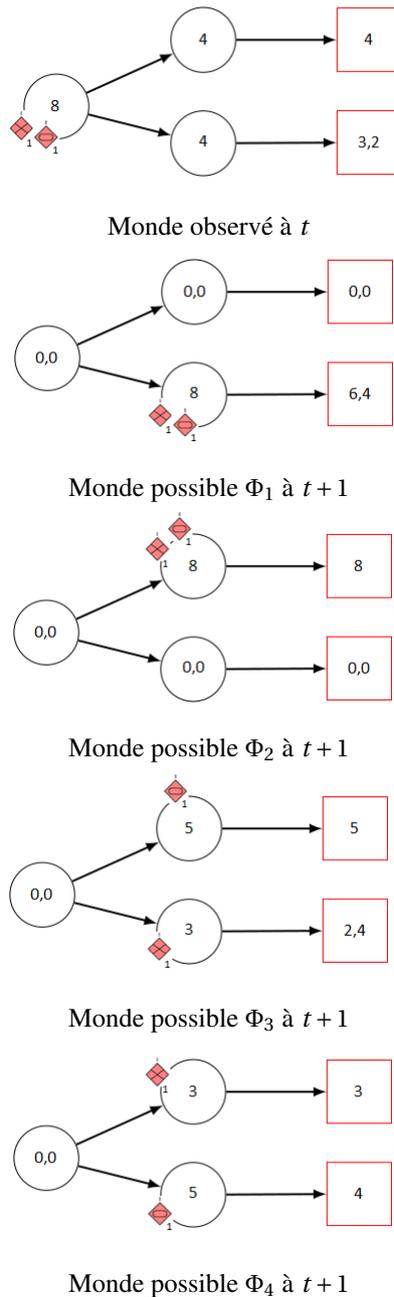


FIGURE 7.2 – Exemple de propagation de menace sur une carte de chaleur de menace.

La carte de l'environnement résultante pour chaque monde correspond à

une **carte de chaleur de la menace** permettant ainsi de comprendre facilement pour un opérateur humain quels chemins vont être empruntés et quelles zones sont les plus exposées.

7.3.3 Processus algorithmiques

L'implémentation nécessite de calculer une combinatoire de mouvements non-concurrents pour chaque compagnie (i.e. les combinaisons qui peuvent exister au sein d'un même monde à une même étape de temps afin que les compagnies ne puissent pas être présentes dans plusieurs zones). Cependant, même si la complexité augmente avec le nombre de zones accessibles et le nombre de compagnies, dans tous les cas d'usage étudiés, ces deux paramètres n'atteignent jamais un nombre de zones ou de compagnies empêchant de générer tous les mondes possibles.

La génération des mondes possibles est réalisée telle que le décrit l'Algorithme 3. Le nombre de mondes possibles renvoyés correspond au nombre voulu de *k*-best stratégies par l'opérateur humain. Les résultats sont triés en ordre décroissant afin de prioriser les stratégies avec le plus haut score de menace globale selon l'Équation 7.8.

Algorithm 3 Generation of all potential worlds

```

1: PotentialWorlds ← ∅
2: for each HPIZ  $z \in Z$  do
3:   Combinations ← generateAllMovementCombinations()
4:   for each combination  $comb \in C$  do
5:     potentialWorld ← generateWorldFrom(comb)
6:     propagateThreat() ▷ see Algorithm 4
7:     PotentialWorlds ← PotentialWorlds ∪ potentialWorld
8:   end for
9: end for
10: NonConcurrentWorlds ← combineNonConcurrentWorldsFrom(PotentialWorlds)
11: sortByHighestThreatScore(NonConcurrentWorlds)
12: return NonConcurrentWorlds

```

En application, la propagation de menace est calculée comme le montre l'Algorithme 4. La menace est propagée depuis les nœuds racines jusqu'aux AP. Et seules les zones avec des compagnies sont prises en considération afin que la fonction ne prenne en compte que le score de menace de ses parents et la propage pour tous ses enfants (*flooding*).

Algorithm 4 Threat Propagation

```

1: for each phase  $p \in P \setminus p_k$  do
2:   for each HPIZ  $z \in p$  do
3:     if  $z$  is a root node then
4:       threat  $\leftarrow$  sumCompaniesThreat()            $\triangleright$  see Equation 7.1
5:        $z$ .threatScore  $\leftarrow$  threat
6:     end if
7:     for each children  $child \in \pi(z)$  do
8:       threat  $\leftarrow$  propagateThreatFrom( $z$ )        $\triangleright$  see Equation 7.6
9:        $child$ .threatScore  $\leftarrow$  threat
10:    end for
11:  end for
12: end for

```

7.4 La menace à horizon défini

Une fois la carte de chaleur de menace disponible afin de monitorer la situation, l'opérateur humain a également besoin de savoir quand l'attaque est susceptible de se produire. Pour se faire, les experts ont besoin de comprendre comment la menace globale de chaque zone se diffuse à travers les prochaines étapes de temps jusqu'au moment où les troupes ennemies arriveront à leur cible.

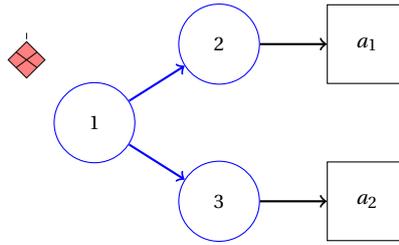
Considérant H comme l'horizon maximal des évènements (ici, le moment où l'ennemi atteindra les AP). Soit h l'horizon des évènements à un temps spécifique auquel nous voulons connaître la propagation potentielle de la menace.

Sachant que $Vel(c)$ est la vitesse d'une compagnie c représentant la distance que c peut traverser en une itération de temps, et $Dist(z_i \rightarrow z_j)$ est la distance entre les zones z_i et z_j basée sur la même unité que $Vel(c)$, nous notons $Zones(c)^{t+h}$ l'ensemble des zones que la compagnie c peut atteindre à l'horizon h . Inversement, toutes les compagnies pouvant atteindre une zone z sont notées telles que $Comp(z)^{t+h}$ à l'itération de temps $t+h$.

La Figure 7.3 montre un bref exemple théorique avec $Vel(c) = 1$ et pour chaque zone z_i et ses enfants z_j , $Dist(z_i \rightarrow z_j) = 1$. La compagnie présente dans z_1 peut atteindre toutes les zones à l'horizon H tel que $Zones(c)^{t+H} = [z_2, z_3, a_1, a_2]$ et pour $h = 1$, $Zones(c)^{t+h} = [z_2, z_3]$.

La propagation de menace peut donc être définie telle que :

$$M(c_k)^{t+h} = M(c_k^{t+1}) \cdot e \quad (7.9)$$


 FIGURE 7.3 – Illustration de zone atteignable par une compagnie selon $Vel(c)$.

$$\epsilon = \begin{cases} 1, & \text{if } Dist(z_c \rightarrow z_j) \leq Vel(c) \cdot h \\ 0, & \text{otherwise} \end{cases} \quad (7.10)$$

Avec $M(c_k^{t+1})$ de l'Équation 7.7 et $Dist(z_c \rightarrow z_j)$ l'ensemble des arcs traversés depuis la zone z_c où se trouve la compagnie c jusqu'à z_j tel que :

$$Dist(z_c \rightarrow z_j) = \sum_{d \in z_c \rightarrow z_i \cup \dots \cup z_{j-1} \rightarrow z_j} Dist(d) \quad (7.11)$$

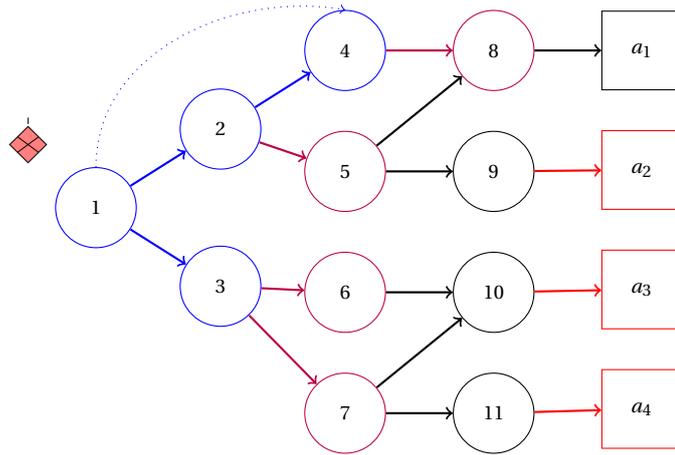
Dans le cas où plusieurs chemins permettent d'atteindre z_j depuis z_c , la seule distance qui nous intéresse est celle du plus court chemin vu que le seul but est de savoir si une zone est atteignable par la compagnie et si la menace doit être propagée jusqu'à cette zone ou non.

Ce concept peut se résumer à une estimation du nombre d'étapes de temps nécessaires pour qu'une compagnie observée dans une zone spécifique puisse atteindre une autre zone. Pour cela, un équivalent de l'algorithme de Dijkstra est utilisé.

La Figure 7.4 illustre cela avec un exemple à $t = 1$ où la compagnie se tient dans la zone z_1 . Un aspect intéressant ici est de considérer la possibilité que c peut atteindre la zone z_4 tel que $Zones(c)^{t+1} = [z_2, z_3, z_4]$. Pour un opérateur humain, une telle information peut être cruciale afin de comprendre comment déployer ses capteurs, d'évaluer plus rapidement la stratégie de l'ennemi et se faire un avis plus promptement.

Cette amélioration du modèle permet également de savoir comment la menace va se diffuser à travers le temps. La menace maximum étant connue, comme vu précédemment, la menace à un horizon spécifique permet de savoir quand une compagnie peut arriver en un minimum de temps dans une zone et donc de connaître subséquemment la menace de cette zone à tout horizon.

Donc la menace d'une zone est représentée maintenant par un ensemble de scores de menace tel que $M(z) = [M(z)^t, M(z)^{t+1}, \dots, M(z)^{t+H}]$ avec H le dernier horizon des événements (i.e. le score maximal de menace calculé via l'Équation 7.7). De plus, un monde potentiel Φ possède un temps associé décrivant le nombre total d'itérations de temps avant que le scénario de la menace maximale arrive. Cela permet d'avoir un second paramètre pour


 FIGURE 7.4 – Exemple à $t = 1$ avec une compagnie dans z_1

traiter de façon plus ou moins prioritaire les k -best stratégies. Par exemple, dans le monde Φ de la Figure 7.4, a_1 est menacé par la compagnie à $h = 3$ et a_2, a_3, a_4 à l'horizon $h = 4$.

Chaque score de menace $M(z)^{t+i}$ (avec $1 \geq i \geq H$) de chaque zone est donc calculé tel que :

$$M(z)^{t+i} = \sum_{c_k \in \text{Comp}(z)^{t+i}} M(c_k^{t+1}) \quad (7.12)$$

Avec ce système d'information, un opérateur humain est en mesure de se focaliser sur les scénarios les plus critiques et dangereux en prenant en compte à la fois la menace et l'urgence de la situation. Cela grâce à la possibilité de savoir combien de temps il reste avant qu'un scénario se produise. C'est un apport crucial puisque le fait d'observer toutes les zones n'est pas possible avec des ressources limitées dans une situation de crise. Avec le temps et le niveau de menace, la décision de déployer des capteurs ou des défenses est grandement facilitée et permet de réagir plus efficacement tout du long du scénario.

7.5 Généralisation

Cette méthode peut s'appliquer à tout type de propagation de menace. Voici entre autres quelques exemples :

- Propagation d'agents pathogènes
- Propagation des populations
- Gestion de l'immigration
- Gestion des manifestations

- Gestion de catastrophes naturelles
- Faille de sécurité sur des réseaux

Nous pouvons encore imaginer d'autres cas applicatifs nécessitant une modélisation adaptée, mais le procédé fonctionnerait sur tout ces exemples avec quelques modifications.

7.6 Conclusion

Cette contribution introduit un système de propagation de menace automatisé qui s'applique au domaine militaire dans des structures topographiques. L'outil présenté permet à un opérateur humain de monitorer une situation de crise sur un champ de bataille et de comprendre comment l'ennemi se comporte. La stratégie de l'ennemi peut ainsi être correctement inférée (comme nous le verrons dans les résultats et expérimentations, Chapitre 10) en montrant la vulnérabilité de chaque cible et le temps restant avant l'attaque. L'horizon des événements permet de rendre la situation plus facilement compréhensible et aide à anticiper les prochaines zones à observer afin de discriminer plus efficacement les possibles stratégies de l'ennemi.

Il reste cependant de nombreuses améliorations possibles. Par exemple, représenter des systèmes de défense plus ou moins connus par l'ennemi sur les AP. Cela pourrait influencer l'ennemi à changer de stratégie, même au cours du scénario en fonction de la façon dont le défenseur réagit.

Une autre perspective intéressante, serait la possibilité de permettre à l'observateur humain d'ajouter des informations sur des compagnies que nous n'avons pas pu observer. Par exemple, l'opérateur peut, par son expérience de terrain, vouloir imaginer un scénario avec la présence d'autres troupes telles que des compagnies du génie militaire permettant de construire un pont par dessus une rivière pour voir quelles seraient les conséquences d'une telle situation. Cela ajouterait la possibilité d'anticiper de potentielles stratégies grâce à la connaissance métier d'un expert et d'améliorer les capacités d'inférence des stratégies dans un environnement partiellement observable.

Optimisation association capteurs / variables via le *Scored Maximum Flow*

8.1 Introduction

Ce chapitre présente des travaux préliminaires sur la dernière étape de ce système global (Figure 8.1) sur la décision et l'optimisation multi-agents où nos agents sont les capteurs correspondant à nos sources hétérogènes collectant l'information.

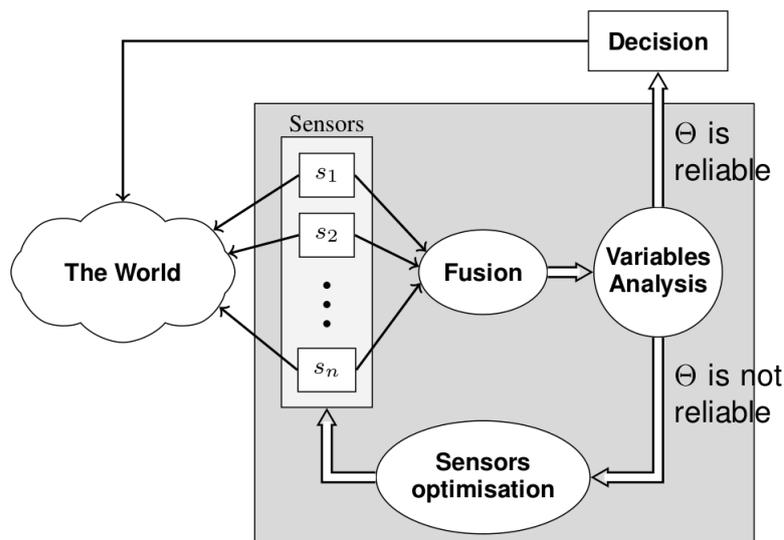


FIGURE 8.1 – Système ASAAP

Cette brique propose une première solution à la question qui est de savoir comment optimiser la gestion de capteurs pour obtenir des informations spé-

cifiques et critiques dans un processus d'évaluation de situation. Plus précisément, comment sélectionner les capteurs et leurs actions de façon optimale et automatisée.

Ce chapitre présente notre modèle *Scored Maximum-Flow* développé et basé sur la théorie des graphes. Une première section servira à formaliser le graphe de notre modèle ainsi que son utilisation pour définir l'environnement à travers ce dernier. Puis deux notions seront présentées, le *poids* et le *score*. Chacune des sous-sections suivantes définira ces deux concepts respectivement ainsi que la valeur attribuée aux arcs du graphe.

Pour rappel, le concept de variables utiles (MVV) utilisé tout au long de ce chapitre se réfère au Chapitre 6 Section 6.3.1.

8.2 Modélisation de l'environnement via un graphe biparti

Notre modèle de graphe se base sur un graphe orienté, pondéré et acyclique. Notons notre graphe $G = (S, E)$ avec S notre ensemble de sommets et E notre ensemble d'arêtes (arcs). Une arête sera notée (u, v) représentant un arc du sommet u vers le sommet v . Il est à noter que l'arc $(u, v) \neq (v, u)$ car ce graphe est orienté.

L'environnement est constitué de variables et de capteurs pouvant observer ces variables. Les nœuds du graphe se divisent en deux ensembles, \mathcal{V} pour les variables et \mathcal{C} pour les capteurs où pour tout arc (u, v) , $u \in \mathcal{V}$ et $v \in \mathcal{C}$. Les arêtes représentent le fait qu'une variable puisse être observée par un capteur tel que représenté dans la Figure 8.2.

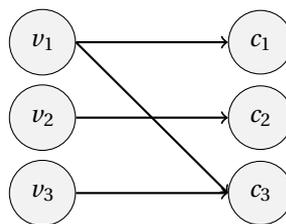


FIGURE 8.2 – Exemple de représentation d'un environnement par un graphe

Dans cet exemple, la variable v_1 peut être observée par les capteurs c_1 et c_3 , la variable v_2 par le capteur c_2 et la variable v_3 par le capteur c_3 .

8.3 Notations

Voici l'ensemble des notations et symboles qui serviront pour la suite de ce chapitre. Soit :

- $\mathcal{V} = \{v_1, \dots, v_n\}$ un ensemble de variables observables
- $\mathcal{U} = \{u_1, \dots, u_q\}$ un ensemble de variables observables utiles (MVV)
- $\mathcal{I} = \{i_1, \dots, i_o\}$ un ensemble représentant les variables considérées non-utiles, soit $\mathcal{V} \setminus \mathcal{D}$
- $\mathcal{C} = \{c_1, \dots, c_l\}$ l'ensemble de tous les capteurs
- $\mathcal{R} = \{r_1, \dots, r_p\}$ un ensemble de capteurs couvrant l'ensemble \mathcal{D}
- $\mathcal{U} = \{u_1, \dots, u_m\}$ un ensemble de capteurs couvrant l'ensemble \mathcal{Q} soit $\mathcal{C} \setminus \mathcal{R}$

Soit les fonctions :

- $\mathcal{F}(c_i)$ retourne toutes les variables observables par le capteur c_i
- $\mathcal{F}_a^{\mathcal{V}}(c_i)$ retourne toutes les variables observables dans \mathcal{V} par le capteur c_i dans l'action $a \in C^{\mathcal{A}}(c_i)$ ¹
- $C_{\mathcal{V}}^{\mathcal{A}}(c_i)$ retourne toutes les actions du capteur c_i permettant d'observer une variable dans \mathcal{V}
- $\mathcal{L}(v_i)$ retourne tous les capteurs pouvant observer la variable v_i
- $\Delta(c_i)$ le degré de confiance du capteur c_i (soit l'inverse de la marge d'erreur $\delta(c_i)$)
- $\lambda_{v_i}(c_i)$ la richesse d'information du capteur c_i par rapport à la variable v_i .

À titre d'information, les fonctions concernant l'ensemble \mathcal{C} ont leur équivalent pour les capteurs appartenant aux ensembles \mathcal{R} et \mathcal{U} et il en est de même pour les fonctions concernant \mathcal{V} pour \mathcal{D} et \mathcal{Q} .

8.4 Poids et capacité

Un graphe pondéré l'est par un *poids* w qui stocke le *poids* lié à une arête (notée $w^{(u,v)}$) de notre ensemble E . Dans notre cas, ce poids est donné par une fonction $w : E \rightarrow \mathbb{N}$. Tout *poids* $w^{(u,v)}$ ne peut aller que dans le sens de l'arc (u, v) tel que le flot va de u vers v , ce qui fait qu'ils sont tous strictement positifs tels que $w^{(u,v)} \geq 0$.

Chaque arc possède aussi une *capacité* notée $c^{(u,v)}$ pour l'arc allant de u vers v . La capacité impose une contrainte à notre *poids* telle que :

$$\text{Pour tout } u, v \in S : 0 \leq w^{(u,v)} \leq c^{(u,v)}$$

1. $C^{\mathcal{A}}(c_i)$ retourne toutes les actions disponibles pour le capteur c_i

8.4.1 Le problème du Flot Maximal

Le problème du Flot Maximal [Edmonds and Karp,] va nécessiter l'ajout de deux nouveaux nœuds, s et t qui représentent respectivement la *source* et le *puits* (voir figure 8.3). La *source* représente le point de départ unique du flot et le *puits* son point d'arrivée unique. Le but va être de maximiser le flot global en partant de la source jusqu'au puits sans excéder la capacité des arcs du graphe.

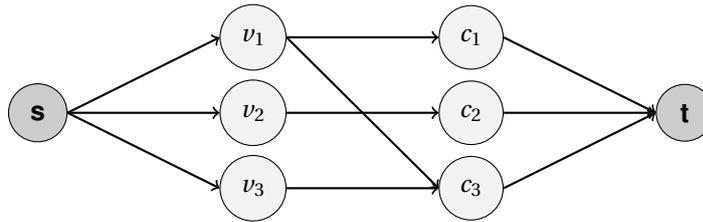


FIGURE 8.3 – Graphe avec les nœuds de la source et du puits

Un flot est une chaîne reliant la source s au puits t avec un poids w . Le premier sommet produit le flot et le second le consomme. Ce flot va passer par des sommets, contraint par un chemin d'arêtes orientées.

Ce flot est continu, ce qui signifie que le *poids* est le même à travers tous les arcs que ce flot traverse. Son poids correspond à la capacité minimale rencontrée à travers toutes les arêtes par lesquelles il passe. Dans notre cas, le flot prend comme *poids* la valeur maximale qu'il peut atteindre de s à t , soit 1, car il passera forcément par un arc de *capacité* $c^{(u,v)} = 1$.

Le flot maximal a pour but de générer des flots jusqu'à ce que la *capacité* maximale du graphe soit atteinte. Chaque flot représente les capteurs par lesquels les variables sont observées.

Le concept de notre modèle est qu'un flot représente une observation d'une variable par un capteur. De là, le flot maximal représente donc le fait que tous les capteurs sont utilisés et il représente donc une couverture maximale des variables.

Le modèle a donc pour but que le flot maximal sature la *capacité* du puits $c^{(t)}$. Quand le flot maximal est atteint, cela signifie que tous les capteurs sont utilisés pour observer nos variables observables.

Pour représenter cette modélisation, les capacités des différents arcs seront définis comme suit.

Capacité de la source

La *capacité* de la source correspond à la somme du nombre total de capteurs pouvant observer chaque variable $v \in \mathcal{V}$ telle que :

$$c^{(s)} = \sum_{v \in \mathcal{V}} |\mathcal{L}(v)|$$

Par exemple, deux variables v_1 et v_2 , pouvant être atteintes respectivement telles que $\mathcal{L}(v_1) = \{c_1, c_2\}$ et $\mathcal{L}(v_2) = \{c_2\}$, la *capacité* de la source serait donc $c^{(s)} = 3$.

Arcs Source → Variables

Ici la *capacité* correspond pour chaque arc au nombre total de capteurs pouvant observer la variable en bout d'arc soit :

$$c^{(s,v)} = |\mathcal{L}(v)|$$

Dans notre exemple précédent, l'arc de s vers v_1 aurait une *capacité* $c^{(s,v_1)} = 2$. Il est à noter que v peut être remplacé par d ou q si la variable appartient à l'ensemble \mathcal{D} ou \mathcal{Q} .

Arcs Variables → Capteurs

La *capacité* est telle que :

$$c^{(v,c)} = \begin{cases} 1, & \text{si } v \in \mathcal{F}_a^{\mathcal{V}}(c) \\ 0, & \text{sinon} \end{cases}$$

Cela représente l'impossibilité de passer par un arc si l'action courante du capteur c ne permet pas d'observer la variable v . Sinon, la capacité est de 1.

Arcs Capteurs → Puits

La *capacité* de ces arcs correspond au nombre de variables pouvant être atteintes par le capteur d'où part l'arc (dans l'action courante a dans laquelle il se trouve) noté :

$$c^{(c,t)} = |\mathcal{F}_a^{\mathcal{V}}(c)|$$

Par exemple, un capteur c_2 exécutant l'action a_2 telle que $\mathcal{F}_{a_2}^{\mathcal{V}}(c_2) = \{v_1, v_2\}$ aurait une *capacité* $c^{(c_2,t)} = 2$. Il est à noter qu'ici c peut correspondre aussi bien à un capteur u ou r selon qu'il appartient à l'ensemble \mathcal{U} ou \mathcal{R} .

Capacité du Puits

La *capacité* du puits correspond au nombre maximum de variables observables par tous les capteurs chacun dans leur action courante a telle que :

$$c^{(t)} = \sum_{c \in \mathcal{C}} |\mathcal{F}_a^{\mathcal{V}}(c)|$$

La capacité du puits est systématiquement inférieure ou égale à la capacité de la source telle que $c^{(t)} \leq c^{(s)}$. Cela du fait qu' au mieux, s'il n'y a qu'une action par capteur, il y aura le même nombre d'arcs que celui de capteurs pouvant observer les variables et les capacités seront telles que $c^{(t)} = c^{(s)}$ car il n'y aura qu'un moyen d'observer une variable par un capteur. Dans le cas où il y a plusieurs actions, $c^{(t)} < c^{(s)}$ car il y a plus de moyens d'observer une variable que de capteurs pouvant l'observer.

Cependant, ce seul concept ne suffit pas pour nos besoins. Il faut ajouter celui du *score* qui, associé au flot maximal, permettra de rendre prioritaire la couverture des variables de l'ensemble \mathcal{D} (voir sous-section suivante).

8.4.2 Score

Nous ajoutons à la *capacité* la notion de *score* qui va nous permettre de définir des priorités quant au fait de passer par un arc ou un autre. Plus le *score* de l'arc est élevé, plus il est prioritaire sur les autres. Le *score* est une valeur strictement positive telle que $s \geq 0$ et $s \in \mathbb{R}$. Une capacité $c = 0$ amènera à un score lui aussi égal à 0 afin de respecter la représentation de l'impossibilité de passer par un arc si l'action courante du capteur ne permet pas l'observation de la variable.

Nous définissons ici l'intérêt et l'utilisation du *score* pour orienter le choix des arcs pour le problème de flot maximal.

Maximisation du score

La maximisation du score a pour but de diriger le choix des flots avec un système de priorité. Le flot retenu sera celui générant le score maximal en faisant la somme du score des arcs par lesquels il passe. Le second flot sera généré de la même façon en respectant la capacité du graphe avec les flots déjà en place jusqu'à atteindre une situation de flot maximal.

Ce mécanisme assure que l'on ordonne l'observation des variables $\in \mathcal{D}$ vis à vis de \mathcal{Q} via la maximisation du score afin de garantir la couverture de \mathcal{D} avant celle de \mathcal{Q} .

Tant que le graphe n'est pas saturé, le modèle est conçu de sorte à ce qu'il y ait toujours au moins un arc de score ≥ 1 pour atteindre le puits, donc

lorsque le flot rencontre un arc de score 0, il a systématiquement le choix avec un autre chemin.

Le *score maximum* que l'on peut atteindre dans le graphe correspond à la somme maximale que l'on peut atteindre en passant par les arcs tout en respectant le flot maximal tel que :

$$s_{max} = s^{(s)} + \sum_{v \in \mathcal{V}} s^{(s,v)} + \sum_{v \in \mathcal{V}, c \in \mathcal{C}} s^{(v,c)} + \sum_{c \in \mathcal{C}} s^{(c,t)} + s^{(t)}$$

Ce *score maximal* représente la couverture la plus optimale possible, mais cependant il n'est pas systématiquement atteint. Du fait de rendre l'observation des variables utiles \mathcal{D} prioritaire, il se peut que des variables non-utiles \mathcal{Q} ne soit plus observables par les capteurs (voire parfois d'autres variables $\in \mathcal{D}$).

Score général

Les arcs suivants ont un *score* de 1 tel que :

$$\begin{aligned} s^{(s)} &= 1 \\ s^{(s,v)} &= 1 \\ s^{(t)} &= 1 \end{aligned}$$

Il est envisageable que l'arc $s^{(s,v)}$ puisse avoir un *score* variable (tel que $1 \leq s^{(s,v)}$) dans le cas où certaines variables utiles deviennent prioritaires vis à vis d'autres variables utiles en terme d'observation. Cela pourrait se produire par exemple si on souhaite concentrer plusieurs capteurs pour couvrir plus de fois une variable d plutôt qu'une autre.

Autrement, seuls les arcs $s^{(v,c)}$ et $s^{(c,t)}$ ont un score variable comme vu ci-dessous.

Arcs Variables → Capteurs

Le *score* est défini par la richesse d'observation du capteur c sur la variable v tel que :

$$s^{(v,c)} = \begin{cases} \lambda_v(c), & \text{si } v \in \mathcal{F}_a^{\mathcal{V}}(c) \\ 0, & \text{sinon} \end{cases}$$

Cela favorise les capteurs pouvant observer le plus d'informations sur la variable v .

Arcs Capteurs → Puits

Ici le *score* se définit par le degré de confiance du capteur c tel que :

$$s^{(c,t)} = \Delta(c)$$

Ce *score* permet de favoriser le capteur ayant le plus grand score de confiance (soit la plus petite marge d'erreur).

8.5 Processus de perception active

L'utilisation de notre modèle se déroule en deux étapes : Une première ne se concentrant que sur les variables utiles (dans \mathcal{D}) et une seconde pour toutes les autres (dans \mathcal{Q}).

8.5.1 Première étape : variables utiles

Cette étape se concentre sur les variables utiles (dans \mathcal{D}) afin de réduire notre espace de recherche et de réduire la complexité de notre processus. Ces variables étant prioritaires en terme de couverture par nos capteurs, nous générons l'ensemble des graphes possibles afin de trouver le meilleur jeu d'actions optimisant la couverture de ces dernières.

Un jeu d'actions correspond à toutes les actions fixées, une pour chaque capteur de \mathcal{R} (étant les seuls capteurs à pouvoir observer \mathcal{D}). On parle de jeu d'actions *complet*. Un jeu d'actions est forcément complet du fait qu'il existe au moins une action a par capteur pour observer une variable dans \mathcal{D} sinon le capteur ne serait pas dans \mathcal{R} . Le but ici est de trouver le meilleur jeu d'actions pour maximiser notre couverture de \mathcal{D} à l'itération suivante.

Pour cela, nous réalisons un graphe par jeu d'actions possibles. Ce jeu d'actions α correspond au produit cartésien de toutes les actions pour chaque variable pouvant permettre l'observation d'une variable dans \mathcal{D} tel que $\alpha = \prod_{r \in \mathcal{R}} C_{\mathcal{D}}^{\mathcal{A}}(r)$. Pour chaque jeu d'actions, nous avons un graphe sur lequel nous appliquons notre algorithme de flot maximal tout en cherchant à maximiser le *score*.

Par exemple, 3 capteurs tels que $r_1^{\mathcal{A}} = \{a_1, a_2\}$, $r_2^{\mathcal{A}} = \{a_3, a_4\}$ et $r_3^{\mathcal{A}} = \{a_7\}$. Il faudra générer 4 graphes avec comme jeu d'actions :

- $r_1^a = a_1, r_2^a = a_3, r_3^a = a_7$
- $r_1^a = a_1, r_2^a = a_4, r_3^a = a_7$
- $r_1^a = a_2, r_2^a = a_3, r_3^a = a_7$
- $r_1^a = a_2, r_2^a = a_4, r_3^a = a_7$

Le graphe obtenant le *score* final le plus élevé sera celui qui maximisera l'efficacité de la couverture de nos variables utiles. C'est aussi celui qui contient le jeu d'actions que nous souhaitons appliquer sur nos capteurs à la prochaine itération.

Graphe

Le graphe suivant (voir Figure 8.4) est la représentation du modèle décrit précédemment pour la première étape. Les valeurs en rouge représentent le *score*, et les valeurs en bleu la *capacité*. Les observations représentent la source du graphe et les résultats les puits.

A titre d'information, les arêtes entre les variables et les capteurs ne sont pas représentées par souci de clarté.

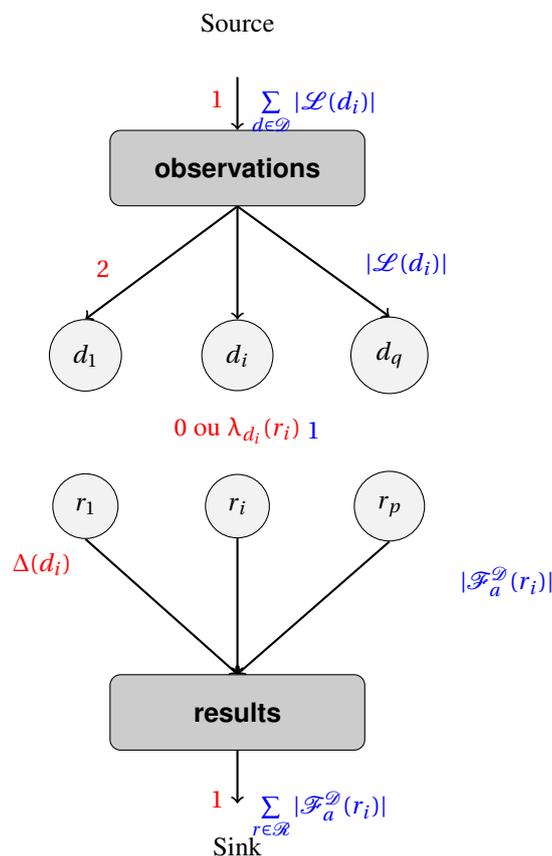


FIGURE 8.4 – Première étape : application du processus sur les variables utiles

Algorithme

Le processus pour permettre d'appliquer un flot maximal sur le graphe en ordonnant les flots via la maximisation du *score* est le suivant. Il faut ajouter

un flot jusqu'à ce que le puits soit saturé (voire la source si une seule action par capteur). Chaque flot ajoute un poids de 1 sur chaque arête qu'il traverse (cela du fait qu'une chaîne allant de s à t passe systématiquement par un arc (v, c) de capacité $c^{(v,c)} = 1$). À partir de là, on peut affirmer qu'il faudra un nombre de flots égal à la capacité du puits $c^{(t)}$ pour le saturer. Le choix du chemin se fera en donnant la priorité aux arêtes ayant le score le plus élevé et n'étant pas saturées.

L'algorithme suivant décrit le processus de la première étape (voir Algorithme 5).

Algorithm 5 GraphProcess(**Graph** graph)

```

source_node ← graph.getSource()
sink_node ← graph.getSink()
while source_node.getWeight() < source_node.getCapacity() do
    current_node ← source_node
    path ← {source_node}
    while current_node ≠ sink_node do
        max_score ← 0
        for each edge edge in getReachableEdgesFrom(current_node)
do
            if edge.getScore() > max_score AND
edge.getWeight() < edge.getCapacity() then
                best_edge ← edge
                max_score ← edge.getScore()
            end if
        end for
        current_node ← best_edge.getEndNode()
        path.add(current_node)
    end while
    flow_weight_value ← path.minCapacityValue()
    graph.setPathWeight(flow_weight_value)    ▷ Apply flow's
weight on all edges on the path
end while
return graph

```

La complexité de l'algorithme est $\mathcal{O}\left(\sum_{d \in \mathcal{D}} 3 \cdot |\mathcal{L}(d)|\right)$. Et cet algorithme est répété pour chaque combinaison d'actions possible pour les capteurs. Donc notre complexité devient :

$$\mathcal{O}\left(\prod_{r \in \mathcal{R}} C_{\mathcal{D}}^{\mathcal{A}}(r) \cdot \sum_{d \in \mathcal{D}} (3 \cdot |\mathcal{L}(d)|)\right)$$

8.5.2 Deuxième étape : ensemble des variables observables

Cette deuxième étape permet de couvrir toutes les autres variables (dans \mathcal{D}) à partir du jeu d'actions fixé lors de la première étape. Cela afin de couvrir le maximum de variables observables même sans qu'elles soient utiles. Cependant, toujours dans un souci de réduction de la complexité, il n'est pas question ici de trouver l'action optimale d'un capteur $\in \mathcal{D}$. Le but est de voir quelles seront les variables pouvant encore être observées après l'application des meilleures actions sur les capteurs $\in \mathcal{D}$. Comme dit précédemment, il se peut même que certaines variables ne soient plus couvertes par aucun capteur.

Lors de cette étape, nous ne travaillons donc que sur l'ensemble de variables \mathcal{D} . Pour cela, nous appliquons à notre graphe le sous-graphe généré à la première étape (avec son *score* et sa *capacité*). Les arcs de la source vers les variables dans \mathcal{D} sont déjà tous saturés ainsi que ceux des variables \mathcal{D} vers les capteurs \mathcal{R} . Cependant, les arcs \mathcal{R} vers le puits ne sont plus forcément saturés car ils ont une nouvelle *capacité* qui est $|\mathcal{F}_a^{\mathcal{V}}(r_i)|$ et non $|\mathcal{F}_a^{\mathcal{D}}(r_i)|$ telle que $|\mathcal{F}_a^{\mathcal{V}}(r_i)| \geq |\mathcal{F}_a^{\mathcal{D}}(r_i)|$. Cela se justifie du fait qu'il puisse y avoir des arcs des variables \mathcal{D} vers les capteurs \mathcal{R} . Cependant, le poids fixé par les flots lors de la première étape est tout de même appliqué sur les arcs \mathcal{R} vers le puits. Si $|\mathcal{F}_a^{\mathcal{V}}(r_i)| = |\mathcal{F}_a^{\mathcal{D}}(r_i)|$, l'arc reste saturé, et il ne l'est pas sinon.

Graphe

De la même manière que précédemment, la Figure 8.5 est la représentation du modèle décrit précédemment pour la seconde étape.

Ici, les arêtes en rouge sont déjà saturées (celles couvrant les variables dans \mathcal{D} , soit les arcs (s, d) et (d, r) pour $\forall d \in \mathcal{D}$ et $\forall r \in \mathcal{R}$). Les arêtes entre les variables et les capteurs ne sont toujours pas représentés par souci de lisibilité. De plus, des arcs peuvent aller d'une variable appartenant à \mathcal{D} vers l'ensemble de capteurs \mathcal{R} . Cependant, l'inverse n'est pas vrai, il ne peut pas y avoir d'arcs de l'ensemble \mathcal{D} vers l'ensemble de capteurs \mathcal{U} (sinon le capteur u appartiendrait à \mathcal{R}).

Algorithme

L'algorithme de cette étape est le même que pour l'étape précédente, mais cette fois-ci, il n'est appliqué qu'une fois car nous ne cherchons pas à trouver les actions maximisant le score (afin de réduire la complexité).

Cependant, avant d'appliquer l'algorithme précédent (voir Algorithme 5), on applique sur le graphe le sous-graphe généré lors de la première étape afin de n'avoir plus qu'à travailler sur les variables dans \mathcal{D} .

La complexité est telle que $\mathcal{O}\left(\sum_{q \in \mathcal{Q}} 3 \cdot |\mathcal{L}(q)|\right)$.

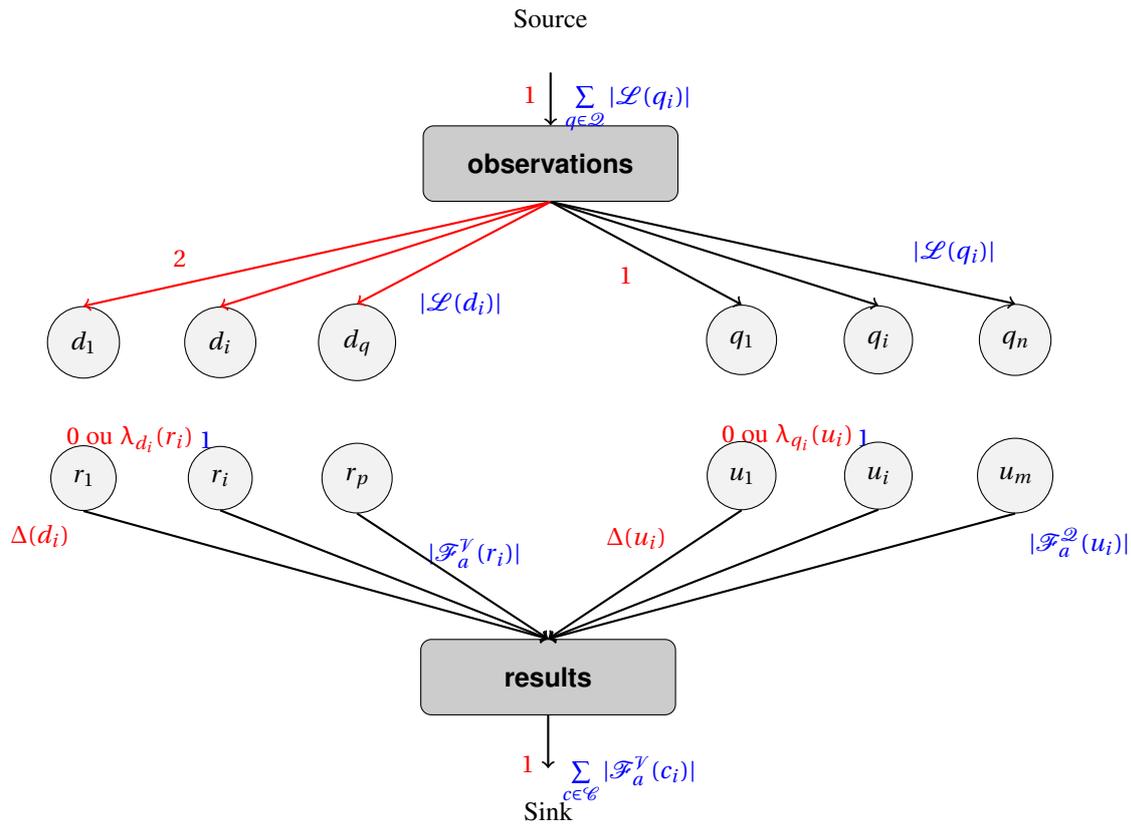


FIGURE 8.5 – Deuxième étape : application du processus sur toutes les variables

8.5.3 Conclusion

Ce processus nous permet en 2 étapes de maximiser la couverture des variables utiles en maximisant aussi la prise d'information en fonction de la richesse d'information des capteurs vis à vis de ces variables et de leur taux de confiance. De plus, les variables non-utiles restent tout de même observées de façon optimale par les capteurs restants.

Le processus complet a pour complexité totale :

$$\mathcal{O}\left(\left|\prod_{r \in \mathcal{R}} \mathcal{C}_{\mathcal{D}}^{\mathcal{A}}(r)\right| \cdot \sum_{d \in \mathcal{D}} (3 \cdot |\mathcal{L}(d)|) + \sum_{q \in \mathcal{Q}} (3 \cdot |\mathcal{L}(q)|)\right)$$

Troisième partie

Évaluation du système

CHAPITRE 9

Cas d'usage maritime

Le cas d'usage maritime a été réalisé pour mettre en place une expérimentation sur l'efficacité de l'analyse des variables les plus utiles (notées MVV) présentée dans le Chapitre 6.

Le scénario mis en avant a été imaginé à partir de certains besoins dans le domaine du renseignement et de la surveillance maritime comme ceux que l'on est susceptible de devoir traiter au sein d'Airbus Defence & Space.

9.1 Définition du cas d'usage

L'objectif de ce cas d'usage est d'être en mesure d'évaluer la menace de navires selon des informations *Hard & Soft*. Dans ce scénario d'évaluation de situation (SA) on considère la menace d'un navire comme le risque que ce dernier coule ainsi que le risque environnemental dû à son chargement dans le cas où il coulerait.

Nous avons défini dans ce scénario spécifique que les navires ne sont plus en mesure de communiquer avec les gardes-côtes et qu'ils ont des trajectoires suspectieuses car ils ne suivent pas les chemins maritimes tout en s'approchant trop près des côtes.

Ce danger amenant à une situation d'urgence (considérée comme situation de crise), tous les capteurs à disposition sont déployés afin de permettre d'évaluer la situation dans le but d'être en mesure de prendre les décisions nécessaires afin d'éviter un naufrage et une catastrophe naturelle possible.

9.1.1 Les capteurs

Les capteurs d'informations dites *Hard* sont un radar pour estimer la position et la vitesse, les AIS (*Automatic Identification System*) pouvant être reçus des navires pour la position et la vitesse également et un "*direction finder*"¹.

Les capteurs d'origine *Soft* se composent d'un observateur humain aux jumelles, une base de connaissances (*Knowledge Data Base* notée KDB) obtenue via des sites *Open Source* spécialisés ou directement de compagnies possédant des navires, et les données (*Ship Transmitted Data* notées STD) nous informant sur son chargement.

Le Tableau 9.1 décrit les niveaux de confusion normalisés de l'ensemble des capteurs tel que $\epsilon = [0, 1] \in \mathbb{R}$. Cet ϵ décrit le bruit d'un capteur par rapport à la variable qu'il peut observer. Cela permet de savoir la qualité d'information qu'il est en mesure de récupérer par rapport à telle ou telle variable.

TABLEAU 9.1 – Niveau de confusion normalisé des capteurs ϵ

Sensor	MVV	ϵ
Radar	pos	0.12
AIS	pos	0.15
	speed	0.09
Dir. Finder	dir	0.08
STD	load	0.05
Human obs	Name	0.07
	Flag	0.04
KDB	Name	0.08
	Flag	0.05

Chaque capteur peut donc observer différentes variables via ce que nous considérons comme une action. Cette action peut être à la fois le fait de déplacer ou orienter un capteur vers une variable, ou bien de procéder à une analyse spécifique des données renvoyées afin de chercher à obtenir une information précise sur telle ou telle variable. Une action, généralement, empêche l'observation d'une autre variable. Dans notre scénario théorique, nous considérons qu'une action lie l'observation d'un capteur à une seule variable.

Par exemple, le radar a deux actions possibles. La première action est le *scanning*, qui consiste à observer l'environnement avec un large champ de vision afin de trouver des cibles et leurs positions mais de manière peu précise. La seconde est l'action de *tracking* qui affine l'information en cherchant

1. Composé par une antenne qui envoie et reçoit des signaux à la radio du navire afin de déterminer une direction sur la carte maritime via l'historique des signaux émis et reçus.

dans un espace beaucoup plus réduit afin de préciser au mieux la position des navires.

9.1.2 Les hypothèses à monitorer

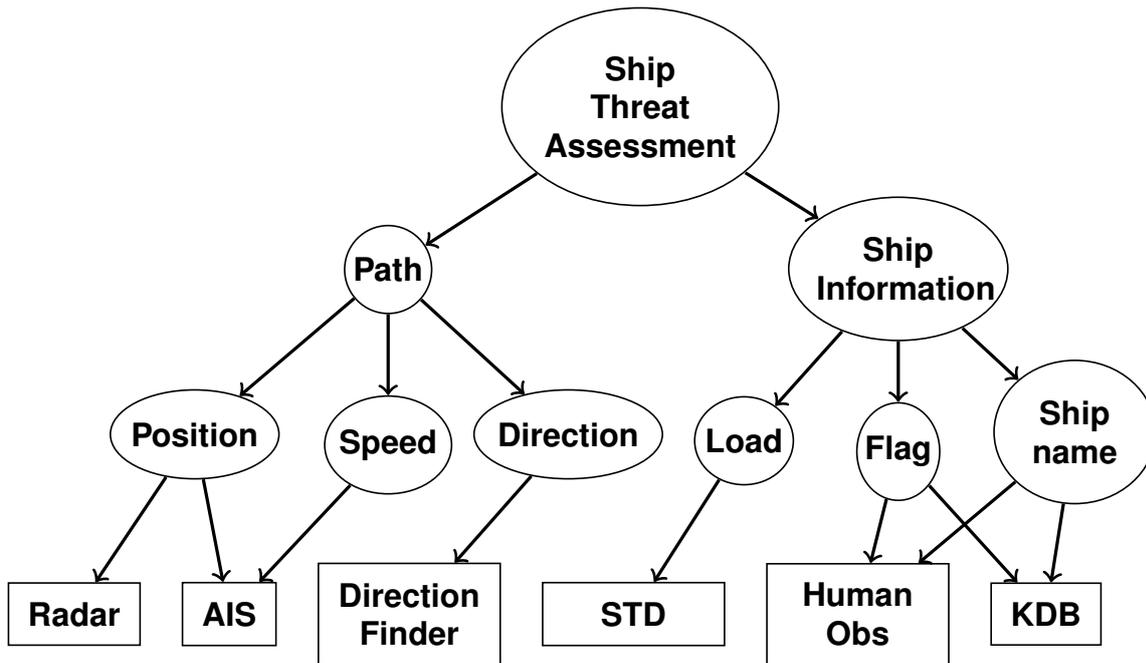
La situation à évaluer dans notre scénario comprend trois navires. Considérons donc $\Theta = \langle \theta_1, \theta_2, \theta_3 \rangle$ la situation de crise à évaluer. Chaque θ_i représente l'évaluation de menace d'un navire. Ces trois navires sont trop proches des côtes et en dehors des voies maritimes habituelles, donc ils représentent un risque potentiel.

Afin d'être en mesure de comprendre rapidement la situation et de prendre les décisions adéquates, le système est mis en place et déploie tous les capteurs mentionnés précédemment.

La Figure 9.1 décrit les hypothèses θ_i qui dans ce scénario sont définies par le même réseau bayésien dynamique (DBN) mais il faut noter qu'il est tout à fait possible d'avoir des DBN différents.

Les nœuds ovales sont les variables aléatoires du DBN décrivant l'hypothèse. Le nœud racine est l'hypothèse que l'on cherche à évaluer, les nœuds possédant à la fois des ascendants et des descendants dans le DBN sont des variables inférables. Ici le chemin est noté *Path* et les informations globales du bateau sont notées *Ship Information*. Enfin, les nœuds correspondant aux feuilles du DBN (sans prendre en compte les capteurs) sont les variables observables. Les arcs entre chacun de ces nœuds représentent les dépendances causales permettant l'inférence du DBN.

Enfin, les nœuds carrés sont les capteurs qui sont reliés par un arc lorsqu'ils sont en mesure d'observer une variable observable.

FIGURE 9.1 – Hypothèse θ_i décrite par son DBN

9.2 Résultats des expérimentations

Cette section présente les résultats d'un scénario simulé sur les bases définies dans la section précédente. Les contraintes de l'expérimentation sont d'abord définies, puis le scénario est présenté étape de temps par étape de temps avec les résultats sur les MVV et les décisions prises sur le choix des capteurs pour observer ces MVV.

9.2.1 Contraintes de l'expérimentation

Dans cette expérimentation, nous ne nous intéressons pas aux valeurs des variables aléatoires à proprement parler, mais à leur score de confiance γ (voir Chapitre 6 Section 6.3.1). Le seuil de confiance a été défini à $\Gamma = -0.10$.

L'expérimentation ne commence pas avec une connaissance nulle sur les navires afin de tester l'intérêt de connaître déjà ou non certaines informations sur les hypothèses.

Enfin, les graphes des résultats ne mentionneront pas le nom des variables pour des raisons de lisibilité. Mais il correspondent à la Figure 9.1 présentée précédemment.

9.2.2 Déroulement du scénario

La Figure 9.2 représente les résultats de l'analyse des MVV à la première étape de temps du scénario. À t_1 , l'hypothèse θ_1 sur l'évaluation de menace

du premier navire est considérée comme déjà connue avec suffisamment de confiance pour être exploitée par l'opérateur humain (de fait, aucune variable du DBN de l'hypothèse θ_1 n'est une MVV). Mais les deux autres hypothèses sur les deux autres navires nécessitent de nouvelles observations pour pouvoir atteindre une connaissance suffisante sur leur état. L'intention derrière cette configuration à cette première étape de temps est de mettre en avant que le système permet de choisir uniquement les variables d'intérêts et peut se focaliser indépendamment sur différentes hypothèses.

Il est à noter que dans la Figure 9.2 (et les suivantes), les nœuds en pointillés sont les variables aléatoires considérées comme connues avec suffisamment de confiance ($\gamma(X) \geq \Gamma$) et les nœuds rouges sont les MVV.

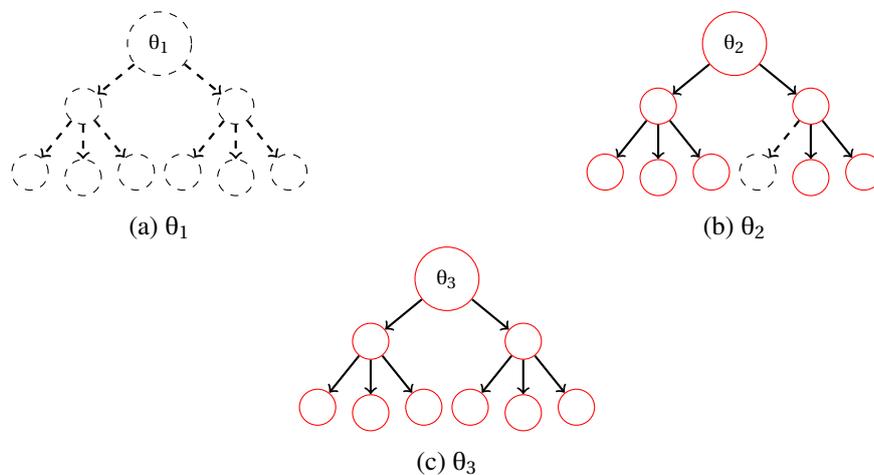


FIGURE 9.2 – Analyses des MVV à l'étape de temps t_1

Le Tableau 9.2 décrit l'évolution du score de confiance de chaque MVV pour des hypothèses θ_2 et θ_3 . Lorsqu'une valeur est nulle, c'est que la variable correspondante n'est plus à observer car le score de confiance est suffisamment élevé et elle ne correspond donc plus à une MVV. Les valeurs de ce tableaux sont obtenues via l'entropie de Shannon décrites dans le Chapitre 6 Section 6.3.1.

Le Tableau 9.3 montre l'attribution des capteurs aux MVV à observer à chaque étape de temps.

La première orientation des capteurs à t_1 met en avant la façon qu'a le système de choisir quel capteur est associé à quelle MVV. Par exemple, le score de confiance le plus bas des MVV est la variable *Name* de θ_2 . Pour sélectionner le capteur le plus à même de l'observer entre *Human Observer* et la *KDB* (les deux capteurs capables d'obtenir de l'information sur cette variable), le processus vérifie simplement quel capteur a le niveau de confusion normalisé le moins élevé afin de maximiser le gain d'information sur la MVV. Par conséquent, la MVV *Name* de θ_2 va être observée par le capteur *Human Obs* et le capteur *KDB* sera utilisé pour obtenir de l'information sur

TABLEAU 9.2 – Score de confiance de θ_2 et θ_3 durant les trois étapes de temps du scénario

MVV	t_1		t_2		t_3	
	θ_2	θ_3	θ_2	θ_3	θ_2	θ_3
Position	-0.29	-0.55	-0.29	\emptyset	-0.13	\emptyset
Speed	-0.55	-0.11	-0.17	-0.11	\emptyset	-0.11
Direction	-0.39	-0.66	-0.39	\emptyset	-0.19	\emptyset
Load	\emptyset	-0.29	\emptyset	\emptyset	\emptyset	\emptyset
Flag	-0.49	-0.46	\emptyset	-0.46	\emptyset	\emptyset
Name	-0.68	-0.44	\emptyset	-0.44	\emptyset	\emptyset

TABLEAU 9.3 – Attribution des capteurs pour observer les MVV à t_1 et t_2

Sensor	t_1	t_2
Radar	Pos(θ_3)	Pos(θ_2)
AIS	Speed(θ_2)	Speed(θ_2)
Dir. finder	Dir(θ_3)	Dir(θ_2)
STD	Load(θ_3)	\emptyset
Human obs	Name(θ_2)	Flag(θ_3)
KDB	Flag(θ_2)	Name(θ_3)

la *MVV Flag* (qui est le deuxième score de confiance le plus bas dans les variables observables par *KDB*).

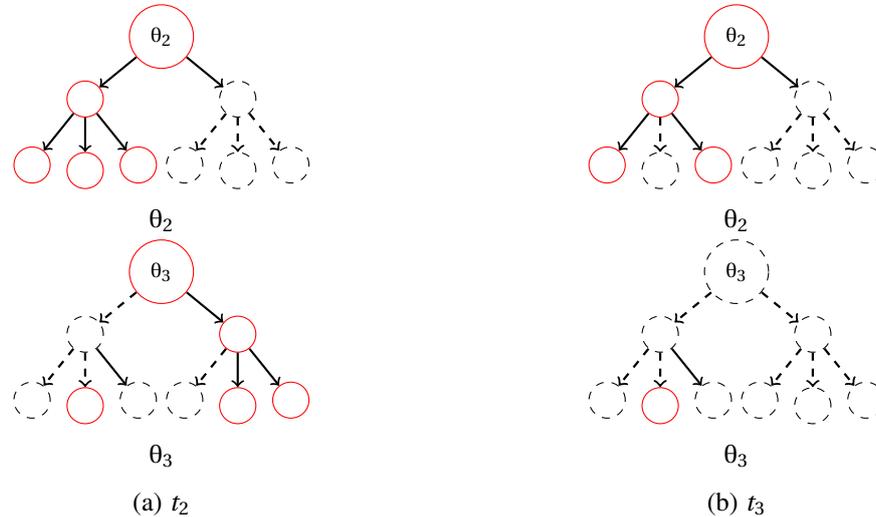


FIGURE 9.3 – Résultats de l'analyse des MVV à t_2 et t_3

La figure 9.3a met en avant un point important sur θ_3 . Ici, même si la variable observable correspondant à la vitesse du navire (*Speed*) est considérée comme non-fiable, son nœud ascendant (qui est une variable inférable) représentant la trajectoire du navire est quant à elle fiable. Cela est dû à l'inférence qui a été permise via les deux autres variables observables du navire, la position et la direction, qui ont permis une inférence avec suffisamment de confiance sur la trajectoire. De ce fait, la variable *Speed* n'a plus besoin d'être observée car nous n'avons pas besoin d'inférer à nouveau la trajectoire du navire pour le moment. Cela montre l'avantage significatif du système pour comprendre rapidement quelles sont les variables utiles et permettre ainsi une économie de ressources d'observation conséquente.

À travers cette expérimentation, le système a été capable d'accélérer le score de confiance sur chaque hypothèse en réduisant le nombre d'étapes nécessaires pour considérer ces hypothèses comme fiables. Dans ce scénario, le nombre de variables à observer et de capteurs à gérer est faible et donc compréhensible humainement. Mais dans des cas complexes (et plus réalistes), les opérateurs humains ne sont pas en mesure de tout gérer et analyser en temps voulu. Le système présenté est en mesure de comprendre automatiquement si une variable est prioritaire ou non afin d'économiser au mieux les ressources pour les informations les plus importantes et comprendre rapidement une situation.

9.3 Conclusion

La fusion d'information dans le domaine de la perception active rencontre des défis significatifs. Les trois difficultés majeures sont les multiples niveaux d'incertitude, la modélisation de l'environnement avec ses sources d'informations hétérogènes et la façon de gérer la fusion d'information et l'optimisation des capteurs.

Le système proposé à travers cette contribution permet de gérer ces difficultés et apporte de nouvelles perspectives pour améliorer la qualité de l'information en réduisant l'incertitude sur la situation à évaluer grâce aux MVV. Cette solution en deux étapes permet de travailler avec plus d'efficacité sur l'optimisation de l'utilisation des capteurs grâce à l'ajout de connaissances sur la valeur et l'utilité des variables de l'environnement.

De plus, l'algorithme d'association capteurs/variables que nous proposons (qui est actuellement un algorithme naïf) permet de décider de l'action à réaliser par le capteur en se basant sur le besoin de la mission plutôt qu'une simple activation capteur comme étant fait habituellement.

Cependant, cet algorithme a une complexité exponentielle du fait de la combinatoire capteurs/actions. Des travaux futurs concernent la recherche d'heuristiques quasi-optimales (*near-optimal*) afin d'améliorer la vitesse de convergence sur l'état de croyance de la situation à évaluer. De plus, il est nécessaire d'avoir une fonction de coût et d'utilité pour mieux décider de l'action à choisir pour chaque capteur. Cette fonction devra prendre comme paramètres à la fois la réduction de l'incertitude et le coût d'activation du capteur vis-à-vis de l'action réalisée. Des premiers essais avec ce genre de fonction ont été réalisés sur des capteurs dits *myopes* (vision à court terme, c'est à dire utilité à $t + 1$) mais l'idéal serait de réussir à porter l'utilité sur un horizon plus lointain. Les perspectives de ce travail doivent s'inspirer des travaux autour des POMDP ([Chanel et al., 2012] et [Renoux, 2015]).

CHAPITRE 10

Cas d'usage OPEX

Le cas d'usage OPEX est une expérimentation sur la propagation de menace dans la cadre d'une évaluation de situation de crise (Chapitre 7). L'idée est de proposer des scénarios crédibles et plausibles en s'inspirant de la doctrine militaire ([PFT RENS, 2016] et [RENS, 2016]).

L'objectif de cette expérimentation est de montrer que le système est capable de réaliser une propagation de menace à travers ces scénarios pour comprendre la stratégie de l'ennemi. Cela comprend l'analyse du chemin qu'emprunterait ce dernier lors de son attaque ainsi que la prédiction de la ou des zone(s) attaquée(s) afin de mettre en place une contre-mesure efficace.

10.1 Modélisation de l'environnement

La modélisation de l'environnement reprend ce qui a été défini dans le Chapitre 7 Section 7.2.1. Les scénarios présentés se basent, tous, sur le même graphe topographique (voir Figure 10.1).

Ces scénarios prennent en considération trois types de compagnie ; l'infanterie, les tanks et l'artillerie. Les scores de menace de chaque type sont représentés dans le Tableau 10.1 (les symboles des compagnies du tableau respectent les standards APP-6).

Les chemins de la carte sont de trois types différents, nommés A, B et C (que l'on peut considérer respectivement comme des routes goudronnées, des forêts et des rivières) avec leur index de traversabilité correspondant pour chaque compagnie décrite dans le Tableau 10.2. Ces index sont définis par une connaissance experte dans le domaine militaire considérant leur rôle et leur capacité de mouvement dans un cadre opérationnel.

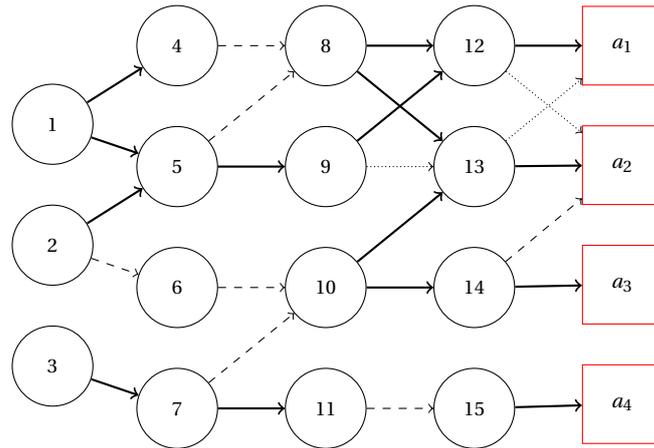


FIGURE 10.1 – Graphe topologique des scénarios de l’expérimentation

TABLEAU 10.1 – TS(c)

Company Type	Threat Score
♦Infantry	3
♦Tank	5
♦Artillery	1

TABLEAU 10.2 – Cr(c)

Company Type	Path Type		
	A	B	C
♦Infantry	1.0	0.8	0.2
♦Tank	1.0	0.6	0.1
♦Artillery	1.0	0.4	0.05

Les trois scénarios sont décrits étape par étape dans le Tableau 10.3 afin de permettre la reproductibilité de l’expérimentation. Leurs résultats respectifs sont présentés à la fois dans les Figures 10.3, 10.5, 10.7 et dans les Tableaux 10.4, 10.5, 10.6 dans les sous-sections de la section suivante. Enfin, la Figure 10.2 montre un exemple de carte de chaleur de la menace durant l’une des *k-best* stratégie (ici la stratégie *1-best* du scénario 1 à l’étape de temps t_2).

TABLEAU 10.3 – Scenarios

Company Type	t_1	t_2	t_3	t_4	t_5	t_6
◆Infantry	1 : z_1 1 : z_2	2 : z_5	2 : z_9	2 : z_{12}	2 : z_{12}	2 : a_1
◆Tank	1 : z_1 1 : z_2	1 : z_2 1 : z_5	1 : z_9 1 : z_5	1 : z_{12} 1 : z_9	2 : z_{12}	2 : a_1
◆Artillery	\emptyset	2 : z_2	1 : z_5 1 : z_2	1 : z_9 1 : z_5	2 : z_9	2 : z_{12}

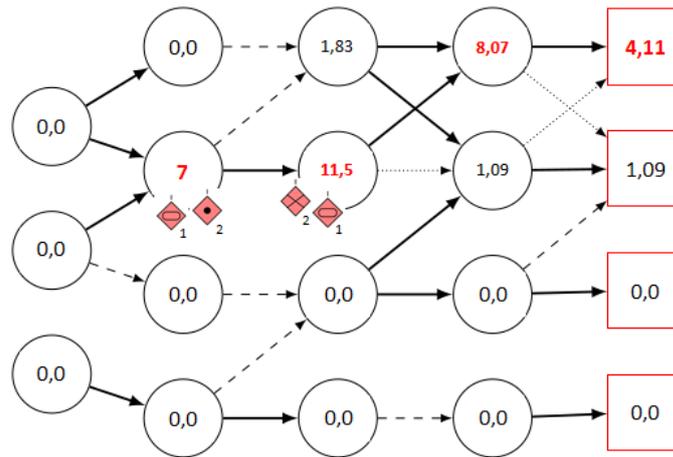
(a) Scenario 1 - attaque optimale

Company Type	t_1	t_2	t_3	t_4	t_5	t_6
◆Infantry	2 : z_1 1 : z_3	2 : z_5 1 : z_7	2 : z_9 1 : z_{10}	2 : z_{12} 1 : z_{14}	2 : z_{12} 1 : z_{14}	2 : a_1 1 : a_3
◆Tank	1 : z_3	2 : z_1 1 : z_3 1 : z_7	2 : z_5 1 : z_7 1 : z_{10}	2 : z_9 1 : z_{10} 1 : z_{14}	2 : z_{12} 2 : z_{14}	2 : a_1 2 : a_3
◆Artillery	\emptyset	1 : z_3	2 : z_1 1 : z_3 1 : z_7	2 : z_5 2 : z_7	2 : z_9 2 : z_{10}	2 : z_{12} 2 : z_{14}

(b) Scenario 2 - multi-objectifs

Company Type	t_1	t_2	t_3	t_4	t_5	t_6
◆Infantry	2 : z_2 1 : z_3	2 : z_6 1 : z_7	3 : z_{10}	3 : z_{13}	3 : z_{13}	3 : a_2
◆Tank	\emptyset	2 : z_2 1 : z_3	2 : z_6 1 : z_7	3 : z_{10}	3 : z_{13}	3 : a_2
◆Artillery	\emptyset	1 : z_3	1 : z_2 2 : z_3 1 : z_7	1 : z_6 3 : z_7	1 : z_7 3 : z_{10}	4 : z_{10}

(c) Scenario 3 - stratégie de feinte

FIGURE 10.2 – Exemple d'une carte de chaleur de menace du scénario 1 (à t_2)

10.2 Présentation des trois scénarios

Bien que les scénarios proposés se veuillent crédibles et plausibles, la maturité actuelle du système oblige à simplifier certains paramètres. De ce fait, nous considérons que l'ennemi va tout droit dans le sens où il ne fait pas de demi tour. Cependant, ces limites ne sont pas réellement impactantes car on imagine toujours le pire cas où la menace arrive le plus tôt possible. Chaque pas de temps, le système propose et compare les 5-best stratégies.

10.2.1 Premier scénario - preuve du concept

Le premier scénario sert de preuve que le concept fonctionne afin de démontrer l'efficacité du modèle de propagation de menace du fait qu'il révèle correctement la stratégie de l'ennemi.

Les premières compagnies observées sont dans les zones d'informations prioritaires (notées HPIZ pour *High Priority Information Zone*) z_1 et z_2 et vont à travers le chemin le plus optimal et efficace (z_5, z_9, z_{12}) pour aller vers le point d'attaque (noté AP pour *Attack Point*) a_1 . L'attaquant ne frappe qu'une cible dans ce scénario et y concentre toutes ses forces afin de réaliser une attaque-éclair.

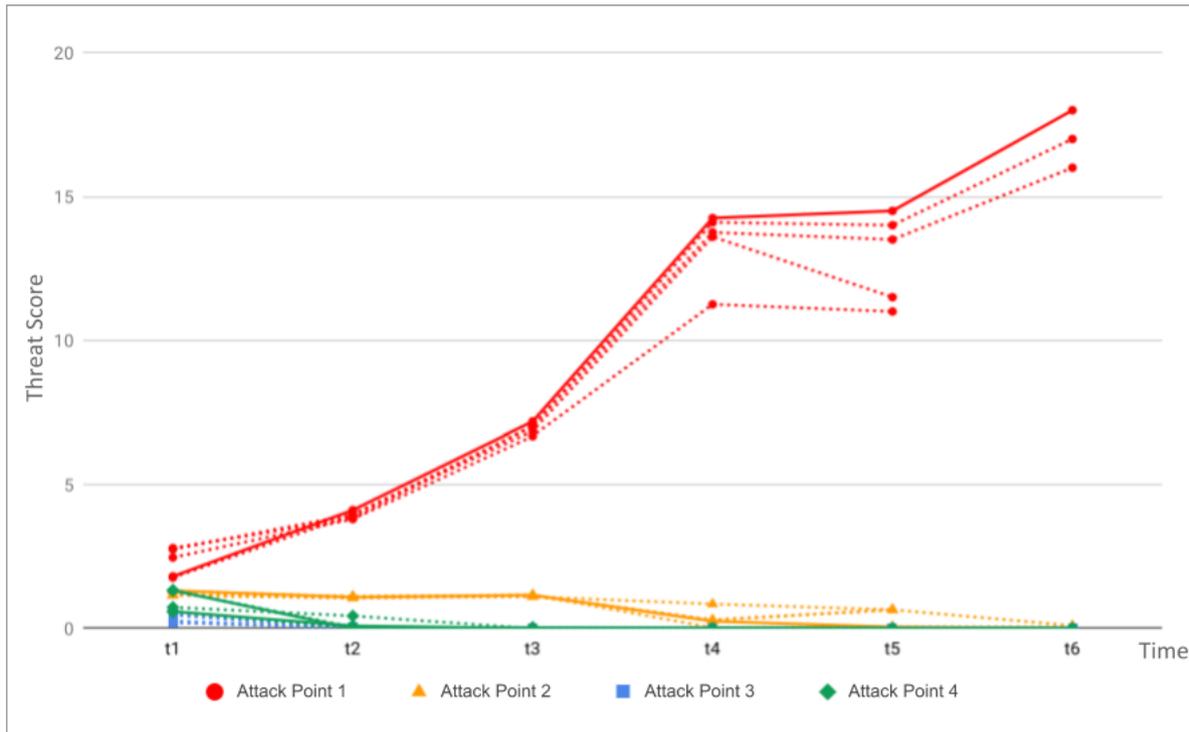
La Figure 10.3 montre clairement a_1 comme la seule cible dès l'étape de temps t_2 et cela est confirmé par toutes les stratégies 5-best et ce à toutes les étapes de temps suivantes.

La Figure 10.4 représente les résultats de la stratégie 1-best à t_2 . Cette étape de temps spécifique est intéressante à analyser car c'est le moment où la stratégie de l'ennemi commence à être inférée correctement.

Grâce à cela, l'opérateur humain est en mesure de comprendre que a_1 est sûrement la seule cible de l'attaque et que celle-ci peut se produire dans 3

TABLEAU 10.4 – Score de menace des points d'attaque (AP) - Scénario 1

AP	k-best	t_1	t_2	t_3	t_4	t_5	t_6
a_1	1-best	1,81	4,11	7,18	14,25	14,5	18
	2-best	1,77	3,96	7,01	14,1	14	17
	3-best	2,79	3,83	7,03	13,75	13,5	16
	4-best	2,75	3,96	6,86	13,6	11,5	-
	5-best	2,47	3,81	6,68	11,25	11	-
a_2	1-best	1,31	1,09	1,16	0,25	0,05	0
	2-best	1,3	1,1	1,17	0,02	0,05	0,05
	3-best	1,17	1,12	1,13	0,3	0,65	0,1
	4-best	1,15	1,06	1,14	0,28	0,65	-
	5-best	1,15	1,07	1,1	0,85	0,65	-
a_3	1-best	0,47	0	0	0	0	0
	2-best	0,47	0,02	0,02	0	0	0
	3-best	0,21	0,05	0	0	0	0
	4-best	0,21	0	0,02	0	0	-
	5-best	0,26	0,02	0	0	0	-
a_4	1-best	1,32	0	0	0	0	0
	2-best	1,32	0,04	0,03	0	0	0
	3-best	0,58	0,087	0	0	0	0
	4-best	0,58	0	0,03	0	0	-
	5-best	0,73	0,43	0	0	0	-

FIGURE 10.3 – Résultats des stratégies *5-best* pour le scénario 1

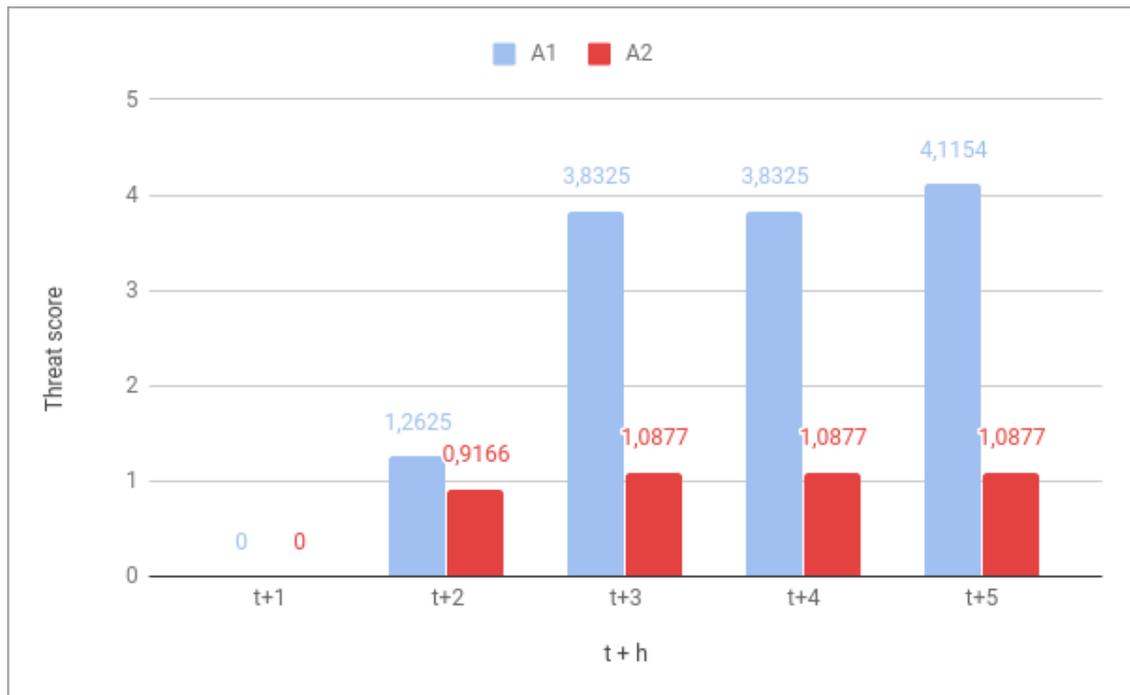
itérations de temps ($h = 3$) même si le score maximal de menace est atteint à $h = 5$. Le principal intérêt ici est de comprendre qu'il n'est pas nécessaire d'observer la zone a_1 avant $h = 3$, car aucune troupe ne peut y arriver avant, et de rester focalisé sur les HPIZ précédentes (dans ce cas z_{12} et z_{13}) pour confirmer ou non ce qui a été inféré.

Ce premier scénario confirme la capacité du système d'inférer correctement une attaque optimale dans un temps très satisfaisant. Cela permet d'optimiser les observations entre chaque étape de temps, et ainsi, d'être en mesure de mettre en place les contre-mesures nécessaires.

10.2.2 Second scénario - l'attaque multi-objectifs

Le deuxième scénario montre la capacité de monitorer une attaque multi-objectifs, c'est à dire sur plusieurs AP. Dans ce cas précis, les cibles sont a_1 et a_3 . Pour se faire, l'attaquant va se focaliser sur la ligne z_5, z_9, z_{12} (comme pour le premier scénario) et la ligne z_6, z_{10}, z_{13} en partant des HPIZ z_1 et z_2 .

Dans ce scénario, on constate tout d'abord qu'il n'y a pas systématiquement 5 stratégies comme dans la première itération de temps t_1 . Durant les deux premières étapes de temps, l'intention de l'ennemi n'est pas clairement identifiée comme nous pouvons le voir car l'AP a_4 est toujours considérée comme une cible potentielle. Cependant, le score de a_1 augmente substan-

FIGURE 10.4 – Horizon des évènements de la stratégie *1-best* à t_2 pour le scénario 1

tiellement. La fiabilité de la stratégie observée commence à être révélée à partir de t_4 où le score de menace de a_2 et a_4 diminue drastiquement pendant que celui de a_1 et a_3 augmente considérablement. Toutes les stratégies des *5-best* décrivent la même situation et à t_5 et t_6 , le système confirme bien que la stratégie de l'ennemi est d'attaquer à la fois a_1 et a_3 .

La Figure 10.6 est la représentation de la stratégie *1-best* à l'étape de temps t_3 où toutes les AP semblent être des cibles potentielles. L'histogramme montre que a_1 est très menacé dans un court laps de temps, $h = 2$. Pour toutes les autres AP, le delta entre les différents scores de menace ne sont pas assez fiables, cependant, le moment de l'attaque est assez proche. Ce qui est intéressant dans ce cas de figure, c'est de comprendre l'urgence des attaques potentielles et le temps qu'il reste même si nous ne sommes pas en mesure de définir la cible exactement.

Ces informations permettent à un expert humain de décider conséquemment quelles sont les zones à observer pour discriminer les AP entre elles et savoir lesquelles seront attaquées. Les a_2 , a_3 et a_4 sont suffisamment menacées pour les considérer comme cibles potentielles alors que a_1 est déjà connue comme cible dans la ou les prochaines itération(s) de temps.

Ce scénario confirme que notre système de propagation de menace automatisé est en mesure de révéler une attaque multi-objectifs dans un temps raisonnable avec une fiabilité élevée.

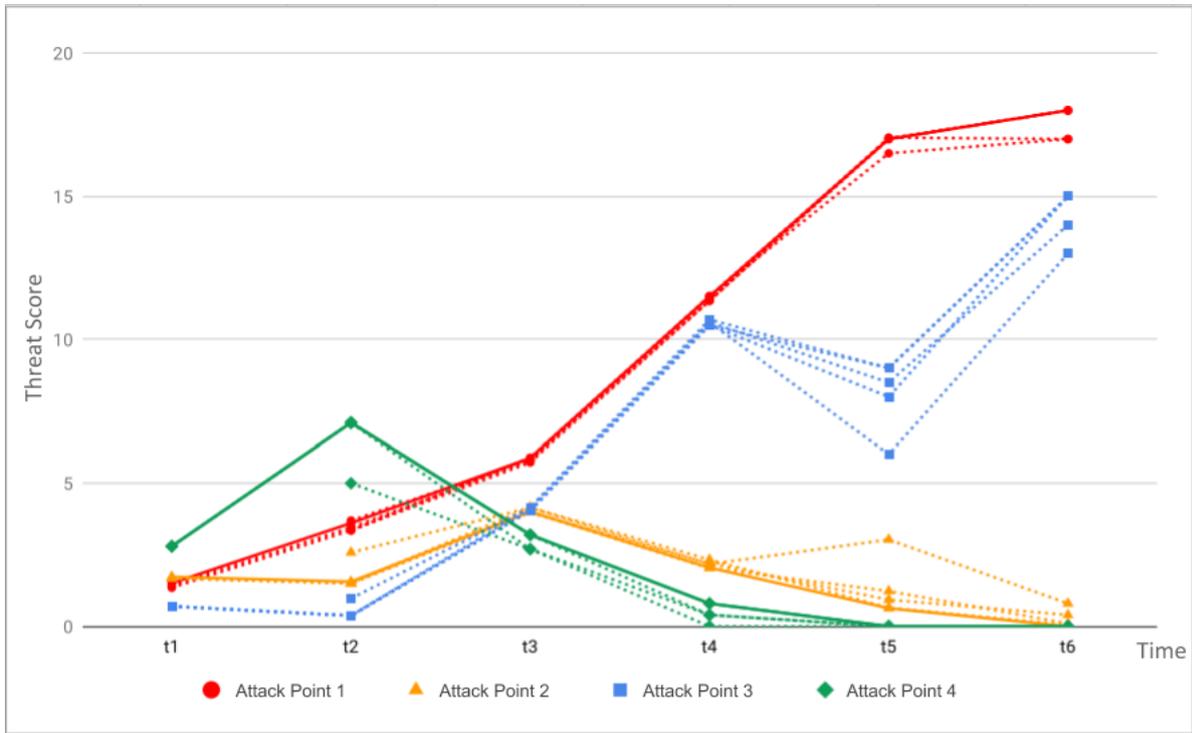


FIGURE 10.5 – Résultats des stratégies 5-best pour le scénario 1

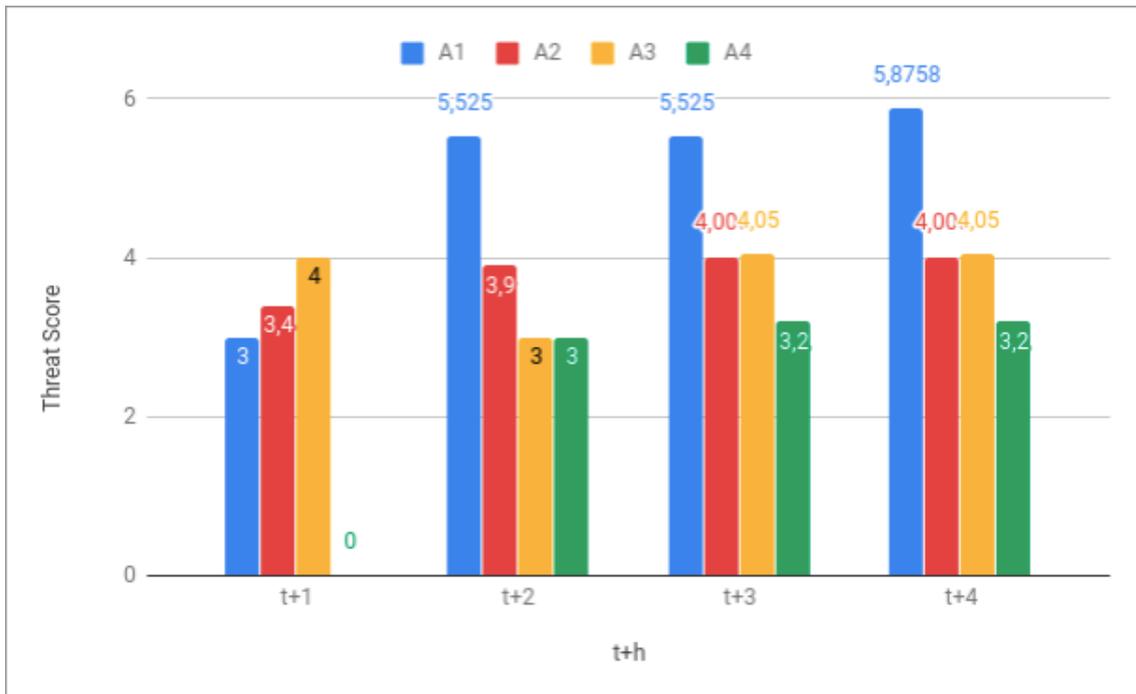


FIGURE 10.6 – Horizon des évènements de la stratégie 1-best à t₃ pour le scénario 2

TABLEAU 10.5 – Score de menace des points d'attaque (AP) - Scénario 2

AP	k-best	t_1	t_2	t_3	t_4	t_5	t_6
a_1	1-best	1,51	3,61	5,88	11,5	17	18
	2-best	1,43	3,45	5,8	11,51	17,02	18
	3-best	1,35	3,35	5,73	11,3	5 17,05	17
	4-best	-	3,35	5,88	11,51	16,5	17
	5-best	-	3,7	5,81	11,35	17	18
a_2	1-best	1,73	1,56	4,01	2,05	0,63	0
	2-best	1,7	1,5	3,99	2,19	0,93	0,4
	3-best	1,67	1,51	3,99	2,03	1,23	0,1
	4-best	-	1,51	4,15	2,33	0,65	0,05
	5-best	-	2,58	4,15	2,17	3,03	0,8
a_3	1-best	0,7	0,37	4,05	10,5	9	15
	2-best	0,7	0,37	4,05	10,6	8,5	14
	3-best	0,7	0,37	4,05	10,5	8	15
	4-best	-	0,37	4,15	10,7	9	15
	5-best	-	0,97	4,15	10,6	6	13
a_4	1-best	2,8	7,1	3,2	0,8	0	0
	2-best	2,8	7,1	3,2	0,4	0	0
	3-best	2,8	7,1	3,2	0,8	0	0
	4-best	-	7,1	2,7	0	0	0
	5-best	-	5	2,7	0,4	0	0

10.2.3 Troisième scénario - une stratégie de feinte

Le dernier scénario permet d'évaluer les limites du modèle dans sa formalisation actuelle avec une stratégie de feinte de l'attaquant. Cette fois, l'ennemi commence aux HPIZ z_2 et z_3 et passe à travers la ligne z_6, z_{10}, z_{13} et la ligne z_7, z_{10}, z_{13} pour faire croire à une attaque sur a_3 alors qu'en réalité, il compte changer au dernier moment sa trajectoire pour attaquer a_2 .

Ce scénario est plus complexe à inférer du fait que l'ennemi simule un comportement en feignant de suivre une trajectoire favorisant une attaque vers a_3 et finalement, finit par attaquer seulement a_2 .

Bien que le système présente a_2 comme la cible la plus menacée à t_4 , il faut attendre l'étape de temps suivante pour réellement comprendre l'intention de l'ennemi. Le delta entre a_2 et a_3 est suffisamment conséquent pour que l'on comprenne que seul a_2 sera la cible de l'attaque. Mais cette information arrive tardivement.

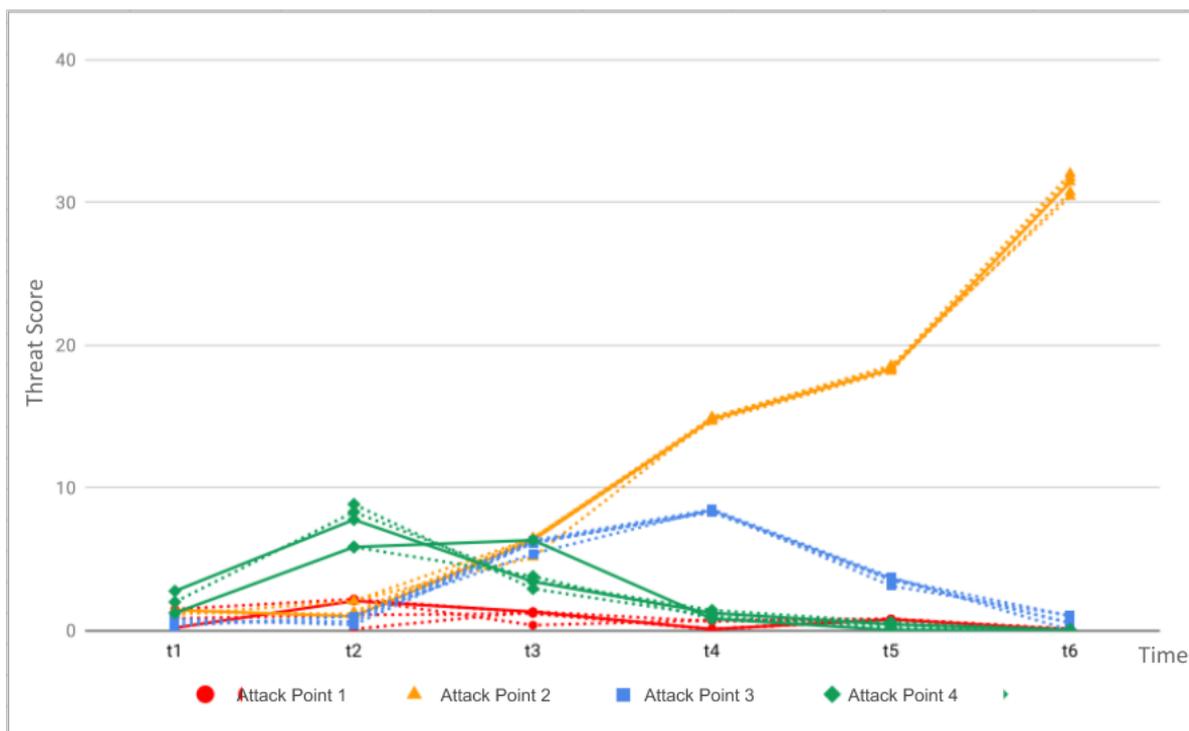


FIGURE 10.7 – Résultats des stratégies 5-best pour le scénario 3

Comme pour le second scénario, la Figure 10.8 (basé sur la stratégie 5-best à t_3) montre une attaque probable sur les deux prochaines itérations. Vu que les AP a_2 et a_3 sont les plus menacées, les prochaines zones à observer sont de façon évidente z_{13} et z_{14} . De plus, l'horizon des événements de ces deux zones montre que l'attaque va bientôt se produire et qu'obtenir l'information sur leur mouvement entre z_{13} et z_{14} permettrait très probablement de savoir avec une plus grande fiabilité quelle est la cible de l'attaque.

TABLEAU 10.6 – Score de menace des points d'attaque (AP) - Scénario 3

AP	k-best	t_1	t_2	t_3	t_4	t_5	t_6
a_1	1-best	0,16	2,05	1,29	0,06	0,75	0
	2-best	0,81	1,06	1,16	0,06	0,75	0,025
	3-best	1,46	2,17	1,21	0,07	0,76	0,05
	4-best	-	2,17	0,34	0,69	0,78	0,05
	5-best	-	0,07	1,29	0,61	0,75	0,075
a_2	1-best	1,40	0,96	6,31	14,77	18,27	31,4
	2-best	1,24	1,12	6,33	14,62	18,13	31,7
	3-best	1,08	2,04	5,11	14,91	18,41	32
	4-best	-	2,04	6,45	14,91	18,54	30,4
	5-best	-	1,28	6,46	14,76	18,27	30,7
a_3	1-best	0,78	0,37	6,1	8,35	3,6	1
	2-best	0,54	0,6	6,12	8,25	3,5	0,5
	3-best	0,3	0,97	5,35	8,45	3,7	0
	4-best	-	0,97	6,28	8,45	3,1	1
	5-best	-	0,82	6,2	8,35	3,6	0,5
a_4	1-best	2,74	7,74	3,4	1,2	0,4	0
	2-best	1,97	8,28	3,45	1,4	0,56	0
	3-best	1,2	5,82	6,3	0,8	0	0
	4-best	-	5,82	3,77	0,8	0,4	0
	5-best	-	8,82	2,9	1	0,16	0

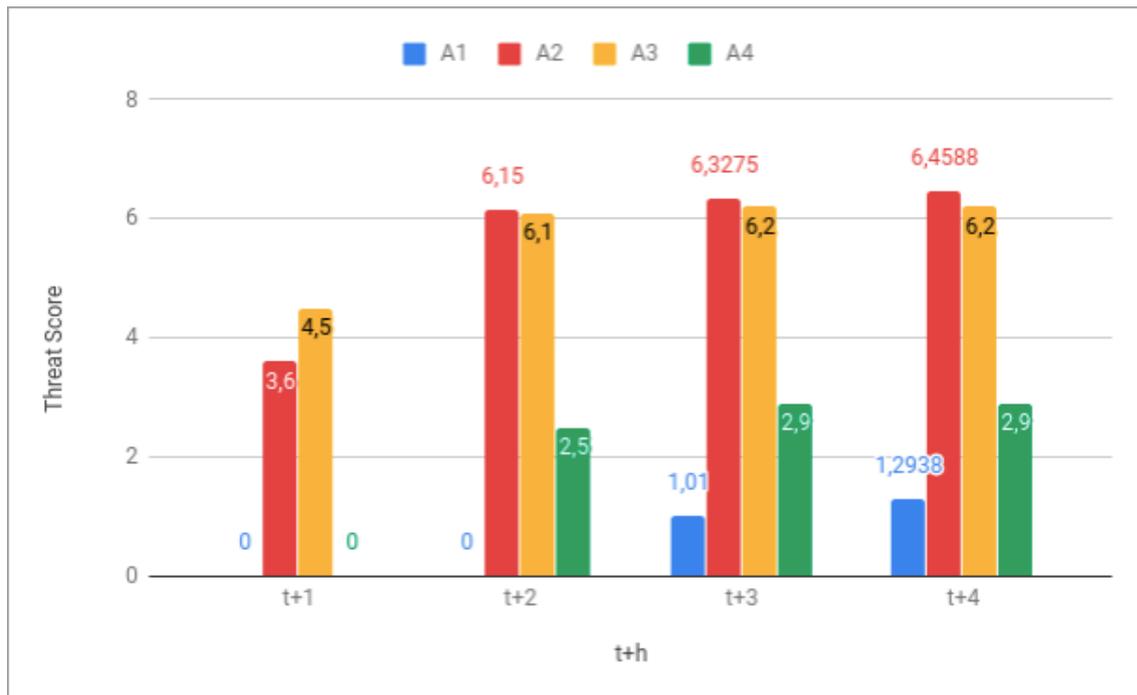


FIGURE 10.8 – Horizon des évènements de la stratégie 5-best à t_3 pour le scénario 3

Dans ce scénario, le système arrive à comprendre la stratégie de l'ennemi avec des résultats moins satisfaisants que dans les deux premiers cas. Bien que la cible soit confirmée avant l'attaque à t_5 , le score de menace des AP a été susceptible tout du long de mener l'expert dans une mauvaise appréhension de la stratégie de l'ennemi.

10.3 Conclusion

Cette expérimentation met en avant l'application de notre système de propagation de menace automatisé dans le cadre du domaine militaire dans une structure topologique. Les outils présentés permettent à un opérateur humain de monitorer une situation sur un champ de bataille et de comprendre les comportements ennemis. La stratégie de l'ennemi est correctement inférée en montrant la vulnérabilité de chaque cible et le temps avant que celles-ci soient attaquées. De plus, l'horizon des évènements permet de comprendre plus simplement quelles sont les zones à observer en priorité afin de mieux discriminer la stratégie de l'ennemi aux prochaines étapes de temps.

Cependant, deux types de limites ont été identifiés. Une stratégie où l'ennemi feint ralentit considérablement l'inférence et peut même mener à une mauvaise interprétation des cibles dans un premier temps. Les stratégies *k-best* peuvent ne pas être la meilleure des heuristiques pour comprendre un faux comportement des troupes ennemies.

Afin d'améliorer le système et de rendre plus réaliste les scénarios, il faut se focaliser pour la suite sur les possibilités de représenter des systèmes de défense sur les cibles qui peuvent être connues ou non par l'ennemi avec une certaine probabilité. Cette probabilité pourra diriger l'intention de l'ennemi sur son choix de cible qui pourra donc changer sa stratégie en cours de scénario.

Une autre perspective intéressante serait d'ajouter la possibilité pour un opérateur humain d'ajouter des informations sur des compagnies que nous ne sommes pas en mesure d'observer. Par exemple, le preneur de décision peut imaginer la présence d'autres troupes, comme des compagnies du génie militaire qui sont en mesure de faire des ponts pour que les tanks traversent les rivières. Cette fonctionnalité permettrait d'anticiper des stratégies potentielles grâce aux connaissances d'experts pendant le déroulement d'une attaque.

Enfin, une autre direction serait d'utiliser les travaux de N. Leguillarme ([Le Guillarme, 2016]) sur la tromperie dans la théorie des jeux.

CHAPITRE 11

Résultats préliminaire sur l'optimisation des capteurs

11.1 Un problème de complexité combinatoire

Le problème d'optimisation de l'utilisation des capteurs pour observer les variables de l'environnement peut-être considéré comme un problème d'association de graphe biparti (comme vu dans le Chapitre 8 Section 8.2). Le souci étant que sa complexité combinatoire rend ce problème difficilement traitable en des temps raisonnables. Et dans le cas de l'évaluation de situations (Chapitre 2), nous avons pu voir que la notion temporelle est vitale pour être en mesure de répondre à la mission. En effet, la complexité augmente en fonction du nombre de capteurs et du nombre de variables de façon quasi-exponentielle.

Le but ici est de montrer que l'algorithme proposé permet de réduire le champs d'exploration des associations et donc de réduire la complexité et le temps de calcul sans perdre en précision ni en efficacité sur les résultats attendus. Pour cela, nous proposons deux scénarios théoriques pour présenter nos résultats préliminaires.

11.2 Exemple scénario

Cette section décrit un premier exemple de scénario trivial afin de mettre en image le modèle (voir Figure 11.1). Dans ce scénario, l'environnement est composé de trois pièces et de trois capteurs. Les pièces sont les variables à observer afin de savoir si le terroriste se situe dans l'une d'elles. Les trois

capteurs sont composés de deux caméras fixes (c_1 et c_2) qui ne peuvent observer que la pièce dans laquelle ils se trouvent, et d'un observateur humain (o_1) qui peut se déplacer de sorte à pouvoir observer la pièce x ou la pièce z à travers des fenêtres. Soit formellement :

- Variables : $\mathcal{V} = \{x, y, z\}$
- Capteurs : $\mathcal{C} = \{c_1, c_2, o_1\}$
- Jeu d'action des capteurs :
 - $C_{c_1}^{\mathcal{A}} = \{look_x\}$
 - $C_{c_2}^{\mathcal{A}} = \{look_y\}$
 - $C_{o_1}^{\mathcal{A}} = \{look_x, look_z\}$

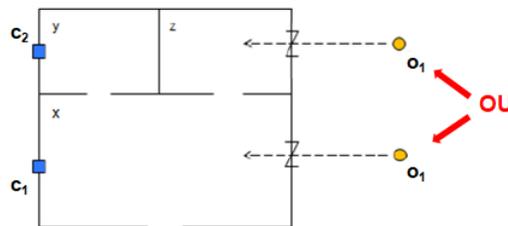


FIGURE 11.1 – Schéma du scénario

On présume que la variable utile définie en entrée de notre modèle est la variable x . Cela implique donc :

- $\mathcal{D} = \{x\}$
- $\mathcal{Q} = \{y, z\}$
- $\mathcal{R} = \{c_1, o_1\}$
- $\mathcal{U} = \{c_2\}$

11.2.1 Première étape

La première étape de notre processus est représentée par les graphiques de la Figure 11.2. Les *scores* des degrés de confiance des capteurs et de la richesse d'informations d'un capteur sur une variable ont été définis arbitrairement pour souligner le propos.

Dans cet exemple, il y a 2 combinaisons d'actions possibles, donc 2 graphes. L'un où $c_1^{a_1} = stay$ et $o_1^{a_2} = move_to_x$ et l'autre où seul c_1 regarde la pièce x car o_1 est dans l'action $look_z$.

L'algorithme se déroulera de la façon suivante :

- **Première combinaison :**

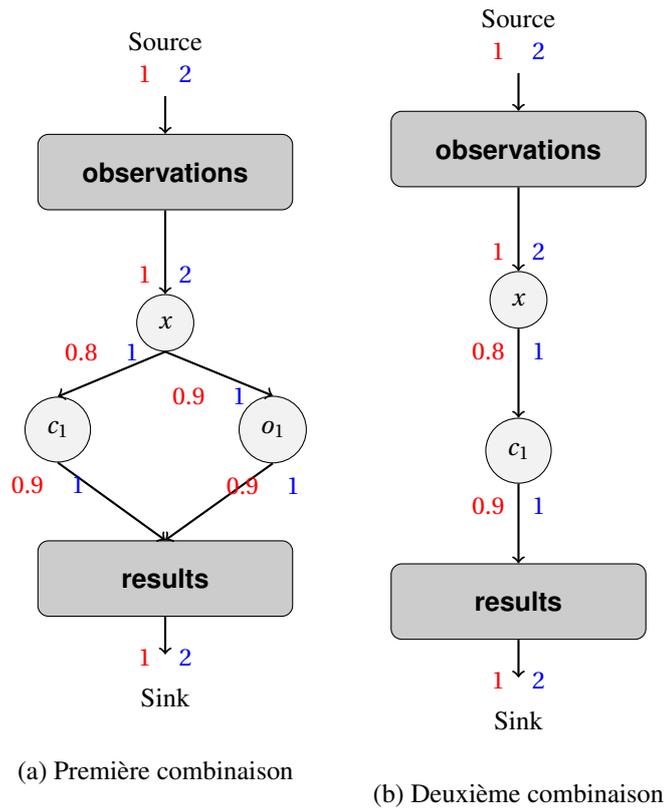


FIGURE 11.2 – Combinaisons possibles

- Premier flot $f_1 : s \rightarrow x \rightarrow o_1 \rightarrow t$ avec un score $s = 3.8$ et de poids $w = 1$
- Second flot $f_2 : s \rightarrow x \rightarrow c_1 \rightarrow t$ avec un score $s = 3.7$ et de poids $w = 1$
- Fin : le graphe est en situation de flot maximal avec un score total $s = 7.5$.

• **Deuxième combinaison :**

- Premier flot $f_1 : s \rightarrow x \rightarrow c_1 \rightarrow t$ avec un score $s = 3.7$ et de poids $w = 1$
- Fin : le graphe est en situation de flot maximal avec un score total $s = 3.7$.

Dans cet exemple, la première combinaison obtient le score le plus élevé, et donc représente le jeu d'actions optimal à mettre en place à $t + 1$.

Une première remarque est que tous les flots sont bien de poids $w = 1$. Donc il faut autant de flots que la capacité du puits peut en recevoir. Par exemple, dans la première combinaison, $c^{(t)} = 2$, il faut bien 2 flots pour saturer le graphe. Toujours dans la première combinaison, les flots ont été ordonnés via leur score, ce qui explique que le premier flot passe par le capteur o_1 .

11.2.2 Deuxième étape

La deuxième partie va consister à finir de couvrir le reste des variables (non-utiles). Il en résulte le graphe Figure 11.3.

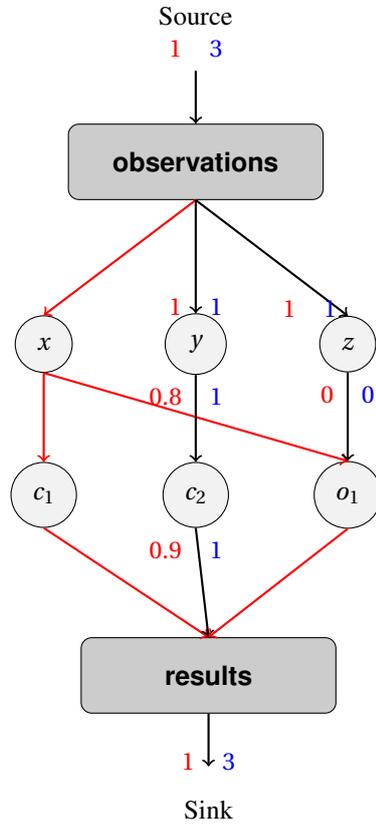


FIGURE 11.3 – Résultats de l'étape 2

En appliquant le sous-graphe de la première étape à ce graphe, nous saturons l'axe de la source vers x . les axes de x vers c_1 et o_1 sont eux aussi saturés. Enfin les axes de c_1 et o_1 vers le puits sont eux aussi saturés car $|\mathcal{F}_a^{\mathcal{V}}(c_1)| = |\mathcal{F}_a^{\mathcal{D}}(c_1)|$ et de même pour o_1 .

De là, nous avons une *capacité* du puits telle que $c^{(t)} = 3$ avec un flot montant le poids du puits à 2. Donc il nous faudra un seul flot pour atteindre notre flot maximal.

- Premier flot $f_1 : s \rightarrow y \rightarrow c_2 \rightarrow t$ avec un *score* $s = 2.7$ et de poids $w = 1$
- Fin : le graphe est en situation de flot maximal.

Nous avons donc maximisé la couverture de notre environnement observable ce qui nous a permis de définir le jeu d'actions optimal à réaliser sur nos capteurs dans \mathcal{R} pour l'itération suivante ainsi que la couverture possible des variables non-utiles.

Dans ce cas, on constate que la variable z ne sera pas observée au prochain pas de temps. Il est à noter que le fait que donner une priorité sur la couverture de certaines variables peut amener à ne plus en observer d'autres.

11.3 Premières expérimentations :

L'implémentation de ce modèle a été réalisée en Java. Le but est de développer une brique de façon indépendante pouvant par la suite se connecter aux autres briques du système global ¹.

La brique logicielle du modèle prend en entrée un environnement décrit au format Json ². Il génère l'environnement à partir du fichier Json puis applique l'algorithme du modèle. En sortie, il renvoie (toujours au format Json) l'environnement mis à jour avec le meilleur jeu d'actions des capteurs utiles. Cette sortie servira d'entrée à la brique de collecte de notre système ASAAP.

11.3.1 Test sur le premier scénario

Le scénario décrit précédemment a été proposé à la brique qui a obtenu les résultats attendus. À la fin du traitement, nous obtenons en sortie le jeu d'action optimal, les différents scores de chaque graphe généré pour la première étape de l'algorithme et enfin, des graphes sont générés en image représentant les différentes combinaisons ainsi que le graphe de résultat final (comme le montrent les figures 11.4 et 11.5).

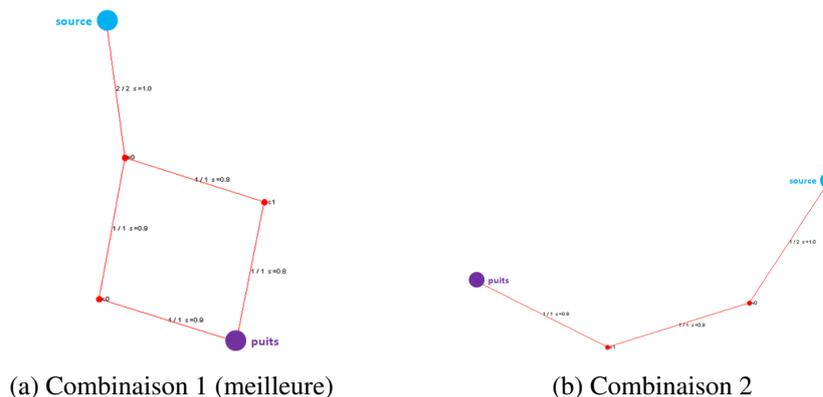


FIGURE 11.4 – Premier scénario : combinaisons étape 1

Les deux combinaisons qui sont proposés dans la Figure 11.4 sont les deux seules possibles avec (a) la combinaison la plus optimale où le capteur c_1 (correspondant à c_1) et le capteur c_0 (correspondant à o_1) observe tous deux

1. Voir le résumé du Processus d'évaluation de situation

2. JavaScript Object Notation : syntaxe permettant de stocker ou d'échanger des données rapidement

la variable utile v_0 (correspondant à x) alors que dans la combinaison (b), seul c_1 observe v_0 car c_0 observerait v_2 . Dans le premier cas (a) nous obtenons un score total sur l'observation de x de $s = 2.6$ et sur (b) un score de $s = 4.4$. La première combinaison est donc celle choisie.

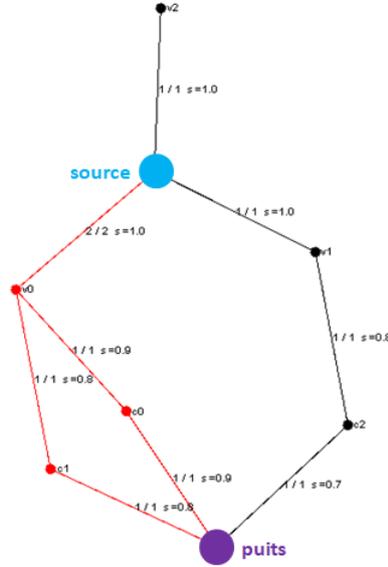


FIGURE 11.5 – Premier scénario : résultats étape 2

Dans la Figure 11.5, on applique la deuxième étape de l'algorithme pour tenter de couvrir les variables non-utiles avec les capteurs restant, ce qui amène c_2 (correspondant à c_2) à observer v_1 (correspondant à y) et la variable v_2 (correspondant à z) n'est du coup pas observée.

11.3.2 Test sur le second scénario

Un second scénario théorique a été mis en place avec plus de variables et plus de capteurs. L'environnement est composé de 6 variables pour 4 capteurs, avec 2 à 3 actions par capteurs. Cela amène à 18 combinaisons d'actions possibles dans le cas testé avec comme variables utiles $\mathcal{D} = \{v_0, v_1\}$. Dans le cas où nous n'aurions pas priorisé l'observation des variables les plus utiles, nous obtiendrions 54 combinaisons à étudier. Et aucune des combinaisons n'étant pas celles obtenues par la priorisation des variables les plus utiles (les 38 autres combinaisons) n'obtiennent un score supérieur à ces dernières.

La Figure 11.6 nous présente les trois meilleurs scores de combinaisons (a), (b) avec (d) qui est la meilleure des trois combinaisons. Et la combinaison (c) qui possède le moins bon score des 18 combinaisons. Cette dernière nous montre que nous calculons potentiellement des combinatoires qui n'ont peu, voire aucune chance d'être retenues car elle ne permettent pas l'observation de toutes les variables utiles.

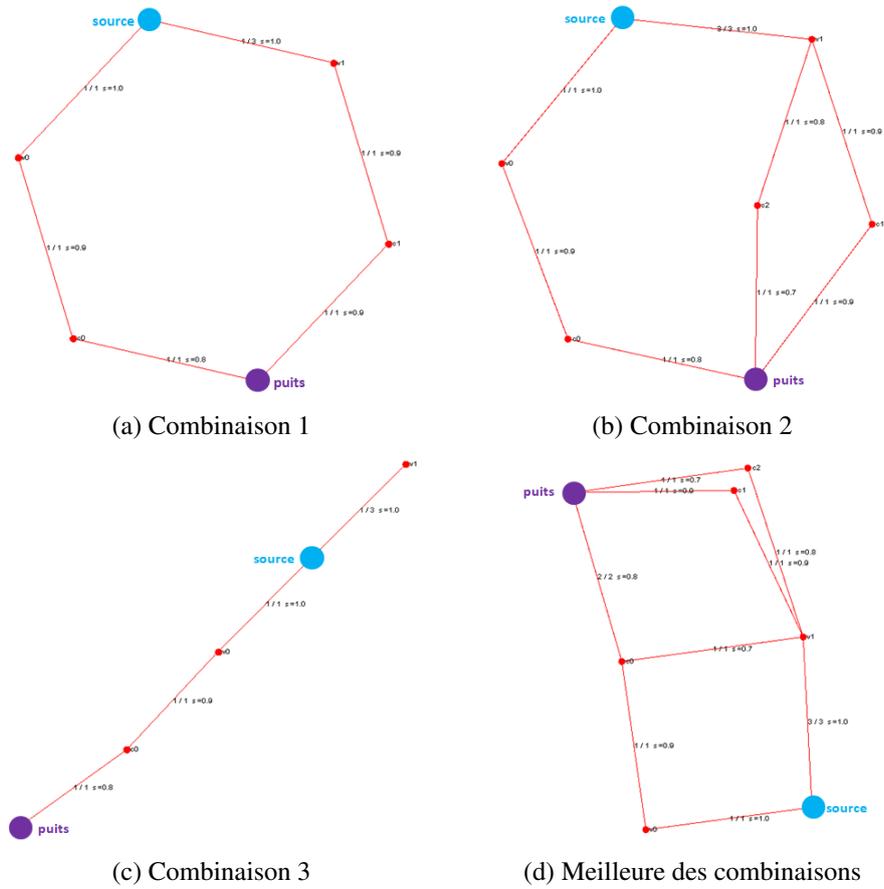


FIGURE 11.6 – Deuxième scénario : quelques exemples de l'étape 1

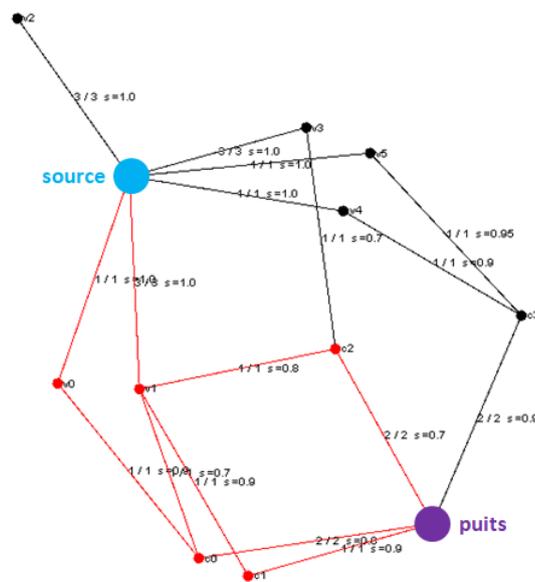


FIGURE 11.7 – Second scénario : résultats étape 2

La Figure 11.7 montre l'association optimale où la variable v_2 n'est pas observé pour permettre de concentrer les capteurs c_0 sur v_0 et c_1 et c_2 qui observent v_1 . De fait, v_2 , v_3 et v_4 ne sont pas observés et c_3 observe v_5 .

A travers ces exemples (Figure 11.6c), on peut s'apercevoir que certaines combinaisons sont susceptibles d'empêcher l'observation de certaines variables utiles. Ce point est intéressant et amène à penser qu'une heuristique sera probablement nécessaire pour réduire encore le champ d'exploration des combinaisons dès lors qu'elles ne permettent pas d'observer toutes les variables utiles (à savoir, moins de variables que d'autres combinaisons). Les temps de calcul sont inférieurs à une seconde, mais cela reste un scénario simple en terme de complexité par rapport à un scénario réaliste.

11.4 Conclusion

L'objectif de ces résultats préliminaires était de réduire le champ d'exploration des combinaisons possibles afin de ne pas calculer celles qui n'ont aucune chances d'être retenues car sous-optimales dans l'observation de l'environnement.

Le modèle fonctionne comme attendu au vu des premiers résultats. En effet, les combinaisons possibles qui ne couvrent pas de façon prioritaire les variables les plus utiles proposent des résultats avec des scores systématiquement en dessous des combinaisons priorisant les variables utiles.

L'implémentation a été réalisée de sorte à pouvoir être connectée facilement dans le système global afin de faciliter le futur développement des autres briques et les futures améliorations qui seront à apporter à l'ensemble du système.

Cependant, il est nécessaire de pouvoir tester les algorithmes sur des scénarios plus réalistes et donc plus complexes afin d'estimer le risque sur le passage à l'échelle dû à l'explosion combinatoire en fonction du nombre de capteurs. De plus, il faut étudier d'autres possibilités d'heuristiques pour voir s'il n'est pas possible de réduire encore plus le nombre de combinaisons à étudier pour trouver la combinaison optimale.

Quatrième partie

Conclusion et perspectives

CHAPITRE 12

Synthèse

Dans cette thèse nous nous intéressons au problème d'évaluation de situations et plus particulièrement au cas des situations de crise.

L'évaluation de situations nécessite de réfléchir à plusieurs problèmes dont la fusion d'informations, la représentation de connaissances et la modélisation de l'environnement à analyser, l'inférence des états des objets de l'environnement et l'optimisation de l'utilisation des capteurs.

Dans ce chapitre, nous proposons une synthèse des travaux réalisés avec leurs avantages et leurs limites ainsi que les perspectives des travaux à venir.

12.1 Un système d'évaluation de situation automatisé

L'étude des différents domaines connexes à l'évaluation de situations de crise a mené à la définition du système ASAAP (*Automated Situation Awareness for Active Perception*). Ce système est une répartition en trois briques majeures avec la brique de fusion d'informations, la brique d'analyse des variables et la brique d'optimisation des capteurs.

Nos travaux ont permis des contributions dans la brique d'analyse des variables les plus utiles (*Most Valuable Variables*) avec la mise en place d'une perception active en cherchant à comprendre quelles sont les variables qui permettront de maximiser le gain d'informations sur la situation que nous cherchons à évaluer.

L'autre principale contribution est celle de la propagation de menace appliquée au domaine de la défense et du renseignement. Ce procédé permet de

définir une carte de chaleur de la menace sur un graphe topologique représentant la carte du champs de bataille afin d'estimer quelle(s) zone(s) sera(ont) attaquée(s) et par quel chemin.

Des travaux préliminaires ont aussi permis de proposer une première solution pour la brique d'optimisation de l'utilisation des capteurs. Cette brique fait suite à l'analyse des variables les plus utiles afin de maximiser la couverture en terme d'observation de ces dernières.

Enfin, la brique fusion a permis des travaux en parallèle de la thèse qui seront discutés dans le Chapitre 13.

Notre système reste cependant incomplet et nécessitera encore des travaux pour être fonctionnel. En effet, les briques ne sont pas encore mises les unes avec les autres pour une expérimentation globale et elles nécessitent des améliorations. L'heuristique d'optimisation des capteurs notamment méritera d'être approfondie et testée sur des scénarios plus réalistes. De plus le système est basé actuellement sur une planification "myope" (c'est à dire sur une optimisation pour le pas de temps suivant) alors qu'il faudrait pouvoir essayer d'optimiser et de permettre des actions qui anticipent à plusieurs pas de temps à l'avance.

12.2 Champs d'applications possibles

Le principal champ d'application retenu dans ces travaux et celui du domaine de la défense et du renseignement avec les expérimentations sur les scénarios OPEX (OPération EXtérieure) où la situation à évaluer et celle d'une attaque sur un champ de bataille. Un deuxième champ d'application est celui de la surveillance maritime avec notamment l'évaluation de menace de navires.

Cependant, nous pouvons facilement imaginer d'autres champs applicatifs avec quelques travaux d'adaptations sur les modèles. Il pourrait s'agir d'aide aux secours pour la gestion de catastrophes naturelles en estimant les zones les plus dangereuses et prioritaires à gérer en premier en fonction du nombre de personnes présentes dans ces zones par exemple.

Nous pouvons aussi imaginer la gestion de manifestations avec des zones de débordements à gérer en fonction des événements en temps réel. Anticiper les zones dangereuses ou susceptibles de le devenir pour mettre en place les dispositifs des forces de l'ordre afin d'empêcher au mieux les mouvements de violence.

Il est aussi possible d'imaginer un cas applicatif en épidémiologie où la situation de crise serait une épidémie qui se propage via différents foyers infectieux. Et le but serait de comprendre et prioriser les zones à protéger et

confiner pour limiter la diffusion de la maladie.

12.3 Liste des publications réalisées au sein de la thèse

Les travaux présentés dans cette thèse ont permis la réalisation de quatre articles et d'un brevet dont voici la liste :

- Articles :
 - Multi-Level Information Fusion Approach with Dynamic Bayesian Networks for an Active Perception of the environment, *K. Vasnier, A-I. Mouaddib, S. Gatepaille, & S. Brunessaux*, In 21st International Conference on Information Fusion (FUSION), IEEE, 2018, pp. 1844-1850.
 - Multi-Level Information Fusion and Active Perception Framework : Towards a Military Application, *K. Vasnier, A-I. Mouaddib, S. Gatepaille, & S. Brunessaux*, In NATO SET-262 RSM on Artificial Intelligence for Military Multisensor Fusion Engines, 2018.
 - Automated threat propagation model through a topographical environment modelling, *K. Vasnier, A-I. Mouaddib, S. Gatepaille, & S. Brunessaux*, In 19th International Conference on Intelligent Systems Design and Applications (ISDA), Springer, 2019.
 - An automated system of threat propagation using a horizon of events model, *K. Vasnier, A-I. Mouaddib, S. Gatepaille, & S. Brunessaux*, In Intelligent System Conference (IntelliSys2020), Springer, 2020.
- Brevet :
 - Procédé et système de fusion d'informations, *K. Vasnier, V. Justine, & S. Gatepaille*, n° FR1906376, 04/06/2019.

CHAPITRE 13

Perspectives

13.1 Perspectives à court terme

Les premiers points d'amélioration qui sont à réaliser concernent tout d'abord la modélisation et le scénario OPEX pour la propagation de menace. En effet, des opérationnels sont intéressés par ces travaux et il faudrait réussir à complexifier encore les scénarios en ajoutant des paramètres ou des informations supplémentaires. Par exemple, des systèmes de défenses qui pourront ou non être connus par l'ennemi, mais aussi d'autres types de compagnie.

L'autre perspective immédiate, serait de faire fonctionner ensemble le système d'analyses de variables les plus utiles (*Most Valuable Variables*, MVV) avec le système d'optimisation d'utilisation des capteurs pour comparer les résultats sur des scénarios plus longs.

13.2 Perspectives à moyen terme

Pour ce qui est de la propagation de menace, le scénario où l'ennemi cherche à duper le défenseur montre des limites sur l'efficacité de la prédiction. Les travaux présentés par [Le Guillaume, 2016] ont modélisé la prise en compte de la tromperie. Il serait très intéressant de voir si l'utilisation de ces travaux permettrait d'améliorer le système que nous proposons dans cette thèse.

Enfin, le système d'optimisation de l'utilisation des capteurs ne permet une optimisation qu'à court terme (c'est à dire uniquement au pas de temps suivant). Le principal problème est que des actions qui pourraient ne pas

maximiser l'information immédiatement ne seront jamais choisies alors qu'elles seraient optimales malgré tout d'ici deux à trois pas de temps par exemple. Il faudrait mettre en place une fonction d'utilité/coût permettant d'optimiser en imaginant les conséquences d'une action à horizon lointain (sur plusieurs itération de temps).

13.3 Perspective à long terme

Les travaux sur la fusion d'informations réalisés en parallèle de cette thèse au sein d'Airbus permettraient de développer une première brique de fusion qui pourrait être intégrée au système ASAAP. Cependant, il reste encore des travaux à réaliser pour qu'elle puisse être complète et intégrable de sorte à faire fonctionner l'intégralité du système.

Une dernière perspective serait de permettre à l'opérateur humain (le preneur de décision) de pouvoir ajouter des informations par lui-même afin que le système les prenne en compte et pouvoir tester des scénarios alternatifs considérants que nous n'avons pas été en mesure de tout observer. Cela apporterait cependant une nouvelle complexité et une mise à jour de la boucle logique du traitement des informations.

Cinquième partie

Annexes

Liste des publications

Articles :

- Multi-Level Information Fusion Approach with Dynamic Bayesian Networks for an Active Perception of the environment, *K. Vasnier, A-I. Mouaddib, S. Gatepaille, & S. Brunessaux*, In 21st International Conference on Information Fusion (FUSION), IEEE, 2018, pp. 1844-1850.
- Multi-Level Information Fusion and Active Perception Framework : Towards a Military Application, *K. Vasnier, A-I. Mouaddib, S. Gatepaille, & S. Brunessaux*, In NATO SET-262 RSM on Artificial Intelligence for Military Multisensor Fusion Engines, 2018.
- Automated threat propagation model through a topographical environment modelling, *K. Vasnier, A-I. Mouaddib, S. Gatepaille, & S. Brunessaux*, In 19th International Conference on Intelligent Systems Design and Applications (ISDA), Springer, 2019.
- An automated system of threat propagation using a horizon of events model, *K. Vasnier, A-I. Mouaddib, S. Gatepaille, & S. Brunessaux*, In Intelligent System Conference (IntelliSys2020), Springer, 2020.

Brevet :

- Procédé et système de fusion d'informations, *K. Vasnier, V. Justine, & S. Gatepaille*, n° FR1906376, 04/06/2019.

Bibliographie

- [Aamodt and Nygård, 1995] Aamodt, A. and Nygård, M. (1995). Different roles and mutual dependencies of data, information, and knowledge—an ai perspective on their integration. *Data & Knowledge Engineering*, 16(3) :191–222. 46
- [Ajroud et al., 2012] Ajroud, A., Omri, M. N., Youssef, H., and Benferhat, S. (2012). Loopy belief propagation in bayesian networks : origin and possibilistic perspectives. *arXiv preprint arXiv :1206.0976*. xvi, 72
- [Allen and Darwiche, 2002] Allen, D. and Darwiche, A. (2002). New advances in inference by recursive conditioning. In *Proceedings of the Nineteenth conference on Uncertainty in Artificial Intelligence*, pages 2–10. Morgan Kaufmann Publishers Inc. 56
- [Bajcsy, 1988] Bajcsy, R. (1988). Active perception. *Proceedings of the IEEE*, 76(8) :966–1005. 37
- [Baxter et al., 1999] Baxter, J., Tridgell, A., and Weaver, L. (1999). Knightcap : a chess program that learns by combining td (λ) with game-tree search. *arXiv preprint cs/9901002*. 67
- [Bayes, 1763] Bayes, T. (1763). Lii. an essay towards solving a problem in the doctrine of chances. by the late rev. mr. bayes, frs communicated by mr. price, in a letter to john canton, amfr s. *Philosophical transactions of the Royal Society of London*, (53) :370–418. 53
- [Bellenger, 2013] Bellenger, A. (2013). *Semantic Decision Support for Information Fusion Applications*. PhD thesis, Rouen, INSA. xv, xvi, 35, 46, 47, 49, 52
- [Bellinger et al., 2004] Bellinger, G., Castro, D., and Mills, A. (2004). Data, information, knowledge, and wisdom. 46
- [Bestman, 1995] Bestman, M. (1995). The semiotic triangle. 45

- [Biferno and Dawson, 1977] Biferno, M. A. and Dawson, M. E. (1977). The onset of contingency awareness and electrodermal classical conditioning : An analysis of temporal relationships during acquisition and extinction. *Psychophysiology*, 14(2) :164–171. 10
- [Blasch, 2006] Blasch, E. (2006). Sensor, user, mission (sum) resource management and their interaction with level 2/3 fusion. In *2006 9th International Conference on Information Fusion*, pages 1–4. IEEE. 26
- [Blasch and Plano, 2005] Blasch, E. and Plano, S. (2005). Dfig level 5 (user refinement) issues supporting situational assessment reasoning. In *2005 7th International Conference on Information Fusion*, volume 1, pages xxxv–xliii. IEEE. 26
- [Blasch et al., 2012] Blasch, E. P., Lambert, D. A., Valin, P., Kokar, M. M., Llinas, J., Das, S., Chong, C., and Shahbazian, E. (2012). High level information fusion (hlif) : Survey of models, issues, and grand challenges. *IEEE Aerospace and Electronic Systems Magazine*, 27(9) :4–20. xv, 31
- [Blasch and Plano, 2003] Blasch, E. P. and Plano, S. (2003). Ontological issues in higher levels of information fusion : User refinement of the fusion process. Technical report, AIR FORCE RESEARCH LAB WRIGHT-PATTERSON AFB OH. 26
- [Boisot and Canals, 2004] Boisot, M. and Canals, A. (2004). Data, information and knowledge : have we got it right? *Journal of evolutionary economics*, 14(1) :43–67. 46
- [Borst, 1999] Borst, W. N. (1999). Construction of engineering ontologies for knowledge sharing and reuse. 48
- [Boyd, 1987] Boyd, J. R. (1987). Organic design for command and control. *A discourse on winning and losing*. 14
- [Brehmer, 2005] Brehmer, B. (2005). The dynamic ooda loop : Amalgamating boyd’s ooda loop and the cybernetic approach to command and control. In *Proceedings of the 10th international command and control research technology symposium*, pages 365–368. 15
- [Chanel et al., 2012] Chanel, C. C., Teichteil-Königsbuch, F., and Lesire, C. (2012). Pomdp-based online target detection and recognition for autonomous uavs. 130
- [Chavira and Darwiche, 2005] Chavira, M. and Darwiche, A. (2005). Compiling bayesian networks with local structure. In *IJCAI*, volume 5, pages 1306–1312. 56
- [Cheng and Druzdzel, 2000] Cheng, J. and Druzdzel, M. J. (2000). Ais-bn : An adaptive importance sampling algorithm for evidential reasoning

- in large bayesian networks. *Journal of Artificial Intelligence Research*, 13 :155–188. 56
- [Claverie and Desclaux, 2016] Claverie, B. and Desclaux, G. (2016). C2-command and control : un système de systèmes pour accompagner la complexité. *Communication Organisation*, (2) :255–278. 14
- [Cooper, 1990] Cooper, G. F. (1990). The computational complexity of probabilistic inference using bayesian belief networks. *Artificial intelligence*, 42(2-3) :393–405. 56, 73
- [Darwiche, 2001] Darwiche, A. (2001). Recursive conditioning. *Artificial Intelligence*, 126(1-2) :5–41. 56
- [Dastani et al., 2005] Dastani, M., Hulstijn, J., and Van der Torre, L. (2005). How to decide what to do? *European Journal of Operational Research*, 160(3) :762–784. 71
- [Davis et al., 1993] Davis, R., Shrobe, H., and Szolovits, P. (1993). What is a knowledge representation? *AI magazine*, 14(1) :17–17. 45
- [Dawson and Biferno, 1973] Dawson, M. E. and Biferno, M. A. (1973). Concurrent measurement of awareness and electrodermal classical conditioning. *Journal of Experimental Psychology*, 101(1) :55. 10
- [Dean and Kanazawa, 1989] Dean, T. and Kanazawa, K. (1989). A model for reasoning about persistence and causation. *Computational intelligence*, 5(2) :142–150. 57
- [Dechter, 1999] Dechter, R. (1999). Bucket elimination : A unifying framework for reasoning. *Artificial Intelligence*, 113(1-2) :41–85. 56
- [Dietze and Domingue, 2009] Dietze, S. and Domingue, J. (2009). Bridging between sensor measurements and symbolic ontologies through conceptual spaces. xv, 32, 33, 34
- [Dretske, 1981] Dretske, F. (1981). The pragmatic dimension of knowledge. *Philosophical studies*, 40(3) :363–378. 46
- [Dubois, 2007] Dubois, D. (2007). Uncertainty theories : a unified view. In *IEEE Cybernetic Systems Conference, Dublin, Ireland, Invited Paper*, pages 4–9. 52
- [Edmonds and Karp,] Edmonds, J. and Karp, R. M. Theoretical improvements in algorithmic efficiency for network flow problems,’. *J. ACM*, 19(2) :248264. 112
- [Endsley, 1995] Endsley, M. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1). 18

- [Endsley, 1987] Endsley, M. R. (1987). Sagat : A methodology for the measurement of situation awareness (nor doc 87-83). *Hawthorne, CA : Northrop Corporation*. 18
- [Endsley, 1988a] Endsley, M. R. (1988a). Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors Society annual meeting*, volume 32, pages 97–101. SAGE Publications Sage CA : Los Angeles, CA. 18
- [Endsley, 1988b] Endsley, M. R. (1988b). Situation awareness global assessment technique (sagat). In *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, pages 789–795. IEEE. 18
- [Fein and Vossekuil, 1998] Fein, R. A. and Vossekuil, B. (1998). *Protective intelligence and threat assessment investigations : A guide for state and local law enforcement officials*. DIANE Publishing. 64
- [Fein et al., 1995] Fein, R. A., Vossekuil, B., and Holden, G. A. (1995). *Threat assessment : An approach to prevent targeted violence*, volume 2. US Department of Justice, Office of Justice Programs, National Institute of 65
- [Fenz et al., 2009] Fenz, S., Tjoa, A. M., and Hudec, M. (2009). Ontology-based generation of bayesian networks. In *2009 International Conference on Complex, Intelligent and Software Intensive Systems*, pages 712–717. IEEE. 58
- [Foo and Ng, 2013] Foo, P. H. and Ng, G. W. (2013). High-level information fusion : An overview. *J. Adv. Inf. Fusion*, 8(1) :33–72. 22, 30
- [Ford Jr, 1956] Ford Jr, L. R. (1956). Network flow theory. Technical report, Rand Corp Santa Monica Ca. 84
- [Forrester, 1971] Forrester, J. W. (1971). *World dynamics*. Wright-Allen Press. 11
- [García González et al., 2005] García González, R. et al. (2005). *A semantic web approach to digital rights management*. Universitat Pompeu Fabra. 45
- [Gross et al., 2014] Gross, G. A., Date, K., Schlegel, D. R., Corso, J. J., Llinas, J., Nagi, R., and Shapiro, S. C. (2014). Systemic test and evaluation of a hard+ soft information fusion framework : Challenges and current approaches. In *17th International Conference on Information Fusion (FUSION)*, pages 1–8. IEEE. 33
- [Gruber, 1993] Gruber, T. R. (1993). A translation approach to portable ontology specifications. *Knowledge acquisition*, 5(2) :199–220. 48

- [Guarino, 1995] Guarino, N. (1995). Formal ontology, conceptual analysis and knowledge representation. *International journal of human-computer studies*, 43(5-6) :625–640. 43
- [Hall and Llinas, 1997] Hall, D. L. and Llinas, J. (1997). An introduction to multisensor data fusion. *Proceedings of the IEEE*, 85(1) :6–23. 22
- [Hall and McMullen, 2004] Hall, D. L. and McMullen, S. A. (2004). *Mathematical techniques in multisensor data fusion*. Artech House. 14
- [Hamilton et al., 2002] Hamilton, S. N., Miller, W. L., Ott, A., and Saydjari, O. S. (2002). Challenges in applying game theory to the domain of information warfare. In *Information Survivability Workshop (ISW)*. Citeseer. 97
- [Jensen, 1990] Jensen, F. (1990). Bayesian updating in recursive graphical models by local commutations. *Comput. Stat. Data Anal.*, 4 :269–282. 56
- [Johansson and Falkman, 2008] Johansson, F. and Falkman, G. (2008). A bayesian network approach to threat evaluation with application to an air defense scenario. In *2008 11th International conference on information fusion*, pages 1–7. IEEE. 67
- [Johnson-Laird, 2006] Johnson-Laird, P. N. (2006). *How we reason*. Oxford University Press, USA. 11
- [Jordan et al., 1999] Jordan, M. I., Ghahramani, Z., Jaakkola, T. S., and Saul, L. K. (1999). An introduction to variational methods for graphical models. *Machine learning*, 37(2) :183–233. 56
- [Klein, 2008] Klein, G. (2008). Naturalistic decision making. *Human factors*, 50(3) :456–460. 21
- [Lambert, 2001] Lambert, D. A. (2001). Situations for situation awareness. *Proc. of Fusion 2001*. 65
- [Larkin and Dechter, 2003] Larkin, D. and Dechter, R. (2003). Bayesian inference in the presence of determinism. In *AISTATS*. 56
- [Lauritzen and Spiegelhalter, 1988] Lauritzen, S. L. and Spiegelhalter, D. J. (1988). Local computations with probabilities on graphical structures and their application to expert systems. *Journal of the Royal Statistical Society : Series B (Methodological)*, 50(2) :157–194. 56, 73
- [Le Guillaume, 2016] Le Guillaume, N. (2016). *A Game-Theoretic Planning Framework for Intentional Threat Assessment*. PhD thesis. xvi, 66, 68, 69, 97, 143, 159
- [Little and Rogova, 2006] Little, E. G. and Rogova, G. L. (2006). An ontological analysis of threat and vulnerability. In *2006 9th International Conference on Information Fusion*, pages 1–8. IEEE. 68

- [Littman et al., 2001] Littman, M. L., Majercik, S. M., and Pitassi, T. (2001). Stochastic boolean satisfiability. *Journal of Automated Reasoning*, 27(3) :251–296. 56
- [Lundberg, 2015] Lundberg, J. (2015). Situation awareness systems, states and processes : a holistic framework. *Theoretical Issues in Ergonomics Science*, 16(5) :447–473. 20
- [McAnally et al., 2018] McAnally, K., Davey, C., White, D., Stimson, M., Mascaro, S., and Korb, K. (2018). Inference in the wild : A framework for human situation assessment and a case study of air combat. *Cognitive science*, 42(7) :2181–2204. 21, 88
- [Mihaylova et al., 2002] Mihaylova, L., Lefebvre, T., Bruyninckx, H., Gadeyne, K., and De Schutter, J. (2002). A comparison of decision making criteria and optimization methods for active robotic sensing. In *International Conference on Numerical Methods and Applications*, pages 316–324. Springer. 38
- [Minsky, 1974] Minsky, M. (1974). A framework for representing knowledge. 43
- [Murphy, 2002] Murphy, K. P. (2002). Dynamic bayesian networks : Representation. *inference and learning*, 8 :2004–06. 58
- [Neapolitan, 1990] Neapolitan, R. E. (1990). Probabilistic reasoning in expert systems. a wiley-interscience publication. 54
- [Niklasson et al., 2008] Niklasson, L., Riveiro, M., Johansson, F., Dahlbom, A., Falkman, G., Ziemke, T., Brax, C., Kronhamn, T., Smedberg, M., Warston, H., et al. (2008). Extending the scope of situation analysis. In *2008 11th international conference on information fusion*, pages 1–8. IEEE. 14
- [Nilsson, 2007] Nilsson, M. (2007). Human decision making and information fusion : Extending the concept of decision support. 14
- [O’Toole, 2000] O’Toole, M. E. (2000). *The school shooter : A threat assessment perspective*. DIANE Publishing. 65
- [Paradis et al., 2005] Paradis, S., Benaskeur, A., Oxenham, M., and Cutler, P. (2005). Threat evaluation and weapons allocation in network-centric warfare. In *2005 7th international conference on information fusion*, volume 2, pages 8–pp. IEEE. 67
- [Pearl, 1982] Pearl, J. (1982). *Reverend Bayes on inference engines : A distributed hierarchical approach*. Cognitive Systems Laboratory, School of Engineering and Applied Science 72
- [Pearl, 1986] Pearl, J. (1986). Fusion, propagation, and structuring in belief networks. *Artificial intelligence*, 29(3) :241–288. 73

- [Pearl, 1988] Pearl, J. (1988). *Probabilistic reasoning in intelligent systems : networks of plausible inference*. Morgan Kaufman Publishers Inc. 54, 56, 72, 73
- [Pek and Gee, 2013] Pek, H. and Gee, W. (2013). High-level information fusion : an overview [j]. *Journal of Advances in Information Fusion*, 8(1) :1–40. 28
- [PFT RENS, 2016] PFT RENS, C. (2016). *Manuel de l'Unité de Renseignement de Brigade*. Ministère de la défense. 74, 97, 131
- [Pigeau and McCann, 2002] Pigeau, R. and McCann, C. (2002). Re-conceptualizing command and control. Technical report, Defence and Civil Institute of Environmental Medicine Toronto Canada. 14
- [Plaat et al., 1996] Plaat, A., Schaeffer, J., Pijls, W., and De Bruin, A. (1996). Exploiting graph properties of game trees. In *AAAI/IAAI, Vol. 1*, pages 234–239. 67
- [Poole and Zhang, 2003] Poole, D. and Zhang, N. L. (2003). Exploiting contextual independence in probabilistic inference. *Journal of Artificial Intelligence Research*, 18 :263–313. 56
- [Pravia et al., 2009] Pravia, M. A., Babko-Malaya, O., Schneider, M. K., White, J. V., Chong, C.-Y., and Willsky, A. S. (2009). Lessons learned in the creation of a data set for hard/soft information fusion. In *2009 12th International Conference on Information Fusion*, pages 2114–2121. IEEE. xix, 29, 31
- [Reddy et al., 2001] Reddy, M., Borum, R., Berglund, J., Vossekuil, B., Fein, R., and Modzeleski, W. (2001). Evaluating risk for targeted violence in schools : Comparing risk assessment, threat assessment, and other approaches. *Psychology in the Schools*, 38(2) :157–172. 65
- [Renoux, 2015] Renoux, J. (2015). *Contribution to multiagent planning for active information gathering*. PhD thesis. 47, 52, 130
- [RENS, 2016] RENS, C. (2016). *Manuel d'emploi du sous-groupement recherche multicateurs*. Ministère de la défense. 74, 97, 131
- [Roger, 1991] Roger, B. M. (1991). Game theory : analysis of conflict. *The President and Fellows of Harvard College, USA*. 66
- [Roy et al., 2007] Roy, J., Breton, R., and Rousseau, R. (2007). Situation awareness and analysis models. *Concepts, Models, and Tools for Information Fusion*, pages 27–67. xvi, 23, 66, 70
- [Roy and Guyard, 2012] Roy, J. and Guyard, A. B. (2012). Supporting threat analysis through description logic reasoning. In *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, pages 308–315. IEEE. 70

- [Salerno, 2008] Salerno, J. (2008). Measuring situation assessment performance through the activities of interest score. In *2008 11th International Conference on Information Fusion*, pages 1–8. IEEE. 65
- [Schank and Abelson, 2013] Schank, R. C. and Abelson, R. P. (2013). *Scripts, plans, goals, and understanding : An inquiry into human knowledge structures*. Psychology Press. 44
- [Schroyens et al., 2003] Schroyens, W., Schaeken, W., and Handley, S. (2003). In search of counter-examples : Deductive rationality in human reasoning. *The Quarterly Journal of Experimental Psychology Section A*, 56(7) :1129–1145. 11
- [Serfaty et al., 1997] Serfaty, D., MacMillan, J., Entin, E. E., and Entin, E. B. (1997). The decision-making expertise of battle commanders. *Naturalistic decision making*, pages 233–246. 12
- [Serrano, 2014] Serrano, L. (2014). *Vers une capitalisation des connaissances orientée utilisateur : extraction et structuration automatiques de l'information issue de sources ouvertes*. PhD thesis. xvi, 50, 51
- [Shachter and Peot, 1990] Shachter, R. D. and Peot, M. A. (1990). Simulation approaches to general probabilistic inference on belief networks. In *Machine Intelligence and Pattern Recognition*, volume 10, pages 221–231. Elsevier. 56
- [Shafer, 1976] Shafer, G. (1976). A theory of statistical evidence. In *Foundations of probability theory, statistical inference, and statistical theories of science*, pages 365–436. Springer. 58
- [Shannon, 1948] Shannon, C. E. (1948). A mathematical theory of communication. *Bell system technical journal*, 27(3) :379–423. 59, 60
- [Shenoy and Shafer, 1986] Shenoy, P. P. and Shafer, G. (1986). Propagating belief functions with local computations. *IEEE Expert*, 1(3) :43–52. 56
- [Smith, 1985] Smith, B. C. (1985). Prologue to reflection and semantics in a procedural language. *Readings in Knowledge Representation*, pages 31–40. 44
- [Sølvberg, 1999] Sølvberg, A. (1999). Data and what they refer to. In *Conceptual Modeling*, pages 211–226. Springer. 45
- [Sowa, 2014] Sowa, J. F. (2014). *Principles of semantic networks : Explorations in the representation of knowledge*. Morgan Kaufmann. 43
- [Steinberg, 2007] Steinberg, A. (2007). Predictive modeling of interacting agents. In *2007 10th International Conference on Information Fusion*, pages 1–6. IEEE. 68

- [Steinberg, 2009] Steinberg, A. N. (2009). Foundations of situation and threat assessment. *Handbook of multisensor data fusion : theory and practice*, pages 437–501. 32, 65, 66
- [Steinberg and Bowman, 2004] Steinberg, A. N. and Bowman, C. L. (2004). Rethinking the jdl data fusion levels. *Nssdf Jhaptl*, 38 :39. xix, 22, 24
- [Steinberg et al., 1999] Steinberg, A. N., Bowman, C. L., and White, F. E. (1999). Revisions to the jdl data fusion model. In *Sensor Fusion : Architectures, Algorithms, and Applications III*, volume 3719, pages 430–441. International Society for Optics and Photonics. 22
- [Town, 2004] Town, C. (2004). Ontology-driven bayesian networks for dynamic scene understanding. In *2004 Conference on Computer Vision and Pattern Recognition Workshop*, pages 116–116. IEEE. 58
- [Tzu, 2019] Tzu, S. (2019). *L'art de la guerre*. J'ai Lu. 10
- [Van Creveld, 1985] Van Creveld, M. (1985). *Command in war*. Harvard University Press. 16
- [Van Harmelen et al., 2008] Van Harmelen, F., Lifschitz, V., and Porter, B. (2008). *Handbook of knowledge representation*, volume 1. Elsevier. xvi, 54, 55
- [Vasnier et al., 2019] Vasnier, K., Justine, V., and Gatepaille, S. (2019). Procédé et système de fusion d'informations. 37, 83
- [Wallenius, 2004] Wallenius, K. (2004). Support for situation awareness in command and control. In *Proceedings of the Seventh International Conference on Information Fusion (FUSION 2004)*, volume 2, pages 1117–1124. Citeseer. xv, 23, 25
- [Waltz et al., 1990] Waltz, E., Llinas, J., et al. (1990). *Multisensor data fusion*, volume 685. Artech house Boston. 30
- [Weyns et al., 2004] Weyns, D., Steegmans, E., and Holvoet, T. (2004). Towards active perception in situated multi-agent systems. *Applied Artificial Intelligence*, 18(9-10) :867–883. xv, 40
- [Yedidia et al., 2005] Yedidia, J. S., Freeman, W. T., and Weiss, Y. (2005). Constructing free-energy approximations and generalized belief propagation algorithms. *IEEE Transactions on information theory*, 51(7) :2282–2312. 56
- [Yoo et al., 2014] Yoo, D., No, S., and Ra, M. (2014). A practical military ontology construction for the intelligent army tactical command information system. *International Journal of Computers Communications & Control*, 9(1) :93–100. xvi, 48, 49

- [Zhang and Ji, 2006] Zhang, Y. and Ji, Q. (2006). Active and dynamic information fusion for multisensor systems with dynamic bayesian networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 36(2) :467–472. 40

