HAL
open science

Recognized Cyber Picture et Confiance interpersonnelle : optimiser les activités collaboratives cyber militaires

Florent Bollon

To cite this version:

Florent Bollon. Recognized Cyber Picture et Confiance interpersonnelle : optimiser les activités collaboratives cyber militaires. Automatique. Université de Bordeaux, 2020. Français. NNT : 2020BORD0113 . tel-03097633

HAL Id: tel-03097633

https://theses.hal.science/tel-03097633

Submitted on 5 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.

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE BORDEAUX

Spécialité : **Automatique, Productique, Signal et Image, Ingénierie cognitique**

Présentée par :

Florent BOLLON

Thèse dirigée et co-encadrée par : **Jean-Marc SALOTTI, Nicolas MAILLE, Anne-Lise MARCHAND, Laurent CHAUDRON, Cédric CIVEIT**

Préparée au sein du **Laboratoirede l'Intégration du Matériau au Système (IMS)**
Dans **l'école doctorale des sciences physiques et de l'ingénieur (EDSPI)**

Recognized Cyber Picture et Confiance interpersonnelle : Optimiser les activités collaboratives cyber militaires

Soutenue le 09/10/2020

Composition du Jury :

M. Laurent KARSENTY, Docteur, HDR - - - - - - - - - - - - CNAM – CRTD, Rapporteur
M. Mickaël CAUSSE, Professeur - - - - - - - - - - - - - - ISAE-SUPAERO, Rapporteur
Mme Cécile GODÉ, Professeur - - - CRETLOG EA 881, Aix Marseille Université, Présidente
M. Bernard CLAVERIE, Professeur - - - - - - - - - - - - - - - ENSC, Bordeaux INP
M. Jean-Marc SALOTTI, Professeur - - - - - - - ENSC, Bordeaux INP, Directeur de thèse
M. Nicolas MAILLE, Docteur - ONERA
Mme Anne-Lise MARCHAND, Docteur - CReA
M. Laurent CHAUDRON, Docteur, HDR - CReA
Mme Dominique ARBIOL, Général - - - - - - - Général commandant de l'Ecole de l'air
M. Cédric CIVEIT - THALES La Ruche

Recognized Cyber Picture et Confiance interpersonnelle : Optimiser les activités collaboratives cyber militaires

Sous la direction de : Jean-Marc Salotti, Nicolas Maille, Anne-Lise Marchand, Laurent Chaudron, Cédric Civeit

_____ Résumé _____

Depuis le début des années 2000, les réseaux civils et militaires sont confrontés à une augmentation constante du nombre de cyber attaques. Afin d'accélérer le processus décisionnel et de coordonner au mieux les actions en cas d'attaque provenant du cyberespace il devient nécessaire, pour l'armée de l'air française (AA), de mettre en place un système ou un outil permettant d'avoir une représentation partagée de l'état cyber de ses infrastructures. Ce système (ou outil), nommé recognized cyber picture (RCP), n'est actuellement pas totalement défini mais sera probablement placé dans les centres de commandement et de conduite (C2) de l'AA. Le rôle de cette RCP sera de repérer et mettre en évidence d'éventuels problèmes concernant les informations reçues par les C2 (informations modifiées, ajoutées, perdues…). Les opérateurs de C2 dotés de RCP peuvent donc se retrouver confrontés à une dissonance en terme de traitement et de transmission de l'information. Afin de faciliter la prise de décisions, ces opérateurs devront probablement mettre en place des mécanismes permettant de « compenser » cette dissonance. Parmi ces mécanismes, le niveau de confiance est déjà étudié dans la littérature comme facilitant les prises de décisions dans les environnements à forte incertitude. Cette thèse propose donc d'étudier le rôle de la confiance sur les comportements des opérateurs présents dans les C2 intégrant cette dimension cyber. Afin de répondre à cette problématique, un protocole expérimental, permettant d'induire différents niveaux de confiance et d'étudier l'influence de ces différents niveaux de confiance sur le comportement des individus, a été développé puis testé. Sur la base de ce protocole expérimental, 4 expérimentations, avec comme participants de potentiels opérateurs de la RCP, ont été réalisées en laboratoire. La première expérimentation (menée auprès de 200 personnes de l'AA dont 160 opérationnels et 40 élèves) portait sur le rôle des caractéristiques psychosociales des individus et sur leur comportement lorsqu'ils travaillent avec des collaborateurs inconnus plus ou moins dignes de confiances. La deuxième expérimentation (menée auprès de 40 élèves de l'école de l'air) portait sur l'identification de différences de comportement dans le cas d'une activité reposant sur la confiance entre deux opérateurs humains ou entre un opérateur humain et un système automatisé (ici une intelligence artificielle émulée). La troisième expérimentation (menée auprès de 35 élèves ingénieurs) portait sur l'influence du niveau de confiance en soi d'un individu sur son comportement envers des coéquipiers plus ou moins dignes de confiance. Ces 3 premières expérimentations montrent, notamment, des modifications comportementales peu étudiées dans la littérature, engendrées par le niveau de confiance présent dans la relation. Ces comportements portent sur la supervision, la qualité des supervisions, la gestion du temps mais également l'acceptation des informations transmises par le coéquipier. Enfin, la dernière expérimentation (menée auprès de 40 élèves ingénieurs) portait sur l'influence du niveau de confiance présent dans une relation ainsi que de l'incertitude provenant des données sur la prise de décision d'un opérateur. Cette expérimentation montre que la cohérence des informations disponibles ainsi que le niveau de confiance jouent un rôle dans la prise de décision des opérateurs. Les résultats des différentes expérimentations ont été confrontés aux modèles issus de la littérature et ont permis d'apporter des éléments permettant d'affiner et adapter ces modèles au cas des C2 ayant une composante cyber. La thèse présente donc à la fois une contribution fondamentale sur la compréhension des ressorts de la confiance et un apport plus applicatif pouvant orienter des éléments de mise en œuvre de la RCP au sein des C2.

Recognized Cyber Picture and Interpersonal trust: optimizing cyber-military collaborative activities

Under the supervision of: Jean-Marc Salotti, Nicolas Maille, Anne-Lise Marchand, Laurent Chaudron, Cédric Civeit

Abstract

Since the early 2000s, civilian and military networks are faced with an increasing number of cyber-attacks. In order to facilitate decision making and to better coordinate actions in case of attacks coming from the cyberspace, it has become necessary for the French Air Force (armée de l'air, AA) to put in place a system or tool that would allow a shared representation of the cyber state of its infrastructures. Although this system (or tool), named Recognized Cyber Picture (RCP), is not yet entirely defined, it will probably be deployed in the command and control centres (C2) of the AA. The role of the RCP will be to identify and highlight potential problems in the information received by the C2 (modified, added or lost information). Therefore, operators of C2 equipped with RCP may be confronted with a dissonance in terms of information processing and transmission. To facilitate decision making, C2 operators would need to put in place mechanisms to "compensate" for this dissonance. Among these mechanisms, interpersonal trust has been identified in the literature as a decision making facilitator in highly uncertain environments. This thesis proposes to study the role of trust on the behaviors of operators present in C2 integrating this cyber dimension. In order to answer this (research) question, we developed and then tested an experimental protocol that allows to induce several levels of trust and to investigate their impact on behaviours. Based on this protocol, 4 experiments were carried out in the laboratory with potential operators of the RCP. The first experiment (conducted on 200 participants from the AA, including 160 operational and 40 students from the AA Academy) focused on the role of psychosocial characteristics of individuals, and their behaviours when working with unknown and more or less trustworthy collaborators. The second experiment (conducted with 40 participants from the AA Academy), investigated the differences in behaviour when activity relies on trust between two human operators or between a human operator and an automated system (an emulated artificial intelligence). The third experiment (conducted with 35 engineering students) explored the influence of self-confidence of an individual on his behaviour towards more or less trustworthy co-workers. These first three experiments highlight, in particular, behavioural changes induced by the level of trust within the relationship, which have been little studied to date. This includes supervision, quality of supervision, time management, but also the acceptance of the information transmitted by the co-worker. The last experiment (conducted with 40 engineering students) explored the influence of both the level of confidence in a relationship and the uncertainty in the data on operator decision making. This experiment shows that the level of coherence of available information and trust levels play an important role in the operator's decisional processes. The results of these experiments have been confronted to models from the literature, and have allowed to bring into light new elements to adjust and adapt these models to the case of a C2 with a cyber component. This thesis makes a theoretical contribution to the understanding of trust mechanisms, and a practical contribution to support the implementation of the RCP in Command and Control centers.

Remerciements

J'ai commencé cette thèse après 3 ans passés à travailler sur les C2, à l'heure où j'écris ces lignes, j'ai enfin compris, qu'à l'époque, je n'y comprenais rien. Je pensais qu'une thèse était longue et fastidieuse, finalement, je ne peux que regretter qu'elle ne dure plus longtemps. L'apprentissage est un chemin semé d'embûches, mais grâce au soutien de nombreuses personnes les problèmes sont plus légers à porter et l'on finit par apprécier le paysage. Cette page est dédiée aux personnes qui m'ont permis d'avancer tant scientifiquement que personnellement.

Je tiens à remercier les équipes de Salon de Provence, de Bordeaux et de Rennes. Plus particulièrement merci à Anne-Lise et Nicolas qui m'ont soutenu jusqu'au bout et qui se sont investis au maximum de leurs capacités afin que tout se déroule pour le mieux. Passer de l'ingénierie à la méthode scientifique n'a pas été de tout repos et sans vous, il pas sûr que je serais allé au bout. Je remercie de tout cœur Laurent, Jean-Marc, Jean-Pierre, Pierre et Cédric d'avoir permis de lancer et de finir ce sujet et d'avoir été là à chaque fois que c'était nécessaire mais également les membres du jury pour avoir accepté et pris le temps de relire de manière critique et commenté ce travail de thèse. Merci à Colin, Jean-Christophe et Bruno pour leur aide mais également à mes co-doctorants (anciens et nouveaux) de l'ONERA et du CReA qui ont toujours été là dans les moments difficiles. Une pensée toute particulière à Patrick et Emma qui partagent le bureau et qui m'ont toujours soutenu mais également aux personnels administratifs et plus particulièrement à Francine et Brigitte qui ont veillé sur moi et qui ont toujours répondu positivement à mes demandes parfois (souvent) effectuées à contretemps.

Dans cette thèse de multiples expérimentations ont été effectuées et je sais pertinemment que je n'aurais pas obtenu ces résultats sans l'aide de nombreuses personnes. Merci aux lieutenants Céline Marchal et Théo Bécart qui ont permis au sujet de prendre toute son importance mais également aux sous lieutenants Jean-Baptiste Suchet, Geoffrey De Abreu Azevedo, Tony Blanchon et Alexandre De la Filolie qui ont, par leur travail, fortement contribués aux résultats présentés ici. Je tiens, bien tout particulièrement à remercier l'ensemble des commandants d'unités qui nous ont ouvert leur porte et sans qui nous n'aurions pas eu de tels résultats. Merci aux participants qui ont « joué le jeu » et m'ont donné de leur temps personnel pour me permettre d'effectuer mon travail professionnel.

Bien sûr, après/pendant les heures de boulot, il y a les moments de repos et je tiens à remercier toutes les personnes qui ont, à un moment donné été présentes et toutes celles avec qui j'ai pu rire et me détendre. Merci aux membres d'ICNA et du CReA, Bertille, Emma, Sala, Kelly, Anne-Laure, Adrien, Quentin, Camille et Yves, aux joueurs de foot, Mick, Alex, Johnas, Mathieu, Raph, Christian, Nawfel, Greg, Bruno, Jean-Christophe, Simon et Pierrot. Merci à l'équipe de Bordeaux qui m'a accueilli pendant presque 1 mois, Baptiste, Théo et Elisa, grâce à vous je savais, avant de prendre l'avions, que je passerai d'excellentes soirées. Merci aux marseillais et rennais qui sont là depuis des années et sur qui je peux toujours compter, merci à la Banda du dock, à Sully, Noé, Val, Guigue, Amar, Clément, Fanny et merci à tous ceux qui me font passer de bon moments.

Pour finir, mes plus profonds remerciements vont à ma famille et en premier lieu à Camille qui a passé tout ce temps à mes côtés. Sans toi je n'aurais pas eu la force de commencer ce travail, c'est ton soutien au quotidien et l'assurance d'une vie paisible qui me permettent d'avancer sereinement, une thèse passée sans qu'un couple ne s'engueule c'est très fort (mais j'y suis pour beaucoup). Merci à mes parents, mon frère, ma sœur, ma belle-sœur, ma tante, mes beaux-parents mais aussi a Liam et Meryl qui ont vu le jour pendant que je ne le voyais plus. Annie, Jean-Louis, Julien, Emilie, Sidney, Paulette, Claire, Marie-Jo et Jeff, les repas avec vous étaient, sont et seront toujours des moments joyeux, un espace de détente dans une vie difficile. Merci à mes grands-parents, ceux qui restent avec nous et ceux qui nous ont quittés, sans vous je ne serai pas qui je suis.

Table des matières

Table des matières 5
Table des illustrations 10
Introduction 16
Guide de lecture 18
1 Constat opérationnel 20
1. La guerre réseau-centrée (NCW) 21
2. De la NCW au risque cyber 23
3. Du risque cyber à la recognized cyber picture (RCPair) 24
4. Généralités sur la RCPair « AB » 25
A. Définition et concept de la RCPair « AB » 26
B. Choix du décideur final de la RCPair « AB » 27
C. Flux d'informations dans la RCP « AB » 29
D. Vue conceptuelle globale de la RCPair « AB » 29
5. De la RCPair à la cyber-résilience 30
6. Le C2, un concept et non pas un système 32
A. Eléments fondamentaux du concept de C2 34
B. Eléments contextuels du concept de C2 36
Analyse conceptuelle de l'organisation possible des C2 de l'AA 38
7. La RCPair dans les C2 42
Point clés 47
2 La confiance 49
1. Introduction 50
2. Définitions et modèles utilisés dans la littérature sur la confiance 50
A. Généralités et définition utilisée pour la thèse 50
B. Les différentes approches de la CI 52
a. Approche probabiliste réalisée dans la littérature portant sur les relations économiques 52
b. Approche psychologique réalisée dans la littérature managériale 53
3. Types de confiance 55
A. Composantes de la CI 55
B. La CI évolutive ou dynamique 57
C. La CI statique ou confiance rapide 59

4. Modèles de confiances 60
5. Intégration des principales contributions de la littérature à la construction du modèle utilisé dans la thèse 63
A. Facteurs contribuant à la mise en place de la confiance (*antecedents*) 64
a. Caractéristique propre au confiant 64
b. Caractéristiques propres au mandant 66
c. Caractéristiques de la situation 68
d. Actions et conséquences du niveau de confiance 70
e. Différences entre un modèle dynamique et un modèle statique 72
6. Méthodes d'inductions et études sur la confiance 74
A. Management et organisation 74
B. Psychologie et neuroscience 76
C. Informatique 77
7. Conclusion 77
Points clés 80
Résumé général des deux premiers chapitres et perspectives 81
3 Etude de la possibilité d'induire de la CI chez les aviateurs cibles de la RCPair 86
1. Introduction et cadre théorique 87
2. Méthode 89
A. Participants 89
B. Matériel & Procédure 89
3. Résultats et discussion 91
Points clés 95
4 Validation du processus d'induction de CI pour les expérimentations 96
1. Introduction 97
2. Protocole expérimental 97
3. Précautions expérimentales 100
4. Variables mesurées 101
5. Test du matériel expérimental 104
A. Participants 105
B. Résultats 105
6. Conclusion 106
Points clés 108
5 Etude expérimentale de l'impact des différents niveaux de CI sur le comportement des opérateurs cibles de la RCPair 109

1. Introduction 110
2. Niveau de Confiance et comportements 111
3. Comportements et caractéristiques psychosociales du confiant 114
4. Matériel et méthodes 116
A. Participants 116
B. Matériel 116
5. Résultats 117
A. Test des hypothèses 2, 3, 4, 5 et 6 120
a. Test de l'hypothèse 2 : Une diminution du niveau de CI entraîne une augmentation du nombre de supervisions 120
b. Test de l'hypothèse 3 : Une diminution du niveau de CI entraîne une augmentation du temps total utilisé par la confiant pour réaliser les tâches. 120
c. Test de l'hypothèse 4 : Une augmentation du niveau de CI entraîne une plus grande acceptation, par le confiant, des informations transmises par le mandant. 120
d. Test de l'hypothèse 5 : Une augmentation du niveau de CI entraîne une diminution du nombre de supervisions contre-productives 120
e. Test de l'hypothèse 6 : Sous forte pression temporelle, le niveau de CI ne module pas le nombre de supervisions, ni l'augmentation du temps total, ni l'acceptation par le confiant des informations transmises par le mandant, ni le nombre de supervisions contre-productives 121
B. Test des hypothèses 7, 8, 9 et 10 122
a. Test de l'hypothèse 7 : Dans un même milieu professionnel, le métier des individus et non pas le niveau de CI fait varier les comportements. 123
Hypothèse 7, Test du matériel d'induction : Perception de la performance du coéquipier 124
Hypothèse 7 : Pourcentage de supervision 124
Hypothèse 7 : Pourcentage de temps total utilisé 125
Hypothèse 7 : Pourcentage de modifications 126
Hypothèse 7 : Pourcentage de supervisions contre-productives 126
b. Test de l'hypothèse 8 : Dans un même métier, le niveau d'expertise des individus et non pas le niveau de CI fait varier les comportements. 127
Hypothèse 8 : Perception de la performance du coéquipier 127
Hypothèse 8 : Pourcentage de supervision 128
Hypothèse 8 : Pourcentage de temps total utilisé 128
Hypothèse 8 : Pourcentage de modifications 129
Hypothèse 8 : Pourcentage de supervisions contre-productives 130

c. Test de l'hypothèse 9 : Dans un même métier, l'exposition au risque des individus et non pas le niveau de CI fait varier les comportements. 130

Hypothèse 9 : Perception de la performance du coéquipier 131

Hypothèse 9 : Pourcentage de supervision 131

Hypothèse 9 : Pourcentage de temps total utilisé 132

Hypothèse 9 : Pourcentage de modifications 132

Hypothèse 9 : Pourcentage de supervisions contre-productives 133

d. Test de l'hypothèse 10 : Pour une même exposition au risque, le métier des individus et non pas le niveau de confiance fait varier les comportements. 134

Hypothèse 10 : Perception de la performance du coéquipier 135

Hypothèse 10 : Pourcentage de supervision 135

Hypothèse 10 : Pourcentage de temps utilisé sur le temps disponible 136

Hypothèse 10 : Pourcentage de modification 136

Hypothèse 10 : Pourcentage de supervisions contre-productives 136

6. Discussion 137

7. Apports de l'expérimentation au choix du décideur final de la RCPair 140

Points clés 144

6 Etude de l'influence de la confiance en soi et de la confiance dans le système sur le comportement de l'opérateur 145

1. Cadre théorique 146

2. Expérimentation portant sur la différence entre la CI et la confiance dans la machine 150

A. Matériel et méthode 150

a. Participants 150

b. Protocole 150

B. Résultats 151

a. Evaluation subjective des résultats transmis par le coéquipier 152

b. Evaluation comportementale 153

Pourcentage de supervisions 153

Pourcentage de temps passé à superviser 154

Pourcentage de modifications 155

3. Discussion 157

4. Apport de l'expérimentation 2 à la RCPair 158

Points clés 160

5. Expérimentation portant sur les modifications comportementales liées à la confiance en soi et à la confiance interpersonnelle 161

A. Matériel et méthode 161
a. Matériel 161
b. Mise en place du calibrage 161
Introduction 161
Matériel et méthode 162
Résultats 165
B. Déroulé de l'expérimentation 3 167
C. Participants 168
D. Résultats 168
a. Pré analyse 168
b. Analyse des questionnaires 168
Agrégation des données et analyse descriptive 168
Statistiques inférentielles 170
Statistiques inférentielles pour les données de PT 170
Conclusion sur les questionnaires 172
c. Analyse du calibrage 172
Analyse du niveau initial de CS 173
Analyse de la variation du niveau de VCS 175
Conclusion des pré-analyses 176
d. Analyse des données expérimentales 176
Niveau de certitude dans la réponse du coéquipier 176
Analyses comportementales 178
Analyse du pourcentage de supervisions 178
Pourcentage de temps utilisé 179
Pourcentage de modifications 181
E. Discussion 183
6. Apport de l'expérimentation à la RCPair 185
Points clés 186
7 Etude expérimentale de la prise de décision à l'aveugle d'un opérateur en fonction de son niveau de CI en univers incertain 187
1. Introduction et cadre théorique 188
2. Matériel et Méthode 192
A. Participants 193
B. Protocole 193

3. Résultats 196
4. Discussion 198
5. Apport de l'expérimentation à la RCPair 200
Points clés 202
8 Discussion générale et perspectives 203
1. Résumé de la thèse 204
2. Apports méthodologiques de la thèse aux méthodes d'induction de confiance en laboratoire 207
3. Apports théoriques de la thèse aux liens entre confiance interpersonnelle et de la confiance dans la machine 210
4. Apports théoriques de la thèse à la connaissance des caractéristiques propres au confiant 211
5. Apports théoriques de la thèse a la connaissance des comportements engendrés par différents niveaux de confiance interpersonnelle 213
6. Apports théoriques de la thèse a la connaissance du rôle de la situation dans la mise en place des comportements engendrés par différents niveaux de confiance interpersonnelle 215
7. Apport de la thèse à la RCPair 216
8. Conclusions et perspectives 219
Bibliographie 230
Glossaire 243
ANNEXE 1 : Exemple de questions posées et analyse du besoin de la RCPair 245
ANNEXE 2 : Exemple de feuille de consentement et questionnaire utilisés dans les expérimentations effectuées sur les opérationnels de l'AA 259
ANNEXE 3 : Expérimentation 1, Résultats des tests post-hocs 262
ANNEXE 4 : Feuille consentement et questionnaire utilisés dans les expérimentations 3 et 4 266

Table des illustrations

Figures

Figure 1 : Image inspirée de celle présente dans le livre « Network Centric Warfare: Developing and Leveraging Information Superiority » (Alberts, Garstka, & Stein, 2000) 21
Figure 2 : Ecran de visualisation embarqué dans un Mirage 2000D (Armée de l'air, 2019). 22
Figure 3 : Exemple de traitement de l'information dans la RCP 29
Figure 4 : Représentation des liens présents dans la RCP obtenus après l'analyse du besoin (à gauche) et représentation de ce qui sera analysé au cours de cette thèse (à droite). 30
Figure 5 : Répartition des sujets d'étude dans la cyber resilience (résultats donnés par SCOPUS) 32

Figure 6 : Représentation conceptuelle du fondement opérationnel des C2 provenant de « SAS-050 Exploring new command and control concepts and capabilities » (NATO, 2006). 35
Figure 7 : Figure provenant du rapport « NATO NEC C2 Maturity Model » (Alberts, Huber, & Moffat, 2010)..... 36
Figure 8 : Figure provenant du livre « Command and Control: The Sociotechnical Perspective » (Walker, stanton, & Jenkins, 2017) 37
Figure 9 : Représentation de l'agilité du C2 au cours d'une mission (le temps représente la durée de la mission). 38
Figure 10 : Exemple de mission classique effectuée par les CDC..... 39
Figure 11 : Exemple de mission posture permanente de sureté (pps). 40
Figure 12 : Agilité du C2 sur des missions de l'AA. En mission normale le CDC est au stade de *conflicted C2*, au plus la situation devient complexe au plus l'organisation du C2 se déplace vers le stade de *Edge C2*. 41
Figure 13 : Exemple de Mission DPSA (Medeiros, 2019). 42
Figure 14 : Ajout de la composante RCPair à la représentation conceptuelle des C2 43
Figure 15 : Impact de l'arrivée de la composante cyber (par le biais de la RCPair) dans les C2 de l'AA. 44
Figure 16 : Le décideur cyber et le décideur air doivent permettre de prendre des décisions sur la base d'informations pouvant être contradictoires. 44
Figure 17 : Schéma conceptuel des C2air avec ajout de la composante RCPair. 46
Figure 18 : composantes de la CI mobilisées dans les différents niveaux de confiance 59
Figure 19 : Modèle de Mayer et al. (Mayer et al., 1995) présentant la dynamique de la confiance.... 61
Figure 20 : Modèle de la dynamique de la confiance proposé par Karsenty (2011). 62
Figure 21 : Modèle conceptuel de base de la dynamique de la confiance qui représente le pont commun à tous les modèles de la littérature. 62
Figure 22 : Bases du modèle qui sera utilisé dans ce manuscrit. 63
Figure 23 : Modèle incluant les caractéristiques propres au confiant pouvant être mobilisées dans la mise en place du niveau de confiance présent dans une relation. 66
Figure 24 : Modèle incluant les caractéristiques propres au mandant ayant pour rôle d'agir sur une situation donnée. 68
Figure 25 : Modèle incluant les caractéristiques de la situation..... 70
Figure 26 : Modèle complet reliant les trois entités et prenant en compte les caractéristiques de chacune d'entre elles. 72
Figure 27 : Adaptation du modèle à la confiance rapide de la confiance. 73
Figure 28 : Représentation de la partie du modèle testée dans cette expérimentation, à savoir les RS que le confiant associe au mandant..... 87
Figure 29 : Exemple d'échelle non segmentée utilisées afin de tester les différentes paires de mots 91
Figure 30 : Présentation de l'expérimentation qui se compose d'un certain nombre d'essais différents de trois phases chacun. 98
Figure 31 : La phase 2 de l'expérimentation correspond à la phase de comptage et de supervision. 100
Figure 32 : Présentation du tirage aléatoire qui permet une équiprobabilité (en moyenne) des tirages. 101
Figure 33 : Echelles non segmentées présentées en dernière phase 103
Figure 34 : Test du matériel expérimental. 105
Figure 35 : Représentation des deux approches étudiées dans l'expérimentation 1..... 111

Figure 36 : Présentation de l'expérimentation qui se compose de 42 essais différents de 3 phases chacun. 117
Figure 37 : Matrice montrant les caractéristiques sociales des participants. 118
Figure 38 : Résultats de l'expérimentation portant sur les caractéristiques psychosociales du confiant. 138
Figure 39 : Représentation conceptuelle du C2 utilisée pour la thèse. En couleur sont présentées les parties du modèle étudiées au cours de cette expérimentation. 141
Figure 40 : Représentations des parties du modèle étudiées dans le chapitre 6 146
Figure 41 : Représentations des composantes du modèle de confiance étudiées dans le chapitre 6 149
Figure 42 : Schéma représentant l'induction de confiance utilisée dans l'expérimentation 2..... 151
Figure 43 : Statistiques descriptives et représentation graphique des résultats obtenus par chaque groupe d'induction à la VD *CertitudeCoéquipier* en fonction du niveau de confiance induit..... 152
Figure 44 : Statistiques descriptives et représentation graphique des résultats obtenus par chaque groupe d'induction à la VD *%VDsup* en fonction du niveau de confiance induit..... 154
Figure 45 : Statistiques descriptives et représentation graphique des résultats obtenus par chaque groupe d'induction à la VD *%TempsSuperv* en fonction du niveau de confiance induit. 155
Figure 46 : Statistiques descriptives et représentation graphique des résultats obtenus par chaque groupe d'induction à la VD % VDmodif en fonction du niveau de confiance induit. 156
Figure 47 : résultats de l'expérimentation 2 158
Figure 48 : Schéma représentant les différentes phases de la pré-expérimentation..... 162
Figure 49 : Phase 1 et 2 de la pré expérimentation. 163
Figure 50 : Phase 3 de la pré-expérimentation. 164
Figure 51 : Phase 4 de la pré expérimentation 165
Figure 52 : Evaluation subjective effectuée par le participant de son score obtenu à la tâche de comptage et de sa performance finale. 165
Figure 53 : Choix du nombre de plages d'essais pour l'expérimentation finale. 167
Figure 54 : Histogramme et graphique d'estimations de densité pour la classe CS-..... 171
Figure 55 : Evolution au cours du temps du niveau de confiance en soi du participant. 173
Figure 56 : Boites de Tukey pour les valeurs initiales du niveau de CS pour chaque classe expérimentales. 174
Figure 57 : Boites de Tukey pour la variation du niveau de CS pour chaque classe expérimentales . 175
Figure 58 : Répartition des résidus pour les données complètes (à gauche) et pour les données modifiées à droite (en enlevant les lignes 59 et 14) 178
Figure 59 : Pourcentage de supervisions en fonction du niveau de confiance induit pour les classes CS+ et CS-..... 179
Figure 60 : Boites du Tukey pour le pourcentage de temps utilisé en fonction du niveau de confiance induit pour chaque classe de CS. 181
Figure 61 : Pourcentage de modification en fonction du niveau de confiance pour chaque classe de CS 182
Figure 62 : Résultats de l'expérimentation 3. 185
Figure 63 : Liens analysés dans l'expérimentation 4..... 189
Figure 64 : Présentation des brouillages pouvant survenir dans l'expérimentation 4. 192
Figure 65 : Affichage utilisé par le participant en phase 2 afin d'effectuer sa tâche de comptage.... 194
Figure 66 : Affichage de la phase 3..... 195

Figure 67 : pourcentages de brouillages transmis par le coéquipier et non validés par le participant en fonction du niveau de confiance 197
Figure 68 : pourcentages de brouillages transmis par le coéquipier et non validés par le participant en fonction du niveau de confiance et du caractère « consistants » *ou* « non-consistants » des essais 198
Figure 69 : Résultats de l'expérimentation 4. 199
Figure 70 : Modèle provisoire proposé dans l'état de l'art 204
Figure 71 : Modèle prenant en compte les résultats obtenus dans cette thèse 207
Figure 72 : Organisation possible des C2air utilisant la RCPair 217
Figure 73 : Représentation de l'approche unidimensionnelle de la confiance. 220
Figure 74 : Différences entre les approches unidimensionnelles (« A ») et multidimensionnelles (« B »). 221
Figure 75 : Différentes possibilité d'analyse des comportements modifiés par le niveau de confiance. 222
Figure 76 : Niveaux de confiance intégrative potentiellement étudiés dans chaque groupe social de l'expérimentation 1 223
Figure 77 : Modèle représentant la mise en place du niveau de confiance intégrative en prenant en compte le principe de réciprocité. 226
Figure 78 : Modèle, mis en place en se basant sur le principe de réciprocité, représentant la confiance dans la machine 229

Tableaux

Tableau 1 : Fréquence de réfutation et valeur chi2 des inducteurs potentiels de la représentation sociale de la CI (tous p < 0.001). 90
Tableau 2 : Résultats de l'évaluation par échelle visuelle analogique pour les 51 paires de mots (M = 4.5, SD = 3.2) choisies pour créer 17 paires de mots visant à induire un niveau élevé (M = 8.6, SD = 0.3), moyen (M = 3.9, SD = 0.69) et faible (M = 1, SD = 0.19) de CI chez les aviateurs. 92
Tableau 3 : Résultats de l'évaluation par échelle visuelle analogique pour les 51 paires de mots (M = 4.45, SD = 2.35) choisies pour créer 6 paires de mots utilisées pour induire une forte (M = 7.25, S = 0.13), moyenne (M = 4.6, SD = 0.35) et faible (M = 1.5, SD = 0.15) de CI chez les élèves ingénieurs 93
Tableau 4 : Nom, type, valeurs possibles et unités des variables dépendantes et indépendantes récupérées dans l'expérimentation et phase de l'essai dans laquelle ces variables sont récupérées. 104
Tableau 5 : Moyenne, écart type et comparaison par paire pour degré de certitude de la réponse du coéquipier (niveau de certitude associée au coéquipier dans ce tableau) et pour le temps de supervision. 106
Tableau 6 : Matrice de répartition des 200 participants. 119
Tableau 7 : Moyenne, écart type et résultats de l'ANOVA à mesures répétées pour la variable indépendante pression temporelle et pour les variables dépendantes *CertitudePartenaire, %VDsup, %Tempstot, %VDmodif et %VDm_sup* 121

Tableau 8 : Résultats, pour toutes les variables dépendantes, des effets simples obtenus sur la variable indépendante CI pour les différents groupes sociaux 123
Tableau 9 : Moyenne, écart type et résultats de l'ANOVA a mesures répétées pour les groupes contrôleurs aériens et mécaniciens n'ayant jamais fait d'OPEX et pour les variables dépendantes *CertitudePartenaire, %VDsup, %Tempstot, %VDmodif et %VDm_sup* 124
Tableau 10 : Test post-hoc HSD de Tukey pour la variable dépendante %VDsup et pour les groupes contrôleur aérien et mécanicien n'ayant jamais fait d'OPEX (*Cf.* annexe 3). 125
Tableau 11 : Test post-hoc HSD de Tukey pour la variable dépendante %TempsTot et pour les groupes contrôleur aérien et mécanicien n'ayant jamais fait d'OPEX (*Cf.* annexe 3). 126
Tableau 12 : Moyenne, écart type et résultats de l'ANOVA a mesures répétées pour les groupes PN expérimentés et élèves PN et pour les variables dépendantes *CertitudePartenaire,* %VDsup*,* %Tempstot*,* %VDmodif et *%VDm_sup* 127
Tableau 13 : Test post-hoc HSD de Tukey pour la variable dépendante %VDsup et pour les groupes PN expérimentés et élèves PN (*Cf.* annexe 3)..... 128
Tableau 14 : Test post-hoc HSD de Tukey pour la variable dépendante %TempsTot et pour les groupes PN expérimentés et élèves PN (*Cf.* annexe 3). 129
Tableau 15 : Test post-hoc HSD de Tukey pour la variable dépendante %VDmodif et pour les groupes PN expérimentés et élèves PN (*Cf.* annexe 3). 130
Tableau 16 : Moyenne, écart type et résultats de l'ANOVA a mesures répétées pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX et pour les variables dépendantes *CertitudePartenaire, %VDsup, %Tempstot, %VDmodif et %VDm_sup* 131
Tableau 17 : Test post-hoc HSD de Tukey pour la variable dépendante %VDmodif et pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX (*Cf.* annexe 3). 133
Tableau 18 : Test post-hoc HSD de Tukey pour la variable dépendante %VDm_sup et pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX (*Cf.* annexe 3). 134
Tableau 19 : Moyenne, écart type et résultats de l'ANOVA a mesures répétées pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX et pour les variables dépendantes *CertitudePartenaire,* %VDsup*,* %Tempstot*,* %VDmodif *et %VDm_sup* 134
Tableau 20 : Test post-hoc HSD de Tukey pour la variable dépendante CertitudePartenaire et pour les groupes mécaniciens ayant déjà fait des OPEX et PN expérimentés (*Cf.* annexe 3)..... 135
Tableau 21 : Vulgarisation des résultats obtenus. 140
Tableau 22 : Moyenne générale pour les différentes VD et pour les groupes mécaniciens (OPEX) et PN expérimentés. Moyenne générale et moyenne pour les niveaux de CI faible et élevés pour les différentes VD et pour les mécaniciens (Base) les contrôleurs aériens et les élèves PN..... 143
Tableau 23 : Statistiques descriptives des réponses aux différents questionnaires (VD) en fonction de la classe de CS attribuée..... 170
Tableau 24 : Statistiques descriptives du niveau initial de confiance des participants de chaque classe de CS attribuée 174
Tableau 25 Statistiques descriptives de la variation du niveau de confiance en soi des participants de chaque classe de CS attribuée..... 175
Tableau 26 : Statistiques descriptives pour le niveau de certitude dans la réponse du coéquipier, toute classe de CS confondues puis pour les classes CS- et CS+ 177
Tableau 27 : Statistiques descriptives pour le pourcentage de supervisions, toute classe de CS confondues puis pour les classes CS- et CS+ 179

Tableau 28 : Statistiques descriptives pour le pourcentage de temps utilisé, toutes classes de CS confondues puis pour les classes CS- et CS+ 180
Tableau 29 : Statistiques descriptives pour le pourcentage de modifications, toute classe de CS confondues puis pour les classes CS- et CS+. 182
Tableau 30 : Moyenne générale pour les différentes VD et pour les différents groupes sociaux..... 184
Tableau 31 : Matrice montrant, pour chaque groupe social, les comportements modulés par le niveau de CI dans l'expérimentation 1. 212

Introduction

Introduction

Depuis plusieurs années, l'armée de l'air est confrontée à l'augmentation croissante des tâches collaboratives, parfois éphémères, avec des personnes pouvant appartenir à d'autres unités, d'autres nations (langue et nomenclatures différentes) voir même des collaborations civiles-militaires. Dans ce contexte, afin d'augmenter l'efficacité et la rapidité des échanges d'information, des nouveaux modes de communication utilisant des réseaux informatisés, sont fréquemment utilisés. Jusqu'au début des années 2000 les transferts d'informations réseaux centrés paraissaient être sécurisés. Toutefois, avec l'explosion de la bulle internet, des nouvelles menaces provenant du cyberespace apparaissent et touchent dans un premier temps, des réseaux civils, comme en Estonie en 2007 ou en Géorgie en 2008 (Farwell & Rohozinski, 2011).

Rapidement, la menace cyber s'étend aux infrastructures des armées comme aux Etats Unis, en Angleterre et en France en 2009 (Baud, 2012) et des sites et réseaux protégés comme en Iran en 2010 (Farwell & Rohozinski, 2011). Ces premières cyber-attaques entrainent une remise en cause de la confiance qu'ont les opérateurs dans leurs systèmes informatisés et emmènent les Etats à mieux définir leurs besoins et leurs stratégies de gestion de la cyber sécurité. Afin d'accélérer le processus décisionnel et de coordonner au mieux les actions en cas d'attaque provenant du cyberespace, l'armée de l'air française (AA) doit se doter d'un système ou d'un outil, nommé Recognized Cyber Picture (RCPair), permettant de représenter l'état cyber de ses réseaux.

Cette RCPair n'est actuellement pas totalement définie, que ce soit en termes d'organisation technique ou humaine, mais viendra probablement s'additionner aux outils opérationnels actuellement utilisés dans les centres de commandement et de conduite (C2) de l'AA. Cette RCPair sera alimentée tant par des analyses automatiques des activités sur les différents réseaux que par des opérateurs identifiant des anomalies.

Bien que cette RCPair ne soit pas encore déployé, il est fort probable qu'un tel dispositif, complexe et nouveau, entrainera des problématiques liées aux activités des différentes équipes en charge de la gestion de la cyber-sécurité et à leurs coopération avec les autres membres des C2 pour arriver aux meilleures décisions communes. Parmi ces problématiques, les opérationnels de l'AA identifient déjà la confiance interpersonnelle (Marchand, 2013) comme étant un enjeu majeur. Cette thèse propose donc d'étudier les problématiques liées à un manque ou un excès de confiance interpersonnelle (CI) pouvant être présents entre les différents opérateurs humains des C2 utilisant la RCPair. La thèse qui est soutenue ici est qu'il est possible d'identifier expérimentalement les composantes inter et intra individuelles impactant le lien entre confiance et comportement chez les opérateurs potentiels de la RCPair.

La CI, semble jouer un rôle essentiel dans les activités collaboratives (De Jong, Dirks, Gillespie, 2016) et est notamment considérée comme étant un modulateur du comportement des opérateurs et de la performance d'une équipe (Dirks, 1999). Ainsi, les résultats d'études, pour la plupart qualitatives, montrent qu'un niveau de CI faible envers le chef d'équipe ou entre les membres d'une équipe,

entraine une diminution de la performance (De Jong et al., 2016) de l'équipe et une augmentation des tâches de supervision.

Si beaucoup d'études établissent des liens entre CI et performance, les études concernant la CI et la supervision sont plus rares. Toutefois les liens entre confiance et supervision ont été établis dans un autre champ de recherche, à savoir, celui de la confiance dans la machine (CM). Les études réalisées dans le champ de recherche portant sur la CM indiquent globalement que lorsque la confiance augmente, la supervision diminue (Lee & Moray, 1992). Cependant, à partir d'un certain niveau de confiance, un phénomène de surconfiance, qui se caractérise par une absence de supervision de la part de l'opérateur, peut apparaitre. Si ces résultats étaient généralisables à la CI, cela suggèrerait qu'un niveau inadéquat de CI entre les membres d'une équipe pourrait mener à des situations de supervision excessive (Lee & Moray, 1992) ou au contraire à une excès de confiance (Parasuraman et al., 1993) entrainant une absence de supervision. Ainsi, l'influence de la confiance sur la supervision pourrait être un point clef de l'efficience d'un système sociotechnique complexe tel que les C2 ayant une composante cyber. Cette thèse propose donc d'étudier si les modulations du niveau de CI présent entre les opérateurs d'un système sociotechnique complexe peuvent entrainer des comportements impactant la gestion de la nouvelle composante cyber des C2

Guide de lecture

Ce manuscrit est constitué de 7 chapitres et d'une discussion générale. Les 2 premiers chapitres constituent un état de l'Art nécessaire à la compréhension de la problématique et à la mise en place des différentes expérimentations. Le premier chapitre de ce manuscrit est une présentation du contexte opérationnel des missions de l'Armée de l'Air, du concept de C2 et de l'impact des systèmes de cyberdéfense dans l'organisation de ces C2. Ce premier chapitre permet de mettre en évidence les enjeux liés à la CI entre les opérationnels des C2 agissant dans le contexte cyber.

Le deuxième chapitre correspond à un état de l'art proposant d'étudier les différents mécanismes de confiances, qu'ils soient interpersonnels ou entre un opérateur humain et un système automatisé. Dans cette partie académique sont notamment étudiés le processus de mise en place d'un niveau de confiance entre deux opérateurs mais également les conséquences comportementales engendrées par ce niveau de confiance. A la fin de ce deuxième chapitre, un modèle est présenté. Toutes les parties de ce modèle sont ensuite étudiées dans la suite du manuscrit.

Les cinq chapitres suivants correspondent aux développements expérimentaux conduits durant la thèse. Le chapitre 3 propose d'étudier la possibilité d'induire différents niveaux de confiance chez les potentiels décideurs finaux de la RCPair. Le chapitre 4 est une présentation et un test du protocole expérimental utilisé pour les 4 expérimentations suivantes. Le chapitre 5 propose d'étudier expérimentalement (expérimentation 1) les conséquences d'un excès ou d'un manque de CI en fonction des caractéristiques psychosociales des opérateurs.

Le chapitre 6 est divisé en deux expérimentations (expérimentations 2 et 3). La première expérimentation propose d'étudier le lien entre les conséquences comportementales engendrées par une modulation du niveau de CI et celles engendrées par une modulation du niveau de de CM. La deuxième expérimentation a pour but d'étudier le lien entre la confiance en soi (CS) et les conséquences comportementales engendrées par une modulation du niveau de CI. Prise ensembles,

les deux expérimentations présentées au chapitre 6 permettent d'observer les interactions entre les différentes confiances (CI et CM) pouvant rentrer en jeux dans les C2. Enfin le chapitre 7 propose d'étudier expérimentalement (expérimentation 4) l'impact d'un environnement cyber sur le comportement des opérateurs soumis à différents niveaux de confiance.

Dans la mesure du possible, tous les chapitres ont été pensés de telle sorte à ce qu'ils puissent être lus séparément. Sur la première page de chaque chapitre un résumé est proposé. Ce résumé comprend le/les objectif(s) du chapitre, la démarche utilisée et le/les conclusion(s) de ce chapitre. Sur la dernière page de chaque chapitre (à la fin de chaque expérimentation dans le chapitre 6) les points les plus importants à retenir sont énumérés.

Afin que les chapitres puissent être lus indépendamment les uns des autres il a été décidé d'inclure, au début de chaque chapitre mettant en œuvre une expérimentation (chapitres 5, 6 et 7) un cadre théorique. Ce cadre théorique reprend les éléments et notions essentielles à la compréhension du chapitre correspondant. Cependant, ce cadre théorique se focalise sur un des aspectsdu cadre théorique présenté aux chapitres 1 et 2. De fait, dans tous les cas, les notions présentées dans les cadres théoriques des chapitres 5, 6 et 7 auront été vues dans les chapitres 1 et 2.

1 Constat opérationnel

Résumé du chapitre

Objectif : Identifier le contexte et les objectifs de la mise en place de la RCPair dans les C2 de l'Armée de l'Air

Démarche : Faire une synthèse portant sur :

- l'évolution de l'utilisation des technologies de l'information et de la communication au sein de l'Armée Française
- l'impact des premières cybers attaques sur les infrastructures militaires et sur les besoins de l'Armée de l'Air
- le fonctionnement et le rôle des C2 au sein de l'Armée de l'Air

Conclusion : Ce chapitre permet de comprendre le rôle de la RCPair ainsi que les potentiels bouleversements que pourront engendrer la mise en place de cette RCPair dans les C2 de l'Armée de l'Air

Chapitre 1 : Constat opérationnel

1. La guerre réseau-centrée (NCW)

La notion de guerre réseau-centrée (Network Centric Warfare - NCW) (*Cf.* Figure 1), apparait dans les années 1990 en s'inspirant des transformations du monde économique de l'époque, dans lequel le développement des réseaux informatiques modifie profondément les organisations, la productivité et la réactivité des entreprises (De Neve & Henrotin, 2006). Cette nouvelle organisation des opérations militaires permet une augmentation des liens entre les différentes entités travaillant ensemble dans une zone de combat et fait prendre une place prépondérante aux technologies de l'information et de la communication (TIC) dans la guerre moderne.

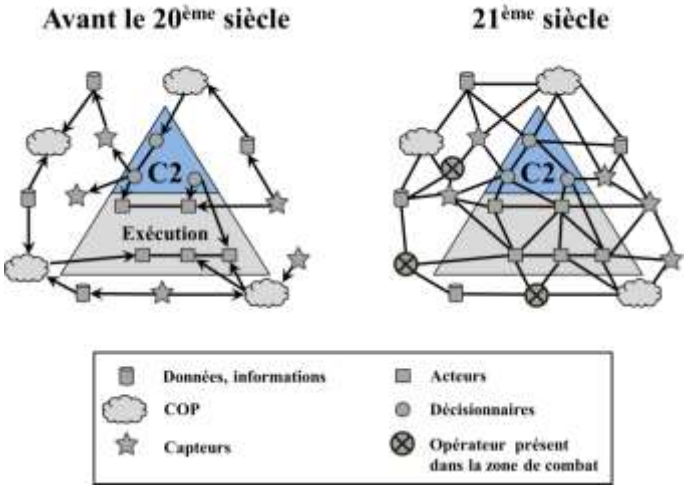


Figure 1 : Image inspirée de celle présente dans le livre « Network Centric Warfare: Developing and Leveraging Information Superiority » (Alberts, Garstka, & Stein, 2000).
Ce schéma représente l'évolution au cours du temps, du rôle, de chacune des entités présentes sur le champ de bataille dans le transfert d'information,. L'image de gauche montre une représentation schématique du théâtre d'opération avant la NCW. Cette représentation montre un système pyramidal avec le C2 en haut de la pyramide. Toutes les informations transitent vers ce C2. Les opérateurs à l'intérieur des C2 prennent des décisions et donnent les ordres aux entités présentes sur le champ de bataille. Dans la NCW (à droite de l'image) toutes les entités se transfèrent des informations entre elles ce qui permet une prise de décision « collaborative ». Le C2 est toujours présent mais l'organisation est à présent « en grappe » ce qui permet un meilleur échange d'informations et une amélioration de la fiabilité de la représentation partagée (Common Operational Picture, ou COP sur ce schéma).

Dans l'organisation militaire opérant avant l'apparition de la NCW, toutes les informations recueillies par les différents « acteurs » étaient transmises au centre de commandement et de conduite des opérations (C2) (*Cf.* Figure 1) qui avait pour rôle de coordonner les opérations militaires en cours. Selon la complexité de la mission, un ou plusieurs centres pouvaient coopérer entre eux (*Cf.* partie 5 de ce chapitre « Le C2, un concept et non un système »). Les opérateurs présents dans le C2 étaient en charge de trier, d'analyser et de mettre en relation les différentes informations reçues afin de prendre des décisions. Les décisions prises dans le C2 étaient ensuite transmises aux différents « acteurs » qui devaient exécuter les ordres. Schématiquement, dans cette organisation

pyramidale, le flux d'informations montantes correspondait au transfert de données non triées et non traitées alors que le flux d'informations descendantes correspondait au transfert d'ordres résultants du tri et du traitement des données par les opérateurs du C2. Avec l'avènement des TIC, cette organisation « C2 centrée » s'est transformée en une organisation « réseau centrée » (*Cf.* Figure 1). Le principe central de la NCW, est que tous les « acteurs » puissent transférer des informations et avoir accès à l'intégralité des informations présentes sur le réseau. Dès lors, dans la NCW, le C2 peut toujours être considéré comme étant le décisionnaire « final » ; cependant il n'est plus uniquement « collecteur » de données mais acteur à part entière du théâtre d'opération.

En 1999, pendant la guerre du Kosovo, la mise en place de la NCW a permis des prises de décision pouvant faire intervenir une dizaine d'acteurs de pays et d'unité différentes par le biais de communications satellites, de fibres sous-marines et de radiofréquences (Alberts & Hayes, 2003). Durant cette guerre, la NCW a démontrée son utilité dans l'amélioration de la coordination des frappes en permettant une intervention des troupes aériennes moins d'une heure après une demande d'appui feu. Durant la guerre en Irak (début des années 2000) ce temps a été réduit à moins de vingt minutes (De Neve & Henrotin, 2006). Ceci a été rendu possible grâce notamment au perfectionnement et à la prépondérance des TIC, que ce soit dans l'observation des informations présentes, dans l'orientation des actions, dans la décision de la stratégie ou encore dans le passage à l'action (Levieux, 2005).

Au niveau OTAN, le concept de la NCW a notamment été mis en place à l'aide de liaisons de données tactiques pensées et développées comme des outils d'aide à la décision centrés réseau (Godé, Hauch, Lasou, & Lebraty, 2012) interopérables (Asenstorfer, Cox, & Wilksch, 2003). Dès lors, toutes les unités, quel que soit leur pays et quelle que soit leur armée, peuvent, si elles sont équipées de ces liaisons de données interopérables, aider à la création d'une représentation partagée de la situation tactique (SiTac) (*Cf.* Figure 2) (Asenstorfer et al., 2003).

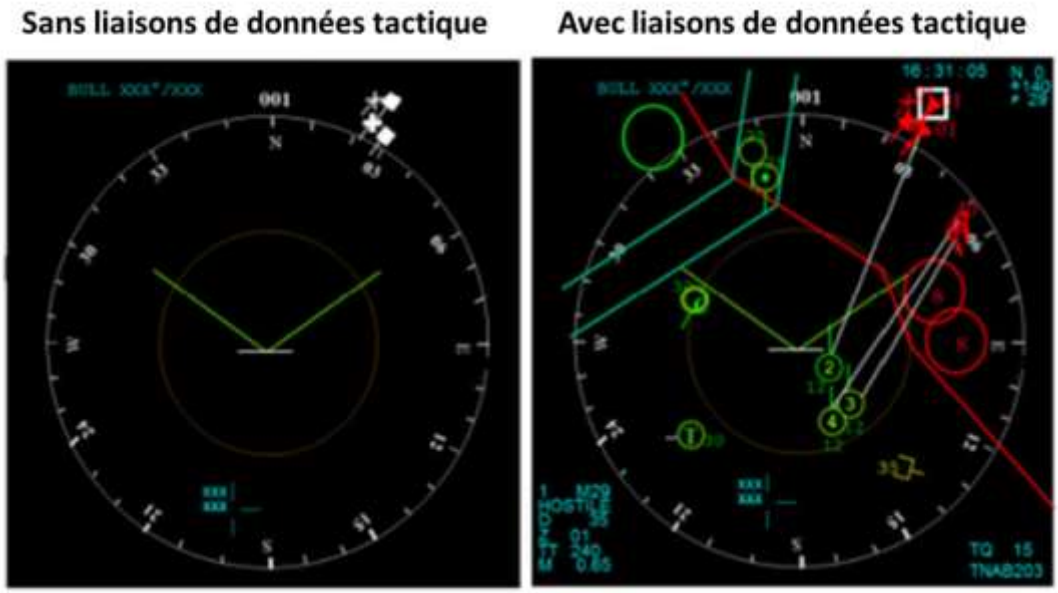


Figure 2 : Ecran de visualisation embarqué dans un Mirage 2000D (Armée de l'air, 2019).
A gauche de l'image est présentée la visualisation obtenue grâce à l'utilisation exclusive des capteurs de l'aéronef. A droite de l'image est présentée un exemple de SiTac obtenue grâce à l'utilisation de liaisons de données tactiques interopérables. Sur cette SiTac se trouvent différentes informations transmises par le

réseau comme les ennemis (en rouge en haut), ce qui semble être la ligne ennemie (en rouge), ce qui semble être un corridor de passage qui coupe la ligne ennemie (lignes parallèles en vert) et un avion non reconnu volant à une altitude de 35000 pieds (en jaune en bas). Toutes ces informations sont transmises au Mirage 2000D par les différents membres du réseau et peuvent être affichées ou non par l'équipage.

2. De la NCW au risque cyber

Afin de bénéficier pleinement des avantages de cette organisation réseau-centrée, en 2006 la France commence à équiper ses chasseurs, et en premier lieu le *Rafale,* d'une liaison de données tactiques nommée « Liaison 16 » (L16) (Godé et al., 2012). L'implémentation de la L16 entraine un changement d'échelle dans la NCW en permettant les communications au-delà de la ligne d'horizon[1] et une standardisation au sein des troupes alliées. Dès lors, la SiTac, créée par les forces armées Françaises peut être augmentée d'informations provenant d'autres pays. Cette pluralité des sources d'information constitue la force du système mais rend aussi le processus plus complexe.

En effet, pour les équipages de *Rafale* ou tout autre opérateur engagé dans les opérations, ces changements d'échelle (de l'Armée à l'interarmée, du national à l'international) obligent à passer de l'utilisation d'une SiTac relativement limitée, alimentée par ses proches et sa hiérarchie, à une SiTac plus complète réalisée à partir de sources disparates. En d'autres termes, dans un système pyramidal, le C2 était responsable de la construction et du maintien de la SiTac alors que dans la NCW la responsabilité devient partagée et diffuse entre les différents commandements. Dès lors, les acteurs des opérations (personnels navigants, troupes sur le terrain, opérateurs des C2) se doivent d'avoir confiance en des SiTac de plus en plus complexes réalisées sur la base d'informations dont la véracité est difficilement vérifiable.

Au début des années 2000, du fait de la fiabilité supposée des TIC et du nombre d'informations recoupées pour créer une SiTac, le système semblait être fiable. Cependant, en raison de la prolifération des TIC et de l'avènement d'internet, des nouvelles menaces provenant du cyberespace apparaissent dans le domaine civil comme en Géorgie en 2008 ou encore en Iran en 2010 (Farwell & Rohozinski, 2011). Dès 2007, les attaques cyber touchent les infrastructures militaires ; pour l'opération *outside the box* (ORCHARD) les Israéliens utilisent une cyberattaque sophistiquée (Adee, 2008) permettant de brouiller les signaux radars Syriens afin de détruire, en toute discrétion, un site suspecté d'être un réacteur nucléaire (Opall-Rome, 2018). Ces nouvelles menaces remettent en cause la fiabilité des TIC et la confiance que les opérateurs peuvent avoir dans les données échangées.

En 2009, le virus *Conflicker* infecte le département américain de la défense, le ministère de la défense britannique et empêche, pendant 2 semaines, le décollage des *Rafale* de l'aéronavale française (Baud, 2012). Cette première cyberattaque d'envergure mondiale met à jour les vulnérabilités des TIC mais également des failles propres aux facteurs organisationnels et humains. En effet, à l'inverse de ce que rapportait la presse spécialisée, les dommages engendrés par *Conflicker* en 2009 n'étaient pas imputables au virus lui-même mais aux décisions prises lors de

[1] Traditionnellement, afin d'assurer la transmission d'une information, les liaisons de données nécessitaient une « vue » directe entre l'émetteur et le récepteur. Si l'émetteur et le récepteur étaient trop éloignés (au-delà de la ligne d'horizon…) ou séparés par un obstacle (montagne…), les informations ne pouvaient pas bien transiter. Les nouvelles liaisons de données (et notamment la L16) ont permis de s'affranchir de cette contrainte.

l'attaque ; c'est en réalité plus la méconnaissance des impacts engendrés par une coupure du réseau infecté et le temps mis pour effectuer cette coupure (plus de deux jours) qui ont posé problème plutôt que le virus lui-même (Ghernaouti-Hélie, 2009). Comme l'indiquait d'ailleurs Laurent Teisseire, le porte-parole du ministère de la Défense à l'époque des faits **«** *C'est le déclenchement des procédés curatifs qui a entrainé l'arrêt du réseau Intramar de la Marine »* (Ghernaouti-Hélie, 2009).

3. Du risque cyber à la recognized cyber picture (RCPair)

Ces premières cyber-attaques touchant les infrastructures militaires ont entrainé une prise de conscience de la vulnérabilité des systèmes de défense et ont amené les États à mieux définir leurs besoins et leurs stratégies de gestion de la cyber sécurité. En 2011, l'Agence Nationale de la Sécurité des Systèmes d'Information publie la stratégie de la France en matière de cyber sécurité (ANSSI, 2011). En 2016, les différents États membres de l'Union Européenne signent une directive visant à renforcer leur capacité nationale de cybersécurité et à faciliter le partage d'informations sur les vulnérabilités cyber (Directive, 2016). Bien que les stratégies institutionnelles en matière de management des crises cyber restent très hétérogènes et spécifiques aux différents Etats (Boeke, 2017), les besoins en matière d'analyse et de compréhension de la situation cyber sont similaires. De fait, tous les États doivent disposer d'outils de monitoring et de centre de coordination prenant en compte la cyber sécurité. Dans ces C2 consacrés au cyber, la collecte et l'analyse des informations devront permettre aux opérateurs et décideurs de « donner du sens »[2] à une crise cyber (Boin, Busuioc, & Groenleer, 2014).

Pour l'armée de l'air française (AA), il devient nécessaire d'avoir une représentation partagée au sein de la chaîne de commandement, de l'état cyber du réseau, qu'il soit passé, présent ou futur (Vilchenon, 2015). Ceci implique de pouvoir, sur la base de l'activité observée, identifier les systèmes et les informations qui pourraient être corrompus ou dégradés, afin d'anticiper au mieux l'impact des anomalies observées sur l'état futur du réseau de communication. Actuellement, aucune visualisation globale ne permet de rassembler et représenter les failles détectées, puis d'identifier et d'analyser les effets de bord, c'est-à-dire les comportements non prévus du système ou de son environnement numérique.

Dans les années à venir, l'AA devra donc se doter d'un outil permettant de superviser et cartographier les liens entre les différents systèmes d'information et d'agir par anticipation en préparant les systèmes à affronter les agressions. C'est sur la base de cette représentation que les décisions pourront être prises et coordonnées. Pour l'AA, l'outil permettant cette représentation se nomme la « Recognized Cyber Picture » (RCPair) et sera alimenté tant par des analyses automatiques des activités sur les différents réseaux, que par des opérateurs identifiant des anomalies.

La RCPair a vocation à constituer un système entièrement français, géré par des militaires français, déployé à différents niveaux hiérarchiques afin de surveiller et gérer la cyber sécurité des systèmes d'information, de communication et de défense français. Toutefois, cette RCPair n'étant pas encore totalement définie, aucune information permettant d'en comprendre son fonctionnement et son

[2] Prendre conscience de la situation, comprendre les causes de cette situation, anticiper les futurs possibles de cette situation et leurs conséquences sur les infrastructures, les organisations ou encore sur la réussite d'une mission. Donner du sens permet aux opérateurs de prendre des décisions. (NATO, 2006)

organisation n'est disponible dans la littérature. Afin de mieux comprendre cette RCPair il est donc nécessaire d'effectuer une analyse du besoin auprès des opérationnels de l'AA.

Durant les six premiers mois de la thèse une analyse du besoin a donc été réalisée auprès de différentes personnes de l'AA et a donné lieu à la rédaction d'un document nommé « Analyse du besoin opérationnel des différentes unités Air concernées par la Recognized Cyber Picture GT 16 – feuille de route Cyber » transmis à l'AA. Les parties présentées ci-dessous, dont le titre est suivi de « AB », proviennent de cette analyse du besoin et correspondent aux informations nécessaires à la compréhension de la suite du manuscrit. Le document complet présentant les résultats de l'analyse du besoin est présenté en annexe 1. Cette analyse du besoin ayant été terminée il y a plus de deux ans il est fort probable que les éléments présentés ici aient évolué depuis l'étude.

4. Généralités sur la RCPair « AB »

La RCP n'est pas définie mais une étude de la chaine de lutte informatique défensive (LID) Française montre qu'elle pourrait intervenir à différents niveaux distincts :

- Au niveau des bases aériennes, auprès des Responsables Cybersécurité (Rcyb) ou des Correspondants Sécurité des Systèmes d'Information (CSSI) ;
- Au haut niveau de la chaîne de lutte informatique défensive (LID) Air, auprès du Centre Air de Conduite Cyberdéfense (CACC), qui a pour rôle la conduite des opérations cyber et l'entrainement cyber des forces de l'AA, et de l'Escadron des systèmes d'information opérationnelle et de cyberdéfense (ESIOC) qui a pour rôle de développer des applications et d'assurer le soutien de systèmes d'informations opérationnels ainsi que la cyberdéfense des systèmes métiers ;
- Au haut niveau de la chaîne LID Interarmées, auprès du Centre d'Analyse de Lutte Informatique défensive (CALID) et du Centre Opérationnel de la Cyberdéfense (COCyber).

L'étude présentée ici s'axe uniquement sur une vision AA de cette RCP (notée RCPair) et non sur le volet interarmées de la RCP, ce qui exclut de cette analyse du besoin le haut niveau de la chaîne LID Interarmées. Cette RCPair consiste en l'amélioration des représentations d'une attaque cyber sur les structures de l'AA. De fait la RCPair devrait se placer au niveau du Centre National des Opérations Aériennes (CNOA) qui est « *chargé de la synthèse permanente de la situation aérienne générale, de la programmation et de la conduite des opérations aériennes* » (Sirpa Air, 2010). A terme, cette RCPair pourrait descendre dans les échelons hiérarchiques afin d'être intégrée dans les différents centres de détection et de contrôle (CDC)[3], au CACC et à l'ESIOC.

L'analyse du besoin a été effectuée auprès d'acteurs de la chaine de la LID de l'AA pouvant être des potentiels opérateurs de la RCPair :

- Des équipes spécialisées dans la LID Air
  - Équipes du CACC ;

[3] Afin d'effectuer ses missions de contrôle aérien l'AA possède, sur le territoire Français, 3 CDC actifs et un CDC en « sommeil » (*Cf* infra « Analyse conceptuelle de l'organisation possible des C2 de l'AA »)

- Équipes de l'ESIOC ;
- Equipe de Marque Cyber (EM Cyber).

- Des agents cybers présents sur les bases aériennes
  - Commandant de la base aérienne 113 de Saint-Dizier-Robinson ;
  - Responsable cybersécurité de la base aérienne 113 de Saint-Dizier-Robinson ;
  - Responsable cybersécurité de la base aérienne 133 de Nancy-Ochey ;
  - Bureau de la sécurité des systèmes informatiques (BSSI) de la base aérienne 118 de Mont-de-Marsan.

- Des personnels non experts cybers présents dans les CDC
  - Contrôleurs aériens de la base aérienne 705 de Cinq-Mars-La-Pile.

A. Définition et concept de la RCPair « AB »

La RCPair, telle qu'envisagée par les différents membres de l'AA (En prenant en compte le besoin de tous les opérateurs de la LID de l'AA et pas seulement le besoin des opérateurs du CNOA ou des CDC), pourrait être un Méta-Système matriciel (un système au-dessus de tous les autres systèmes de l'AA et récupérant leur données) alimenté par différents moyens matériels et humains et ayant pour sorties différentes interfaces homme-machine (IHM) selon les besoins utilisateurs. Si la RCPair devait répondre aux besoins de tous les membres de la chaine LID de l'AA, la RCPair serait un outil permettant, grâce à des IHM de sorties spécifiques, d'obtenir et de partager la représentation partagée des états cyber. La définition, qui a fait consensus auprès des différents membres de l'AA contactés est la suivante :

« La RCP est un outil d'aide à la compréhension et à la représentation des états cybers des systèmes permettant d'améliorer la lutte informatique défensive et de faciliter la prise de décision des opérateurs ».

Cette définition permet de mettre en évidence les deux volets de développement, technique et humain, de la RCPair. Le volet technique est défini par la notion de « *représentation des états cybers des systèmes* » et le volet humain par la « *prise de décision des* opérateurs ». La notion « *d'outil d'aide à la compréhension et à la représentation* » est extrêmement importante dans cette définition en plaçant la RCPair non comme étant un outil de protection des systèmes de l'AA mais comme un outil permettant d'assurer les prestations et les missions. Cette définition décrit donc la RCPair comme étant un outil, placé dans un C2, permettant de donner du sens à une crise cyber.

Une telle RCPair est actuellement inenvisageable tant au niveau de sa complexité matérielle que de sa mise en place humaine. Les conclusions de l'analyse du besoin indiquent que si la RCPair devait

s'adapter aux besoins de tous les opérateurs de la chaine LID de l'AA, elle devrait en réalité s'adapter à tout le personnel de l'Armée. Cela rejoint ce qu'indiquait d'ailleurs la ministre de la Défense en 2018 « *La cyberdéfense n'est pas l'affaire d'un ministère : c'est l'affaire de tous* **»** (Ministère des armées, 2018). Pour ces raisons, l'analyse du besoin a été particulièrement focalisée à l'utilisation de la RCPair pour la défense aérienne (ce qui pourrait correspondre aux besoins du CNOA et des CDC).

B. Choix du décideur final de la RCPair « AB »

Pour la défense aérienne, la RCPair serait un outil pouvant permettre de détecter des attaques cyber visant les écrans de contrôle (une perte, un ajout ou une multiplication du nombre d'aéronefs par exemple). Cette RCPair pourrait être utilisée en opération extérieure ou dans le cadre de la posture permanente de sureté (PPS)[4] afin de détecter une intrusion cyber sur tout type de système de défense aérienne.

Dans ce cas, différents profils d'opérateurs experts pourraient être envisagés afin d'utiliser la RCPair. A ce stade, ceux-ci ne sont pas identifiés mais ils seront probablement issus des différentes « familles » de spécialités présentes dans l'AA :

1. Afin de différencier au mieux les vraies intrusions sur les différents écrans de contrôle il pourrait être nécessaire que des **contrôleurs aériens** fassent parti des opérateurs de la RCPair ;

2. Afin de détecter au mieux la provenance des potentielles défaillances (problème matériel ou attaque cyber) il pourrait être nécessaire que des **mécaniciens spécialistes des Systèmes d'Informations et de Communication** fassent parti des opérateurs de la RCPair ;

3. Afin de faciliter la prise de décisions, il pourrait être nécessaire que des **personnels navigants** (pilotes ou navigateurs officiers systèmes d'armes), fassent parti des opérateurs de la RCPair. En effet, dans l'AA, les personnels navigants sont formés à prendre des décisions rapides et sont privilégiés dans les hautes carrières ainsi que dans les postes à forte responsabilités ;

4. Afin de comprendre les risques liés à une menace cyber il pourrait être nécessaire que des **experts en cyber sécurité** ou des **officiers renseignement** fassent parti des opérateurs de la RCPair.

Parmi ces opérateurs potentiels, le décideur final de la RCPair n'a pas pu être déterminé dans l'analyse du besoin (les expérimentations présentées dans cette thèse permettront « d'orienter » le choix de ce décideur final). Cependant, la liste des opérateurs potentiels montre plusieurs différences interindividuelles, présentes entre ces opérateurs, qui devraient être prises en compte lors du choix du décideur final et qui seront donc étudiées dans cette thèse.

Premièrement, les potentiels opérateurs envisagés ont des grades différents, les contrôleurs aériens (CA) et les mécaniciens sont en grande majorité des sous-officiers quand les personnels navigants (PN) sont des officiers. Cette différenciation au niveau des grades entraine une différence

[4] Mission permettant d'assurer la défense aérienne au-dessus du territoire national (*Cf.* infra « Analyse conceptuelle de l'organisation possible des C2 de l'AA »)

au niveau de la formation mais également au niveau de la prise de décision (dans ce domaine, les officiers ont une formation plus « aboutie » que les sous-officiers et sont en charge quotidiennement de prendre des décisions).

Deuxièmement, les potentiels opérateurs envisagés ont des métiers différents ce qui entraine des compétences et des connaissances différentes selon l'opérateur. En effet, les mécaniciens spécialistes des systèmes d'informations sont formés aux potentiels problèmes (informatiques ou mécaniques) pouvant survenir sur les différents systèmes d'informations. Les experts en cyber sécurité ou les officiers renseignements sont quant à eux formés aux risques de « fuites » d'informations et aux risques d'attaques cybers. De leur côté, les personnels navigants sont formés au fait que les systèmes ne sont pas fiables dans toutes les conditions d'utilisation. Pour ces quatre catégories d'opérateurs une attaque cyber détectée par le système RCPair pourrait être facilement « acceptée ». D'un autre coté les contrôleurs aériens sont formés à avoir confiance dans leur système et à le considérer comme étant fiable et non « attaquable ». Pour cette catégorie d'opérationnel une attaque cyber sur leur système semble « inenvisageable » (d'après les différents contrôleurs interrogés durant l'AB).

Troisièmement, les potentiels opérateurs envisagés n'ont pas le même environnement de travail. Les mécaniciens et les CA ont l'habitude de travailler en équipe, les experts en cyber sécurité travaillent généralement seuls ou en petit groupe alors que les PN sont généralement seul ou à deux dans leur avion mais en interaction à distance avec plusieurs interlocuteurs. Outre cette différence au niveau de l'environnement de travail, des différences peuvent également apparaitre au niveau du risque présent dans l'environnement de travail ; les PN et les mécaniciens peuvent partir en opérations extérieures (OPEX) alors que les CA restent sur le territoire national. En OPEX les opérateurs sont éloignés de leur famille et confrontés à la « réalité de la guerre ». En OPEX, le risque permanent de déclenchement d'une situation hostile est omniprésent ce qui augmente le stress des individus dans leur environnement de travail. De plus, en OPEX, l'opérateur est éloigné de son domicile et davantage restreint dans ses cercles de vie professionnelle et extraprofessionnelle. Ainsi contraint de travailler en équipes restreintes et difficilement changeables, les relations extraprofessionnelles se confondent avec les relations professionnelles. Afin d'appréhender ces différents risques, des formations spécifiques sont données aux opérationnels devant effectuer des OPEX. Cependant, il est possible que l'environnement de travail a fort risque vital ainsi que l'éloignement du cadre familial puisse modifier le comportement des individus ayant fait des OPEX.

Quatrièmement, les potentiels opérateurs envisagés n'ont pas le même niveau d'étude et ne font pas tous partis de la même institution. Les PN, les CA et les mécaniciens sont membres de l'AA et peuvent avoir des niveaux d'études très disparates allant du baccalauréat au diplôme de niveau 7 alors que les experts en cybers sécurité ne font pas forcément partie de l'AA ont en général un diplôme de niveau 6 voir supérieur.

Outre le grade, l'environnement de travail ou encore le niveau d'étude, des différences pourraient être présentes sur les profils psychologiques (personnalité) des potentiels opérateurs de la RCPair. Bien qu'il semblerait que les profils psychologiques (Goldberg, 1992) jouent un rôle dans le comportement des individus (Salgado, 2002) il a été décidé de ne pas les prendre en compte dans cette thèse ; en effet, il a été considéré que tous les opérationnels de l'AA et les professionnels de la cybersécurité avaient préalablement subi différents processus de sélections, et que, par conséquent,

ces différents profils psychologiques avaient déjà été considérés comme aptes par les différentes institutions au cours de la sélection.

C. Flux d'informations dans la RCP « AB »

Afin d'analyser, de traiter et de transférer au mieux les informations, la RCPair pourrait devoir associer une intelligence artificielle (IA) au décideur final. Dans cette approche, une IA permettra de classer et d'analyser rapidement des informations déjà répertoriées, ou ressemblant à des informations connues, afin d'effectuer un stockage efficace (en terme de temps et de ressources) de ces informations. Seulement, du fait de l'évolution constante du monde cyber il sera nécessaire qu'un opérateur humain puisse intervenir à tout moment pour traiter les informations ambigües ou non utilisables par le système. Il est donc essentiel qu'une personne physique soit présente dans la boucle de la RCPair ce qui exclut la possibilité d'un système autonome.

Dans ce type d'approche, les pannes ou problèmes redondants pourraient être gérés automatiquement par l'IA afin d'éviter à l'opérateur humain, la surcharge engendrée par une masse importante de données. Les pannes ou problèmes plus rares mais ressemblant à des données déjà vues pourraient être traités indépendamment par l'IA ou l'opérateur humain, voire de manière semi-automatique. Enfin, les pannes ou problèmes jamais répertoriés pourraient être traités entièrement par l'opérateur humain (*Cf.* Figure 3).

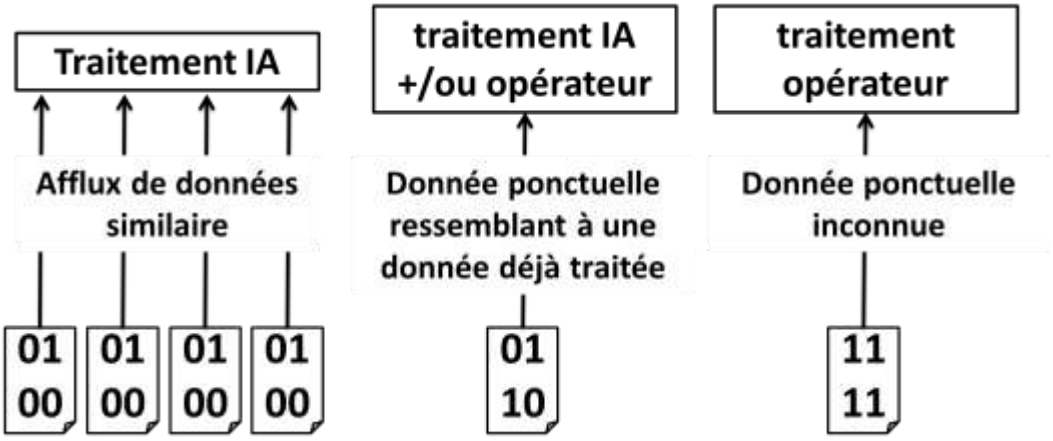


Figure 3 : Exemple de traitement de l'information dans la RCP

D. Vue conceptuelle globale de la RCPair « AB »

L'analyse du besoin a donnée lieu a une vue conceptuelle globale de la RCP (*Cf.* Figure 4) dont une version simplifiée aux besoins de la RCPair a été ajoutée pour les besoins du manuscrit. La vue conceptuelle de la RCPair montre un système en 3 parties comprenant :

- Les données d'entrée ;
- Le système de traitement ;
- Les données de sortie.

La partie portant sur les données d'entrée indique que seulement deux types de données peuvent alimenter la RCPair : les données matérielles ou logicielles, et des données humaines. Le système de traitement a été décrit dans le paragraphe précédent et est représenté dans le schéma comme étant une boite noire car ce système fera probablement appel à des algorithmes complexes et ne pourra pas en cas de rupture, être suppléé par un humain. Enfin, les données de sorties correspondront probablement à une IHM présentant une cartographie des systèmes et de leurs interactions. Cette IHM n'étant pas définie il a été décidé de l'indiquer sous le terme *IHM RCPair* dans le schéma.

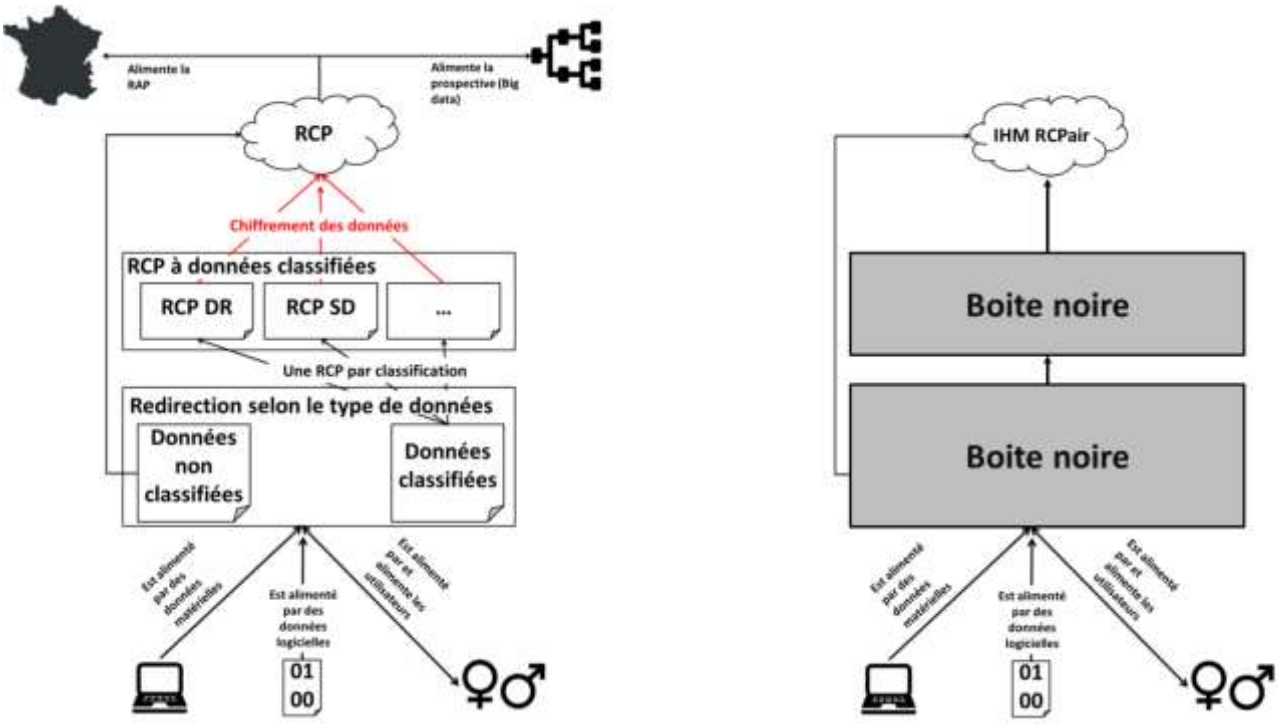


Figure 4 : Représentation des liens présents dans la RCP obtenus après l'analyse du besoin (à gauche) et représentation de ce qui sera analysé au cours de cette thèse (à droite).

5. De la RCPair à la cyber-résilience

Le concept de cette RCPair est fondé sur les bases de fonctionnement de la *Recognized Air Picture, ou* RAP (Mercier, 2015) qui peut être définie comme une capacité de l'AA « *d'afficher sur un seul écran des vues combinées des images reconnues (ER) et de les compléter par des améliorations fonctionnelles (par exemple, logistique, renseignement et environnement) visant à améliorer la connaissance de la situation du commandant.* **»** (Fanti & Beach, 2002)[5]. Cette représentation partagée de l'espace aérien est générée et distribuée aux différents acteurs puis affichée et utilisée dans les C2 afin de permettre l'exécution de différentes tâches (Bélanger, Maupin, Berger, Boukhtouta, & Allouche, 2007).

L'IHM RCPair, fondée sur les principes de la RAP, devrait présenter sur un même écran une vue intégrée de la situation cyber de l'ensemble des systèmes ainsi que des informations et des outils

[5] « to display on a single screen integrated views of the Recognized Pictures (RPs) and to complement them with functional enhancements (e.g. logistics, intelligence and environmental) aimed at enhancing the Commander's situational awareness**. »** (Fanti & Beach, 2002)

permettant au commandement d'appréhender au mieux la situation présente et son évolution probable. Cette RCPair devrait avoir des problématiques similaires à celle de la RAP et devrait être implémentée dans le même type de centre que la RAP à savoir les C2 de l'AA (C2air).

Les C2 sont actuellement repensés comme devant être agiles et résilients afin de prendre en compte les nouveaux enjeux résultant du cyber espace (Maybury, 2013 ; Ministry of Defense, 2017). L'agilité fait référence à la capacité de se reconfigurer, par exemple en changeant les rôles des différents acteurs ou en modifiant des canaux de communication, dans le but de rester adapté aux contraintes de la situation. La notion de résilience fait elle référence à la capacité à pouvoir continuer son activité avec un certain niveau de performance malgré des conditions d'opération dégradées. Dans cette lignée, la notion de cyber-résilience, peut être définie comme étant « *La capacité à fournir en permanence le résultat escompté malgré les cyber événements indésirables* **»** (Björck, Henkel, Stirna, & Zdravkovic, 2015)[6].

La cyber-résilience est décrite par des notions équivalentes à celles de la cyber sécurité mais avec pour objectif principal d'assurer des prestations et non de protéger les systèmes (Björck et al., 2015). En 2013, Linkov et al. caractérisent la cyber-résilience comme étant une combinaison des domaines de la physique, de l'information, de la cognition et des sciences sociales (Linkov et al., 2013). Ces quatre grands domaines sont scindés en deux champs disciplinaires différents. Les domaines de la physique et de l'information appartiennent à la Science de la data, à l'informatique et à l'ingénierie alors que les domaines des sciences sociales et de la cognition se rapprochent des Sciences humaines (Alberts et al., 2003). De manière similaire à la RCPair, aborder la question de la cyber-résilience invite donc à considérer tant les aspects techniques des systèmes mis en œuvre que les composantes organisationnelles liées aux opérateurs qui les utilisent. Cependant, une étude bibliométrique (Borgman & Furner, 2001) effectuée avec l'outil d'analyse de Scopus met en évidence une inégalité des champs de recherche dans la cyber-résilience. Avec un total supérieur à 60%, les documents consacrés aux sciences de l'informatique et de l'ingénieur sont largement plus représentés que les différentes sciences sociales (qui atteignent moins de 15%) (Cf. Figure 5). En élargissant cette analyse bibliométrique à tout le domaine de recherche portant sur le terme « cyber » ces proportions restent quasiment identiques. Ainsi, bien que les États définissent la résilience et l'agilité comme étant fondamentales pour les C2 et les systèmes de cyber-sécurité, la communauté scientifique semble axer les recherches sur des domaines techniques plutôt que sociaux et semble ainsi ne considérer qu'une de ces composantes de la résillience.

[6] « The ability to continuously deliver the intended outcome despite adverse cyber events **»** (Björck et al., 2015)

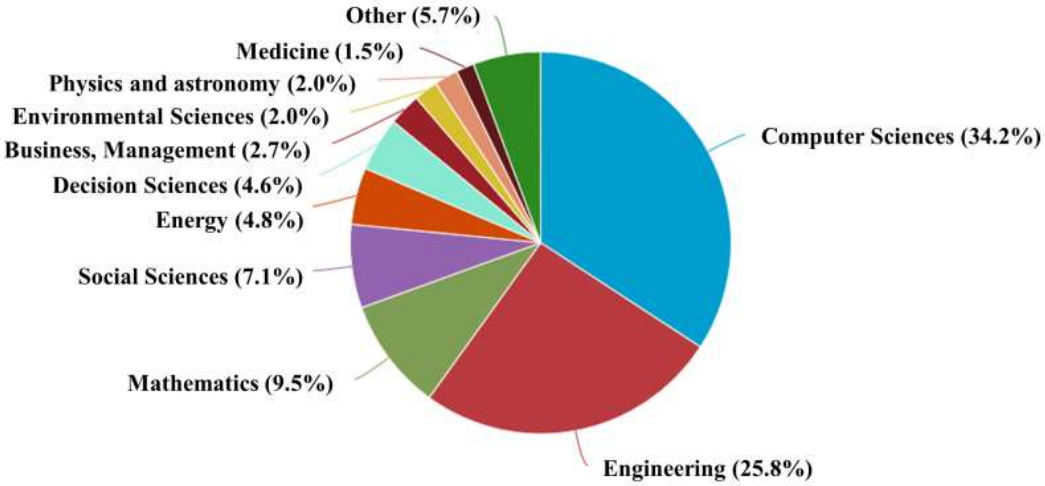


Figure 5 : Répartition des sujets d'étude dans la cyber resilience (résultats donnés par SCOPUS)

Dans le domaine relativement nouveau qu'est le cyber « en général », lorsque le système est considéré uniquement dans sa dimension informatique il est étudié comme un acteur autonome capable de recueillir, analyser et interpréter le grand nombre d'informations nécessaires à l'étude de la cyber-sécurité, des cyber-attaques, des cyber-menaces, des cyber-guerres, des cyber-crimes ou encore du cyber-terrorisme. Cette approche technique permet de répondre aux besoins de différentes disciplines composant la cyber (cyber-sécurité, cyber-attaques, cyber-menaces, cyber-guerres, cyber-crimes, cyber-terrorisme…).

Si la RCPair était considérée uniquement sous l'angle d'un système isolé de cyber-sécurité mis en jeu dans la cyber-guerre pour anticiper et contrer les cyber-menaces, cette approche technique ferait sens. Cependant, la RCPair ne sera pas un système isolé mais un outil permettant de donner une fonction cyber aux C2 de l'AA. Comme vue précédemment, la RCPair aura donc une fonction « technique » de représentation des états cybers qui permettra de soutenir une fonction « humaine » en transmettant des informations cybers à des opérateurs devant prendre des décisions.

L'analyse du besoin présentée ci-dessus, traitant des caractéristiques propres au système RCPair, parait donc être incomplète car pour comprendre le fonctionnement de la RCPair (comment la RCPair pourra permettre aux opérateurs de prendre une décision) il est nécessaire d'étudier cette RCPair dans son « environnement final », à savoir, l'environnement sociotechnique des C2air.

6. Le C2, un concept et non pas un système

Dans le « NATO glossary of terms and definitions » de 1988, le C2 est présenté comme assurant « *les fonctions des commandants, des états-majors et des autres organes de commandement et de contrôle dans le maintien de l'état de préparation au combat de leurs forces, la préparation des opérations et la direction des troupes dans l'accomplissement de leurs tâches. Le concept englobe l'acquisition, la fusion, l'examen, la représentation, l'analyse et l'évaluation continues des informations sur la situation ; la publication du plan du commandant ; l'attribution des tâches aux forces ; la planification opérationnelle ; l'organisation et le maintien de la coopération de toutes les*

forces et de toutes les formes de soutien ». (Alberts & Hayes, 2006, p.73; Cooper, 2019, p80)[7]. Dans cette définition très axée « armée », le C2 n'est pas présenté comme un système ou une organisation mais bien comme un concept ayant une dimension technique (« *l'acquisition, la fusion, l'examen, la représentation, l'analyse et l'évaluation continus des informations sur la situation »*) et une dimension organisationnel et humain (« *la publication du plan du commandant ; l'attribution des tâches aux forces ; la planification opérationnelle ; l'organisation et le maintien de la coopération de toutes les forces et de toutes les formes de soutien »).*

Au sens strict du terme, un C2 n'est pas un centre physique (centre de commandement, centre de détection et de contrôle…) figé dans le temps et l'espace mais un concept évolutif adapté au contexte (civil ou militaire) dans lequel des « moyens », matériels et humains, sont déployés afin d'atteindre des buts divers. Le concept C2 réfère donc à un système sociotechnique pouvant prendre forme dans tout type de situation, ce qui rejoint les propos d'Alberts et Hayes « *Le commandement et le contrôle sont des concepts fractals. Ils peuvent être appliqués à tous les sous-ensembles d'une entreprise, aux fonctions exercées, aux niveaux des organisations, à l'objet de l'activité, qu'il soit stratégique ou tactique. L'appartenance à ces fractales peut se chevaucher avec des entités individuelles et des groupes appartenant à plusieurs fractales de façon dynamique. »* (Alberts & Hayes, 2006, p.9)[8]**.**

Dans le domaine militaire, afin d'intégrer les nouvelles technologies et de répondre au mieux à la complexité des nouvelles missions, le concept de C2 a évolué. Au cours du temps, le C2 est passé, de manière non chronologique, au stade de C2ISR (command and control, intelligence, surveillance and reconnaissance), C3 (consultation command and control), C4 (command, control, communications and computers) (NATO, 2010), C4ISR (command, control, communications, computers, Intelligence, surveillance and reconnaissance) (Department of Defense, 1997). Cependant, ces différents stades ne représentent pas une évolution conceptuelle du C2, qui reste toujours une organisation de réponse à une crise, mais une évolution opératoire et instrumentale (Claverie & Desclaux, 2016). Dans le domaine des gestions de crises civiles, le concept de C2 est également utilisé mais sous d'autres appellations ; pour l'organisation de la réponse de sécurité civile (ORSEC) par exemple, la crise est gérée par l'activation d'une chaine de commandement et d'un Centre Opérationnel Départemental (COD) (Direction de la défense et de la sécurité civile, 2006). La réponse à une crise sanitaire est quant à elle effectuée par la mobilisation d'un centre opérationnel de régulation et de réponse aux urgences sanitaires et sociales (CORRUSS) (Ministère des Solidarités et de la Santé, 2020). Ainsi, la différence d'utilisation du C2 dans les gestions de crises civiles et militaires réside dans une différence d'appellation et de moyens mis en œuvre, et non dans une différence au niveau conceptuelle. La finalité de cette thèse étant l'étude de la RCPair qui est un moyen technique qui

[7] « the functions of commanders, staffs, and other Command and Control bodies in maintaining the combat readiness of their forces, preparing operations, and directing troops in the performance of their tasks. The concept embraces the continuous acquisition, fusion, review, representation, analysis and assessment of information on the situation; issuing the commander's plan; tasking of forces; operational planning; organizing and maintaining cooperation by all forces and all forms of supports » (David S. Alberts & Hayes, 2006, p.73; Cooper, 2019, p80).

[8] « *Command and Control are fractal concepts. They can be applied to all subsets of an enterprise; to the functions performed; to the levels of the organizations; to the focus of the activity, whether strategic or tactical. Membership in these fractals may overlap with individual entities and groups belonging to multiple fractals dynamically. »* (David S. Alberts & Hayes, 2006, p.9)**.**

sera mis en œuvre dans les C2air, il est proposé ici de n'étudier que les fondements théoriques du C2 (C2air) et non pas toutes les déclinaisons possibles (C2ISR, C3, C4, C4ISR…).

Comme tout concept théorique, le C2 présente des aspects stables et des aspects variables. La dimension stable du concept de C2 peut être considérée comme son « fondement opérationnel » alors que ses aspects variables pourraient correspondre aux différents « moyens » mis en œuvre. En d'autres termes la dimension stable pourrait répondre au « pourquoi » (pourquoi dans telle situation avons-nous besoin de mettre en place un C2?) quand les aspects variables répondraient au « comment » (comment organiser le C2 afin de répondre à une situation donnée ?)

A. Eléments fondamentaux du concept de C2

Le fondement opérationnel du concept de C2 est de permettre aux opérateurs de réaliser des missions aux travers d'actions de commandement et d'actions de conduite (*control* en anglais). Au sens de l'OTAN, le commandement est défini comme « *L'autorité conférée à un membre des forces armées pour la direction, la coordination et le contrôle des forces militaires.* »[9] et est utilisé « *Pour dominer une zone ou une situation* »[10] (NATO, 2019). Le *control* quant à lui est définit comme « *L'autorité exercée par un commandant sur une partie des activités d'organisations subordonnées, ou d'autres organisations qui ne sont pas normalement sous son commandement, qui englobe la responsabilité de l'exécution des ordres ou des directives* »[11] et est utilisé pour « *Exercer une influence sur une entité, un processus, un objet ou une zone pour établir, maintenir ou prévenir une situation ou un événement spécifique.* »[12] (NATO, 2019).

Les définitions indiquent clairement que la conduite (*control*) fait partie intégrante du commandement et que le rôle fondamental (la mission) du C2 est d'exercer différentes actions sur des zones, des situations ou des objets, afin de prévenir ou maintenir une situation ou un événement spécifique. Le centre du concept de C2 est donc de donner du sens à une situation, d'anticiper les différentes évolutions possibles de cette situation et d'agir sur cette situation afin de la mener à un état souhaité (*Cf.* Figure 6).

[9] « The authority vested in a member of the armed forces for the direction, coordination, and control of military forces. » (NATO, 2019)

[10] « To dominate an area or situation. » (NATO, 2019)

[11] « The authority exercised by a commander over part of the activities of subordinate organizations, or other organizations not normally under his command, that encompasses the responsibility for implementing orders or directives » (NATO, 2019)

[12] « To exert influence over an entity, process, object or area to establish, maintain or prevent a specific situation or event. »(NATO, 2019)

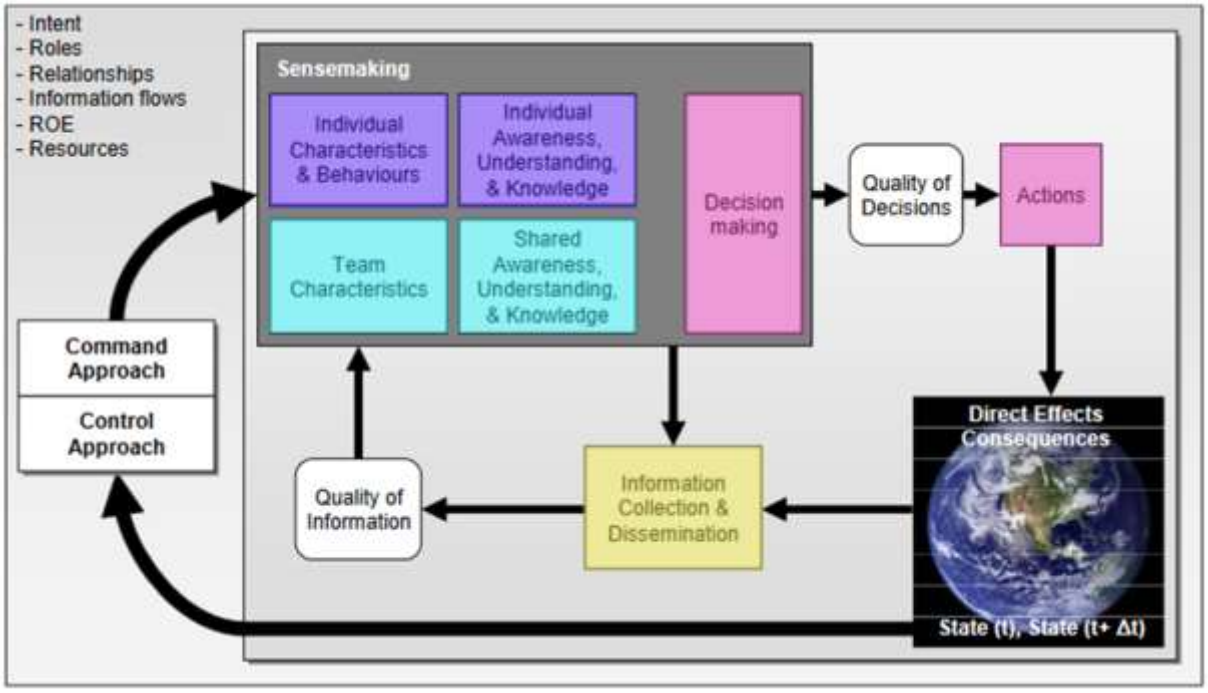


Figure 6 : Représentation conceptuelle du fondement opérationnel des C2 provenant de « SAS-050 Exploring new command and control concepts and capabilities » (NATO, 2006).
Le rôle des C2 est de donner du sens à une situation afin de prendre des décisions permettant de faire évoluer cette situation vers un état souhaité. Pour cela, les opérateurs des C2 reçoivent des informations sur l'état de la situation, analysent collectivement et personnellement ces informations et prennent des décisions sur la base de ces analyses. Les décisions mènent à des actions qui modifient la situation ce qui actionne un nouveau cycle. Ceci renvoie d'ailleurs au concept de boucle OODA (pour « Observe, Orient, Decide and Act »[13]) qui est actuellement étudié dans les approches C2 (Brehmer, 2005)

Comme le montre la figure 6, afin de donner du sens à une situation le C2 doit avoir, *a minima*, trois composantes :

- Une situation ;
- Des opérateurs de traitement permettant de prendre des décisions ;
- Des informations renseignant sur l'état de la situation.

Conceptuellement, aucune discrétisation n'est faite sur la nature, humaine ou matérielle, des opérateurs de traitements. Quelle que soit la nature de l'opérateur, pour être intégré dans un C2, il doit avoir des caractéristiques et des comportements qui lui sont propres (une spécialité, une zone d'expertise, des outils…) (en violet sur la figure 6). En se basant sur les informations disponibles, les caractéristiques et les comportements de l'opérateur vont lui permettre d'avoir une compréhension et des connaissances sur la situation qui lui sont propres et qui sont donc uniques au sein du C2 (en violet sur la figure 6). Chaque opérateur apporte au collectif (l'ensemble des opérateurs présents dans le C2) ses connaissances et compétences spécifiques afin que le collectif puisse former, sur la base des informations disponibles, une compréhension et une connaissance commune de la situation (en bleu sur la figure 6).

[13] Traduit ici par « Observer, orienter, décider et agir »

Dans les C2, c'est donc la pluridisciplinarité et les différences présentes entre les opérateurs qui vont permettre de donner un « sens unique » à une situation et ainsi de prendre une décision sur d'éventuelles actions à mener afin de faire évoluer cette situation (en rose sur la figure 6). Ainsi, les caractéristiques propres à chaque opérateur donneront au C2 une caractéristique d'équipe unique qui mènera à une prise de décision et à des actions uniques. Conceptuellement, les conséquences et les actions prises dans un C2 sont donc fonction des opérateurs présents dans les C2. Les actions effectuées par les opérateurs du C2 ont pour but, de modifier l'état de la situation. Des informations, portant sur le nouvel état de la situation (en jaune sur la figure 6) sont alors recueillies par les opérateurs afin de donner du sens au nouvel état de la situation.

B. Eléments contextuels du concept de C2

Afin de s'adapter aux nouvelles missions et situations, le C2 a théoriquement évolué au cours du temps, que ce soit en terme d'interactions entre les différents individus qui le composent, qu'en terme d'organisation. Ce changement théorique est lié tant à une nécessité d'adaptation du C2 à l'évolution de la complexité des conflits qu'à la possibilité de cette adaptation due notamment à l'augmentation de la rapidité et de la fiabilité des TIC. Cette évolution a amené le C2 à prendre différentes formes (*Cf.* Figure 7) (dans cette partie, les termes anglais correspondent à des « concepts » et ne sont pas traduits).

- Le *conflicted C2*
- Le *de-conflicted* C2
- Le *coordinated* C2
- Le *colaborative* C2
- Le *Edge* C2

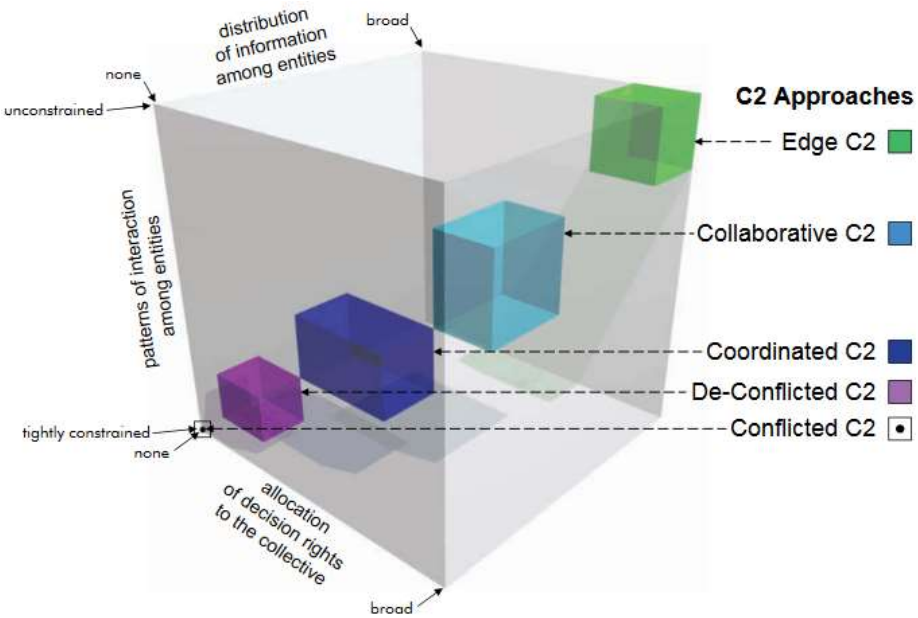


Figure 7 : Figure provenant du rapport « NATO NEC C2 Maturity Model » (Alberts, Huber, & Moffat, 2010).

Cette figure montre l'évolution du concept de C2, de son stade le plus « basique » (le *Conflicted C2*) à son stade le plus « avancé » (l'*Edge C2*). L'évolution du concept de C2 s'est faite tant en terme de transfert d'information qu'en terme d'organisation

Comme le montre la figure 7, deux grandes « révolutions franches » et une « évolution lente » ont eu lieu dans le concept de C2. La première « révolution franche » a portée sur le nombre d'interaction et a fait passer le concept du stade de c*onflicted C2* à celui de *de-conflicted C2.* Au stade de *conflicted C2* toutes les interactions sont effectuées entre les membres d'une même « entité » (une « entité » correspond ici à un regroupement de moyens matériels et humains comme un centre de commandement par exemple), aucune interaction n'est présente entre les membres « d'entités » différentes.

Au stade de *de-conflicted C2* la majorité des interactions sont effectuées entre des membres d'une même « entité » mais des interactions minimales et épisodiques sont présentes entre les membres « d'entités » différentes. A partir de ce stade, une « évolution lente », portant sur le nombre d'interaction entre les différents individus et les différentes entités, a eu lieu et a fait passer le concept du stade de *de-conflicted C2* à celui de *coordinated C2* puis à celui de *collaborative C2*.

Au stade de *coordinated C2* les interactions entre les opérateurs deviennent plus fréquentes et des « entités » différentes interagissent ensemble pour effectuer des tâches communes. Au stade de *collaborative C2,* les « entités » collaborent afin de développer un plan unique permettant de réaliser des tâches communes. L'apparition de ces 3 stades a été permise par l'augmentation des possibilités de communications due à l'avènement des TIC.

Enfin, la deuxième « révolution franche » a porté sur le facteur organisationnel des C2. Dans cette dernière évolution (qui est actuellement en cours) le concept est passé du stade de *collaborative C2* à celui d'*Edge C2*. En terme de nombre de communications ces deux stades sont relativement similaires, cependant, dans l'approche *Edge C2*, la coopération et la coordination entre les individus et entre les « entités » ne sont plus dictées par des normes mais sont le résultat d'une auto-synchronisation (*Cf.* Figure 8).

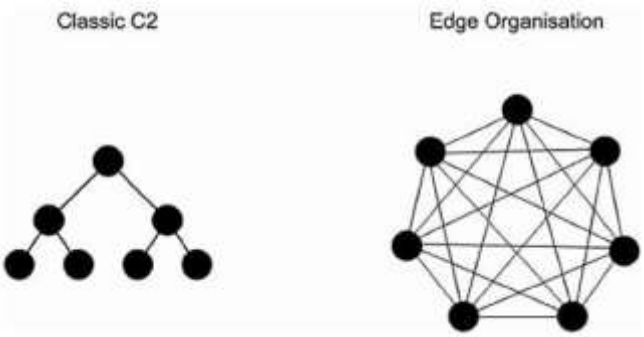


Figure 8 : Figure provenant du livre « Command and Control: The Sociotechnical Perspective » (Walker, stanton, & Jenkins, 2017) .
A gauche de cette figure est représentée l'organisation « classique » des liens présents entre les différents opérateurs ou les différentes entités, qui était, à l'origine, de type pyramidale. L'avènement des TIC a permis d'accroitre le nombre de liens entre les différents acteurs et les différentes entités et a peu à peu changé l'organisation en une organisation auto-organisatrice de type « grappe ». Actuellement cette organisation en « grappe » est peu à peu mise en place.

Aujourd'hui, de plus en plus d'équipes utilisant le concept de C2 tendent à vouloir mettre en place une organisation de type *Edge C2* qui parait être la plus adaptée aux caractéristiques des conflits asymétriques modernes. Cependant, le *Edge C2* est la forme du C2 la plus adaptée uniquement aux conflits et situations complexes nécessitant, pour être traités, la mise en commun d'un grand nombre d'informations, de ressources, de savoirs faires et de moyens. Dans les C2 civils et militaires les différents stades (du *conflicted C2* au *Edge C2*) sont en réalité utilisés et l'utilisation de l'un ou l'autre de ces stades dépend uniquement de la complexité de la situation. Schématiquement, pour traiter une situation « routinière » le stade du *conflicted C2* est majoritairement employé mais lorsque la situation évolue le stade du C2 utilisé évolue également afin de s'adapter à l'augmentation de la complexité (Farrell, Jobidon, & Banbury, 2012). Le C2 est donc un concept agile dont l'agilité dépend de la complexité de la situation (*Cf.* Figure 9).

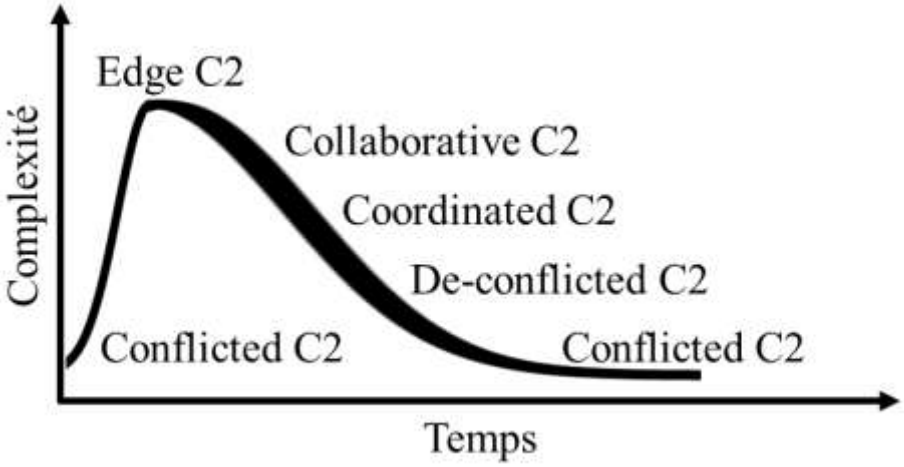


Figure 9 : Représentation de l'agilité du C2 au cours d'une mission (le temps représente la durée de la mission).
Image inspirée de celle présentée dans « Organizational Agility Olympic Event Case Studies » (Farrell et al., 2012)

Analyse conceptuelle de l'organisation possible des C2 de l'AA

Etant donné que la RCPair sera un outil de l'AA et sera donc probablement mis dans différents centres de l'AA il est proposé ici d'étudier l'agilité des C2 à travers différents exemples tirés des missions effectuées par l'AA.

Pour assurer ses missions de contrôle de l'espace aérien l'AA dispose, sur le territoire national, de 4 CDC (*Cf.* Figure 10). Sur ces 4 CDC, 3 sont opérationnels (les CDC de Cinq-Mars-la-Pile, de Mont-de-Marsan et de Lyon Mont Verdun) et 1 est en sommeil mais pourrait être redémarré (le CDC de Drachenbronn). Chaque CDC effectue le contrôle de l'espace aérien d'une zone particulière de la France. Ainsi le CDC de Cinq-Mars-la-Pile est chargé du contrôle de l'espace aérien Nord-Ouest et du contrôle de l'espace aérien Nord-Est (initialement effectué par le CDC de Drachenbronn). Le CDC de Mont-de-Marsan est chargé du contrôle de l'espace aérien Sud-Ouest et le CDC de Lyon-Mont-Verdun est chargé du contrôle de l'espace aérien Sud-Est.

Un CDC militaire est généralement composé de plusieurs travées divisées en plusieurs postes. Les opérateurs de chaque poste ont des représentations de la situation et des rôles différents les uns des autres. Chaque opérateur remonte les informations importantes au chef de travée qui transmet ensuite les informations au chef du CDC. Lorsqu'un aéronef pénètre ou prend naissance dans la zone

de responsabilité du CDC un opérateur lui associe un comportement (normal, anormal ou dangereux). Lorsqu'un appareil a un comportement non conforme (pénétration dans une zone interdite, déviation du plan de vol) (*Cf.* Figure 10), les différents opérateurs des CDC doivent analyser et comprendre la situation afin de replacer l'aéronef dans la légalité. Dans la grande majorité des cas, grâce à une coordination intra CDC la situation retrouve sa normalité. Pour effectuer ce type de missions habituelles les opérateurs du CDC utilisent donc une approche de type *Conflicted C2* ou *De-conflicted C2.*

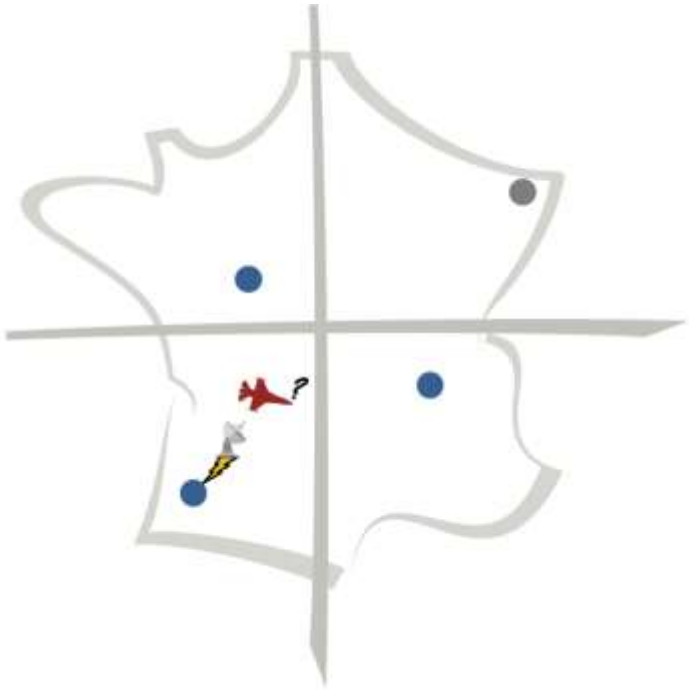


Figure 10 : Exemple de mission classique effectuée par les CDC.
Dans ce type de mission, un aéronef (en rouge sur la figure) a un comportement non conforme (l'aéronef dévie de son plan de vol par exemple). Le radar, relié au CDC (éclair jaune sur la figure), transmet les informations aux opérateurs. Les opérateurs présents dans le CDC et les membres de l'aéronef collaborent ensemble afin de comprendre la situation et d'éviter un incident plus grave. L'organisation utilisée dans ce type de mission pourrait correspondre à une approche de type *Conflicted C2* ou *De-conflicted C2.*

Dans certains cas, les opérateurs des CDC ne peuvent pas gérer seuls la situation (aéronef qui ne coopère pas, problème de communication…) et le dispositif Posture Permanente de Sureté (PPS) est déclenché. Ceci peut par exemple être le cas pour un aéronef tentant de pénétrer dans une zone interdite (*Cf.* Figure 11). Lorsqu'un opérateur du CDC constate qu'un appareil se dirige vers une zone interdite à un niveau inférieur au plafond imposé il prévient son chef de travée pour lui faire part de la situation. Le chef de travée est alors en charge d'appeler le CNOA. Une classification particulière est alors accordée à l'aéronef ayant un comportement anormal. En fonction du déroulé de l'opération l'appareil changera sa route et sortira de la zone en question ; sinon, sur ordre du CNOA, la Permanence Opérationnelle (PO) peut être déclenchée pour intercepter l'appareil en question, comprendre ses intentions (détresse, panne, méconnaissance de la zone, pénétration volontaire…) et agir s'il le faut. L'intervention de la PO peut aller jusqu'à la destruction de cet appareil selon les Mesures Actives de Sûreté Aérienne et sur décision de la haute autorité de défense aérienne. Pour effectuer ce type de mission une communication active se met en place entre les opérateurs de

différents centres (CDC et CNOA) qui collaborent afin de réaliser une tâche donnée, ce qui ressemble donc à une approche de type *Coordinated C2* ou *Collaborative C2.*

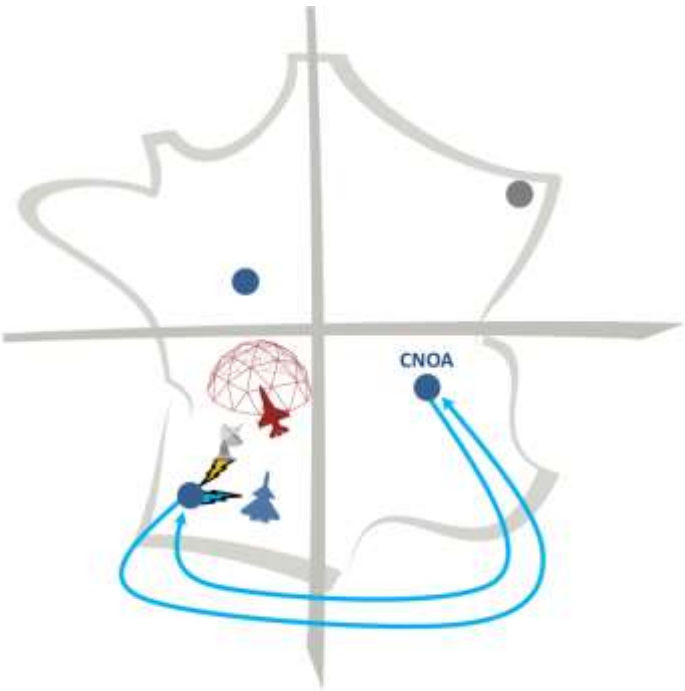


Figure 11 : Exemple de mission posture permanente de sureté (pps).
Contrairement aux missions classiques (*Cf.* Figure 10), dans certains cas les opérateurs du CDC ne parviennent pas à améliorer la situation et doivent communiquer avec le centre national des opérations aériennes (CNOA) afin de faire décoller la permanence opérationnelle (PO). Cette figure représente le cas d'un aéronef (en rouge sur la figure) essayant d'effectuer le survol d'une zone interdite comme une centrale nucléaire par exemple (dôme rouge sur la figure). L'aéronef ne répondant pas aux demandes du CDC, la PO (le *Rafale* en bleu sur l'image) doit décoller afin de rendre compte de la situation. Seulement le CDC n'a pas le droit de donner l'ordre au *Rafale* de décoller et doit demander au CNOA (situé à Lyon) de faire décoller la PO. Les opérateurs du CNOA prennent connaissance de la situation et agissent en collaboration avec les membres du CDC. L'organisation utilisée dans ce type de mission pourrait correspondre à une approche de type de type *Coordinated C2* ou *Collaborative C2.*

Les deux exemples ci-dessus permettent d'observer l'agilité du C2. Dans sa mission de « routine » le CDC (ici celui de Mont de Marsan) contrôle l'espace aérien qui lui est dédiée (ici le sud-ouest). Si les opérateurs du CDC ne détectent aucun comportement « déviant » de la part d'aéronefs présents dans la zone alors le CDC se trouve dans une organisation ressemblant à un *conflicted C2 (Cf.* Figure 12). Si un comportement déviant est détecté (par exemple un aéronef déviant de son plan de vol) alors le CDC devra communiquer avec l'aéronef en question afin de retrouver une situation normale, le CDC passe alors dans une organisation ressemblant à un *De-conflicted C2 (Cf.* Figure 12). Si l'aéronef ne répond pas aux sollicitations du CDC et continue à dévier de son plan de vol pour, par exemple, rentrer dans une zone interdite le CDC devra communiquer avec le CNOA afin de faire décoller la PO. Le CDC passe alors dans une organisation ressemblant à du *collaborative C2* ou *coopérative C2* (*Cf.* Figure 12). Enfin, si, par exemple, la zone interdite se trouve à la limite entre deux espaces de contrôle (la zone interdite se trouve entre l'espace controlé par Mont de Marsan et celui contrôlé par saint Mars la Pile) (non présenté dans les exemples ci-dessus) alors deux CDC reçoivent et transmettent des informations sur l'aéronef et le CNOA fait décoller la PO. Le CDC passe alors dans une organisation ressemblant à du *Edge C2* (*Cf.* Figure 12).

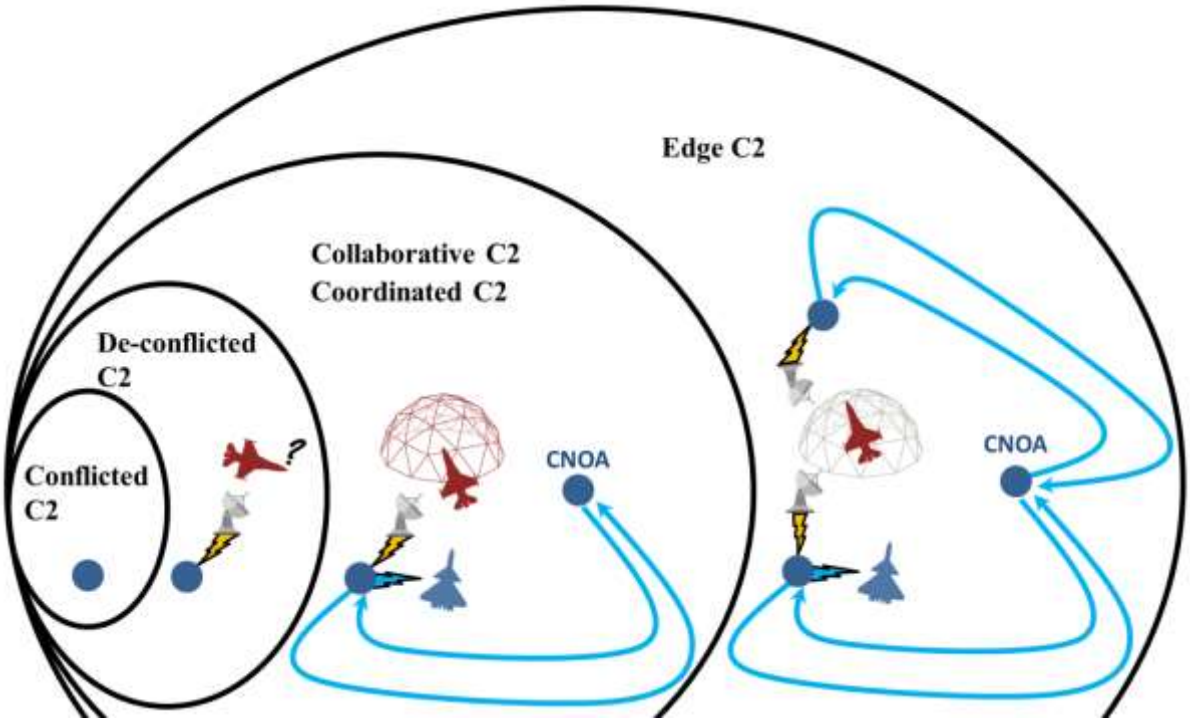


Figure 12 : Agilité du C2 sur des missions de l'AA. En mission normale le CDC est au stade de *conflicted C2*, au plus la situation devient complexe au plus l'organisation du C2 se déplace vers le stade de *Edge C2.*

Ces différents exemples montrent que l'organisation du C2 peut découler d'une agilité du C2. Cependant, le choix de l'organisation « de base » est dépendant de la complexité de la mission et ne correspond donc pas toujours au *conflicted C2*. Par exemple, pour la protection d'évènements importants comme le 14 Juillet ou le salon du Bourget un Dispositif Particulier de Sureté Aérienne (ou DPSA) est utilisé (*Cf.* Figure 13)(Medeiros, 2019). L'objectif de ce DPSA est de quadriller entièrement la zone de l'évènement avec des moyens sols (défense sol air, guets à vue…) des moyens aériens de surveillance (drone Reaper…), des moyens aériens d'interception (hélicoptères, *Rafale…*) des moyens aériens de commandement et de contrôle (E-3F) mais également le CNOA.

Dans les DPSA tous ces moyens matériels et humains collaborent afin de prévenir une crise. Pour ce faire, un réseau de communication est déployé permettant, en temps réel, aux différents membres du dispositif d'informer et de récupérer de l'information transmise par d'autres membres. Pour le DPSA le premier ministre est garant de la décision à prendre en cas de problème mais les moyens sont déployés par le CNOA. Ce type d'organisation, en maillage ou grappe, mise en place pour réaliser un objectif donné peut correspondre à une organisation de type *Edge C2.* Cet exemple montre que dans les DPSA le *Edge C2* ne provient pas d'une agilité du C2 mais d'une nécessité provenant de la complexité de la situation.

Figure 13 : Exemple de Mission DPSA (Medeiros, 2019).
Ces missions sont mises en place dans le cadre de la protection de grands évènements. Différentes sortes d'aéronefs comme des chasseurs, des hélicoptères, des drones ou encore l'E-3F (avion radar/C2 AWACS) sont déployés pour quadriller une zone géographique donnée. Tous ces aéronefs collaborent avec le CNOA en partageant des informations sur le réseau. En cas d'incident la décision d'agir serait prise par le premier ministre et les informations utilisées pour prendre les décisions ne proviendraient pas d'un processus pyramidal mais d'un processus en grappe (chaque entité, quelle que soit sa hiérarchie participe à l'élaboration des informations nécessaires à la prise de décision). L'organisation utilisée dans ce type de mission pourrait correspondre à une approche de type de type *Edge C2.*

7. La RCPair dans les C2

Le C2 est donc un concept qui a pour fonction principale de prendre des décisions permettant de réaliser une mission donnée. Les différentes prises de décisions effectuées par les membres du C2 permettent d'agir sur une situation afin d'en modifier l'état. La mission des C2 de l'AA est de contrôler l'espace aérien francais. Actuellement, afin de permettre cette mission, les C2 de l'AA sont formés de différents opérationnels (contrôleurs aériens, mécaniciens spécialisés en systèmes d'informations et de communications…) interagissant ensemble afin de donner du sens à la situation air. Cependant, l'arrivée de la composante cyber (par le biais de la RCPair) dans les C2 de l'AA pourrait modifier l'organisation voire le comportement des membres actuels des C2 de l'AA. Afin de vérifier cela il parait intéressant d'analyser la représentation conceptuelle du fondement opérationnel des C2 en y ajoutant les composantes de cette RCPair.

La RCPair, en tant que système, aura des caractéristiques et des comportements qui lui seront propres et qui permettront de mettre en place une représentation et une compréhension de la situation cyber de la situation (en violet sur la figure 14). Cette représentation et ces compréhensions basées sur des données cyber seront ensuite mises en commun avec les représentations obtenues par les opérateurs airs (humains ou matériels) afin de créer une représentation partagée de la situation (en bleu sur la figure 14). Pour l'AA cette représentation partagée aura donc une composante air « classique » (des informations provenant de la situation air) mais également une

composante cyber (des informations provenant de la situation cyber). Sur la base de cette représentation partagée, des décisions seront prises ce qui mènera à des actions qui modifieront la situation. La RCPair récupèrera les informations cyber recueillies sur le nouvel état de la situation et un nouveau cycle commencera.

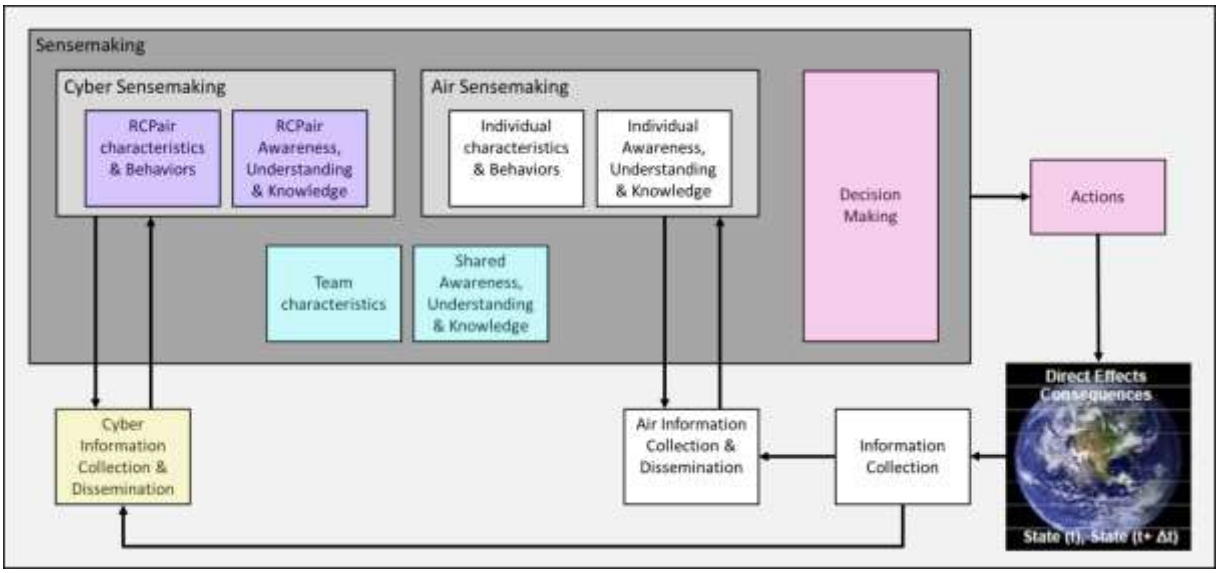


Figure 14 : Ajout de la composante RCPair à la représentation conceptuelle des C2

Conceptuellement, l'ajout de la composante cyber ne modifie donc pas le fondement opérationnel du C2 et peut être vue uniquement comme un ajout de fonctionnalité. Dans cette approche, les opérateurs air (contrôleurs aériens) sont toujours en charge de donner du sens à la situation air (comprendre et anticiper les différents évènements air) alors que les opérateurs cyber sont en charge de donner du sens à la situation cyber (comprendre et anticiper les différents évènements cyber). Une collaboration entre les opérateurs air et cyber permettent d'obtenir une compréhension globale de la situation afin de prendre des décisions. Seulement, l'ajout de cette composante cyber entraine un bouleversement du C2 au niveau de la collecte, du traitement et de l'analyse de l'information.

En effet, le rôle de cette RCPair sera de donner du sens à la crise cyber. Or, une cyber attaque « *consiste en toute action entreprise pour porter atteinte aux fonctions d'un réseau informatique à des fins politiques ou de sécurité nationale* » (Hathaway et al., 2011)[14] et peut donc intervenir sous différentes formes allant de la surcharge réseau à la falsification de l'information. La détection d'une anomalie cyber sur les informations collectées devrait donc entrainer une remise en cause de l'intégralité des informations collectées (ces informations étant le point de départ de la mise en place de la conscience de situation). Le schéma présenté à la figure 14 serait donc erroné, car, en rajoutant de l'incertitude aux informations collectées afin de mettre en place la situation air, la cyber conscience de situation impacterait la conscience de situation globale mais également la conscience de situation air (*Cf.* Figure 15) et par voie de conséquence la prise de décision et les actions qui en découleraient.

[14] « *consists of any action taken to undermine the functions of a computer network for a political or national security purpose* » (Hathaway et al., 2011)

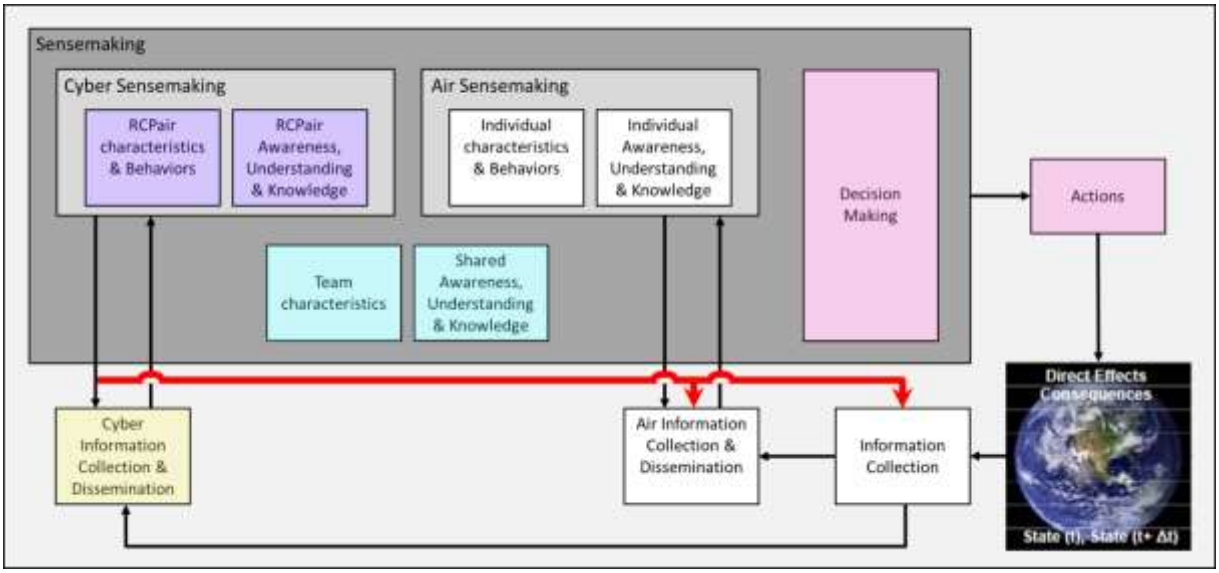


Figure 15 : Impact de l'arrivée de la composante cyber (par le biais de la RCPair) dans les C2 de l'AA.
En détectant un possible problème cyber la RCPair pourrait entrainer une remise en cause de la validité de toutes les informations utilisées par les différents opérateurs du C2 (flèche rouge sur le schéma). Dès lors, la RCPair pourrait avoir un impact sur la conscience de situation globale du C2 et pourrait modifier la prise de décision, et, par voie de conséquence, les actions menées par les opérateurs du C2.

Un nouveau problème semble donc apparaitre : le décideur cyber (utilisant la RCPair) et le décideur air pourraient avoir des informations contradictoires, basées sur des données incertaines provenant de sources différentes (les informations air proviennent directement de capteurs tel que les radars par exemple alors que les informations cyber proviennent d'une fusion de données pouvant être multifactorielles). Ces opérateurs devraient se transmettre ces différentes informations contradictoires afin de prendre des décisions (*Cf.* Figure 16). Cette contradiction présente entre les différentes informations reçues devraient entrainer une augmentation de la complexité, et, par voie de conséquence, une évolution du type de C2 utilisé. Dès lors, il est fort possible qu'en cas d'attaque cyber détectée une organisation de type *Edge C2* soit mise en place rapidement entrainant une réorganisation de la chaine de responsabilité ainsi qu'une augmentation des communications et des liens interpersonnels.

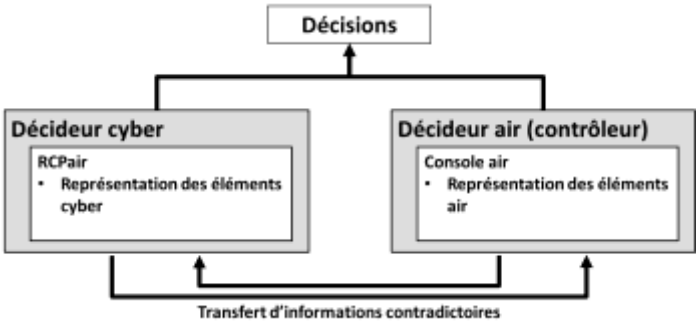


Figure 16 : Le décideur cyber et le décideur air doivent permettre de prendre des décisions sur la base d'informations pouvant être contradictoires.

Une attaque cyber détectée par un CDC, effectuant une mission routinière, organisé en *conflicted C2* entrainerait donc un passage rapide d'une organisation pyramidale a une organisation en grappe. Dans le cas d'une attaque cyber, les opérateurs à l'intérieur d'une « entité » (un CDC par exemple) devraient donc collaborer entre eux mais également collaborer avec des opérateurs d'une autre « entité » (le CNOA par exemple) pour réaliser une tâche donnée. Dans cette organisation *Edge C2* plusieurs types de liens pourraient être mis en jeu. Les opérateurs présents dans la même « entité » travaillant ensemble tous les jours auront appris à se connaitre alors que les opérateurs de deux « entités » différentes n'ayant pas l'habitude de travailler ensemble pourraient potentiellement ne pas se connaitre. De manière similaire aux premières cyberattaques qui ont entrainé une détérioration de la confiance qu'ont les opérationnels dans leurs systèmes informatisés un tel bouleversement organisationnel pourrait entrainer des problématiques portant sur les différents types de confiance mais plus particulièrement sur la confiance interpersonnelle au niveau des différentes composantes des C2air (caractéristiques d'équipes et caractéristiques de l'information) qui pourraient impacter les comportements des opérateurs. Cette thèse a donc pour objectif de répondre à la problématique suivante :

Quelles sont les conséquences comportementales d'un manque ou d'un excès de confiance interpersonnelle sur les opérateurs travaillants dans la RCPair recevant des données soumises à une forte incertitude

Pour répondre à cette problématique, cette thèse propose d'étudier, dans l'ordre suivant, les conséquences comportementales engendrées par la confiance interpersonnelle et, dans une moindre mesure, par les différents types de confiance pouvant rentrer en jeu dans la RCPair. L'agrégation des données obtenues dans cette analyse du besoin et le schéma conceptuel du C2 permet de mettre en évidence les différentes études qui seront réalisées dans cette thèse (*Cf.* Figure 17)

- Une étude portant sur le rôle du choix du décideur final dans les conséquences d'un manque ou d'un excès de confiance interpersonnelle entre un opérateur air et un opérateur cyber (en violet et en bleu sur la figure 17)
- Une étude portant sur les conséquences d'un manque ou d'un excès de confiance dans la machine sur le comportement de l'opérateur cyber (en jaune sur la figure 17)
- Une étude portant sur les conséquences de la dualité entre la confiance interpersonnelle et la confiance en soi sur le comportement de l'opérateur cyber (en violet sur figure 17)
- Le lien entre la confiance interpersonnelle, la situation et la prise de décision (en rose sur la figure 17)

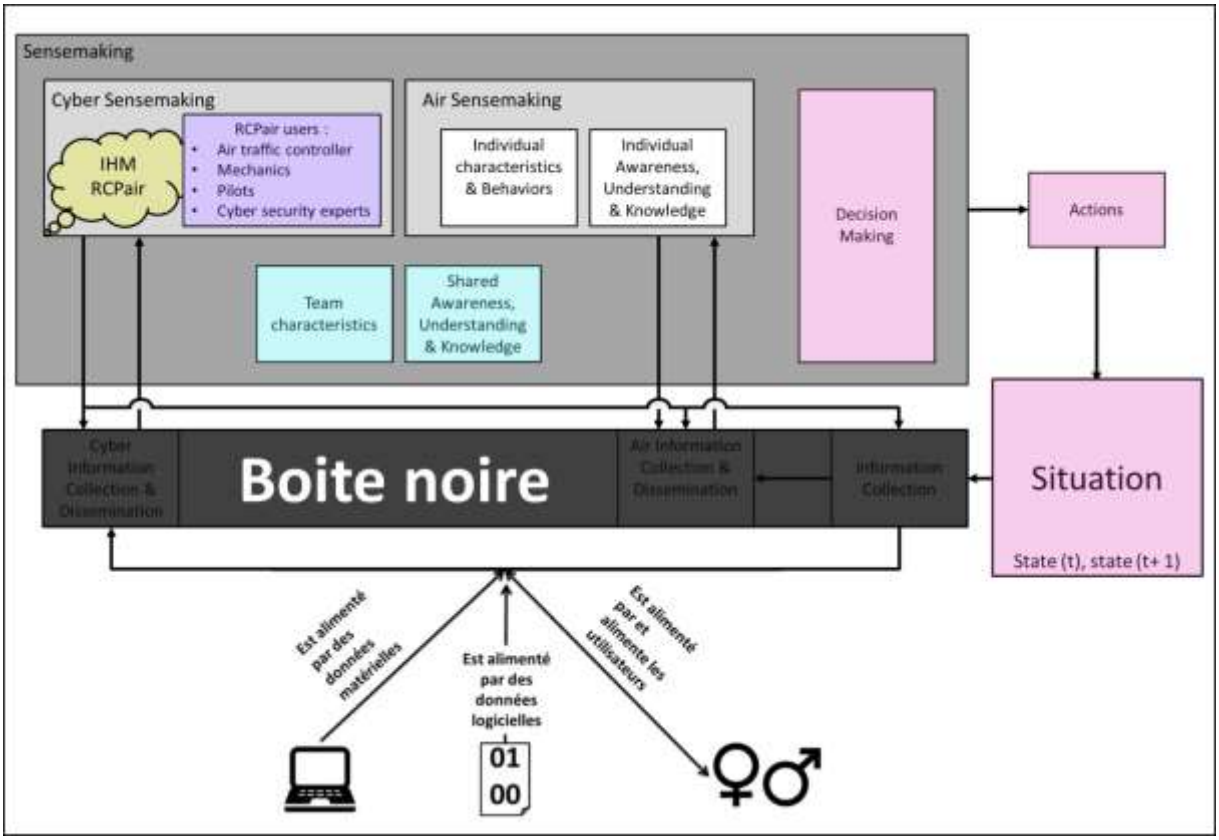


Figure 17 : Schéma conceptuel des C2air avec ajout de la composante RCPair.
Dans ce schéma sont représentées toutes les études effectuées durant cette thèse à savoir, une étude portant sur le choix du décideur final de la RCPair (en violet sur cette figure) et sur le comportement engendré par différents niveaux de confiance interpersonnelle (CI) (en bleu sur la figure), une étude portant sur la confiance dans la machine (en jaune sur la figure), une étude portant sur le rôle de la confiance en soi de l'opérateur dans ses comportements (en violet) et une étude portant sur le rôle de la situation dans la prise de décision (en rose sur cette figure)

Point clés

Au début des années 2000, l'augmentation des nouvelles technologies de l'information et de la communication a amené les Armées, et notamment l'Armée de l'air a fortement se digitaliser. L'accroissement du nombre de systèmes interconnectés a entrainé un accroissement du nombre de cyber-menaces et de cyber-attaques. Les premières cyberattaques survenues sur les infrastructures civiles puis militaires ont amené les Etats à remettre en cause leur gestion de la cybersécurité. La stratégie de l'état Français en matière de cybersécurité consiste en la mise en place des centres de conduite des opérations dédiés au cyber ; dans ces centres la collecte et l'analyse des informations doit permettre aux opérateurs et décideurs de donner du sens à une crise cyber.

Pour l'Armée de l'Air Française la gestion de la cybersécurité des opérations aériennes se réalisera via un outil de représentation de l'état cyber du système nommé RCPair. Cette RCPair n'est encore pas définie en termes de besoin matériel et humain. Toutefois il semble maintenant fort probable qu'elle sera déployée dans des centres de types C2. Selon les directives des différents Etats européens, les nouveaux C2 devraient être pensés comme devant être résilients ; cependant, une analyse bibliométrique montre que la communauté scientifique semble délaisser les facteurs organisationnels et humains de la cyber-résilience au profit des recherches plus techniques. Dans le domaine cyber, constitué des différents champs de recherches portant sur la cyber-sécurité, les cyber-attaques, les cyber-menaces, les cyber-guerres, les cyber-crimes ou encore le cyber-terrorisme, cette approche technique peut paraitre sensée. Toutefois, dans l'étude d'un système tel que la RCPair qui sera probablement déployé dans un système sociotechnique complexe, à savoir les apparait incontournable.

Le C2 est un concept évolutif adapté au contexte (civil ou militaire) dans lequel des moyens, matériels et humains, sont déployés afin de donner du sens et de résoudre a des crises diverses. Une organisation de type C2 se met en place autour de trois composantes :

- Une mission (ou situation)
- Des opérateurs
- Des flux informationnels et décisionnels

Dans sa forme conceptuelle, un C2 est composé d'opérateurs humains et matériels qui reçoivent traitent et analysent des informations sur l'état d'une situation donnée et prennent différentes décisions permettant de faire évoluer cette situation vers l'atteinte d'un objectif et la réalisation de la mission. Parallèlement à l'apport de nouvelles

informations essentielles à la mission, la composante cyber apportée par la RCPair entrainera probablement de l'ajout d'incertitude quant à la véracité ou la fiabilité des informations reçues par les opérateurs des C2 de l'AA ce qui pourrait impacter le comportement des opérateurs. Cette thèse propose de répondre à la problématique suivante :

Quelles sont les conséquences comportementales d'un manque ou d'un excès de confiance interpersonnelle sur les opérateurs travaillants dans la RCPair recevant des données soumises à une forte incertitude ?

2 La confiance

Résumé du chapitre

Objectif : Identifier les éléments ou conditions qui influent sur la confiance d'un opérateur dans une situation donnée, ainsi que sur son comportement.

Démarche : Afin de répondre à la problématique de cette thèse, il est nécessaire de réaliser un état de l'art des connaissances actuelles des différentes littératures étudiant la confiance. La notion de confiance étant étudiée dans de nombreux domaines, les différentes définitions proposées et les éléments qui lui sont associés seront mises en perspectives dans un premier temps. Puis l'importance de la dimension temporelle sur la mise en place et le maintien de la confiance seront étudiés afin de mettre en place un modèle et de sélectionner les éléments les plus pertinents pour le fonctionnement envisagé de la RCPair.

Conclusion : Plusieurs définitions de la notion de confiance sont adoptées ainsi qu'un modèle permettant d'identifier les éléments utiles à la construction de la confiance et ceux impactés par le niveau de confiance en cohérence avec notre cadre applicatif.

Chapitre 2 : La confiance

1. Introduction

Dans la partie précédente le fait que la mise en place de la RCPair allait probablement entrainer des problématiques liées aux conséquences d'un manque ou d'un excès de confiance interpersonnelle (CI) a été présenté. Afin de répondre à la problématique qui porte sur les conséquences comportementales d'un manque ou d'un excès de CI présent entre les opérateurs travaillants dans la RCPair il est donc nécessaire de définir ce qu'est la CI et quelles sont les conséquences comportementales d'un manque ou d'un excès de CI. Dans cette partie, le mot confiance non suivi des termes « dans la machine » ou « en soi », correspondra à la confiance en général.

2. Définitions et modèles utilisés dans la littérature sur la confiance

A. Généralités et définition utilisée pour la thèse

La confiance est étudiée dans de nombreux domaines tels que la psychologie, la sociologie, le management, le marketing, le comportement organisationnel, l'informatique ou les relations publiques (Watson, 2004). Elle est perçue comme un élément essentiel, ou du moins désirable, pour assurer un bon fonctionnement, tant à l'intérieur d'une organisation qu'entre les organisations. Bien qu'aucune définition ne fasse consensus, les différentes disciplines s'accordent à caractériser la confiance comme étant un lien entre, *a minima*, trois entités distinctes. La première entité correspond à la situation (la tâche à effectuer dans un contexte donné) et les deux autres entités correspondent aux opérateurs (humains ou matériel) qui vont agir sur cette situation. Ces deux opérateurs peuvent être aussi bien deux collaborateurs, qu'un responsable hiérarchique et un membre de son équipe, un employeur et un employé, deux organisations, une personne et une institution ou encore un humain et une machine. Pour qu'il y ait confiance un opérateur (humain ou matériel) a besoin d'un autre opérateur (humain ou matériel) afin de réaliser une tâche donnée, sur une situation donnée, dans un contexte donné (Baier, 1986; Dietz & Den Hartog, 2006; Gambetta, 1988; Hardin, 2004; Karsenty, 2011; Luhmann, 1979; Rousseau, Sitkin, Burt & Camerer, 1998).

Bien que la confiance soit étudiée dans de nombreux domaines, aucune définition consensuelle de ce concept, ni de la manière dont elle doit être mesurée ne semble émerger. Cependant, au-delà des particularités relatives à chaque disciplines (McKnight & Chervany, 2000) certaines constantes semblent apparaitre. La confiance semble être un concept composite (Pinto, Slevin, & English, 2009), multidimensionnel, articulant une dimension affective, une dimension cognitive et une dimension sociale, et qui va dépendre en partie du contexte applicatif retenu (Möllering, Bachmann, & Lee, 2004). Selon la discipline, la confiance peut être définie comme un état psychologique (Rousseau et al., 1998) , une volonté (Mayer, Davis et Schoorman, 1995) ou encore une évaluation de la fiabilité d'autrui fondée sur les interactions sociales et des *a priori* sur des catégories personnes (Pinto et al., 2009; Quéré, 2011).

Dans la littérature sur la confiance, et plus particulièrement dans la littérature sur la CI, la première personne, celle qui fait confiance, est dénommée confiant (« trustor » dans la littérature anglophone). La seconde personne, celle à qui le confiant fait confiance et qui est donc la cible du lien de confiance, est dénommée mandant (« trustee » dans la littérature anglophone). Généralement, le confiant est amené à faire confiance au mandant car il se trouve dans une situation où l'apport de l'autre peut lui amener un gain. Le confiant a donc des attentes vis-à-vis des actions futures du mandant et considère, s'il entre dans cette relation de confiance, que le risque qu'il prend en se fiant à l'autre est moins élevé que celui qu'il prend en agissant ou décidant seul (Karsenty, 2011). Le niveau de confiance présent entre le confiant et le mandant est donc fortement modulé par la situation ce qui implique que différents niveaux de confiance, entre deux individus, peuvent coexister au même moment (X peut avoir un certain niveau de confiance dans Y pour qu'il fasse une action Z mais, au même moment, X peut avoir un autre niveau de confiance dans Y pour qu'il fasse une action W).

L'identification des 3 entités de la confiance (e.g. confiant mandant et situation) est issue des travaux menés par le psychologue Deutsch (Deutsch, 1958) qui définit la confiance comme « *la personne qui fait confiance perçoit qu'elle sera plus mal lotie si elle fait confiance et que sa confiance n'est pas honorée que si elle ne fait pas confiance* »[15] et « *On peut dire qu'une personne a confiance dans la survenance d'un événement si elle s'attend à ce qu'il se produise et si son attente conduit à un comportement qu'elle perçoit comme ayant des conséquences motivationnelles négatives plus importantes si l'attente n'est pas confirmée que des conséquences motivationnelles positives si elle est confirmée* »[16]. Sur la base des travaux de Deutsch (Deutsch, 1958) et Simmel (Simmel, 1950 ; Möllering, 2001) la littérature sur la confiance s'est scindée vers deux champs distincts. Le premier champ de la littérature, portant sur la CI, a étudiée les liens de confiance présents entre deux opérateurs humains. Le deuxième champ de la lttérature, portant sur la confiance dans la machine (CM), a étudiée les liens de confiance présents entre un opérateur humain et un système informatique. Dans la littérature sur la CI, des approches différentes mais complémentaires ont alors été étudiées :

- Les recherches réalisées en sociologie notamment dans l'étude des relations économiques (Lewis & Weigert, 1985; Luhmann, 1968) se sont axées sur le lien entre CI et type de situation (quel est le rôle de la situation dans la mise en place du niveau de CI et quels sont les comportements engendrés par ce niveau de CI selon les situations).

- les différentes études réalisées dans la littérature portant sur le management et les organisations (Costa, Fulmer, & Anderson, 2018; Mayer, Davis, & Schoorman, 1995; Mayer & Gavin, 2005; McAllister, 1995; Burke, Sims, Lazzara, & Salas, 2007) ont axées leurs recherches sur les caractéristiques du mandant et sur les conséquences engendrées par le niveau de CI (quelle sont les caractéristiques propre au mandant qui permettent la mise en place du niveau de CI et quels sont les comportements engendrés par ce niveau de CI).

[15] « the trusting individual perceives that he will be worse off if he trusts and his trust is not fulfilled than if he does not trust. » (Deutsch, 1958)

[16] « An individual may be said to have trust in the occurrence of an event if he expects its occurrence and his expectation leads to behavior which he perceives to have greater negative motivational consequences if the expectation is not confirmed than positive motivational consequences if it is confirmed. » (Deutsch, 1958)

B. Les différentes approches de la CI

a. Approche probabiliste réalisée dans la littérature portant sur les relations économiques

Dans la CI, l'approche probabiliste de la confiance se fonde sur le fait que la relation de CI permet de diminuer la complexité d'une situation en réduisant le champ des possibles (Lewis & Weigert, 1985; Luhmann, 1968). En ce sens, Lewis et Weigert considèrent que dans les relations sociales « *Il n'est pas possible d'élaborer des plans d'action qui tiennent compte de tous les futurs possibles. Si tous les futurs événements possibles se voyaient accorder une probabilité égale, l'avenir apparaîtrait avec une complexité telle qu'elle empêcherait toute action rationnelle dans le présent*. » (Lewis & Weigert, 1985, p. 968)[17]. Dans les relations sociales et plus particulièrement dans des situations complexes le mécanisme de CI permettrait alors de supprimer un grand nombre d'alternatives. En ce sens, la confiance permettrait de s'affranchir de l'insuffisance des informations disponibles (ou du temps nécessaire pour les récupérer et les traiter) et contribuerait ainsi à la prise de décision.

Dans la littérature portant sur les relations économiques plusieurs définitions existent pour parler du concept de CI. Pour cette littérature, il est proposé ici de prendre en compte la définition de Gambetta qui caractérise bien les différentes notions sous-tendant les théories « probabilistes » de la confiance.

« *a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to monitor it) and in a context in which it affects his own action* » (Gambetta, 1988, p. 217)[18]

Dans cette définition de Gambetta et de manière plus globale dans les recherches menées en économie et dans certains champs de la littérature en sociologie, la notion d'évaluation probabiliste est clairement évoquée. Pour cette littérature, le fondement de la CI peut être envisagé comme étant le calcul du coût/bénéfice perçu d'une relation qui détermine le risque de la relation. Selon ce type d'approches, la CI émerge lorsque l'intention de réaliser une action bénéfique est perçue (Lewicki & Bunker, 1995; Rousseau et al., 1998; Shapiro, Sheppard, & Cheraskin, 1992). La relation de CI est ensuite maintenue par la récompense que la relation apporte aux deux parties. La relation de CI peut ainsi être résumée sous l'angle économique par un simple calcul de probabilités (Williamson, 1993) ; si, dans une situation donnée, le confiant pense obtenir plus de bénéfices en entrant dans la

[17] « It is not possible to develop plans of action which take into account all possible contingent futures. If all possible future events were accorded equal probability, the future would appear with such enormous complexity as to preclude rational action in the present. » (Lewis & Weigert, 1985, p. 968)

[18] Traduit ici par : « un niveau particulier de la probabilité subjective avec laquelle un opérateur évalue qu'un autre opérateur ou un groupe d'opérateurs va effectuer une action particulière, à la fois avant qu'il ne puisse contrôler cette action (ou indépendamment de sa capacité à la contrôler) et dans un contexte où elle affecte sa propre action » (Gambetta, 1988, p. 217)

relation de CI que ce qu'il pourrait en obtenir sans entrer dans la relation de CI alors le confiant entrera dans la relation de CI.

Cette notion de calcul de probabilité permet de comprendre pourquoi, dans la littérature portant sur les relations économiques, la situation est au centre des recherches effectuées sur la confiance (que celle-ci soit mise en place entre deux individus ou entre une marque et un individu). En effet, ce calcul de probabilité effectué par le confiant est le lien entre la notion de confiance et la notion de prise de décision qui est au centre de la littérature économique (cette littérature s'intéresse particulièrement aux mécanismes sous tendant le passage à un acte d'achat). Conceptuellement la décision correspond à « *un choix ou un ensemble de choix tirés des alternatives disponibles* » (Bellman & Zadeh, 1970, p. 19)[19]. La prise de décision peut être interprétée comme le choix de l'alternative présentant subjectivement le meilleur ratio coût/bénéfices. Dans cette approche la prise de décision correspond à une évaluation probabiliste des conséquences de différents choix (Lowenstein, 2003).

Dans le processus de prise de décision, le mécanisme de confiance pourrait être vu comme un réajustement des probabilités perçues par un opérateur des futurs possibles engendrés par différentes options, l'option choisie par l'opérateur étant celle ayant le meilleur ratio coût/bénéfice. Cette interprétation rejoint d'ailleurs la définition de Lewis et Weigert qui décrivaient la confiance comme « *to trust is to live as if certain rationally possible futures will not occur.* » (Lewis & Weigert, 1985, p. 969)[20]. Cette réduction de l'incertitude engendrée par la relation de confiance (Meyerson, Weik, & Kramer, 1996) permettrait donc de faciliter la prise de décision dans les environnements à forte incertitude.

Dans le cas de la RCPair, du fait du grand nombre d'informations et du traitement complexe des données, les opérateurs auront une incapacité à assigner des probabilités fiables quant aux évènements futurs engendrés par une décision. Dans les C2air, le cyber pourrait apporter une part d'incertitude et par conséquent une incapacité à prévoir avec précision les résultats d'une décision (Duncan, 1972; Schmidt & Cummings, 1976) ; cette incertitude pourrait être atténuée par la confiance. L'étude de cette littérature portant sur l'aspect probabiliste permet de mettre à jour l'importance de la confiance dans la prise de décision dans les situations à forte incertitude. Comme vu au chapitre précédent, la problématique de cette thèse est d'étudier les conséquences comportementales d'un manque ou d'un excès de confiance interpersonnelle sur les opérateurs travaillants dans la RCPair recevant des données soumises à une forte incertitude. Dans cette thèse, l'étude menée sur la prise de décision dans les environnements à forte incertitude s'appuiera donc sur cette littérature.

b. Approche psychologique réalisée dans la littérature managériale

Contrairement à la littérature économique qui axe ses recherches sur la notion de situation et de prise de décision, la littérature managériale axe ses recherches sur les relations entre le confiant et le

[19] « a choice or a set of choices drawn from the available alternatives » (Bellman & Zadeh, 1970, p. 19)
[20] « *to trust is to live as if certain rationally possible futures will not occur.* » (Lewis & Weigert, 1985, p. 969).

mandant. Plus particulièrement, la littérature managériale donne des informations sur les caractéristiques propres au mandant et au confiant et sur les conséquences comportementales engendrées par le niveau de CI présent entre deux individus. Dans cette littérature, la notion de CI peut être définie comme étant un état psychologique (Rousseau & Sitkin, 1998) qui traduit la volonté (*the wellingness*) (Mayer et al., 1995) d'un individu d'être vulnérable aux actions effectuée par un tiers.

La littérature managériale étudie la dynamique de la CI qui peut être vue soit comme un processus évolutif (Lewicki & Bunker, 1995; Rousseau & Sitkin, 1998; Shapiro et al., 1992) qui se bâtit dans la durée et dont le niveau est lié à la répétition des interactions entre les opérateurs, soit comme un processus immédiat et relativement stable lors du travail en équipes éphémères (Meyerson et al., 1996). Cette double approche (processus évolutif ou processus éphémère) semble particulièrement intéressante dans l'étude de la CI dans les C2. Comme vu dans le premier chapitre, dans une organisation *Edge C2* les opérateurs peuvent avoir à travailler avec des personnes qu'ils connaissent mais également avec des personnes qu'ils ne connaissent pas, des personnes qu'ils n'ont jamais vues et qu'ils ne verront probablement jamais. L'étude de la littérature managériale permet de connaitre les différences entre le niveau de CI présent dans les équipes constituées d'opérateurs ayant appris à se connaitre et le niveau de CI présent dans les équipes éphémères.

Il est admis dans la littérature managériale que le niveau de CI entre les membres d'une équipe est un modulateur des stratégies d'équipe et que ce niveau de CI est indépendant du type d'équipe. Ainsi, que ce soit dans les équipes formées de personnes qui travaillent ensemble depuis longtemps ou dans des équipes éphémères formées de personnes qui ne se connaissent pas, un niveau de confiance faible ou élevé sera mis en place et ce niveau de confiance sera un modulateur de la stratégie de l'équipe.

Dans la littérature portant sur la CI et la prise de décision, la relation de CI est décrite comme favorisant la satisfaction (Driscoll, 1978) et l'action (Jarvenpaa, Knoll, & Leidner, 1998) des individus. Plus généralement, que ce soit dans le domaine de la confiance dans le leader ou dans la dynamique de groupe, la CI semble être un modulateur de la performance (Colquitt, Scott, & Lepine, 2007; De Jong et al., 2016; Dirks & Ferrin, 2002). Au niveau comportemental elle est considérée comme modulant le temps de supervision de telle sorte qu'une augmentation du niveau de CI est lié à une diminution du nombre de ressources utilisées pour superviser le coéquipier (Colquitt et al., 2007; De Jong & Elfring, 2010; McAllister, 1995).

La littérature managériale étudie donc largement les comportements engendrés par différents niveaux de CI dans des équipes formées de personnes qui se connaissent ou dans des équipes formées de personnes qui ne se connaissent pas. Or, les modulations comportementales engendrées par différents niveaux de CI (modulation de la supervision et des ressources utilisées) pourraient altérer les décisions prises dans les C2air ; c'est pourquoi, les travaux de cette thèse se fondent sur cette littérature managériale pour étudier les conséquences comportementales d'un manque ou d'un excès de CI entre les différents opérateurs.

3. Types de confiance

La CI est donc étudiée tant dans des équipes évoluant ensemble depuis longtemps que dans les équipes éphémères (dans lesquelles les membres ne peuvent pas apprendre à se connaitre). Il est proposé ici d'étudier les différentes composantes de la mise en place d'un niveau de CI mais également les différents types de CI à savoir :

- La CI évolutive ou dynamique qui est mise en place dans des relations qui ont le temps d'évoluer (intra CDC par exemple) ;
- La CI rapide ou statique (« swift trust » dans la littérature anglophone) qui est mise en place dans les relations formées de personnes qui ne se connaissent pas et dont la relation de CI va être éphémère (inter CDC par exemple).

A. Composantes de la CI

Il ressort des différentes définitions que la confiance n'est ni un comportement ni un choix mais un état psychologique évolutif permettant la réduction de la complexité qui nécessite *a minima* pour être mis en place, des conditions de risque et d'interdépendance. Pour Shapiro et Lewicki la force du lien de CI entre individus, groupes ou institutions est fondée sur plusieurs composantes (ou bases) qui sont internes ou externes (Lewicki & Bunker, 1995; Shapiro, 1987) au confiant **:**

- La composante cognitive (Lewis & Weigert, 1985) ;
- La composante affective (Lewis & Weigert, 1985) ;
- La composante comportementale (Lewis & Weigert, 1985) ;
- La composante institutionnelle (Shapiro, 1987).

La composante cognitive de la confiance correspond à un processus de discrimination permettant de catégoriser des personnes ou des institutions comme étant dignes de confiance, associées à de la méfiance ou inconnues (Lewis & Weigert, 1985). Cette composante cognitive peut se baser sur le succès d'interactions passées avec la personne ou l'objet de confiance mais peut également être liée à des signaux plus institutionnels comme des titres professionnels par exemple (McAllister, 1995)**.** Grâce à des observations portant sur les comportements de différents coéquipiers au sein de différentes relations, la connaissance s'accumule, ce qui permet, à terme, de construire des représentations sociales (RS) (*Cf.* chapitre 2.A. «a. Caractéristique propre au confiant ») qui faciliteront la mise en place du niveau de confiance initial dans des nouvelles relations. Enfin, les premières interactions avec la personne ou l'objet de confiance permettent de confirmer ou d'infirmer les impressions antérieures (Johnston, McCutcheon, Stuart, & Kerwood, 2004; Lewis & Weigert, 1985)**.** Cette composante cognitive rejoint donc le concept des RS qui sous-tend que chaque groupe social (Abric, 2003) possède ses propres RS qui correspondent à un ensemble d'opinions, d'attitudes et de croyances à propos d'un objet ou d'une personne donnée. Si le mandant appartient à un groupe ou à une catégorie de personne avec qui le confiant est déjà rentré en contact (Tajfel, 1974) alors la confiance pourra émerger sur la base des RS que le confiant a du mandant.

La composante affective de la confiance quant à elle se base sur des investissements émotionnels (McAllister, 1995). Cette composante affective est généralement limitée aux interactions fréquentes

et aux relations étroites (Lewis & Weigert, 1985). Les relations de confiance affective sont notamment utilisées dans le commerce ou le e-commerce afin de former la base de confiance de la relation client grâce à la création d'un sentiment de sécurité et à une perception de force dans la relation (Johnston et al, 2004).

Les composantes cognitives et affectives peuvent exister de manière combinées (Lewis & Weigert, 1985). Cependant, bien que certains auteurs pensent que la confiance affective arrive après un certain niveau de composante cognitive (McAllister, 1995) d'autres soutiennent seulement qu'un des deux types de confiance doit exister avant qu'il y ait une confiance à deux niveau (Webber, 2008).

Pour qu'un mécanisme de confiance se mette en place il est souvent nécessaire qu'il y ait une redondance d'interaction ou qu'une troisième personne (différente du confiant ou du mandant) se porte garante du mécanisme de confiance. La réputation de l'institution peut jouer le rôle du médiateur de confiance permettant de faciliter l'apparition de la confiance (Rousseau & Sitkin, 1998). Cette composante institutionnelle est notamment facilitée grâce au fait que les dirigeants des institutions, qu'ils soient chef d'entreprise ou simples recruteurs, sont en mesure en choisissant les individus, de créer des familiarités entre eux (Shapiro, 1987). De plus, la mise en place de normes, de structures et de procédures connues et partagées dans l'institution permet une orientation des comportements des individus qui la composent, garante de la relation de confiance (Bachmann & Inkpen, 2011).

Enfin, la qualité et l'évolution de la confiance vont dépendre de la composante comportementale présente dans chaque relation. La pratique de la confiance garantit une action sociale (Lewis & Weigert, 1985) dont la qualité est modulée par la présence, la fréquence et la sincérité des communications. En l'absence de communications ou en présence de coopération évasive par exemple la situation de confiance ne peut pas être clairement définie (Schlenker, Helm, & Tedeschi, 1973). Une mesure de la confiance peut, par exemple, être mise en place uniquement par la fréquence des communications, sans prendre en compte le contenu de ces dernières (Adali et al., 2010). Cependant, le processus comportemental de la confiance ne peut se résumer uniquement à la présence ou absence de communication mais doit également prendre en compte la fiabilité des échanges (Rotter, 1980).

Les différentes composantes de la confiance présentées ci-dessus ne correspondent pas à l'ensemble des composantes étudiées dans la littérature. Dans la théorie des organisations par exemple des composantes relativement proches de celles vues précédemment mais aux dénominations différentes sont présentes, c'est le cas par exemple de la confiance :

- basée sur la catégorie (*category-based-trust*) ;
- basée sur les rôles (*role-based-trust*) ;
- basée sur les règles (*rules-based-trust*) ;
- basée sur les relations passées (*history-based-trust*) ;
- basée sur des caractéristiques propres au confiant (*dispositional-trust*) ;
- basée sur un tiers (*Third Parties as Conduits of Trust*) (Kramer, 1999).

Afin de faciliter la compréhension de la mise en place et de l'évolution de la CI, des auteurs ont choisi de rassembler plutôt que de décomposer les différentes composantes de la CI. Adam et Webb en 2002 définissent la construction de la CI comme étant un processus dynamique pouvant se réaliser grâce à deux grandes composantes, la composante liée aux caractéristiques générales du mandant (*category-based-trust*) et la composante liée aux caractéristiques propres au mandant (*person-based-trust*) (Adams & Webb, 2002). Dans les premiers temps de l'interaction, c'est le mécanisme de *category-based*-trust qui s'enclenche ; au premier contact, le confiant identifie les stéréotypes et les pratiques associées aux caractéristiques connues du mandant (Ashforth & Mael, 1989). Si le mandant appartient à un groupe ou à une catégorie de personne à qui le confiant fait confiance (Tajfel, 1974) alors le mécanisme de *category-based-trust*, peut s'enclencher. Puis, selon Adams et Webb, lorsque le confiant a le temps d'interagir suffisamment avec le mandant, il peut évaluer *in situ* la fiabilité du comportement du mandant. Ce mécanisme, dénommé *person-based-trust* nécessite une accumulation et une analyse d'informations, et, par conséquent, un grand nombre d'interactions et de temps (Adams & Webb, 2002). Ces deux mécanismes permettent l'un et l'autre l'émergence de la CI.

B. La CI évolutive ou dynamique

Dans le modèle de confiance décrit par Shapiro Sheppard et Cheraskin en 1992, la CI est un processus qui évolue au cours du temps et qui comprend trois niveaux distincts :

- Le *deterrence based trust* (confiance basée sur un rapport de force et la menace d'une perte de réputation) ;
- Le *knowledge based trust* (la confiance basée sur la connaissance de la personne ou de l'institution) ;
- L' *identification based trust* (la confiance basée sur une identification de la personne ou de l'institution).

Du fait de la difficulté de traduction, les termes anglais seront utilisés afin de définir les différents niveaux de CI étudiés dans cette partie. Il est également à noter que dans cette partie le terme « niveau » est relatif à la force du lien de confiance. Que ce soit dans le *deterrence* le *knowledge* ou l'*identification based trust* le niveau de confiance peut être relativement faible ou élevé.

Pour Shapiro et al., le premier niveau de CI correspond au *deterrence-based-Trust*, bien que ce dernier puisse être vu comme étant plus proche d'un faible niveau de méfiance plutôt que d'un niveau de confiance (Rousseau & Sitkin, 1998)**.** Le *deterrence-based-trust* peut être décrit comme une modification de l'incertitude liée au comportement d'un individu qui permet une diminution du besoin de surveillance et de supervision. Selon Shapiro et al., le *deterrence-based-trust* existe « *lorsque les coûts potentiels de l'actualisation de la relation ou la probabilité d'une action rétributive l'emportent sur l'avantage à court terme d'un comportement méfiant* » (Shapiro et al., 1992, p. 366)[21] et peut être mis en place grâce à des actions répétées, des interactions multiples mais surtout par la menace d'une perte de réputation. Le *deterrence-based-trust* peut être résumé de la

[21] « *when the potential costs of discountinuing the relationship or the likelihood of retributive action outweigh the short-term advantage of acting in a distrustful way* **»** (Shapiro et al., 1992, p. 366)

façon suivante , pour qu'il y ait confiance il faut que les bénéfices obtenus grâce à un comportement de « non-confiance » soient inférieurs aux préjudices engendrés par une perte de réputation (Shapiro et al., 1992). Du fait de la notion de perte de réputation, qui est souvent assortie d'une perte de profits pour l'entreprise, le *deterrence-based-trust a* été largement étudiée en économie et dans le champ de recherche relatif aux liens commerciaux entre entreprise.

En 1995 Lewicki et Bunker ont repris le concept de *deterrence-based-trust* (Lewicki & Bunker, 1995), qui était basé exclusivement sur des notions de menace de la punition (Ratnasingham, 1998), et l'ont fait évoluer en celui de *calculus-based-trust* (la confiance basée sur un calcul). Comme pour le *deterrence-based-trust,* dans le *calculus-based-trust* la CI est maintenue par la menace d'une perte de réputation. Seulement, dans le *caluclus-based-trust* la CI est également maintenue par la récompense que la relation de CI apporte aux deux parties (Lewicki & Bunker, 1995). Les *deterrence-based-trust* et *calculus-based-trust* émergent donc lorsque que l'intention de réaliser une action bénéfique est perçue (Lewicki & Bunker, 1995; Rousseau et al., 1998; Shapiro et al., 1992).

Avec le temps, et dans des situations non risquées, certaines relations de *deterrence-based-trust* ou *calculus-based-trust* peuvent évoluer en un deuxième niveau appelé *knowledge-based-trust* (Lewicki & Bunker, 1995). Ce niveau de CI permet au confiant de libérer des ressources temporelles. Pour cela, le confiant effectue une prédiction des comportements futurs du mandant afin d'augmenter la prévisibilité et de réduire l'incertitude plus efficacement que dans du *deterrence-based-trust* ou *calculus-based-trust*. Les différents niveaux de CI étant liés à la tâche, le *deterrence-based-trust* ou *calculus-based-trust* et le *kowledge-based-trust*, peuvent coexister au même moment d'une relation de CI.

Enfin, le dernier des trois niveaux de confiance défini par Shapiro et al. correspond à *l'identification-based-trust.* A mesure que la prédiction et la connaissance des valeurs et des besoins de l'autre apparait une appartenance à un groupe de confiance se crée. Du fait du temps nécessaire à la mise en place d'une *identification-based-trust* l'investissement nécessaire est beaucoup plus important que pour les deux niveaux précédents ce qui implique que ce niveau n'est que rarement atteint (Lewicki & Bunker, 1995; Shapiro et al., 1992). Parce que l' *identification-based-trust* est basée sur les deux autres niveaux de CI précédents, les relations caractérisées par une *identification-based-trust* sont plus « solides » que les relations de *deterrence-based-trust*, *calculus-based-trust* et *kowledge-based-trust* (Lewicki & Bunker, 1995). C'est pour cela que les études portants sur ce niveau de CI sont réalisées notamment dans le domaine du e-commerce (Chadwick, 2001).

En résumé, les différents niveaux de CI vus dans cette partie sont liés aux différentes composantes de la confiance (*Cf.* Figure 18). Le niveau initial de CI s'appuie en premier lieu sur des composantes cognitives probablement basées sur des RS que le confiant associe au mandant. Ces RS peuvent provenir de lien de confiance antérieur avec des individus ressemblant au mandant mais peuvent être également médiées par l'institution que le mandant représente. Au cours de la relation, le niveau de CI va évoluer en fonction des comportements du mandant dans la relation de confiance mais également sur des notions plus affectives créées par la qualité et la quantité des échanges entre les différents acteurs du lien de confiance.

	Deterrence-based-trust / Calculus –based-trust	Knowledge-based-trust	Identification-based-trust
Composante **cognitive**	V	V	V
Composante **affective**			V
Composante **institutionnelle**	V	V	V
Composante **comportementale**		V	V

Figure 18 : composantes de la CI mobilisées dans les différents niveaux de confiance

C. La CI statique ou confiance rapide

Les théories étudiant la confiance comme un processus dynamique et évolutif sont les plus courantes dans la littérature. Comme vu au sous-chapitre précédent, dans ce type d'approche la confiance est identifiée comme étant un processus nécessitant un grand nombre d'interactions tant pour sa mise en place (Jensen, Johansson, & Löfström, 2006) que pour son maintien ou son évolution. Cependant, l'avènement des TIC a mené à l'accroissement du nombre d'équipes temporaires dans lesquelles le développement des interactions n'est pas toujours possible. Ce type d'équipe distribuée (Fiore, Salas, Cuevas, & Bowers, 2003) est défini par Wildman, Fiore, Burke, Salas & Garven (2011) comme des *STAT*s, i.e. *Swift Starting Action Team* (Mckinney, Barker, Davis, & Smith, 2005; Wildman, Fiore, Burke, Salas, & Garven, 2011). Les équipes éphémères formées dans les *Edge C2* sont un exemple de STATs. Les membres de ces équipes ont chacun des compétences spécifiques et doivent agir conjointement afin d'effectuer une tâche. Dans ce type d'équipe le niveau de confiance n'évolue pas (ou peu) et est basé sur un mécanisme de confiance spécifique, la confiance rapide.

Ces STATs, qu'elles soient civiles ou militaires, ont toutes différents points communs. En premier lieu l'équipe est formée pour une mission donnée dans un temps donné qui peut aller d'une dizaine de minutes à plusieurs jours. Deuxièmement les membres de l'équipe peuvent être co-localisés ou non mais ne se connaissent pas avant le début de la mission. Enfin, chaque individu membre de l'équipe est expert d'un domaine et n'a pas forcément de connaissances sur d'autres domaines nécessaires à la réalisation de la mission.

Dans ce contexte de STATs, le confiant va dans un premier temps vérifier la correspondance entre ce qu'il sait du mandant et les RS associées à de la CI dont il dispose (Adams & Webb, 2002; Foddy, Platow, & Yamagishi., 2009). L'appartenance du mandant à une organisation présupposant l'usage de règles connues (Kramer, 1999), sa catégorie sociale (Foddy et al., 2009) ou encore sa fonction (Kramer, 1999) permettent alors au confiant d'évaluer le mandant. Ce processus est qualifié par Kramer de *presumptiv trust* (1999), ou plus communément de confiance rapide (Crisp & Jarvenpaa, 2013; Meyerson et al., 1996; Robert, Denis, & Hung, 2009). Celle-ci correspond, aux premières impressions apparentes au moment où le système temporaire commence à fonctionner et sont basées sur des attentes consistant en des hypothèses catégorielles et des cadres d'interprétation (Meyerson et al., 1996).

Cette confiance rapide est donc issue de la seule activation des RS et constitue un niveau de confiance initial spécifique, non modulé par itérations. Une fois le niveau de confiance rapide fixé, si le confiant peut interagir suffisamment avec le mandant, il évaluera *in situ* la fiabilité du

comportement du mandant au travers du mécanisme *d'history based trust* (Kramer, 1999). Cependant, la durée très courte de certaines missions des STATs ne permet pas l'émergence d'*history-based-trust* (Adams & Webb, 2002; McAllister, 1995). Afin de faciliter la compréhension il est considéré ici que le mécanisme de confiance rapide peut être considéré comme un *calculus-based-trust* non évolutif.

4. Modèles de confiances

Dans les parties précédentes, les définitions de la confiance, les deux grandes approches (probabiliste et basée sur les caractéristiques des personnes) et les deux types (évolutive ou confiance rapide) de CI étudiées dans la littérature ont été comparées. Les informations qui ressortent de la partie précédente sont que la CI, qu'elle soit évolutive ou statique, modifie le comportement des individus et que, *a minima* trois entités (un confiant un mandant et une situation) sont nécessaires afin de mettre en place un niveau de confiance. Pour, qu'il y ait confiance il faut que le confiant ait besoin que le mandant effectue des actions permettant de modifier une situation donnée. Cependant, ni les caractéristiques propres à chacune des entités ni le lien qui les unit n'ont encore été vus. Afin de les étudier il est nécessaire d'aborder différents modèles présentés dans la littérature.

C'est de la littérature managériale et des organisations que proviennent la plupart des modèles portant sur la CI (Costa et al., 2018; Mayer et al., 1995; Mayer & Gavin, 2005; McAllister, 1995; Burke et al., 2007). Le point commun à ces différents modèles est qu'ils proposent tous deux parties distinctes : la première partie correspond aux *antecedents* (i.e. les mécanismes de la mise en place du niveau de confiance), et la seconde partie correspond aux *outcomes* (i.e. les conséquences comportementales du niveau de confiance).

Le modèle classiquement utilisée dans la littérature sur la CI est celui de Mayer Davis et Schoorman (1995). Dans ce modèle (*Cf.* Figure 19), les caractéristiques propres au confiant ainsi que la perception qu'a le confiant des caractéristiques du mandant (*antecedents*) permettent la mise en place d'un niveau de confiance. Ce niveau de confiance, ainsi que la prise en compte du risque présent perçu, modifient le comportement qu'à le confiant dans la relation (*outcomes*).

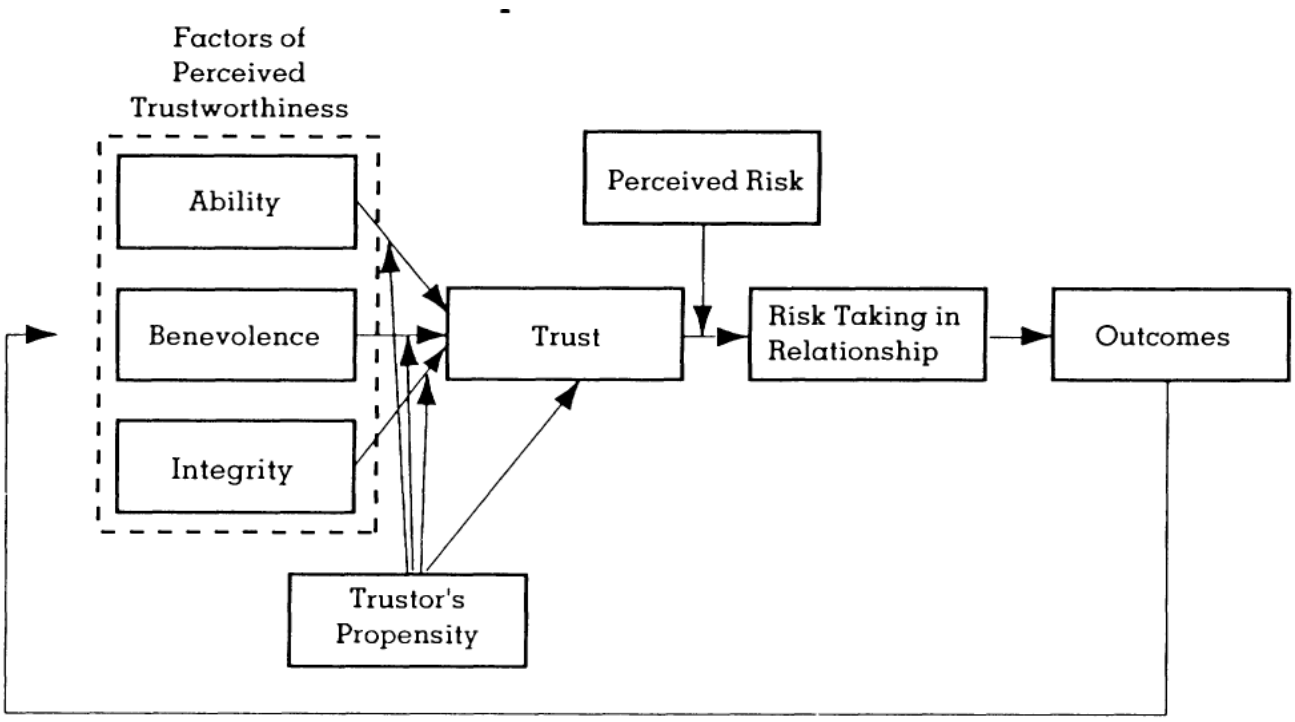


Figure 19 : Modèle de Mayer et al. (Mayer et al., 1995) présentant la dynamique de la confiance.

Ce modèle classique est facilement compréhensible ne permet pas de mettre en lien les 3 entités (la situation en tant que telle n'apparait pas dans le modèle de Mayer et al.). En réalité, les modèles faisant apparaitre les trois entités sont extrêmement rares, sans doute en raison de la dualité vue précédemment à savoir qu'une littérature axe plus ses recherches sur la situation alors qu'une autre littérature axe plus ses recherches sur le confiant et le mandant. Afin de trouver des modèles faisant apparaitre les trois entités il est nécessaire de changer de littérature. Ainsi, dans la littérature ergonomique ce type de modèle se retrouve notamment dans les travaux de Karsenty (2011) (*Cf.* Figure 20). Dans le modèle de Karsenty, les trois entités de la confiance (confiant, mandant, *situation*) sont représentées comme étant des *antecedents,* et, comme dans le modèle de Mayer, ce niveau de confiance modulerait le comportement des individus. Cependant, ce modèle ne caractérise pas explicitement les actions effectuées par le confiant, les actions effectuées par le mandant et quel est le rôle de la situation et de son évolution.

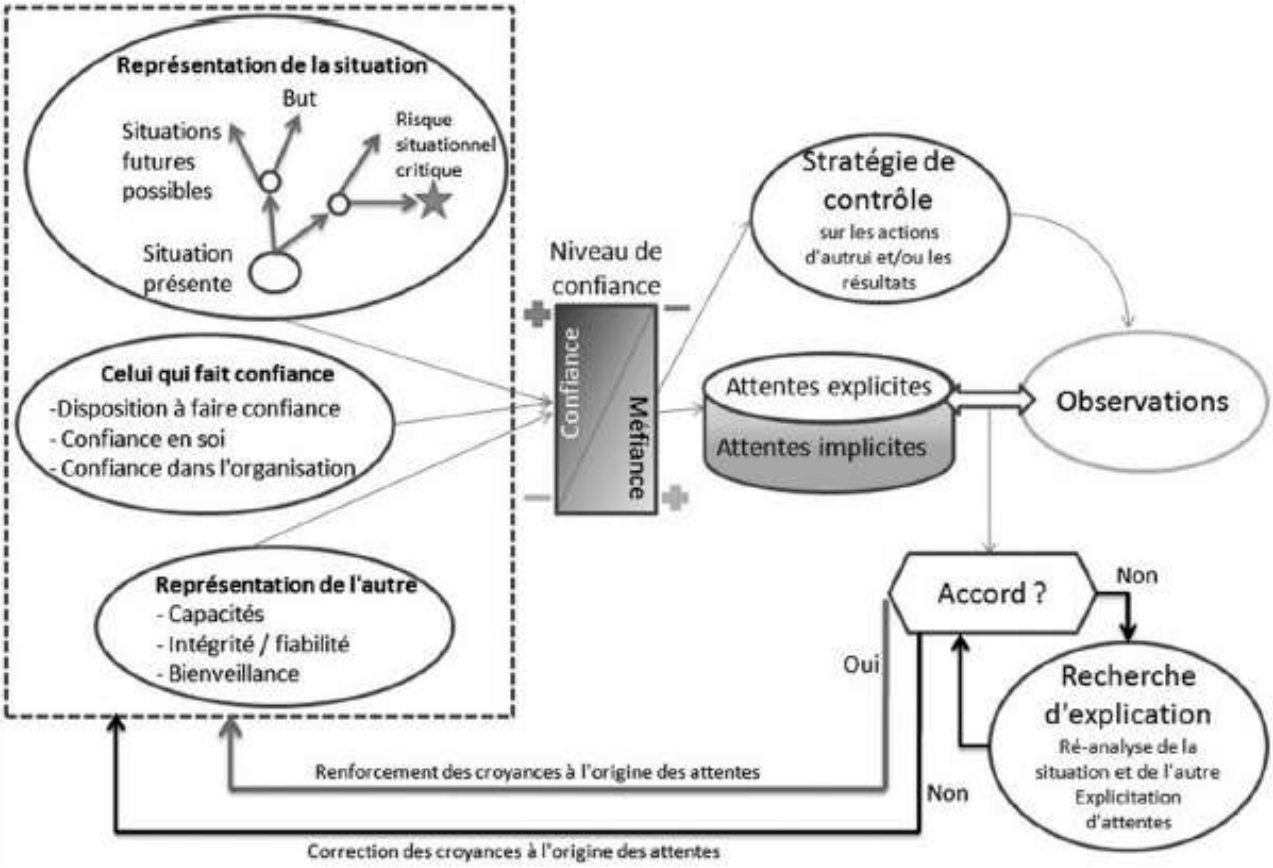


Figure 20 : Modèle de la dynamique de la confiance proposé par Karsenty (2011).
Dans ce modèle, les trois entités (confiant, mandant et situation) permettent la mise en place du niveau de confiance présent dans la relation. Ce niveau de confiance va entrainer des modulations comportementales.

Dans la littérature il semble y avoir un manque de modèle faisant apparaitre distinctement le lien entre les trois entités. Tous les modèles s'accordent sur le fait que des *antecedents* vont permettre la mise en place d'un niveau de confiance et que ce niveau de confiance va entrainer des *outcomes* (*Cf.* Figure 21). Dans la littérature, certaines études se sont focalisées sur l'une ou l'autre des parties et ont enrichi le modèle soit par le biais de l'étude des facteurs de mise en place du niveau de confiance (*antecedents*) soit par le biais de l'étude des différentes *outcomes* (Doney, Cannon, & Mullen, 1998; Sendjaya & Pekerti, 2010; Williamson, 1993). Les caractéristiques de chacune des différentes entités vont être à présent étudiées afin de réaliser un modèle qui sera utilisé tout au long de ce manuscrit.

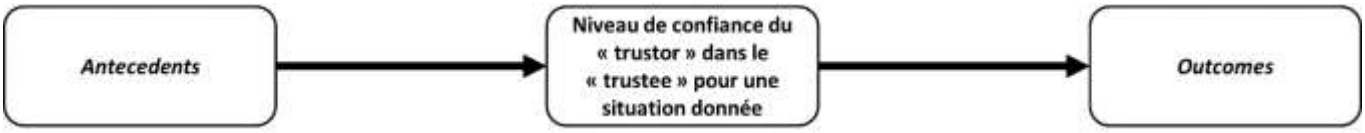


Figure 21 : Modèle conceptuel de base de la dynamique de la confiance qui représente le pont commun à tous les modèles de la littérature.
Dans tous les modèles présentés dans la littérature des *antecedents* permettent la mise ne place du niveau de confiance qui entrainera des *outcomes*.

5. Intégration des principales contributions de la littérature à la construction du modèle utilisé dans la thèse

Le centre du modèle est l'évaluation, souvent subjective, que le confiant a de la fiabilité du mandant (Quéré, 2001) pour réaliser une tâche donné, à un moment et dans un environnement donné (*Cf.* Figure 22). Ceci correspond aux définitions de la confiance provenant des différentes littératures telle que celle de Gambetta (1988: 217) « *un niveau particulier de la probabilité subjective avec laquelle un agent évalue qu'un autre agent ou groupe d'agents effectuera une action particulière, à la fois avant qu'il ne puisse contrôler cette action (ou indépendamment de sa capacité à la contrôler) et dans un contexte où elle affecte sa propre action* » ; de Rousseau et al. (1998)[22] « *La confiance naît lorsque le* confiant *perçoit que le* mandant *a l'intention d'accomplir une action qui est bénéfique* » (Rousseau, Sitkin, Burt & Camerer, 1998, p.399)[23] ; ainsi que de Dietz et Den Hartog « *A fait confiance B pour faire X (ou pour ne pas faire Y)* » (Dietz & Den Hartog, 2006)[24].

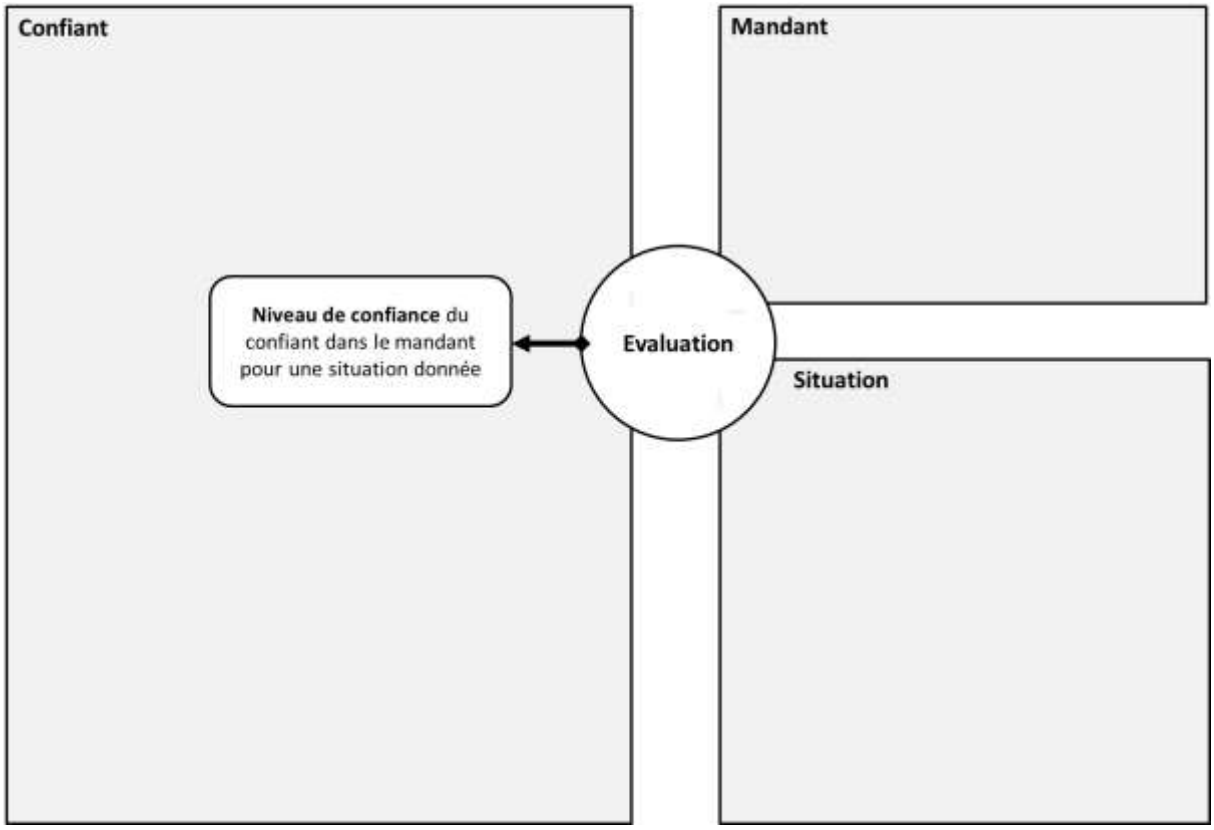


Figure 22 : Bases du modèle qui sera utilisé dans ce manuscrit.
Le confiant évalue la fiabilité du mandant pour réaliser une action dans une situation donnée. Cette évaluation permet la mise en place du niveau de confiance.

[22] « a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to monitor it) and in a context in which it affects his own action » (Rousseau et al, 1998)

[23] « Trust emerges when the trustor perceives that the trustee intends to perform an action that is beneficial » (Rousseau, Sitkin, Burt & Camerer, 1998, p.399)

[24] « A trusts B to do X (or not to do Y) » (Dietz & Den Hartog, 2006)

A. Facteurs contribuant à la mise en place de la confiance (*antecedents*)

a. Caractéristique propre au confiant

Sur l'étude des facteurs contribuant à la mise en place de la confiance (les *antecedents*) certains concepts sont utilisés ponctuellement et ne font pas consensus dans leur littérature respective. En informatique par exemple des études suggèrent que des concepts tels que la perception de la facilité d'utilisation ou encore la perception de la sécurité du système (Koufaris & Hampton-Sosa, 2004) sont des facteurs permettant la mise en place d'un niveau de confiance. Dans les champs de la littérature relatifs aux organisations et au management, des concepts tels que la confiance dans les institutions, les processus cognitifs (McKnight, Cummings, & Chervany, 1998)**,** les normes sociales ou encore la culture (Doney et al., 1998) sont évoqués comme étant des *antecedents.* Ces différents concepts apportent, chacun à leur niveau, des informations sur la mise en place du niveau de confiance ; cependant afin de faciliter la lecture du modèle il est préférable de ne prendre en considération que les concepts faisant consensus dans leur littérature respective.

L'un des concepts les plus repris dans les différentes littératures est celui de prédisposition individuelle à faire confiance, nommée *disposition to trust.* Ce concept provient des sciences humaines (Karsenty, 2011; Mayer et al., 1995) dans lesquelles il est considéré comme central dans l'étude de la mise en place du niveau de confiance initial**.** Ce concept a ensuite été étudié dans la littérature informatique et notamment dans le fonctionnement des équipes virtuelles médiées par ordinateur (Greenberg, Greenberg, & Antonucci, 2007)**,** le e-commerce (Lee & Turban, 2001; McKnight, Choundhury, & Kacmar, 2002) ou encore les compagnies en ligne (Koufaris & Hampton-Sosa, 2004)**.** Cette augmentation des études sur la *disposition to trust* dans les différents champs de la littérature tend à rendre ce concept généralisable dans l'étude des facteurs contribuant à la mise en place de la confiance.

Cette *disposition to trust* est propre au confiant et caractérise en grande partie le niveau de confiance initial qu'un confiant accordera à un mandant. Pour une partie de la littérature, cette *disposition to trust* est essentiellement fondée sur un concept nommé *propensity to trust* (Karsenty, 2011; Mayer et al., 1995; McKnight et al., 1998, 2002). Cette *propensity to trust* est considérée comme un trait de personnalité issu de la petite enfance, qui constitue une posture générale venant impacter fortement le niveau de confiance initial accordé à un tiers lors d'une première rencontre (McKnight et al., 1998). Cette *propensity to trust,* qui est stable dans le temps, serait particulièrement influente dans les premiers temps d'une relation et définirait quasiment le niveau de confiance initial attribué par le confiant à n'importe quel individu lorsqu'aucune information sur la fiabilité de cet individu n'est présente (Alarcon et al., 2018).

Parallèlement, une autre partie de la littérature envisage la CI comme étant fonction du contexte social (Cook & Hardin, 2001; Kramer, 1999). La CI pourrait être fonction du pays mais également du type de société et de culture (Huff & Kelley, 2003; Zaheer & Zaheer, 2006) auxquelles appartient le confiant, et serait notamment fortement déterminée par certaines normes propres à chaque communauté (Delhey, Newton, & Welzel, 2011). Pour cette littérature, la *disposition to*

trust (appelée « confiance par apprentissage social » dans la suite de ce manuscrit) se construirait par incrémentation à partir des rencontres vécues de manière positives ou négatives (Hardin, 2004; Jones & Shah, 2016; Rotter, 1967) et ne serait plus un caractère stable dans le temps comme l'est la *propensity to trust*.

Pour la littérature étudiant la confiance par apprentissage social, la *disposition to trust* est également modulée par la situation (sa nouveauté par exemple selon Rotter (1971)), le type de personne impliquées dans la relation, et les expériences antérieures du confiant. Cette modulation se fonde probablement sur le mécanisme des Représentations Sociales (ou RS) de l'individu, qui évoluent toute sa vie en fonction des groupes sociaux auxquels il appartient (Abric, 2003). Ces RS permettent à l'individu de reconnaitre une personne comme appartenant à une catégorie (par exemple « de confiance » ou « pas de confiance ») en fonction de certaines caractéristiques de cette personne (Posten & Mussweiler, 2019; Rateau, Molliner, Guimelli, & Abric, 2012). Par ailleurs, ces RS (Abric, 2003) ne sont pas homogènes dans la population mais dépendent du groupe social dans lequel elles sont employées. Chaque groupe social (Abric, 2003) possède ses propres RS, i.e. un ensemble d'opinions, d'attitudes et de croyances à propos d'un objet donné, qui conditionnent ses comportements.

Pour résumer, il sera considéré dans ce manuscrit que la *disposition to trust* est une caractéristique propre au confiant contribuant à la mise en place du niveau de confiance dans la relation et qui comprend la *propensity to trust* et la confiance par apprentissage social (*Cf.* Figure 23).

La *disposition to trust* peut être considérée comme étant la caractéristique fondamentale propre au confiant permettant la mise en place du niveau initial de CI. Cependant, en analysant le modèle de Karsenty il apparait qu'une autre caractéristique propre au confiant pourrait être mobilisée dans la mise en place du niveau de confiance : la confiance en soi (CS). La CS a été très peu étudiée dans la littérature sur la CI est majoritairement étudiée dans la littérature portant sur les systèmes automatisés et l'informatique (de Vries, Midden, & Bouwhuis, 2003; Kantowitz, Hanowski, & Kantowitz, 1997; Lee & Moray, 1992; Lee & Moray, 1994). Bien que la CS soit mobilisée dans la littérature, elle semble être un concept relativement vague dont la notion regroupe différents termes anglais tel que *self-trust, self-confidence* ou encore *self-esteem.* Comme pour la CI, la CS ne semble pas avoir de définition qui fasse consensus. Cependant, afin de définir la CS il est possible de se référer aux travaux de de Bandura qui décrit indirectement la CS par le biais de la perception de l'efficacité (*self-percepts of efficacity*) (Bandura, 1982), autrement dit, la perception qu'a un individu de sa propre efficacité à réaliser une tâche donnée. Selon Bandura « *La perception de l'efficacité n'est pas simplement une estimation inerte de l'action future. Les auto-évaluations des capacités opérationnelles fonctionnent comme un ensemble de déterminants immédiats du comportement des personnes, de leurs schémas de pensée et des réactions émotionnelles qu'elles rencontrent dans des situations éprouvantes. »* (Bandura, 1982, p. 122‑123)[25]. Pour Bandura et plus généralement pour les auteurs de la littérature informatique le niveau de CS l'individu d'adapter son comportement. Par conséquent, la CS ne jouerait pas sur les *antecedents* mais sur les *outcomes.* Pour cette raison, il a été choisi d'exclure la notion de CS du modèle à ce stade du manuscrit, (*Cf.* Figure 23). L'impact de la CS sur la mise en place du niveau de confiance et sur le comportement du confiant sera cependant

[25] « Self-percepts of efficacy are not simply inert estimates of future action. Self-appraisals of operative capabilities function as one set of proximal determinants of how people behave, their thought patterns, and the emotional reactions they experience in taxing situations. » (Bandura, 1982, p. 122‑123).

étudié plus tard (*Cf.* chapitre 6 « Etude de l'influence de la confiance en soi et de la confiance dans le système sur le comportement de l'opérateur »).

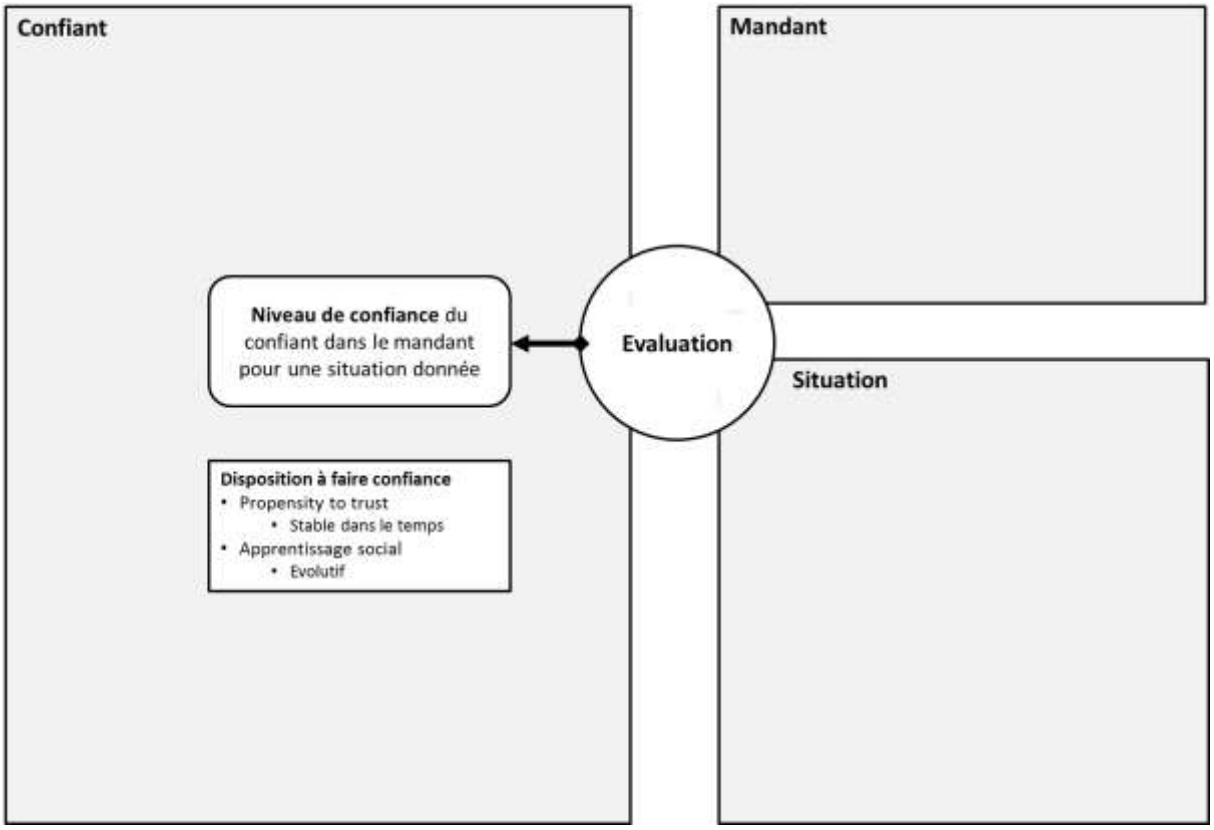


Figure 23 : Modèle incluant les caractéristiques propres au confiant pouvant être mobilisées dans la mise en place du niveau de confiance présent dans une relation.

b. Caractéristiques propres au mandant

Dans une relation de CI, le rôle du *mandant* est d'agir sur la situation afin de la faire évoluer (Burke et al., 2006). De fait, si la relation de CI met en jeu des caractéristiques propres du confiant, elle repose également sur la perception que ce confiant a du mandant. Cette perception est souvent rassemblée sous le concept de crédibilité mais est ensuite décrite par de nombreux facteurs plus ou moins bien définis et souvent liés entre eux (McKnight et al., 2002). En 1995 Mayer et al. synthétisent la littérature sur la CI et en ressortent les trois attributs de la fiabilité que sont, l'aptitude (*ability*), l'intégrité (*integrity*) et la bienveillance (*benevolence*). Dès lors, ces trois attributs de la fiabilité semblent faire consensus dans les différents domaines (Greenberg et al., 2007; Karsenty, 2011; Lee & Turban, 2001; Mayer et al., 1995; McKnight & Chervany, 2000).

Mayer et al. (1995) attribuent le lien entre l'intégrité et la confiance à Lieberman (Lieberman, 1981). L'intégrité est un concept multifactoriel utilisé de manière différente selon les littératures. Sur le rôle de l'intégrité du mandant dans la mise en place du niveau de CI il est cependant fréquent de se référer a Mayer et al. qui définissent le rôle de l'intégrité comme « *Des aspects telles que la cohérence des actions passées du parti, les communications crédibles sur le* mandant *provenant d'autres parties, la conviction que le* mandant *a un sens aigu de la justice et la mesure dans laquelle*

les actions du parti sont conformes à ses paroles, tout cela affecte le degré de jugement de son intégrité. »[26].

L'aptitude est décrite par Deutsch en 1960 « *pour faire confiance à une autre personne pour produire un événement bénéfique X [...] une personne doit avoir confiance que l'autre personne a la capacité et l'intention de le produire* » (Deutsch, 1960)[27]**.** L'aptitude est un attribut de la fiabilité directement lié aux compétences du mandant qui lui permettent de « *prévenir ou résoudre les conflits en matière de responsabilités* »[28] et « *de considérer les objectifs des autres comme ses propres objectifs* » (Deutsch, 1958)[29].

Enfin, le concept de bienveillance peut être directement associé aux comportements du mandant dans la relation. Le lien entre le comportement de bienveillance et la confiance semble provenir des travaux de Solomon (1960)[30] qui indiquait que « *La confiance fait référence aux attentes de bienveillance, tandis que la suspicion fait référence aux attentes de malveillance* **».** La bienveillance pourrait être définit comme un « *les comportements qui reflètent une motivation sous-jacente à faire passer l'intérêt de la personne de confiance avant son propre intérêt* » (Sirdeshmukh, Singh, & Sabol, 2002)[31].

L'évaluation des attributs de la fiabilité du mandant se fait principalement sur la base des échanges entre le confiant et le mandant. De fait la communication entre le confiant et le mandant permet la mise en place du niveau initial de CI mais également le maintien et l'évolution de ce niveau (Jarvenpaa & Leidner, 1999). Ces trois attributs de la fiabilité ne semblent pas intervenir au même moment de la relation de CI. L'intégrité, comme définie par Mayer et al. (1995) demande une évaluation longue de la part du confiant alors que les deux autres attributs de la fiabilité sont perfectibles plus facilement. L'évaluation de l'aptitude et de l'intégrité est fortement influencée par les premières interactions. Ces deux caractéristiques permettent au confiant de juger si les comportements du mandant seront prévisibles et explicables, ce qui est nécessaire puisque le fait de faire confiance génère chez le confiant des attentes vis-à-vis du comportement de son coéquipier (Kramer & Carnevale, 2003).

Le niveau accordé par le confiant aux différents attributs de la fiabilité est donc réajusté tout au long de la relation de confiance. Une évolution de la situation, due aux actions effectuées par le mandant et perçue par le confiant, entraine une réévaluation des attributs de la fiabilité, et, par conséquent, fait évoluer le niveau de CI présent dans la relation (Flèches circulaire sur la figure 24) (ce qui permet le fonctionnement de la CI dynamique vue précédemment). Ces différents attributs de fiabilité sont donc principalement mobilisés dans le maintien et l'évolution du niveau de CI mais moins dans la

[26] « Such issues as the consistency of the party's past actions, credible communications about the trustee from other parties, belief that the trustee has a strong sense of justice, and the extent to which the party's actions are congruent with his or her words all affect the degree to which the party is judged to have integrity. » (Mayer et al., 1995)

[27] « To trust another person to produce a benefical event X […] an individual must have confidence that the other individual has the ability and intention to produce it » (Morton & Deutsch, 1960)

[28] « to prevent or resolve conflict on responsabilities »(Morton & Deutsch, 1958)

[29] « to take the goals of others as goal of one's own » (Morton & Deutsch, 1958)

[30] « Trust refers to expectations of benevolence; whereas suspicion refers to expectations of malevolence **»** (Solomon, 1960)

[31] « behaviors that reflect an underlying motivation to place the [trustor's] interest ahead of self-interest **»** (Sirdeshmukh et al., 2002)

mise en place de ce dernier (il est impossible d'évaluer l'aptitude d'un individu sans l'observer *in situ*).

Afin de mettre en place le niveau initial de CI, le confiant accorde un niveau de fiabilité au mandant sur la base de différentes propriétés directement vérifiables. Ces propriétés correspondent aux différentes caractéristiques sociales du mandant tel que le sexe, la tranche d'âge ou encore la nationalité. Sur la base de ces propriétés et des interactions passées avec des individus ayant des caractéristiques similaires, le confiant classe le mandant dans un groupe social spécifique (par exemple personne de confiance ou non). Ces propriétés « activent » les différentes RS du confiant qui permettent la mise ne place du niveau de CI initial. Dans le modèle présenté ici, les propriétés du mandant correspondent à des « signaux » (des RS) qui permettent « d'activer » l'apprentissage social du confiant (*Cf.* Figure 24).C'est pour cela que les RS sont indiquées comme appartenant au mandant.

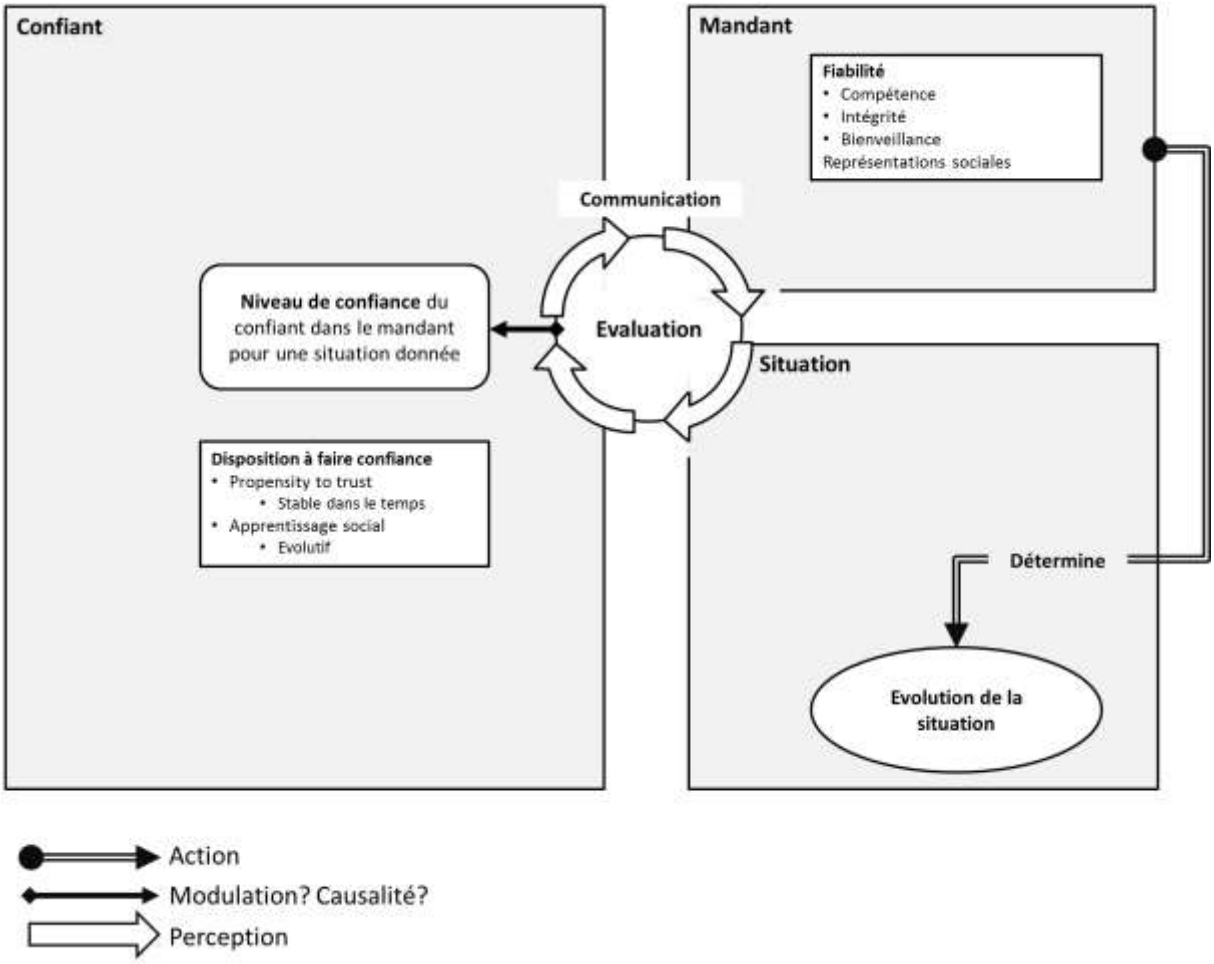


Figure 24 : Modèle incluant les caractéristiques propres au mandant ayant pour rôle d'agir sur une situation donnée.
Les différentes propriétés du mandant vont permettre, par le biais des RS activées, de mettre en place un niveau de CI initial. Dans un second temps, la communication entre le confiant et le mandant va permettre au confiant d'évaluer *in situ* les différents attributs de la fiabilité et de faire évoluer le niveau de CI.

c. Caractéristiques de la situation

La situation est la troisième composante de la mise en place et de l'évolution du niveau de CI. Dans la littérature, les notions de risque et de confiance semblent être indissociables. En 1973, Schlenker Helm et Tedeshi définissent la CI comme étant « *la dépendance à l'égard d'informations communiquées par une autre personne sur des états environnementaux incertains et leurs conséquences dans une situation risquée.* » (Schlenker et al., 1973, p. 419)[32]. Cette définition permet d'identifier les trois entités du modèle mais ne permet pas de montrer l'interdépendance du risque et de la confiance.

La perception du risque présent dans une situation joue un rôle tant sur la détermination du niveau de CI que sur le comportements du confiant (Mayer et al., 1995). Cette notion de situation, et plus particulièrement le ressenti ou la perception qu'à le confiant d'une situation donnée, est fortement liée à plusieurs facteurs tel que le cadre de survenu (milieu professionnel ou personnel) ou encore la notion d'institution. Une institution est régie par des normes et des procédures connues et partagées par tous ses membres ce qui permet l'orientation des comportements des individus qui la composent (Bachmann & Inkpen, 2011). Ainsi, une situation mise en place dans un certain cadre institutionnel pourrait paraitre normale (McKnight et al., 1998) et sembler être non risquée alors qu'elle serait perçue différemment dans un autre cadre. Par exemple, une étude menée sur des membres d'équipes travaillant dans des environnements pouvant être qualifiés comme étant à risque élevé (e.g. centrale nucléaire) montrent que la connaissance qu'a l'individu du risque associé à une tache pourrait permettre de diminuer le risque perçu (Sjoberg & Drottz-Sjoberg, 1991). En outre, le niveau de CI global étant un autre facteur pouvant influencer la perception du risque (Siegrist et al., 2005; Siegrist & Cvetkovich, 2000), la perception du risque présent dans une situation pourrait varier pour chaque individu et dépendante de plusieurs facteurs. En d'autres termes, une situation caractérisée par certains individus comme étant fortement risquée, pourrait être ressentie par d'autres comme étant normale (*Cf.* Figure 25).

Dans d'autres champs de la littérature et plus particulièrement dans la littérature économique, la CI n'est plus définie comme étant liée au risque présent dans la situation mais comme étant un niveau d'appréciation du ratio coût bénéfice d'une relation (Lewicki & Bunker, 1996). Dans les relations de travail la CI pourrait être facteur de la représentation que se fait le confiant des futurs possibles engendrés par une situation (Karsenty, 2011) et non pas de la situation elle-même. Dans le présent modèle, il est considéré que le niveau de CI n'est pas influencé par la normalité ou le risque ressenti par le confiant dans une situation donnée mais par les nouveaux futurs possibles engendrés par les actions du mandant sur la situation (*Cf.* Figure 25).

[32] « a reliance upon information received from another person about uncertain environmental states and their accompanying outcomes in a risky situation. » (Schlenker et al., 1973, p. 419)

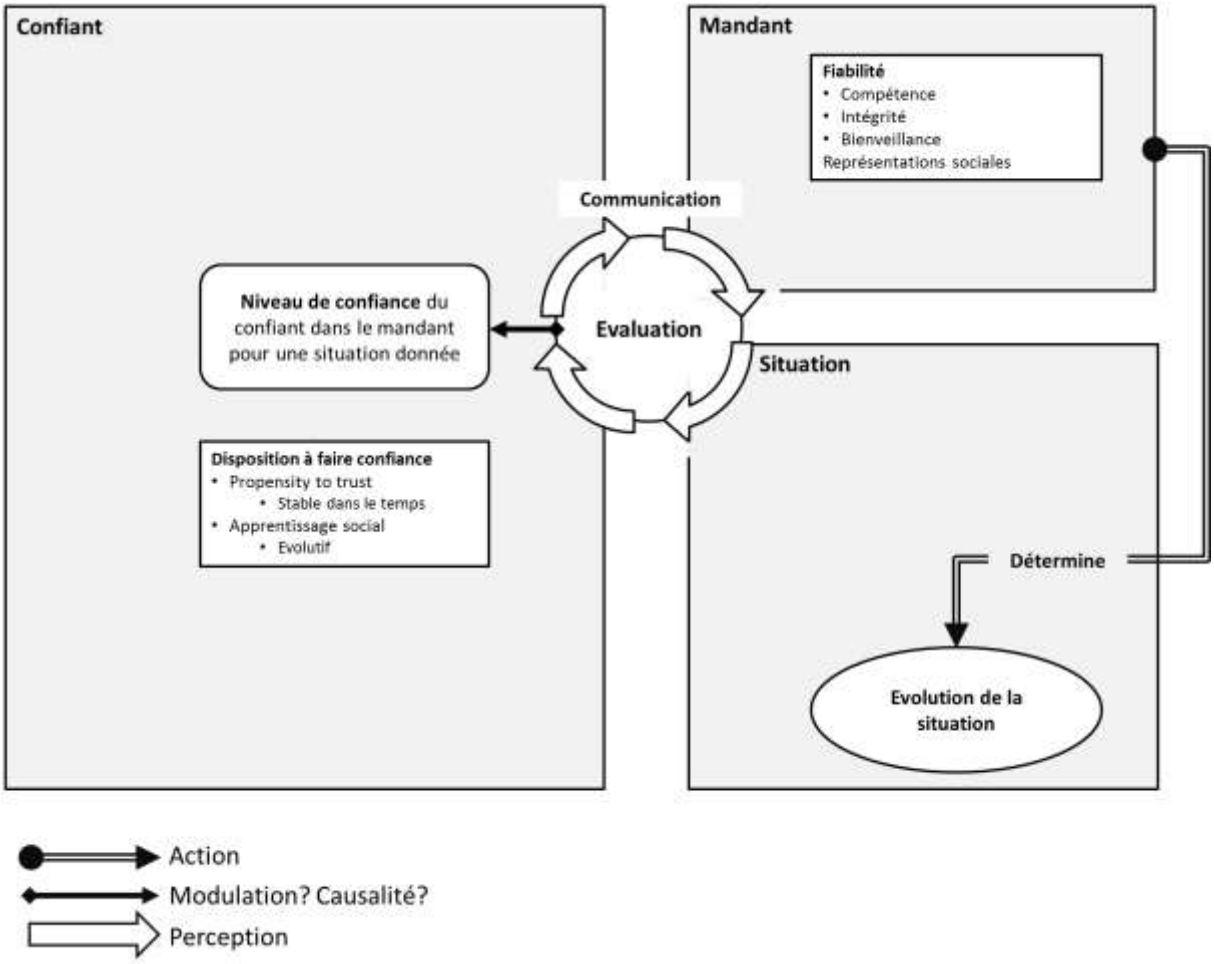


Figure 25 : Modèle incluant les caractéristiques de la situation.
Une situation peut être perçue comme étant à risque ou comme étant normale, cependant, quelle que soit la situation, la perception qu'a le confiant de l'évaluation des futurs possible devrait moduler le niveau de CI.

d. Actions et conséquences du niveau de confiance

Du point de vue des équipes, les facteurs résultants d'un excès ou d'un manque de CI ont largement été étudiés, dans le domaine du management et de l'analyse de la performance d'équipe (De Jong, Dirks, & Gillespie, 2016; Mayer et al., 1995). Dans les entreprises, la CI aurait pour effet de modifier les comportements du confiant lorsqu'il travaille avec le mandant en facilitant la prise de risque (Mayer et al., 1995). Cette prise de risque se manifesterait par le biais de différents comportements regroupées sous le terme d'« *Organizational citizenship behaviors* » (OCB) (Mayer & Gavin, 2005; Wong, Ngo, & Wong, 2006). Un manque de CI entre les membres d'une équipe serait également lié à une augmentation des comportements déviants (Colquitt et al., 2007), une diminution de l''effort d'équipe (De Jong & Elfring, 2010) ou encore à une diminution de la satisfaction des membres de l'équipe (Dirks & Ferrin, 2002).

Au niveau du comportement du confiant, une diminution de la CI dans le mandant s'accompagne généralement d'une augmentation du temps et des ressources consacrées par le confiant à la supervision du mandant (*Cf.* Figure 26), réduisant ainsi ses performances sur les autres tâches qui lui sont attribuées (Colquitt et al., 2007; De Jong & Elfring, 2010; McAllister, 1995). Dans la littérature

portant sur la prise de décision certains auteurs considèrent que la relation de confiance favorise la satisfaction (Driscoll, 1978) et l'action (Jarvenpaa et al., 1998) des individus.

Le résultat le plus largement repris dans la littérature est le lien entre la CI et la performance (*Cf.* Figure 26). Que la performance corresponde à un rendu d'équipe ou à une action personnelle, un niveau élevé de CI semble modifier positivement cette dernière. Cependant, différentes méthodes permettent de mesurer la performance et la force du lien entre CI et performance est différente selon les méthodes utilisées ce qui était noté par De Jong et al. (2016) dans leur méta analyse de 2016 « *Lorsque la performance est mesurée de manière objective, la relation entre la confiance et la performance est plus faible que lorsque la performance est mesurée de manière subjective* **»** (De Jong et al., 2016, p. 31)[33].

Différentes méta-analyses prenant en compte la CI et la performance ont été effectuée dans le domaine de la CI dans le leader et de la performance d'équipe et concluent à un lien entre les deux facteurs (Colquitt et al., 2007; De Jong et al., 2016; Dirks & Ferrin, 2002). Ces résultats, généralement obtenus à partir de données issues de questionnaire semblent être moins reproductibles, en prenant en compte des données non auto-déclarées (Dirks & Ferrin, 2002). Ceci est potentiellement due au fait que la mesure de la performance d'une équipe peut dépendre des actions du confiant ou du mandant mais peut également dépendre des actions réalisées par le confiant et le mandant ce qui peut entrainer un biais d'analyse des données. Dans la littérature sur la CI, la performance est recueillie soit de manière qualitative, à l'aide de questionnaires par exemple, soit de manière quantitative. Le recueil des données qualitatives peut se faire soit de manière auto-déclarée (Dirks & Ferrin, 2002), soit en passant par le superviseur des participants (Mayer & Gavin, 2005) par exemple. Les mesures quantitatives de la performance ont beaucoup moins été utilisées dans la littérature du fait du faible nombre d'expérimentations en laboratoire dans le champ de recherche sur la CI (De Jong et al., 2016; Dirks & Ferrin, 2002). Quantitativement, la performance peut se traduire par différentes mesures comme un calcul de point sur le rendement d'une équipe (Boies, Fiset, & Gill, 2015), le nombre de jours séparant la soumission d'un rapport à une date limite (Crisp & Jarvenpaa, 2013) ou encore le temps moyen de départ d'un avion (Schneider et al., 2009). La mesure de la performance, qu'elle soit qualitative ou quantitative est donc largement sujette à différents biais qui entrainent des résultats non généralisables.

[33] « *the trust-performance relationship is substantially weaker when performance was measured objectively than when it is measured subjectively* **»** (De Jong et al., 2016, p. 31)

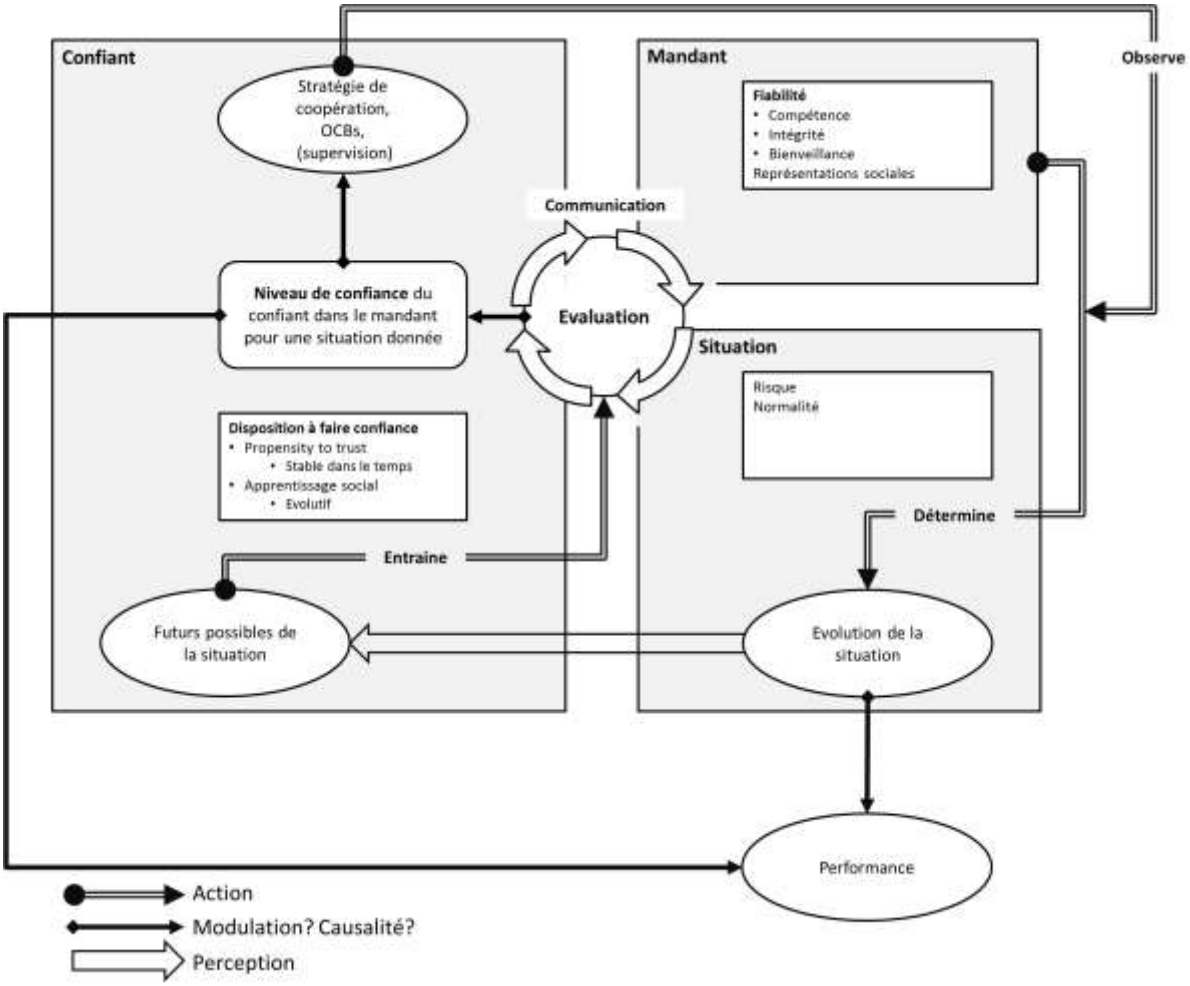


Figure 26 : Modèle complet reliant les trois entités et prenant en compte les caractéristiques de chacune d'entre elles.

e. Différences entre un modèle dynamique et un modèle statique

Les caractéristiques et les liens du modèle réalisé précédemment correspondent au fondement de la confiance dynamique. Dans ce type d'approche, lorsque le mandant fait une action le confiant peut voir évoluer la situation ce qui permet une réévaluation, *in situ*, des nouveaux futurs possibles, et une modulation du niveau de fiabilité à accorder au mandant. Lorsque le niveau de confiance est faible la stratégie de supervision permet de donner au confiant des informations, en temps réel sur les actions mises en place par le mandant pour faire évoluer cette situation, et, par extension, permettent au confiant d'évaluer plus rapidement les nouveaux futurs possibles. Dans ce type d'approches, le niveau de CI n'est pas figé mais évolue au cours du temps avec la fréquence et la qualité des échanges entre le confiant et le mandant (Lewis & Weigert, 1985; Shapiro et al., 1992) jusqu'à ce que la situation ne nécessite plus de collaboration.

Dans l'approche d'une confiance dynamique, ce sont les changements de la situation engendrés par les actions du mandant qui entrainent une réévaluation par le confiant de la fiabilité du mandant et, par conséquent un réajustement du niveau de CI. Dans l'approche dynamique, le niveau de CI initial est basé sur la perception subjective qu'à le confiant de la fiabilité du mandant alors que le niveau final de CI est basé sur des analyses objectives de la fiabilité du mandant et sera, par conséquent,

possiblement différent. Du fait de cette possible différence entre le niveau de CI initial et le niveau de CI final, avec une approche dynamique, il semble difficile d'étudier les conséquences comportementales d'un manque ou d'un excès de CI. En effet, dans le cas d'expérimentations réalisées en laboratoire, le niveau de CI induit en début d'expérimentation pourrait être différent du niveau de CI présent lors du recueil des données comportementales. Ainsi, afin de pouvoir répondre à la problématique de cette thèse il semble nécessaire d'empêcher que le niveau de CI évolue entre le début et la fin d'une expérimentation ce qui correspond à une approche de type confiance rapide. En effet, comme vu précédemment (*Cf.* 2.3 «E. La CI statique ou confiance rapide »), dans la confiance rapide, le niveau de CI n'évolue pas au cours du temps ce qui fait que le niveau initial et le niveau final de CI sont similaires.

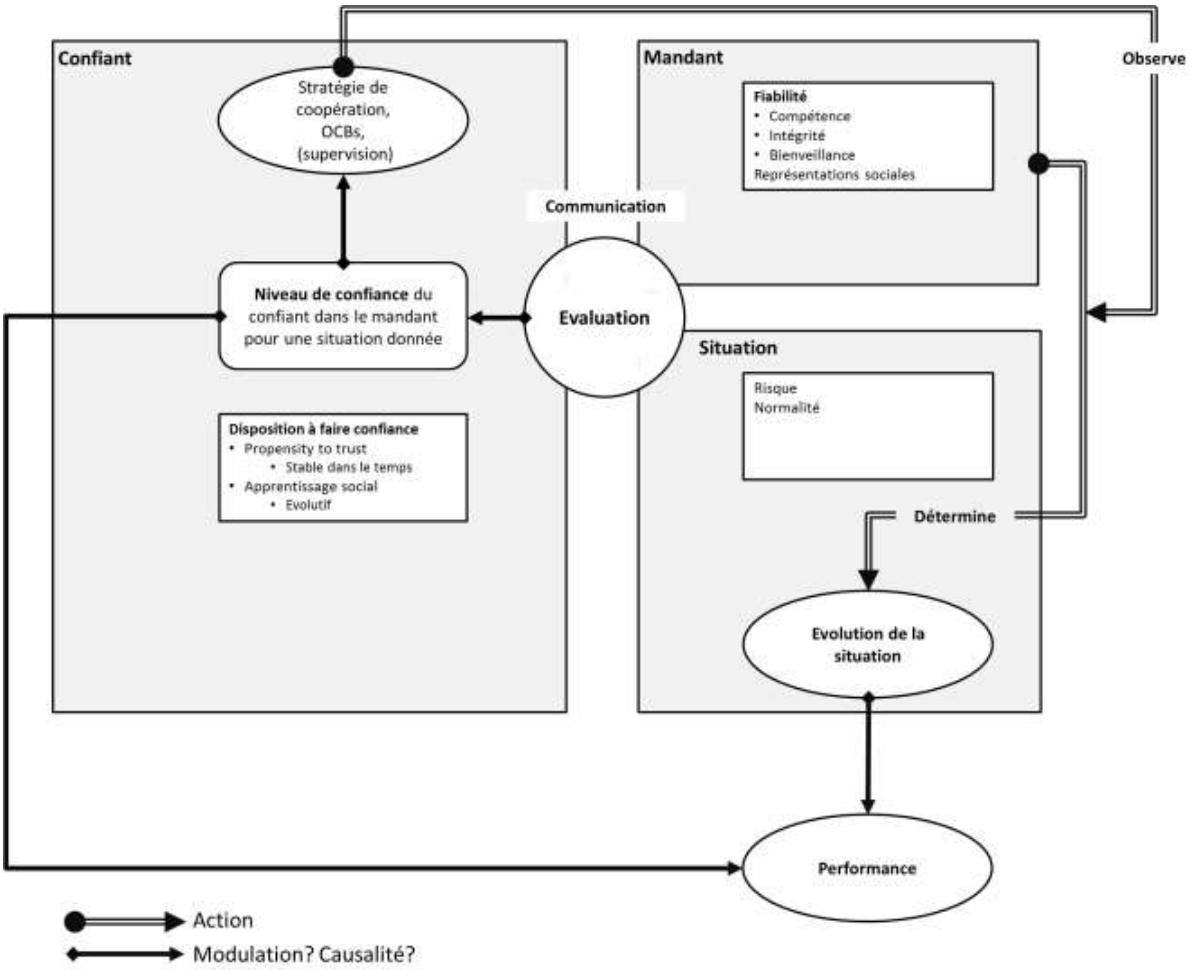


Figure 27 : Adaptation du modèle à la confiance rapide de la confiance.

Cette version en confiance rapide (*Cf.* Figure 27) permet donc de de s'assurer que le niveau de CI sera similaire tout au long de la relation et sera donc utilisée pour les expérimentations présentées dans ce manuscrit. Dans cette ve rsion du modèle le confiant évalue la fiabilité du mandant. Cette évaluation de la fiabilité du mandant, par le biais des RS, permet de mettre en place le niveau initial de CI présent dans la relation. Ce niveau initial de CI module le comportement du confiant dans la relation. Si le niveau de CI initial est faible le confiant peut superviser le mandant et ainsi évaluer l'évolution possible de la situation cependant, quelles que soient les actions effectuées par le mandant la situation sera terminée à la fin d'un cycle. De fait, il devient impossible pour le confiant

d'évaluer quantitativement la fiabilité du mandant pour une tâche donnée. Ce type de modèle correspond bien aux modèles de confiance rapide étudiés dans les recherches portant sur les équipes éphémères formées d'experts de différents domaines (Meyerson et al., 1996). Dans ce type d'équipe, du fait du manque de connaissances, la supervision ne permet pas au confiant d'évaluer les différents futurs possibles déterminés par les actions du mandant. De fait le niveau de CI initial présent dans la relation correspond au niveau de CI final de la relation.

6. Méthodes d'inductions et études sur la confiance

Les éléments vus dans les parties précédentes correspondent aux définition et modèles mobilisés dans les différents champs de la littérature relatifs à la confiance. Bien que la plupart des définitions proviennent de recherches théoriques, la majorité des modèles ont été testés empiriquement. Afin d'étudier les facteurs de mise en places de différents niveaux de CI mais également les conséquences comportementales de ces différents niveaux de CI, deux types d'approches empiriques sont généralement employées :

- l'approche par questionnaires (De Cremer, Van Dijke, Schminke, De Schutter, & Stouten, 2018) ;
- l'approche en laboratoire (Schilke & Huang, 2018).

L'approche utilisée, tout comme les méthodes d'induction en laboratoire, sont fonction du champ de recherche. Dans cette partie il est proposé d'étudier les méthodes d'induction utilisées en management et dans la théorie des organisations, en psychologie et neuroscience puis en informatique. Ces disciplines ont été choisies car les modes d'induction de confiance y sont extrêmement différents et semblent être généralisés au champ correspondant.

A. Management et organisation

Dans le champ d'étude portant sur le management et les organisations, l'approche par questionnaire est prépondérante. De fait, que ce soit dans les méta-analyses portant sur la performance d'équipe ou dans les méta-analyse portant sur la confiance dans le leader un manque d'études réalisées en laboratoire ressort de façon significative (De Jong et al., 2016; Dirks & Ferrin, 2002). Bien que des questionnaires permettant d'étudier le niveau de confiance général d'un individu ou son niveau de *propensity to trust* semblent faire consensus (Mayer & Davis, 1999), des questionnaires spécifiques sont mis en place afin de réaliser la plupart des études. Ainsi, les études réalisées à l'aide de questionnaires peuvent analyser des variables similaires en les évaluant à l'aide de questions différentes ce qui peut apporter des résultats différents.

Dans le champ d'étude portant sur le management et les organisations l'approche en laboratoire se fait généralement par l'induction de seulement deux niveaux de CI (un niveau de CI faible et un niveau de CI élevé). Ces deux niveaux de CI sont directement induits par l'expérimentateur en début d'expérimentation (Dirks, 1999) ou en cours d'expérimentation (Ferrin & Dirks, 2003). Pour induire ces deux niveaux différents de CI, l'expérimentateur décrit longuement et en utilisant des exemples, aux membres d'une équipe, la fiabilité d'autres membres de l'équipe. Afin d'induire un niveau de CI élevé le membre de l'équipe à décrire est caractérisé comme étant fiable et/ou ayant bien effectué la

tâche, alors que pour induire un niveau de CI faible il est caractérisé comme étant non fiable et/ou comme ayant mal effectué la tâche demandée (Dirks, 1999; Ferrin & Dirks, 2003).

Ces deux approches utilisées en management et en science des organisations semblent avoir un problème lié à la fiabilité de l'induction et/ou à la fiabilité des données recueillies. Dans les études effectuées à l'aide de questionnaire, l'expérimentateur ne peut pas vérifier la fiabilité des réponses des participants. Or, par exemple, dans les études portant sur la performance du leader, les membres d'une équipe peuvent être amenés à surestimer leur leader afin de ne pas avoir de contreparties néfastes. Dans les études effectuées en laboratoire l'induction n'est pas contrôlée (aucune échelle de mesure ne permet au confiant d'indiquer le niveau de confiance qu'il a dans le mandant) ; de fait, il est impossible de s'assurer que les inductions aient fonctionné comme attendue.

Dans les études réalisées en management les membres des équipes travaillent et interagissent ensemble pendant toute la durée de l'expérimentation. Dès lors, le niveau de CI initialement induit par l'expérimentateur peut ne pas être similaire au niveau de CI présent à la fin de l'expérimentation ce qui peut entraîner un biais de mesure. Enfin, dans ces expérimentations réalisées en laboratoire, le participant n'effectue sa tâche que dans une seule condition (confiance ou non confiance) et avec un seul coéquipier ou groupe de coéquipiers ce qui peut entrainer certains biais liés au recueil de données. En effet, dans les expérimentations réalisées en management, le fonctionnement de l'induction n'est pas contrôlé, par conséquent, il est possible que certains individus devant réaliser l'expérimentation avec un niveau de CI faible la réalisent, en réalité, avec un CI élevé (et inversement).

Exemple d'expérimentation en laboratoire dans la littérature managériale

Dans la littérature managériale, la première expérimentation en laboratoire avec induction de confiance a été réalisée par Dirks en 1999. Dans cette expérimentation, Dirks induit chez chaque participant différents niveaux de CI dès le début de l'expérience. Il propose l'hypothèse que la CI module la performance des équipes éphémères au niveau individuel et collectif (Dirks, 1999). Pour tester cela, 42 équipes sont mobilisées. Chacune des équipes compte trois participants qui travaillent ensemble pour construire une tour où le plus grand nombre possible de blocs doit être placé, individuellement et collectivement. Cette tâche établit une forte interdépendance entre les tâches de chacun afin de maximiser l'impact de la confiance interpersonnelle. Seule la CI varie à travers les scénarios proposés à chaque participant concernant leurs partenaires. Certains partenaires sont présentés comme fiables (pour induire une CI forte) et d'autres comme non fiables (pour induire une CI faible). Trois essais sont réalisés et seuls le deuxième et le troisième sont pris en considération. Les résultats n'indiquent pas un impact direct de la CI sur la performance du groupe, contrairement à ce que la littérature suggère, mais un effet indirect, en tant que « modérateur » : « *la confiance semble influencer la manière dont la motivation est convertie en processus et performances de groupe de travail* » (Dirks, 1999, p. 2)[34]. Cependant, le participant peut reconsidérer son évaluation initiale de la fiabilité du partenaire en tenant compte des performances réalisées durant le premier et le

[34] « *trust seems to influence how motivation is converted into work group processes and performance* »(Dirks, 1999, p. 2)

deuxième essai. La détermination du niveau de CI peut donc se réaliser en partie sur des évaluations rationnelles. Cette évaluation rationnelle s'apparente au mécanisme de *person-based-trust* mis en place dans le cadre d'une CI évolutive.

En 2003, Ferrin et Dirks améliorent le procédé d'induction de la CI en évitant toute interaction directe et durable entre le participant et son partenaire (Ferrin & Dirks, 2003). Tous les participants sont rassemblés dans une salle pour effectuer une tâche mais chacun travaille sur un PC sans savoir qui est le partenaire qui lui est assigné. Les participants ne se rencontrent pas, ce qui limite le développement des interactions. Ainsi, ils ne peuvent évaluer la fiabilité de leur partenaire *in situ*, ce qui pourrait avoir un impact sur le niveau de CI initialement induit. Cependant, dans cette expérimentation les participants n'ont pas tous eu la même induction du niveau de confiance. En effet, dans cette expérimentation, le niveau de confiance a été induit après une première tâche collaborative. Pour chaque participant, ce niveau de CI (faible ou fort), était induit par un rapport manuscrit, qui, pour être plus crédible et précis utilisait des faits survenues dans la première phase de l'expérimentation. Cette étude de Ferrin et Dirks en 2003 met en évidence l'importance de maîtriser l'induction de la CI dans un protocole expérimental de façon à limiter les possibilités d'une estimation de la fiabilité d'autrui fondée sur les interactions continues (i.e. le mécanisme de *person-based-trust*).

B. Psychologie et neuroscience

Les études menées en psychologie et neurosciences utilisent dans la grande majorité des cas, la méthode expérimentale. Contrairement aux études réalisées dans le domaine du management, dans les études réalisées en psychologie et neuroscience, les participants réalisent des tâches très courtes avec un grand nombre de coéquipiers de différents niveaux de CI. Le mécanisme d'induction qui semble faire consensus dans ces littératures est un mécanisme d'induction par visages, qu'ils soient réels et tirés de vraies photographies (Klapper, Dotsch, Van Rooij, & Wigboldus, 2016; Rule, Krendl, Ivcevic, & Ambady, 2013; Slepian & Ames, 2016; Willis & Todorov, 2006) ou créés ou modifiés par ordinateur (Klapper et al., 2016; Marzi, Roghi, Ottonello, Cincotta, & Viggiano, 2014; Oosterhof & Todorov, 2008; Schul, Mayo, & Burnstein, 2004; Todorov, Olivola, Dotsch, & Mende Siedlecki, 2015). Dans ces études, la forme et les traits du visage (Oosterhof & Todorov, 2008) ou encore le plissement des yeux (Schul et al., 2004) sont autant de données permettant de mettre en place le niveau de CI présent entre le confiant et mandant. Les différences entre les visages permettent de modifier la fiabilité perçue, et, par conséquent, la mise en place du niveau de CI initial. Ce type d'induction est souvent suivie par une méthode de renforcement (Schul et al., 2004) du niveau de confiance induit et d'une échelle de lickert permettant de recueillir la fiabilité perçu du participant (Klapper et al., 2016; Willis & Todorov, 2006).

De manière similaire aux méthodes utilisées en management, le mécanisme d'induction par visage se base sur les attributs de fiabilité du mandant. Cependant, plusieurs points diffèrent entre les mécanismes d'induction en management et en psychologie. Tout d'abord, la modélisation informatique des visages en trois classes de niveau de CI (niveau de CI faible, niveau de CI neutre et niveau de CI élevé) découlent des travaux de Todorov et Oosterhof en 2008. Toutes les bases de données de visages sont donc réalisées sur les mêmes principes de modifications, standardisés, d'une image « de référence ». Pour réaliser une base de données, l'expérimentateur utilisent des photographies de visages « quelconques » et y appose différentes formules mathématiques afin d'en

grossir ou réduire les traits (plissement et écartement des yeux, taille des joues…). Chaque photographie utilisée est alors « transformée » en plusieurs photographies différentes qui correspondent au nombre de niveaux de CI souhaités. Bien que les photographies « de base » puisses être différentes, le traitement de ces photographies rend ce mécanisme d'induction plus standardisé que les mécanismes d'inductions utilisés en management.

Deuxièmement, les échelles de lickert permettent de vérifier l'induction et de s'assurer de la présence de différents niveaux de confiance perçus par le participant. Enfin, en psychologie et neurosciences les tâches sont extrêmement courtes (généralement inférieures à une seconde) et il n'y a aucune interactions entre le participant et le mandant qui lui est présenté ce qui ne permet pas au niveau de confiance initial d'évoluer au cours du temps.

Ce type d'induction pourrait donc bien correspondre aux besoins expérimentaux de cette thèse, cependant, de récentes études suggèrent que ce type d'induction est peu fiable (Rule et al., 2013; Todorov et al., 2015). En effet, les visages ont été réalisés sans prendre en compte les groupes sociaux des participants (confiant) ce qui fait que la force d'induction n'est pas homogène dans la population. De plus, dans la littérature, ce type d'induction est majoritairement utilisé dans les recherches en psychologie portant sur des tâches très courtes et rien ne permet d'indiquer que ce type d'induction fonctionnerait pour des tâches collaboratives de plus longue durée.

C. Informatique

Les recherches effectuées en informatique sont essentiellement expérimentales. Dans les recherches menées sur les robots-conversationnels les chercheurs utilisent des avatars plus ou moins souriants ou encore des photos (Elkins & Derrick, 2013; Przegalinska, Ciechanowski, Stroz, Gloor, & Mazurek, 2019) ce qui permet des mécanismes d'induction proches des ceux utilisés en psychologie et neuroscience. Dans les recherches menées notamment dans le e-commerce, l'induction de confiance se fait à l'aide de pourcentage de fiabilité que la communauté a accordé à un vendeur (Ba & Pavlou, 2002; Resnick, Zeckhauser, Swanson, & Lockwood, 2004). Dans ce type de recherche le participant doit effectuer des actes d'achat sur la base soit d'un simple pourcentage soit d'un pourcentage allié au nombre d'avis positifs ou de nombre d'avis négatifs.

Comparé aux mécanismes d'induction présents dans les autres disciplines l'induction par pourcentage de fiabilité semble la plus facile à mettre en œuvre. Cependant, comparé aux études réalisées en psychologies dans lesquelles l'induction est généralement vérifiée à l'aide une échelle de lickert permettant de recueillir la fiabilité perçu du participant, dans ce type de recherche aucun mécanisme de vérification de l'induction ne semble être utilisé.

7. Conclusion

Toutes les théories et modèles présents dans la littérature décrivent la confiance comme étant un réducteur d'incertitude et un élément clef du bon fonctionnement des équipes et des organisations. Un bon niveau de confiance permettrait, notamment par le biais d'une modulation du comportement des individus et de leur perception du risque, de maximiser la performance des équipes. *A minima* trois entités sont nécessaires pour qu'un lien de confiance se mette en place, un

confiant, un mandant, et une situation. La relation de confiance peut être résumée par la relation « A trusts B to do X » (Hardin, 1993). Bien que les différentes théories sur la confiance se basent sur la littérature psychologique (Deutsch, 1958) et sociologique (Simmel, 1950) différents axes de recherche, étudiant une ou plusieurs entités, ont été mis en place. De fait, selon l'axe d'étude il semble préférable d'utiliser l'une ou l'autre des littératures et c'est ce qui sera fait tout au long du manuscrit en s'appuyant sur le constat suivant :

- La littérature portant sur l'économie et les échanges commerciaux oriente ses recherches sur la notion de risque et de probabilité. Dans la suite de ce manuscrit cette littérature sera dénommée **littérature économique** et sera utilisée dans l'étude portant sur lien entre niveau de CI, situation et prise de décision.
- La littérature portant sur les relations de confiance entre un opérateur humain et un système informatique ou automatisé oriente ses recherches sur les caractéristiques propres au confiant et plus particulièrement sur la confiance en soi du confiant. Dans la suite de de ce manuscrit cette littérature sera dénommée **littérature informatique** et sera notamment utilisée dans l'étude portant sur le comportement d'un opérateur lorsqu'il travaille avec un système automatisé.
- La littérature portant sur le management et les organisations axe principalement ses recherches sur les caractéristiques propres au mandant, comme les attributs de la fiabilité et les caractéristiques propres au confiant telles que la propension individuelle à faire confiance ou la confiance par apprentissage social. Dans la suite de ce manuscrit cette littérature sera dénommée **littérature managériale** et sera mobilisée dans toutes les études.

Dans les différentes littératures aucun modèle faisant intervenir les trois entités ne semble faire consensus ; cependant toutes les littératures s'accordent sur des modèles en deux parties, la première correspond à la mise en place du niveau de CI et la seconde aux conséquences engendrées par ce niveau de confiance. Le confiant attribuerait au mandant un niveau de CI en évaluant sa fiabilité (première partie). Ce niveau de CI modifierait le comportement du confiant dans la relation (deuxième partie).

Ces modèles décrivent le processus permettant la mise en place du niveau de CI mais n'indiquent pas comment ce niveau de CI évolue au cours du temps. Sur l'évolution du niveau de CI, la littérature s'est scindée en deux grandes orientations. La première part du principe que la CI est un processus évolutif et que le niveau de CI entre les membres d'une équipe ne peut qu'évoluer au cours du temps. La deuxième, prénommée confiance rapide, considère que dans certains types d'équipes, notamment éphémères et formées d'experts, le niveau de CI ne va pas évoluer au cours du temps.

Dans la littérature portant sur la CI comme étant un processus évolutif, après la mise en place du niveau de confiance initial le confiant évalue *in situ* la fiabilité du mandant et ajuste le niveau de confiance. Pour cette partie de la littérature, lorsque les membres d'une équipe ont le temps d'apprendre à se connaitre, le niveau de CI ne cessera de fluctuer au cours du temps ce qui entraine que le niveau initial de CI sera différent du niveau de CI final de la relation. Le champ de la littérature portant sur la confiance rapide quant à lui considère que, dans certains types d'équipes, dont les membres n'ont pas le temps ni la capacité d'apprendre à se connaitre, (telles que les équipes éphémères médiées par ordinateurs, les STATs…) la CI ne peut pas évoluer au cours du temps. Ceci est notamment dû au fait que dans ce type d'équipes il est impossible (par manque d'expertise, de

temps, de moyens de communication approprié…) pour le confiant d'évaluer *in situ* la fiabilité du mandant. Pour cette partie de la littérature le niveau de CI initial présent dans la relation devrait donc être identique au niveau de confiance final.

Dans la suite de ce manuscrit le modèle de confiance rapide explicité dans cette partie sera utilisé. Dans ce modèle le confiant évalue la fiabilité du mandant pour réaliser une tâche donnée. Ceci permet de mettre en place le niveau de CI (faible ou élevé) présent dans la relation. En l'absence de réévaluation possible du nouvel état de la situation ce niveau de CI n'évolue pas au cours du temps et le niveau de CI de base sera donc le niveau de CI final de la relation. Cette approche permet de bloquer le cycle d'évolution de la CI et donc de maitriser le niveau de CI induit du début à la fin d'une tâche expérimentale. Finalement, ce type d'approche ressemble à ce qui est fait expérimentalement dans la littérature en psychologie, à savoir, des tâches très courtes dans lesquelles aucune situation n'évolue et donc dans lesquelles le niveau de CI induit en début de tâche est le niveau de CI final.

Points clés

Pour qu'il y ait confiance il faut, *a minima*, trois parties : un confiant, un mandant et une situation. Dans une relation de confiance le confiant est amené à faire confiance au mandant car l'apport de l'autre peut lui amener un gain. Les différentes littératures orientent leurs recherches sur une ou plusieurs de ces entités, notamment, la littérature en économie axe ses recherches sur les caractéristiques de la situation quand la littérature managériale oriente ses recherches sur les caractéristiques propres au confiant et au mandant.

Cette différence dans les littératures entraine qu'aucune définition ni modèle n'aient fait consensus. Dans la littérature portant sur les organisations et le management beaucoup de modèles ont été réalisés sur la dynamique d'une relation de CI (Costa et al., 2018; Mayer et al., 1995; Mayer & Gavin, 2005; McAllister, 1995; Shawn Burke et al., 2007). Ces différents modèles semblent découler des travaux réalisés par Morton et Deutsch en psychologie (Deutsch, 1958) et Simmel en sociologie (Simmel, 1950; Möllering, 2001) et sont tous composés de deux parties distinctes : la première partie correspond à l'étude de la mise en place du niveau de confiance (les *antecedents*) et la seconde partie correspond aux conséquences du niveau de confiance (les *outcomes*). Bien que certaines études s'orientent sur l'une ou l'autre des parties (Doney et al., 1998; Sendjaya & Pekerti, 2010; Williamson, 1993), tous les modèles prenant en compte les deux parties, indiquent que des caractéristiques propres au confiant définissent le niveau de confiance initial, et que ce niveau de confiance détermine la façon (les comportements) dont le confiant agira dans la relation. Du fait de l'absence de modèle faisant consensus et de l'absence de modèle associant les trois entités, une analyse de la littérature a été effectuée afin de proposer le modèle permettant de renseigner la problématique de la thèse.

Dans la littérature portant sur le management et la théorie des organisations très peu d'expérimentations ont été réalisées en laboratoire et la méthode par questionnaire semble être la plus utilisée. Le manque d'études réalisées en laboratoire semble provenir du manque de méthode fiable d'induction. Dans cette littérature, le niveau d'induction ne semble pas être maitrisé et peut changer au cours de l'expérimentation (souvent longue dans cette littérature) ce qui peut entrainer un biais quant à l'analyse des résultats et à leur interprétation.

Dans d'autres littératures différents matériels d'induction sont utilisés. En psychologie des visages réels (modifiés par ordinateur) ou entièrement créés par ordinateurs sont utilisés. Cependant, ce type d'induction est utilisé pour des tâches extrêmement courtes et rien n'indique que ces inductions fonctionneraient pour des tâches longues. En informatique l'utilisation du niveau de fiabilité permet d'induire différents niveaux de confiance. A notre connaissance ce type d'induction n'a pas été testé dans des recherches portant sur des collaborations homme-homme, cependant, comme pour l'induction par visage, ce type d'induction semble être utilisé pour des tâches courtes (acte d'achat…) et n'a jamais été testé pour du collaboratif.

Résumé général des deux premiers chapitres et perspectives

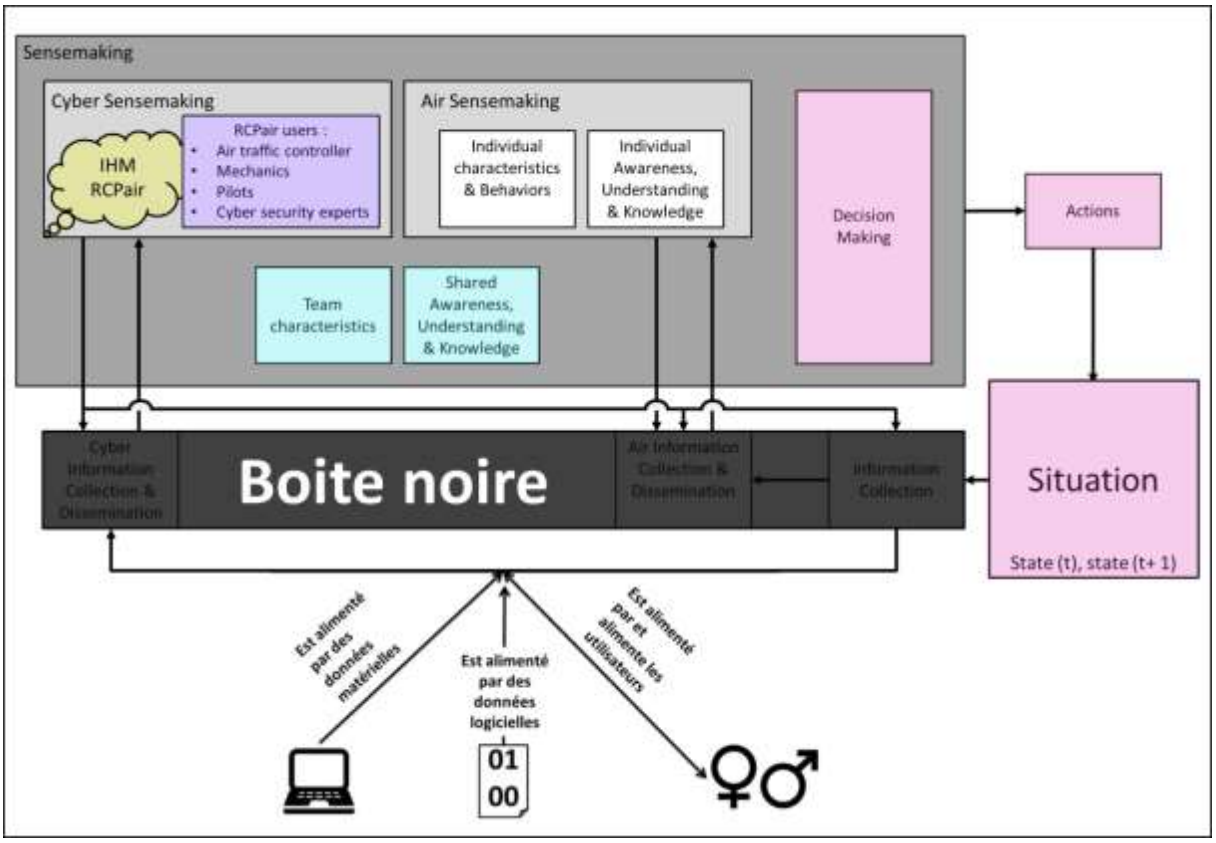
L'augmentation du nombre de systèmes interconnectés a entrainé une augmentation du nombre de cyber-menaces sur les infrastructures civiles et militaires. Afin de réagir efficacement à une attaque cyber l'AA, va, dans les années à venir, se doter d'une compétence cyber nommée ici RCPair. Le but de cette RCPair sera de donner une représentation de l'état cyber des systèmes de l'AA et d'afficher les infrastructures infectées ainsi que les cyber-vulnérabilités potentielles. Cette RCPair, qui n'est pas encore déployée ni totalement définie, sera mise en place dans les C2air et entrainera probablement une remise en cause de la chaine d'information de ces C2air.

Les C2air, comme tous les C2, ont pour rôle principal de prendre des décisions permettant d'agir sur des situations spécifiques afin d'améliorer l'état de ces situations (par exemple lors d'un incendie le rôle du C2 est de prendre des décisions permettant de limiter la propagation de l'incendie voir de stopper l'incendie). Pour réaliser cette mission, le C2 dispose d'opérateurs humains et technologiques collaborant ensemble. L'organisation des C2 est dépendante de la nature ainsi que de la complexité de la mission. De fait, les opérateurs des C2 peuvent devoir collaborer, soit uniquement avec des personnes qu'ils connaissent (ceci renvoyant au concept de *conflicted C2*) soit avec des personnes qu'ils connaissent et d'autres qu'ils ne connaissent pas (ceci renvoyant au concept de *Edge C2*). En termes purement organisationnel, il est donc impossible d'anticiper quelles seront les problématiques liées à l'arrivée du composant cyber dans les C2.

Outre cette base organisationnelle qui est fonction de la mission, les C2 ont une base fixe qui est stable dans le temps et commune à tous. Ainsi, pour fonctionner les C2 sont tous dotés d'opérateurs (humain et matériel) qui reçoivent des informations provenant de la situation. Un opérateur est doté de caractéristiques qui lui sont propres et qui vont lui permettre de comprendre la situation d'une manière qui lui est propre. Cette compréhension de la situation est mise en commun avec la compréhension de la situation des autres opérateurs du C2 afin de « créer » une compréhension de la situation (de groupe) propre au C2. Sur la base de cette compréhension commune de la situation, les opérateurs prennent une décision permettant d'agir sur la situation.

Une analyse du besoin effectuée auprès d'opérationnels de l'AA ainsi qu'une mise en commun du concept de C2 avec le concept de RCPair tend à montrer que l'arrivée de la RCPair ne modifiera probablement pas le fondement organisationnel du C2air. La RCPair sera un système, formé d'une IHM et d'un ou plusieurs opérateurs humains, déployé en complément des autres systèmes présents dans le C2. Ces caractéristiques de la RCPair sont strictement identiques aux caractéristiques des autres systèmes présents dans les C2air à la différence près que, la RCPair modifiera la notion de véracité des informations reçues par les différents opérateurs du C2. En détectant une anomalie cyber sur des données reçues dans le C2air la RCPair remettra en cause la confiance que les opérateurs accordent à toutes les informations reçues par les différents opérateurs du C2air. Ces informations peuvent être transmises par un système informatique à l'opérateur RCPair (en jaune et violet sur la figure ci-dessous), ou par l'opérateur RCPair à un autre opérateur humain du C2 (en bleu sur la figure ci-dessous). Quelles que soient leur nature ou leur provenance ces informations seront

ou non, prises en compte par les membres du C2 ce qui mènera à des décisions qui permettront d'agir sur une situation qui sera par nature plus ou moins incertaine C2 (en rose sur la figure ci-dessous).



Les premiers chapitres ont donc permis la formulation de la problématique qui sera étudiée dans cette thèse :

Quelles sont les conséquences comportementales d'un manque ou d'un excès de confiance interpersonnelle sur les opérateurs travaillants dans la RCPair recevant des données soumises à une forte incertitude ?

Dans cette problématique apparaissent deux parties. Une des parties est opérationnelle et axée sur la RCPair (« *les opérateurs travaillants dans la RCPair recevant des données soumises à une forte incertitude* »). Pour renseigner cette partie opérationnelle de la thèse, le schéma présenté sur la figure ci-dessus est utilisé tout au long de ce manuscrit. Chaque étude présentée ici se réfère à une ou plusieurs composantes de ce schéma et permet d'émettre des recommandations sur différents points de la RCPair. La deuxième partie est plus académique et se réfère à l'étude des

comportements engendrés par différents niveaux de confiance (« *Quelles sont les conséquences comportementales d'un manque ou d'un excès de confiance ?* »).

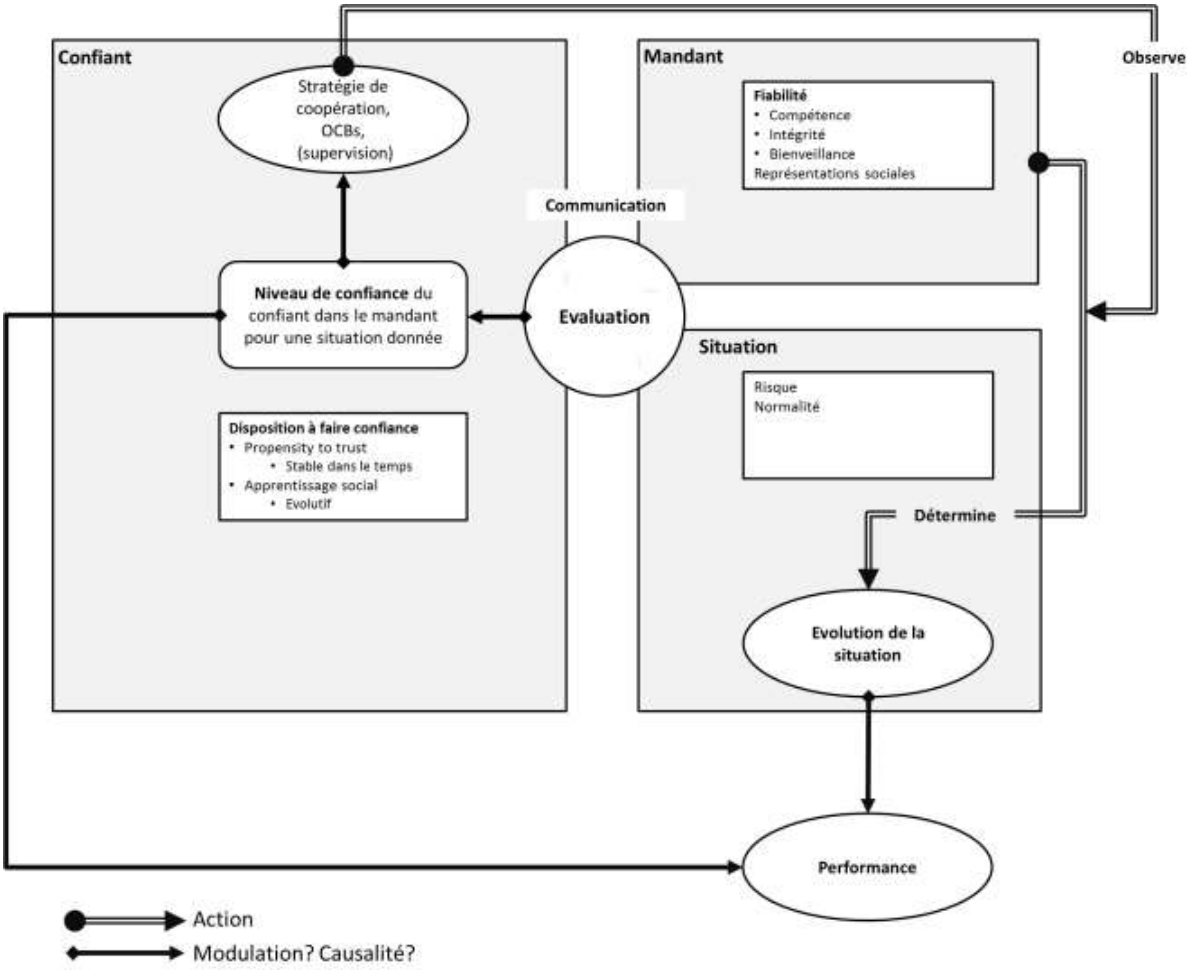
Afin de pouvoir poser les bases de cette deuxième partie, un état de l'art portant sur la confiance a été effectué. Cet état de l'art a permis de constater que la confiance était une relation entre trois entités, un confiant, un mandant et une situation. Pour qu'il y ait confiance il faut que le confiant ait besoin du mandant pour agir sur la situation. Bien que ces trois entités semblent faire consensus dans les différents champs, elles sont cependant étudiées de manière séparées dans la littérature. Les études portant sur le rôle de la situation dans la mise en place du niveau de confiance sont réalisées en majorité dans la littérature économique, alors que les études portant sur les caractéristiques du confiant et du mandant dans la mise en place du niveau de confiance sont réalisées en majorité dans la littérature managériale.

Le fait que le rôle de chacune des entités dans la mise en place du niveau de confiance initial soit étudié dans des littératures différentes entraine qu'aucun modèle ne fasse consensus. Ainsi, les différentes littératures s'accordent uniquement sur le fait que les trois entités permettent la mise en place d'un niveau de confiance et que ce niveau de confiance entraine une modulation des comportements. Ainsi, afin d'étudier les conséquences comportementales d'un manque ou d'un excès de confiance il était nécessaire d'avoir un *modèle* permettant de comprendre la mise en place et les conséquences de la confiance. Pour cela un modèle a été construit sur la base des différentes littératures existantes.

Ce modèle traduit notamment le fait que le niveau de confiance initial est mis en place par le confiant uniquement sur la base d'une évaluation subjective des attributs de la fiabilité du mandant à agir sur la situation (les RS). Une évaluation subjective des premières actions effectuées par le mandant permet ensuite de faire évoluer ce niveau de confiance initial. Ce modèle représente donc bien la confiance comme étant un processus dynamique évoluant au cours du temps. Ce type de confiance, mis en place dans des équipes formées de membres qui se connaissent et qui travaillent ensemble régulièrement serait prédominant dans des organisations de type *conflicted C2.*

Cependant, les C2 sont agiles et peuvent se « transformer » rapidement afin de pallier la complexité d'une mission. Dans les différents stades du C2 (autre que le *conflicted C2*) le nombre d'interactions éphémères entre personnes inconnues augmente. L'analyse de la littérature portant sur la CI entre les membres des équipes éphémères a montré que dans ce type de mission, un niveau de CI pouvait être mis en place et ne jamais évoluer. Ainsi, dans des relations éphémères, lorsqu'il est impossible pour le confiant d'évaluer *in situ* la fiabilité du mandant, une relation de type confiance rapide se met en place. Dans ce type de relations, le niveau de CI n'évolue pas au cours de la relation. Le modèle présenté précédemment a donc été affiné pour prendre en compte cette approche non évolutive de la confiance,

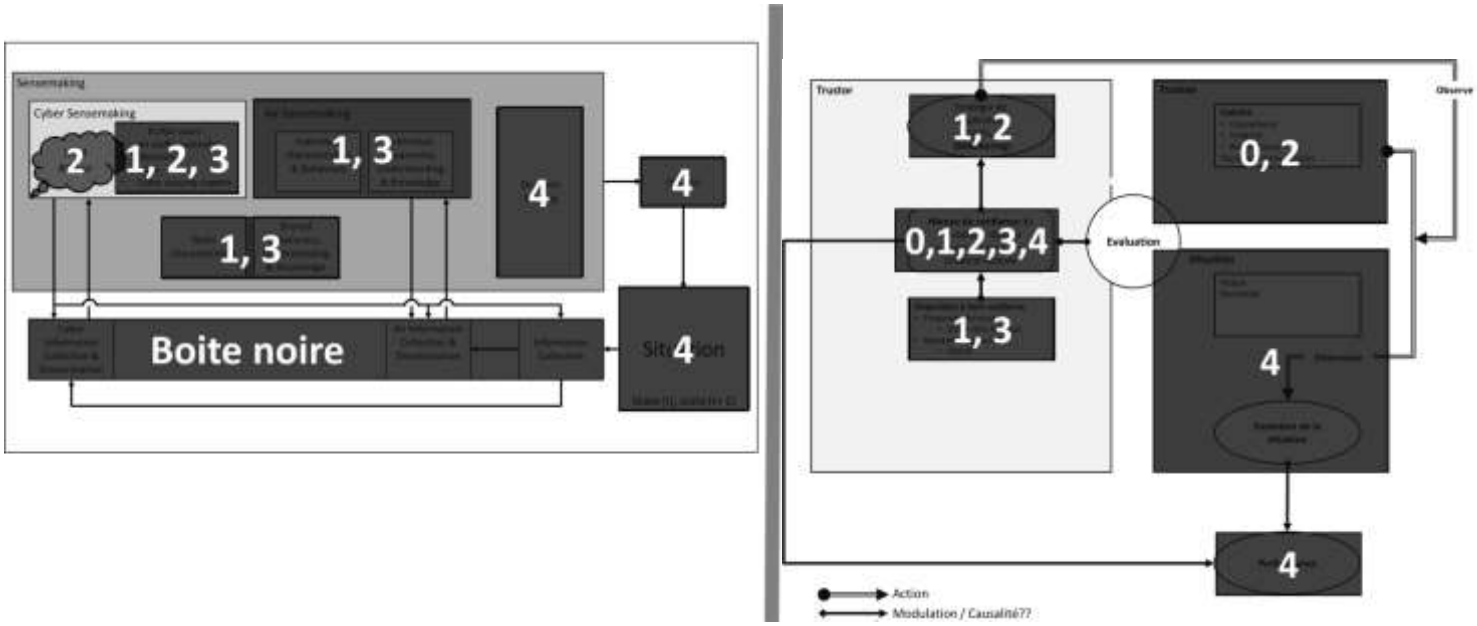
Cette approche non évolutive de la confiance est particulièrement intéressante dans l'étude des conséquences comportementales d'un manque ou d'un excès de confiance qui nécessite de maitriser le niveau de confiance du début à la fin de l'expérimentation ; en effet avec une approche non évolutive, en arrivant à induire différents niveaux de confiance à des opérateurs, il serait possible d'étudier le comportement de ces opérateurs en limitant le risque que le niveau de confiance induit ait pu évoluer au cours de l'expérimentation. C'est cette approche qui est utilisée dans cette thèse.



Au cours de cette thèse toutes les parties du modèle présenté ci-dessous ont été étudiées et les résultats ont été analysés sous l'angle de l'apport académique et sous l'angle de l'apport opérationnel. Toutes les expérimentations expliquent et font évoluer une partie distincte du modèle de confiance et permettent d'analyser l'impact de la confiance dans l'utilisation de la RCPair. La suite de ce manuscrit est divisée en plusieurs parties.

- Mise en place d'un matériel permettant d'induire différents niveaux de confiances CI aux opérateurs potentiels de la RCPair
    - Etude des caractéristiques propres au mandant (RS) dans la mise en place du niveau de confiance initial (0 sur la figure ci-dessous)
- Test de ce matériel d'induction par le biais d'un protocole expérimental
- Evaluation des conséquences d'un manque ou d'un excès de CI sur les futurs opérateurs de la RCPair
    - Etudes des caractéristiques propres au confiant (l'apprentissage social) sur son comportement mis en place dans une relation de confiance interpersonnelle (1 sur la figure ci-dessous)

- Evaluation des conséquences d'un manque ou d'un excès de confiance dans la machine sur les futurs opérateurs de la RCPair
    - Etudes des caractéristiques propres au mandant (l'influence des attributs de fiabilités quand le mandant est une machine ou quand le mandant est un humain) sur le comportement du confiant mis en place dans une relation de confiance (2 sur la figure ci-dessous)
- Evaluation des conséquences d'un manque ou d'un excès de confiance en soi sur les futurs opérateurs de la RCPair
    - Etudes des caractéristiques propres au confiant (la confiance en soi) sur le comportement du confiant mis en place dans une relation de confiance (3 sur la figure ci-dessous)
- Evaluation des conséquences d'un manque ou d'un excès de confiance interpersonnelle sur la prise de décision des opérateurs de la RCPair
    - Etudes des caractéristiques de la situation et du niveau de confiance (incertitude) sur la prise de décision du leader (4 sur la figure ci-dessous)



3 Etude de la possibilité d'induire de la CI chez les aviateurs cibles de la RCPair

Résumé du chapitre

Objectif : Identifier des éléments centraux des représentations sociales des futurs opérateurs de la RCP afin de pouvoir contrôler des niveaux de CI dans les expérimentations à venir.

Démarche : L'état de l'art réalisé au chapitre précédent montre qu'il est théoriquement possible d'induire et de maitriser l'induction de plusieurs niveaux de CI en utilisant les représentations sociales que le confiant se fait du mandant. Dans ce chapitre il est proposé, dans un premier temps, d'identifier les termes générateurs de CI sur une population large de l'AA afin de construire des paires de mots correspondant aux éléments centraux des RS censés induire différents niveaux de CI. Dans un second temps ces paires de mots sont testées sur une population ciblée et homogène (opérateurs potentiels de la RCPair) afin de vérifier qu'elles induisent bien différents niveaux de CI.

Conclusion : Il est possible d'induire et de maitriser l'induction de deux niveaux de CI différents (faible et élevé) aux potentiels opérateurs de la RCP en utilisant la méthode des représentations sociales.

Chapitre 3 : Etude de la possibilité d'induire de la CI chez les aviateurs cibles de la RCP

1. Introduction et cadre théorique

Afin de réaliser des études en laboratoire permettant de déterminer les conséquences d'un manque ou d'un excès de CI il est nécessaire d'induire et de maitriser l'induction de différents niveaux de CI. Une analyse du modèle présenté précédemment indique que le niveau de CI présent dans une relation est fonction des caractéristiques de fiabilité du mandant. Lorsque le confiant et le mandant n'ont pas encore pu travailler ensemble le niveau de CI est mis en place par le biais des Représentations sociales (RS) que le confiant impute au mandant (*Cf.* Figure 28). Ces RS sont activées à partir des données directement assimilables par le confiant tel que la tranche d'âge ou le genre du mandant. La méthode des RS devrait donc permettre d'induire différents niveaux de CI.

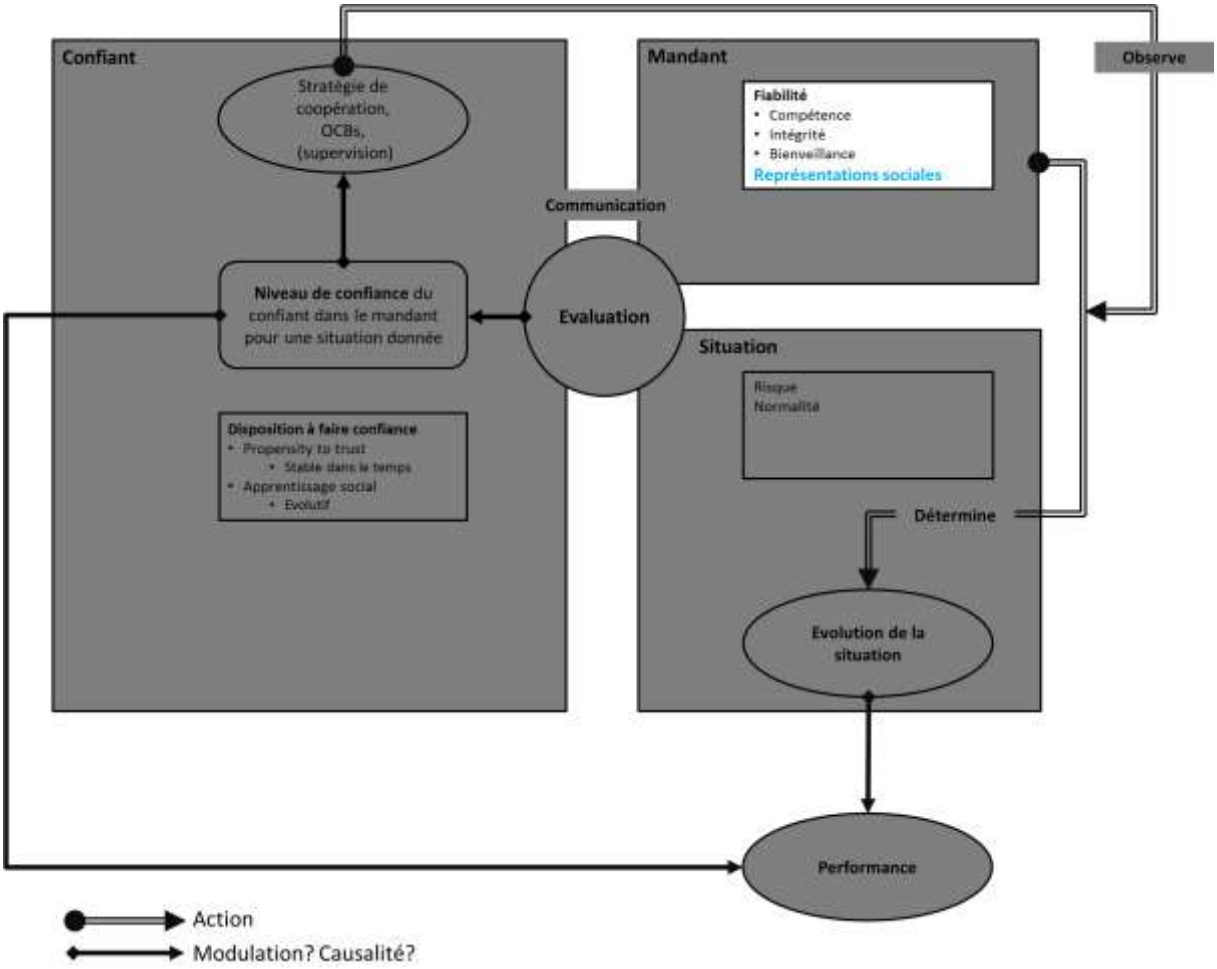


Figure 28 : Représentation de la partie du modèle testée dans cette expérimentation, à savoir les RS que le confiant associe au mandant

Dans la littérature, la méthode d'induction par visage est parfois utilisée (Ballew & Todorov, 2007; Oosterhof & Todorov, 2008, 2008; Todorov et al., 2015) et peut, en quelques sortes, se rapprocher d'une induction par données observables qui est à la base des RS. Dans ce type d'induction, des visages ayant des caractéristiques différentes (couleur de peau, plissement des yeux, largeur de la région labiale…) sont présentés aux participants qui doivent, dans un laps de temps très court, leur attribuer un niveau de CI.

Ce type d'induction aurait pu être utilisée pour effectuer les expérimentations de cette thèse. Cependant, afin d'utiliser ce type d'induction il aurait fallu déterminer les traits caractéristiques des visages induisant différents niveaux de CI aux futurs opérateurs de la RCPair et vérifier que ce type d'induction puisse être utilisé dans des tâches collaborative. Or, la littérature ne présente aucune méthode fiable permettant de déterminer les traits caractéristiques des visages induisant différents niveaux de CI à une population cible. De plus, dans les C2air, les dialogues sont généralement effectués par téléphone ou *chat* ce qui rendrait une induction par visage non écologique. Dès lors, afin d'induire les niveaux de CI nécessaires aux expérimentations présentées dans cette thèse, il a été décidé de mettre en place une nouvelle méthode d'induction utilisant les RS.

Les RS permettent aux individus de reconnaître une personne comme appartenant à une catégorie (par exemple de confiance ou pas de confiance) en fonction de certaines caractéristiques de cette personne (Abric, 2003). Par ailleurs, ces RS ne sont pas homogènes dans la population mais dépendent du groupe social dans lequel elles sont employées. Chaque groupe social (Abric, 2003) possède ses propres savoir et savoir-faire mais également ses propres RS, i.e. un ensemble d'opinions, d'attitudes et de croyances à propos d'un objet donné, qui conditionnent ses comportements.

Les RS sont donc fonctions du groupe social auxquels appartient le confiant, sont dépendantes des caractéristiques du mandant perceptibles par le confiant et devraient permettre au confiant de reconnaître une personne comme étant digne de confiance ou non digne de confiance. En utilisant les RS du confiant, il devrait donc être possible d'induire différents niveaux de CI. Pour cela, il est nécessaire d'identifier précisément la composition des RS qui sont composées d'éléments centraux (stables et communs dans un groupe social), entraînant des comportements homogènes, et d'éléments périphériques (variables selon les individus ou le contexte), entraînant des comportements variables. Ce sont donc les éléments centraux qui seront mobilisés dans ce dispositif expérimental, car 1) ce sont eux qui entrainent des comportements homogènes, comportements qui seront testés par la suite, et 2) ce sont eux qui sont le plus susceptibles d'être les plus fortement inducteurs dans un groupe social car ce sont les plus stables et les plus partagés.

Une étape importante lors de l'utilisation des RS est donc d'identifier les caractéristiques pertinentes qui vont correspondre aux éléments centraux. Ceci se fait généralement par la méthode d'évocation (Abric, 2003), i.e. à partir des déclarations de personnes représentant les personnes ciblées à propos de leur représentation du concept visé. Cependant, les travaux sur les RS montrent que les individus lorsqu'ils s'expriment librement pour catégoriser un objet social peuvent évoquer deux items qu'ils jugent d'égale importance, alors que la procédure dite de Mise en Cause révèle qu'objectivement ça n'est pas le cas. Par exemple, l'étude de Moliner (1989) montre que des individus considèrent comme de même importance la « communauté d'opinions » (75%) et « l'égalité des membres » (74%) pour désigner un groupe comme « idéal ». Mais lorsque l'auteur décrit un groupe d'amis en mettant en cause l'un (communauté d'opinion) ou l'autre

élément (égalité des membres), l'approbation passe de 75% à 73% lorsque la communauté d'opinions est absente, et de 74% à 21% lorsque l'égalité des membres est absente. Autrement dit, cette méthode met en évidence qu'en dépit des déclarations initiales des participants, la communauté d'opinions n'est pas essentielle à la représentation sociale du « groupe idéal », alors que l'égalité des membres, l'est. Ainsi, la communauté d'opinion est considérée comme un élément périphérique, et l'égalité des membres[35], est au contraire, considérée comme un élément central. Parce qu'elle permet la distinction entre éléments centraux et périphériques, la méthode d'évocation associée à la méthode de la mise en cause, a été choisie.

Puisque dans l'expérience de Moliner (1989), les participants se représentent un groupe comme idéal quand on leur présente les membres du groupe comme égaux, alors on peut considérer que cet élément central induit la représentation sociale qui lui est associée. De même, les éléments centraux de la CI devraient permettre d'induire cette représentation sociale de la CI, et *a contrario*, les antonymes des éléments centraux n'induiront pas de la CI (Hypothèse 1). Il est donc proposé ici de chercher à identifier ces éléments centraux et vérifier qu'ils induisent bien des niveaux de CI différents.

Hypothèse 1 : Les éléments centraux de la CI devraient permettre d'induire la représentation sociale de la CI élevée et les antonymes des éléments centraux devraient permettre d'induire la représentation sociale de la CI faible

2. Méthode

A. Participants

Afin de trouver les RS des opérateurs cibles de la RCPair, cette première étude a été axée sur les potentiels opérateurs ayant été identifiés dans l'analyse du besoin de la RCPair (*Cf.* chapitre 1). 373 aviateurs (83% d'hommes, 14% de femmes, et 3% qui n'ont pas répondu à cet item démographique) ont participé aux différentes phases de cette étude. Les participants avaient passé en moyenne 277 jours en Opérations Interalliées (SD : 238.33 jours) en 4 missions distinctes (SD : 4.01 missions), et avaient en moyenne 41 ans (SD : 7.65 ans). Différents participants de cet échantillon ont été mobilisés pour chaque étape de l'étude.

B. Matériel & Procédure

Afin d'identifier les éléments centraux permettant de constituer les inducteurs de CI et de les tester, la première étude a été menée en plusieurs étapes.

Dans une première étape, un recueil de données explicites a été conduit en suivant la méthode d'évocation (Abric, 2003). Un questionnaire a été créé et distribué à 4344 aviateurs. 302 réponses ont été collectées. Dans ce questionnaire, les participants devaient produire 5 mots ou expressions

[35] Dans l'expérience de Moliner les membres ne sont plus considérés comme égaux lorsqu'un individu du groupe donne des ordres et impose sa volonté aux autres membres du groupe

qui leur venaient à l'esprit lorsqu'ils pensaient à "quelqu'un de confiance avec qui on travaille pour la première fois". Le participant hiérarchisait ensuite les 5 mots qu'il avait évoqués (du plus important au moins important). Cette libre association de mots a mis en évidence 49 éléments cités plus de trois fois et liés à la CI.

Dans un deuxième temps, les 49 éléments ont été vérifiés auprès de 39 aviateurs (différents de l'étape 1) en utilisant la méthode de la mise en cause (Lo Monaco et al., 2017; Moliner, 1988). Ces participants devaient décider si une personne caractérisé par la négation d'un des 49 éléments (e.g. quelqu'un de non-compétent) pouvait être une personne de confiance. En rejetant la proposition, les participants confirmaient le fait que l'élément était essentiel à la CI (e.g. « une personne non compétente ne peut pas être quelqu'un de confiance »). Dans le but de tester l'importance de ces éléments essentiels, chacun a été testé en comparant la fréquence de réfutation à la fréquence d'une distribution aléatoire (ici, 0.5). En accord avec la littérature (Lo Monaco, Piermattéo, Rateau, & Tavani., 2017), les éléments ayant une fréquence de réfutation supérieure à 75% ont été classé comme étant des éléments centraux, i.e. les « inducteurs potentiels » les plus susceptibles d'activer de la CI chez les aviateurs. La table 1 montre les 18 éléments dont la fréquence de réfutation est supérieure à 75% (*Cf.* Tableau 1).

Tableau 1 : Fréquence de réfutation et valeur chi2 des inducteurs potentiels de la représentation sociale de la CI (tous p < 0.001).

Inducteurs	Fréquence de réfutation	Valeur du Khi²
Responsable	94.87	31.41
Crédible	94.87	31.41
Honnête	94.87	31.41
Fiable	94.87	31.41
Juste	94.87	31.41
Loyal	92.30	27.92
Professionnel	92.30	27.92
Respectueux	89.74	24.64
Sincère	89.74	24.64
Direct	87.18	21.56
Avec qui vous vous sentez en sécurité	87.18	21.56
Sérieux	84.61	18.69
Compétent	84.61	18.69
Fidèle	84.61	19.69
Réactif	82.05	16.02
Opérationnel	79.48	13.56
Rigoureux	76.92	11.60
Impliqué dans sa mission	76.92	11.30

Ainsi ces éléments centraux identifiés devraient induire un niveau élevé de CI, alors que leurs antonymes devraient induire un niveau faible de CI. Dans un troisième temps ces éléments centraux et leurs antonymes ont donc été combinés pour constituer des profils de coéquipiers. Ces profils ont été constitués soit de deux éléments centraux (30 paires d'éléments centraux, e.g. "compétent" et "honnête"), soit de deux antonymes d'éléments centraux (30 paires de mots créés avec les antonymes des éléments centraux, e.g. " incompétent" et "malhonnête"), soit d'un élément central et d'un antonyme d'un élément central (30 paires de mots créés en utilisant un élément central et un antonyme, e.g." compétent" et "malhonnête").

Les RS étant liées aussi aux caractéristiques du confiant, il est important pour la suite de l'étude de disposer de paires de mots adaptées aux différents groupes qui vont être testés par la suite. Le premier groupe correspond au personnel de l'AA (appelés « aviateurs » quelle que soit leur spécialité) qui a généré les mots initiaux (il n'a pas été jugé utile d'affiner les RS en fonction d'autres critères au sein du personnel de l'AA compte tenu de l'homogénéité des résultats). Le deuxième groupe correspond au personnel non militaire, représentatif des acteurs cyber, qui peuvent avoir des relations différentes (par exemple à l'autorité ou aux règlements). Ainsi, les paires de mots les plus pertinents à conserver pourraient être différentes entre ces deux populations. Pour vérifier cela, une deuxième évaluation a été effectuée sur ces 2 populations. Dans cette deuxième évaluation, les 90 paires différentes ont été testées à travers des échelles non segmentées (*Cf.* Figure 29)(de type Echelle Visuelle Analogique allant de « Pas de confiance » à « Grande confiance ») auprès de 32 aviateurs (différents des étapes 1 et 2) et de 7 élèves ingénieurs en informatique. Sur chaque échelle (pour chaque paire de mots) les participants devaient déplacer un curseur. L'emplacement de ce curseur déterminait la note (/10) que le participant accordait à la paire de mot correspondant.

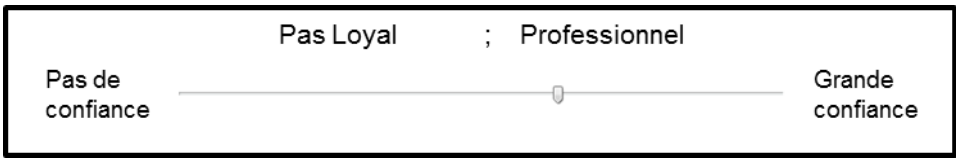


Figure 29 : Exemple d'échelle non segmentée utilisées afin de tester les différentes paires de mots

3. Résultats et discussion

Afin de vérifier si ces 90 paires pouvaient induire des niveaux de CI différentes chez tous les opérateurs potentiels de la RCPair, ces 90 paires ont, dans un premier temps, été testées à travers des échelles non segmentées (de type Echelle Visuelle Analogique) auprès de 32 aviateurs.

Pour les 32 aviateurs, les notes données pour les 30 paires censées induire un niveau de CI élevé ont une moyenne comprise entre 7.2/10 et 9.9/10. Celles associées aux 30 paires censées induire un niveau de CI faible ont une moyenne comprise entre 0.2/10 et 2.4/10. Les 30 paires hybrides ont une moyenne comprise entre 0.6/10 et 5.9/10.

Les résultats obtenus vont dans le sens de l'hypothèse 1, i.e. la possibilité d'induire des niveaux de CI différents à partir de différentes associations d'éléments centraux et de leurs antonymes. Les évaluations moyennes de chacune de ces 90 paires de mot ont permis d'identifier 69 paires susceptibles de produire les inductions nécessaires aux différentes études présentées dans ce manuscrit (*Cf.* Tableau 2) :

- Pour un niveau de CI élevé, les 23 paires avec le plus haut score ont été sélectionnées : moyennes comprises entre 8.1 et 9.9/10 (e.g. honnête et professionnel) ;
- Pour un niveau de CI faible, les 23 paires avec le plus bas score ont été sélectionnées : moyennes comprises entre 0.2 et 1.5 / 10 (e.g. malhonnête et non-professionnel) ;
- Pour un niveau de CI intermédiaire, les 23 paires avec le score le plus proche de la médiane ont été sélectionnés : moyennes comprises entre 2.7 et 5.9 / 10 (e.g. honnête et non-professionnel).

Tableau 2 : Résultats de l'évaluation par échelle visuelle analogique pour les 51 paires de mots (M = 4.5, SD = 3.2) choisies pour créer 17 paires de mots visant à induire un niveau élevé (M = 8.6, SD = 0.3), moyen (M = 3.9, SD = 0.69) et faible (M = 1, SD = 0.19) de CI chez les aviateurs.

Paire de mot créée pour induire un niveau de confiance interpersonnelle élevé		Moyenne	Paire de mot créée pour induire un niveau de confiance interpersonnelle moyen		Moyenne	Paire de mot créée pour induire un niveau de confiance interpersonnelle faible		Moyenne
Opérationnel	Loyal	9.9	Méprisant	Loyal	5.9	Non opérationnel	Impuissant	1.5
Fidèle	Honnête	9.7	Hypocrite	Professionnel	5.8	Pas loyal	Pas professionnel	1.4
Intègre	Professionnel	9.6	Pas professionnel	Fidèle	5.4	Décontracté	Pas professionnel	1.4
Honnête	Professionnel	9.5	Opérationnel	Désinvolte	5.4	Impuissant	Dédaigneux	1.3
Fidèle	Responsable	9.4	Non fidèle	Responsable	5.0	Décontracté	Pas crédible	1.3
Loyal	Sérieux	9.4	Compétent	Pas crédible	4.9	Négligeant	Décontracté	1.3
Crédible	Honnête	9.4	Opérationnel	Méprisant	4.8	Non opérationnel	Pas loyal	1.2
Compétent	Loyal	9.4	Pas intègre	Honnête	4.7	Désinvolte	Pas professionnel	1.1
Fidèle	Opérationnel	9.4	Professionnel	Non fidèle	4.3	Non fidèle	Pas intègre	1.1
Crédible	Sérieux	9.3	Sérieux	Pas intègre	4.2	Pas crédible	Non fidèle	1.1
Intègre	Honnête	9.1	Non opérationnel	Honnête	4.1	Non fidèle	Non opérationnel	0.9
Professionnel	Respectueux	8.6	Méprisant	Fiable	4.0	Pas professionnel	Incapable	0.9
Professionnel	Loyal	8.4	Désinvolte	Crédible	4.0	Désinvolte	Inconstant	0.9
Fiable	Intègre	8.4	Inconstant	Pas professionnel	3.9	Pas intègre	Pas crédible	0.6
Professionnel	Intègre	8.3	Responsable	Pas crédible	3.9	Méprisant	Négligent	0.6
Intègre	Respectueux	8.3	Inconstant	Fidèle	3.9	Méprisant	Hypocrite	0.6
Respectueux	Compétent	8.3	Négligent	Respectueux	3.7	Pas loyal	Professionnel	0.6
Responsable	Sérieux	8.3	Pas intègre	Loyal	3.6	Pas crédible	Pas loyal	0.5
Compétent	Fidèle	8.2	Fidèle	Pas intègre	3.4	Incapable	Désinvolte	0.4
Compétent	Honnête	8.1	Compétent	Hypocrite	3.4	Incapable	Non fidèle	0.4
Honnête	Loyal	8.1	Pas opérationnel	Respectueux	3.1	Négligent	Pas professionnel	0.4
Responsable	Honnête	8.1	intègre	Pas professionnel	2.8	Non fidèle	Hypocrite	0.4
Compétent	Crédible	8.1	Responsable	Pas loyal	2.7	Désinvolte	Méprisant	0.2

Afin de vérifier si ces 90 paires pouvaient induire des niveaux de CI différentes chez tous les opérateurs potentiels de la RCPair, ces 90 paires ont, dans un second temps, été testées à travers des échelles non segmentées (de type Echelle Visuelle Analogique) auprès de 7 élèves ingénieurs en informatique. Ces élèves n'étaient pas à proprement parler des experts mais avaient les caractéristiques identifiées dans l'analyse du besoin, à savoir, un diplôme équivalent au niveau 6 (Bachelor), ne faisant pas partie de l'AA et « formés » au domaine cyber.

Pour les élèves ingénieurs, les 30 paires censées induire un niveau de CI élevé ont une moyenne comprise entre 8.3/10 et 6.2/10. Les 30 paires censées induire un niveau de CI faible ont une moyenne comprise entre 0.7/10 et 2.4/10. Les 30 paires hybrides ont une moyenne comprise entre 2.6/10 et 6.2/10.

Les résultats obtenus vont dans le sens de l'hypothèse 1, i.e. la possibilité d'induire des niveaux de CI différents à partir de différentes associations d'éléments centraux et de leurs antonymes. Les évaluations moyennes de chacune de ces 90 paires de mots ont permis d'identifier 69 paires susceptibles de produire les inductions nécessaires aux différentes études présentées dans ce manuscrit soit (*Cf.* Tableau 3)

- Pour un niveau de CI élevé, les 23 paires avec le plus haut score ont été sélectionnées : moyennes comprises entre 6.9 et 8.3/10 (e.g. honnête et professionnel) ;
- Pour un niveau de CI faible, les 23 paires avec le plus bas score ont été sélectionnées : moyennes comprises entre 0.7 and 2.1 / 10 (e.g. malhonnête et non-professionnel) ;
- Pour un niveau de CI intermédiaire, les 23 paires avec le score le plus proche de la médiane ont été sélectionnées : moyennes comprises entre 6.2 and 3.3 / 10 (e.g. honnête et non-professionnel).

Tableau 3 : Résultats de l'évaluation par échelle visuelle analogique pour les 51 paires de mots (M = 4.45, SD = 2.35) choisies pour créer 6 paires de mots utilisées pour induire une forte (M = 7.25, S = 0.13), moyenne (M = 4.6, SD = 0.35) et faible (M = 1.5, SD = 0.15) de CI chez les élèves ingénieurs

Paire de mot créée pour induire un niveau de confiance interpersonnelle élevé		Moyenne	Paire de mot créée pour induire un niveau de confiance interpersonnelle moyen		Moyenne	Paire de mot créée pour induire un niveau de confiance interpersonnelle faible		Moyenne
Professionnel	Respectueux	8.3	Pas loyal	Responsable	6.2	Non opérationnel	Honnête	2.1
Fiable	Compétent	7.9	Compétent	Hypocrite	6.2	Incapable	Méprisant	1.9
Compétent	Honnête	7.7	Crédible	Désinvolte	6.2	Désinvolte	Pas professionnel	1.8
Respectueux	Compétent	7.7	Hypocrite	Professionnel	6.1	Incapable	Désinvolte	1.8
Sérieux	Fidèle	7.6	Professionnel	Non fidèle	5.9	Pas intègre	Pas crédible	1.7
Compétent	Loyal	7.6	Pas loyal	Professionnel	5.6	Désinvolte	Pas crédible	1.6
Compétent	Crédible	7.6	Opérationnel	Désinvolte	5.5	Pas professionnel	Pas loyal	1.6
Responsable	Sérieux	7.5	Crédible	Non fidèle	5.4	Hypocrite	Négligeant	1.6
Fiable	Honnête	7.4	Sérieux	Pas intègre	5.4	Hypocrite	Pas crédible	1.5
Opérationnel	Intègre	7.4	Non fidèle	Responsable	5.3	Non opérationnel	Pas intègre	1.5
Compétent	Fidèle	7.4	Opérationnel	Méprisant	5.1	Négligent	Pas professionnel	1.5
Honnête	Loyal	7.3	Compétent	Pas crédible	5.1	Méprisant	Négligent	1.4
Respectueux	Fiable	7.3	Méprisant	Loyal	4.9	Négligent	Désinvolte	1.4
Professionnel	Loyal	7.2	Responsable	Pas crédible	4.8	Non fidèle	Non opérationnel	1.3
Fidèle	Opérationnel	7.2	Fiable	Pas intègre	4.8	Désinvolte	Inconstant	1.3
Fidèle	Intègre	7.2	Méprisant	Fiable	4.7	Pas crédible	Non fidèle	1.2
Intègre	Respectueux	7.2	Pas professionnel	Fidèle	4.2	Inconstant	Pas intègre	1.1
Honnête	Professionnel	7.1	Intègre	Pas professionnel	4.1	Négligent	Inconstant	1.1
Responsable	Fidèle	7.1	Pas intègre	Loyal	4.1	Inconstant	Pas professionnel	1.1
Intègre	Honnête	7.1	Intègre	Inconstant	3.8	Non opérationnel	Pas loyal	0.9
Intègre	Professionnel	7.1	Pas intègre	Honnête	3.7	Non opérationnel	Incapable	0.8
Opérationnel	Loyal	7.0	Responsable	Incapable	3.5	Pas loyal	Inconstant	0.7
Loyal	Sérieux	6.9	Respectueux	Pas professionnel	3.3	Pas professionnel	Incapable	0.7

Les résultats obtenus entre les deux populations cibles de la RCP (aviateurs de l'AA et experts en cybersécurité) indiquent que les RS ayant un impact sur la CI sont relativement proches entre ces deux groupes. Pour la catégorie élèves ingénieurs, les paires de mots ont obtenu des moyennes plus faibles que pour les aviateurs ce qui pourrait entraîner une différence dans la force de l'induction.

Cependant, l'ordre d'attribution des notes (qui est le critère le plus important) a été similaire entre les deux catégories. 100% des paires de mots censées induire un niveau de CI élevées ont obtenus les notes les plus élevées chez les deux groupes sociaux, 100% des paires de mots censées induire un niveau de CI faible ont obtenu les notes les plus faibles et 100% des paires de mots intermédiaires ont obtenu des notes intermédiaires. Ceci est possiblement due au fait que les deux populations

avaient une proximité culturelle et démographique (tous les participants étaient français et avait un âge compris entre 20 et 35 ans).

Pour le niveau de CI élevé, les 23 paires de mots générées par les 2 groupes se recoupent à 78% (18 paires de mots appartiennent aux 2 groupes et chaque groupe à 5 paires qui ne sont pas dans l'autre). Pour le niveau de CI élevé, les 23 paires de mots générées par les 2 groupes se recoupent à 69% (16 paires de mots appartiennent aux 2 groupes et chaque groupe à 7 paires qui ne sont pas dans l'autre). Pour le niveau de CI élevé, les 23 paires de mots générées par les 2 groupes se recoupent à 86% (20 paires de mots appartiennent aux 2 groupes et chaque groupe à 3 paires qui ne sont pas dans l'autre). Les 69 paires de mots devraient donc induire différents niveaux de CI aux différents groupes sociaux cibles de la RCPair.

Points clés

Dans ce chapitre les inducteurs potentiels les plus susceptibles d'activer de la CI chez les aviateurs et chez les élèves ingénieurs (potentiels futurs experts cyber) ont été identifiés. Une fois cela fait, ces inducteurs potentiels ont été regroupés en paires de mots :

- 23 paires de mots censées induire un niveau de CI élevé chez les aviateurs et 23 (autres) paires de mots censées induire un niveau de CI élevé chez les élèves ingénieurs ;
- 23 paires de mots censées induire un niveau de CI faible (antonyme des mots censées induire un niveau de CI élevé chez les aviateurs) et 23 (autres) paires de mots censées induire un niveau de CI faible chez les élèves ingénieurs (antonyme des mots censées induire un niveau de CI élevé chez les élèves ingénieurs) ;
- 23 paires de mots censées induire un niveau de CI intermédiaire chez des aviateurs (formées d'un mot censé induire un niveau de CI élevé et d'un mot censé induire un niveau de CI faible) et 23 (autres) paires de mots censées induire un niveau de CI intermédiaire chez les élèves ingénieurs (formées d'un mot censé induire un niveau de CI élevé et d'un mot censé induire un niveau de CI faible).

Ces différentes paires de mots ont ensuite été testées auprès de futurs opérateurs potentiels de la RCPair, à savoir des pilotes et navigateurs opérationnels, des contrôleurs aériens, des mécaniciens et des élèves ingénieurs. Les résultats ont montré que les différentes paires de mots devraient bien induire différents niveaux de CI aux futurs opérateurs de la RCPair.

4 Validation du processus d'induction de CI pour les expérimentations

Résumé du chapitre

Objectif : Tester la méthode d'induction de confiance qui sera ensuite commune à toutes les expérimentations de la thèse.

Démarche : Les paires de mots définies dans le chapitre précédent devraient induire différents niveaux de CI auprès d'individus appartenant au groupe social des futurs opérateurs de la RCPair. Cependant, les données du chapitre précédent n'ont été obtenues qu'avec l'aide de questionnaires. Afin de tester expérimentalement le bon fonctionnement des paires de mots inductrices, il est indispensable de tester expérimentalement leur corrélation à des conséquences comportementales d'un manque ou d'un excès de CI. Pour ce faire, un protocole expérimental a été réalisé et testé. Ce protocole correspond au protocole de base décliné dans les expérimentations réalisées dans cette thèse.

Conclusion : Les paires de mots étalonnées dans le chapitre précédent semblent bien induire différents niveaux de CI auprès des aviateurs. Cependant, un problème d'induction a été détecté sur le niveau de CI intermédiaire qui semble être plus proche d'un niveau de CI faible que d'un niveau de CI élevé.

Chapitre 4 : Validation du processus d'induction de CI pour les expérimentations

1. Introduction

Quatre expérimentations ont été réalisées durant cette thèse à partir du protocole présenté dans ce chapitre. Les spécificités des différentes expérimentations sont ensuite expliquées dans leurs parties respectives.

La tâche à réaliser est une tâche de comptage collaborative sur ordinateur qui consiste à repérer et dénombrer les aéronefs présents sur deux images différentes. Le travail est réalisé par une équipe de deux personnes composée du participant (le confiant) et d'un coéquipier fictif (le *truste*), c'est à dire dont le comportement est en fait simulé par ordinateur et donc entièrement contrôlé au cours de l'expérimentation.

Le rôle du participant est de donner le nombre d'aéronefs présents sur son image puis de valider le nombre d'aéronefs présents sur l'ensemble des deux images. Chaque membre de l'équipe est en charge du comptage des aéronefs présents sur une image différente. Cependant, le participant, qui est également le chef d'équipe, peut à tout moment visualiser l'image traitée par son coéquipier et éventuellement ajuster le résultat donné par ce coéquipier.

Cette activité a été choisie car elle peut être réalisée rapidement (moins d'une minute), qu'elle repose sur une prise d'information, que la performance de l'équipe va dépendre de la performance de chacun des membres et qu'elle donne au chef d'équipe la possibilité de contrôler plus ou moins l'activité de l'autre membre, malgré une contrainte temporelle forte.

Le fait que cette tâche puisse être réalisée rapidement permet d'effectuer, pour chaque participant, un grand nombre d'essais dans chaque catégorie de CI. Cela permet également de limiter que le niveau de CI entre le participant et le coéquipier évolue au cours de l'interaction. Le fait que cette tâche repose sur une prise de d'information permet d'utiliser cette expérimentation dans un contexte cyber en « falsifiant » les informations. Enfin, le fait que la performance de l'équipe dépende de la performance de chacun des membres permet de rapprocher cette expérimentation du contexte des C2.

2. Protocole expérimental

L'expérimentation est composée de plusieurs essais comprenant chacun trois phases successives (*cf.* Figure 30) :

- Phase 1 : induction du niveau de CI ;
- Phase 2 : tâche de comptage et tâche (facultative) de supervision ;

- Phase 3 : évaluations subjectives des degrés de certitude de la réponse du coéquipier, du comptage du participant et du score global.

Un essai correspond à l'ensemble de ces trois phases. Un certain nombre d'essais (variable selon les différentes expérimentations) doivent être validés pour mettre fin à l'expérimentation. L'expérimentation se déroule sur un ordinateur portable avec un écran de 15 pouces d'une résolution de 1920*1080 et une souris.

Pour la mise en œuvre expérimentale, le participant a toujours le rôle de chef d'équipe. Le coéquipier étant fictif, la tâche de comptage du coéquipier est automatisée. Les résultats transmis par le coéquipier peuvent être modifiés par le participant mais le coéquipier ne modifie, ni ne peut modifier, en aucun cas, les résultats transmis par le participant.

La première phase comprend deux affichages distincts et correspond à la mise en place du niveau de confiance (*cf.* Figure 30). Sur un premier affichage, la paire de mots caractérisant le coéquipier est présentée au participant. Les paires de mots utilisées dans cette phase sont les paires de mots testées dans le chapitre précédent pour les groupes sociaux d'utilisateurs potentiels de la RCPair. Dans un tiers des cas ces paires de mots devraient induire un niveau de CI élevé dans le coéquipier, dans un tiers des cas les paires de mots devraient induire un niveau de CI intermédiaire et dans le tiers restant les paires de mots devraient induire un niveau de CI faible (dans certaines expérimentations le niveau de CI intermédiaire a été supprimé). Afin de s'assurer que le participant ait pris en compte les caractéristiques du coéquipier, il lui est demandé, sur le deuxième affichage, de retrouver la paire de mots parmi dix distracteurs. Une fois cette tâche terminée, la deuxième phase commence.

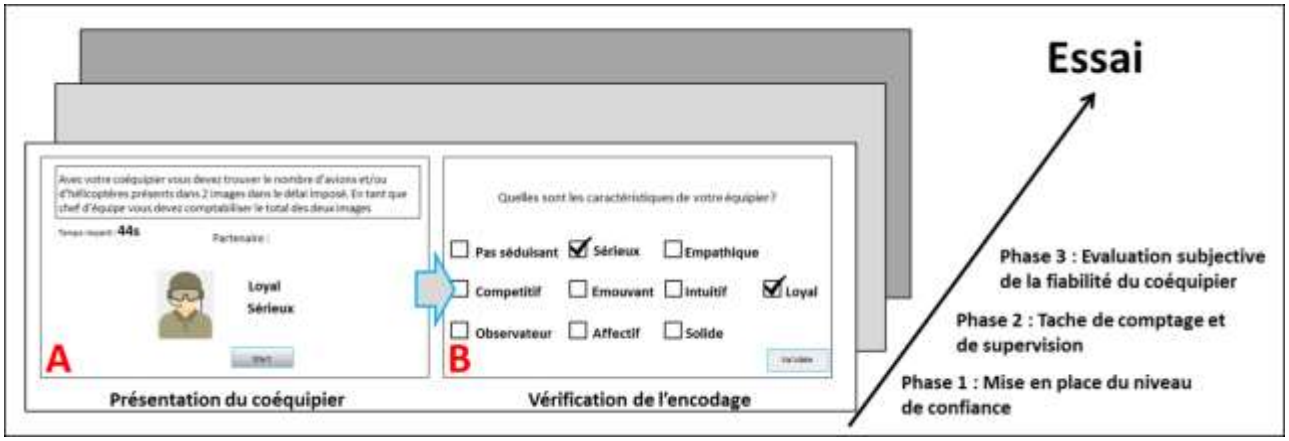


Figure 30 : Présentation de l'expérimentation qui se compose d'un certain nombre d'essais différents de trois phases chacun.
Chaque essai est effectué avec un coéquipier différent représenté par une paire de mots en phase 1. Sur le premier affichage de la phase 1 (« A » sur la figure), le participant prend connaissance de la consigne (similaire tout au long de l'expérimentation), du temps alloué à la tache (ce temps est différent selon les images) et des caractéristiques de son coéquipier. Sur le deuxième affichage de la phase 1 (« B » sur la figure) le participant doit retrouver les deux caractéristiques parmi dix distracteurs avant de pouvoir passer en phase 2.

La deuxième phase comprend trois affichages différents et correspond à la phase de comptage collaboratif et de supervision (*Cf.* Figure 31). Au début de la deuxième phase le participant se trouve devant un affichage de contrôle (*Cf.* Figure 31 « A ») sur lequel lui est présenté le score total (somme des aéronefs comptés par le participant et par le coéquipier) et deux boutons. Le premier bouton

permet au participant d'afficher une interface présentant son image (*Cf.* Figure 31 « B ») et ainsi effectuer sa tâche de comptage. Lorsque le participant valide le compte des aéronefs présents sur son image, l'affichage de contrôle réapparait automatiquement (*Cf.* Figure 31 « A »). Le participant peut alors soit valider le score total correspondant au comptage des aéronefs dans les deux images et passer à la troisième phase, soit cliquer sur le bouton lui permettant d'afficher de nouveau son image (*Cf.* Figure 31 « B »), soit cliquer sur le deuxième bouton lui permettant d'afficher l'image du coéquipier (*Cf.* Figure 31 « C ») et ainsi superviser son activité afin de se faire une idée sur le résultat transmis par celui-ci. Lorsque le coéquipier finit de compter les aéronefs présents sur son image, une indication est donnée au participant (par le bais d'un flash lumineux durant 2 secondes).

Sur l'affichage de supervision, l'image sur laquelle le coéquipier a effectué le comptage, ainsi que le score transmis par le coéquipier, sont présentées. Sur cet affichage, le participant peut uniquement compter les aéronefs présents sur l'image du coéquipier ; il ne peut en aucun cas modifier le nombre d'aéronefs transmis par le coéquipier. Si le participant veut modifier le nombre d'aéronef transmis par le coéquipier il doit cliquer sur l'intéracteur permettant de retourner sur l'écran de contrôle, et le faire à partir de cet écran.

Ainsi, lorsque le participant se trouve sur l'écran de contrôle et qu'il estime que la somme des aéronefs présents sur les deux images est la bonne, il peut la valider, terminer la phase 2 et passer à la phase 3. Il peut également modifier le score total qui s'est incrémentée automatiquement (le score total est l'addition du nombre d'aéronefs comptés par le participant et du nombre d'aéronefs comptés par le coéquipier) s'il estime que le compte donné par le partenaire n'est pas correct. Si le participant ne valide pas la somme des aéronefs présents sur les deux images dans le temps imparti (temps calibré en phase de test pour permettre de compter convenablement les aéronefs présents sur les deux images) le test est considéré comme étant échoué et une nouvelle paire d'images est tirée à la fin de l'expérimentation, avec un coéquipier de même niveau de CI.

Au cours de l'expérimentation chaque image est unique (une image n'est tirée qu'une seule fois) et les images sont associées par paires (les deux images d'une même paire sont donc différentes). Cette association par paire d'images permet de contrôler la pression temporelle. En effet, le délai alloué pour la tache de comptage est calculé en fonction du nombre d'aéronefs présents sur les 2 images associées et de la qualité de ces images. Le nombre d'aéronefs sur chacune des images varie entre 9 et 39. Le délai imparti varie dans une plage de valeurs comprises entre 20 et 44 secondes et correspond à la moyenne des temps mis par 7 personnes extérieures à l'expérimentation pour compter le plus rapidement possible le nombre exact d'aéronefs présents sur chaque paire d'images. Dans la mesure où ces 7 personnes n'ont pas eu à passer par l'écran de contrôle alors que les participants de l'étude devraient le faire au minimum deux fois, ce dispositif devrait induire de la pression temporelle.

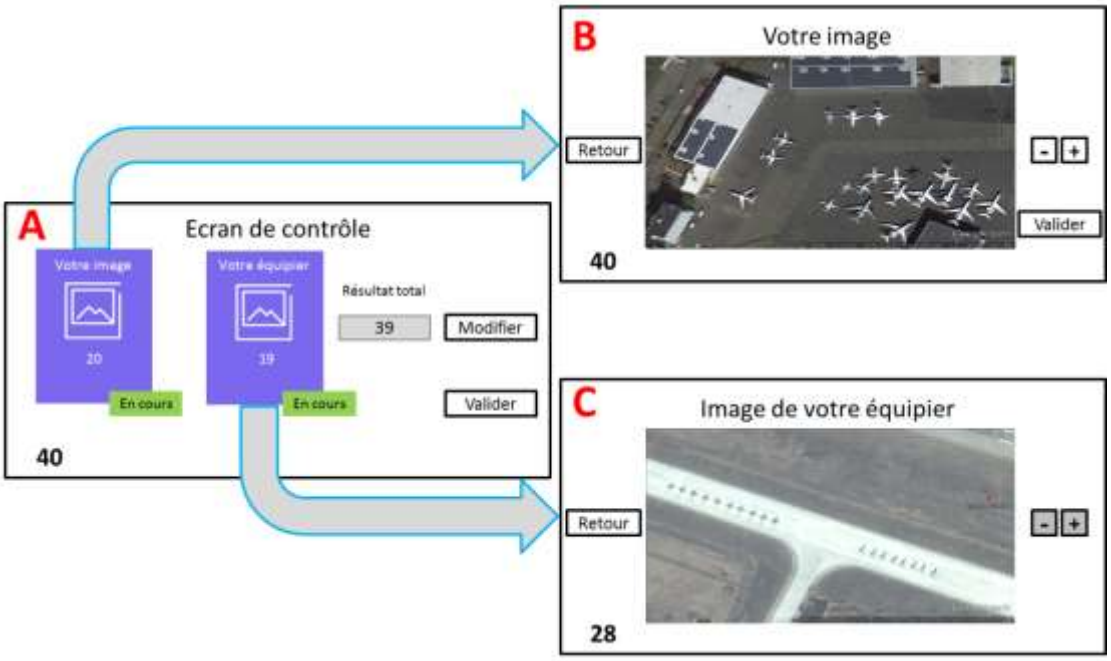


Figure 31 : La phase 2 de l'expérimentation correspond à la phase de comptage et de supervision. Afin d'effectuer la tâche de comptage le participant initialement en « A » doit afficher l'interface « B ». S'il souhaite superviser le coéquipier, le participant doit afficher l'interface « C ».

Enfin, la phase 3 comprend un affichage et correspond à l'évaluation subjective du niveau de confiance. Dans cette troisième phase, 3 échelles non segmentées allant de 0 à 10 sont présentées au participant afin de recueillir :

- Le niveau de certitude qu'a le participant quant au résultat de sa tâche de comptage ;
- Le niveau de certitude qu'a le participant quant au résultat transmis par son coéquipier ;
- Le niveau de certitude qu'a le participant quant au résultat collectif (e.g. la somme des aéronefs présents sur les deux images).

Lorsque le participant renseigne les différentes échelles de la phase 3, il finit la tâche liée à cette image et doit réaliser une nouvelle série de 3 phases, avec une nouvelle paire de mots inductrice de niveau de confiance, un nouvel équipier et une nouvelle paire d'images. Chaque participant réalise ainsi un certain nombre de fois la tâche avec des coéquipiers fictifs toujours différents caractérisés par différentes paires de mots. Afin de limiter, notamment, les possibles biais d'apprentissages au cours de l'expérimentation, aucune indication n'est transmise entre chaque essai, que ce soit au niveau de la réussite personnelle, de la réussite du coéquipier ou de la réussite collective.

3. Précautions expérimentales

Afin de contrôler l'expérimentation en ne gardant que deux variables aléatoires, i.e. la paire de mots inductrice du niveau de CI et la réussite du coéquipier, l'ordre d'arrivée des différentes paires d'images est similaire pour chaque participant (*cf.* Figure 32). Afin de rendre plus réaliste la tâche effectuée par le coéquipier, plusieurs paramètres ont été pris en compte. En premier lieu, le compte du coéquipier ne démarre pas directement à l'affichage de l'écran de contrôle mais après un temps variable tiré aléatoirement étant *a minima* égal à 2 secondes. De même, pour qu'il paraisse réaliste, l'intervalle de temps entre chaque incrémentation du score du coéquipier n'est pas uniforme pour

tous les essais mais tiré aléatoirement en début d'essai afin qu'il reste dans une plage de valeur supérieure à 0.3 seconde et inférieure à 0.9 secondes. Enfin, la réussite ou non de la tâche de comptage du coéquipier est également tirée aléatoirement. Pour chaque niveau de CI le coéquipier transmet 50% de résultat corrects et 50% de résultats erronés. Les résultats erronés correspondent à une erreur positive dans 50% des cas et négative dans 50% des cas. Afin que l'erreur ne soit pas facilement détectable par le participant, celle-ci se trouve toujours dans une plage de -10% à +10% du nombre total d'aéronefs présents sur l'image.

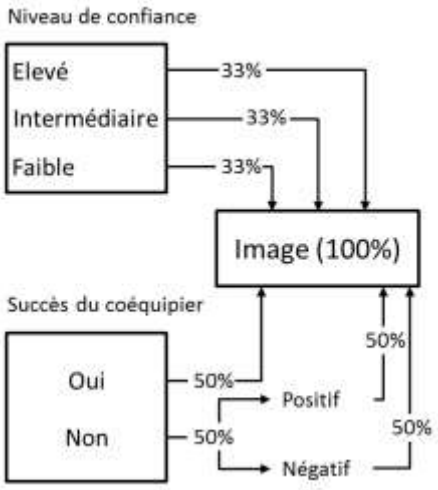


Figure 32 : Présentation du tirage aléatoire qui permet une équiprobabilité (en moyenne) des tirages. Fixer l'ordre des images permet d'assurer que chaque image ait été passée dans toutes les catégories de CI et avec succès ou non du coéquipier. La limite de temps étant liée aux images, grâce à ce type de tirage la complexité est similaire entre les différents niveaux de CI. Si les images avaient également été tirées aléatoirement, l'équiprobabilité des tirages n'aurait pas pu être assurée pour chaque image.

4. Variables mesurées

Plusieurs variables sont récupérées durant ce protocole expérimental (*Cf.* Tableau 4). La phase 1 permet l'induction du niveau de CI. Le niveau de CI induit durant cette phase correspond à la Variable indépendante confiance (Vconf). Cette variable Vconf prend (selon les expérimentations) 2 (faible ou élevé) ou 3 valeurs (faible, moyen, élevé).

En phase 2 la plupart des variables nécessaires au test des différentes hypothèses sont récupérées et sont classées en 3 catégories, les variables binaires (0 ou 1), les variables temporelles (en ms) et les variables calculées :

Les variables binaires récupérées en phase 2 sont :

- Le clic ou non du participant sur le bouton permettant d'accéder à l'image du coéquipier (VDsup). Si durant l'essai le participant clique sur le bouton permettant d'afficher l'image cette variable vaut 1 sinon cette variable vaut 0. Cette variable permet d'obtenir le nombre d'essais où le participant est allé voir l'image de son coéquipier afin de superviser son travail. Cette variable permet de calculer le « pourcentage de supervision » qui sera utilisé dans la suite du document et dont le calcul exact est expliqué ci-après ;

- Le clic ou non du participant sur le bouton permettant de modifier le score total (VDmodif). Si durant l'essai le participant clique sur le bouton permettant d'effectuer une modification cette variable vaut 1 sinon cette variable vaut 0. Cette variable permet d'obtenir le nombre d'essais où le participant a modifié le nombre d'aéronefs transmis par son coéquipier. Cette variable permet de calculer le « pourcentage de modifications », qui sera utilisé dans la suite du document et dont le calcul exact est expliqué ci-après ;
- Le nombre de supervisions contre-productives (VDm_sup). Si, après avoir cliqué sur le bouton permettant d'accéder à l'image du coéquipier, le participant clique sur le bouton de modification alors que le coéquipier avait transmis un bon score ou si le participant ne clique pas sur le bouton de modification alors que le coéquipier avait transmis un mauvais score cette variable vaut 1 sinon cette variable vaut 0. Cette variable permet d'obtenir le nombre d'essais où le participant a mal pris en compte, lors d'une supervision, les résultats transmis par son coéquipier. Cette variable permet de calculer le « pourcentage de supervisions contre-productives », qui sera utilisé dans la suite du document et dont le calcul exact est expliqué ci-après.

Ces variables binaires sont ensuite transformées en pourcentage en divisant leur score total (par niveau de CI) par le nombre d'essais. Les variables étudiées ici sont donc le pourcentage de fois où le participant a cliqué sur le bouton permettant d'afficher l'image du coéquipier (%VDsup), le pourcentage de fois où le participant a cliqué sur le bouton permettant de modifier le score total (%VDmodif) et le pourcentage de fois ou le participant a effectué une supervision contre-productive (%VDm_supf). Par exemple, un participant doit réaliser 10 essais en CI faible. Si dans 6 de ces 10 essais le participant décide de superviser son coéquipier, la valeur de %VDsup pour ce participant et pour le niveau de confiance faible sera de 60%. Si dans 8 de ces 10 essais le participant clique sur le bouton de modifications, la valeur de %VDmodif pour ce participant et pour le niveau de confiance faible sera de 80%. Si dans 3 de ces modifications le coéquipier avait transmis le bon score et dans les 2 essais sans modifications le coéquipier avait transmis un mauvais score, la valeur de %VDm_sup pour ce participant et pour le niveau de confiance faible sera de 50%.

Les variables temporelles récupérées en phase 2 sont :

- Le temps passé par le participant à effectuer sa propre tâche de comptage (TempsPart). A chaque fois que le participant clique sur le bouton d'affichage de son image, ce temps reprend son incrémentation. A chaque fois que le participant clique sur le bouton de retour à l'écran de contrôle, ce temps arrête de s'incrémenter ;
- Le temps passé par le participant à effectuer la tâche de supervision (TempsSuperv). A chaque fois que le participant clique sur le bouton d'affichage de l'image du coéquipier ce temps reprend son incrémentation. A chaque fois que le participant clique sur le bouton de retour à l'écran de contrôle, ce temps arrête de s'incrémenter ;
- Le temps total mis par le participant avant de valider l'essai (TempsTot). Lorsque le participant clique sur le bouton permettant de passer en phase 2 ce temps est remis à 0 et commence son incrémentation. Lorsque le participant clique sur le bouton permettant de passer en phase 3 ce temps arrête de s'incrémenter.

Les variables TempsPart et TempsSuperv sont ensuite transformées en pourcentage en les divisant par la variable TempsTot afin d'obtenir les variables de pourcentages qui seront utilisées au cours des différentes analyses.

- Le pourcentage de temps passé par le participant à effectuer sa propre tâche de comptage (%TempsPart) ;
- Le pourcentage de temps passé par le participant à effectuer la tâche de supervision (%TempsSuperv).

La variable TempsTot est transformée en pourcentage en divisant son score par le temps disponible pour réaliser un essai. La variable étudiée ici correspond donc au pourcentage de temps total (%TempsTot).

Durant la dernière phase, 3 variables sont récupérées grâce aux 3 échelles non segmentées allant de « Pas sur » (0) à « sur » (10) (*Cf.* Figure 33) :

- Le niveau de certitude qu'a le participant quant au résultat de sa tâche de comptage (CertitudePerso) ;
- Le niveau de certitude qu'a le participant quant au résultat transmis par son coéquipier (CertitudeCoéquipier) ;
- Le niveau de certitude qu'a le participant quant au résultat collectif (Certitudecollectif).

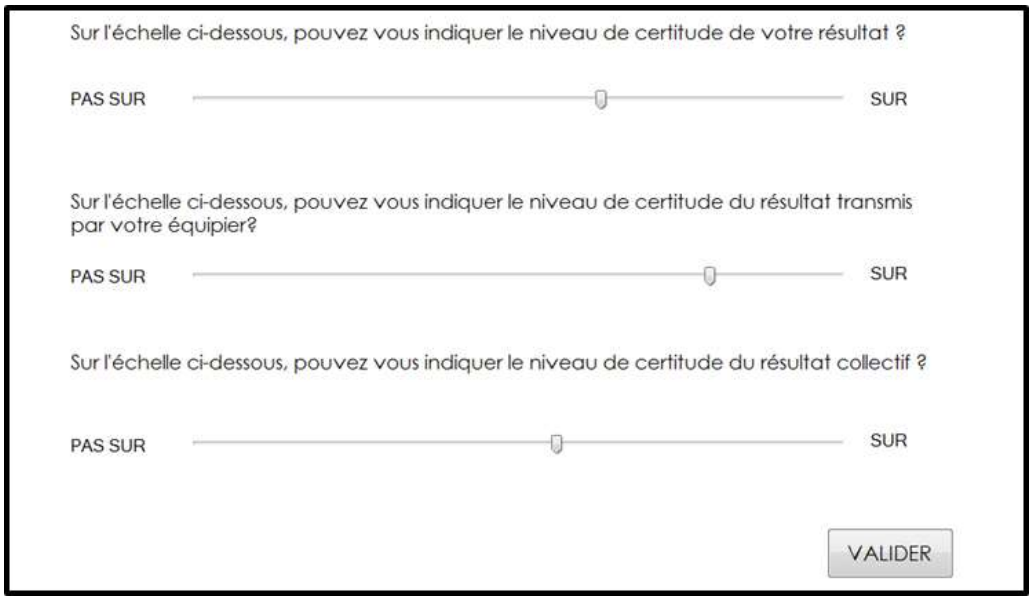


Figure 33 : Echelles non segmentées présentées en dernière phase

Les niveau de CertitudeCoéquipier et de Certitudecollectif ont été récupérés car des études antérieures suggèrent que la confiance est un modérateur de la performance perçue sur la tâche du coéquipier (Dirks & Ferrin, 2001) et de la performance perçue sur la tâche collective (Costa, 2003). Dès lors ces deux niveaux devaient permettre de vérifier le bon fonctionnement de l'induction de différents niveaux de CI. Cependant, l'analyse des résultats obtenus dans cette thèse indiquent que, dans les différentes expérimentations, le niveau de CertitudeCoéquipier correspondait à une moyenne du niveau de CertitudePerso et du niveau de CertitudeCoéquipier. Le niveau de

CertitudePerso n'étant pas dépendant du niveau de CI il a été décidé de n'utiliser que le niveau de CertitudeCoéquipier comme variable permettant de valider l'induction.

Le niveau CertitudeCoéquipier devrait être plus élevé pour les essais effectués avec une induction de CI élevée que pour une induction de CI faible. Pour toutes les expérimentations présentées dans cette thèse cette variable a été contrôlée, avant l'analyse des résultats, afin de s'assurer du bon fonctionnement de l'induction durant l'expérimentation.

Tableau 4 : Nom, type, valeurs possibles et unités des variables dépendantes et indépendantes récupérées dans l'expérimentation et phase de l'essai dans laquelle ces variables sont récupérées.

Phase de récupération	Nom de la variable	Type de variable	Valeurs possibles	Unités
1	Vconf	VI	Faible ; (moyen) ; élevé	-----
2	%VDsup	VD continue	0 - 100	%
2	%VDm_sup	VD continue	0 - 100	%
2	%VDmodif	VD continue	0 - 100	%
2	%TempsPart	VD continue	0 - 100	%
2	%TempsSuperv	VD continue	0 - 100	%
2	%TempsTot	VD continue	0 - 100	%
3	CertitudePerso	VD continue	0 - 10	/10
3	CertitudeCoéquipier	VD continue	0 - 10	/10

5. Test du matériel expérimental

Afin de vérifier le bon fonctionnement de l'induction et la pertinence du protocole, une expérimentation a été effectuée. Cette expérimentation étant un préalable aux autres expérimentations de la thèse, elle est donc considérée ici comme une pré-expérimentation. Le but de cette pré-expérimentation était de vérifier que le protocole expérimental permettait bien d'induire différents niveaux de CI en utilisant les paires de mots évaluées au chapitre précédent. Pour cela, le fait que cette induction permettait de retrouver les différents résultats présentés dans la littérature (en bleu sur la figure 34) en jouant sur les RS associées au mandant a été vérifié. Si le protocole expérimental était bien fonctionnel, une induction de CI élevée devait entrainer un niveau de certitude dans le résultat transmis par le coéquipier plus élevé (Dirks & Ferrin, 2001) et un temps de supervision plus faible (Colquitt et al., 2007; De Jong & Elfring, 2010; McAllister, 1995) qu'une induction de CI faible.

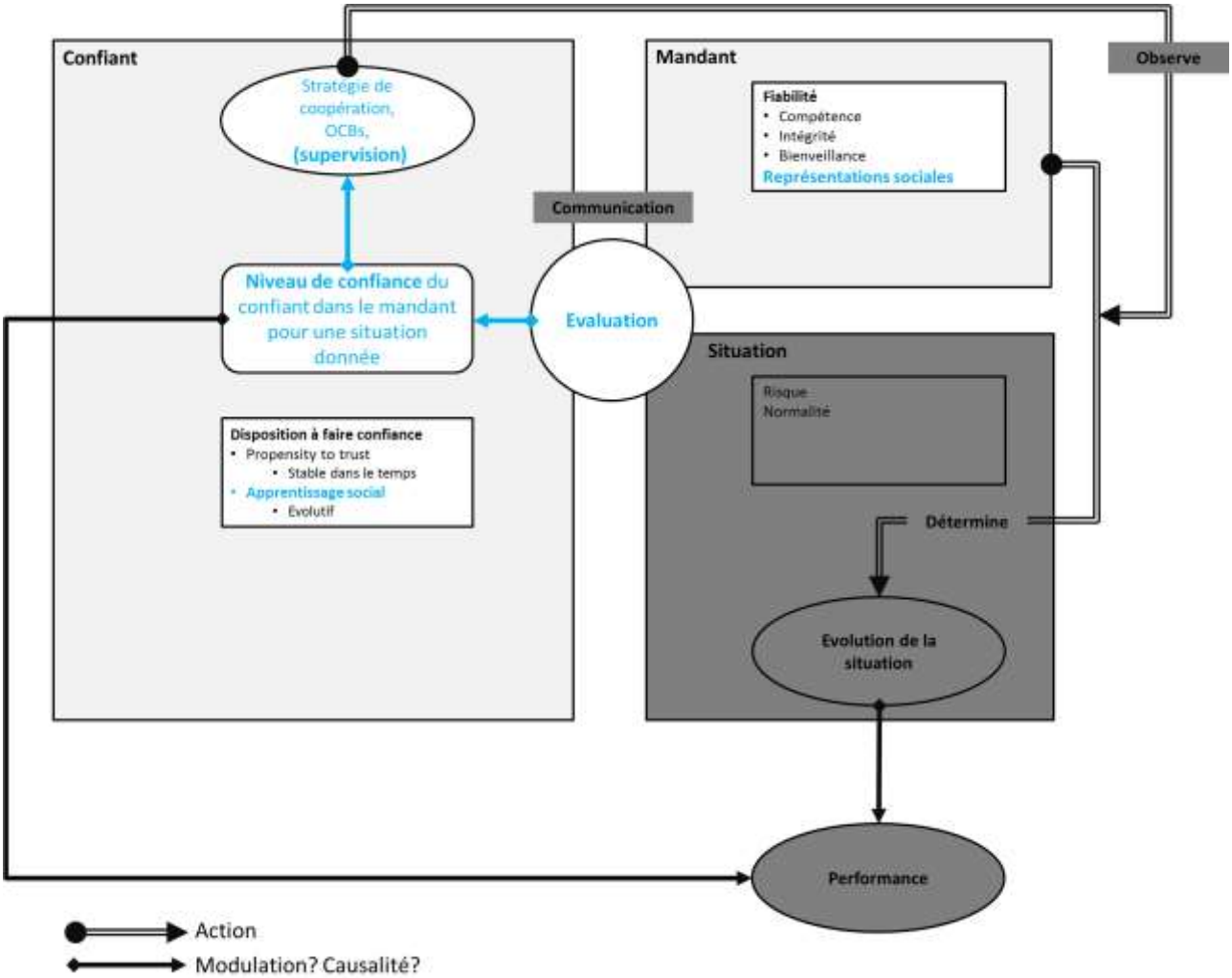


Figure 34 : Test du matériel expérimental.
Pour être validé, le matériel expérimental doit induire différents niveaux de CI auprès des participants et ces niveaux de CI doivent modifier le comportement des participants.

A. Participants

39 aviateurs (18 % de femmes et 82% d'hommes) d'âge moyen 27,5 ans (SD : 6,94 ans) ont participé à cette pré-expérimentation. Aucun d'entre eux n'avait été impliqué dans l'étude portant sur la création des paires de mots (*Cf.* Chapitre 3). Les participants avaient une vue normale ou corrigée et n'étaient pas informés de l'objectif de l'étude. Un document relatif au déroulement de l'expérimentation a été lu avant chaque passation à chaque participant afin d'obtenir son consentement éclairé (ce document est présenté en annexe 2).

B. Résultats

Les données des 39 participants sont incluses dans l'analyse. Pour chaque participant, les résultats des variables dépendantes sont moyennés en fonction du niveau de CI. Les moyennes sont effectuées en prenant en considération uniquement les essais réussis, soit 17 par niveau de CI et par participant. Les essais échoués (lorsque le participant ne valide pas le score total avant la fin du

temps imparti) sont en moyenne de 8.65% (SD = 6.65%). Les comparaisons de moyennes présentées dans le tableau ci-dessous (*Cf.* Tableau 5) sont effectuées par des Tests de Student bilatéraux.

Bien qu'aucune indication de performance du participant ne lui soit transmise après chaque essai, et que chaque image soit différente, un effet d'apprentissage pouvait survenir. Des tests de Student ont été réalisés afin de regarder s'il existait une différence, en termes de stratégie, entre les premières et les dernières images. Aucun effet d'apprentissage n'a pu être montré statistiquement. De plus, le pourcentage d'erreur donné par le coéquipier fictif étant de 50% dans chaque condition de CI, une baisse du niveau de confiance du participant envers ses coéquipiers aurait pu survenir au fur et à mesure de l'expérimentation. Là encore, aucun effet de ce type n'a pu être montré statistiquement en utilisant des tests de Student.

Comme le montre les résultats (*Cf.* Tableau 5), une différence significative est bien présente sur le degré de certitude qu'a le participant sur les résultats transmis par son coéquipier entre les niveaux de CI élevé et faible. Une différence significative est également présente sur le temps de supervision entre les niveaux de CI élevés et les niveaux de CI faibles. Pris ensemble ces résultats tendent à montrer que le protocole expérimental ainsi que le mécanisme d'induction fonctionnent bien et que différents niveaux de CI sont bien induits chez les participants.

Cependant, la non significativité des résultats entre le niveau de CI faible et le niveau de CI intermédiaire sur le temps de supervision ne permet pas de conclure à une discrétisation suffisante des 3 classes de confiance. En effet, si le niveau de CI intermédiaire était à « équidistance » du niveau de CI élevé et du niveau de CI faible, une différence significative aurait été trouvée entre ces 3 classes. Le niveau de CI intermédiaire semble donc être plus proche du niveau de CI faible que du niveau de CI élevé. Ceci est probablement dû au fait que le niveau de CI intermédiaire est formé de deux mots antinomiques. Dès lors, il est possible que les participants aient « pris en compte » le mot induisant le niveau de CI le plus faible.

Tableau 5 : Moyenne, écart type et comparaison par paire pour degré de certitude de la réponse du coéquipier (niveau de certitude associée au coéquipier dans ce tableau) et pour le temps de supervision.

Variable dépendante	Moyenne (M) et écart type (SD) pour chaque variable dépendante			Comparaison par paire pour chaque variable dépendante en fonction du niveau de confiance interpersonnelle induit		
	Faible	Intermédiaire	Elevé	Faible	Intermédiaire	
Niveau de certitude accordé au partenaire (/10)	M = 5.6 SD = 2.27	M = 5.89 SD = 1.80	M = 6.34 SD = 2.07	- $t(38) = -5.33$. $p = .001$**. $d = 0.49$	$t(38) = -3.84$. $p < .001$**. $d = 0.30$ $t(38) = -3.01$. $p = .004$***. $d = 0.23$	Faible Elevé
Temps de supervision (ms)	M = 5864.48 SD = 1949.86	M = 5709.50 SD = 1884.88	M = 5096.69 SD = 1913.65	- $t(38) = 3.54$. $p = .001$**. $d = 0.40$	$t(38) = 0.76$. $p = .45$. $d = 0.08$ $t(38) = 4.21$. $p < .001$***. $d = 0.32$	Faible Elevé

6. Conclusion

Dans la première partie de ce chapitre le protocole servant de base aux différents protocoles expérimentaux utilisés dans cette thèse a été présenté. Dans toutes les expérimentations présentées dans ce manuscrit, les participants ont réalisé, en tant que chef d'équipe, une tâche collaborative de comptage avec un coéquipier fictif. Ce coéquipier était représenté par une paire de mots, censée induire, chez le participant, différents niveaux de CI.

Les paires de mots utilisées pour induire les différents niveaux de CI sont les paires de mots identifiées au chapitre précédent. Cependant, comme vu précédemment, le caractère « inducteur de confiance » de ces paires de mots n'avait jamais été testé expérimentalement.

Dans la deuxième partie de ce chapitre, le protocole expérimental, et, par extension, le caractère « inducteur de confiance » des différentes paires de mots ont été testés sur 39 opérationnels de l'AA. Les participants de cette première expérimentation faisaient tous parti de l'AA mais avaient des âges, grades et métiers différents. Cette hétérogénéité populationnelle explique que les résultats obtenus aient une taille d'effet relativement faible (*Cf.* la valeur du d de Cohen dans le tableau 5) mais n'enlève en rien à la significativité des tests de Student bilatéraux.

Les résultats montrent qu'une augmentation du niveau de confiance induit entraine une diminution du temps passé par le participant à superviser son coéquipier ainsi qu'une augmentation du niveau de certitude dans la réponse transmise par son coéquipier. Ces observations, cohérentes avec celles présentes dans la littérature indiquent que le protocole expérimental fonctionne correctement et que les différentes paires de mots induisent bien différents niveaux de CI à des opérationnels de l'AA.

Points clés

Le but de cette première expérimentation étant de démontrer le bon fonctionnement des paires de mots inductrices de confiance, cette expérimentation a été effectuée avec tout type d'aviateurs, sans aucune distinction. De fait, les résultats de cette expérimentation ne permettent pas d'apporter des informations sur les résultantes comportementales d'un manque ou d'un excès de CI sur les opérateurs cibles de la RCPair mais permettent de valider :

- la pertinence du protocole expérimental ;
- le bon fonctionnement de l'induction de confiance présentée dans le chapitre précédent.

5 Etude expérimentale de l'impact des différents niveaux de CI sur le comportement des opérateurs cibles de la RCPair

Résumé du chapitre

Objectif : Tester expérimentalement l'impact des différents niveaux de CI sur le comportement des opérateurs cibles de la RCPair dans une tâche de travail collaboratif.

Démarche : L'analyse du besoin réalisée au chapitre 1 montre une grande disparité de profils chez les potentiels opérateurs cibles de la RCPair. La littérature sur la confiance indique un lien entre le niveau de confiance présent entre les membres d'une équipe et le comportement des individus formants cette équipe ; toutefois, ces conséquences comportementales ne semblent être liées qu'au niveau de confiance et non aux caractéristiques sociales du confiant. Dès lors, sachant qu'il est possible d'induire différents niveaux de CI à des individus (*Cf* chapitre précédent) et que les potentiels opérateurs de la RCPair sont connus (*Cf* chapitre 1), il est possible de tester si le comportement de tous les individus cibles de la RCPair sera similaire en fonction du niveau de CI présent dans l'équipe ou si des caractéristiques sociales modifieront ces comportements.

Conclusion : De nouvelles modifications comportementales, non étudiées dans la littérature, ont été identifiées. Les caractéristiques sociales des individus ne semblent pas directement influer sur le comportement des individus mais semblent plutôt avoir une influence sur la prise en compte, par l'individu, du niveau de CI présent dans l'équipe

Chapitre 5 : Etude expérimentale de l'impact des différents niveaux de CI sur le comportement des opérateurs cibles de la RCPair

1. Introduction

La problématique opérationnelle de cette thèse est d'identifier des leviers permettant d'améliorer la performance du système sociotechnique que représente un C2air intégrant la RCPair. Afin d'améliorer le fonctionnement de la RCPair, deux approches peuvent être utilisées. La première approche (qui sera appelée « approche directe ») consiste à choisir le décideur final le plus adapté à la RCPair en prenant en compte les différentes caractéristiques sociales (métier, compétences, environnement de travail…) de cet opérateur. La deuxième approche (qui sera appelée « approche indirecte ») consiste à mettre en place des outils permettant d'améliorer les interactions entre les différents opérateurs présents dans les C2air. Dans la littérature ces deux approches sont étudiées dans des théories différentes.

La première approche est soutenue par différentes littératures tel que la *social cognitive theory* (Bandura, 1991) qui suggèrent que les caractéristiques psychosociales d'un individu ainsi que la situation influencent directement les comportements de cet individu (Davis & Luthans, 1980). Pour ces théories, le niveau de CI présent dans une relation n'est pas pris en compte comme étant un modulateur de la performance ou du comportement. Selon ces théories les comportements et donc la performance seraient indépendants du niveau de confiance mais uniquement dépendants des caractéristiques psychosociales de l'individu.

La deuxième approche est soutenue par la littérature portant sur la CI qui indique qu'un niveau élevé de CI génère habituellement des comportements favorables au bon fonctionnement d'une organisation (De Cremer et al., 2018; Schilke & Huang, 2018) notamment dans les cas où les individus doivent collaborer parfois sans se connaitre préalablement (Wildman et al., 2011) afin de réaliser une tâche dans une situation donnée.

Ces deux approches semblent donc opposées, l'une (la littérature sur la CI) ayant une approche indirecte du comportement, et l'autre (la littérature portant sur l'apprentissage social) ayant une approche plus directe du comportement. Selon que l'une de ces littératures prenne le pas sur l'autre, les conséquences, en terme de choix du décideur final de la RCPair et de mise en place ou non de systèmes techniques favorisant l'émergence de la CI (quel type de communication, quels informations échangées…), seraient être différentes. Ici, il s'agit donc de trancher sur l'existence d'un postulat, de l'autre ou des deux simultanément. Le point commun entre les deux approches est le confiant.

L'approche indirecte, par CI (lien bleu dans la figure 35) indique que le comportement du confiant devrait être modulé par le niveau de CI qu'il accorde au mandant. L'approche directe (lien orange dans la figure 35) indique quant à elle que les caractéristiques psychosociales du confiant influencent directement son comportement. Dans ce cas, le comportement du confiant serait plus modifié par ses caractéristiques psychosociales que par le niveau de CI présent dans la relation. Ainsi, afin de pouvoir se prononcer sur l'apport de l'une ou l'autre approche (ou aiguiller sur une approche différente), une étude en deux parties est proposée. Dans la première partie (paragraphe 2) les comportements qui pourraient être modifiés par le niveau de CI présent dans une relation sont étudiés. Dans une deuxième partie (paragraphe 3) on vérifie si, en prenant en compte les caractéristiques psychosociales du confiant, ces comportements sont toujours modifiés par le niveau de confiance.

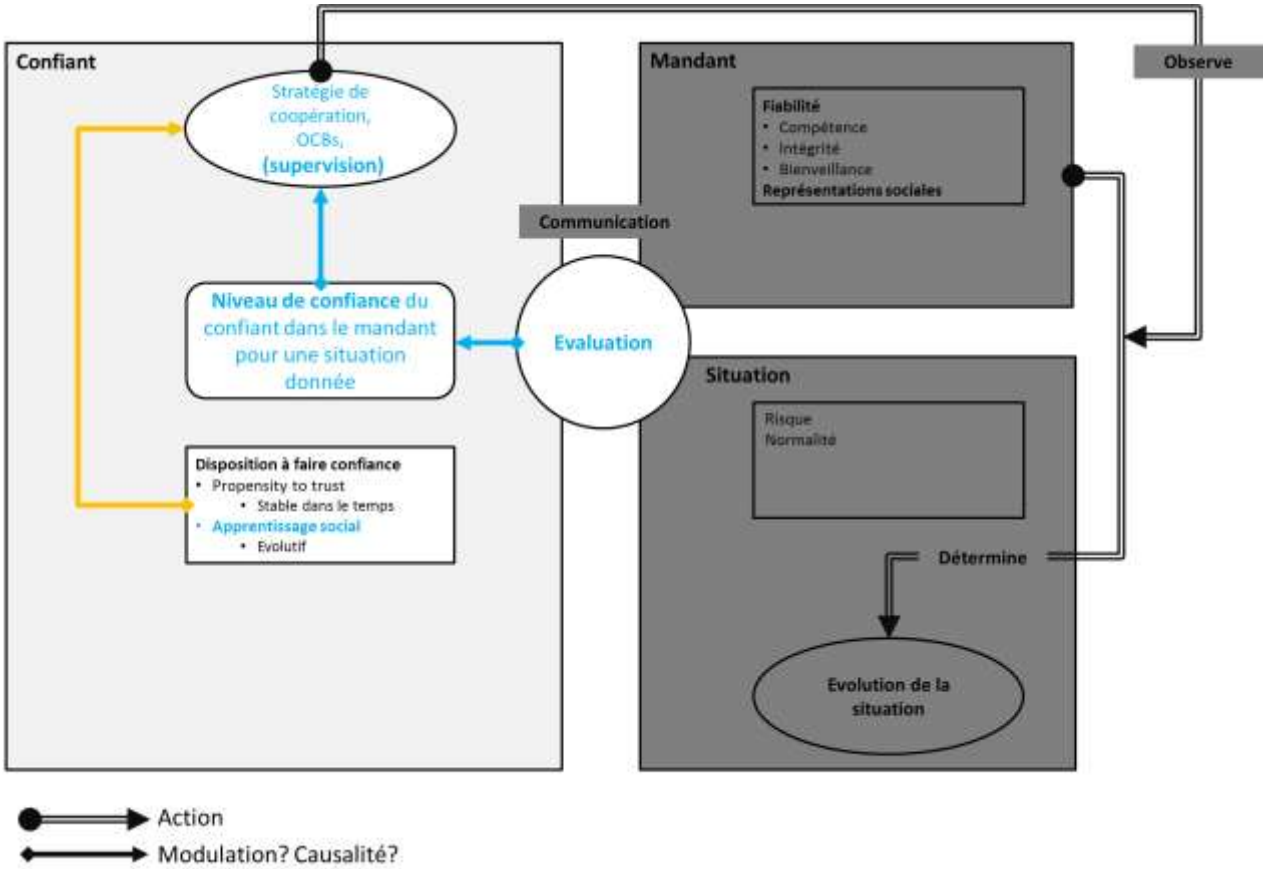


Figure 35 : Représentation des deux approches étudiées dans l'expérimentation 1.
En bleu, l'approche directe sous-tend que le comportement d'un individu est dépendant du niveau de confiance présent dans la relation. En orange, l'approche indirecte sous-tend que les caractéristiques psychosociales du confiant modifient son comportement indépendamment du niveau de confiance présent dans la relation.

2. Niveau de Confiance et comportements

Dans cette partie seront posées les hypothèses relatives aux liens présents entre le niveau de CI et le comportement des individus (liens bleus dans la figure 35). La littérature portant sur l'étude des liens entre le niveau de CI et le comportement des personnes, indique que le niveau de CI est étroitement lié à la notion de performance (Colquitt et al., 2007; De Jong et al., 2016; Dirks & Ferrin, 2002) de

telle sorte qu'un niveau de CI élevé entraîne une meilleure performance qu'un niveau de CI faible. Outre ce lien entre CI et performance, la CI modifierait également les comportements du confiant dans la relation (Colquitt et al., 2007; De Jong & Elfring, 2010; Dirks & Ferrin, 2002) (*Cf.* Figure 35 lien bleu). Le niveau de CI modifierait notamment les stratégies de coopération du confiant (Colquitt et al., 2007; De Jong & Elfring, 2010; Dirks & Ferrin, 2002) qui peuvent prendre différentes formes telles que l'altruisme ou la courtoisie (Mayer & Gavin, 2005; Wong et al., 2006). La modification comportementale qui semble faire consensus dans la littérature sur la confiance est une modulation de la tâche de supervision (Colquitt et al., 2007). Cette tache de supervision est effectuée par le confiant en parallèle de sa tâche principale et permet au confiant de s'assurer que « *tout fonctionne convenablement* **»** (McIntyre & Salas, 1995, p. 23) [36]. Ainsi, lorsqu'un confiant fait confiance à un mandant, quasiment toute l'attention du confiant peut être dédiée à la tâche principale ou au but à atteindre, alors que dans le cas contraire, une partie plus conséquente de ses ressources est utilisée à superviser le mandant (Colquitt et al., 2007; De Jong & Elfring, 2010; McAllister, 1995).

Cette modification comportementale a notamment été observée dans la littérature managériale et est principalement mise en évidence dans les études portant sur le lien entre un manager et ses subordonnées. Dans cette littérature, la tâche principale du manager est d'observer *in situ* les actions effectuées par ses subordonnés afin d'évaluer la performance, d'obtenir des feedback (De Jong & Elfring, 2010; Komaki, Zlotnik, & Jensen, 1986; McIntyre & Salas, 1995) et de voir si le travail est ou sera achevé. La tâche principale d'un manager se rapproche donc fortement d'une tâche de supervision. Pour les managers, une augmentation du nombre de supervisions liée à la diminution du niveau de CI (Colquitt et al., 2007; De Jong & Elfring, 2010; McAllister, 1995) sur un subordonné devrait donc être compensée par une diminution du nombre de supervisions sur un autre subordonné. Cependant, pour des opérateurs, tels que les opérateurs de la RCPair, dont la tâche principale n'est pas de superviser mais d'analyser, traiter et comprendre des données, une augmentation du nombre de supervisions liée à la diminution du niveau de CI (Colquitt et al., 2007; De Jong & Elfring, 2010; McAllister, 1995) serait contre-productive. Dans ce cas-là, le temps passé à superviser serait autant de temps qui n'est pas consacré à la tâche principale et pourrait entrainer une perte d'efficacité de l'opérateur sur cette tâche principale. Ceci rejoint la notion de suivi mutuel de la performance (traduction de *mutual performance monitoring*) (Salas et al., 2008) qui est mise en place par des membres d'une équipe afin de contrôler la performance d'équipe et qui consiste, pour les opérateurs, à « *suivre le travail des autres membres de l'équipe tout en effectuant leur propre travail* » (McIntyre & Salas, 1995, p. 23)[37]. En ce sens, afin d'éviter la perte d'efficacité de l'opérateur sur sa tâche principale, l'opérateur devrait effectuer une compensation en augmentant le temps total alloué à la réalisation des tâches (la tâche de supervision viendrait « en supplément » de la « tâche normale » de l'opérateur). Ceci amène à formuler les deux hypothèses suivantes :

Hypothèse 2 : Une diminution du niveau de CI entraîne une augmentation du nombre de supervisions.

[36] « *everything is running as expected* » (McIntyre & Salas, 1995, p. 23)

[37] « keep track of fellow team member's work while carrying out their own » (McIntyre & Salas, 1995, p. 23)

Hypothèse 3 : Une diminution du niveau de CI entraîne une augmentation du temps total mis par le confiant pour réaliser les tâches, ce qui constitue un comportement de compensation.

La littérature sur la CI mentionne déjà des comportements de compensation mis en place par le confiant lorsqu'il n'a pas confiance dans les décisions du mandant. Le niveau de confiance du confiant dans le mandant aurait pour conséquence de modifier la manière dont le confiant perçoit les actions effectuées par le mandant (Dirks & Ferrin, 2001) mais aussi la manière dont il perçoit la performance de l'équipe. Cette modification de perception qu'a le confiant des résultats des tâches effectuées par le mandant peut alors entraîner une supervision contre-productive. Dans certains cas le confiant pourrait prendre en compte des mauvaises informations fournies par le mandant et dans d'autres cas le confiant pourrait ne pas prendre en compte de bonnes informations fournies par le mandant. Ainsi, lorsque le niveau de confiance entre le confiant et le mandant est faible, le confiant perçoit les actions effectuées par le mandant comme étant mauvaises ce qui entraîne la mise en place de comportements permettant de rattraper les erreurs détectées. Les hypothèses suivantes sont donc proposées :

Hypothèse 4 : Une augmentation du niveau de CI entraîne une plus grande acceptation, par le confiant, des informations transmises par le mandant.

Hypothèse 5 : Une augmentation du niveau de CI entraîne une diminution du nombre de supervisions contre-productives.

Ces notions de perception et d'action sous-tendant les hypothèses 2, 3, 4 et 5 se retrouvent fréquemment dans la littérature sur la prise de décision et plus particulièrement dans la littérature portant sur la prise de décision sous pression temporelle. Comme pour la CI , une augmentation de la pression temporelle serait fortement liée à une réduction de la recherche d'information (hypothèse 2) mais également à une mauvaise perception des informations (hypothèse 4) entrainant un mauvais jugement (Zakay, 1993). De plus, comme la CI, le temps serait un modulateur des stratégies (Johnston et al., 2004). La pression temporelle et la CI auraient donc des conséquences comportementales similaires. Seulement, dans la littérature, la pression temporelle est considérée comme l'une des variables les plus importantes dans la réalisation des tâches (Payne, Bettman, & Johnson, 1988) et devrait donc plus fortement modifier le comportement des individus que ce que le fait la CI. La pression temporelle étant un phénomène majeur en termes d'arbitrage de prise de décision, montrer que la CI a le pas dessus serait un résultat majeur. L'hypothèse suivante est proposée :

Hypothèse 6 : Sous forte pression temporelle, le niveau de CI ne module pas le nombre de supervisions, ni l'augmentation du temps total, ni l'acceptation par le confiant des informations transmises par le mandant, ni le nombre de supervisions contre-productives.

3. Comportements et caractéristiques psychosociales du confiant

Dans cette deuxième partie seront posées les hypothèses relatives aux liens présents entre le groupe social et le comportement des individus (liens orange dans la figure 35). Cette deuxième partie vise à observer si les comportements sont homogènes au sein du groupe social du confiant, indépendamment du niveau de CI induit. Cette deuxième partie visera à tester si les facteurs sociaux (différences interindividuelles) identifiés chez les potentiels opérateurs de la RCPair dans la partie analyse du besoin, sont à même de modifier le comportement de l'individu. Pour rappel, dans l'analyse du besoin les facteurs sociaux identifiés étaient :

- Le métier ;
- Le grade et les études (qui correspondent ici à l'expérience) ;
- l'environnement de travail (certains opérationnels de l'AA travaillent toujours sur des bases aériennes présentes sur le territoire français alors que d'autres peuvent partir en OPEX. Dans l'environnement de travail « OPEX », un fort risque vital est présent ce qui est moins le cas dans l'autre environnement de travail).

Par "comportements", seront considérés ici ceux utilisés dans les hypothèses 2, 3, 4 et 5, c'est à dire le fait de superviser, l'augmentation du temps total, l'efficacité des supervisions et l'acceptation par le confiant des informations transmises par le mandant.

Il a été mentionné dans le cadre théorique que le niveau de confiance entre deux individus pouvait être mis en place par un mécanisme dénommé confiance par apprentissage social. Dans cette littérature, le confiant se base sur les RS qu'il a du mandant. Ces RS permettent aux individus de reconnaître une personne comme appartenant à une catégorie (par exemple « de confiance » ou « pas de confiance ») en fonction de certaines caractéristiques de cette personne. Par ailleurs, ces RS (Abric, 2003) ne sont pas homogènes dans la population mais dépendent du groupe social dans lequel elles sont mobilisées.

Chaque groupe social (Abric, 2003) possède ses propres RS qui sont un ensemble d'opinions, d'attitudes et de croyances à propos d'un objet donné, qui conditionnent ses comportements. Les éléments les plus partagés de ces RS (ou éléments centraux) génèrent par ailleurs au sein du groupe social des comportements homogènes (Abric, 2003). Cette théorie suggère donc que dans un groupe social, les comportements ne seront pas fonction du niveau de CI présent dans la relation mais fonction des RS du groupe.

Les RS que le confiant a du mandant sont conditionnées par les caractéristiques du groupe social auquel appartient le confiant. Ainsi, dans le cadre professionnel, la littérature s'est déjà attachée à étudier le lien entre CI et culture (Huff & Kelley, 2003), ou entre CI et communauté partageant les mêmes normes (Delhey et al., 2011). Cependant, ces différentes études ont été menées afin de comparer la confiance de personnes provenant de localités différentes (comparaison entre pays voire continents). Dans ces études, le groupe social caractérisant le confiant était par conséquent multifactoriel (langue, culture…) car dépendant du pays voire du continent d'appartenance. Les différents opérateurs potentiels de la RCPair seront tous des français travaillant dans le milieu de l'aéronautique et devraient donc avoir des RS similaires. Cependant, le métier de ces opérateurs (personnel navigant, contrôleurs aériens, mécaniciens) pourrait constituer un sous-

groupe social qui pourrait moduler le comportement des individus indépendamment du niveau de CI. Ceci amène à l'hypothèse suivante :

Hypothèse 7 : Dans un même milieu professionnel, le métier des individus et non pas le niveau de CI fait varier les comportements.

D'autre part, ces comportements peuvent être fonction du groupe ou de l'institution auquel appartient l'individu (Bachmann & Inkpen, 2011) mais peuvent également être fonction de l'expérience de l'individu. De fait, les experts ont des stratégies différentes pour la réalisation d'une tâche (Kasarskis et al., 2001), des compétences plus adaptées à la tâche et un plus grand nombre de connaissances que les novices. Cet ensemble permet aux experts d'utiliser moins de temps pour analyser les situations et de mieux planifier les tâches à faire (Chi et al., 2014). La supervision comme la compensation nécessitent que le confiant ait les connaissances et compétences nécessaires à l'analyse de ce que le mandant doit faire pour améliorer la situation (Dickinson & McIntyre, 1997), et il est donc plausible que le niveau d'expertise puisse participer à la modification du comportement. Autrement dit, un expert réaliserait une supervision et une compensation plus efficaces qu'un novice.

Hypothèse 8 : Dans un même métier, le niveau d'expertise des individus et non pas le niveau de CI fait varier les comportements.

Les comportements des individus dépendent également de la perception du risque et de la situation (Grazioli & Jarvenpaa, 2000; van der Heijden et al., 2003). Dans le milieu militaire notamment, la CI s'établit sur la perception qu'a le confiant de la situation et du risque (Dirks, 1999 ; Rotter, 1980). Cette perception du risque est fortement liée à la *disposition to trust* (Siegrist et al., 2005; Siegrist & Cvetkovich, 2000) mais également au cadre de survenu (personnel ou professionnel) de cette situation. Une situation mise en place dans un certain cadre institutionnel pourrait paraître normale à un groupe social donné (McKnight et al., 1998) et sembler être non risquée, alors qu'elle serait perçue différemment dans un autre cadre par un autre groupe social. De fait, le risque présent dans l'environnement de travail d'un individu modifie la perception qu'a cet individu du risque. Ainsi, selon l'environnement de travail, une situation, caractérisée par certains groupe sociaux, comme étant fortement risquée, pourrait être ressentie, par d'autres groupes sociaux, comme étant normale. Par extension, on suppose que l'exposition au risque est un facteur constitutif d'un groupe social spécifique. Ceci permet de proposer les hypothèses suivantes :

Hypothèse 9 : Dans un même métier, l'exposition au risque des individus et non pas le niveau de CI fait varier les comportements.

Hypothèse 10 : Pour une même exposition au risque, le métier des individus et non pas le niveau de CI fait varier les comportements.

Les hypothèses 2, 3, 4, 5 et 6 permettront donc d'étudier le lien entre niveau de CI et comportement (lien bleu sur la figure 35). Les hypothèses 7, 8, 9 et 10 permettront d'étudier si un lien direct est présent entre le groupe social d'appartenance de l'individu et le comportement (lien orange sur la figure 35). Ces dernières hypothèses permettront d'étudier si les comportements sont directement liés aux caractéristiques psychosociales de l'individu ou si ces comportements sont liés au niveau initial de CI du confiant. Le but de cette expérimentation est donc de trancher entre deux alternatives contradictoires permettant d'étudier les facteurs pouvant impacter le comportement des individus dans le cas particulier d'un contexte représentatif de la RCPair.

4. Matériel et méthodes

A. Participants

200 personnes (11.9% de femmes et 88.1% d'hommes) d'âge moyen 29.9 ans (SD = 6 ans) ont participé à cette étude.

Parmi ces 200 participants

- 40 (17.5% de femmes et 82.5% d'hommes) étaient des contrôleurs aériens expérimentés d'âge moyen 34.2 ans (SD = 9.40 ans) et travaillant sur base ;
- 40 (9.5% de femmes et 90.5% d'hommes) étaient des élèves pilotes ou navigateurs (PN) non expérimentés d'âge moyen 22 ans (SD = 1.2 ans) étant encore à l'école ;
- 40 (2.5% de femmes et 97.5% d'hommes) étaient des pilotes ou navigateurs expérimentés d'âge moyen 33.9 ans (SD = 6.12%) ayant effectué des OPEX ;
- 40 (11% de femmes et 88% d'hommes) étaient des mécaniciens expérimentés d'âge moyen 27.5 ans (SD = 6.43) ayant toujours travaillé sur base ;
- 40 (19% de femmes et 81% d'hommes) étaient des mécaniciens expérimentés d'âge moyen 32.1 ans (SD = 6.85) ayant effectué des OPEX.

B. Matériel

L'expérimentation suit exactement le protocole expérimental présenté au chapitre 5. L'expérimentation est découpée en 42 essais comprenant chacun les trois phases successives (*cf.* Figure 36). Phase (1) induction du niveau de CI, (2) tâche de comptage et tâche de supervision (facultative) et (3) évaluation subjective des degrés de certitude de la réponse du partenaire, du comptage du participant et du score global. Un essai correspond à l'ensemble des 3 phases. 42 essais doivent être validés pour mettre fin à l'expérience. Il y a 14 essais par condition de niveau de CI (fort, intermédiaire, faible). L'expérimentation se déroule sur un ordinateur portable avec un écran de 15 pouces d'une résolution de 1920*1080 et une souris.

Afin de tester l'hypothèse 6 (selon laquelle sous forte pression temporelle le niveau de CI ne modulera pas le nombre de supervisions, ni l'augmentation du temps total, ni l'acceptation par le confiant des informations transmises par le mandant), deux conditions expérimentales ont été mises en œuvre. La première condition consistait à faire passer l'expérimentation sous forte pression temporelle et la deuxième sans pression temporelle. 50% des participants ont passé l'expérimentation dans la condition expérimentale pression temporelle et 50% des participants ont passés l'expérimentation dans la condition expérimentale sans pression temporelle. La condition

expérimentale pression temporelle correspondait à ce qui a été présenté au chapitre 4 (*Cf.* chapitre 4 « 2. Protocole expérimental »). Dans cette condition les images étaient calibrées en prenant la moyenne des temps mis par 7 personnes pour compter, le plus rapidement possible le nombre d'aéronefs présents sur chaque image. Pour mettre en œuvre la condition expérimentale sans pression temporelle la moyenne du temps mis par 7 personnes (qui n'ont jamais participé ni à aucune de des expérimentations ni à la calibration de la condition expérimentale pression temporelle) pour compter les images le plus exactement possible et sans limite de temps, a été considérée. Dans la condition expérimentale sans pression temporelle, les participants avaient approximativement 30% de temps en plus pour réaliser les tâches que les participants dans la condition pression temporelle.

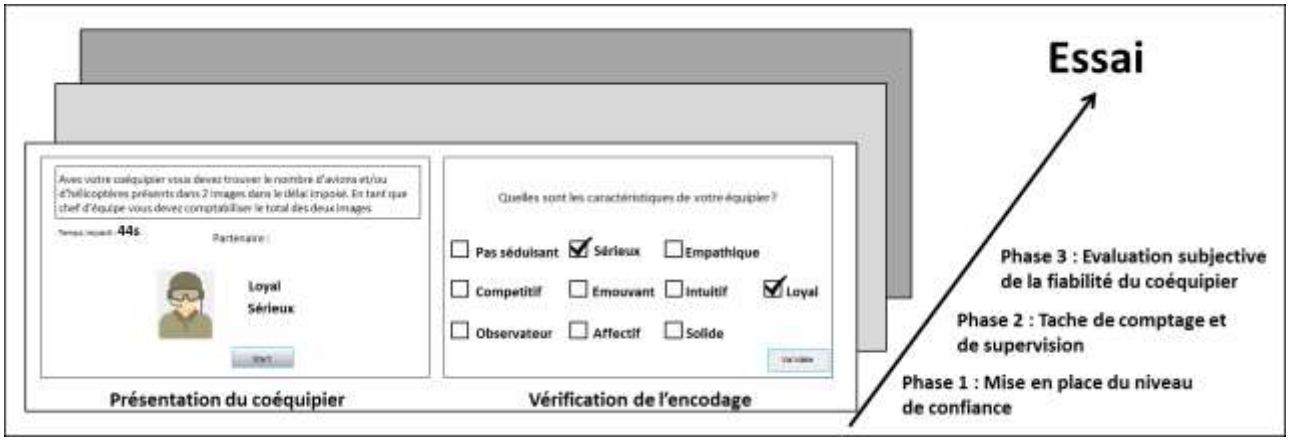


Figure 36 : Présentation de l'expérimentation qui se compose de 42 essais différents de 3 phases chacun. Chaque essai est effectué avec un partenaire différent représenté par une paire de mots en phase 1. Sur l'affichage de la phase 1 le participant prenait connaissance de la consigne (similaire tout au long de l'expérimentation), du temps alloué à la tache (ce temps est différent selon les images) et des caractéristiques de son coéquipier. Ces caractéristiques induisaient, chez le participant un niveau de confiance soit faible soit moyen soit élevé.

5. Résultats

Les données des 200 participants sont incluses dans l'analyse, soit dans leur intégralité (test des hypothèses 2, 3, 4 et 5) soit regroupées en différentes classes de caractéristiques sociales (test des hypothèses 6, 7, 8, 9 et 10) (*Cf.* Figure 37). Pour le test de l'hypothèse 6 les données des 200 participants sont incluses dans l'analyse mais divisées en deux classes (avec ou sans pression temporelle).

Les 200 participants font tous parti du même milieu professionnel, l'aéronautique militaire, mais n'ont pas tous les mêmes caractéristiques « sociales ». Ainsi, ces participants sont divisés en :

- 3 groupes de métier (les PN, les contrôleurs aériens et les mécaniciens) ;
- 2 groupes d'expérience (en formation et expérimentés) ;
- 3 groupes d'environnement de travail (Ecole, Base et OPEX).

Comme le montre la figure 37 :

- 40 PN étaient encore en formation et étaient encore à l'école (ils n'avaient jamais exercé) ;
- 40 PN étaient expérimentés et avaient effectués des OPEX ce qui correspond à un environnement à fort risque vital perçu ;

- 40 contrôleurs aériens étaient expérimentés et avaient toujours travaillé sur base ce qui correspond à un environnement à faible risque vital perçu ;
- 40 mécaniciens étaient expérimentés et avaient effectués des OPEX ce qui correspond à un environnement à fort risque vital perçu ;
- 40 mécaniciens aériens étaient expérimentés et avaient toujours travaillé sur base ce qui correspond à un environnement à faible risque vital perçu.

Dans la matrice présentée à la figure 37 les groupes ayant le même symbole et étant sur la même ligne sont comparables entre eux. Les groupes partageant une même case ou étant sur la même colonne sont également comparables entre eux

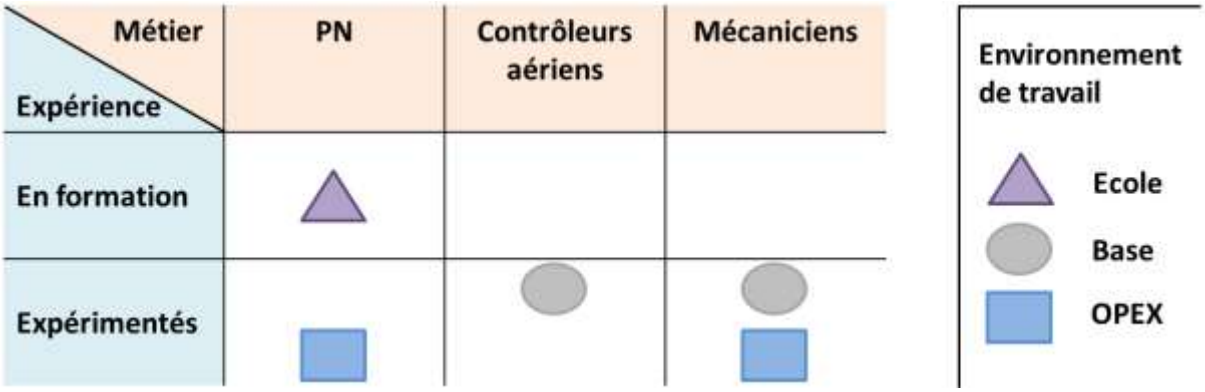


Figure 37 : Matrice montrant les caractéristiques sociales des participants.
Les participants sont divisés en 3 groupes métier, 2 groupes d'expérience et 3 groupes d'environnement de travail. Chaque symbole présenté dans cette matrice correspond à 40 participants

Afin de choisir les groupes nécessaires aux tests des hypothèses 6, 7, 8 et 9 une matrice de répartition des 200 participants a été tracée (*Cf.* Tableau 6). Cette matrice de répartition montre les différences, en terme de caractéristiques sociales (métier expérience et environnement) entre chaque groupes de participants (contrôleurs aériens, élèves PN, PN expérimentés, mécaniciens - OPEX, mécaniciens – Base) représentés. Dans la mesure du possible, seuls les groupes ayant une seule différence sociale ont été comparés.

Pour la différence portant sur le métier (hypothèse 7) les groupes contrôleurs aériens et mécaniciens travaillant sur base ont été comparés. Aucune paire de groupe n'avait comme seule différence le niveau d'expérience (hypothèse 8). Ainsi, afin d'étudier cette différence, les groupes PN expérimentés et élèves PN (qui semblent être les groupes les plus proches car ayant seulement deux différences sociales) ont été comparés. Pour la différence portant sur l'environnement de travail dans un même métier (hypothèse 9) les groupes mécaniciens ayant déjà fait des OPEX et le groupe mécaniciens travaillant sur base ont été comparés. Enfin, pour la différence portant sur l'exposition au risque dans des métiers différents (hypothèse 10) les mécaniciens ayant fait des OPEX et le groupe PN ayant fait des OPEX ont été comparés.

Tableau 6 : Matrice de répartition des 200 participants.
Chaque case (contrôleurs aériens, élèves PN, PN expérimentés, mécaniciens - OPEX, mécaniciens – Base) représente 40 participants. Chaque case est composée de 3 caractéristiques (métier, expérience et environnement). Cette matrice montre les caractéristiques sociales différentes entre chaque groupe. Les cases en bleu correspondent aux groupes qui ont été choisis pour observer une différence comportementale due aux caractéristiques psychosociales des individus.

	Contrôleurs aériens	**Élèves PN**	**PN expérimentés**	**Mécaniciens – OPEX**	**Mécaniciens – Base**
Contrôleurs aériens					
Élèves PN	Métier Expérience Environnement				
PN expérimentés	Métier Environnement	**Expérience Environnement**			
Mécaniciens – OPEX	Métier Environnement	Métier Expérience Environnement	**Métier ****		
Mécaniciens – Base	**Métier***	Métier Expérience Environnement	Métier Environnement	**Environnement**	

*** pour des opérateurs expérimentés, dans un environnement base (à faible risque perçu)**
**** pour des opérateurs expérimentés, dans un environnement OPEX (à fort risque perçu)**

Les variables dépendantes étudiées sont : la perception qu'a le participant des performances de son coéquipier (CertitudePartenaire), le pourcentage de supervisions (%VDsup), le pourcentage total de temps passé avant de terminer un essai (%Tempstot), le pourcentage de modifications (%VDmodif) et le pourcentage de supervisions contre-productives (%VDm_sup).

Pour chaque variable dépendante les moyennes sont calculées en fonction du niveau CI induit, faible moyen ou élevé. Afin de tester les différentes hypothèses, des ANOVA à mesures répétées sont effectuées sur chaque variable dépendante. La sphéricité de la matrice de covariance est vérifiée avec un test de Mauchly (Mauchly, 1940). En cas de non sphéricité, le test F est corrigé par la méthode de Greenhouse-Geisser (McCall & Appelbaum, 1973). Lorsqu'il ne donne pas de résultats différents au test F non corrigé (changement de significativité), le F corrigé n'est pas reporté ici. Dans le cas d'une ANOVA multifactorielle significative des tests post-hoc de type Tukey HSD sont réalisés.

A. Test des hypothèses 2, 3, 4, 5 et 6

Les tests des hypothèses 2, 3, 4, 5 et 6 ont été réalisés sur l'ensemble des 200 participants. Aucune distinction d'expérience, de métier ou d'environnement de travail n'a été prise en compte dans les différentes analyses présentées ci-dessous.

a. Test de l'hypothèse 2 : Une diminution du niveau de CI entraîne une augmentation du nombre de supervisions

Afin de tester cette hypothèse, les données relatives au pourcentage de supervision ont été utilisées. L'analyse descriptive de ces données tend à montrer que le pourcentage de supervision est différent entre le niveau de confiance faible (M = 88.04%, SD = 22.06%), le niveau de confiance moyen (M = 85.93%, SD = 23.20%) et le niveau de confiance élevé (M = 79.13%, SD = 28.86%). Le résultat significatif, $F(2,398) = 32.66$, $p < .001$*** permet de valider l'hypothèse 2. En d'autres termes, une diminution du niveau de CI entraîne bien une augmentation du nombre de supervisions.

b. Test de l'hypothèse 3 : Une diminution du niveau de CI entraîne une augmentation du temps total utilisé par la confiant pour réaliser les tâches.

Afin de tester cette hypothèse, les données relatives au pourcentage de temps total passé avant de terminer un essai ont été utilisées. L'analyse descriptive de ces données tend à montrer que pourcentage de temps total passé avant de terminer un essai est différent entre le niveau de confiance faible (M = 80.43%, SD = 8.20%), le niveau de confiance moyen (M = 79.72%, SD = 8.44%) et le niveau de confiance élevé (M = 78.07%, SD = 9.97%). Le résultat significatif, $F(2,398) = 22.54$, $p < .001$*** permet de valider l'hypothèse 3. En d'autres termes, une diminution du niveau de CI entraîne une augmentation du temps total mis par la confiant pour réaliser les tâches.

c. Test de l'hypothèse 4 : Une augmentation du niveau de CI entraîne une plus grande acceptation, par le confiant, des informations transmises par le mandant.

Afin de tester cette hypothèse, les données relatives au pourcentage de modification ont été exploitées. L'analyse descriptive de ces données tend à montrer que le pourcentage de modification est différent entre le niveau de confiance faible (M = 48.52%, SD = 27.66%), le niveau de confiance moyen (M = 45.14%, SD = 27.46%) et le niveau de confiance élevé (M = 40.09%, SD = 28.13%). Le résultat significatif, $F(2,398) = 25.94$, $p < .001$*** permet de valider l'hypothèse 4. En d'autres termes, une augmentation du niveau de CI entraîne une plus grande acceptation, par le confiant, des informations transmises par le mandant.

d. Test de l'hypothèse 5 : Une augmentation du niveau de CI entraîne une diminution du nombre de supervisions contre-productives

Afin de tester cette hypothèse, les données relatives au pourcentage de supervisions contre-productives ont été exploitées. L'analyse descriptive de ces données tend à montrer que le pourcentage de supervisions contre-productives est différent entre le niveau de confiance faible (M = 48.87%, SD = 26.99%), le niveau de confiance moyen (M = 47.57%, SD = 26.87%) et le niveau de

confiance élevé (M = 43.32%, SD = 28.75%). Le résultat significatif, $F(2,398) = 8.71$, $p < .001$*** permet de valider l'hypothèse 5. En d'autres termes, une augmentation du niveau de CI entraîne une diminution du nombre de supervisions contre-productives.

e. *Test de l'hypothèse 6 : Sous forte pression temporelle, le niveau de CI ne module pas le nombre de supervisions, ni l'augmentation du temps total, ni l'acceptation par le confiant des informations transmises par le* mandant*, ni le nombre de supervisions contre-productives*

Tableau 7 : Moyenne, écart type et résultats de l'ANOVA à mesures répétées pour la variable indépendante pression temporelle et pour les variables dépendantes *CertitudePartenaire, %VDsup, %Tempstot, %VDmodif et %VDm_sup*

Variable dépendante	Moyenne (M) et écart type (SD) pour les différentes VD sous forte pression temporelle			Moyenne (M) et écart type (SD) pour les différentes VD sans pression temporelle			ANOVA simple effet (CI)		ANOVA simple effet (pression temporelle)		ANOVA effet d'interaction (CI*pression temporelle)	
	Faible	Moyen	Elevé	Faible	Moyen	Elevé	F(2, 396)	P-value	F(1, 198)	P-value	F(2, 156)	P-value
CertitudePartenaire	M = 4.80 SD = 2.09	M = 5.67 SD = 1.90	M = 6.75 SD = 1.82	M = 4.95 SD = 2.44	M = 5.67 SD = 2.07	M = 6.62 SD = 2.02	131.5	<.001***	.001	.95	.79	.45
%VDsup	M = 81.86 SD = 26.60	M = 79.16 SD = 27.50	M = 72.34 SD = 31.23	M = 94.21 SD = 13.90	M = 92.71 SD = 15.26	M = 85.91 SD = 24.62	32.52	<.001***	17.66	<.001***	.18	.83
%TempsTot	M = 83.97 SD = 6.69	M = 83.24 SD = 6.94	M = 81.45 SD = 8.17	M = 76.89 SD = 8.08	M = 76.20 SD = 8.36	M = 74.69 SD = 10.49	22.44	<.001***	41.14	<.001***	.11	.89
%VDmodif	M = 31.97 SD = 23.90	M = 27.86 SD = 22.68	M = 23.82 SD = 22.17	M = 65.07 SD = 20.35	M = 62.42 SD = 19.96	M = 56.36 SD = 23.76	25.85	<.001***	139.50	<.001***	.39	.67
%VDm_sup	M = 34.41 SD = 26.06	M = 31.49 SD = 24.47	M = 27.22 SD = 25.98	M = 63.34 SD = 19.03	M = 63.66 SD = 18.18	M = 59.42 SD = 21.52	8.71	<.001***	124.21	<.001***	.91	.40

Les résultats obtenus en comparant les groupes ayant passé l'expérimentation avec et sans pression temporelle (*Cf.* Tableau 7) montrent que, qu'elle que soit la pression temporelle, l'induction de différents niveaux de CI a bien fonctionné (les résultats de l'ANOVA montrent un effet simple de la CI). L'absence d'effet d'interaction est ici interprétée comme montrant une absence d'influence de la pression temporelle sur le niveau de confiance que le participant attribue à son coéquipier.

Les résultats des statistiques descriptives portant sur les différentes variables comportementales étudiées (%VDsup, %Tempstot, %VDmodif et %VDm_sup) semblent montrer que, quelle que soit la pression temporelle, le niveau de confiance présent dans la relation modifie le comportement de supervision, de gestion du temps, d'acceptation des informations transmises par le coéquipier et l'efficacité de la supervision. Les résultats obtenus en statistiques inférentielles valident cela et montrent, pour chaque variable comportementale, un effet simple du niveau de confiance mais aucun effet d'interaction. Pris tous ensemble, ces résultats ne permettent pas de valider l'hypothèse 6. En d'autres termes, que ce soit sous faible ou sous forte pression temporelle, le niveau de CI module, chez le confiant, son comportement de supervisions, l'efficacité (productivité) de ces supervisions, son comportement de gestion du temps et acceptation des informations transmises par le mandant.

B. Test des hypothèses 7, 8, 9 et 10

Afin de tester ces différentes hypothèses, les données ont été comparées groupe à groupe. Il est important de noter qu'une interaction significative (groupe * niveau de CI) n'indique pas forcément qu'un groupe a un comportement différent en fonction du niveau de CI alors que l'autre groupe a un comportement similaire quel que soit le niveau de CI. En effet, une interaction significative peut également signifier qu'un groupe à une différence très forte de comportement selon le niveau de CI alors que l'autre groupe a une différence de comportement plus faible (comparé au groupe précédent) selon le niveau de CI. Il est donc important, avant d'analyser les résultats d'interaction, de prendre en compte, pour chaque groupe social, les résultats des effets simples qui sont détaillés dans le tableau 8 (pour plus de lisibilité les moyennes et écart type ne sont pas reportés dans ce tableau mais sont reportés dans la suite du document) et qui sont présentés ci-dessous.

- Le niveau de certitude attribué au participant est dépendant du niveau de CI pour tous les groupes sociaux. Ce résultat confirme que pour tous les groupes sociaux les inducteurs de CI ont bien fonctionnés et que les coéquipiers sont bien ressentis de manière différente en fonction de leurs caractéristiques.
- Le pourcentage de supervision est dépendant du niveau de CI pour les PN expérimentés, les contrôleurs aérien et les élèves PN. Cependant, rien ne permet d'affirmer que le pourcentage de supervision soit dépendant du niveau de CI pour les deux groupes de mécaniciens.
- Le pourcentage de temps total passé à effectuer les tâches est dépendant du niveau de CI pour les groupes mécaniciens (Base), contrôleurs aériens et élèves PN. Rien ne permet d'affirmer que le pourcentage de temps total passé à effectuer les tâches soit dépendant du niveau de CI pour les groupes mécaniciens (OPEX) et PN expérimentés.
- Enfin, le pourcentage de modifications est dépendant du niveau de CI pour les groupes mécaniciens (Base), contrôleurs aériens et élèves PN. Rien ne permet d'affirmer que le pourcentage de modifications soit dépendant du niveau de CI pour les groupes mécaniciens (OPEX) et PN expérimentés.
- Enfin, le pourcentage de supervisions contre-productives est dépendant du niveau de CI pour les groupes mécaniciens (Base) et élèves PN. Rien ne permet d'affirmer que le pourcentage le pourcentage de supervisions contre-productives soit dépendant du niveau de CI pour les groupes mécaniciens (OPEX), PN expérimentés et contrôleurs aériens.

Tableau 8 : Résultats, pour toutes les variables dépendantes, des effets simples obtenus sur la variable indépendante CI pour les différents groupes sociaux

Variable dépendante	ANOVA simple effet (CI) pour les différentes VD pour le groupe mécaniciens (OPEX)		ANOVA simple effet (CI) pour les différentes VD pour le groupe mécaniciens (Base)		ANOVA simple effet (CI) pour les différentes VD pour le groupe PN expérimentés		ANOVA simple effet (CI) pour les différentes VD pour le groupe contrôleurs aériens		ANOVA simple effet (CI) pour les différentes VD pour le groupe élèves PN	
	F(2, 78)	P-value	F(2, 78)	P-value	F(2, 78)	P-value	F(2, 78)	P-value	F(2, 78)	P-value
CertitudePartenaire	13.40	<.001***	21.67	<.001***	30.37	<.001***	26.88	<.001***	47.79	<.001***
%VDsup	1.15	.31	2.08	.13	4.31	.01*	11.78	<.001***	18.60	<.001***
%TempsTot	.75	.47	3.94	.02*	.94	.39	12.90	<.001***	13.84	<.001***
%VDmodif	1.49	.23	6.29	0.002**	3.06	0.05	8.95	.003**	16.05	<.001***
%VDm_sup	1.31	.27	5.31	0.006**	1.34	.26	1.36	.26	5.76	.004**

Cette première analyse globale permet d'identifier l'impact de la CI sur le comportement de chaque groupe d'opérateurs. Ces effets vont maintenant être comparés entre des groupes particuliers afin de valider une à une les hypothèses. Pour chaque hypothèse, les résultats des 5 VD (CertitudePartenaire, %VDsup, %TempsTot, %VDmodif et %VDm-sup) sont étudiés. Afin de faciliter la lecture, un paragraphe spécifique est alloué à l'étude des résultats de chacune de ces VD. Cependant, il est à noter que tous les paragraphes sont rédigés de manière identique et ont des éléments de langages communs.

a. Test de l'hypothèse 7 : Dans un même milieu professionnel, le métier des individus et non pas le niveau de CI fait varier les comportements.

Afin de tester cette hypothèse, les données obtenues auprès des 40 contrôleurs aériens expérimentés et auprès des 40 mécaniciens expérimentés travaillant sur base ont été exploitées. Les variables dépendantes utilisées afin de tester cette hypothèse sont similaires aux variables dépendantes utilisées pour tester les hypothèses 2, 3, 4 et 5. Avant de tester cette hypothèse, le bon fonctionnement du matériel d'induction sur ces deux classes de populations a été testé.

Tableau 9 : Moyenne, écart type et résultats de l'ANOVA a mesures répétées pour les groupes contrôleurs aériens et mécaniciens n'ayant jamais fait d'OPEX et pour les variables dépendantes *CertitudePartenaire, %VDsup, %Tempstot, %VDmodif et %VDm_sup*

Variable dépendante	Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe contrôleurs aériens			Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe mécaniciens (Base)			ANOVA simple effet (CI)		ANOVA simple effet (Métier)		ANOVA effet d'interaction (CI*Métier)	
	Faible	Moyen	Elevé	Faible	Moyen	Elevé	F(2, 156)	P-value	F(1, 78)	P-value	F(2, 156)	P-value
CertitudePartenaire	M = 4.62 SD = 2.77	M = 5.42 SD = 2.35	M = 6.58 SD = 2.21	M = 5.14 SD = 1.75	M = 5.71 SD = 1.73	M = 6.59 SD = 1.54	48.47	<.001***	.41	.52	1.08	.34
%VDsup	M = 84.82 SD = 25.89	M = 81.87 SD = 27.17	M = 70.71 SD = 34.30	M = 88.21 SD = 22.38	M = 86.42 SD = 22.57	M = 84.55 SD = 22.44	13.42	<.001***	1.76	.18	5.20	.006**
%TempsTot	M = 80 SD = 7.01	M = 77.74 SD = 8.68	M = 75.90 SD = 10.44	M = 80.46 SD = 7.33	M = 80.82 SD = 7.91	M = 79.01 SD = 7.72	14.21	<.001***	1.61	.20	4.13	.01*
%VDmodif	M = 48.03 SD = 30.56	M = 43.66 SD = 29.44	M = 36.25 SD = 29.04	M = 42.32 SD = 28.58	M = 36.78 SD = 28.96	M = 34.74 SD = 28.53	14.62	<.001***	.57	.45	1.24	.29
%VDm_sup	M = 47.02 SD = 30.10	M = 47.21 SD = 30.88	M = 42.82 SD = 31.27	M = 42.09 SD = 26.43	M = 36.61 SD = 27.70	M = 35.26 SD = 27.67	4.35	.01*	1.57	.21	1.15	.31

Hypothèse 7, Test du matériel d'induction : Perception de la performance du coéquipier

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 9 ligne CertitudePartenaire) que dans le groupe contrôleurs aériens la perception qu'a le participant des performances de son coéquipier est différente entre le niveau de confiance faible (M = 4.62, SD = 2.77), le niveau de confiance moyen (M = 5.42, SD = 2.35) et le niveau de confiance élevé (M = 6.58, SD = 2.21). Dans le groupe mécaniciens (Base), la perception qu'a le participant des performances de son coéquipier semble également être différente entre le niveau de confiance faible (M = 5.14, SD = 1.75), le niveau de confiance moyen (M = 5.71, SD = 1.73) et le niveau de confiance élevé (M = 6.59, SD = 1.54). L'effet simple du niveau de confiance, $F(2,156) = 48.47$, $p < .001$*** permet de valider que le niveau de confiance induit influe sur la perception qu'a le participant de la performance de leur coéquipier. En d'autres termes, le matériel d'induction fonctionne sur ces deux populations et induit différents niveaux de confiance aux participants. L'absence d'effet simple sur le métier, $F(1,78) = .41$, $p = .52$ et l'absence d'effet d'interaction, $F(2,156) = 1.08$, $p = .34$ sont ici interprétés comme montrant une absence d'influence du métier sur le niveau de confiance que le participant attribue à son coéquipier.

Hypothèse 7 : Pourcentage de supervision

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 9 ligne %VDsup) que dans le groupe contrôleurs aériens une différence est présente sur le pourcentage de supervision entre le niveau de confiance faible (M = 84.82%, SD = 25.89%), le niveau de confiance moyen (M = 81.87%, SD = 27.17%) et le niveau de confiance élevé (M = 70.71%, SD = 34.30%). Dans le groupe mécaniciens (Base) le pourcentage de supervisions semble être relativement proche entre le niveau de confiance faible (M = 88.21%, SD = 22.38%), le niveau de confiance moyen (M = 86.42%, SD = 22.57%) et le niveau de confiance élevé (M = 84.55%, SD = 22.44%). L'interaction significative, $F(2,156) = 5.20$, $p = .006$** et les résultats des tests post-hoc (*Cf.* Tableau 10) permettent de valider ces observations qui ne vont pas dans le sens de l'hypothèse 7. Autrement dit, à environnement de travail et niveau d'expérience égal, le comportement de supervision est

différent selon le métier et selon le niveau de CI présent dans la relation. Les contrôleurs aériens adaptent leur comportement de supervision en fonction du niveau de CI présent dans la relation alors que les mécaniciens ont un comportement de supervision similaire quel que soit le niveau de confiance présent dans la relation.

Tableau 10 : Test post-hoc HSD de Tukey pour la variable dépendante %VDsup et pour les groupes contrôleur aérien et mécanicien n'ayant jamais fait d'OPEX (*Cf.* annexe 3).
Ce test post-hoc indique que chez les contrôleurs aériens une différence significative est présente entre les valeurs de la variable %VDSup quand on compare la classe CI faible avec la classe CI Elevé (première colonne, deuxième ligne, p<.001*) ainsi que pour la comparaison des classes de CI moyen avec CI élevée (deuxième colonne, deuxième ligne, p<.001***). Pour toutes les autres comparaisons, les différences sur les valeurs de la variable %VDsup ne sont pas significatives (p=1).**

	Test post-hoc HSD de Tukey pour la variable dépendante %VDsup		
	Faible	**Moyen**	
Contrôleurs aériens	-	$p = 1$	**Faible**
	$p < .001$***	$p < .001$***	**Elevé**
Mécaniciens (Base)	-	$p = 1$	**Faible**
	$p = 1$	$p = 1$	**Elevé**

Hypothèse 7 : Pourcentage de temps total utilisé

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 9 ligne %TempsTot) que dans le groupe contrôleurs aériens une différence est présente sur le pourcentage de temps total utilisé entre le niveau de confiance faible (M = 80%, SD = 7.01%), le niveau de confiance moyen (M = 77.74%, SD = 8.68%) et le niveau de confiance élevé (M = 75.90%, SD = 10.44%). Dans le groupe mécaniciens (Base), le pourcentage de temps total utilisé semble être relativement proche entre le niveau de confiance faible (M = 80.46%, SD = 7.33%), le niveau de confiance moyen (M = 80.82%, SD = 7.91%) et le niveau de confiance élevé (M = 79.01%, SD = 7.72%). L'interaction significative, $F(2,156) = 4.13$, $p = .01$* et les résultats des tests post-hoc (*Cf.* Tableau 11) permettent de valider ces observations qui ne vont pas dans le sens de l'hypothèse 7. Autrement dit, à environnement de travail et niveau d'expérience égal le comportement de gestion du temps est différent selon le métier et selon le niveau de CI présent dans la relation. Les contrôleurs aériens adaptent leur gestion du temps en fonction du niveau de confiance présent dans la relation alors que les mécaniciens utilisent leur temps de manière similaire quel que soit le niveau de confiance présent dans la relation.

Tableau 11 : Test post-hoc HSD de Tukey pour la variable dépendante %TempsTot et pour les groupes contrôleur aérien et mécanicien n'ayant jamais fait d'OPEX (*Cf.* annexe 3).

Test post-hoc HSD de Tukey pour la variable dépendante %TempsTot			
	Faible	**Moyen**	
Contrôleurs aériens	-	$p = .03$*	**Faible**
	$p < .001$***	$p = .20$	**Elevé**
Mécaniciens (Base)	-	$p = 1$	**Faible**
	$p = .79$	$p = .23$	**Elevé**

Hypothèse 7 : Pourcentage de modifications

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 9 ligne %VDmodif) que dans le groupe contrôleurs aériens le pourcentage de modification est différent entre le niveau de confiance faible (M = 48.03%, SD = 30.56%), le niveau de confiance moyen (M = 43.66, SD = 29.44) et le niveau de confiance élevé (M = 36.25%, SD = 29.04%). Dans le groupe mécaniciens (Base), le pourcentage de modifications semble également être différent entre le niveau de confiance faible (M = 42.32%, SD = 28.58%), le niveau de confiance moyen (M = 36.78, SD = 28.96) et le niveau de confiance élevé (M = 34.74%, SD = 28.53%). L'effet simple du niveau de confiance, $F(2,156) = 14.62$, $p < .001$*** permet de valider que le niveau de CI influe sur le comportement de modification. L'absence d'effet simple sur le métier, $F(1,78) = .57$, $p = .45$ et l'absence d'effet d'interaction, $F(2,156) = 1.24$, $p = .29$ sont ici interprétés comme montrant une absence d'influence du métier sur le comportement de modifications. Les résultats ne vont pas dans le sens de l'hypothèse 7. Autrement dit, à environnement de travail et niveau d'expérience égal, le comportement de modification des contrôleurs aériens et des mécaniciens est différent selon le niveau de CI présent dans la relation.

Hypothèse 7 : Pourcentage de supervisions contre-productives

Les données obtenues en statistiques descriptives semblent montrer (Cf. Tableau 9 ligne %VDm_sup) que dans le groupe contrôleurs aériens le pourcentage de supervisions contre-productives est différent entre le niveau de confiance faible (M = 47.02%, SD = 30.10%), le niveau de confiance moyen (M = 47.21%, SD = 30.88%) et le niveau de confiance élevé (M = 42.88%, SD = 31.27%). Dans le groupe mécaniciens (Base), le pourcentage de supervisions contre-productives semble également être différente entre le niveau de confiance faible (M = 42.09%, SD = 26.43%), le niveau de confiance moyen (M = 36.61%, SD = 27.70%) et le niveau de confiance élevé (M = 35.26%, SD = 27.67%). L'effet simple du niveau de confiance, $F(2,156) = 4.35$, $p = .01$* permet de valider que le niveau de confiance induit influe sur l'efficacité des supervisions. L'absence d'effet simple sur le métier, $F(1,78) = 1.57$, $p = .21$ et l'absence d'effet d'interaction, $F(2,156) = 1.15$, $p = .31$ sont ici interprétés comme montrant une absence d'influence du métier sur l'efficacité des supervisions. Les résultats ne vont pas dans le sens de l'hypothèse 7. Autrement dit, à environnement de travail et niveau d'expérience égal, l'efficacité des supervisions des contrôleurs aériens et des mécaniciens est différente selon le niveau de CI présent dans la relation.

Pris tous ensemble, les résultats permettent de réfuter l'hypothèse 7. Cette expérimentation montre que deux groupes d'individus issus d'un même milieu professionnel (aéronautique militaire) travaillant depuis des durées équivalentes (même niveau d'expertise) et ayant le même environnement de travail (Base) mais ayant des métiers différents, ont, à minima, des comportements de supervision et de gestion du temps modulés différemment par le niveau de CI présent dans la relation.

b. Test de l'hypothèse 8 : Dans un même métier, le niveau d'expertise des individus et non pas le niveau de CI fait varier les comportements.

Afin de tester cette hypothèse, les données obtenues auprès des 40 élèves PN et auprès des 40 PN expérimentés ont été exploitées. Les variables dépendantes utilisées afin de tester cette hypothèse sont similaires aux variables dépendantes utilisées pour tester les hypothèses 2, 3, 4 et 5. Avant de tester cette hypothèse le bon fonctionnement du matériel d'induction sur ces deux classes de populations a été testé.

Tableau 12 : Moyenne, écart type et résultats de l'ANOVA a mesures répétées pour les groupes PN expérimentés et élèves PN et pour les variables dépendantes *CertitudePartenaire,* %VDsup, %Tempstot, %VDmodif et *%VDm_sup*

Variable dépendante	Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe PN expérimentés			Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe élèves PN			ANOVA simple effet (CI)		ANOVA simple effet (Experience)		ANOVA effet d'interaction (CI*Experience)	
	Faible	Moyen	Elevé	Faible	Moyen	Elevé	F(2, 156)	P-value	F(1, 78)	P-value	F(2, 156)	P-value
CertitudePartenaire	M = 4.93 SD = 2.31	M = 5.93 SD = 1.91	M = 6.92 SD = 1.90	M = 4.21 SD = 1.98	M = 5.48 SD = 1.68	M = 6.88 SD = 1.80	77.66	<.001***	1.16	.28	1.68	.18
%VDsup	M = 95.71 SD = 11.41	M = 94.62 SD = 12.50	M = 90.86 SD = 15.25	M = 89.78 SD = 19.33	M = 84.92 SD = 22.80	M = 70.59 SD = 31.94	22.88	<.001***	9.09	.003**	8.06	<.001***
%TempsTot	M = 83.82 SD = 8.51	M = 84.18 SD = 7.23	M = 83.26 SD = 7.81	M = 78.60 SD = 8.88	M = 77.36 SD = 8.28	M = 73.72 SD = 11.92	12.29	<.001***	14.8	<.001***	6.85	.01*
%VDmodif	M = 57.50 SD = 23.87	M = 53.47 SD = 23.90	M = 51.54 SD = 25.38	M = 56.54 SD = 21.23	M = 50.20 SD = 23.70	M = 40.08 SD = 25.29	17.22	<.001***	1.14	.28	4.17	.01*
%VDm_sup	M = 56.67 SD = 22.15	M = 54.27 SD = 20.64	M = 51.70 SD = 23.87	M = 59.70 SD = 20.97	M = 55.74 SD = 23.76	M = 46.71 SD = 28.49	6.84	.001**	.0002	.98	1.62	.20

Hypothèse 8 : Perception de la performance du coéquipier

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 12 ligne CertitudePartenaire) que dans le groupe PN expérimentés la perception qu'a le participant des performances de son coéquipier est différente entre le niveau de confiance faible (M = 4.93, SD = 2.31), le niveau de confiance moyen (M = 5.93, SD = 1.91) et le niveau de confiance élevé (M = 6.92, SD = 1.90). Dans le groupe élèves PN, la perception qu'a le participant des performances de son coéquipier semble également être différente entre le niveau de confiance faible (M = 4.21, SD = 1.98), le niveau de confiance moyen (M = 5.48, SD = 1.68) et le niveau de confiance élevé (M = 6.88, SD = 1.80). L'effet simple du niveau de confiance, $F(2,156) = 77.66$, $p < .001$*** permet de valider que le niveau de confiance induit influe sur la

perception qu'a le participant de la performance de leur coéquipier. En d'autres termes, le matériel d'induction fonctionne sur ces deux populations et induit différents niveaux de confiances aux participants. L'absence d'effet simple sur l'expérience, $F(1,78) = 1.16$, $p = .28$ et l'absence d'effet d'interaction, $F(2,156) = 1.68$, $p = .18$ sont ici interprétés comme montrant une absence d'influence de l'expertise sur le niveau de confiance que le participant attribue à son coéquipier.

Hypothèse 8 : Pourcentage de supervision

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 12 ligne %VDsup) que dans le groupe PN expérimentés le pourcentage de supervision est relativement proche entre le niveau de confiance faible (M = 95.71%, SD = 11.41%), le niveau de confiance moyen (M = 94.62%, SD = 12.50%) et le niveau de confiance élevé (M = 90.86%, SD = 15.25%). Dans le groupe élèves PN, une différence semble être présente sur le pourcentage de supervisions entre le niveau de confiance faible (M = 89.78%, SD = 19.33%), le niveau de confiance moyen (M = 84.92%, SD = 22.80%) et le niveau de confiance élevé (M = 70.59%, SD = 31.94%). L'interaction significative sur ces données, $F(2,156) = 8.06$, $p < .001$*** et les résultats des tests post-hoc (*Cf.* Tableau 13) permettent de valider ces observations qui ne vont pas dans le sens de l'hypothèse 8. Autrement dit, dans un même métier, le comportement de supervision est différent selon le niveau d'expertise des individus et selon le niveau de CI présent dans la relation. Les élèves PN adaptent leur stratégie de supervision en fonction du niveau de confiance présent dans la relation alors que les PN expérimentés ont une stratégie de supervision similaire quel que soit le niveau de confiance présent dans la relation.

Tableau 13 : Test post-hoc HSD de Tukey pour la variable dépendante %VDsup et pour les groupes PN expérimentés et élèves PN (*Cf.* annexe 3).

	Test post-hoc HSD de Tukey pour la variable dépendante %VDsup		
	Faible	**Moyen**	
PN expérimentés	-	$p = 1$	**Faible**
	$p = .95$	$p = 1$	**Elevé**
Élèves PN	-	$p = .99$	**Faible**
	$p < .001$***	$p < .001$***	**Elevé**

Hypothèse 8 : Pourcentage de temps total utilisé

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 12 ligne %TempsTot) que dans le groupe PN expérimentés le pourcentage de temps total utilisé est relativement proche entre le niveau de confiance faible (M = 83.82%, SD = 8.51%), le niveau de confiance moyen (M = 84.18%, SD = 7.23%) et le niveau de confiance élevé (M = 83.26%, SD = 7.81%). Dans le groupe élèves PN une différence semble être présente entre le niveau de confiance faible (M = 78.60%, SD = 8.88%), le niveau de confiance moyen (M = 77.36%, SD = 8.28%) et le niveau de confiance élevé (M = 73.72%, SD = 11.92%). L'interaction significative, $F(2,156) = 6.85$, $p = .01$* et les résultats des tests post-hoc (*Cf.* Tableau 14) permettent de valider ces observations qui ne vont

pas dans le sens de l'hypothèse 8. Autrement dit, dans un même métier, le comportement de gestion du temps est différent selon le niveau d'expertise des individus et selon le niveau de CI présent dans la relation. Les élèves PN adaptent leur stratégie de gestion du temps en fonction du niveau de confiance présent dans la relation alors que les PN expérimentés ont une stratégie de gestion du temps similaire quel que soit le niveau de confiance présent dans la relation.

Tableau 14 : Test post-hoc HSD de Tukey pour la variable dépendante %TempsTot et pour les groupes PN expérimentés et élèves PN (*Cf.* annexe 3).

	Test post-hoc HSD de Tukey pour la variable dépendante %TempsTot		
	Faible	**Moyen**	
PN expérimentés	-	$p = 1$	**Faible**
	$p = 1$	$p = 1$	**Elevé**
Élèves PN	-	$p = 1$	**Faible**
	$p < .001$***	$p < .001$***	**Elevé**

Hypothèse 8 : Pourcentage de modifications

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 12 ligne %VDmodif) que dans le groupe PN expérimentés le pourcentage de modifications est relativement proche entre le niveau de confiance faible (M = 57.50%, SD = 23.87%), le niveau de confiance moyen (M = 53.47%, SD = 23.90%) et le niveau de confiance élevé (M = 51.54%, SD = 25.38%). Dans le groupe élèves PN une différence semble être présente sur le pourcentage de modifications entre le niveau de confiance faible (M = 56.54%, SD = 21.23%), le niveau de confiance moyen (M = 50.20%, SD = 23.70%) et le niveau de confiance élevé (M = 40.08%, SD = 25.29%). L'interaction significative sur ces données, $F(2,156) = 4.17$, $p = .01$* et les résultats des tests post-hoc (*Cf.* Tableau 15) permettent de valider ces observations qui ne vont pas dans le sens de l'hypothèse 8. Autrement dit, dans un même métier, le comportement de modification est différent selon le niveau d'expertise des individus et selon le niveau de CI présent dans la relation. Les élèves PN adaptent leur stratégie de modification en fonction du niveau de confiance présent dans la relation alors que les PN expérimentés ont une stratégie de modification similaire quel que soit le niveau de confiance présent dans la relation.

Tableau 15 : Test post-hoc HSD de Tukey pour la variable dépendante %VDmodif et pour les groupes PN expérimentés et élèves PN (*Cf.* annexe 3).

	Test post-hoc HSD de Tukey pour la variable dépendante %VDmodif		
	Faible	Moyen	
PN expérimentés	-	$p = 1$	Faible
	$p = .41$	$p = 1$	Elevé
Élèves PN	-	$p = .28$	Faible
	$p < .001$***	$p = .002$**	Elevé

Hypothèse 8 : Pourcentage de supervisions contre-productives

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 12 ligne %VDm_sup) que dans le groupe PN expérimentés le pourcentage de supervisions contre-productives est différent entre le niveau de confiance faible (M = 56.67%, SD = 22.15%), le niveau de confiance moyen (M = 54.27%, SD = 20.6%4) et le niveau de confiance élevé (M = 51.70%, SD = 23.87%). Dans le groupe élèves PN, pourcentage de supervisions contre-productives semble également être différent entre le niveau de confiance faible (M = 59.70%, SD = 20.97%), le niveau de confiance moyen (M = 55.74%, SD = 23.76%) et le niveau de confiance élevé (M = 46.71%, SD = 28.49%). L'effet simple du niveau de confiance, $F(2,156) = 6.84$, $p = .001$** permet de valider que le niveau de confiance induit influe sur l'efficacité des supervisions. L'absence d'effet simple sur l'expérience, $F(1,78) = .0002$, $p = .98$ et l'absence d'effet d'interaction, $F(2,156) = 1.62$, $p = .20$ sont ici interprétés comme montrant une absence d'influence de l'expérience sur l'efficacité des supervisions. Les résultats ne vont pas dans le sens de l'hypothèse 8. Autrement dit, l'efficacité des supervisions des PN expérimentés et des élèves PN est différente selon le niveau de CI présent dans la relation.

Pris tous ensemble les résultats permettent de réfuter l'hypothèse 8. Cette expérimentation montre que deux groupes d'individus issus d'un même milieu professionnel (aéronautique militaire) mais ayant des niveaux d'expertises différents, ont, à minima, des comportements de supervision, de gestion du temps et de modifications modulés différemment par le niveau de CI présent dans la relation.

c. *Test de l'hypothèse 9 : Dans un même métier, l'exposition au risque des individus et non pas le niveau de CI fait varier les comportements.*

Afin de tester cette hypothèse, les données obtenues auprès des 40 mécaniciens ayant déjà fait des OPEX et les données obtenues auprès des 40 mécaniciens travaillant sur base ont été exploitées. Les variables dépendantes utilisées afin de tester cette hypothèse sont similaires aux variables dépendantes utilisées pour tester les hypothèses 2, 3, 4 et 5. Avant de tester cette hypothèse le bon fonctionnement du matériel d'induction sur ces deux classes de populations a été testé.

Tableau 16 : Moyenne, écart type et résultats de l'ANOVA a mesures répétées pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX et pour les variables dépendantes *CertitudePartenaire, %VDsup, %Tempstot, %VDmodif et %VDm_sup*

Variable dépendante	Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe mécaniciens (OPEX)			Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe mécaniciens (Base)			ANOVA simple effet (CI)		ANOVA simple effet (Environnement)		ANOVA effet d'interaction (CI*Environnement)	
	Faible	Moyen	Elevé	Faible	Moyen	Elevé	F(2, 156)	P-value	F(1, 78)	P-value	F(2, 156)	P-value
CertitudePartenaire	M = 5.46 SD = 2.31	M = 5.81 SD = 2.20	M = 6.46 SD = 2.12	M = 5.14 SD = 1.75	M = 5.71 SD = 1.73	M = 6.59 SD = 1.54	34.93	<.001***	.05	.80	1.10	.33
%VDsup	M = 81.67 SD = 26.30	M = 81.78 SD = 26.62	M = 78.92 SD = 31.61	M = 88.21 SD = 22.38	M = 86.42 SD = 22.57	M = 84.55 SD = 22.44	2.85	.06	1.04	.31	.23	.79
%TempsTot	M = 79.28 SD = 8.52	M = 78.48 SD = 8.46	M = 78.46 SD = 9.11	M = 80.46 SD = 7.73	M = 80.82 SD = 7.91	M = 79.01 SD = 7.72	2.79	.06	.59	.43	1.56	.21
%VDmodif	M = 38.21 SD = 28.91	M = 41.60 SD = 28.74	M = 37.85 SD = 30.22	M = 42.32 SD = 28.58	M = 36.78 SD = 28.96	M = 34.74 SD = 28.53	3.17	.04*	.04	.83	4.23	.01*
%VDm_sup	M = 39.17 SD = 29.26	M = 44.03 SD = 27.03	M = 40.10 SD = 30.53	M = 42.09 SD = 26.43	M = 36.61 SD = 27.70	M = 35.26 SD = 27.67	1.39	.25	.28	.59	3.83	.02*

Hypothèse 9 : Perception de la performance du coéquipier

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 16 ligne CertitudePartenaire) que dans le groupe mécaniciens ayant déjà fait des OPEX la perception qu'a le participant de la performance de son coéquipier est différente entre le niveau de confiance faible (M = 5.46, SD = 2.31), le niveau de confiance moyen (M = 5.81, SD = 2.20) et le niveau de confiance élevé (M = 6.46, SD = 2.12). Dans le groupe mécaniciens travaillant sur base, la perception qu'à le participant des performances de son coéquipier semble également être différente entre le niveau de confiance faible (M = 5.14, SD = 1.75), le niveau de confiance moyen (M = 5.71, SD = 1.73) et le niveau de confiance élevé (M = 6.59, SD = 1.54). L'effet simple du niveau de confiance, $F(2,156) = 34.93$, $p < .001$*** permet de valider que le niveau de confiance induit influe sur la perception qu'a le participant de la performance de leur coéquipier. En d'autre terme le matériel d'induction fonctionne sur ces deux populations et induit différents niveaux de confiances aux participants. L'absence d'effet simple sur l'environnement de travail, $F(1,78) = .05$, $p = .80$ et l'absence d'effet d'interaction, $F(2,156) = 1.10$, p = .33 sont ici interprétés comme montrant une absence d'influence de l'exposition au risque sur le niveau de confiance que le participant attribue à son coéquipier.

Hypothèse 9 : Pourcentage de supervision

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 16 ligne %VDsup) que dans le groupe mécaniciens ayant déjà fait des OPEX le pourcentage de supervision est relativement proche entre le niveau de confiance faible (M = 81.67%, SD = 26.30%), le niveau de confiance moyen (M = 81.78%, SD = 26.62%) et le niveau de confiance élevé (M = 78.92%, SD = 31.61%). Dans le groupe mécaniciens travaillant sur base le pourcentage de supervision semble également être relativement proche entre le niveau de confiance faible (M = 88.21%, SD = 22.38%), le niveau de confiance moyen (M = 86.42%, SD = 22.57%) et le niveau de confiance élevé (M = 84.55%, SD = 22.44%). L'absence d'effet simple du niveau de confiance, $F(2,156) = 2.85$, p = .06 est ici interprétée comme une absence d'influence du niveau de CI sur le comportement de

supervision. L'absence d'effet simple sur l'environnement de travail, $F(1,78) = 1.04$, $p = .31$ est ici interprétée comme une absence d'influence de l'exposition au risque sur le comportement de supervision. Ces observations ne vont pas dans le sens de l'hypothèse 9. Autrement dit, ni l'exposition au risque des individus ni le niveau de CI présent dans la relation n'influence le comportement de supervision chez ces groupes d'individus.

Hypothèse 9 : Pourcentage de temps total utilisé

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 16 ligne %TempsTot) que dans le groupe mécaniciens ayant déjà fait des OPEX le pourcentage de temps total utilisé est relativement proche entre le niveau de confiance faible (M = 79.28%, SD = 8.52%), le niveau de confiance moyen (M = 78.48%, SD = 8.46%) et le niveau de confiance élevé (M = 78.46%, SD = 9.11%). Dans le groupe mécaniciens travaillant sur base, le pourcentage de temps total utilisé est également relativement proche entre le niveau de confiance faible (M = 80.46%, SD = 7.33%), le niveau de confiance moyen (M = 80.82%, SD = 7.91%) et le niveau de confiance élevé (M = 79.01%, SD = 7.72%). L'absence d'effet simple du niveau de confiance, $F(2,156) = 2.79$, $p = .06$ est ici interprétée comme une absence d'influence du niveau de CI sur le comportement de gestion du temps. L'absence d'effet simple sur l'environnement de travail, $F(1,78) = .59$, $p = .43$ est ici interprétée comme une absence d'influence de l'exposition au risque (environnement de travail sur le comportement de gestion du temps. Ces observations ne vont pas dans le sens de l'hypothèse 9. Autrement dit, ni l'exposition au risque des individus ni le niveau de CI présent dans la relation n'influence le comportement de gestion du temps chez ces groupes d'individus.

Hypothèse 9 : Pourcentage de modifications

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 16 ligne %VDmodif) que dans le groupe mécaniciens ayant déjà fait des OPEX le pourcentage de modification est relativement proche entre le niveau de confiance faible (M = 38.21%, SD = 28.91%), le niveau de confiance moyen (M = 41.60%, SD = 28.74%) et le niveau de confiance élevé (M = 37.85%, SD = 30.22%). Dans le groupe mécaniciens travaillant sur base, une différence semble être présente sur le pourcentage de modification entre le niveau de confiance faible (M = 42.32%, SD = 28.58%), le niveau de confiance moyen (M = 36.78%, SD = 28.96%) et le niveau de confiance élevé (M = 34.74%, SD = 28.53%). L'interaction significative sur ces données, $F(2,156) = 4.23$, $p = .01$* et les résultats des tests post-hoc (*Cf.* Tableau 17) permettent de valider ces observations qui ne vont pas dans la sens de l'hypothèse 9. Autrement dit, dans un même métier, le comportement de modification est différent selon l'exposition au risque et selon le niveau de CI présent dans la relation. Les mécaniciens travaillant sur base adaptent leur comportement de modification en fonction du niveau de confiance présent dans la relation alors que les mécaniciens ayant déjà fait des OPEX ont des comportements de modification similaire quel que soit le niveau de confiance présent dans la relation.

Tableau 17 : Test post-hoc HSD de Tukey pour la variable dépendante %VDmodif et pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX (*Cf.* annexe 3).

	Test post-hoc HDS de Tukey pour la variable dépendante %VDmodif		
	Faible	**Moyen**	
Mécanicien (OPEX)	-	$p = 1$	**Faible**
	$p = 1$	$p = 1$	**Elevé**
Mécanicien (Base)	-	$p = .22$	**Faible**
	$p = .01$*	$p = 1$	**Elevé**

Hypothèse 9 : Pourcentage de supervisions contre-productives

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 16 ligne %VDmodif) que dans le groupe mécaniciens ayant déjà fait des OPEX le pourcentage de supervisions contre-productives est relativement proche entre le niveau de confiance faible (M = 39.17%, SD = 29.26%), le niveau de confiance moyen (M = 44.03%, SD = 27.03%) et le niveau de confiance élevé (M = 40.10%, SD = 30.53%). Dans le groupe mécaniciens travaillant sur base, une différence semble être présente sur le pourcentage de supervisions contre-productives entre le niveau de confiance faible (M = 42.09%, SD = 26.43%), le niveau de confiance moyen (M = 36.61%, SD = 27.70%) et le niveau de confiance élevé (M = 35.26%, SD = 27.67%). L'interaction significative sur ces données, $F(2,156) = 3.83$, $p = .02$* et les résultats des tests post-hoc (*Cf.*Tableau 18) permettent de valider ces observations qui ne vont pas dans la sens de l'hypothèse 9. Autrement dit, dans un même métier, l'efficacité des supervisions est différente selon l'exposition au risque et selon le niveau de CI présent dans la relation. Les mécaniciens travaillant sur base ont des supervisions plus ou moins efficaces en fonction du niveau de confiance présent dans la relation alors que les mécaniciens ayant déjà fait des OPEX ont des supervisions d'une efficacité similaire quel que soit le niveau de confiance présent dans la relation

Tableau 18 : Test post-hoc HSD de Tukey pour la variable dépendante %VDm_sup et pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX (*Cf.* annexe 3).

Test post-hoc HSD de Tukey pour la variable dépendante %VDm_sup			
	Faible	**Moyen**	
Mécaniciens (OPEX)	-	$p = .07$	**Faible**
	$p = .73$	$p = .15$	**Elevé**
Mécaniciens (Base)	-	$p = .04$*	**Faible**
	$p = .01$*	$p = .62$	**Elevé**

Pris tous ensemble les résultats permettent de réfuter l'hypothèse 9. Cette expérimentation montre que deux groupes d'individus issus d'un même milieu professionnel (aéronautique militaire), ayant des niveaux d'expertises similaires mais ayant eu des expositions au risque différentes, ont, à minima, un comportement de modifications et une efficacité de supervision modulés différemment par le niveau de CI présent dans la relation.

d. Test de l'hypothèse 10 : Pour une même exposition au risque, le métier des individus et non pas le niveau de confiance fait varier les comportements.

Afin de tester cette hypothèse, les données obtenues auprès des 40 mécaniciens ayant déjà fait des OPEX et les données obtenues auprès des 40 PN expérimentés ont été exploitées. Les variables dépendantes utilisées afin de tester cette hypothèse sont similaires aux variables dépendantes utilisées pour tester les hypothèses 2, 3, 4 et 5. Avant de tester cette hypothèse le bon fonctionnement du matériel d'induction sur ces deux classes de populations a été testé.

Tableau 19 : Moyenne, écart type et résultats de l'ANOVA a mesures répétées pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX et pour les variables dépendantes *CertitudePartenaire,* %VDsup, %Tempstot, %VDmodif *et %VDm_sup*

Variable dépendante	Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe mécaniciens (OPEX)			Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe PN expérimentés			ANOVA simple effet (CI)		ANOVA simple effet (Environnement)		ANOVA effet d'interaction (CI*Environnement)	
	Faible	**Moyen**	**Elevé**	**Faible**	**Moyen**	**Elevé**	**F(2, 156)**	**P-value**	**F(1, 78)**	**P-value**	**F(2, 156)**	**P-value**
CertitudePartenaire	M = 5.46 SD = 2.31	M = 5.81 SD = 2.20	M = 6.46 SD = 2.12	M = 4.93 SD = 2.31	M = 5.93 SD = 1.91	M = 6.92 SD = 1.90	43.26	<.001***	.001	.97	4.80	.009**
%VDsup	M = 81.67 SD = 26.30	M = 81.78 SD = 26.62	M = 78.92 SD = 31.61	M = 95.71 SD = 11.41	M = 94.62 SD = 12.50	M = 90.86 SD = 15.25	4.53	.01*	7.67	.007**	.25	.74
%TempsTot	M = 79.28 SD = 8.52	M = 78.48 SD = 8.46	M = 78.46 SD = 9.11	M = 83.82 SD = 8.51	M = 84.18 SD = 7.23	M = 83.26 SD = 7.81	0.97	.38	8.12	.005**	0.70	.49
%VDmodif	M = 38.21 SD = 28.91	M = 41.60 SD = 28.74	M = 37.85 SD = 30.22	M = 57.50 SD = 23.87	M = 53.47 SD = 23.90	M = 51.54 SD = 25.38	2.05	.13	6.88	.01*	2.54	.08
%VDm_sup	M = 39.17 SD = 29.26	M = 44.03 SD = 27.03	M = 40.10 SD = 30.53	M = 56.67 SD = 22.15	M = 54.27 SD = 20.64	M = 51.70 SD = 23.87	1.16	.31	6.22	.01*	1.49	.22

Hypothèse 10 : Perception de la performance du coéquipier

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 19 ligne CertitudePartenaire) que dans le groupe mécaniciens ayant déjà fait des OPEX la perception qu'a le participant de la performance de son coéquipier est différente entre le niveau de confiance faible (M = 5.46, SD = 2.31), le niveau de confiance moyen (M = 5.81, SD = 2.20) et le niveau de confiance élevé (M = 6.46, SD = 2.12). Dans le groupe PN expérimentés la perception qu'a le participant de la performance de son coéquipier semble également être différente entre le niveau de confiance faible (M = 4.93, SD = 2.31), le niveau de confiance moyen (M = 5.93, SD = 1.91) et le niveau de confiance élevé (M = 6.92, SD = 1.90). L'effet simple du niveau de confiance, $F(2,156) = 43.26$, $p < .001$*** permet de valider que le niveau de confiance induit influe sur la perception qu'a le participant de la performance de leur coéquipier. En d'autres termes le matériel d'induction fonctionne sur ces deux populations et semble donc induire différents niveaux de confiances aux participants. L'effet d'interaction, $F(2,156) = 4.80$, $p = .009$** montre que le métier des individus ayant une sensibilité au risque similaire a une influence sur le niveau de confiance que le participant attribue à son coéquipier. Cependant, les résultats des tests post-hoc (*Cf.* Tableau 20), indiquent qu'il y a une différence significative, pour les deux groupes sociaux, entre le niveau de CI faible et le niveau de CI élevé. Les résultats montrent donc que le comportement est similaire entre les deux groupes avec une perception de la performance significativement plus forte quand la CI est élevée que quand la CI est faible. Ici, l'effet d'interaction montre que c'est l'amplitude du phénomène qui est significativement différent entre les deux groupes (le gain en performance perçue est plus fort pour les PN que pour les mécaniciens). En d'autres termes, statistiquement, cet effet d'interaction n'indique pas une différence de type de comportement mais une différence dans l'amplitude de l'influence.

Tableau 20 : Test post-hoc HSD de Tukey pour la variable dépendante CertitudePartenaire et pour les groupes mécaniciens ayant déjà fait des OPEX et PN expérimentés (*Cf.* annexe 3).

	Test post-hoc HSD de Tukey pour la variable dépendante CertitudePartenaire		
	Faible	**Moyen**	
PN expérimentés	-	$p < .001$***	**Faible**
	$p < .001$***	$p < .001$***	**Elevé**
Mécaniciens (OPEX)	-	$p = 1$	**Faible**
	$p < .001$***	$p = .06$	**Elevé**

Hypothèse 10 : Pourcentage de supervision

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 19 ligne %VDsup) que dans le groupe mécaniciens ayant déjà fait des OPEX le pourcentage de supervision est relativement proche entre le niveau de confiance faible (M = 81.67%, SD = 26.30%), le niveau de confiance moyen (M = 81.78%, SD = 26.62%) et le niveau de confiance élevé (M = 78.92%, SD = 31.61%). Dans le groupe PN expérimentés le pourcentage de supervision semble également être relativement proche entre le niveau de confiance faible (M = 95.71%, SD = 11.41%), le niveau de

confiance moyen (M = 94.62%, SD = 12.50%) et le niveau de confiance élevé (M = 90.86%, SD = 15.25%). L'effet simple du niveau de confiance, $F(2,156) = 4.53$, $p = .01$* ne va pas dans le sens de l'hypothèse 10, alors que l'effet simple sur l'environnement de travail, $F(1,78) = 7.67$, $p = .007$** va dans le sens de l'hypothèse 10. Autrement dit, pour une même exposition au risque le métier et le niveau de CI font varier le comportement de supervision des individus.

Hypothèse 10 : Pourcentage de temps utilisé sur le temps disponible

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 19 ligne %TempsTot) que dans le groupe mécaniciens ayant déjà fait des OPEX le pourcentage de temps utilisé sur le temps disponible est relativement proche entre le niveau de confiance faible (M = 79.28%, SD = 8.52%), le niveau de confiance moyen (M = 78.48%, SD = 8.46%) et le niveau de confiance élevé (M = 78.46%, SD = 9.11%). Dans le groupe PN expérimentés le pourcentage de temps utilisé sur le temps disponible semble également être relativement proche entre le niveau de confiance faible (M = 83.82%, SD = 8.51%), le niveau de confiance moyen (M = 84.18%, SD = 7.23%) et le niveau de confiance élevé (M = 83.26%, SD = 7.81%). L'absence d'effet simple du niveau de confiance, $F(2,156) = .97$, $p = .38$ et l'effet simple significatif du facteur métier, $F(1,78) = 7.67$, $p = .007$** vont dans le sens de l'hypothèse 10. En d'autres termes, pour une même exposition au risque, le métier des individus fait varier leur comportement de gestion du temps mais le niveau de CI ne fait pas varier leur comportement.

Hypothèse 10 : Pourcentage de modification

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 19 ligne %VDmodif) que dans le groupe mécaniciens ayant déjà fait des OPEX le pourcentage de modification est relativement proche entre le niveau de confiance faible (M = 38.21%, SD = 28.91%), le niveau de confiance moyen (M = 41.60%, SD = 28.74%) et le niveau de confiance élevé (M = 37.85%, SD = 30.22%). Dans le groupe PN expérimentés le pourcentage de modification semble être relativement proche entre le niveau de confiance faible (M = 57.50%, SD = 23.87%), le niveau de confiance moyen (M = 53.47%, SD = 23.90%) et le niveau de confiance élevé (M = 51.54%, SD = 25.38%). L'absence d'effet simple du niveau de confiance, $F(2,156) = 2.05$, $p = .13$ et l'effet simple significatif du facteur métier, $F(1,78) = 6.88$, $p = .01$* vont dans le sens de l'hypothèse 10. En d'autres termes, pour une même exposition au risque, le métier des individus fait varier leur comportement de modification mais le niveau de CI ne fait pas varier leur comportement.

Hypothèse 10 : Pourcentage de supervisions contre-productives

Les données obtenues en statistiques descriptives semblent montrer (*Cf.* Tableau 19 ligne %VDmodif) que dans le groupe mécaniciens ayant déjà fait des OPEX le pourcentage de supervisions contre productives est relativement proche entre le niveau de confiance faible (M = 39.17%, SD = 29.26%), le niveau de confiance moyen (M = 41.60%, SD = 28.74%) et le niveau de confiance élevé (M = 44.03%, SD = 27.03%). Dans le groupe PN expérimentés le pourcentage de supervisions contre productives semble être différent entre le niveau de confiance faible (M = 40.10%, SD = 30.53%), le niveau de confiance moyen (M = 54.24%, SD = 20.64%) et le niveau de confiance élevé (M = 51.70%, SD = 23.87%). L'absence d'effet simple du niveau de confiance, $F(2,156) =2.05$, $p = .13$ et l'effet simple significatif du facteur métier, $F(1,78) = 6.22$, $p = .01$* vont dans le sens de l'hypothèse 10. En d'autres termes, pour une même exposition au risque, le métier

des individus fait varier l'efficacité des supervisions mais le niveau de CI ne fait pas varier l'efficacité des supervisions.
Pris tous ensemble les résultats permettent de réfuter l'hypothèse 10. Des individus ayant un même niveau d'expertise, des expositions similaires au risque mais ayant des métiers différents ont, a minima, un comportement de supervision modulé par le niveau de CI présent dans la relation.

6. Discussion

Les différentes hypothèses ont conduit à une expérimentation ayant deux objectifs distincts. Le premier objectif était de voir l'influence de la présence ou l'absence de pression temporelle sur la prise en compte, par un individu, du niveau de CI présent entre lui et d'autres membres d'une équipe. Le deuxième objectif était de trancher entre deux approches (qui ont été notées approche directe et indirecte) présentes dans la littérature. L'approche indirecte (celle de la CI) considère que le niveau de CI présent entre les membres d'une équipe est un facteur influençant le comportement des membres de cette équipe. L'approche directe (celle de l'apprentissage social) indique quant à elle que les caractéristiques psychosociales de l'individu sont le facteur explicatif principal du comportement de cet individu.

Concernant le premier objectif, les résultats obtenus invalident l'hypothèse 6. Les résultats montrent que dans ce cadre applicatif, quelle que soit la pression temporelle, le niveau de CI présent dans la relation module les comportements du confiant. Ces résultats semblent aller à l'encontre de la littérature existante qui prédisait que la pression temporelle était un facteur clef du comportement des individus. Cette expérimentation montre que, pour des équipes éphémères et sur ce type de tâche collaborative, le confiant adapte ses comportements de supervision, de gestion du temps, de modifications mais également l'efficacité de ses supervisions, en fonction du niveau de CI présent dans la relation plutôt qu'en fonction de la pression temporelle. Bien évidemment ce résultat n'est pas forcément généralisable à toutes les situations et tous les types d'opérateurs mais il démontre l'importance que peut prendre le facteur confiance dans certaines situations. Il est à noter que seuls 2 niveaux de pression temporelle ont été utilisés et il serait bon dans des études à venir d'élargir le spectre de cette variable afin affiner la manière dont elle peut se combiner à la confiance.

Concernant le deuxième objectif, la littérature sur la CI indique que le niveau de CI présent entre les membres d'une équipe pourrait modifier le comportement des membres de cette équipe. Si ce mécanisme est effectif, il pourrait être intéressant de choisir le décideur final de la RCPair sur la base de ses « liens d'affinité » potentiel avec les autres membres des C2air. Dans ce cas-là, le décideur final de la RCPair serait celui qui aurait avec les autres membres du C2air, le niveau de CI optimal (le niveau de CI entrainant un comportement optimal du décideur de la RCPair). En ce sens, l'ajout de fonctionnalités permettant d'augmenter le niveau de confiance entre les individus, pourrait être envisagé afin d'optimiser le comportement des membres du C2air.

De son côté, la littérature sur l'apprentissage social montre que les caractéristiques psychosociales influencent directement le comportement des individus, indépendamment du niveau de CI. Dans ce cas, le choix du décideur final de la RCPair pourrait être effectué sur la base des comportements relatifs à son groupe social. En trouvant la caractéristique sociale entrainant le comportement le plus adapté à l'utilisation de la RCPair, le décideur final le plus adapté à l'utilisation de la RCPair pourrait

être identifié. Cependant, dans ce cas, le niveau de CI présent entre les membres du C2air n'influencerait pas le comportement des membres du C2air.

Dans le cadre de coopération entre opérateurs dans des conditions similaires à celles qui seront rencontrées dans la RCPair, cette première expérimentation visait donc à analyser « l'apport » de l'approche indirecte (lien bleu sur la figure 38) et de l'approche directe (lien orange sur la figure 38) dans l'amélioration du système sociotechnique que représente la RCPair intégrée en C2air. Les données obtenues au cours de cette expérimentation montrent que ces deux approches doivent être prises en compte car les caractéristiques psychosociales de l'opérateur impactent les modifications comportementales engendrées par différents niveaux de CI (triple flèche verte sur la figure 38).

Les résultats significatifs du facteur CI sur la VD CertitudePartenaire montrent que, quel que soit leur groupe social, les participants ont bien perçus les différents niveaux de confiance induits. L'induction de différents niveaux de CI a donc fonctionnée chez tous les participants. Cependant, les résultats non significatifs des différents facteurs associés au groupe social sur cette VD CertitudePartenaire ne permettent pas de montrer que le groupe social des individus ait une influence sur la manière dont ces individus perçoivent les différents niveaux de CI. Pris tous ensemble, les résultats obtenus avec la VD CertitudePartenaire montrent que quel que soit le groupe social du participant, différents niveaux de CI ont bien été induits, mais, que la « force » du niveau d'induction n'est pas dépendante de ce groupe social. En d'autres termes, un niveau de CI faible ou élevé pour un pilote expert n'est pas différent d'un niveau de CI faible ou élevé pour un élève pilote. Ces observations pourraient aller dans le sens de l'approche indirecte en corroborant le lien entre les caractéristiques propres au confiant et la mise en place du niveau de CI (première flèche bleue sur la figure 38).

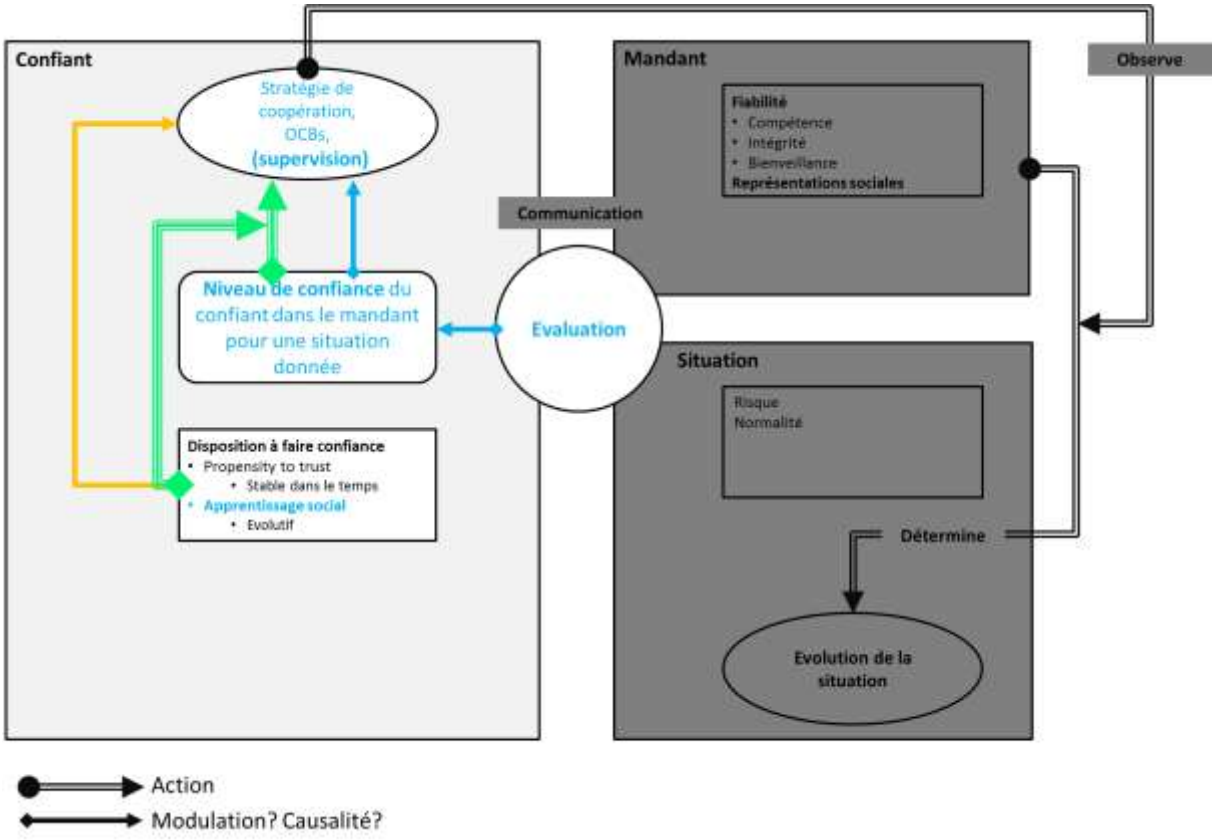


Figure 38 : Résultats de l'expérimentation portant sur les caractéristiques psychosociales du confiant.

En bleu est représentée l'approche indirecte, en orange l'approche directe et en vert les résultats de l'expérimentation

Cependant, les résultats obtenus sur les VD comportementales ne vont pas dans le sens de l'approche indirecte qui sous-tend un lien direct entre le niveau de CI présent dans la relation et le comportement du confiant. Les résultats obtenus sur les différentes VD comportementales montrent que les caractéristiques propres au confiant interviennent en modulant le comportement du confiant dans les différentes relations de CI (différents niveaux de CI) (triple flèche verte sur la figure 38).

Dès lors, les résultats d'interactions significatives obtenus avec le facteur métier (*Cf.* Tableau 21) montrent que le métier modifie le comportement de supervision et de gestion du temps. Les contrôleurs aériens ont eu un comportement de supervision et de gestion du temps dépendants du niveau de CI alors que le niveau de CI ne modifie pas ces comportements chez les mécaniciens n'ayant jamais fait d'OPEX.

Les résultats d'interactions significatives obtenus avec le facteur environnement montrent quand à eux que le fait d'avoir travaillé dans des environnements à fort risque vital perçu (e.g. les opérations extérieures) modifie l'acceptation, par le confiant, des informations transmises par le mandant (pourcentage de modification dans cette expérimentation) mais également l'efficacité des supervisions. Les mécaniciens n'ayant jamais fait d'OPEX ont eu un comportement de modification et une efficacité de supervision dépendants du niveau de CI alors que le niveau de CI n'a pas modifié ces comportements chez les mécaniciens ayant déjà fait des OPEX.

L'absence d'interaction significative sur les résultats obtenus en croisant les facteurs environnement et métier (*Cf.* Tableau 21) montrent que le fait d'avoir fait des OPEX « stabilise » les modifications comportementales engendrées par l'induction de différents niveaux de CI et fait apparaitre les différences comportementales liées au métier. En d'autres termes, bien que l'absence de résultat significatif ne permette pas de conclure à l'absence d'effet, le facteur OPEX semble minimiser l'influence du niveau de CI et maximiser l'apport des caractéristiques psychosociales pour les différents comportements.

Enfin, les résultats d'interactions significatives obtenus avec le facteur expérience (*Cf.* Tableau 21) montrent que l'expérience modifie les comportements de supervision, de gestion du temps et de détection d'erreur. Les élèves PN ont eu un comportement de supervision, de gestion du temps et de détection d'erreur dépendants du niveau de CI alors que le niveau de CI n'a pas modifié ces comportements chez les PN expérimentés. Cependant, il est fort possible que ces résultats obtenus sur le facteur « expérience » proviennent d'un croisement de facteurs. En effets, comme indiqué dans la matrice de répartition, les élèves PN et les PN expérimentés n'ont pas une mais deux différences sociales : l'expérience et l'environnement de travail. Les résultats obtenus sur le comportement de détection d'erreurs peuvent donc être expliquées par la différence de risque présent dans l'environnement de travail. Pour le vérifier, il serait nécessaire de trouver un groupe intermédiaire (par exemple des élèves ayant fini leur formation mais n'étant pas encore partis en escadron).

Tableau 21 : Vulgarisation des résultats obtenus.
Les cases vertes (avec un « V » à l'intérieur) indiquent un effet d'interaction significatif (avec post hoc significatif) entre la variable indépendante manipulée (Expérience, Métier, OPEX) et le comportement modifié par l'induction de CI.

Variation du comportement en fonction du niveau de CI induit					
	Induction du niveau de CI	Comportement de supervision	Comportement de gestion du temps	Comportement de modifications	Efficacité des supervisions
Expérience	X	V	V	V	X
Métier	X	V	V	X	X
OPEX	X	X	X	V	V
OPEX et Métier	X	X	X	X	X

Les approches directes et indirectes semblent donc être complémentaires. Le niveau de CI présent entre l'opérateur de la RCPair et les membres des C2air sera donc essentiel mais le comportement induit par ce niveau de CI sera fonction du groupe social d'appartenance du décideur RCPair. Selon ce groupe social, le décideur devrait avoir tendance soit à modifier plus ou moins son comportement en fonction du niveau de CI présent dans la relation soit à avoir un comportement similaire quel que soit le niveau de CI présent dans la relation.

7. Apports de l'expérimentation au choix du décideur final de la RCPair

Cette expérimentation visait à tester comment les caractéristiques sociales d'un individu (en bleu sur la figure 39) et le niveau de CI présent dans l'équipe pouvaient modifier le comportement de cet individu envers les autres membres de l'équipe (en violet sur la figure 39). Les résultats permettent d'attribuer des comportements aux différents opérateurs potentiels de la RCPair qui ont été identifiés dans l'analyse du besoin (en bleu à gauche sur la figure 39) :

- Les contrôleurs aériens semblent avoir des comportements dépendants du niveau de CI présent dans l'équipe. Pour cette catégorie sociale une diminution du niveau de CI entraine une augmentation du nombre de supervision, une augmentation du temps mis pour réaliser les tâches et une augmentation du nombre de modifications effectuées sur les informations transmises par leur coéquipier. Les contrôleurs aériens ne partant jamais en OPEX le

facteur « environnement » (tel qu'il a été utilisé ici) ne pourrait pas modifier leur comportement ;

- Pour les mécaniciens, il semble y avoir deux groupes distincts
  - Pour les mécaniciens travaillant sur base, une diminution du niveau de CI ne module pas le nombre de supervisions ni le temps mis pour effectuer les tâches mais entraine une augmentation du nombre de modifications effectuées sur les informations transmises par leur coéquipier ;
  - Les mécaniciens ayant déjà fait des OPEX n'ont pas de comportement modulés par le niveau de CI ;
- Pour les PN expérimentés ayant déjà fait des OPEX, une diminution du niveau de CI entraine une augmentation du nombre de supervisions mais ne module pas le temps mis pour effectuer les tâches ni le nombre de modification effectué sur les informations transmises par leur coéquipier ;

Nota bene : Les experts en cybersécurité n'ont pas été testés ici car il n'a pas été possible de trouver 40 participants représentatifs de ce groupe social.

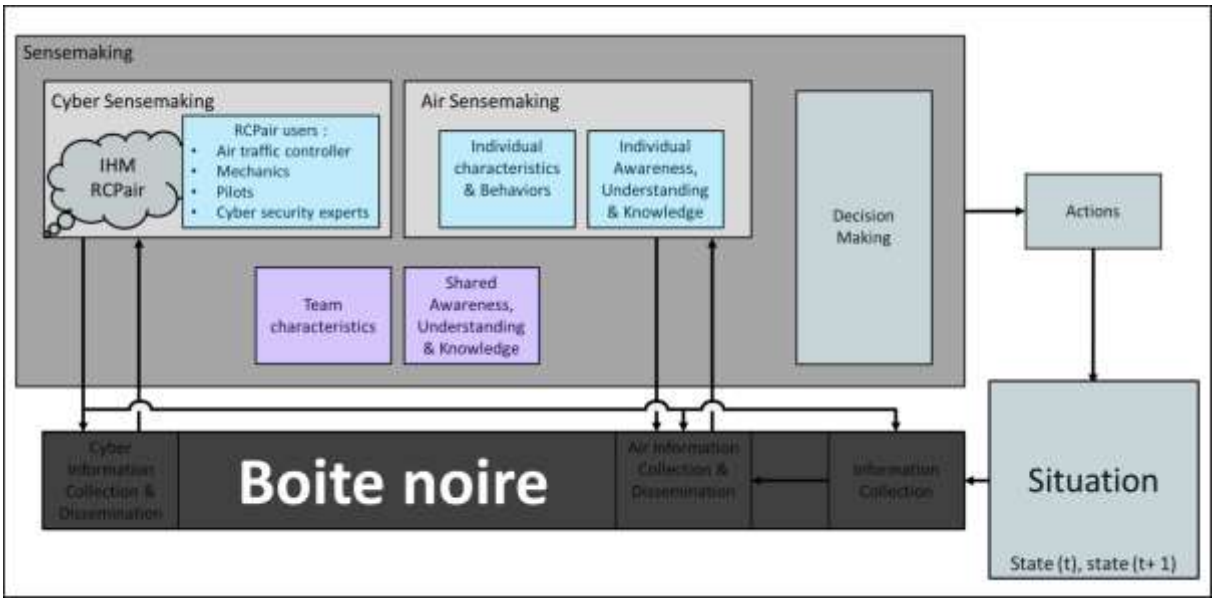


Figure 39 : Représentation conceptuelle du C2 utilisée pour la thèse. En couleur sont présentées les parties du modèle étudiées au cours de cette expérimentation.

Les opérateurs RCPairs devront collaborer avec les autres opérateurs présents dans les C2air. Comme le montre la figure 39, les autres membres des C2air sont des personnes devant « donner le sens air » à une crise et sont, par conséquent, des contrôleurs aériens. Les opérateurs RCPair devront donc collaborer avec des personnes pour qui le niveau de confiance présent dans la relation influence le comportement de supervision et par voie de conséquence les comportements de gestion du temps et de modification. Afin de prévenir les problématiques provenant d'un faible niveau de CI entre les membres du C2air (contrôleurs aériens) et les opérateurs RCPair il est nécessaire de prendre en compte, dès la conception, le besoin du contrôleur et de former ce contrôleur aux actions effectuées par l'opérateur cyber. Ceci permettrait d'éviter que le contrôleur passe trop de temps à superviser et ne prenne pas en compte les données fournies par l'opérateur cyber ce qui pourrait entrainer une mauvaise évaluation de la menace.

La supervision est un processus permettant aux opérateurs de s'assurer que « *Tout fonctionne convenablement* » (McIntyre & Salas, 1995, p.23)[38], si l'opérateur n'a pas les connaissances ni compétences pour s'assurer que « *Tout fonctionne convenablement* » la supervision perd tout son sens. Ainsi, si l'opérateur cyber était également un contrôleur aérien, une supervision mutuelle voire une méfiance sur les informations transmises entre les opérateurs pourrait être mise en place ce qui nuirait au bon fonctionnement du C2air et. Dans ce cas, l'intégration d'outils et d'informations permettant de rehausser le niveau de confiance entre ces opérateurs sera un point crucial qui devra être particulièrement étudiée pour permettre un bon fonctionnement du système sociotechnique.

Les différentes comparaisons effectuées tendent à montrer que le fait d'avoir travaillé dans des environnements à fort risque vital (OPEX) semble « stabiliser » le comportement des individus. Afin que l'opérateur RCpair ne soit pas impacté par le niveau de confiance présent entre lui et les autres opérateurs du C2air il pourrait être intéressant que l'opérateur RCpair ait travaillé dans des environnements à fort risque vital afin d'avoir été sensibilisé au risque et avoir des comportements plus stables. Dans cette expérimentation deux catégories de participants avaient effectué des OPEX : Les PN expérimentés et les mécaniciens. Afin d'analyser le comportement (stables vis-à-vis de la CI) de ces deux catégories il est nécessaire de faire une moyenne des 3 niveaux de CI pour chaque VD. Les moyennes obtenues pour les différentes VD (*Cf.* Tableau 22) pour les mécaniciens (OPEX) sont dans le même « ordre de grandeur » que les moyennes obtenues auprès du groupe contrôleurs aériens. Les mécaniciens OPEX devraient donc avoir, quel que soit le niveau de CI présent dans la relation, un comportement de supervision, de gestion du temps et de modification proche de celui des contrôleurs aériens présents dans le C2air. Dès lors, les comportements des mécaniciens (OPEX), proche de ceux d'un niveau de CI moyen chez les contrôleurs aériens, ne devraient donc pas être un facteur modulant le niveau de CI présent entre les membres de l'équipe. De plus, les mécaniciens sont déjà formés à détecter des pannes sur des systèmes (radar ou arme selon leur spécialité), et par conséquent, formés à ne pas considérer un système comme étant infaillible. Il ne semble donc pas y avoir de contre-indication à ce que le décideur final de la RCPair soit de la catégorie sociale des mécaniciens (OPEX).

Pour toutes les VD, les moyennes obtenues auprès des PN expérimentés sont du même ordre de grandeur que les moyennes obtenues chez tous les autres groupes sociaux dans le niveau de CI faible. Ces résultats tendent à montrer que les PN expérimentés ont un comportement ne dépendant pas du niveau de CI présent dans la relation mais équivalent à un comportement de confiance faible. Cela signifie que s'ils étaient opérateurs de la RCPair les PN expérimentés pourraient faire baisser le niveau de CI présent dans les C2air par leur comportement. Toutefois, ce handicap du point de vue du travail collaboratif pourrait être compensé par d'autres compétences du PN comme sa grande aptitude à prendre des décisions dans l'incertitude.

[38] « *everything is running as expected* » (McIntyre & Salas, 1995, p. 23)

Tableau 22 : Moyenne générale pour les différentes VD et pour les groupes mécaniciens (OPEX) et PN expérimentés. Moyenne générale et moyenne pour les niveaux de CI faible et élevés pour les différentes VD et pour les mécaniciens (Base) les contrôleurs aériens et les élèves PN

Variable dépendante	Moyenne (M) pour les différentes VD pour le groupe mécaniciens (OPEX)	Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe PN expérimentés	Moyenne (M) pour les différentes VD pour le groupe mécaniciens (Base)			Moyenne (M) pour les différentes VD pour le pour le groupe contrôleurs aériens			Moyenne (M) et écart type (SD) pour les différentes VD pour le groupe élèves PN		
	Moyenne des 3 niveaux de CI	Moyenne des 3 niveaux de CI	Faible	Elevé	Moyenne	Faible	Elevé	Moyenne	Faible	Elevé	Moyenne
%VDsup	M = 80.79	M = 93.73	M = 88.21	M = 84.55	M = 86.40	M = 89.78	M = 70.59	M = 79.13	M = 84.82	M = 70.71	M = 81.78
%TempsTot	M = 78.74	M = 83.75	M = 80.46	M = 79.01	M = 80.09	M = 78.60	M = 73.72	M = 77.88	M = 80	M = 75.90	M = 76.56
%VDmodif	M = 39.22	M = 54.17	M = 42.32	M = 34.74	M = 37.94	M = 48.03	M = 36.25	M = 42.64	M = 56.54	M = 40.08	M = 48.94
%VDm_sup	M = 41.1	M = 54.21	M = 42.09	M = 35.26	M = 37.98	M = 47.02	M = 42.82	M = 45.68	M = 59.70	M = 46.71	M = 54.05

Dans ce chapitre il a été considéré que le décideur final de la RCPair serait la personne en charge de donner du sens à la crise cyber. Comme indiqué sur la figure 39 cette personne devrait « rendre compte » de la situation au cyber afin qu'une décision soit prise. Ainsi, les recommandations faites ci-dessus se basent sur la nécessité d'un transfert d'information entre le décisionnaire cyber et le décisionnaire final ayant la connaissance de la situation air. Cependant, l'opérateur RCPair pourrait tout aussi bien être ce décisionnaire final (du CDC voire du CNOA). Dans ce cas-là, le choix du décideur final de la RCPair ne devrait plus se faire sur la base de ses comportements vis-à-vis de différents niveaux de CI (ce qui est proposé ici) mais sur la base de ses connaissances et compétences combinées en air et cyber. Avant de choisir le décideur final de la RCPair il semble donc fondamental de choisir le « milieu d'implantation » de cette RCPair qui pourrait tout aussi bien être un système présent uniquement dans des C2cyber, un système isolé dans un CDC, un système isolé du reste du CDC ou encore un système uniquement accessible par le décisionnaire final. Ce qui est préconisé ici est donc une démarche en 2 parties. Dans un premier temps il sera nécessaire de déterminer le milieu d'implantation du système. Dans un second temps il sera nécessaire de prendre en compte le facteur social (métier, environnement de travail, formation) permettant d'optimiser la prise de décision combinée (air et cyber).

Points clés

200 opérateurs potentiels de la RCPair ont participé à cette deuxième expérimentation. Les opérateurs étaient répartis en 5 groupes ayant des caractéristiques psychosociales différentes. Les résultats de cette deuxième expérimentation ont permis d'acquérir de nouvelles connaissances :

- sur le lien entre niveau de CI et comportement [1]
- sur le lien entre caractéristiques psychosociales du confiant, niveau de CI présent dans la relation et comportement [2]

Sur la relation [1], cette expérimentation tend à montrer que le niveau de CI présent dans une relation modifie les stratégies de supervision, les stratégies de gestion du temps et les stratégies d'acceptation des informations transmises par le coéquipier. Au plus le niveau de CI présent dans une relation diminue, au plus le nombre de supervisions augmente, au plus le temps total pris pour réaliser les tâches augmente et au plus le nombre d'informations transmises par le mandant et acceptées par le confiant diminuent. Ces 3 stratégies comportementales semblent être relativement novatrices au regard de la littérature portant sur le lien entre CI et comportement.

Sur la relation [2], cette expérimentation tend à montrer que les caractéristiques psychosociales de l'individu ne modifient pas le niveau de CI que cet individu accorde à un autre individu. Cependant les caractéristiques psychosociales de l'individu semblent modifier les actions comportementales engendrées par différents niveaux de CI. Selon l'expérience, l'environnement de travail ou encore le métier du confiant, un niveau faible ou haut de CI pourra parfois conduire à une modification des stratégies de supervision, de gestion du temps et d'acceptation des informations transmises par le coéquipier.

6 Etude de l'influence de la confiance en soi et de la confiance dans le système sur le comportement de l'opérateur

Résumé du chapitre

Objectif : Tester expérimentalement le rôle du niveau de confiance en soi (CS) et le rôle de la confiance dans la machine (CM) sur le comportement des individus qui travaillent avec des coéquipiers ayant des niveaux de CI différents

Démarche : Les résultats obtenus au chapitre précédent montrent que, dans une tâche collaborative, le comportement du confiant est modulé par les caractéristiques psychosociales du confiant et par le niveau de CI présent au sein de la relation. La littérature portant sur la CM décrit le comportement du confiant étant fonction du niveau de confiance présent entre le confiant et le système mais également du niveau de CS du confiant. Sachant que les littératures portant sur les relations de confiance lorsque le mandant est un humain ou lorsque le mandant est un système ont des bases communes il est possible que le niveau de CS du confiant explique les résultats obtenus dans le chapitre précédent.

Conclusion : Les résultats tendent à montrer que la confiance dans la machine et la CI ont les mêmes conséquences comportementales. Dans les relations de CI le niveau de CS du confiant semble avoir un rôle dans son comportement au sein de la relation. En faisant diminuer ou augmenter le niveau de CS de participants provenant d'une même catégorie sociale les résultats obtenus dans le chapitre précédent entre les classes ont été retrouvés.

Chapitre 6 : Etude de l'influence de la confiance en soi et de la confiance dans le système sur le comportement de l'opérateur

1. Cadre théorique

Les résultats obtenus au chapitre précédent suggèrent que la connaissance des caractéristiques psychosociales du confiant pourrait permettre d'anticiper l'impact du niveau de CI sur son comportement. Dans le choix du décideur final de la RCPair cette approche par caractéristiques psychosociales du confiant, permet d'émettre des réserves sur certains groupes sociaux spécifiques sur la base de leur comportement potentiel dans les relations interpersonnelles. Cependant, dans un système sociotechnique complexe et dynamique tel que les C2air, les opérateurs interagissent aussi bien avec des partenaires humains que technologiques. Or, la problématique générale de cette thèse est de déterminer les conséquences comportementales d'un manque ou d'un excès de confiance sur les opérateurs travaillant dans la RCPair. Ainsi, il est nécessaire d'étudier si les interactions potentielles entre un opérateur humain et une machine présentent des conséquences similaires à celles identifiées pour les interactions interpersonnelles pour pouvoir *in fine* comparer les mécanismes et les articuler dans une approche globale. L'expérimentation présentée dans ce chapitre vise à comparer le comportement d'opérateurs travaillant avec des systèmes transmettant des informations plus ou moins certaines (en jaune sur la figure 40) avec les comportements observés dans les relations de CI (modification de la stratégie de supervision, de gestion du temps et d'acceptation des informations transmises par le coéquipier) (en bleu sur la figure 40).

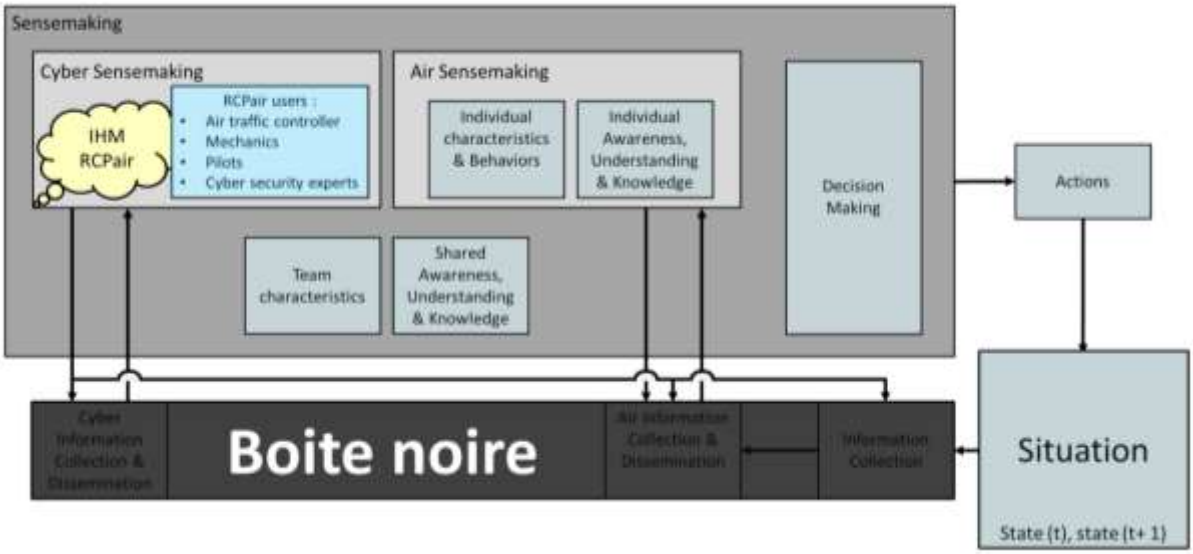


Figure 40 : Représentations des parties du modèle étudiées dans le chapitre 6

Les modèles utilisés dans la littérature portant sur la confiance dans les systèmes automatisés (confiance dans la machine, ou CM) sont basés sur les travaux de Muir, (Muir, 1987; Muir & Moray, 1996). Ces travaux s'appuient sur ceux réalisés en psychologie notamment par Deutsch (1973), Rotter (1980) ou encore Rempel Holmes et Zanna (1985) et suggèrent que les mécanismes de CM sont similaires aux mécanismes de CI. Cette base commune entre les deux littératures est caractérisée par des termes et des définitions identiques. Ainsi, la CM peut être définie comme « *l'attitude selon laquelle un agent aidera un individu à atteindre ses objectifs dans une situation caractérisée par l'incertitude et la vulnérabilité* » (Lee & See, 2004, p. 54)[39] et la CI comme « *la volonté qu'a une personne d'être vulnérable aux actions d'une autre personne en s'attendant à ce que cette dernière accomplisse une action particulière importante pour le confiant, indépendamment de la capacité de surveiller ou de contrôler cette autre personne* » (Mayer et al., 1995, p. 712)[40]. Tout comme la CI, la CM est donc une relation tripartite entre un confiant, un mandant (un système automatisé dans le cas de la CM) et une situation. Le confiant a besoin du système automatisé pour effectuer une tâche donnée permettant d'agir sur une situation donnée.

Cependant, malgré ces bases communes, certaines différences sont présentes entre les approches CM et CI, en premier lieu au niveau des méthodes employées. Le domaine de la CI est étudié majoritairement au travers d'études de terrain et de données subjectives issues de questionnaires (Dirks & Ferrin, 2002) alors que le domaine de la CM s'appuie sur des données comportementales et des méthodes expérimentales similaires à celles utilisées en psychologie (Hoff & Bashir, 2015). Ensuite, des différences sont présentes au niveau des champs théoriques mobilisés. Contrairement à la littérature en psychologie qui se focalise sur le rôle des caractéristiques du mandant dans la relation de confiance, la littérature sur la CM étudie majoritairement les caractéristiques du confiant et plus particulièrement le niveau de confiance en soi (CS) du confiant (de Vries et al., 2003; Kantowitz et al., 1997; Lee & Moray, 1992, 1994) .

Dans la littérature sur la CM, la CS est considérée comme un facteur critique dans la compréhension des interactions entre l'humain et la machine (Lee & See, 2007 ; Hoff et Bashir, 2015). Pour cette littérature, le niveau de CS du confiant est une variable permettant un changement de stratégie dans les interactions avec la machine (de Vries et al., 2003; Kantowitz et al., 1997; Lee & Moray, 1992; Lee & Moray, 1994). Ainsi, les biais liés à la CS comme l'excès de confiance sont connus pour avoir des conséquences sur la CM (Kahneman & Klein, 2009; Lee & See, 2004) et inversement. Si le niveau de CS du confiant est élevé alors que le niveau de CM que le confiant a dans le système automatisé pour réaliser la tâche est bas, alors le confiant réalisera la tâche en mode manuel et non en mode automatique. Inversement, si la CM est haute et que la CS est basse, l'opérateur restera en mode automatique comme l'indiquait Lee et See « *Lorsque la confiance en soi des opérateurs est élevée et que leur confiance dans le système est faible, ils sont plus enclins à se fier au contrôle manuel. L'inverse est également vrai* » (Lee & See, 2004, p. 23)[41].

---

[39] « *the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability* » (Lee & See, 2004, p. 54)

[40] « *the willingness of the party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party* » (Mayer et al., 1995, p. 712)

[41] « *When operators' self-confidence is high and trust in the system is low, they are more inclined to rely on manual control. The opposite is also true* » (Lee & See, 2004, p. 23)

Outre la modification du mode de conduite (automatique/manuel), il semble que le niveau de la CS pondère également le niveau de CM dans d'autres comportements du confiant (Parasuraman & Riley, 1997) comme la supervision par exemple (Lee & Moray, 1994). De même, la combinaison de faibles niveaux de CM et CS augmente la charge de travail en créant une sorte de situation en double aveugle (Lee, Gore, & Campbell, 1999). Si ces résultats sur la CS pouvaient être généralisés à toutes les littératures, ils pourraient expliquer pourquoi certains groupes sociaux ont des comportements modifiés par le niveau de CI présent dans la relation et d'autres non (*Cf.* chapitre 5 « 7. Discussion »). Dans le cas où le niveau de CS serait plus élevé que le niveau de confiance présent dans le coéquipier, le comportement du confiant serait relatif à un niveau de confiance faible. Cependant, bien que la littérature portant sur la CM tire en grande partie ses modèles de la littérature présente en psychologie rien ne permet d'affirmer que les comportements mis en jeu sont similaires.

Les premiers travaux réalisés dans la littérature sur la CM tendent à montrer un effet similaire à ceux qui ont fait l'objet d'hypothèses en psychologie, à savoir des changements de stratégie et un effet du niveau de confiance sur le monitoring (Lee, 1992; Parasuraman, Molloy, & Singh, 1993; Singh et al., 1997). Ces différentes études vont dans le sens d'un comportement similaire entre deux opérateurs humains ou entre un opérateur humain et une machine. Seulement, dans les études portant sur l'automatisation, l'approche méthodologique pour induire un niveau de confiance est réalisée par l'interaction continue entre le participant et son coéquipier « artificiel ». Dans ces études, c'est donc parce que le participant s'aperçoit petit à petit des performances du système, qu'il lui accorde plus ou moins de confiance. D'autres recherches telles que celles présentées par Reeves et Nass (1996) vont dans le sens d'une similitude entre les comportements présents dans les interactions inter-humains ou humain-système (Reeves & Nass, 1996). Dès lors, ces différentes observations suggèrent que 1) les modifications comportementales (comportements de compensation) engendrées par différents niveaux de confiance, présentes dans une relation de CI devraient être retrouvés dans une relation de CM (lien bleu sur la figure 41), 2) L'action effectuée par un confiant dans une relation de confiance est modulée par son niveau de CS (lien violet sur la figure 41) : si l'individu a plus confiance en lui qu'en son coéquipier, l'action effectuée par cet individu sera équivalente à une action correspondant à un niveau de confiance faible.

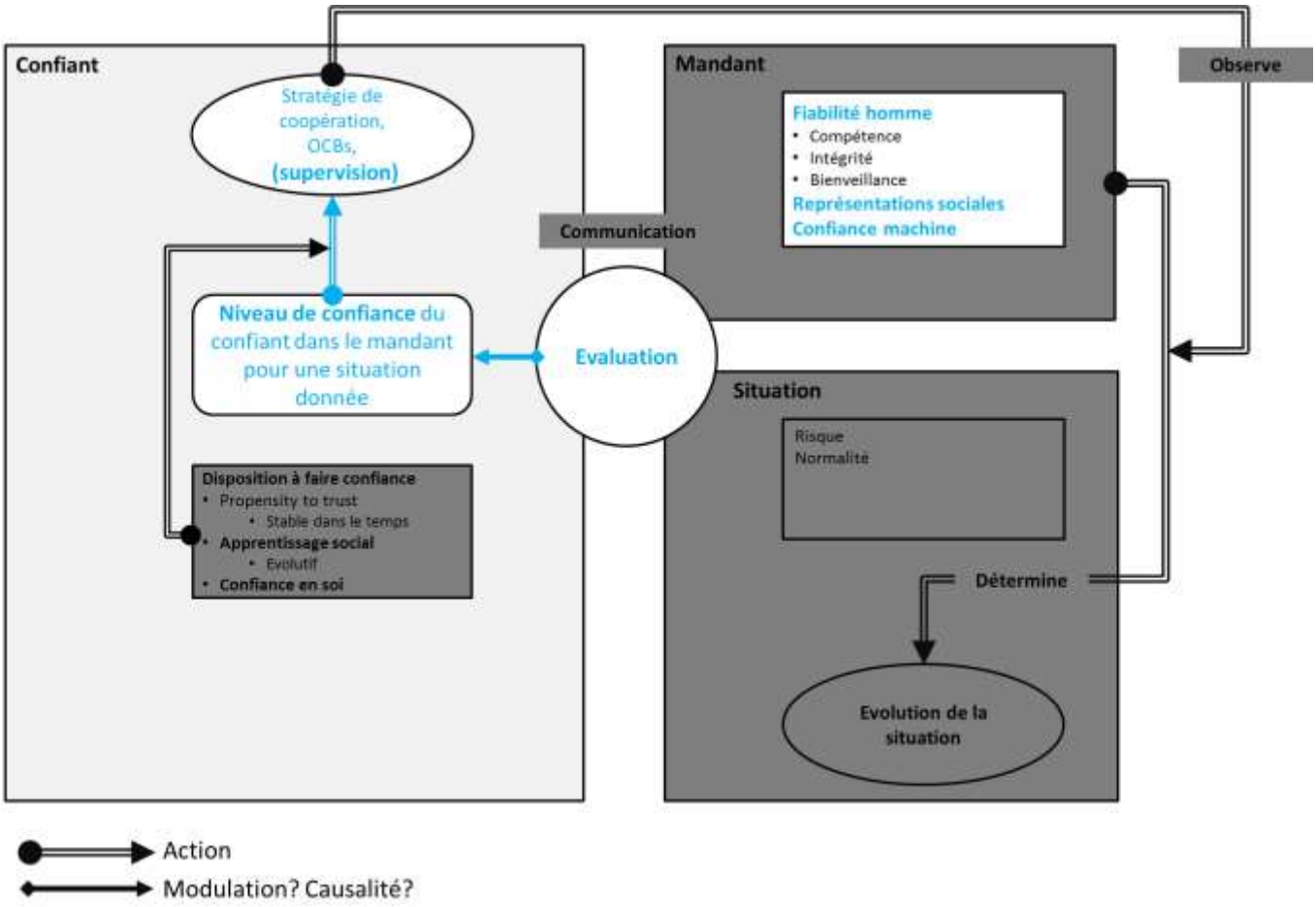


Figure 41 : Représentations des composantes du modèle de confiance étudiées dans le chapitre 6

Hypothèse 11 : Une modulation du niveau de confiance entre deux opérateurs humains ou entre un opérateur humain et un système informatique entraine des comportements de compensation similaires.

Hypothèse 12 : L'action effectuée par un confiant dans une relation de confiance est modulée par le niveau de confiance en soi de ce confiant

Afin de tester ces hypothèses deux études ont été réalisées. Le but de la première expérimentation (deuxième expérimentation de cette thèse) était de comparer le comportement d'individus lorsqu'ils devaient collaborer avec un coéquipier humain et avec un système automatisé. La deuxième expérimentation (troisième expérimentation de cette thèse) avait pour but d'observer les modulations comportementales engendrées par un manque ou excès du niveau de CS d'un individu dans une tache collaborative avec un coéquipier humain.

2. Expérimentation portant sur la différence entre la CI et la confiance dans la machine

Afin de comparer efficacement les modulations comportementales engendrées par différents niveaux de confiance associés par un confiant à un coéquipier humain ou à un système informatisé (hypothèse 11), il était nécessaire que les mécanismes d'induction de confiance soient similaires dans les deux conditions expérimentales (e.g. tâche collaborative avec un coéquipier humain et tâche collaborative avec un coéquipier informatisé). Pour ce faire, l'induction par pourcentage de fiabilité qui est le type d'induction utilisé de manière préférentielle dans les recherches menées en informatique et notamment dans le e-commerce, a été choisie (Resnick et al., 2004).

Cette méthode d'induction qui semble fonctionner lorsque le mandant est un système informatisé, n'a *a priori* jamais été utilisée, testée et validée dans le cas d'un mandant humain. Dans cette étude la confiance a été induite à l'aide de pourcentage de fiabilité (renvoyés par un humain et renvoyés par une machine) et les résultats ont été comparés avec des données obtenues dans l'expérimentation précédente, en utilisant exactement les mêmes classes de catégorie socio-professionnelle de confiant.

A. Matériel et méthode

a. Participants

40 personnes (30% de femmes et 70% d'hommes) d'âge moyen 22.4 ans (SD : 2.1) ont participé à cette étude. Tous les participants étaient des élèves de l'école de l'air ayant des caractéristiques sociales strictement équivalentes à celles de la catégorie « élèves PN » de l'expérimentation précédente. Aucun participant n'avait de problème de santé, tous avaient une vision normale ou corrigée.

b. Protocole

Avant le début de l'expérimentation, un briefing a été effectué et tous les participants ont rempli une feuille de consentement éclairé. Ensuite, les participants ont effectué un entrainement de 5 minutes avant de commencer l'expérimentation. L'expérimentation était basée sur le protocole présenté au chapitre 4, les participants devaient donc réaliser une tâche de comptage et de supervision avec 42 coéquipiers fictifs différents.

Contrairement à ce qui a été présenté au chapitre 4, dans cette expérimentation, le coéquipier (humain et IA), n'était pas représenté par une paire de mots en phase 1 mais par un score de fiabilité présenté en phase 2. Ainsi, dans cette expérimentation, seuls la consigne et le temps disponible étaient présentés en phase 1. Durant la phase 2, lorsque le coéquipier (fictif) avait terminé sa tâche de comptage, il transmettait au participant un score de fiabilité (*Cf.* Figure 42). Dans cette expérimentation le score de fiabilité transmis par le coéquipier (humain et IA), pouvait être :

- Compris entre 71 et 79% (niveau de confiance faible, 14 essais)

- Compris entre 81 et 89% (niveau de confiance intermédiaire 14 essais)
- Compris entre 91 et 99% (niveau de confiance élevé 14 essais)

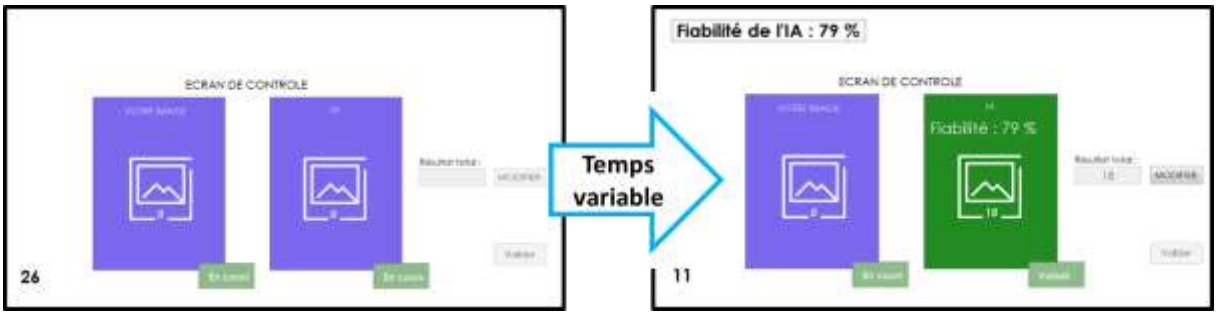


Figure 42 : Schéma représentant l'induction de confiance utilisée dans l'expérimentation 2. Lorsque le coéquipier a terminé sa tâche de comptage il transmet un score de fiabilité au participant. L'induction du niveau de confiance est donc effectuée, après le début de la tâche de comptage.

Pour cette expérimentation, deux conditions expérimentales ont été mises en œuvre. Dans la première, le coéquipier était décrit au participant comme étant une Intelligence artificielle (IA). Dans cette condition expérimentale le temps de réponse de l'IA (i.e le temps passé avant la fin de la tâche de comptage du coéquipier et l'apparition du score de fiabilité) était d'approximativement 1s (tiré aléatoirement entre 0,75 et 1,25 secondes).

Dans la deuxième condition expérimentale, les coéquipiers fictifs étaient décrits au participant comme étant des anciens participants dont les comportements avaient été enregistrés. Dans cette condition expérimentale le temps de réponse était fonction de l'image du coéquipier (calcul présenté dans le chapitre 4 auquel 15% du temps a été retranché) (*Cf.* chapitre 4 « 2. Protocole expérimental »). 50% des participants ont passé l'expérimentation dans la première condition et 50% des participants ont passé l'expérimentation dans la deuxième condition.

Pendant l'expérimentation, les scores de fiabilités (humain et IA) étaient présentés de manière strictement équivalente. Cependant, avant l'expérimentation, le calcul de ces scores était présenté différemment aux participants. Le calcul de fiabilité humain était décrit comme une « autoévaluation transmise par un opérateur qui a préalablement effectué cette tâche ». Le calcul de fiabilité IA était décrit comme « Pourcentage de pixels utilisés pour classer les différents objets présents dans l'image ». Dans cette expérimentation, tous les tirages, aléatoires ou pseudo aléatoires, et toutes les VD recueillies étaient strictement équivalentes à celles présentées au chapitre 5.

B. Résultats

Les données des 40 participants ont été incluses dans l'analyse. A ces données ont été ajoutées les données des 20 participants de la catégorie « élèves PN » ayant passé l'expérimentation 1 en temps court (le groupe social des participants et l'expérimentation étant similaire). Dans l'analyse des résultats ces données sont nommées « Dyade ».

a. Evaluation subjective des résultats transmis par le coéquipier

Une analyse en statistiques descriptives des données portant sur l'évaluation subjective des résultats transmis par le coéquipier (CertitudeCoéquipier) (*Cf.* Figure 43) semble montrer que, quel que soit le type d'induction, lorsque le niveau de confiance est élevé, l'évaluation subjective de la performance du coéquipier est meilleure que lorsque le niveau de confiance est faible. L'évaluation subjective des résultats transmis par le coéquipier semble être plus élevée pour les participants ayant eu une induction de confiance réalisée en utilisant le pourcentage de fiabilité transmis par un opérateur humain que pour les participants ayant reçu un autre type d'induction.

Variable dépendante	Induction	Confiance induit	Min	Max	Moyenne	Médiane	Ecart Type
Niveau de certitude dans la réponse du partenaire	Dyade	C+	4.33	9.27	7.15	7.26	1.46
		C+/-	3.67	8.83	5.77	5.72	1.41
		C-	1.90	8.75	4.77	4.63	1.54
	Homme	C+	3.69	9.62	8.12	8.67	1.56
		C+/-	4.61	8.99	7.37	7.83	1.26
		C-	4.22	8.66	7.06	7.14	1.15
	IA	C+	2.50	9.82	7.48	8.45	2.14
		C+/-	1.30	8.80	6.17	6.70	2.18
		C-	2.24	8.59	5.73	6.20	2.14

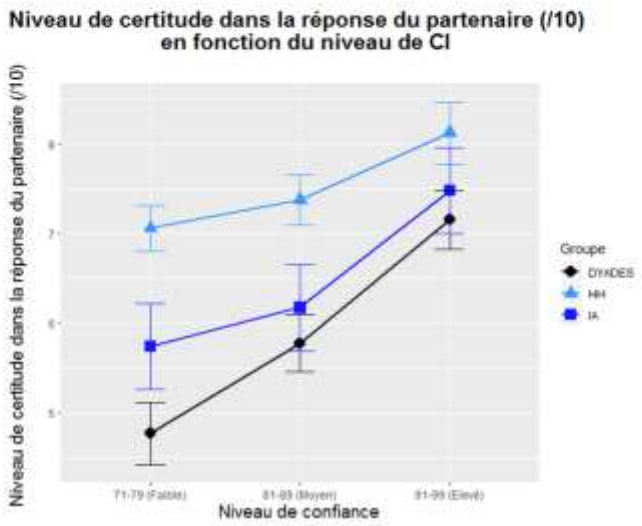


Figure 43 : Statistiques descriptives et représentation graphique des résultats obtenus par chaque groupe d'induction à la VD *CertitudeCoéquipier* en fonction du niveau de confiance induit

Les résultats de l'analyse en statistiques inférentielles montrent un effet simple du type d'induction, $F(2,57) = 5.61$, $P = .005$**, un effet simple du niveau de confiance, $F(2,114) = 66.67$, $P < .001$*** mais également un effet d'interaction, $F(4,114) = 3.28$, $P = .01$*. Le test Tukey HSD réalisé sur l'effet simple portant sur le type d'induction montre :

- une différence significative entre l'induction réalisée en utilisant le pourcentage de fiabilité transmis par un opérateur humain et celle réalisée en utilisant les paires de mots inductrices ($P < .001$***)
- une différence significative entre l'induction réalisée en utilisant le pourcentage de fiabilité transmis par un opérateur humain et celle réalisée en utilisant le pourcentage de fiabilité transmis par une IA ($P = .03$*).

Le test Tukey HSD réalisé sur l'effet d'interaction indique que, quel que soit le moyen d'induction utilisé, une différence significative ($p < .001$***) est présente entre le niveau de CI fort et le niveau de CI faible. L'effet d'interaction présent dans l'ANOVA est donc dû au fait que, selon la méthode d'induction utilisée, des différences significatives n'ont pas été observées entre le niveau de CI faible et le niveau de CI moyen ou entre le niveau de CI moyen et le niveau de CI fort. Il est à noter que pour l'induction par paire de mots (groupe « DYADES ») une différence significative est présente entre le niveau de CI fort et le niveau de CI moyen ($p < .001$***) mais également entre le niveau de CI moyen et le niveau de CI faible ($p < .001$***). Seulement, pour les deux autres méthodes d'induction (groupes « HH » et « IA ») aucune différence significative n'est présente entre le niveau de CI moyen et le niveau de CI faible. Pour cela, le niveau de CI moyen ne sera pas pris en compte dans les analyses en statistiques inférentielles présentées ci-dessous.

b. Evaluation comportementale

Les différentes analyses de la VD CertitudeCoéquipier montrent donc que quelle que soit la méthode d'induction (paires de mots, pourcentages de fiabilité humain, pourcentages de fiabilité IA) différents niveaux de confiance sont bien induits aux participants. Afin de valider cette observation obtenue grâce à des données subjectives, l'analyse de données comportementales a été effectuée sur :

- Le pourcentage de supervisions (%VDsup) ;
- Le pourcentage de temps passé à superviser (%TempsSuperv) ;
- Le pourcentage de modifications (%VDmodif).

Contrairement aux résultats de l'expérimentation précédente, l'analyse du pourcentage de temps total est remplacée par l'analyse du pourcentage de temps passé par le participant pour effectuer la tâche de supervision (facultative). Ce choix de variable est réalisé car dans le protocole expérimental présenté ici, le (affichage du niveau de confiance) est différent selon les conditions expérimentales (environ 1 temps d'affichage du pourcentage de fiabilité seconde dans lors du travail avec une IA et toujours plus de 7 secondes lors du travail avec un coéquipier humain).

Dans la condition expérimentale dans laquelle le pourcentage de fiabilité est transmis par un opérateur humain l'induction du niveau de confiance arrive plus « tardivement » que dans la condition expérimentale dans laquelle le pourcentage de fiabilité est transmis par une IA. Ceci permet de donner l'impression au participant que le comportement du coéquipier est un comportement « réel » pré-enregistré sur un participant ayant préalablement effectué la tâche. Cependant, pour cette raison, les stratégies de gestion « globale » du temps ne peuvent pas être similaires entre les deux conditions alors que les stratégies de supervisions peuvent l'être.

Pourcentage de supervisions

Une analyse en statistiques descriptives des données portant sur la variable %VDsup (*Cf.* Figure 44) semble montrer que, quel que soit le type d'induction, lorsque le niveau de confiance est élevé, le pourcentage de supervision est plus faible que lorsque le niveau de confiance est faible. De plus, le

pourcentage de supervision semble être plus élevé pour les participants ayant eu une induction par paire de mots (groupe « DYADES ») que pour les participants ayant reçu un autre type d'induction.

Variable dépendante	Induction	Confiance induit	Min	Max	Moyenne	Médiane	Ecart Type
Pourcentage de supervisions (%)	Dyade	C+	0.00	100	64.76	75.00	32.56
		C+/-	0.00	100	79.23	89.28	27.59
		C-	0.00	100	86.34	96.42	24.06
	Homme	C+	0.00	100	55.71	57.14	35.87
		C+/-	0.00	100	72.50	85.71	29.70
		C-	7.14	100	76.07	92.85	31.28
	IA	C+	0.00	100	55.00	64.28	34.76
		C+/-	0.00	100	65.35	64.28	30.85
		C-	7.14	100	72.11	75.00	25.49

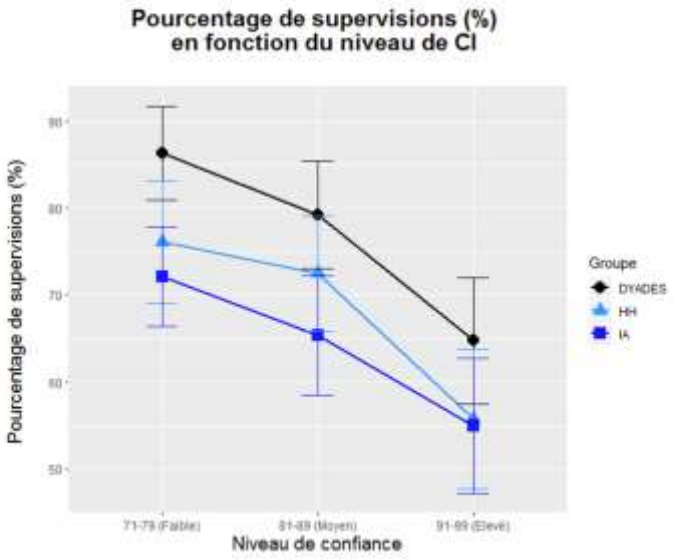


Figure 44 : Statistiques descriptives et représentation graphique des résultats obtenus par chaque groupe d'induction à la VD *%VDsup* en fonction du niveau de confiance induit.

Les résultats de l'analyse en statistiques inférentielles montrent un effet simple du niveau de confiance, $F(2,114) = 27.627$, $P < .001$*** mais aucun effet simple sur le type d'induction, $F(2,57) = 1.06$, $P = .35$ ainsi qu'aucun effet d'interaction, $F(4,114) = .29$, $P = .88$, ce qui va dans le sens de l'hypothèse 11 (une modulation du niveau de confiance entre deux opérateurs humains ou entre un opérateur humain et un système informatique entraine des comportements de compensation similaires). Ces résultats montrent qu'une modulation du niveau de confiance entre deux opérateurs humains ou entre un opérateur humain et un système informatique entraine une modulation du nombre de supervisions. Rien ne permet d'indiquer que cette modulation du nombre de supervisions soit différente selon le type d'induction.

Pourcentage de temps passé à superviser

Une analyse en statistiques descriptives des données portant sur le pourcentage de temps passé à superviser (%TempsSuperv) (*Cf.* Figure 45) semble montrer que, quel que soit le type d'induction, lorsque le niveau de confiance est élevé, le pourcentage de temps passé à superviser est plus faible que lorsque le niveau de confiance est faible.

Variable dépendante	Induction	Confiance induit	Min	Max	Moyenne	Médiane	Ecart Type
Pourcentage de temps utilisé par le participant pour effectuer la tâche de supervision (%)	Dyade	C+	0.00	35.89	17.49	16.90	10.89
		C+/-	0.00	33.76	21.05	22.80	8.84
		C-	0.00	33.82	23.58	24.76	8.30
	Homme	C+	0.00	35.24	14.95	16.49	11.00
		C+/-	0.00	32.75	19.49	20.84	9.25
		C-	1.77	35.54	21.26	24.29	10.21
	IA	C+	0.00	33.39	13.76	14.58	10.05
		C+/-	0.00	31.90	16.40	15.58	9.48
		C-	1.95	31.77	18.36	18.36	8.31

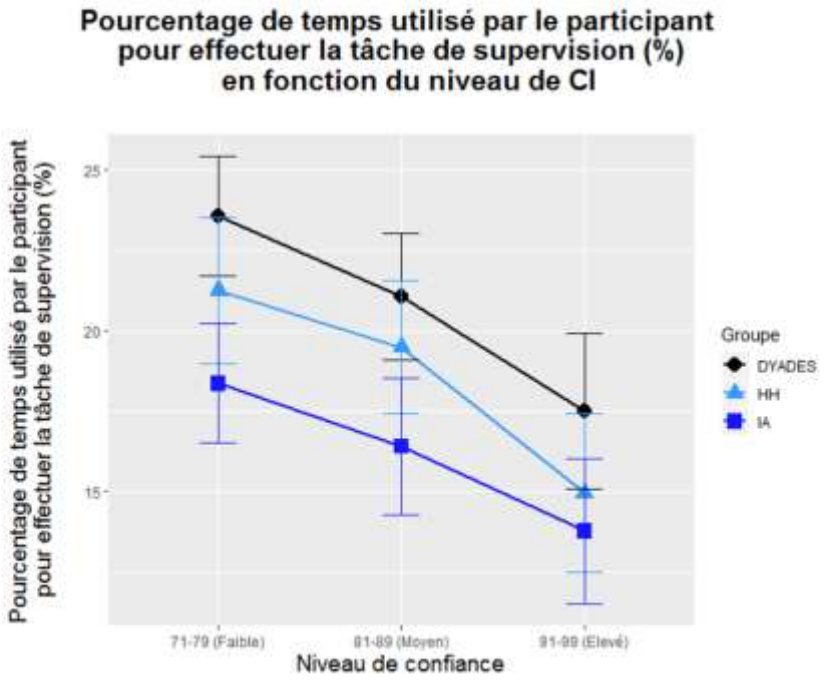


Figure 45 : Statistiques descriptives et représentation graphique des résultats obtenus par chaque groupe d'induction à la VD *%TempsSuperv* en fonction du niveau de confiance induit.

Les résultats de l'analyse en statistiques inférentielles montre un effet simple du niveau de confiance, $F(2,114) = 24.52$, $P < .001$*** mais aucun effet simple sur le type d'induction, $F(2,57) = 1.29$, $P = .28$ ainsi qu'aucun effet d'interaction $F(4,114) = 0.32$, $P = .86$ ce qui va dans le sens de l'hypothèse 11 (une modulation du niveau de confiance entre deux opérateurs humains ou entre un opérateur humain entraine des comportements de compensation similaires). Ces résultats montrent donc qu'une modulation du niveau de confiance entre deux opérateurs humains ou entre un opérateur humain et un système informatique entraine une modulation du temps passé à superviser. Rien ne permet d'indiquer que cette modulation du temps passé à superviser est différente selon le type d'induction.

Pourcentage de modifications

Une analyse en statistiques descriptives des données portant sur le pourcentage de modifications (%VDmodif) (*Cf.* Figure 46) tendent à montrer que, quel que soit le type d'induction, lorsque le niveau de confiance est élevé, le pourcentage de modification est plus faible que lorsque le

niveau de confiance est faible. De plus, le pourcentage de modifications semble être plus élevé pour les participants ayant eu une induction par paire de mots (groupe « DYADES ») que pour les participants ayant reçu un autre type d'induction.

Variable dépendante	Induction	Confiance induit	Min	Max	Moyenne	Médiane	Ecart Type
Pourcentage de modifications (%)	Dyade	C+	0.00	64.28	30.17	28.57	20.48
		C+/-	7.14	78.57	35.76	28.57	21.68
		C-	0.00	78.57	43.80	46.42	20.29
	Homme	C+	0.00	78.57	20.71	7.14	26.51
		C+/-	0.00	64.28	22.50	21.42	22.01
		C-	0.00	64.28	26.78	32.14	24.73
	IA	C+	0.00	64.28	10.35	3.57	16.46
		C+/-	0.00	57.14	15.35	7.14	19.28
		C-	0.00	71.42	19.64	14.28	22.09

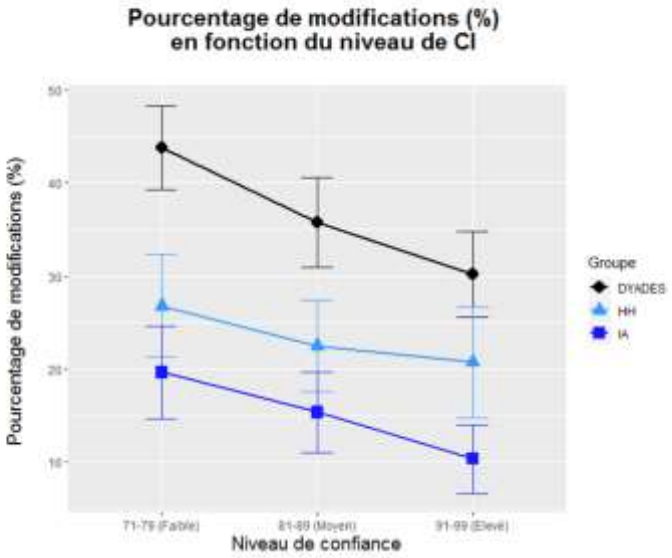


Figure 46 : Statistiques descriptives et représentation graphique des résultats obtenus par chaque groupe d'induction à la VD % VDmodif en fonction du niveau de confiance induit.

Les résultats de l'analyse en statistiques inférentielles montrent un effet simple sur le type d'induction, $F(2,57) = 6.02$, $P = .004$** ainsi qu'un effet simple du niveau de confiance, $F(2,114) = 11.68$, $P < .001$*** mais aucun effet d'interaction, $F(4,114) = 0.63$, $P = .63$. Le test Tukey HSD réalisé sur l'effet simple portant sur le type d'induction indique

- une différence significative entre l'induction réalisée en utilisant les paires de mots inductrices et celle réalisée en utilisant le pourcentage de fiabilité transmis par un opérateur humain ($P = .03$*)
- Une différence significative entre l'induction réalisée en utilisant les paires de mots inductrices et celle réalisée en utilisant le pourcentage de fiabilité transmis par une IA ($P < .001$***).

Ces résultats montrent qu'une modulation du niveau de confiance entre deux opérateurs humains ou entre un opérateur humain et un système informatique entraine une modulation du nombre de supervision. Rien ne permet d'indiquer que cette modulation du nombre de modifications soit différente selon le type d'induction. Cependant, ces résultats montrent, qu'en moyenne, le

pourcentage de modification est significativement plus élevé lorsque le niveau de confiance est induit en utilisant la méthode des paires de mots.

3. Discussion

Pris ensemble les résultats de cette deuxième expérimentation apportent plusieurs informations, que ce soit sur le fonctionnement de la mise en place d'un niveau de confiance ou sur les liens entre CM et CI. Tout d'abord, les résultats de cette expérimentation tendent à montrer que le pourcentage de fiabilité transmis par un opérateur humain ou par un système automatisé permet d'induire différents niveaux de confiance à un opérateur humain. Ceci donne des informations sur les bases nécessaires à la mise en place d'un niveau de confiance et tend en quelque sorte à montrer la coexistence des mécanismes de *propensity to trust* et de confiance par apprentissage social dans la mise en place du niveau de confiance initial.

En effet, dans l'expérimentation précédente, avec l'induction par paires de mots, le mécanisme d'apprentissage social permettait d'induire différents niveaux de CI. La réception par les participants, des RS qu'ils pouvaient associer au mandant permettait de faire varier les niveaux de confiance qu'ils accordaient aux différents mandants. Le fait que l'induction par fiabilité transmise par une IA fonctionne pourrait s'expliquer par ce même mécanisme d'apprentissage et de RS (« sachant que le taux de fiabilité est transmis par une machine et que j'ai un certain niveau de confiance dans les machines alors mon niveau de confiance dans les informations transmises par cette machine est… »). Cependant, le fait que l'induction par fiabilité transmise par un opérateur humain fonctionne ne peut pas être expliqué par ce mécanisme d'apprentissage et de RS. En effet, dans cette condition expérimentale, les participants n'avaient aucune information sociale provenant des différents mandants. Seulement, en l'absence de RS, des niveaux de confiance différents ont pu être induits. Ceci tend à montrer que, dans ce type d'induction, un autre mécanisme de mise en place d'un niveau de confiance est possiblement entré en jeu.

Outre la mise en évidence des différents mécanismes permettant la mise en place d'un niveau de confiance initial, ces résultats permettent d'apporter des informations sur les liens entre CM et CI. Toutes les variables comportementales étudiées ont été modulées par le niveau de confiance et ce, que ce soit dans la condition CM ou dans la condition CI (*Cf.* Figure 47). Ainsi, tous les résultats comportementaux vont dans le sens de l'hypothèse 11 et tendent donc à montrer qu'une modulation du niveau de confiance entre deux opérateurs humains ou entre un opérateur humain et un système informatique entraine des comportements de compensation similaires. Ces résultats permettent de montrer que les deux systèmes de confiance (CM et CI) peuvent être étudiés conjointement et que, par conséquent, il devrait être possible d'utiliser des paradigmes de CM dans les études sur la CI et inversement. D'après ces résultats, l'hypothèse 12 prendrait tout son sens car si l'action effectuée par un confiant dans une relation de CM est réellement modulée par le niveau de CS de ce confiant, alors l'action effectuée par un confiant dans une relation de CI devrait également être modulée par le niveau de CS de ce confiant.

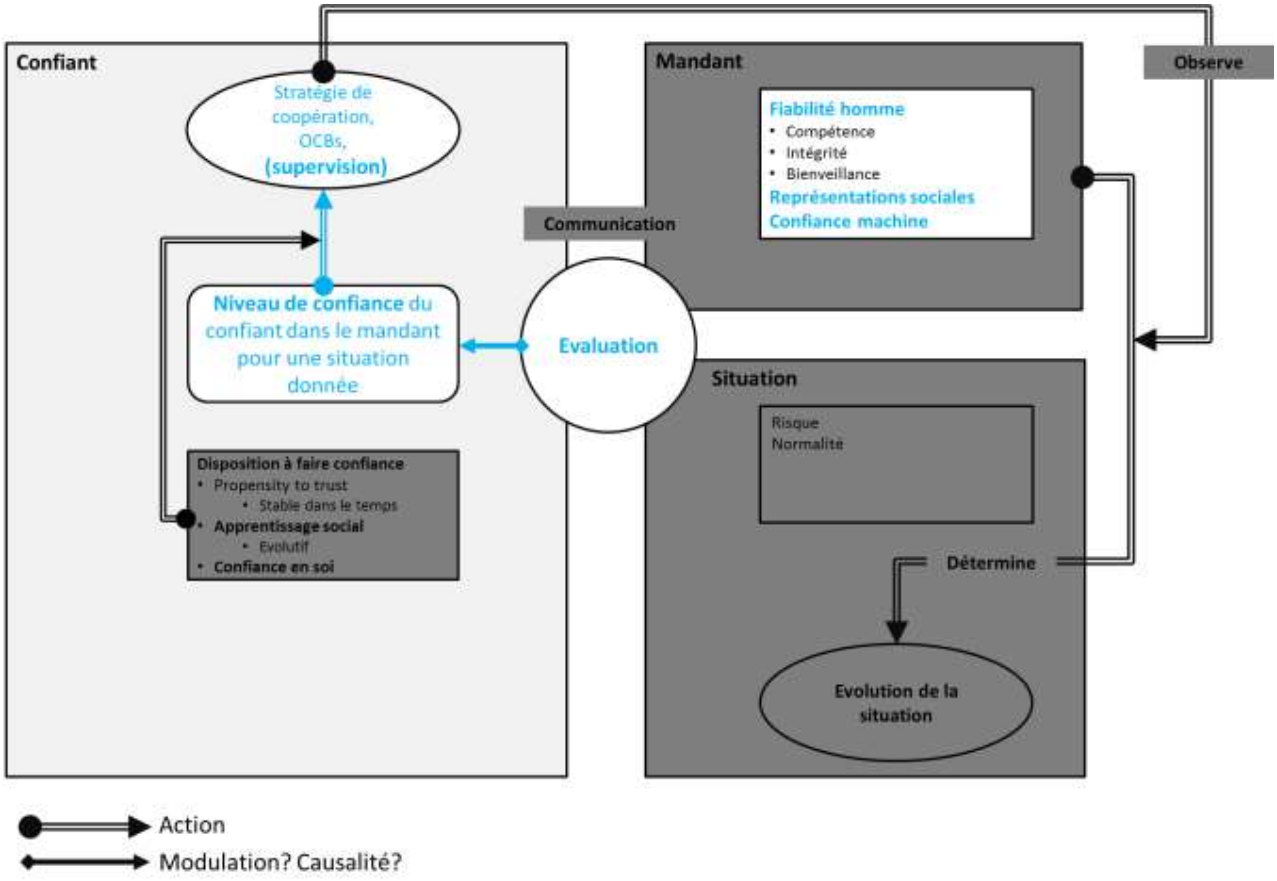


Figure 47 : résultats de l'expérimentation 2
Les RS que le confiant attribue au mandant ainsi que le taux de fiabilité que le mandant s'auto-attribue (que ce mandant soit un humain ou une IA) permettent la mise en place du niveau de confiance qui va modifier le comportement du confiant. Quel que soit le mandant (humain ou IA), les modifications comportementales engendrées par différents niveaux de confiance sont similaires.

4. Apport de l'expérimentation 2 à la RCPair

Les résultats de cette expérimentation tendent à montrer qu'un pourcentage de fiabilité, qu'il soit transmis par un opérateur humain ou par un système (la RCPair) induit un niveau de confiance. Ce niveau de confiance, qu'il soit entre deux opérateurs humains ou entre un opérateur humain et un système automatisé, semble entrainer les mêmes modifications comportementales. En d'autres termes, rien n'indique que les comportements engendrés par un niveau faible de CM soient différents des comportements engendrés par un niveau faible de CI. Le chapitre précédent décrivait les modulations comportementales, qui étaient fonction du niveau de confiance mais également fonction des caractéristiques sociales du confiant. Ainsi, en connaissant les caractéristiques sociales du décideur final de la RCPair et en connaissant la manière dont le niveau de confiance (CM ou CI) influe sur son comportement il devient théoriquement possible d'optimiser le fonctionnement du système sociotechnique.

Selon le profil du décideur final, il pourra être envisagé que le système RCPair transmette des pourcentages de fiabilité de survenu d'un incident cyber pondéré par la gravité de cet incident. Comme pour les matrices de risques, cette pondération pourrait être effectuée en utilisant un code

couleur apposé sur le taux de fiabilité. Cependant, cette pondération pourrait également être directement prise en compte dans le calcul du taux de fiabilité.

Cette approche par taux de fiabilité transmis pourrait être étendue aux relations interpersonnelles intra C2air. Comme vu précédemment, il est préconisé que la RCPair soit utilisée dans des C2air organisés en *Edge C2.* Dans ce type d'organisation, l'opérateur RCPair devra communiquer avec des opérateurs qu'il connait et qu'il a appris à connaitre mais pourra également communiquer de manière éphémère avec des opérateurs totalement inconnus présents dans d'autres centres. Ainsi, le taux de fiabilité transmis par un autre opérateur humain est interprété par le confiant, probablement par le biais du mécanisme de *propensity to trust*, comme un niveau de confiance pouvant être attribué à une personne totalement inconnue sur une tâche donnée. Ainsi, de manière similaire à ce qui a été présenté au paragraphe précédent, il pourrait être intéressant, que dans des C2air, des taux de fiabilité soient apposés aux informations transmises entre opérateurs inconnus.

Points clés

40 élèves PN ont participé à cette expérimentation. Le protocole expérimental était exactement le même entre cette expérimentation et la précédente à ceci près que l'induction de confiance était effectuée différemment. Dans cette expérimentation les élèves devaient collaborer soit avec un opérateur humain (20 élèves PN) transférant des niveaux de fiabilité soit avec un système automatisé (20 élèves PN) transférant des niveaux de fiabilité. Les résultats obtenus dans cette expérimentation ont été comparés avec les résultats obtenus auprès des 20 élèves PN de l'expérimentation précédente. Les résultats indiquent qu'une induction par taux de fiabilité transmis par un opérateur humain induit différents niveaux de CI et qu'une induction par taux de fiabilité transmis par un système automatisé induit également différents niveaux de confiance. Au niveau comportemental, les résultats tendent à montrer que, quelle que soit la méthode d'induction de confiance utilisée (paires de mots, pourcentages de fiabilité machine ou pourcentages de fiabilité humaine) les comportements modulés par le niveau de confiance sont les mêmes. Ainsi, analysés ensemble les résultats tendent à montrer que les comportements observés dans la littérature sur la CI sont équivalents à ceux observés dans la littérature sur la CM.

5. Expérimentation portant sur les modifications comportementales liées à la confiance en soi et à la confiance interpersonnelle

La littérature portant sur la CM indique un lien entre le niveau de CS de l'opérateur, le niveau de CM et le comportement de l'opérateur de telle sorte qu'un opérateur ayant un haut niveau de CS et un faible niveau de CM effectue plus les tâches en mode manuel qu'un opérateur ayant un faible niveau de CS et un haut niveau de CM (Lee & See, 2004). Les résultats de l'expérimentation précédente (*Cf.* chapitre 6 « C. Discussion ») montrent que les relations de CM et de CI amènent, chez les confiants, des modifications comportementales similaires. Ainsi, on s'attend à ce que le niveau de CS module également l'effet de CI sur le comportement de l'opérateur, ce qui fait l'objet de l'hypothèse 12. Afin de tester cette hypothèse selon laquelle l'action effectuée par un confiant dans une relation de confiance est modulée par le niveau de confiance en soi de ce confiant, une nouvelle expérimentation a été menée.

A. Matériel et méthode

a. Matériel

Dans cette expérimentation on cherche à mesurer si la confiance en soi du chef d'équipe va modifier les stratégies mises en place dans sa coopération avec son coéquipier. Cette expérimentation est basée sur le protocole expérimental décrit au chapitre 4, mais cette fois-ci, l'expérimentation est découpée en 28 essais réussis (14 en CI élevée et 14 en CI faible) et est précédée d'une pré expérimentation préliminaire de calibrage de la performance (« calibrage »).

Ce calibrage permet de modifier la confiance qu'a le participant dans sa propre performance pour réaliser la tâche. Ainsi, deux groupes de participants sont créés de manière contrôlée : celui des individus ayant une confiance en eux (pour réaliser la tâche) plutôt forte (classe *CS+*) et celui des individus ayant une plus faible confiance en eux (pour réaliser la tâche) (classe *CS-*). Le contrôle du niveau de CS permet ensuite d'étudier son impact sur les stratégies de coopération.

b. Mise en place du calibrage

Introduction

Dans la littérature portant sur la CS, les recherches, notamment menées dans le domaine de la pratique sportive, sont axées sur différentes méthodes permettant d'augmenter le niveau de CS d'une personne (Smith, Smoll, & Curtis, 1979; Smoll, Smith, Barnett, & Everett, 1993). Pour cela, des méthodes de renforcement (donner des retours positifs) ou d'encouragement (donner des instructions pour corriger les erreurs) sont fréquemment utilisées.

Pour réaliser les différentes classes de CS utilisées au test de l'hypothèse 12, il était nécessaire d'avoir un mécanisme permettant d'augmenter le niveau de CS ainsi qu'un mécanisme permettant de le faire diminuer. Sur la base des mécanismes de renforcement utilisés dans la pratique sportive,

une pré-expérimentation permettant de tester un mécanisme de renforcement positif ou négatif a été effectuée.

Matériel et méthode

12 participants ont effectué cette pré expérimentation (16% de femmes et 84% d'hommes). 6 participants ont réalisé cette pré-expérimentation dans la classe CS+ et 6 participants ont réalisé l'expérimentation dans la classe CS-.

La pré-expérimentation poursuivait plusieurs buts :

- observer la possibilité, en utilisant une technique de renforcement négatif, de faire baisser le niveau de CS de différents individus sur une tâche donnée ;
- observer le temps que prendrait ce mécanisme de renforcement négatif pour induire une diminution du niveau de CS sur une tâche donnée.

Avant de commencer la pré-expérimentation, tous les participants ont rempli deux questionnaires réalisés en 1965 par Rosenberg (Rosenberg, 1965) (*Cf.* « Feuille consentement et questionnaire utilisés dans les expérimentations 3 et 4 »). Les échelles des deux questionnaires étaient constituées de 5 niveaux allant de *Disagree strongly* à *Agree Strongly.* Le premier questionnaire, appelé « GSE » (*general self esteem*) était constitué de 9 items permettant de donner une indication sur le niveau général de CS du participant. Le deuxième, dénommé « SEV » (*self esteem variability*) était constitué de 5 items permettant d'obtenir une mesure relativement fiable de la variation, au cours du temps, de l'estime de soi d'un individu (Webster et al., 2017).

La pré-expérimentation était divisée en 16 essais de 4 phases distinctes (*Cf.* Figure 48) :

- Une phase (1) de comptage ;
- Une phase (2) d'autoévaluation de la performance sur l'image présentée en phase 1 ;
- Une phase (3) d'autoévaluation sur les 4 dernières images présentées ;
- Une phase (4) de renforcement portant sur le résultat des 4 dernières images.

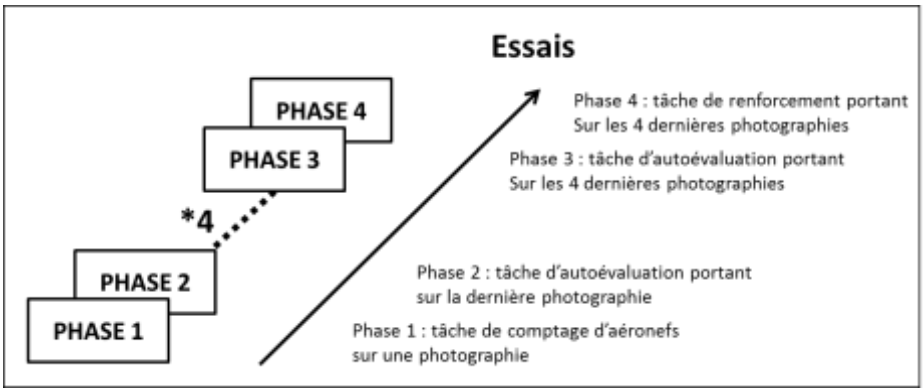


Figure 48 : Schéma représentant les différentes phases de la pré-expérimentation

Dans la phase 1 le participant se trouvait devant un affichage (*Cf.* Figure 49) sur lequel il y avait une image, un compteur et un chronomètre. Toutes les images utilisées durant cette pré-expérimentation étaient des images de l'expérimentation présentée au chapitre 4. Pour terminer la phase 1, le participant devait compter le nombre d'aéronefs présents sur l'image, incrémenter le compteur pour indiquer son résultat (ce qui active le bouton de validation) puis cliquer sur le bouton de validation qui le faisait passer en phase 2.

En phase 2, il était demandé au participant d'évaluer sa performance sur la tâche réalisée en prenant en compte à la fois le temps mis et l'exactitude probable de sa réponse. Pour cela, le participant se trouvait devant une échelle non segmentée (*Cf.* Figure 49). Cette échelle permettait au participant d'indiquer le niveau de certitude relatif à sa performance réalisée sur l'image précédente. Aucun retour sur la performance réelle du participant n'était donné à ce stade. Le participant devait faire bouger le curseur permettant d'indiquer son évaluation de sa performance, ce qui activait le bouton de validation. Après validation le participant retrouvait l'affichage de la phase 1 jusqu'à ce qu'il ait compté 4 images différentes. Lorsque le participant cliquait sur le bouton valider de l'échelle de la quatrième image il passait automatiquement en phase 3.

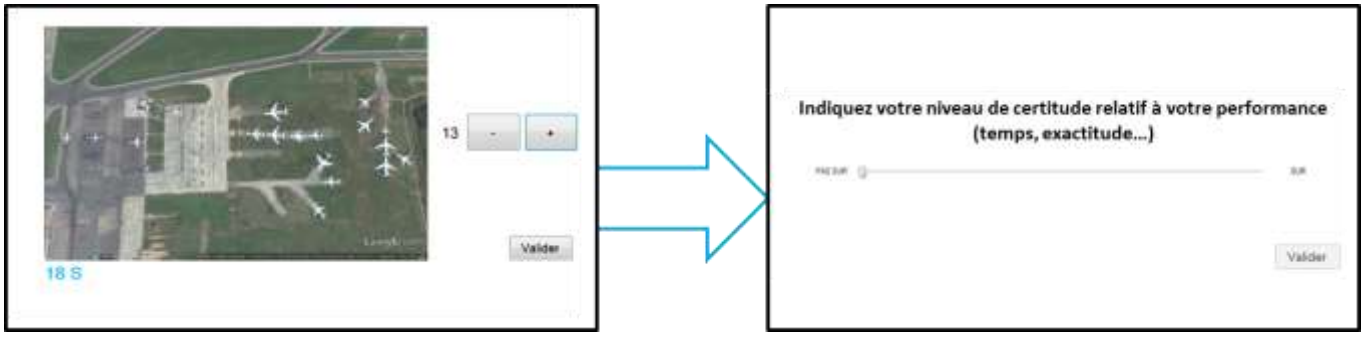


Figure 49 : Phase 1 et 2 de la pré expérimentation.

En phase 3 le participant se trouvait devant un affichage (*Cf.* Figure 50) sur lequel 3 échelles non segmentées étaient présentées. Ces différentes échelles portaient sur les 4 dernières images et permettaient au participant d'indiquer :

- Le score qu'il s'attribue quant à l'exactitude des résultats ;
- Le score qu'il s'attribue quant à la vitesse de comptage ;
- Le score total qu'il s'attribue.

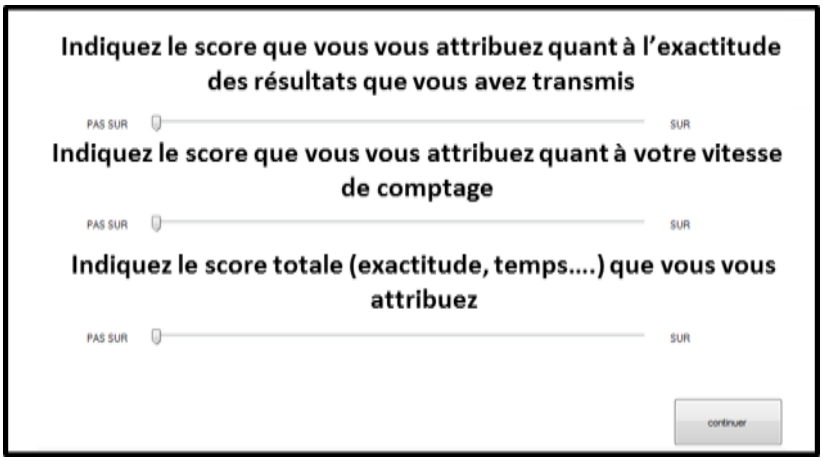


Figure 50 : Phase 3 de la pré-expérimentation.

Le participant devait faire bouger les 3 curseurs lui permettant d'évaluer sa performance sur ces 3 dimensions, ce qui activait le bouton de validation. Pour terminer la phase 3 le participant devait cliquer sur le bouton de validation permettant de passer en phase 4.

En phase 4 le participant se trouvait devant un affichage (*Cf.* Figure 51) sur lequel deux scores étaient indiqués. Le premier score était décrit comme correspondant à l'indice de performance « réel » du participant sur les 4 dernières images et le deuxième score était décrit comme correspondant à l'indice de performance obtenu sur un panel de participants ayant préalablement réalisé l'expérimentation. Ces deux indices de performance étaient en réalité fictifs et similaires pour tous les participants

- Pour les participants de la classe CS- l'indice de performance du participant était toujours en dessous de l'indice de performance obtenu par le panel (fictif) de participants ayant préalablement réalisé l'expérimentation ;
- Pour les participants de la classe CS+ l'indice de performance du participant était toujours au-dessus de l'indice de performance obtenu par le panel (fictif) de participants ayant préalablement réalisé l'expérimentation.

Cet écran permettait d'effectuer le renforcement. Pour pouvoir terminer la phase 4, le participant devait cliquer sur son propre indice de performance mais également sur l'indice de performance du panel de participant. Ceci amenait le participant à lire (et prendre en compte) ces 2 informations et activait le bouton de validation. Un clic sur le bouton de validation permettait au participant de retourner en phase 1. Cet enchainement de phases était réalisé 16 fois. Tous les participants ont eu les images ainsi que les indices de performance présentés en phase 4 tirés dans le même ordre.

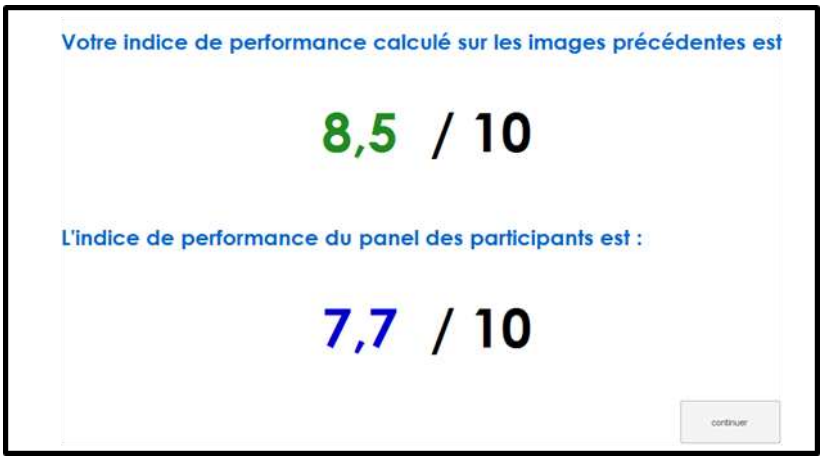


Figure 51 : Phase 4 de la pré expérimentation

Résultats

Afin de voir si le niveau de CS diminuait chez les participants de la classe CS- et augmentait chez les participants de la classe CS+, l'évolution au cours du temps des évaluations subjectives des participants a été étudiée. Pour cela, les droites d'évolution de l'évaluation subjective du bon comptage et de l'évaluation subjective de la performance globale (recueillies en phase 3) en fonction de la plage d'essais ont été tracées. Ici, une plage d'essais correspond à 4 images. Sur les deux courbes présentées ci-dessous, le premier point correspond à l'évaluation subjective (du bon comptage sur l'image de gauche et de la performance globale) des quatre premières images (première plage d'essais). Le deuxième point correspond à l'évaluation subjective (du bon comptage sur l'image de gauche et de la performance globale) des images cinq à huit (deuxième plage d'essais) et ainsi de suite.

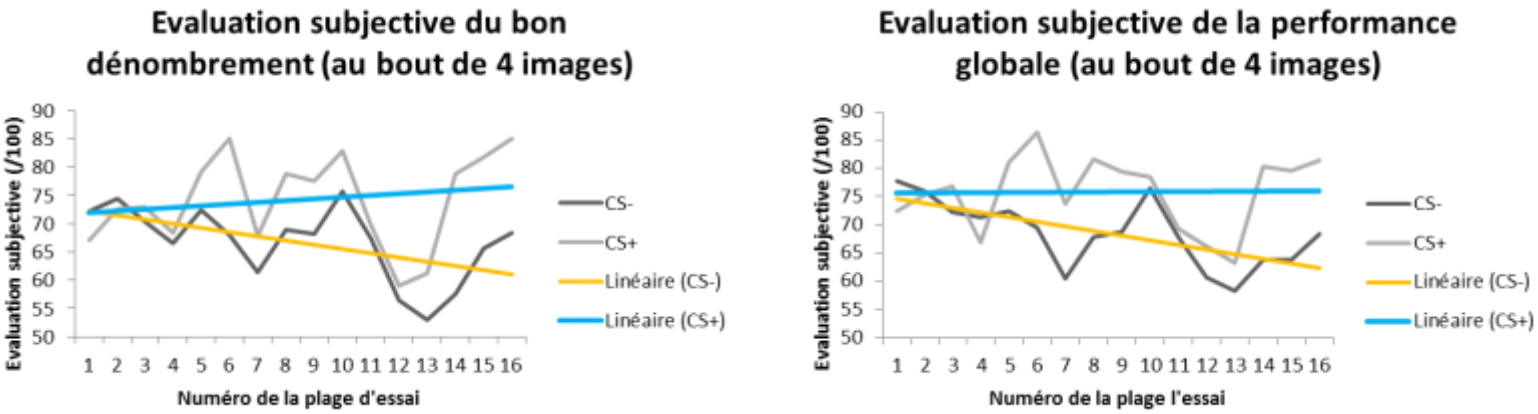


Figure 52 : Evaluation subjective effectuée par le participant de son score obtenu à la tâche de comptage et de sa performance finale.

La « Linéaire (CS-) » correspond à la tendance « globale » de la courbe de CS-. La « Linéaire (CS+) » correspond, quant à elle, à la tendance « globale » de la courbe de CS+.

Les droites d'évolution de l'évaluation subjective du bon comptage (*Cf.* Figure 52) montrent que les participants de la classe CS- ont bien une évaluation subjective décroissante au cours du temps. Parallèlement à cela, les participants de la classe CS+ semblent avoir une évaluation subjective croissante au cours du temps. Cette droite d'évolution n'est pas linéaire sur toutes les plages d'essais mais augmente ou diminue en fonction des plages d'essais. Cette non linéarité est due à la difficulté des images présentes dans les différentes plages d'essais. En effet, les images ont été tirées de manière pseudo-aléatoire, de fait, la difficulté (visibilité, netteté, contrastes…) des 4 images formant une plage d'essais n'a pas été contrôlée afin de ne pas biaiser cette pré-expérimentation. La droite d'évolution de l'évaluation subjective de la performance globale (*Cf.* Figure 52) suit les mêmes tracés que la droite portant sur l'évaluation subjective du bon comptage et montre une diminution (au cours du temps) de l'évaluation subjective des participants de la classe CS- et une augmentation chez les participants de la classe CS+.

Outre ces observations, une différence semble être présente entre les deux courbes CS+ et CS- au niveau de la première évaluation subjective. Une analyse en corrélation entre la première évaluation subjective de la performance globale et les résultats obtenus au questionnaire GSE indiquent une corrélation de 0.46 (p = .17). Ces résultats obtenus sur seulement 12 participants tendent à montrer une corrélation positive entre le niveau de GSE du participant et l'évaluation subjective qu'il s'attribue sur sa performance globale. Cette observation amène à préconiser une homogénéité des niveaux de GSE entre les classes de l'expérimentation finale afin que les niveaux initiaux d'évaluation subjective soient les plus similaires possibles.

Afin de ne pas surcharger les participants de l'expérimentation (ne pas les fatiguer au cours du calibrage en leur faisant compter trop d'images) un nombre de plage d'essais a été déterminé de manière à ce qu'il ne soit pas trop grand mais qui permette également de créer une différenciation entre les classes CS+ et CS-. Visuellement (*Cf.* Figure 53), la différence semble commencer à être mise en place à la cinquième plage d'essais (ligne rouge sur la figure 53) et évoluer (ou du moins ne pas fortement diminuer) jusqu'à la huitième plage d'essais. Le choix s'est donc porté sur les plages d'essais comprises dans l'intervalle allant de la cinquième à la huitième.

Dans cet intervalle, le choix le plus évident correspondait à celui de la plage 6 (représentée avec une ligne violette en pointillé sur la figure 53). En effet, c'est au niveau de cette plage que les valeurs des groupes CS- et des groupes CS+ semblent être les plus éloignées. Cependant, les évaluations subjectives des participants de la classe CS+ semblent fortement augmenter entre la cinquième et la sixième plage d'essais et semblent diminuer chez les participants de la classe CS- alors que les tendances sont parallèles à tous les autres points de l'intervalle. Ces observations indiquent que des images entre la plage 5 et 6 sont potentiellement ambigües et que ce qui est observé ici est potentiellement due à la faible population (6 participants par classe de CS). Les plages 7 et 8 n'ont pas été choisies car le nombre d'image à compter (respectivement 28 et 32) semblait être trop important. Par conséquent, la plage 5 a été choisi pour le calibrage de l'expérimentation car cette plage 5 (tracée en rouge sur la figure 53) répond aux attentes recherchées (calibrage pas trop long mais permettant de discrétiser les classes de CS).

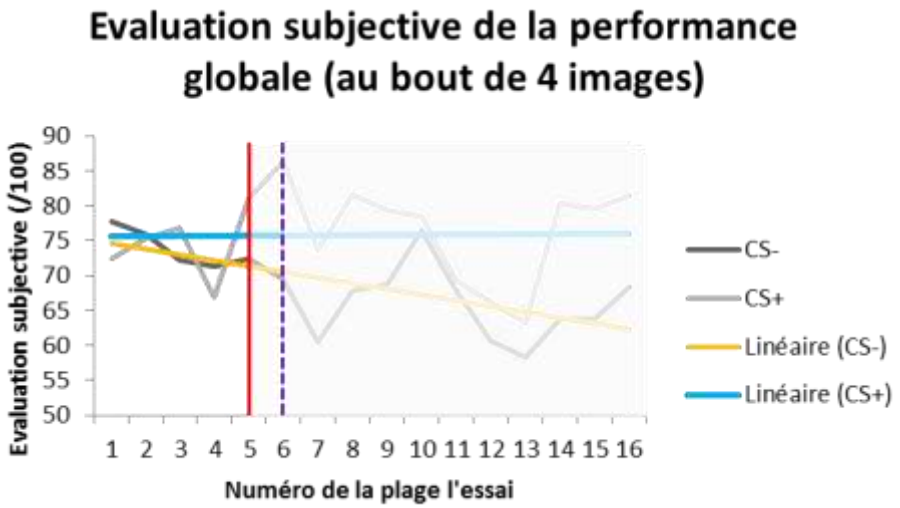


Figure 53 : Choix du nombre de plages d'essais pour l'expérimentation finale.

B. Déroulé de l'expérimentation 3

Le calibrage ayant été testé et validé, la phase d'expérimentation proprement dite a pu se dérouler en 3 parties distinctes :

- Une partie portant sur le recueil du consentement et des réponses aux différents questionnaires (partie 1) ;
- Une partie portant sur la présentation de l'expérimentation et la mise en place du calibrage (partie 2) ;
- Une partie portant sur l'expérimentation (partie 3) ;
- Une partie explicative (partie 4).

La partie 1 a été réalisée en amont de l'expérimentation. 2 semaines avant l'expérimentation un mail a été envoyé à 71 élèves de deuxième année d'école d'ingénieur (Ecole Nationale Supérieure de Cognitique). En pièce jointe de ce mail, les élèves pouvaient trouver une description de l'expérimentation, une feuille de consentement à retourner signée et les différents questionnaires vus précédemment (ces différents documents sont présentés en annexe 4). Sur les 71 mails envoyés, 45 réponses positives ont été reçus afin de passer l'expérimentation.

Pour la deuxième partie les élèves étaient regroupés en 3 groupes de travaux dirigés. Dans chaque groupe une partie des élèves participaient à l'expérimentation (ces élèves avaient renvoyé leur consentement éclairé signé) et une partie des élèves n'y participaient pas conformément à leur souhait. Le calibrage, ainsi que l'expérimentation, n'étaient passé que par les élèves qui avaient donné leur consentement. Avant de commencer le calibrage, les participants étaient aléatoirement distribués dans 2 salles de classe différentes afin de donner « l'illusion » aux participants que l'expérimentation se déroulerait en collaboration avec les individus présents dans l'autre salle et afin

d'éviter que des participants puissent voir les écrans d'autres participants (les données vues durant le calibrage étant similaires pour tous les participants d'une même classe de CS).

Après le calibrage les participants passaient à la phase d'expérimentation. Cette dernière était basée sur le protocole expérimental décrit au chapitre 4, mais était découpée en 28 essais réussis (14 en CI élevée et 14 en CI faible). Enfin, à la fin de l'expérimentation, les participants devaient attendre que tous les participants aient fini afin de pouvoir sortir de la salle et de partir en pause de 10 minutes. Au retour de la pause le protocole expérimental (variable dépendante et variable indépendante, calibrage, conditions de passage) ainsi que le cadre théorique étaient présentés.

C. Participants

En raison d'un problème informatique ayant empêché, pour 10 personnes, la passation de l'expérimentation, seul 35 personnes (46% de femmes et 54% d'hommes) d'âge moyen 22.8 ans (SD = 1.15) ont participé à cette étude. Tous les participants étaient des élèves de deuxième année d'école d'ingénieur soit une catégorie d'opérateurs potentiels de la RCPair. Aucun participant n'avait de problème de santé, tous avaient une vision normale ou corrigée.

D. Résultats

Les données de 35 participants sont incluses dans l'Analyse. Les résultats finaux (testant l'hypothèse 12) de cette expérimentation étant directement dépendant de la vérification d'un grand nombre de résultats préalables, pour cette partie, il a été choisi de décrire, dans son intégralité, la démarche statistique utilisée.

a. Pré analyse

Avant d'étudier les résultats expérimentaux, une analyse des données du calibrage a été effectuée afin de vérifier que deux classes distinctes de CS ont bien été créées avec une population a priori homogène.

b. Analyse des questionnaires

Agrégation des données et analyse descriptive

Comme vu précédemment, préalablement à l'expérimentation les étudiants ont rempli un questionnaire de 13 questions successives, divisées en deux classes différentes :

- la classe *propensity to trust*
- la classe *self esteem variability*

La classe *propensity to trust* (PT) est formée de 8 items tirés du questionnaire créé par Mayer et Davis en 1999 (Mayer & Davis, 1999). Comme vu précédemment, dans la littérature, la PT ou propension individuelle à faire confiance est une caractéristique propre au confiant. Dans cette

étude, une mesure *a priori* de la PT permet de vérifier a posteriori que les différentes classes de CS+ et CS- sont formées de groupes ayant une homogénéité de PT. En cas d'hétérogénéité des groupes les observations recueillies lors de l'expérimentation pourraient dépendre du niveau de confiance de base attribués par les individus et non pas du niveau de confiance en soi induit par les expérimentateurs.

Le classe *self esteem variability (*SEV) est quant à elle formée des 5 Items créés par Rosenberg en 1965 qui correspondent à une mesure relativement fiable de la variation, au cours du temps, de l'estime de soi d'un individu (Webster et al., 2017). Ainsi, plus la mesure de SEV se rapproche de 0, plus l'estime de soi de la personne est stable dans le temps. A contrario, plus la SEV se rapproche de 3 plus le niveau d'estime de soi de la personne varie dans le temps. De manière similaire à la mesure de PT, une homogénéité des niveaux de SEV à l'intérieur des différentes classes de CS+ et CS- pourrait être considérée comme étant un biais expérimental. En effet, placer tous les participants ayant une SEV proche de 3 dans la classe CS- permettrait à l'expérimentateur d'avoir une plus grande maitrise sur le calibrage mais diminuerait nécessairement la normalité des distributions, et, par conséquent, modifierait « artificiellement » les résultats statistiques.

Afin d'obtenir, pour chaque participant, une seule mesure de PT et de SEV la moyenne des réponses à toutes les questions doit être calculée. Cependant, avant d'agréger les données il était nécessaire de s'assurer que toutes les questions correspondaient bien à une mesure de leur classe respective. Pour ce faire, une ICC(2k) (Koo & Li, 2016) ainsi qu'une mesure de la fiabilité (coefficient alpha de Cronbach) (Tavakol & Dennick, 2011) ont été réalisées sur les Items de chaque classe. L'ICC(2k) a été utilisée pour l'analyse de la corrélation car :

- Les questions avaient été sélectionnées aléatoirement parmi une large population de questions (plusieurs questionnaires existent pour chaque mesure étudiée ici).
- La moyenne des réponses aux différentes questions devrait être calculée pour chaque sujet.
- Toutes les questions étaient intéressantes.

Pour la classe PT les résultats indiquent une ICC(2k) de .52 et un Alpha de Cronbach de .55. Ces mesures relativement faibles peuvent s'expliquer relativement facilement. En effet, le questionnaire est en Anglais et les items sont relativement difficiles à comprendre. Pour cette classe de francophones au niveau d'Anglais hétérogène, cela a pu entrainer un biais de compréhension sur certaines questions et ainsi faire baisser la valeur du coefficient Alpha. Cependant, l'agrégation des questions dans cette classe n'a pour seul intérêt que de vérifier l'homogénéité des groupes CS- et CS+. De ce fait les mesures de l'ICC et de alpha étant supérieures à 0.50, l'agrégation est considérée comme étant acceptable.

Les mesures sont ensuite réalisées sur la classe SEV. Dans cette classe, les résultats indiquent une ICC(2k) de .67 et un Alpha de Cronbach de .72. La mesure de l'ICC reste relativement faible (mais acceptable), ce qui peut être causé par les mêmes problèmes que précédemment, ou encore par le faible nombre d'items présents dans cette classe. Cependant, les résultats de l'Alpha de Cronbach permettent de valider l'agrégation des données.

Du fait des mesures de l'ICC(2k) et du Alpha obtenus pour les deux classes, l'agrégation des data est réalisée. Celle-ci permet d'obtenir, pour chaque participant, une seule mesure de PT et de SEV. Ces différentes mesures sont, dans un second temps regroupées dans les groupes de CS- et CS+ attribués aux participants. Les statistiques descriptives, pour chaque mesure et chaque groupe sont présentées dans le tableau 23**.**

Tableau 23 : Statistiques descriptives des réponses aux différents questionnaires (VD) en fonction de la classe de CS attribuée

Variable dépendante	Classe attribuée	Min	Max	Moyenne	Médiane	Ecart Type
PT	CS-	2.25	3.62	2.90	2.87	.44
	CS+	1.75	3.62	2.66	2.87	.47
SEV	CS-	.80	2.60	1.42	1.20	.56
	CS+	.40	2.20	1.36	1.36	.54

Une analyse purement descriptive de ces résultats ne permet pas de voir apparaitre une différence entre les deux classes de CS. En effet, que ce soit au niveau de la PT ou de la SEV les moyennes et écart-types correspondants dans chaque classe semblent être relativement proches (*cf.* Tableau 23**)**.

Afin de valider ou non les observations recueillies en statistiques descriptives, une analyse est menée en statistiques inférentielles. Dans un premier temps, pour les données de PT et de SEV dans chaque classe de CS, la normalité et l'égalité des variances sont testées respectivement avec un test de Shapiro-Wilk et un test de Fisher. Un test de Student est ensuite réalisé pour les données normales,

Statistiques inférentielles

Dans cette partie seront détaillées les statistiques inférentielles effectuées sur les données de PT et de SEV. L'étude en statistiques inférentielles se déroule en 3 tests distincts. Le premier test permet de vérifier que les deux classes de CS+ et de CS- ont des données normalement réparties. Le deuxième test permet d'observer si les variances des deux groupes sont présentes. Enfin, le troisième test, qui se base sur les résultats des deux premiers, permet de comparer les moyennes obtenues dans les classes de CS+ et de CS-. C'est les résultats du dernier tests qui permettent de conclure que les moyennes des deux classes sont, ou non, significativement différentes.

Statistiques inférentielles pour les données de PT

Le test de normalité de PT pour les classes CS- et CS+ donne des p-value de .40 et .15. Ces p-value largement supérieures au seuil de significativité fixé (5% dans ce document) ne permettent pas de rejeter l'hypothèse nulle de normalité. Le test d'égalité des variances indique un ratio des variances de .85. Ce ratio proche de 1 indique une probable égalité des variances qui est confirmée par une p-value de .74 qui ne permet pas de rejeter l'hypothèse nulle d'égalité des variances.

Les données de PT étant normales dans les deux classes et ayant des variances égales un test de Student est réalisé afin de tester si les moyennes sont, ou non, significativement différentes. Les

résultats du test de Student donne un intervalle de confiance compris entre -.07 et .55. Cet intervalle de confiance semble relativement vaste pour des données comprises entre 1 et 5 et plutôt axé vers des valeurs positives. Cependant, la p-value de .13 ne permet pas de rejeter l'Hypothèse indiquant que la différence des moyennes est égale à 0.

Pour conclure les données de PT sont normalement distribuées dans les deux classes et rien ne permet d'indiquer qu'une des deux classes ait un niveau de PT différent de l'autre. En d'autre termes, rien ne permet d'indiquer que les individus des classes CS+ et CS- aient des caractéristiques différentes vis-à-vis de PT.

Statistiques inférentielles pour les données de SEV

Le test de normalité de SEV pour les classes CS- et CS+ donne des p-value de .05 et .32. La p-value de la classe CS+, largement supérieure au seuil de significativité de 5%, ne permet pas de rejeter l'hypothèse nulle de normalité. Bien qu'étant légèrement supérieure à 5%, la p-value de la classe CS- ne permet pas de rejeter « directement » l'hypothèse nulle de normalité. La visualisation d'un histogramme et d'un graphique d'estimation de densité permet d'essayer de comprendre la p-value de la classe CS-.

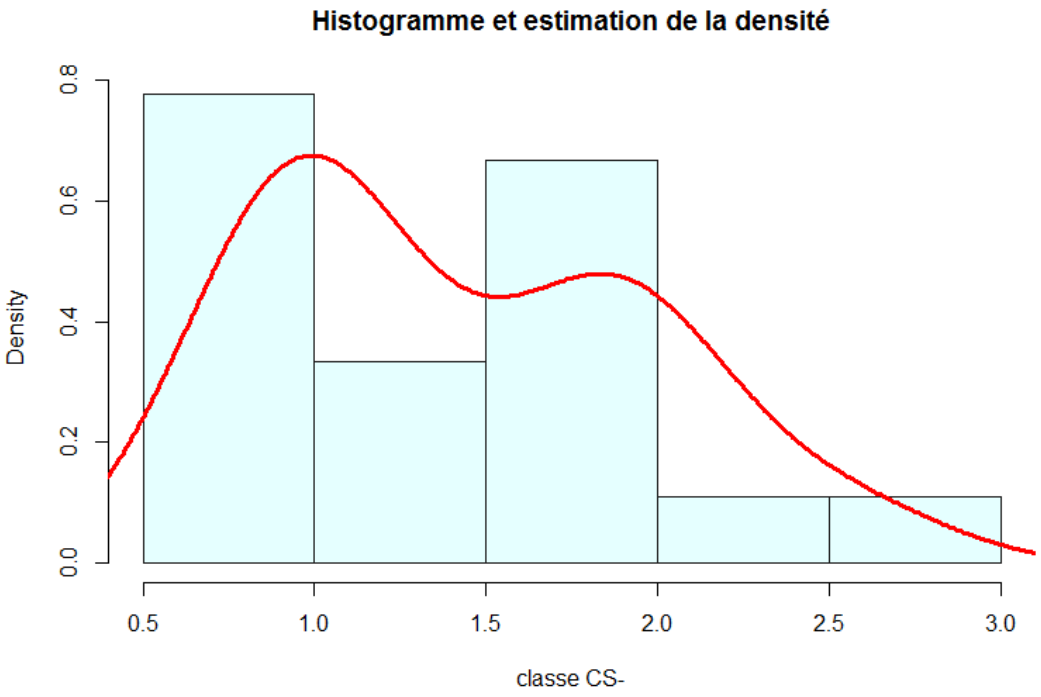


Figure 54 : Histogramme et graphique d'estimations de densité pour la classe CS-

Le graphique présenté à la figure 54 montre que les données ne semblent pas suivre une loi normale. En effet, les queues de distributions ne sont pas symétriques et la « cloche » semble être très aplatie avec une absence de données entre 1.0 et 1.5. Pour vérifier ces observations le coefficient Kurtosis est calculé afin d'évaluer la dispersion des valeurs par rapport à une loi normale. Le coefficient

Kurtosis calculé pour les données de CS- est de -1.16 ce qui équivaut à une distribution platykurtique. Du fait de ces observations, la classe CS- peut être considérée comme n'ayant pas une distribution normale. Le test d'égalité des variances donne un ratio des variances de 1.09. Ce ratio très proche de 1 indique une forte probabilité d'égalité des variances qui est confirmée par une p-value de .85 qui ne permet pas de rejeter l'hypothèse nulle d'égalité des variances.

Les données de SEV étant, au sens de Shapiro, normales dans les deux classes et ayant des variances égales, un test de Student a été réalisé afin de tester si les moyennes étaient, ou non, significativement différentes. Les résultats du test de Student donne un intervalle de confiance compris entre -.31 et .34. Cet intervalle de confiance semble relativement bien centré sur 0 ce qui tend à montrer qu'il n'y a pas de différence entre les moyennes, la p-value de .75 confirme cette information et ne permet pas de rejeter l'Hypothèse indiquant que la différence des moyennes est égale à 0. Comme les données de la classe CS- ne semblent pas (du moins visuellement) suivre une loi normale un test non paramétrique de Wilcoxon est utilisé pour confirmer ou infirmer ces résultats. Avec une p-value de .81 le test de Wilcoxon ne permet pas de rejeter l'Hypothèse indiquant que la différence des moyennes est égale à 0.

Pour conclure les données de SEV ne sont pas normalement distribuées dans les deux classes. Les tests paramétriques et non paramétriques ne permettent pas d'indiquer qu'une des deux classes ait un niveau de SEV différent de l'autre. En d'autre termes, rien ne permet d'indiquer que les individus des classes CS+ et CS- aient des caractéristiques différentes vis-à-vis de SEV.

Conclusion sur les questionnaires

L'analyse des données des deux questionnaires permet d'obtenir, pour chaque participant, une mesure quantitative de leur PT et de leur SEV. En regroupant les données des participants dans les mêmes classes (CS- et CS+) où ils ont été dans l'expérimentation, on constate que les classes de l'expérimentation sont homogènes tant au niveau de la PT que de la SEV. Ainsi, au démarrage de l'expérimentation on peut considérer que les caractéristiques propres aux participants de chaque classes (CS+ et CS-), que ce soit sur leur tendance naturelle à faire confiance ou sur leur faculté à remettre en cause cette confiance, sont similaires et ne devraient pas introduire de biais.

Ayant un nombre impair de participants, la classe CS- est constituée d'un participant de plus que la classe CS+. En pré expérimentation une forte corrélation a été détectée entre la diminution de la valeur de SEV et la diminution du niveau de CS ; de fait, si dans la classe CS- un participant est catégorisé comme n'ayant pas subi de diminution du niveau de CS et que, dans le même temps sa valeur de SEV est proche de 0 alors il pourra être sorti de l'ensemble des résultats afin d'équilibrer les deux classes (ceci n'a cependant pas été fait).

c. Analyse du calibrage

Avant de regarder si une différence de stratégie vis-à-vis de la CI existe entre les classes CS- et CS+ il est fondamental de vérifier que le niveau de CS a bien baissé pour les participants de la classe CS- et est bien resté stable ou a augmenté pour les participants de la classe CS+. En effet, les deux classes

étant homogènes en termes de PT, si le niveau final de CS est similaire dans les différentes classes, aucun résultat ne pourrait être expliqué et par conséquent l'analyse statistique serait inutile.

Au bout de 4 essais terminés le participant évalue, à l'aide d'une échelle, le score qu'il s'attribue (en termes de vitesse de comptage et d'exactitude des scores) sur les 4 dernières images. Cette mesure est répétée 5 fois lors du calibrage (constitué de 24 images). La première échelle de mesure (EM1) correspond au niveau initial de CS du participant. La cinquième échelle de mesure (EM5) correspond au niveau final de CS. La variation du niveau de CS induit par le calibrage (VCS) correspond à « EM5-EM1 ».

Avant de commencer les analyses portant sur la différence de moyenne du VCS il est nécessaire d'analyser, pour chaque classe, l'évolution des EM au cours du temps. Comme le montre la figure 53, le niveau initial de CS semble être similaire entre les membres des deux classes. Cependant ce niveau semble diminuer rapidement pour la classe CS- et rester relativement stable pour la classe CS+, ce qui correspond bien à l'effet recherché (*Cf.* Figure 55).

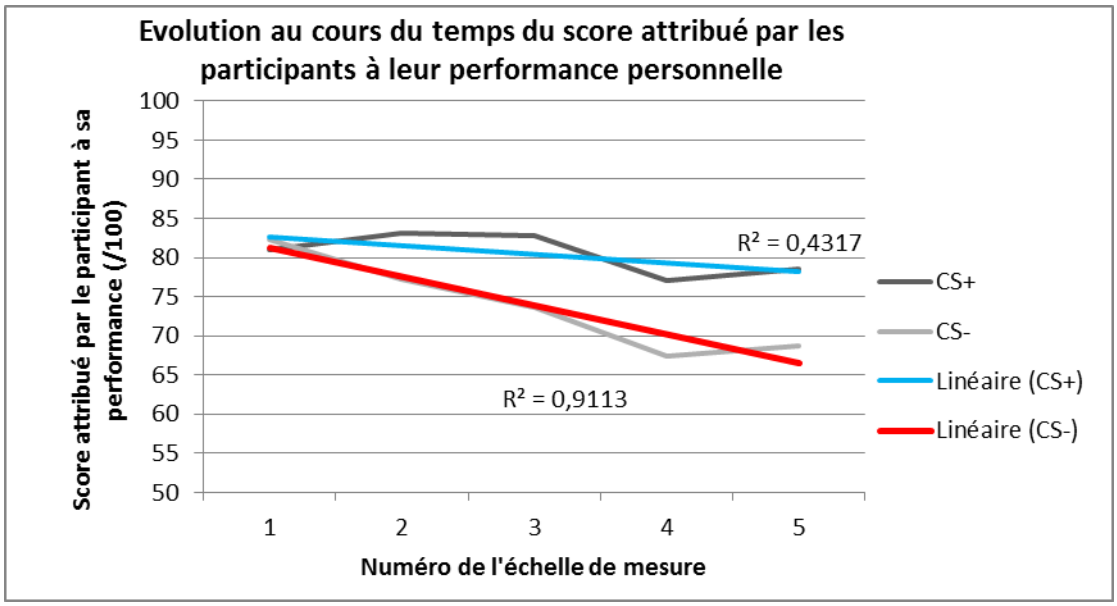


Figure 55 : Evolution au cours du temps du niveau de confiance en soi du participant.
L'approximation linéaire de CS+ est légèrement décroissante mais les données ne collent qu'à 43% à la droite. Ceci est probablement dû aux images présentées entre les échelles 4 et 5 qui devaient être différentes, en terme de complexité, à celles présentées lors des 3 premières échelles.

Analyse du niveau initial de CS

Afin de s'assurer qu'une possible variation du niveau de VCS résulte du calibrage, il est nécessaire, de vérifier en premier lieu que le niveau initial de CS entre tous les participants soit similaire. Une analyse statistique est effectuée sur les données de la première mesure de CS en regroupant ces dernières en fonction dans les classes (CS- et CS+) correspondantes. Les statistiques descriptives de chaque niveau initial de CS sont présentées dans le tableau 24.

Tableau 24 : Statistiques descriptives du niveau initial de confiance des participants de chaque classe de CS attribuée

Variable dépendante	Classe attribuée	Min	Max	Moyenne	Médiane	Ecart Type
CS init	CS-	45	100	78.39	78.50	17.92
	CS+	38	100	76.59	78	15.71

Comme le montre les résultats présentés dans le tableau 24, les deux classes semblent avoir un niveau de CS initial de moyenne très proche. Bien que la classe CS+ semble avoir une étendue légèrement supérieure à la classe CS-, l'écart type plus faible de cette classe incite à penser que la valeur minimum de cette classe est anormale. Une analyse de la représentation des données (*cf.* Figure 56) sous forme de boite de Tukey corrobore ces observations. Ainsi, la figure 56 montre que la variabilité des données est relativement similaire entre les 2 classes. De plus, comme envisagée grâce à l'étude de l'étendue et des écarts type, le minimum de la classe CS+ (le carré rouge sur la boite CS+) correspond à une valeur n'appartenant pas au premier quartile.

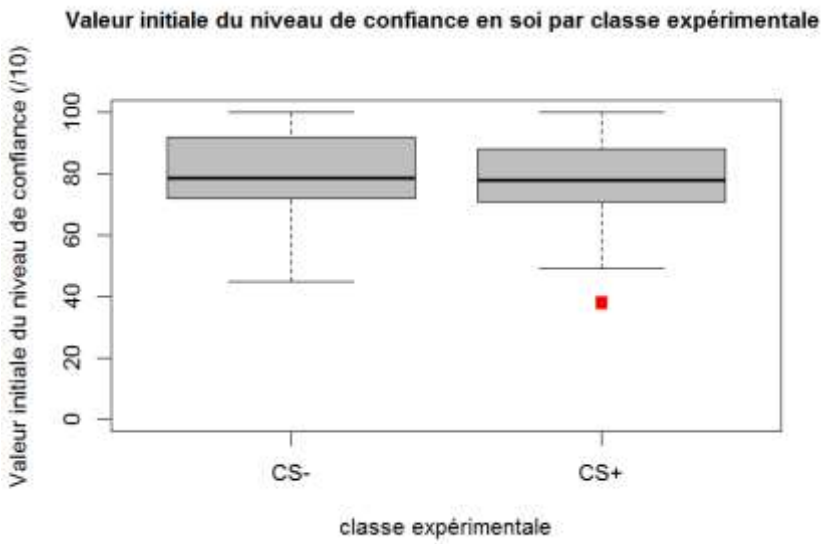


Figure 56 : Boites de Tukey pour les valeurs initiales du niveau de CS pour chaque classe expérimentales.

Afin de de confirmer ou non ces interprétations, des calculs de statistiques inférentielles sont effectués. En premier lieu, la normalité des classes CS- et CS+ est vérifiée à l'aide d'un test de Shapiro dont les p-value respectivement de .12 et .17 ne permettent pas de rejeter l'hypothèse nulle de normalité. Un test d'égalité des variances est ensuite effectué avec un test de Fisher. Avec une p-value de .60 il n'est pas possible de rejeter l'hypothèse nulle d'égalité des variances. Sur la base de ces vérifications préalables, un test de Student est effectué sur ces données. Comme présentées dans le tableau 24 les sorties du test de Student indiquent que les moyennes des deux classes sont relativement proches. De plus, l'intervalle de confiance à 95% (-9.82 à 13.42) est bien centré sur 0 ce qui montre qu'il est peu probable que les moyennes des deux groupes soient significativement différentes. Ceci est confirmé par la p-value de .75 qui ne permet pas de rejeter l'hypothèse nulle d'égalité des moyennes.

L'analyse des données montre donc que le niveau initial de CS des participants est relativement similaire dans les deux classes. De fait, si par la suite une différence significative est trouvée sur les données du VCS en faveur de la classe CS+ (VCS CS- < VCS CS+), il sera possible de conclure que le calibrage a bien fonctionné et que, par conséquent, les participants des classe CS- ont vu leur niveau de CS diminuer. Si par contre une différence significative n'est pas trouvée entre les deux classes ou si une différence significative est trouvée en faveur de la classe CS+, les données seront inexploitables (il est à noter que le cas VCS CS- > VCS CS+ serait très difficilement explicable).

Analyse de la variation du niveau de VCS

Dans un premier temps une étude descriptive du VCS est effectuée. Les résultats présentés dans le tableau 25 indiquent que les moyennes des deux classes semblent relativement éloignées (CS- = -13.67 et CS+ = -1.8). La moyenne et la médiane de CS+ supérieures à 0 reflètent bien l'homogénéité de cette classe. En effet, comme vu précédemment dans l'analyse des questionnaires, les participants présents dans cette classe n'ont pas tous les mêmes niveaux de SEV. De fait, certains participants ont pu être influencés par des facteurs externes (le fait d'être observé, d'être en période d'examen dans une salle de classe…) qui ont pu faire baisser, au cours du temps, leur estime de soi sur la tâche.

Tableau 25 Statistiques descriptives de la variation du niveau de confiance en soi des participants de chaque classe de CS attribuée

Variable dépendante	Classe attribuée	Min	Max	Moyenne	Médiane	Ecart Type
VCS	CS-	-62	13	-13.67	-9	13
	CS+	-38	22	-1.8	3	22

Une analyse des boites de Tukey présentées à la figure 57 (les limites sur l'axe y sont volontairement placées entre -45 et 25 afin de mieux percevoir la variabilité) confirment les observations précédentes.

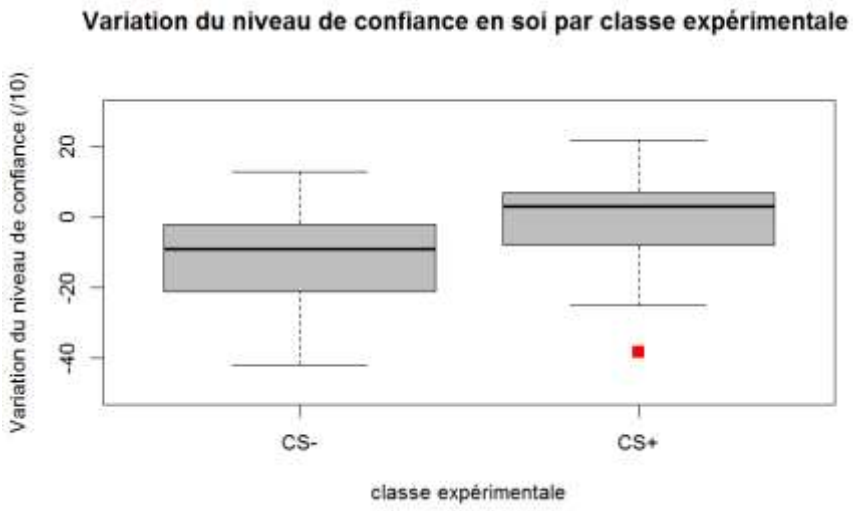


Figure 57 : Boites de Tukey pour la variation du niveau de CS pour chaque classe expérimentales

Comme précédemment, afin de vérifier ces interprétations en statistiques inférentielles la normalité de chaque classe ainsi que l'homogénéité des variances sont préalablement vérifiées avec un test de Shapiro et un test de Fisher. Les tests de Shapiro confirment la normalité des deux classes avec des p-value respectives pour les classes CS- et CS+ de .08 et .38. Avec une p-value de .48 le test de Fisher ne permet pas de rejeter l'hypothèse nulle d'homogénéité des variances.

Etant donné qu'une différence significative est attendue entre les deux classes dans le sens d'une moyenne significativement plus faible pour la classe CS- le test de Student est légèrement modifié afin de chercher la différence dans ce sens-là. L'analyse des résultats du t-test montre un intervalle de confiance allant de – l'infini à -1.92. La borne supérieure de cet intervalle de confiance proche de -2 est probablement due aux valeurs extrêmes de la classe CS+, mais étant donné que cette borne est largement inférieure à 0, une différence entre les moyennes des deux classes doit probablement exister. La p-value de .025 confirme cette information et permet de rejeter l'hypothèse nulle d'égalité des moyennes. Ainsi, il est possible de conclure que la moyenne de CS de la classe CS- est statistiquement inférieure à la moyenne de CS de la classe CS+.

Conclusion des pré-analyses

Cette pré-analyse a permis de vérifier l'homogénéité des groupes ainsi que le bon fonctionnement du calibrage. Comme indiqué dans l'analyse des questionnaires, les deux classes expérimentales (CS- et CS+) sont constituées de participants ayant un niveau de PT et de SEV équivalent. Cela tend à montrer que l'attribution de participants dans chaque classe a été tirée au hasard. Une fois cela effectué l'homogénéité des classes a été statistiquement vérifiée en terme de niveau initial de CS afin d'assurer qu'une différence dans la variation du niveau de CS soit majoritairement due au processus d'induction et non à des facteurs internes à l'individu. Enfin, l'étude de la variation au cours du temps du niveau de CS indique que les participants de la classe CS- ont une variation du niveau de CS statistiquement plus importante que les participants de la classe CS+. Ces résultats pris ensemble montrent que le calibrage a bien fonctionné et que l'expérimentation s'est bien déroulée avec deux classes statistiquement différentes.

d. Analyse des données expérimentales

Niveau de certitude dans la réponse du coéquipier

Dans cette étude, comme dans les études précédentes, l'évaluation du niveau de certitude dans la réponse du partenaire est exploitée comme information sur le niveau de confiance qu'a le participant dans son coéquipier. Afin de vérifier que le matériel d'induction a bien fonctionné sur les participants et valider une partie de l'hypothèse, différentes observations doivent être effectuées sur cette variable dépendante :

- La présence d'un effet simple entre les niveaux de certitude attribués aux coéquipiers en C+ et en C-
- L'absence d'effet d'interaction

Un effet simple du niveau de confiance sans interaction entre niveau de confiance et niveau de CS tendrait à montrer que le niveau de confiance perçu est bien différent selon le coéquipier (C+ et C-) et que cette différence n'est pas dépendante du niveau de CS. En d'autres termes, un effet simple sans interaction indiquerait que quel que soit le niveau de CS, le niveau de certitude dans la réponse du coéquipier est différent lorsque le coéquipier est en C+ ou en C-. Ceci rejoindrait les résultats trouvés dans l'expérimentation portant sur l'influence des caractéristiques psychosociales du confiant. Pour rappel, dans cette expérimentation, les résultats avaient montré pour tous les groupes sociaux comparés, un effet simple du niveau de confiance et une absence d'effet d'interaction.

Tableau 26 : Statistiques descriptives pour le niveau de certitude dans la réponse du coéquipier, toute classe de CS confondues puis pour les classes CS- et CS+

Variable dépendante	Classe attribuée	Confiance induit	Min	Max	Moyenne	Médiane	Ecart Type
Niveau de certitude dans la réponse du partenaire		C+	2.12	9.57	6.79	6.95	1.76
		C-	1.19	9.46	6.09	6.47	1.84
	CS-	C+	2.12	8.53	6.18	6.62	1.76
		C-	1.19	7.86	5.69	6.37	1.86
	CS+	C+	3.86	9.57	7.45	7.80	1.56
		C-	3.96	9.46	6.50	6.50	1.77

Comme le montrent les résultats présentés dans le tableau 26, globalement (classes CS- et Cs+ confondues), les participants ont un niveau moyen de certitude plus important lorsqu'ils travaillent avec un partenaire de la catégorie C+ plutôt qu'avec un partenaire de la catégorie C-. Les écart-types relativement proches ainsi que la médiane supérieure pour la catégorie C+ laissent penser qu'une différence de moyennes existe entre les deux catégories. En tenant compte de la classe attribuée, ces observations perdurent même si l'écart entre les catégories semble plus grand pour la classe CS+. Cette deuxième analyse suggère que le niveau de certitude perçu est plus grand en C+ qu'en C-, et ce, quelle que soit la classe attribuée au participant.

Afin de vérifier statistiquement ces résultats, une ANOVA à mesures répétées et un test de Shapiro sont réalisés. Les résultats de l'ANOVA indiquent un effet simple, $F(1,33) = 22.06$, $p < .001$*** du niveau de confiance induit et aucun effet d'interaction, $F(1,33) = 2.36$, $p = .13$. Cependant les résultats du test de Shapiro ($p = .04$) ne permettent pas de valider ces observations. Comme le montre le graphe des résidus présentés à la figure 58 certaines valeurs dont celles provenant des lignes 59 et 14 (sous le « 59 » sur la figure 58) semblent être très différentes des autres. En ne tenant pas compte de ces données (*Cf.* Figure 58), un effet simple est toujours présent, $F(1,31) = 23.88$, $P < .001$***, l'effet d'interaction est toujours non significatif, $F(1,31) = 1.76$, $p = .19$ et le test de Shapiro indique une p-value de .58, confirmant la normalité. Sur ces données, le ηp^2 de l'effet simple est de .43 ce qui indique qu'une grande proportion de la variance de la perception de la réussite du coéquipier est expliquée par le niveau de confiance.

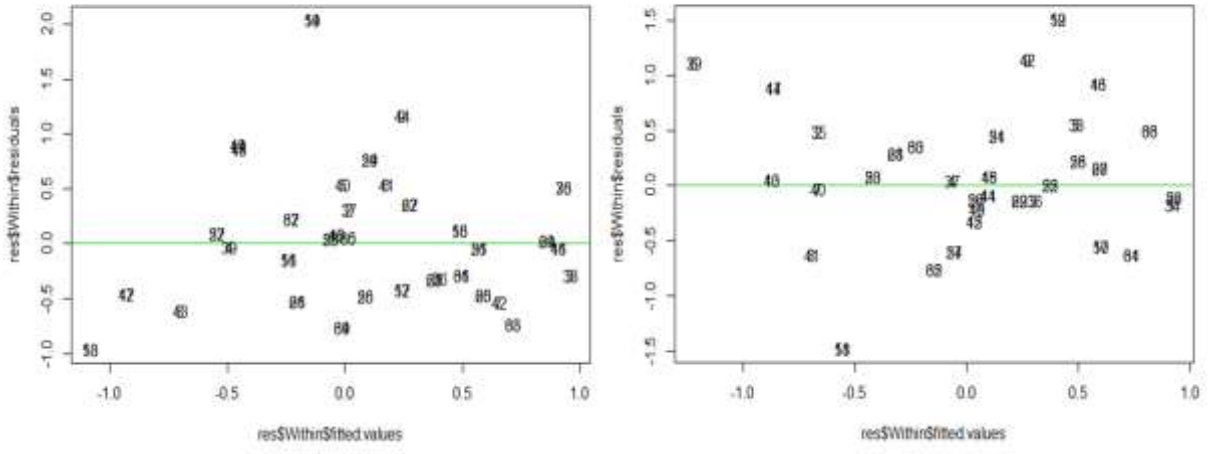


Figure 58 : Répartition des résidus pour les données complètes (à gauche) et pour les données modifiées à droite (en enlevant les lignes 59 et 14)

Analyses comportementales

Afin de valider l'hypothèse 12, les variables comportementales similaires à celles utilisées dans l'expérimentation portant sur les caractéristiques psychosociales ont été analysées à savoir :

- le pourcentage de supervision
- le pourcentage de temps utilisé pour réaliser les taches
- le pourcentage de modifications

Analyse du pourcentage de supervisions

La première variable comportementale à analyser correspond au pourcentage de supervisions. Dans l'expérimentation portant sur les caractéristiques psychosociales, il a été vu que cette variable n'était pas obligatoirement modulée par le niveau de CI présent dans la relation (par exemple, pour la catégorie sociale mécaniciens, rien n'indique que les pourcentages de supervisions soient différents en fonction du niveau de confiance présent dans la relation). Ainsi, dans le cas où un effet simple serait présent sur cette variable, si, comme le propose l'hypothèse, le niveau de CS est un médiateur de l'action réalisée dans une réalisation de confiance, alors un effet d'interaction devrait également être présent.

Les résultats présentés dans le tableau 27 tendent à montrer une différence de moyenne entre la catégorie C+ et C- (72.28 < 76.18). Cependant, la médiane identique entre ces deux catégories et l'écart type supérieure de C+ par rapport à C- suggèrent que cette différence de moyenne n'est probablement due qu'à la dispersion des données. Ces observations (M(C+<C-) et SD(C+>C-)) se retrouvent également pour les deux classes de CS. La figure 59 corrobore ces observations et montre

visuellement que la différence entre CS+ et CS- semble être un peu plus grande dans la classe CS+ mais que la dispersion des données est importante.

Tableau 27 : Statistiques descriptives pour le pourcentage de supervisions, toute classe de CS confondues puis pour les classes CS- et CS+

Variable dépendante	Classe attribuée	Confiance induit	Min	Max	Moyenne	Médiane	Ecart Type
Pourcentage de supervisions (%)		C+	0	100	72.28	85.72	31.74
		C-	0	100	76.18	85.72	27.94
	CS-	C+	0	100	70.41	84.04	32.08
		C-	7.15	100	71.65	78.18	27.24
	CS+	C+	0	100	74.27	85.12	32.24
		C-	0	100	80.97	93.34	28.68

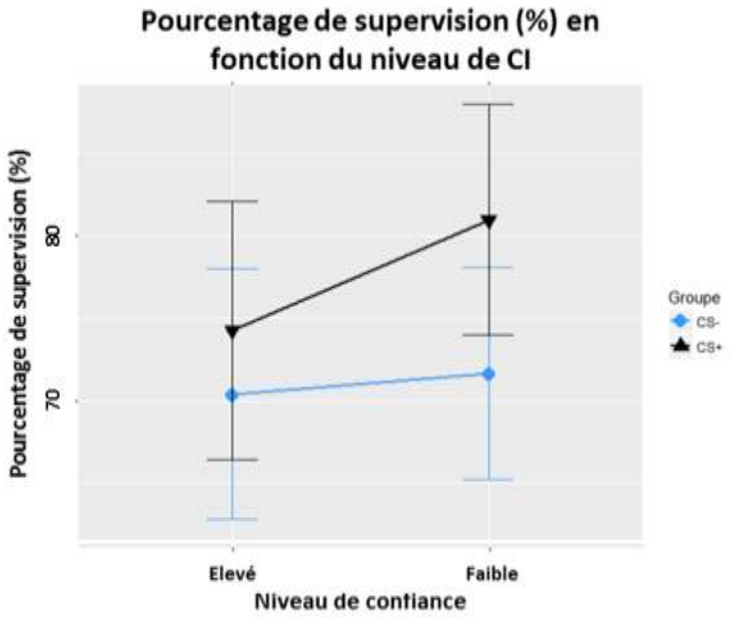


Figure 59 : Pourcentage de supervisions en fonction du niveau de confiance induit pour les classes CS+ et CS-

Comme attendu, les résultats en statistiques inférentielles n'indiquent pas d'effet d'interaction, $F(1,33) = 1.06$, $p = .31$ ni d'effet simple du niveau de confiance, $F(1,33) = 2.16$, $p = .15$ tout en montrant une normalité des résidus ($p = .64$). Analysés ensemble, ces résultats permettent de dire que rien n'indique que les élèves en deuxième année d'école d'ingénieur ont un comportement de supervision dépendant du niveau de CI présent dans la relation.

Pourcentage de temps utilisé

La deuxième variable comportementale à analyser correspond au pourcentage de temps total pris par le participant pour réaliser sa tâche de comptage ainsi que la tâche de supervision de son coéquipier. Dans l'expérimentation portant sur les caractéristiques psychosociales il a été vu que cette variable n'était pas obligatoirement modulée par le niveau de CI présent dans la relation. Ainsi, dans le cas où un effet simple serait présent sur cette variable, si, comme le propose l'hypothèse, le

niveau de CS est un médiateur de l'action réalisée dans une réalisation de confiance alors un effet d'interaction devrait également être présent.

Tableau 28 : Statistiques descriptives pour le pourcentage de temps utilisé, toutes classes de CS confondues puis pour les classes CS- et CS+

Variable dépendante	Classe attribuée	Confiance induit	Min	Max	Moyenne	Médiane	Ecart Type
Pourcentage de temps utilisé, pour effectuer la tâche de comptage et de supervision, sur le temps alloué (%)		C+	33.29	89.32	77.07	79.57	11.08
		C-	35.06	91.59	80.11	80.98	10.19
	CS-	C+	33.29	89.32	76.39	80.70	13.51
		C-	35.06	90.01	77.12	79.46	12.56
	CS+	C+	58.29	88.27	77.80	76.56	8.13
		C-	71.30	91.59	83.27	83.21	5.70

Les résultats du tableau 28 semblent montrer une différence de moyenne entre la catégorie C+ et C- (77.07 > 80.11). Cette différence est également présente dans la médiane et les écarts types entre les deux catégories sont globalement similaires ce qui indique une possible différence significative. Comme le montrent les données, cette différence de moyenne semble être très élevée dans la classe CS+ alors que les moyennes semblent extrêmement proches dans la classe CS-. Les écarts types assez grands de la classe CS- indiquent également une variabilité plus importante au sein de cette classe par rapport à la classe CS+.

Les boxplot présentés à la figure 60 montrent 3 valeurs extrêmes dans la classe CS-. Les 2 valeurs aux alentours de 35% correspondent a un participant qui n'a pratiquement pas supervisé son coéquipier. Comme observé précédemment dans l'analyse quantitative, les boxplot de la classe CS- sont relativement homogènes et ne semblent pas indiquer une variation du pourcentage de temps utilisé en fonction du niveau de confiance. Les boxplot de la classe CS+ laissent cependant apparaitre une différence relativement forte entre les catégories C- et C+.

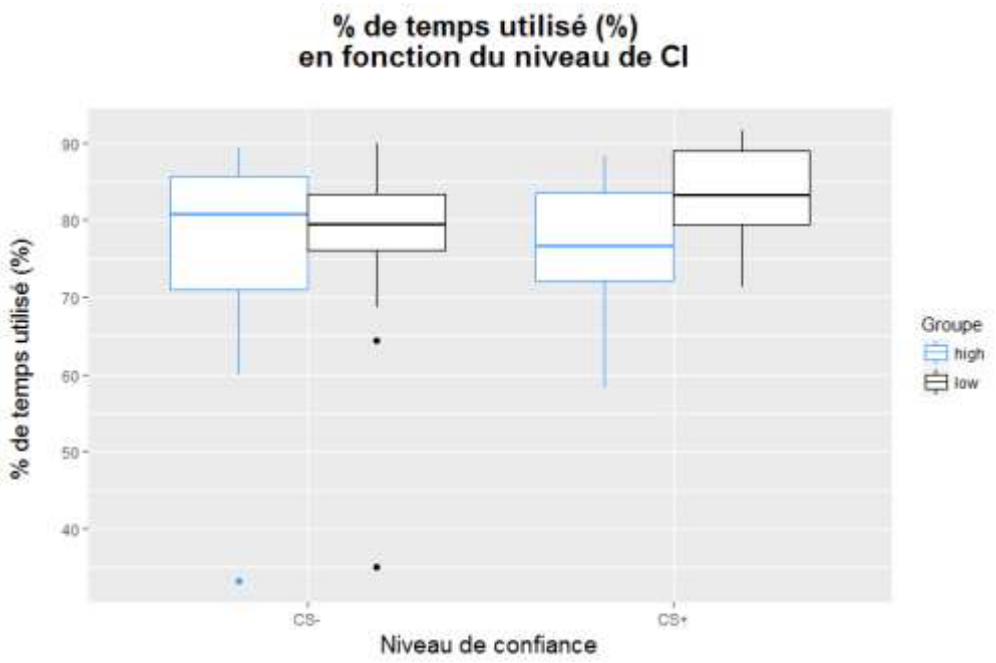


Figure 60 : Boites du Tukey pour le pourcentage de temps utilisé en fonction du niveau de confiance induit pour chaque classe de CS.

Les statistiques inférentielles confirment ces résultats et indiquent une normalité des résidus (p = .88) et la présence d'un effet d'interaction, $F(1,33) = 5.95$, p = .02* entre le niveau de CS et le pourcentage de temps utilisé en C+ et C-. Ainsi, les participants de la classe CS- utilisent autant de temps quel que soit le niveau de confiance qu'ils attribuent à leur coéquipier alors que les participants de la classe CS+ utilisent plus de temps lorsqu'ils n'ont pas confiance dans leur coéquipier que lorsqu'ils ont confiance en lui, ce qui va dans le sens de l'hypothèse 12. Le ηp^2 de .14 indique qu'une part relativement large de la variance est expliquée par cette interaction et que, par conséquent, cette interaction est relativement importante. Ces résultats tendent donc à montrer que le comportement de gestion du temps effectué par un confiant dans une relation de confiance est modulé par le niveau de confiance en soi de ce confiant.

Pourcentage de modifications

Enfin, la dernière variable comportementale à analyser est le pourcentage de modifications. Dans l'expérimentation portant sur les caractéristiques psychosociales ila été vu que cette variable n'était pas obligatoirement modulée par le niveau de CI présent dans la relation. Ainsi, dans le cas où un effet simple serait présent sur cette variable, si, comme le propose l'hypothèse, le niveau de CS est un médiateur de l'action réalisée dans une relation de confiance alors un effet d'interaction devrait également être présent.

Les analyses en statistiques descriptives présentées dans le tableau 29 tendent à montrer une différence entre les catégories C- et C+. Comme attendu, cette différence semble être peu présente dans la classe CS- avec une moyenne entre les catégories relativement proches et un écart type légèrement plus élevé dans la catégorie C-. Cependant, dans la classe CS+ la différence entre les catégories semble être extrêmement forte avec une moyenne et une médiane très nettement inférieure pour la catégorie C+ et des écarts types similaires. Ces observations laissent à penser qu'un

effet d'interaction entre la classe et les catégories existe sur cette variable. La figure 61 corrobore ces observations et montre visuellement que dans la classe CS+ le nombre de modifications augmente lorsque le niveau de CI diminue mais que dans la classe CS- ce nombre de modifications reste relativement constant quel que soit le niveau de CI présent dans la relation.

Tableau 29 : Statistiques descriptives pour le pourcentage de modifications, toute classe de CS confondues puis pour les classes CS- et CS+.

Variable dépendante	Classe attribuée	Confiance induit	Min	Max	Moyenne	Médiane	Ecart Type
Pourcentage de modifications (%)		C+	0	68.75	24.43	23.52	21.99
		C-	0	73.33	30.61	28.57	23.64
	CS-	C+	0	68.75	21.54	18.90	21.97
		C-	0	68.75	22.13	21.76	22
	CS+	C+	0	64.28	27.48	31.25	22.25
		C-	0	73.33	39.60	50	22.51

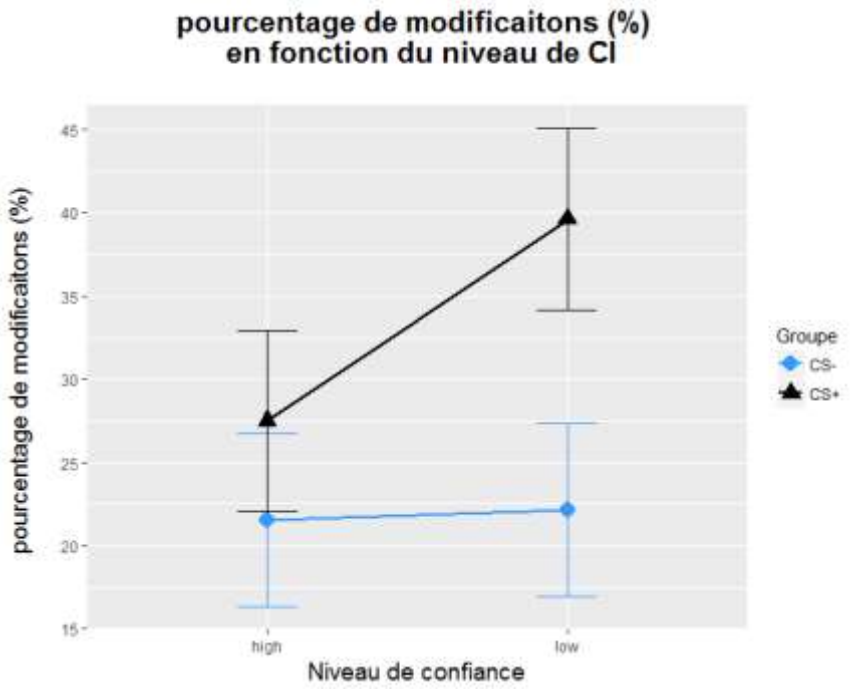


Figure 61 : Pourcentage de modification en fonction du niveau de confiance pour chaque classe de CS

Les analyses en statistiques inférentielles montrent une interaction significative entre la classe et la catégorie, $F(1,33) = 5.95$, $p = .006$**, ainsi qu'une normalité des résidus (p=.24). Analysés ensemble les résultats en statistiques descriptives et inférentielles tendent à valider que les participants de la classe CS- ont modifié les résultats transmis par leur coéquipier de manière équivalente quel que soit le niveau de confiance qu'ils lui attribuaient. Cependant, les participants de la classe CS+ ont plus modifié les résultats de leur coéquipier quand ils ne lui faisaient pas confiance. Ces résultats vont dans le sens de l'hypothèse 12. Ces résultats montrent que le comportement de modifications effectué par un confiant dans une relation de confiance est modulé par le niveau de confiance en soi de ce confiant

E. Discussion

Une analyse des effets simples montre que, chez les élèves ingénieurs, une baisse du niveau de CI module le comportement de gestion du temps, le comportement de modifications mais ne module pas le comportement de supervision. L'analyse des effets simple indique donc que les élèves ingénieurs ayant participés à cette expérimentation ont des modifications comportementales engendrées par différents niveaux de CI similaires à ceux de la catégorie socioprofessionnelle mécaniciens (Base).

Une modification du niveau de CS effectuée sur ces élèves ingénieurs a permis de modifier les comportements engendrés par différents niveaux de CI. Chez les participants de la classe CS-, contrairement à ce que montrent les effets simples, le niveau de CI n'a pas entrainé de modifications comportementales. Quel que soit le niveau de CI induit les participants de la classe CS- avaient un comportement de supervision, de gestion du temps mais également de modifications identiques. Les comportements des participants de la classe CS- sont donc proches des comportements de la catégorie socioprofessionnelle mécaniciens (OPEX). Cependant, chez les participants de la classe CS+, le niveau de CI a entrainé une modulation du comportement de gestion du temps et de modification et n'a pas entrainé de modulation du comportement de supervision. Les comportements des participants de la classe CS+ sont donc identiques aux comportements observés dans la catégorie socioprofessionnelle mécaniciens (Base).

Pris ensemble, les résultats de cette expérimentation tendent à valider l'hypothèse 12 et à montrer que, toute chose égale par ailleurs, une modification du niveau de CS, pour une partie de la population, modifie l'influence du niveau de CI sur le comportement. Sur des participants provenant d'une même catégorie socioprofessionnelle, une modification du niveau de CS permet donc de générer deux groupes différents. Les éléments susceptibles de modifier le niveau de CS des individus (faire des retours sur la performance de cet individu, sur la pertinence de ses actions…) seraient donc également susceptibles de modifier ses comportements vis à vis des niveaux de CI présents dans la relation.

Il est à noter que la ressemblance comportementale observée entre les participants de la classe CS- et les mécaniciens (OPEX) ne signifie pas que les mécaniciens (OPEX) ont un niveau de confiance en eux faible. En effet, en comparant les moyennes obtenues par les différents groupes (mécaniciens OPEX, mécaniciens Base élèves CS+ et élèves CS-), on peut constater que, sur toutes les variables comportementales étudiées, la classe CS- est en dessous des groupes de mécaniciens alors que la classe CS+ est dans la moyenne des groupes de mécaniciens (*Cf.* Tableau 30). Ainsi, tout niveau de CI confondu, les mécaniciens OPEX et Base ainsi que les élèves ingénieurs CS+ ont des stratégies de supervisions, de gestion du temps et de modifications relativement proches alors que les élèves ingénieurs CS- supervisent moins, utilisent moins de temps et modifient beaucoup moins les données transmises par leur coéquipier. En d'autres termes les élèves ingénieurs de la catégorie CS- ont des comportements proches d'un niveau de CI élevé quand les mécaniciens OPEX ont plus un comportement proche d'un niveau de CI faible. Ceci tend donc à montrer que le niveau de CS module le comportement mais que d'autres facteurs doivent être pris en compte.

Tableau 30 : Moyenne générale pour les différentes VD et pour les différents groupes sociaux

Variable dépendante[2]	Moyenne (M) pour les différentes VD pour le groupe mécaniciens (OPEX)	Moyenne (M) pour les différentes VD pour le groupe mécaniciens (Base)	Moyenne (M) pour les différentes VD pour pour la classe CS-	Moyenne (M) pour les différentes VD pour la classe CS+
	Moyenne des 3 niveaux de CI	**Moyenne des 3 niveaux de CI**	**Moyenne des 2 niveaux de CI**	**Moyenne des 2 niveaux de CI**
%VDsup	M = 80.79	M = 86.40	M = 71.03	M = 79.03
%TempsTot	M = 78.74	M = 80.09	M = 76.75	M = 80.53
%VDmodif	M = 39.22	M = 37.94	M = 21.83	M = 33.54

Comme dans l'expérimentation portant sur les caractéristiques psychosociales (expérimentation 1), dans celle présentée ici les participants ont perçu différents niveaux de CI (faibles ou élevé). De même, comme dans l'expérimentation portant sur les caractéristiques psychosociales, les participants ont eu des comportements différents vis-à-vis de la prise en compte de ces niveaux de CI. Cependant, à l'instar de l'expérimentation portant sur les caractéristiques psychosociales, dans l'expérimentation présentée ici tous les participants faisaient partie d'une seule et même catégorie psychosociale et la seule différence entre les participants était le niveau de CS induit au cours de l'expérimentation. En faisant varier le niveau de CS des individus, il a été possible de faire changer leur comportement et de « recréer » en laboratoire les résultats obtenus dans l'expérimentation portant sur les caractéristiques psychosociales. Par conséquent, cette troisième expérimentation tend à montrer le lien entre le niveau de CI et le comportement de l'opérateur, qui est très certainement modulé par son niveau de CS (*Cf.* Figure 62).

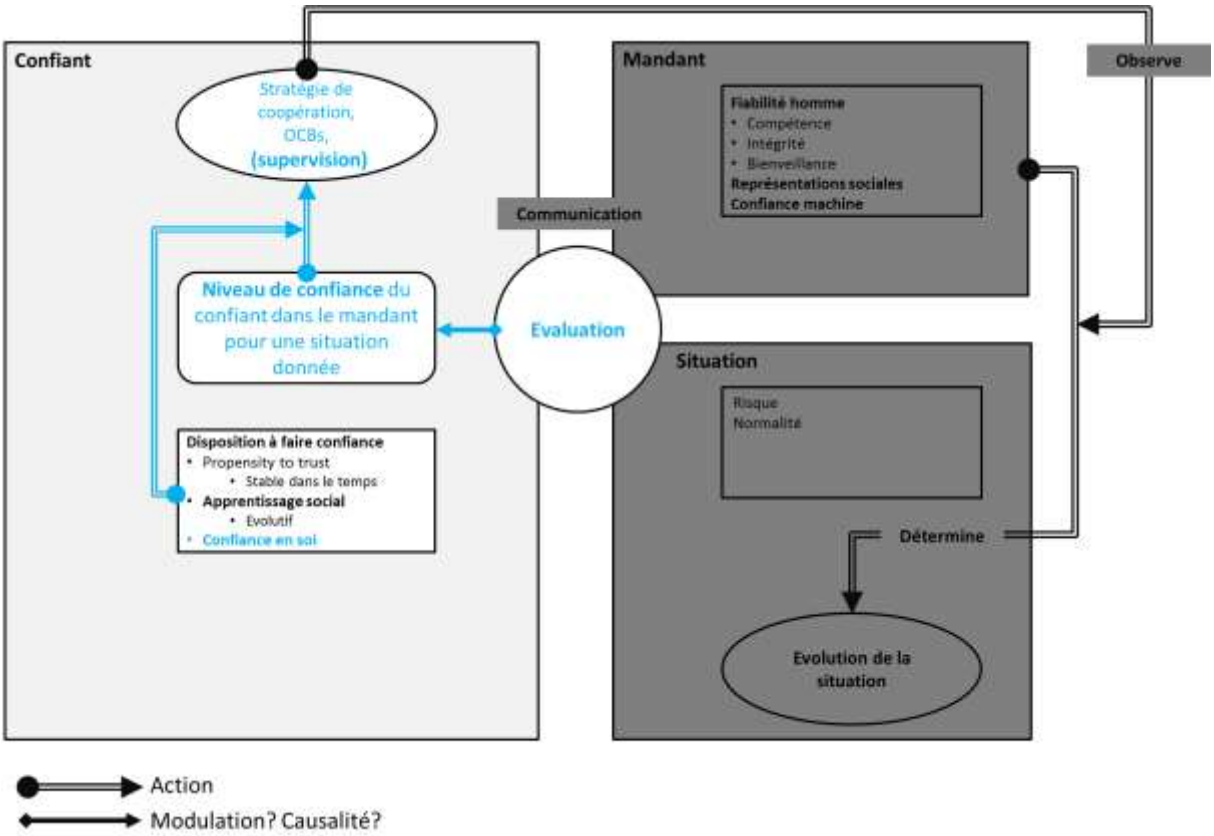


Figure 62 : Résultats de l'expérimentation 3.

6. Apport de l'expérimentation à la RCPair

Les résultats de l'expérimentation 2 (*Cf.* chapitre 6 « 3. Discussion ») suggèrent qu'il serait intéressant d'apposer des taux de fiabilité sur des informations transmises tant au niveau interpersonnel qu'au niveau machine. Les résultats de cette dernière expérimentation (expérimentation sur la CS validant l'hypothèse 12) permettent de donner une première méthode « d'anticipation » des comportements engendrés par ces taux de fiabilité. En effet, les résultats de cette expérimentation montrent que, lorsque le niveau de CS du confiant est bas, le niveau de CI présent dans la relation ne fait plus fluctuer le comportement induit par différents niveaux de CI. Il est donc probable qu'un opérateur ayant un faible niveau de CS ne prenne pas en compte les taux de fiabilités transmis par un autre opérateur ou un système.

Les résultats de cette expérimentation montrent qu'il est possible de calculer (grâce à différents questionnaires) le niveau de CS « général » d'un opérateur mais également le risque de fluctuation, dans un laps de temps très court, de ce niveau de CS. Afin de s'assurer que les informations transmises soient prise en comptes par tous les opérateurs, il est donc préconisé de calculer le niveau de *self esteem* et le niveau de *self esteem variability* de tous les opérateurs afin qu'ils soient homogènes au sein du C2air. Ceci permettrait de s'assurer que le comportement induit par différents niveaux de CI ne soit pas fonction du niveau de CS des différents opérateurs.

Points clés

Cette expérimentation avait pour objectif de montrer l'influence du niveau de CS dans les différentes modulations comportementales engendrées par la modulation des niveaux de CI. Pour pouvoir effectuer cette expérimentation un protocole expérimental permettant de faire diminuer ou augmenter le niveau de CS que des individus ont sur une tâche donnée a été mis au point. Après avoir testé et validé ce protocole expérimental, l'expérimentation a été réalisée avec 35 élèves de deuxième année d'école d'ingénieur. Durant cette expérimentation le niveau de CS a été baissé chez 18 participants, et augmenté chez 17 participants. Les résultats de cette expérimentation tendent à montrer que le niveau de CS d'un individu modifie le comportement qu'il aura dans une relation de confiance. Dans cette expérimentation, les participants de la classe CS- ont eu des comportements similaires, quel que soit le niveau de confiance présent dans la relation alors que les participants de la classe CS+ ont eu des comportements modifiés par le niveau de confiance présent dans la relation.

7 Etude expérimentale de la prise de décision à l'aveugle d'un opérateur en fonction de son niveau de CI en univers incertain

Résumé du chapitre

Objectif : Tester expérimentalement l'impact du niveau de CI sur la prise de décision à l'aveugle des opérateurs en contexte de forte incertitude.

Démarche : Dans les expérimentations précédentes, le confiant pouvait observer les résultats transmis par le mandant avant de prendre une décision (valider ou non le nombre d'aéronefs). Néanmoins, du fait du grand nombre d'informations transitant dans le cyberespace, les opérateurs de la RCPair devront prendre des décisions (acceptation ou non d'une information, validation de la présence d'un virus) sur la base d'informations parfois invérifiables. Dans les modèles de CI décrits dans la littérature, le confiant s'appuie sur la supervision afin de pallier le manque de CI. Dès lors, il est intéressant de se demander si la CI module la prise de décision lorsqu'aucun mécanisme de supervision n'est possible.

Conclusion : Un niveau élevé de CI facilite la prise de décision à l'aveugle lorsque les informations transmises par le mandant vont « dans le même sens » que les informations directement perçues par le confiant.

Chapitre 7 : Etude expérimentale de la prise de décision à l'aveugle d'un opérateur en fonction de son niveau de confiance en univers incertain

1. Introduction et cadre théorique

Les opérateurs de la RCPair, qui surveilleront l'état des systèmes et les flux d'informations véhiculés, seront en charge collectivement de détecter, de mettre en relation et d'analyser les différents indices permettant de donner du sens à une crise cyber (Boin et al., 2014). Ces indices, difficilement perceptibles mais annonciateurs des perturbations du système sont nommés « signaux faibles » (Saritas & Smith, 2011) et sont par nature discrets, éphémères, répartis et difficilement interprétables. Dans un cyberespace complexe et fortement interconnecté, la collecte, la détection tout comme l'analyse et la compréhension des signaux faibles nécessitent l'agrégation des informations provenant de divers acteurs, humains et technologiques, impliqués dans la surveillance du système global. La nature hétérogène de ces signaux accroit également l'incertitude des opérateurs quant à leur interprétation. Dès lors, les décisions prises par le leader d'équipe (le « décideur final » dans ce manuscrit) de la RCPair se feront sur la base d'informations provenant de la situation, mais étant la plupart du temps invérifiables, transmises par les systèmes ou les coéquipiers (qu'ils soient ou non colocalisés). Dans le cas d'une attaque cyber les informations transmises par un coéquipier pourront parfois être contradictoires avec celles du leader ; il pourrait être envisagé que le système RCPair détecte qu'un aéronef n'est qu'un artefact créé par le système alors qu'un opérateur air, analysant la même situation, conclue à un aéronef en détresse. L'étude de ce cas de figure, i.e. la prise de décision des opérateurs des C2air en fonction des données parfois contradictoires provenant de la situation est présentée dans cette expérimentation.

Comme les mécanismes de confiance, les stratégies de prise de décision étudiées en psychologie et en économie reposent parfois sur des éléments probabilistes. Plus particulièrement, la théorie du double processus sous-tend l'existence de deux processus distinct de rationalité~~s~~ (De Neys, 2006; Evans, 2003, 2011; Kahneman & Frederick, 2007) utilisés dans l'optimisation de la prise de décision. Cette théorie, déjà étudiée dans les recherches portant sur la confiance avec induction par visage (Willis & Todorov, 2006) sous-tend que deux systèmes nommés respectivement système 1 et système 2 coexistent. Le système 1 est un système intuitif et rapide qui ne requiert pas l'utilisation de la mémoire de travail (Evans, 2011). Le système 2 est quant à lui utilisé pour des tâches nécessitant une prise de décision réfléchie et, par extension, un calcul de probabilités des futurs possibles engendrés par la décision. Le système 2 est plus lent que le système 1 et requiert des ressources cognitives plus importantes ainsi qu'un accès à la mémoire de travail spécifique à la tâche (Evans, 2011). Ainsi, lorsqu'un individu exploite le système 2, il procède à une estimation de probabilités conditionnelles pour prendre sa décision.

Dans les travaux sous-tendant cette théorie, les lois de probabilités des différentes options sont habituellement clairement identifiables par le participant, permettant de faciliter la prise de décision (Kahneman & Tversky, 1979). Cependant, du fait de la multitude d'informations, dans le cyberespace, aucune loi de probabilité ne semble pouvoir être appliquée rapidement par l'opérateur afin d'analyser la véracité et l'impact des signaux faibles. Lorsqu'un leader d'équipe doit prendre une décision il ne peut le faire que sur la base de ses propres informations (les signaux faibles qu'il a lui-même perçus directement) et des informations transmises par ses différents coéquipiers sans pouvoir les vérifier ou les confronter à une probabilité. Dans ces cas-là, d'autres mécanismes facilitateurs de la prise de décision devraient donc rentrer en jeu. Parmi ces mécanismes, la confiance est souvent décrite comme étant un réducteur de l'incertitude (Meyerson et al., 1996) qui facilite la prise de décision (Bell, 1982). Cette expérimentation propose d'étudier, dans les environnements à forte incertitude, le rôle de la CI dans la prise de décision du leader lorsqu'il ne peut pas apposer une probabilité sur l'évolution de la situation ni vérifier efficacement les informations transmises par son co-équipier (*Cf.* Figure 63). En d'autres termes, cette expérimentation cherche à déterminer si, en l'absence de supervision possible, le niveau de CI joue toujours un rôle dans la prise de décision (lien bleu sur la figure 63) ou si d'autres éléments provenant de la situation peuvent moduler le lien entre la confiance et la prise de décision (lien orange sur la figure 63).

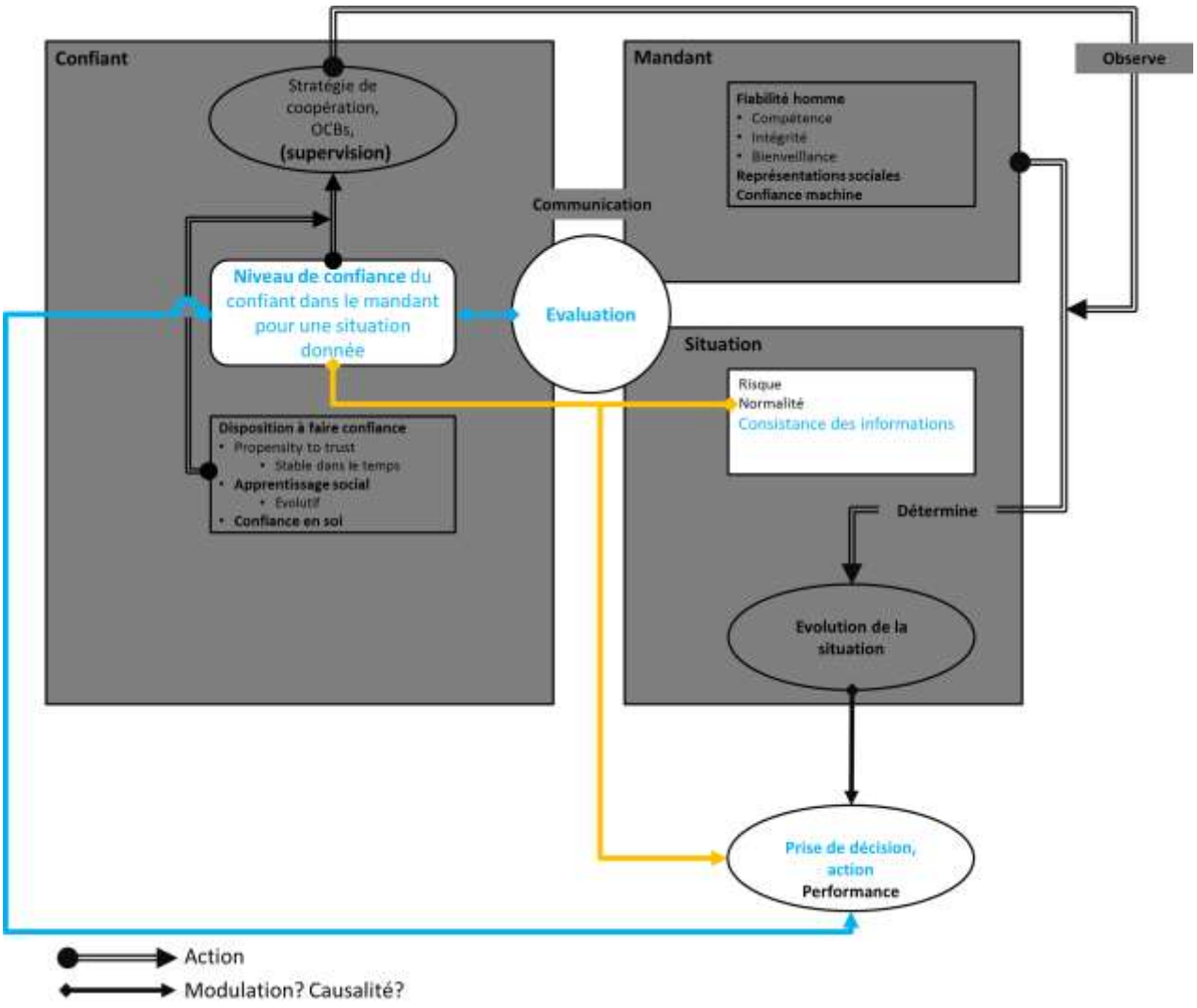


Figure 63 : Liens analysés dans l'expérimentation 4

Posten & Mussweiler (2019) établissent une fonction de prédictibilité de la confiance, autrement dit la confiance permettrait d'anticiper les possibles en calculant leur probabilité d'occurrences. C'est aussi ce que Gambetta indiquait en définissant la confiance comme « *un niveau particulier de la probabilité subjective avec laquelle un opérateur évalue qu'un autre opérateur ou un groupe d'opérateurs va effectuer une action particulière, à la fois avant qu'il ne puisse contrôler cette action (ou indépendamment de sa capacité à la contrôler) et dans un contexte où elle affecte sa propre action* » (Gambetta, 1988, p. 217) [42]. Cette définition de Gambetta ou de manière plus globale les recherches menées en économie (Williamson, 1993) et en sociologie (Coleman, 1990) lient le phénomène de confiance à la notion d'évaluation probabiliste et rejoignent ainsi l'approche de la théorie du double processus de Kahneman.

Selon les théories probabilistes étudiées dans la littérature économique, la confiance peut être envisagée comme étant le calcul du coût-bénéfice (Williamson, 1993) perçu d'une relation. Dans cette approche calculative, « *La confiance émerge lorsque le confiant perçoit que le* mandant *a l'intention d'accomplir une action qui est bénéfique »* (Rousseau et al., 1998, p. 399) [43]. De fait, la confiance ne peut survenir que dans des relations qui apportent une récompense aux deux parties (Lewicki & Bunker, 1995) et peut être résumée, sous l'angle économique par un calcul de probabilité (Williamson, 1993).

Cette notion de calcul de probabilité est le lien entre les littératures portant sur la confiance et celles portant sur la prise de décision. Conceptuellement la décision correspond à « *un choix ou un ensemble de choix tirés des alternatives disponibles* » (Bellman & Zadeh, 1970, p. 636)[44]. La prise de décision correspond donc au choix de l'alternative présentant subjectivement le meilleur ratio coût/bénéfices. Dans cette approche, la prise de décision n'est autre que le résultat d'une évaluation probabiliste des conséquences de différents choix (Lowenstein, 2003). Dans le processus de prise de décision le mécanisme de confiance pourrait donc être vu comme un réajustement des probabilités perçues par un opérateur des futurs possibles engendrés par différentes options (*Cf.* Figure 63), l'option choisie par l'opérateur étant celle ayant le meilleur ratio cout/bénéfice. Cette interprétation rejoint d'ailleurs la définition de Lewis et Weigert (1985, p969) qui décrivent le fait d'avoir confiance comme « *… vivre comme si certains futurs rationnellement possibles ne se produisaient pas. [...] En l'absence de confiance, la monstrueuse complexité que représentent les futurs possibles reviendrait à paralyser l'action* »[45].

Dans les équipes évoluant dans des environnements incertains comme le cyberespace dans lesquels les opérateurs ne peuvent pas assigner des probabilités quant aux évènements futurs engendrés par une décision (Duncan, 1972), la confiance devrait faciliter la prise de décision. Dans les cas où le leader ne peut pas vérifier *in situ* les informations transmises par son coéquipier, et par conséquent assigner une probabilité quant à la fiabilité de ces informations, le niveau de confiance pourrait être

[42] « a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to monitor it) and in a context in which it affects his own action » (Gambetta, 1988, p. 217)

[43] « *Trust emerges when the trustor perceives that the trustee intends to perform an action that is beneficial* » (Rousseau et al., 1998, p. 399)

[44] « a choice or a set of choices drawn from the available alternatives » (Bellman & Zadeh, 1970, p. 636)

[45] « *to trust is to live as if certain rationally possible futures will not occur. [… In] the absence of trust, the monstrous complexity posed by contingent futures would again return to paralyze action* » (Lewis & Weigert, 1985, p. 969)

déterminant dans la prise de décision notamment en facilitant l'acceptation, par le leader, des informations transmises par son coéquipier (lien bleu sur la figure 63). Lorsque le niveau de confiance est élevé entre un leader et son coéquipier, les informations transmises par le coéquipier devraient être perçues par le leader comme étant probablement plus fiables que lorsque le niveau de confiance est faible.

Hypothèse 13 : Pour un leader d'équipe, un niveau de confiance élevé dans son coéquipier entraine une plus grande acceptation des informations invérifiables transmises par le coéquipier.

Dans la RCPair, les signaux faibles remontés par un opérateur peuvent être invérifiables par le leader. Par exemple, les consoles du CNOA et celles des CDC peuvent afficher un nombre de pistes différents. Auquel cas, cette impossibilité de vérifier les informations entraine chez le leader, une impossibilité d'affecter une probabilité effective à ces signaux faibles. De fait, lorsque le leader ne peut pas s'appuyer sur des probabilités effectives, il doit attribuer une probabilité subjective (Kahneman & Tversky, 1972) quant à ces signaux faibles. Pour cela, il ne peut s'appuyer que sur ses propres informations, particulièrement l'évaluation des signaux faibles qu'il a lui-même reçu ; il peut dès lors réaliser une comparaison entre les signaux faibles qu'il a directement perçus et ceux qui lui ont été communiqués ; si l'ensemble de ces signaux faibles correspondent ils sont considérés comme « consistants ». Dans ce cas, le leader devrait percevoir les informations transmises par son coéquipier comme étant probablement plus fiables que dans le cas de signaux « non-consistants ».

Dans le cas de signaux faibles « consistants », la prise de décision pourrait être faite de manière intuitive, sans recourir à une réflexion approfondie puisque tous les indices vont dans le même sens. En utilisant la théorie des doubles-processus, cela reviendrait à mobiliser le système 1 et avoir une décision rapide et intuitive. Dans le cas des signaux inconsistant, l'opérateur pourrait être amené à baser plutôt sa décision sur le système 2 en évaluant les différentes options à travers un calcul probabiliste. Le processus décisionnel serait alors plus long. Sans chercher à vérifier l'exactitude de la théorie des doubles-processus, il est supposé que des signaux faibles « consistants » vont amener une prise de décision plus rapide que la survenue de signaux faibles « non-consistants » (Hypothèse 14). Dans le cas de signaux « non-consistants », le niveau de confiance entre les coéquipiers pourrait participer à l'évaluation des différentes options et influer sur la prise en compte des informations transmises. Par exemple, si le leader n'a pas perçu directement de signes d'une attaque il risque de juger comme étant peu probables des éléments en faveur d'une attaque qui sont fournis par un coéquipier pour lequel le niveau de confiance est faible. Inversement, un leader acceptera davantage la contradiction s'il a confiance dans son coéquipier (hypothèse 15) (lien orange sur la figure 63).

Hypothèse 14 : Les signaux « consistants » sont traités plus rapidement par le leader que les signaux « non-consistants ».

Hypothèse 15 : Dans le cas de signaux « non-consistants », le leader prend davantage en compte les données transmises par son coéquipier lorsque le niveau de CI est élevé entre les membres de l'équipe.

2. Matériel et Méthode

Pour tester ces hypothèses, il est nécessaire d'avoir un contexte expérimental similaire à celui que pourraient rencontrer les leaders cyber. Ainsi, cet environnement doit proposer au participant une tâche principale et une tâche de supervision sur lesquelles peuvent se greffer un ou plusieurs signaux faibles directement perçus par le leader ou transmis par un coéquipier. En dépit du caractère faible, ces signaux doivent être suffisamment détectables. La tâche prescrite doit obliger le leader à prendre une décision sur la base de ces signaux faibles qu'il ne peut pas vérifier alors qu'il a un niveau de confiance variable dans son coéquipier et que ces signaux ne sont pas toujours consistants.

La tâche choisie est une extension de la tâche mobilisée dans les expérimentations précédentes et qui remplit ces conditions : elle propose au participant une tâche principale de comptage d'aéronefs sur une image avec la possibilité de vérifier une tâche similaire chez un coéquipier. Ce coéquipier est fictif et uniquement présenté par les paires de mots mises en place et testées dans la première expérimentation.

Durant cette tâche, des brouillages momentanés de l'image (*Cf.* Figure 64), constituant les signaux faibles, peuvent survenir. De manière similaire à la tâche de comptage des aéronefs, le participant doit aussi dénombrer le nombre de brouillages survenus sur son image puis valider le nombre de brouillage global. Ce nombre de brouillage global comprend ceux de son image mais aussi ceux apparus sur l'image de son coéquipier. L'opérateur ne peut pas vérifier le nombre de brouillages indiqués par son coéquipier. Cette prise en compte de l'information du coéquipier correspond à une décision « à l'aveugle ». C'est cette décision qui est analysée ici et non les décisions relatives à la tâche principale de comptage d'aéronefs, celle-ci pouvant être vérifiée en regardant l'image du coéquipier

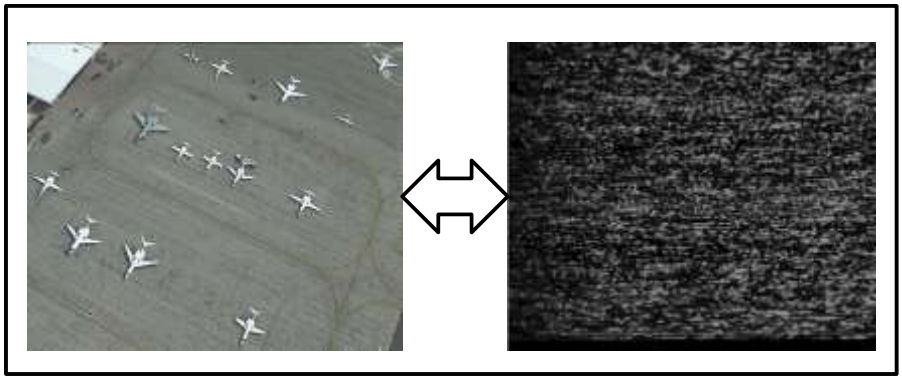


Figure 64 : Présentation des brouillages pouvant survenir dans l'expérimentation 4.
En cas de brouillage l'image de droite apparait durant une seconde avant de disparaitre.

Afin de tester l'impact de la confiance sur l'acceptation des informations transmises (hypothèse 13), il est nécessaire d'induire différents niveaux de confiance chez le participant, de vérifier cette induction et de tester, selon ces niveaux, le pourcentage d'informations transmises par le coéquipier qui sont acceptées par le participant. L'induction du niveau de confiance est une variable indépendante (VI) à deux niveaux contrôlés (faible et élevé). Le pourcentage d'informations transmises par le coéquipier et acceptées par le leader (en %) est une variable dépendante (VD) recueillie au cours de l'expérimentation qui sera notée « décision » dans la suite de ce manuscrit.

Afin de tester l'impact de la consistance sur le choix du système de décision (système 1 ou système 2) (hypothèse 14) il est nécessaire d'induire des signaux « consistants » et « non-consistants » et de comparer le temps mis par le participant à valider une décision selon la nature de ces signaux. Celle-ci est une VI qui sera notée consistance dans la suite de cet article. La distribution de la consistance est contrôlée par l'occurrence des signaux faibles transmis. Le temps mis par le participant à valider une décision (en ms) est une VD, notée « temps », recueillie au cours de l'expérimentation

Afin de déterminer l'impact de la confiance dans la prise de décision lors d'événement « consistants » et/ou « non-consistants » (hypothèse 15) les deux VI explicitées précédemment ainsi que la VD décision sont utilisées.

A. Participants

45 personnes (46.6% de femmes et 53.3% d'hommes) d'âge moyen 22.7 ans (SD : 1.09%) ont participé à cette étude. Tous les participants étaient des élèves de deuxième année d'école d'ingénieur. Aucun participant n'avait de problème de santé, tous avaient une vision normale ou corrigée.

B. Protocole

Avant le début de l'expérimentation, un briefing a été effectué, et tous les participants ont rempli une feuille de consentement éclairé. Ensuite, les participants ont effectué un entrainement de 5 minutes avant de commencer l'expérimentation, qui était découpée en 28 essais comportant chacun 4 phases. Pour chaque essai, le participant travaillait avec un coéquipier différent (comportement simulé par ordinateur). 14 essais étaient effectués avec un coéquipier digne de confiance (confiance élevée) et 14 avec un coéquipier non digne de confiance (confiance faible). Afin d'éviter un effet d'ordre, les profils des coéquipiers étaient tirés aléatoirement. Tous les participants travaillaient donc avec tous les profils des coéquipiers mais dans un ordre différent.

Les participants passaient l'expérimentation en groupe dans des salles informatiques ne leur permettant pas de voir ce qui se passait sur l'écran des autres personnes. A chaque essai, le participant pensait réaliser la tâche en collaboration avec une des autres personnes de la salle, même si en réalité tous les coéquipiers étaient fictifs. Chaque participant réalisait la tâche sur un ordinateur classique en utilisant le clavier et la souris. Les écrans de tous les participants étaient similaires tant en terme de résolution qu'en terme de luminosité.

La réalisation de la tâche comprenait 4 phases. La première et la quatrième phase étaient similaires à la première et à la troisième phase des expérimentations précédentes (présentation des caractéristiques de son nouveau coéquipier en phase 1 et évaluation subjective en phase 4).

La deuxième phase correspondait à la réalisation de la tâche de comptage d'aéronefs et de comptage du nombre de brouillages. Le participant disposait d'un affichage de contrôle similaire à celui utilisé dans les expérimentations précédentes et qui lui permettait de voir le décompte du temps restant ainsi que la somme des aéronefs dénombrés sur les deux images.

L'affichage lui permettant d'effectuer sa propre tâche de comptage était diffèrent de celui utilisé dans expérimentations précédentes. Sur cet affichage le participant trouvait son image, le temps restant (*Cf.* Figure 65 « 1 ») ainsi que 5 intéracteurs qui lui permettaient :

- d'incrémenter ou décrémenter le compte du nombre d'aéronefs (*Cf.* Figure 65 « 2 »),
- D'incrémenter le nombre de brouillages détectés (*Cf.* Figure 65 « 3 »),
- De valider son compte du nombre d'aéronefs (*Cf.* Figure 65 « 4 »)
- De retourner à l'écran d'accueil (*Cf.* Figure 65 « 5 »).

L'affichage de l'écran de travail du coéquipier était exactement le même que celui du participant. Cependant, sur l'écran du coéquipier, les boutons n'étaient pas cliquables (sauf le bouton utilisé pour revenir à l'écran de contrôle). Sur l'écran associé au coéquipier, l'image était différente de celle présentée sur l'écran du participant et ce dernier devait faire les tâches de comptage de l'avion et de brouillage sur cette autre photo. De plus, sur l'écran du coéquipier, il était impossible pour le participant de voir le brouillage (les événements de brouillage n'étaient jamais affichés sur l'écran du coéquipier). Dans cette expérience, le participant ne savait pas qu'il lui était impossible de voir les événements de brouillage se produire sur l'écran du coéquipier.

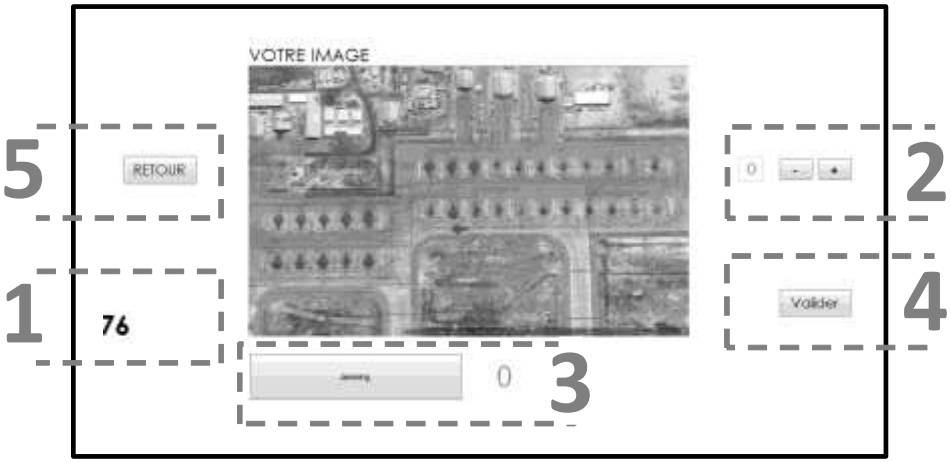


Figure 65 : Affichage utilisé par le participant en phase 2 afin d'effectuer sa tâche de comptage.
Sur cet affichage le participant pouvait prendre connaissance du temps restant (« 1 »). A l'aide de différents intéracteurs, le participant pouvait dénombrer les aéronefs (intéracteur « 2 »), incrémenter le compteur de brouillages (intéracteur « 3 »), valider son compte d'aéronefs (intéracteur « 3 ») ou retourner sur l'Affichage principal (intéracteur « 4 »).

Le participant devait compter les aéronefs de son image et valider le résultat total de l'équipe avant la fin du temps imparti. Si cela n'était pas le cas, l'essai était échoué et un essai supplémentaire avec un coéquipier de même type était ajouté en fin de session. La validation du score total permettait de passer à la phase suivante.

La troisième phase était dédiée à la validation par le participant des brouillages détectés sur les deux images. L'affichage montrait le nombre de brouillages détectés par le coéquipier (*Cf.* Figure 66 « 1 ») et le nombre de brouillages détectés par le participant (*Cf.* Figure 66 « 2 »). Dans la mesure où aucun brouillage réel n'était affiché sur l'écran du coéquipier, le participant ne pouvait pas constater ces brouillages et ne pouvait donc évaluer la validité de l'information transmise par son coéquipier. A côté de chacun de ces chiffres 3 intéracteurs étaient présentés. Ces intéracteurs permettaient de valider ou non les brouillages (aucun, 1 ou plusieurs). Le participant devait obligatoirement prendre une décision quant au nombre de brouillages à valider sur l'image de son coéquipier (*Cf.* Figure 66 « 3 ») ainsi qu'au nombre de brouillages à valider sur sa propre image. Une fois cela fait le participant pouvait passer en phase 4.

Les différentes VD utilisées pour tester les 3 hypothèses ont été recueillies en phase 3. La VD « décision » utilisée pour tester les hypothèses 12 et 14 correspond au pourcentage de brouillages transmis par le coéquipier et non validés par le participant (en %). La VD « temps » utilisée pour tester l'hypothèse 14 correspond au temps mis par le participant à valider cette troisième phase (en ms).

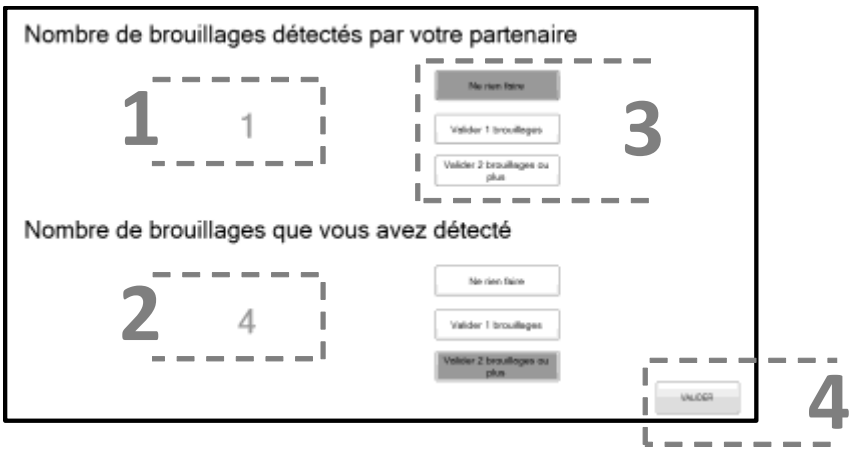


Figure 66 : Affichage de la phase 3.
Sur cet affichage le participant pouvait prendre connaissances du nombre de brouillages détectés par son coéquipier (« 1 ») et du nombre de brouillages qu'il avait lui-même indiqué (« 2 »). Le participant devait prendre une décision sur le nombre de brouillages à valider pour le coéquipier (intéracteurs « 3 ») et pour lui-même avant de pouvoir terminer la phase 3 en cliquant sur le bouton de validation (intéracteur « 4 »).

Afin de maitriser la VI « consistance », dans cette expérimentation, les brouillages présentés au participant étaient liés aux brouillages transmis par le coéquipier fictif afin d'obtenir les 4 dispositions suivantes :

- Aucun brouillage n'était présenté au participant et le nombre de brouillages détectés par le coéquipier était de 0 (25% des cas)
- 1 ou 2 brouillages étaient présentés au participant et le nombre de brouillages détectés par le coéquipier étaient de 1 ou 2 (25% des cas)

- Aucun brouillage n'était présenté au participant mais le nombre de brouillages détectés par le coéquipier étaient de 1 ou 2 (25% des cas)
- 1 ou 2 brouillages étaient présentés au participant mais le nombre de brouillages détectés par le coéquipier était de 0 (25% des cas)

Les deux premiers cas étaient les cas dits « consistants » et les deux autres « non-consistants ».

3. Résultats

Les données des 45 participants ont été incluses dans l'analyse. Avant d'analyser les résultats nécessaires au test des hypothèses, la vérification portant sur l'induction de la confiance dans le protocole expérimental a été effectuée. Les données de l'évaluation subjective des résultats transmis par le coéquipier (récupérées en phase 4) montrent que lorsque le niveau de confiance est élevé (M = 5.68, SD = 2.33) l'évaluation subjective de la performance du coéquipier est plus haute que lorsque le niveau de confiance est faible (M = 5.34, SD = 2.44). Les résultats significatifs sur ces données, $F(1.44) = 4.11$, $p = .04$* permettent de valider la présence de deux niveaux de confiance (élevée et faible).

Afin de tester l'hypothèse qu'un niveau de confiance élevé entre les membres de l'équipe entraine chez le leader une plus grande acceptation des informations transmises par son coéquipier (hypothèse 13), la VD « décision » et la VI « niveau de confiance » ont été utilisées. Pour chaque participant, les données obtenues ont été moyennées pour chaque niveau de confiance. Les données indiquent (*Cf.* Figure 67) que pour les niveaux de confiance faible (M = 23.4%, SD = 35.7%) et élevé (M = 21%, SD = 33%), les performances sont relativement semblables. Des résultats non significatifs sur ces données, $F(1.44) = 1.1$, $p = .30$ ne permettent pas de valider l'hypothèse 1. Autrement dit, rien ne permet d'indiquer que le niveau de CI a un effet direct sur la validation des résultats transmis par le coéquipier.

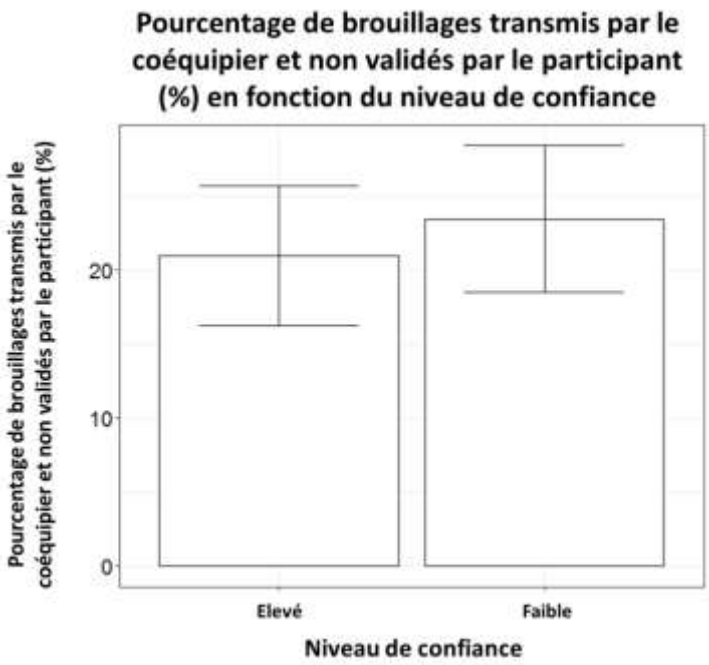


Figure 67 : pourcentages de brouillages transmis par le coéquipier et non validés par le participant en fonction du niveau de confiance

Afin de tester l'hypothèse que les signaux « consistants » sont traités plus rapidement par le leader que les signaux « non-consistants » (hypothèse 14), la VD « temps » et la VI « consistance » ont été utilisées. Pour chaque participant, les données obtenues ont été moyennées pour chaque niveau de consistance. Les résultats montrent que lorsque les signaux sont « consistants » (M = 3750.5 ms, SD = 1192.4 ms) les participants valident la phase 3 plus rapidement que lorsque les signaux sont « non-consistants » (M = 4272.7 ms, SD = 1515.5 ms). Les résultats significatifs sur ces données, $F(1.44) = 13.37$, $p < .001$*** permettent de valider l'hypothèse 14. Il semble donc que les participants aient bien perçu la consistance des signaux de manière différente.

Afin de tester l'hypothèse que dans le cas de signaux « non-consistants », le leader prend davantage en compte les données transmises par son coéquipier lorsque le niveau de CI est élevé entre les membres de l'équipe (hypothèse 15), la VD « décision », la VI « niveau de confiance » et la VI « consistance » ont été utilisées. Pour chaque participant, les données obtenues ont été moyennées, pour chaque niveau de confiance, en fonction de leur consistance. Les données montrent (*Cf.* Figure 68) que lorsque les informations transmises par le coéquipier vont dans le sens de l'évènement perçu comme étant le plus probable (cas « consistants »), le leader valide les informations transmises par son coéquipier de manière similaire, que le coéquipier soit associé à un niveau de confiance élevé (M = 21.3%, SD = 30.8%) ou faible (M = 18.5%, SD = 32%). Cependant, dans le cas où les informations transmises par le coéquipier vont dans le sens d'un évènement perçu comme étant peu probable (cas « non-consistants »), lorsque le niveau de confiance est élevé (M = 20.6%, SD = 35.4%) le leader valide plus facilement les informations transmises par son coéquipier que lorsque le niveau de confiance est faible (M = 28.4%, SD = 38.7%). En accord avec l'hypothèse 15 les résultats de l'ANOVA montrent bien un effet d'interaction, $F(1,132) = 4.86$, $p = .02$* (eta-squared =.068). Une analyse post hoc effectuée avec un test de Tukey HSD indique une différence significative sur les différents niveaux de confiance pour les essais « non-consistants » ($p = .02$*) et aucune différence pour les essais « consistants » ($p = .40$).

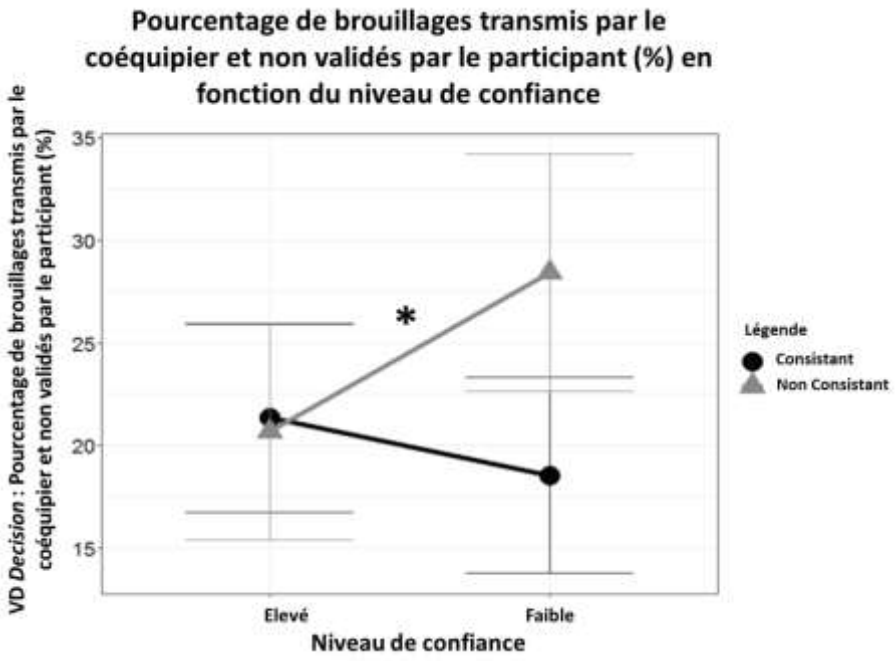


Figure 68 : pourcentages de brouillages transmis par le coéquipier et non validés par le participant en fonction du niveau de confiance et du caractère « consistants » *ou* « non-consistants » des essais

4. Discussion

Cette dernière étude s'intéresse au lien entre la CI et la prise de décision dans les environnements incertains. En se basant sur la théorie des doubles processus (De Neys, 2006; Evans, 2003, 2011; Kahneman & Frederick, 2007), il est attendu que, dans le monde cyber, les prises de décisions puissent reposer soit sur un mécanisme rapide et intuitif qui mobilise peu de ressources (système 1), soit sur un mécanisme plus lent (système 2) (Evans, 2011) faisant intervenir une évaluation de probabilités par rapport aux situations possibles, aux risques et bénéfices de certaines alternatives. Appliqué au sein d'un micro-monde issu de la gestion de crise cyber, l'expérimentation cherche à mieux comprendre l'impact de la confiance entre les opérateurs et celui de la consistance des informations échangées sur le mécanisme de prise de décision (au travers du temps mis pour réaliser la tache), mais aussi sur la décision elle-même (validation de la réponse du coéquipier).

Les résultats montrent que la CI n'impacte pas directement la prise de décision lorsque celle-ci est prise sur des éléments invérifiables (hypothèse 13). Ce résultat semble aller à l'encontre des modèles existants qui établissent des liens entre confiance et prise de décision (Kim et al., 2008). Toutefois la littérature actuelle étudie la CI lors de tâches collaboratives où les participants peuvent *a minima* accéder au travail du coéquipier pour l'évaluer (Bollon et al., 2019; Dirks, 1999), alors que le protocole présenté ici propose une décision à l'aveugle. Il semble nécessaire d'étudier plus avant ce type de situation et son impact sur la confiance. En revanche, la consistance des informations échangées modifie directement le temps mis pour prendre la décision (hypothèse 14). Autrement dit, la consistance des éléments échangés entre les opérateurs serait le premier critère qui détermine le mécanisme qui sous-tend la prise de décision. Une fois le mécanisme de prise de décision (système 1 ou 2) choisi, la confiance intervient dans la décision elle-même dans la mesure où le participant en

système 2 acquiesce davantage le résultat du coéquipier lorsqu'il a confiance même si l'information donnée est non consistante (hypothèse 15) (*Cf.* Figure 69).

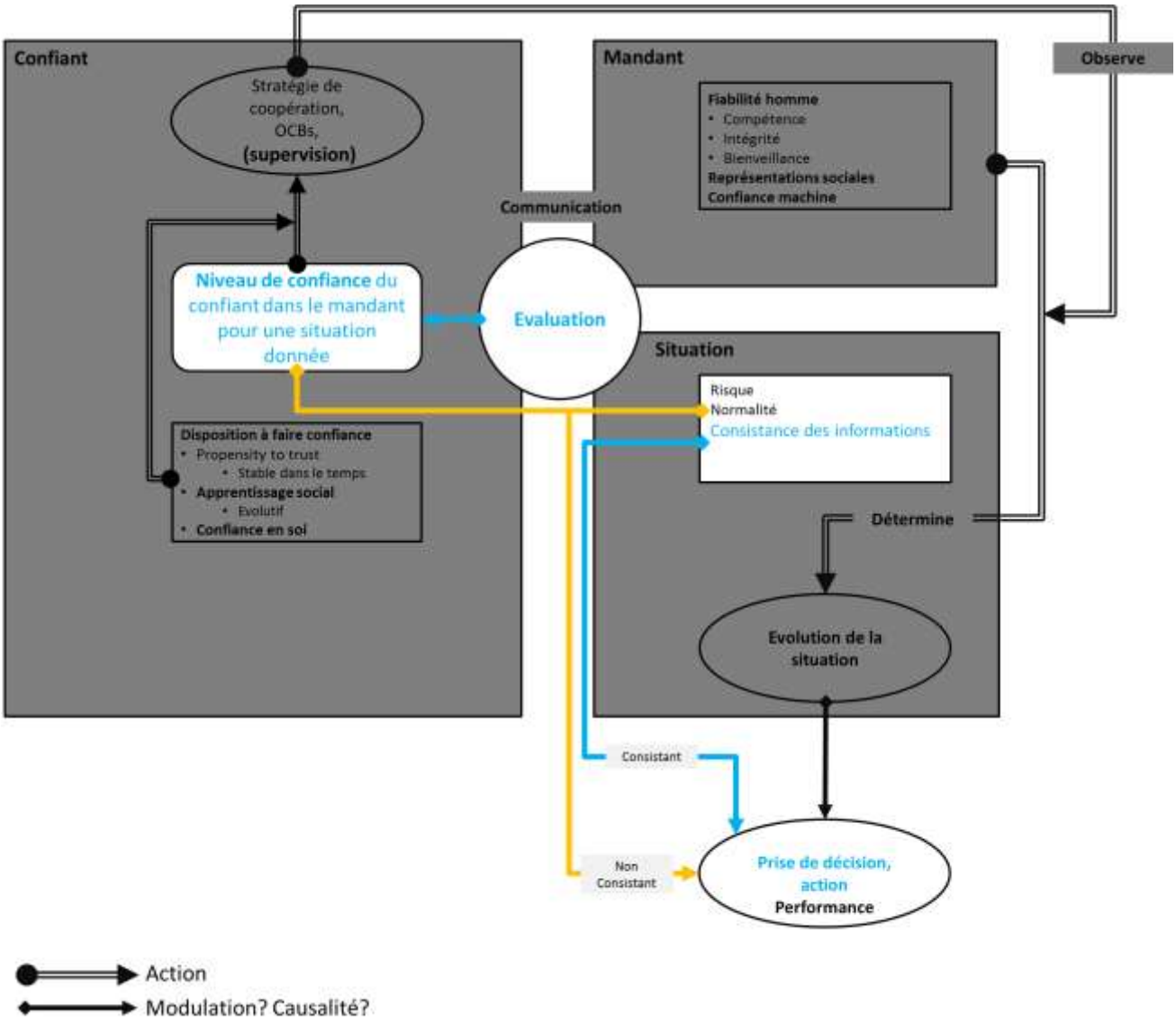


Figure 69 : Résultats de l'expérimentation 4.
Lorsque les signaux faibles directement reçus par le participant et les signaux faibles transmis par le coéquipier sont perçus comme étant « consistants », la prise de décision est rapide et intuitive (système 1) et est indépendante du niveau de confiance (lien bleu sur la figure). Cependant, dans le cas de signaux faibles perçus comme étant « non-consistants » la prise de décision est plus lente (système 2) et fait intervenir le niveau de confiance (lien orange sur la figure). Lorsque le niveau de confiance est élevé la prise de décision du participant va dans le sens des informations transmises par le coéquipier et lorsque le niveau de confiance est faible la prise de décision va dans le sens des informations qu'il a lui-même perçu.

Ainsi, l'étude montre que dans les situations dans lesquelles il est impossible d'apposer une probabilité quant aux futurs de la situation, le résultat de la décision, en termes de validation ou non de l'information du coéquipier, est lié à la fois à la consistance de l'information transmise et au niveau de confiance entre les opérateurs. Quand l'information reçue est consistante avec les observations de l'opérateur, la prise de décision est intuitive et n'est pas liée au niveau de confiance entre les opérateurs. Globalement, l'information est acceptée par l'opérateur. En revanche, quand l'information n'est pas consistante et que l'opérateur mobilise le système 2 pour prendre sa décision,

alors la confiance dans la personne qui lui a donné l'information peut venir modifier la décision ; plus l'opérateur a confiance dans son coéquipier, plus il est enclin à accepter son information, que celle-ci confirme ou infirme ses observations. Le niveau de confiance jouerait donc bien sur la probabilité que l'opérateur va associer à la donnée reçue, ce que la littérature suggérait depuis les travaux de Gambetta (1988).

Un des apports méthodologiques de cette étude est que l'on retrouve de manière expérimentale la mise en œuvre de mécanismes différents de prise de décision en fonction de la consistance, qui seraient cohérents avec la théorie du double processus. Autrement dit, ce micro-monde permettrait d'affecter la prise de décision soit dans le système 1, soit dans le système 2. Toutefois, le protocole utilisé ne permet pas de vérifier que le délai temporel constaté en fonction de la consistance correspond à un « calcul de probabilités ». L'étude ne dit rien sur les mécanismes sous-tendant ces 2 systèmes mais elle conforte l'idée qu'il y a plusieurs mécanismes possibles pour la prise de décision et que le contexte va favoris er le choix d'un mécanisme particulier. Une future étude devra permettre de vérifier ce calcul de probabilités en détaillant comment est réalisé le processus de décision. Elle pourra s'appuyer sur ce micro-monde pour mieux comprendre les mécanismes cognitifs réellement mis en jeu dans chaque stratégie.

Il a été envisagé dans cette étude deux facteurs, consistance et confiance, qui se combinent pour moduler le mécanisme de prise de décision et le contenu de la décision dans les activités collaboratives. Il serait opportun à présent d'étudier dans quelle mesure ces résultats sont liés au fait d'interagir entre opérateurs humains ou s'ils sont plus génériques ; dans la mesure où les résultats de l'expérimentation 2 montrent que les mécanismes de CI et de CM sont identiques, il serait intéressant de voir sir ces mécanismes de prise de décision sont également identiques dans le cas où l'opérateur agit en coopération avec un système automatisé ou une intelligence artificielle.

5. Apport de l'expérimentation à la RCPair

L'impact direct de la consistance est significatif dans le cadre de la mise en œuvre de la RCPair. En effet, il est important, pour la sécurité des membres des C2 et la réussite des missions, de comprendre ce qui peut impacter la manière de prendre les décisions. Ceci peut permettre notamment d'adapter la formation des opérateurs en les sensibilisant à l'effet de la consistance sur leur prise de décision (décision rapide versus décision rationnelle). Ces résultats peuvent participer également à mieux appréhender la manière dont les informations sont présentées sur les interfaces afin d'aider à la meilleure prise de décision.

L'expérimentation montre que dans le contexte d'une décision prise en évaluant les risques ou les coûts associés à chaque choix, la confiance dans la source de l'information vient modifier la décision. Ce résultat semble fondamental d'un point de vue applicatif car il montre que certains signaux faibles remontés vers le décideur pourraient être pris en compte différemment dans la décision en fonction de la relation entre les personnes. Selon la consistance des différents signaux, la confiance entre les personnes viendrait modifier la confiance que l'opérateur accorde à la donnée elle-même. Dans le cadre de la RCPair, et plus généralement dans les systèmes sociotechniques tels que les C2air, il parait nécessaire de prendre en compte cette dimension afin d'optimiser son effet sur le fonctionnement du système. Précédemment, le fait d'apposer un taux de fiabilité et un risque

associé aux informations transmises entre les opérateurs (humains et systèmes) des C2air a été suggéré pour optimiser les processus de décision. La consistance des informations pourrait être prise en compte dans le calcul ou la présentation du risque lié à ces informations. En effet, cette expérimentation montre que les opérateurs prennent plus facilement en compte des informations extérieures qui confirment les informations qu'ils ont eu même perçu. Cependant, dans le cas d'informations contradictoires, l'opérateur semble plus avoir tendance à accepter les informations pour lesquelles il a le plus haut niveau de confiance. Le taux de fiabilité pouvant être interprété, par l'opérateur, comme un niveau de confiance à apposer aux informations, dans le cas d'informations contradictoires (non consistantes) il pourrait être intéressant de maximiser le niveau de risque de l'information la plus risquée ou de maximiser le taux de fiabilité de l'information la plus probable.

Points clés

Cette expérimentation avait pour objectif de montrer l'influence du niveau de CI dans la prise de décision à l'aveugle, d'opérateur travaillant dans des environnements incertains. Pour pouvoir effectuer cette expérimentation le protocole expérimental utilisé tout au long de cette thèse a été modifié afin d'y incorporer une tâche de comptage de brouillages. Le participant devait à la fin de chaque essai indiquer le nombre de brouillages apparu sur son image et sur celle de son coéquipier (le coéquipier transmettait le nombre de brouillage qu'il avait lui-même perçu sur son image). Comparé aux autres expérimentations, le participant ne pouvait, en aucun cas, compter les brouillages perçus par son coéquipier. Afin de valider ou non le nombre de brouillages perçus par son coéquipier, le participant n'avait que deux informations :

- La consistance entre les brouillages reçus par lui-même et par son coéquipier (si les deux opérateurs avaient reçu des brouillages alors il y avait consistance sinon il n'y avait pas consistance) ;
- Le niveau de CI qu'il accordait au coéquipier.

Les résultats de cette expérimentation montrent que, dans une décision à l'aveugle, le niveau de CI présent dans la relation n'est pris en compte que dans le cas d'informations non consistantes. Dans le cas d'informations consistantes, le participant a pris des décisions similaires quel que soit le niveau de CI présent dans la relation. Par contre, dans le cas d'informations non consistantes le participant a plus facilement validé les informations transmises par le coéquipier lorsqu'il avait confiance en lui.

8 Discussion générale et perspectives

Chapitre 8 : Discussion générale

Ce chapitre se compose de 8 parties distinctes. La première partie correspond à un résumé global des différents objectifs de la thèse. Les cinq parties suivantes correspondent aux différents apports théoriques de la thèse à la littérature sur la confiance. La septième partie correspond à des recommandations portant la mise en place de la RCPair. Enfin, dans la dernière partie, différentes perspectives sont proposées.

1. Résumé de la thèse

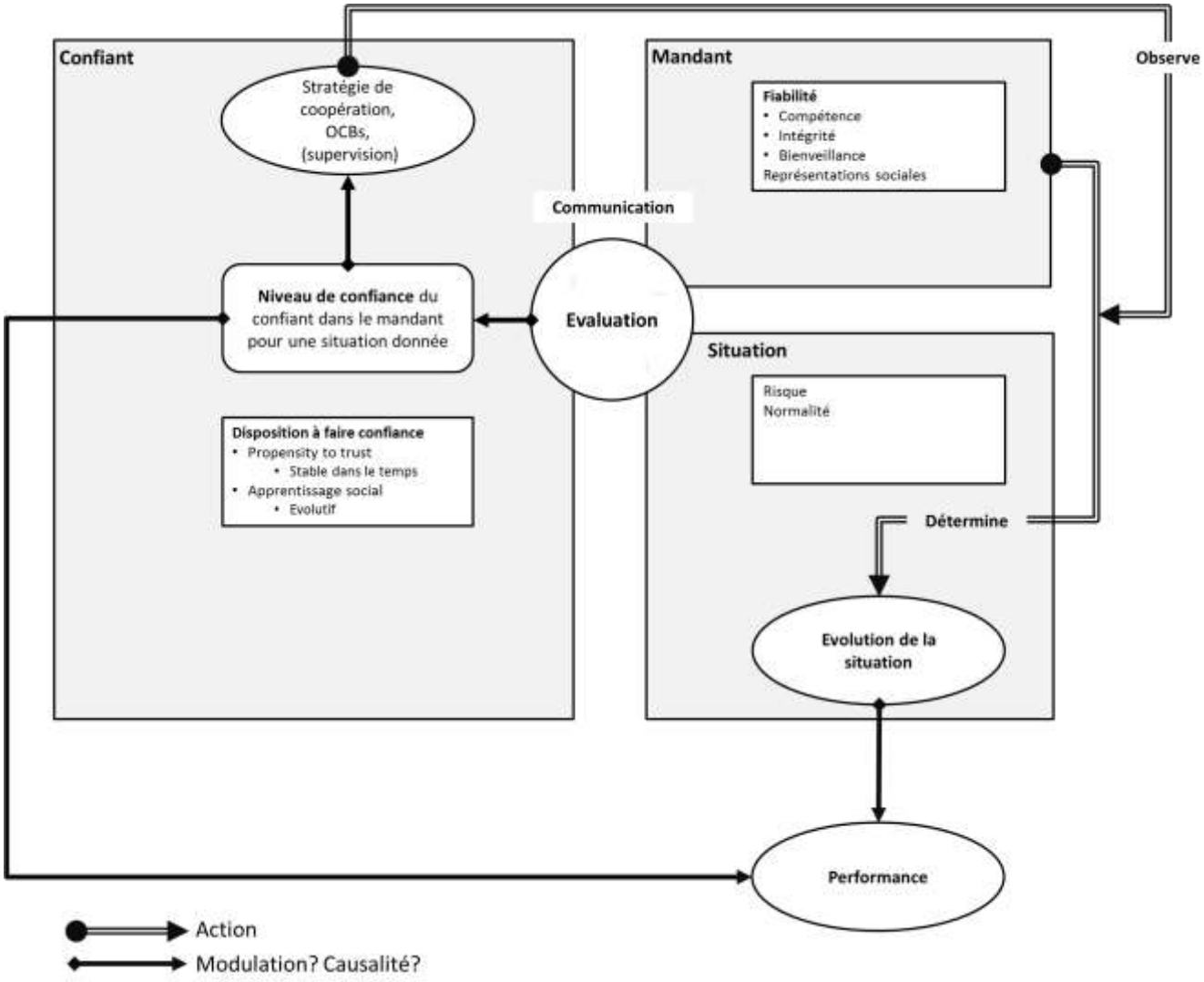


Figure 70 : Modèle provisoire proposé dans l'état de l'art

La problématique de cette thèse portait sur les conséquences comportementales induites par une variation du niveau de confiance interpersonnelle sur les opérateurs travaillant en équipes éphémères et recevant des données soumises à une forte incertitude. Basée sur une approche expérimentale, le cadre de la gestion de la cyber sécurité au sein des C2airs a été choisi pour appréhender les rôles, les tâches mais également les liens entre les différents opérateurs. Cette

problématique était donc construite d'une part autour d'une partie opérationnelle qui correspond à un système socio-technique particulier (les opérateurs travaillant dans la RCPair, recevant des données soumises à une forte incertitude) qui est en cours de définition au sein de l'armée de l'air et que l'on cherche à optimiser. D'autre part elle comprenait un volet académique (étude des conséquences comportementales induites par une variation du niveau de confiance) permettant de mettre ces résultats expérimentaux en regard des diverses connaissances sur la confiance et faire ainsi évoluer les modèles proposés. Pour répondre à la partie opérationnelle de cette thèse, une analyse du besoin a été réalisée auprès d'opérationnels de l'armée de l'air afin de préciser l'organisation et les attendus de ce système en cours de définition. Elle a permis de montrer la nécessité d'intégrer, dans les C2air, une représentation de la situation cyber (nommée RCPair), dédiée à un opérateur cyber, qui viendra s'ajouter aux outils actuels qui permettent d'obtenir une représentation de la situation aérienne et qui sont dédiés à un opérateur air. La communication entre les « mondes » cyber et air par le biais du partage d'informations permettant de prendre des décisions, sera un point clé du fonctionnement du système sociotechnique, mais, est peu défini pour l'instant. Ce transfert d'informations pourrait être réalisé soit par le biais d'algorithmes, soit directement par les opérateurs impliqués dans la supervision cyber et air de la situation. Dans ce cadre applicatif, cette thèse s'est principalement focalisée sur le rôle de la confiance interpersonnelle présente entre les divers opérateurs mais a également abordée son rapport avec la confiance dans les données provenant d'un système automatisé. C'est un point de vue particulier sur ce système socio-technique qui peut permettre d'en optimiser certains aspects mais qui devra être complété par d'autres études, notamment sur la représentation des informations échangées. Pour atteindre nos objectifs, il a été nécessaire de mieux comprendre :

- [1] comment les caractéristiques psychosociales des différents opérateurs influaient sur leur relation de confiance avec d'autres opérateurs humains ;
- [2] dans quelle mesure le niveau de confiance interpersonnelle modifiait le comportement de l'opérateur ;
- [3] dans quelle mesure le niveau de confiance présent entre un opérateur humain et un système automatisé modifiait le comportement de l'opérateur humain ;
- [4] dans quelle mesure le niveau de CI et le type de situation modifiaient les décisions des opérateurs.

Afin d'analyser ces différentes relations, un état de l'art académique portant sur la confiance est présenté au deuxième chapitre de ce manuscrit. Cet état de l'art a montré que pour qu'il y ait confiance, il faut *a minima* trois entités distinctes : un confiant, un mandant et une situation. La relation de confiance devient importante lorsque le confiant a besoin du mandant pour que ce dernier agisse sur une situation donnée. Cet état l'art permet de mettre en évidence que selon le type d'équipes étudiées, la confiance peut être un processus statique (confiance rapide mise en place dans le cadre d'équipes STATs) ou dynamique (dans le cadre d'équipes qui évoluent ensemble au cours du temps). Cependant, quel que soit le type de confiance mis en place (statique ou dynamique), une modulation du niveau de confiance entraine une modulation du comportement des individus (*Cf. infra* « Apports théoriques de la thèse à la connaissance des comportements engendrés par différents niveaux de confiance interpersonnelle »).

Cet état de l'art permet également de montrer que ces trois entités ne sont pas étudiées dans tous les champs de la littérature. Dans la littérature managériale par exemple, les caractéristiques et les liens entre le confiant et le mandant sont majoritairement étudiés en neutralisant la situation (généralement une situation de travail d'équipe entre un leader et son subordonné). D'un autre côté, dans la littérature économique, le rôle de la situation est majoritairement étudié. Autrement dit, beaucoup de modèles sont centrés sur une ou plusieurs de ces entités mais aucun

d'eux ne parait complètement adapté à l'étude de la confiance dans le système sociotechnique visé. Dans l'objectif d'étudier ces liens, et sur la base de ces différentes littératures, un modèle relativement générique articulant l'ensemble des éléments et des liens qu'il est nécessaire d'investiguer est proposé à la fin du deuxième chapitre (*Cf.* Figure 70). Ce modèle, basé sur l'approche statique de la confiance, présente les caractéristiques propres au confiant, au mandant et à la situation, et permet de décrire les liens entre les trois entités mais également entre niveau de confiance et comportement.

Afin de répondre à la problématique qui porte sur les conséquences comportementales d'un niveau faible ou élevé de confiance interpersonnelle, il est nécessaire d'analyser les comportements engendrés par différents niveaux de confiance interpersonnelle. L'état de l'art montre que très peu de modulations comportementales sont étudiées dans la littérature qui décrit seulement la confiance interpersonnelle comme étant un modulateur du nombre de supervision et de la performance. Cependant, l'analyse de la littérature montre que ces conséquences comportementales (supervision et performance) sont, dans la majorité des cas, étudiées en management. Or, dans cette discipline, la tâche principale du confiant est de superviser le mandant alors que dans le système sociotechnique étudié dans cette thèse, l'opérateur a une tâche spécifique de surveillance de systèmes, une tâche de coopération/supervision d'autres opérateurs ainsi qu'un rôle décisionnaire. Il est donc nécessaire de préciser les effets de la confiance sur le comportement de l'opérateur dans ces différentes tâches. Pour ce faire, la démarche de la thèse est :

- De chercher à induire différents niveaux de CI mais également différents niveaux de confiance dans la machine ;
- D'étudier l'influence des caractéristiques propres au confiant dans le comportement engendré par différents niveaux de confiance (permettant de répondre à l'objectif [1]) ;
- D'étudier le comportement des opérateurs travaillant avec d'autres opérateurs humains plus ou moins dignes de confiance (permettant de répondre à l'objectif [2]) ;
- D'étudier le comportement des opérateurs travaillant avec un système automatisé plus ou moins dignes de confiance (permettant de répondre à l'objectif [3]) ;
- D'étudier l'influence des caractéristiques de la situation et du niveau de confiance dans la prise de décision du confiant (permettant de répondre à l'objectif [4]).

Plusieurs expérimentations ont été réalisées et ont permis d'étudier toutes les parties du modèle présenté à la figure 70 et ainsi de faire évoluer les connaissances académiques portant sur la confiance. Le modèle final, obtenu grâce aux résultats des expérimentations est présenté à la figure 71. Tous les liens et caractères en bleu ont été étudiés au cours de cette thèse. Toutefois, les liens, tels que présentés dans ce modèle n'engagent que les stratégies de confiance mises en place en travail collaboratif tel qu'il peut être effectué dans les C2air.

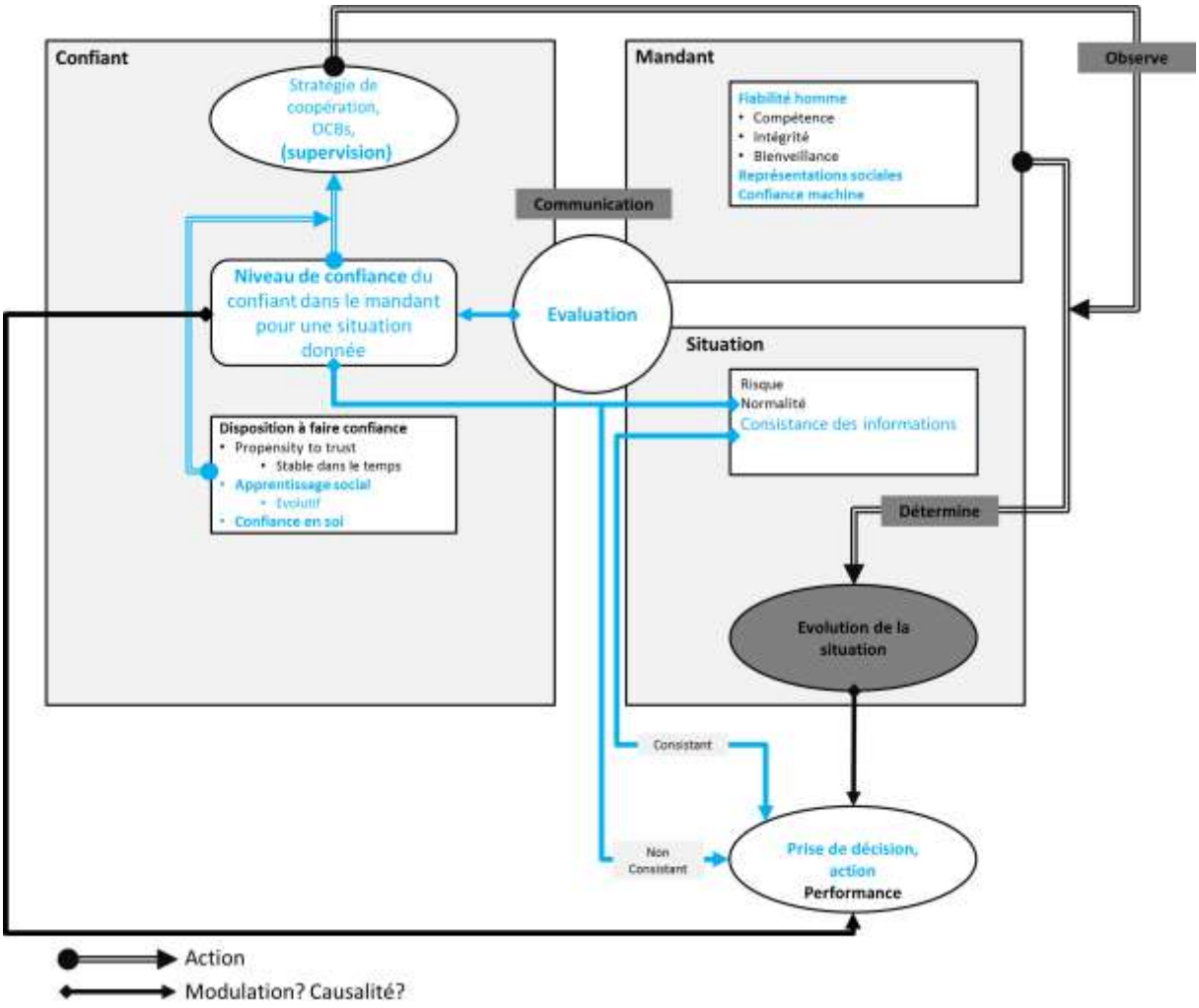


Figure 71 : Modèle prenant en compte les résultats obtenus dans cette thèse

2. Apports méthodologiques de la thèse aux méthodes d'induction de confiance en laboratoire

Durant cette thèse deux moyens d'induction ont été utilisés. Le premier moyen d'induction se basait sur les représentations sociales du mandant et l'apprentissage social du confiant. L'idée sous-jacente à ce type d'induction était qu'il était possible d'induire différents niveaux de confiance interpersonnelle en montrant à un confiant, des représentations sociales de mandant plus ou moins dignes de confiance. Les résultats des différentes expérimentations montrent que cette méthode d'induction est fonctionnelle. En effet, dans toutes les expérimentations réalisées dans cette thèse, une augmentation du niveau de confiance interpersonnelle induit par la méthode des représentations sociales a entrainé une augmentation du score que le confiant a attribué à la performance du mandant, *et vice versa.* Cette méthode d'induction semble donc avoir fonctionné sur

les 239 opérationnels de l'armée de l'air et les 40 élèves ingénieurs qui ont participé aux différentes expérimentations de cette thèse.

Malgré l'efficacité indiquée par ces résultats homogènes, cette méthode d'induction a certaines limites. Tout d'abord, elle a été construite et testée uniquement sur des groupes sociaux pouvant être considérés comme relativement proches. En effet, les différents individus ayant participé aux expérimentations étaient tous des français ayant un âge compris entre 20 et 45 ans et travaillant (ou formés à travailler) en équipes. De fait, rien ne permet d'affirmer que cette méthode proposant des paires de mots pourrait fonctionner de manière similaire sur d'autres populations très éloignées de celles étudiées ici (par exemple des personnes ayant une autre langue, une autre culture, provenant d'un autre pays ou d'un autre continent et travaillant seul). Afin d'induire différents niveaux de confiance interpersonnelle à d'autres groupes sociaux il serait peut être nécessaire de tester les RS de ces nouveaux groupes sociaux afin de créer des inducteurs spécifiques à ce nouveau groupe social puis de tester le bon fonctionnement de ces représentations sociales. Ceci reviendrait, en quelque sorte, à refaire la majeure partie de la démarche présentée aux chapitres 3. Dans le cas d'une campagne d'expérimentation plus courte que celle présentée dans ce manuscrit cela pourrait s'avérer extrêmement couteux.

De plus, le fait que cette méthode d'induction utilise des paires de mots entraine une limitation dans le « nombre » de niveaux de confiance interpersonnelle pouvant être induits. L'utilisation d'une paire de mots ne donne pas beaucoup de latitude pour moduler l'activation des RS du confiant et certains mots peuvent peut-être influer plus ou moins fortement certaines personnes. Dans les différentes expérimentations les paires de mots ont été regroupées en grandes classes de niveaux de confiance interpersonnelle induits (deux ou trois classes selon les expérimentations). Cependant, bien que les niveaux d'induction aient été vérifiés lors de la construction des paires de mots le « poids » de chaque mot au sein de la paire n'a pas été vérifié lors de la mise en place des différents niveaux de confiance interpersonnelle. Dès lors, il est possible que certains mots de la classe confiance interpersonnelle élevée induisent de plus hauts niveaux de confiance interpersonnelle que d'autres mots de la même classe. Cette différence possible de niveau d'induction de chaque mot isolément et le fait que seuls des regroupements par paire aient été effectués peut expliquer notamment pourquoi il a été impossible d'induire un niveau de confiance intermédiaire avec cette méthode (ce niveau intermédiaire a d'ailleurs été supprimé dans les expérimentations 3 et 4). Il est possible qu'en construisant des patterns de mots plus complexes (utiliser 3, 4 ou un grand nombre de mots) il puisse être possible d'induire un plus grand nombre de niveaux de confiance interpersonnelle. Pour résumer, à ce stade de développement, cette méthode semble fiable dans l'induction de niveaux de confiance interpersonnelle faibles ou élevés mais ne peut pas être utilisée pour induire une plus grande diversité de niveau, traduisant un *continuum* de confiance.

Le deuxième moyen d'induction a consisté à considérer qu'il était possible d'induire différents niveaux de confiance en présentant au confiant, des pourcentages de fiabilité auto-évalués et transmis par le mandant. Contrairement à l'approche par paire de mots qui se basait sur les représentations sociales et ne pouvait par conséquent, qu'induire des niveaux de confiance envers une autre personne. Dans l'approche utilisée pour l'expérimentation 2 le mandant pouvait tout aussi bien être un opérateur humain qu'un système automatisé. La comparaison effectuée entre les résultats obtenues par la méthode des paires de mots et ceux obtenues par la méthode d'induction par fiabilité transmises par un opérateur humain montre que ces deux méthodes d'inductions

induisent bien des comportements similaires. Ces résultats, tendent donc à montrer que le pourcentage de fiabilité transmis par un opérateur humain induit bien un niveau de confiance interpersonnelle. Les résultats obtenus en comparant les deux méthodes d'induction par fiabilité (transmises par un opérateur humain et transmis par un système automatisé) tendent à montrer qu'il est possible d'induire différents niveaux de confiance interpersonnelle mais également de confiance dans la machine en utilisant la méthode de la fiabilité transmise. Cependant, ce résultat demande à être confirmé par d'autres études.

Dans l'expérimentation 2, l'induction d'un niveau faible de confiance correspondait à un pourcentage de fiabilité compris entre 71 et 79%, le niveau de confiance intermédiaire était compris entre 81 et 89% et le niveau élevé entre 91 et 99%. Outre le fait que cette méthode soit utilisable à la fois dans l'induction de confiance interpersonnelle et dans l'induction de confiance dans la machine, le fait que les « plages » de pourcentage de fiabilité ne se recoupent pas permet une meilleure maitrise et anticipation du niveau d'induction. Comparés à la méthode des RS, l'utilisation du pourcentage de fiabilité a d'ailleurs permis d'induire trois niveaux de confiance bien distincts. Toutefois, dans les inductions utilisées dans l'expérimentation 2, le niveau de confiance faible (compris entre 71 et 79%) est relativement élevé et pourrait donc correspondre à un niveau de confiance interpersonnelle élevé. Dès lors, il est fort probable que les différences de hauteurs de courbes obtenues entre la méthode d'induction par paire de mots et par pourcentage de fiabilité humain-humain soient en partie dues au fait que le niveau de confiance interpersonnelle faible induit par la méthode de pourcentage de fiabilité soit équivalent au niveau de confiance interpersonnelle élevé induit par la méthode des paires de mots. Il pourrait donc être intéressant de refaire passer l'expérimentation 2 en baissant, peu à peu, les niveaux de fiabilité transmis. Ceci permettrait de vérifier la possibilité de rapprocher les courbes comportementales obtenues avec la méthode d'induction par paire de mots et la méthode d'induction par pourcentage de fiabilité. De plus, en diminuant peu à peu le pourcentage de fiabilité il pourrait être possible de vérifier la linéarité, ou non, de la relation entre niveau de confiance et comportement. En effet, le niveau de confiance pourrait, par exemple, tout aussi bien moduler le comportement de manière continue entre 0 et 100 ou entre 50 et 100 (une fiabilité inférieure à 50 % pourrait induire, quoi qu'il arrive, un même niveau de confiance). De nouvelles expérimentations allant dans ce sens devraient être menées sur différents groupes sociaux et dans différentes situations afin de pouvoir étudier le niveau de confiance « idéal », qui n'est probablement pas un niveau maximal de confiance (Karsenty, 2015; Parasuraman et al., 1993), permettant d'optimiser la performance.

Enfin, comme vu dans l'état de l'art, dans la littérature psychologique une induction par visages est utilisée. Dans ce type d'induction, des visages, qu'ils soient réels et tirés de vraies photographies (Klapper et al., 2016; Rule et al., 2013; Slepian & Ames, 2016; Willis & Todorov, 2006) ou créés ou modifiés par ordinateur (Klapper et al., 2016; Marzi et al., 2014; Oosterhof & Todorov, 2008; Schul et al., 2004; Todorov et al., 2015) sont montrés au confiant afin d'induire différents niveaux de confiance. Ce type d'induction semble fonctionner sur des tâches très courtes (<500 ms) mais il pourrait être intéressant d'associer ce type d'induction au protocole expérimental présenté dans cette thèse afin de comparer les résultats avec ceux obtenus *via* d'autres méthodes d'induction. En faisant cela, il serait possible de montrer les limites et les avantages des différentes méthodes et montrer quelles sont les méthodes les plus adaptées à l'étude en fonction du contexte choisi.

3. Apports théoriques de la thèse aux liens entre confiance interpersonnelle et de la confiance dans la machine

Les champs de recherche relatifs à la confiance dans la machine et à la confiance interpersonnelle sont tous issus des travaux menés en psychologie et en sociologie (Deutsch, 1958; Möllering, 2001; Simmel, 1950). Cette base commune entraine des définitions et des concepts communs sur la notion de confiance. Cependant, malgré cette base commune, les résultats obtenus dans une des littératures ne sont pas utilisés voire même considérés dans l'autre. Par exemple, les liens entre niveau de confiance et supervision ou entre niveau de confiance et performance ont été étudiés parallèlement entre les deux littératures pour donner des résultats similaires (un lien entre niveau de confiance dans la machine ou de confiance interpersonnelle, comportement de supervision et performances) sans qu'aucun rapprochement entre les différentes conclusions obtenues n'ait été effectué. De fait, certaines avancées effectuées dans le champ de recherche portant sur la confiance dans la machine ne sont probablement pas prises en compte dans les recherches portant sur la confiance interpersonnelle et inversement. Ceci peut être dommageable notamment car, par son positionnement, la littérature sur la confiance dans la machine s'intéresse principalement aux caractéristiques propre aux confiants. En effet, dans la confiance dans la machine, le mandant est toujours un système ce qui ne permet pas d'étudier les différents attributs de la fiabilité qui sont décrits dans la littérature sur la confiance interpersonnelle. Par conséquent la littérature portant sur la confiance dans la machine a développée des connaissances plus avancées au sujet du confiant. La confiance dans la machine étudie notamment le rôle du niveau de confiance en soi dans le comportement du confiant alors que cette orientation semble moins étudiée dans la littérature sur la confiance interpersonnelle.

Une des causes de cette absence d'interrelation entre les deux littératures pourrait provenir de l'absence de protocole permettant de « confronter », dans le domaine de la confiance, ces deux littératures. Cette mise en relation existe pourtant dans d'autres domaines, notamment celui de l'agentivité. Cette littérature a par exemple mis en évidence que les représentations que se faisaient un opérateur des actions effectuées par son coéquipier étaient différentes selon que ce coéquipier soit un humain ou un système automatisé (Sahaï, Desantis, Grynszpan, Pacherie, & Berberian, 2019). Cependant, de tels résultats n'ont pu être observés que grâce à l'utilisation de paradigmes provenant de littératures différentes. Dans notre cas, afin de voir si les comportements engendrés par un manque de confiance interpersonnelle et de confiance dans la machine sont ou non « similaires » une expérimentation permettant de « confronter » les deux littératures, avec un seul et même protocole et une seule et même méthode d'induction a été effectuée. Les résultats obtenus dans l'expérimentation 2 tendent à montrer que les comportements engendrés par un niveau haut ou bas de confiance interpersonnelle ou par un niveau haut ou bas de confiance dans la machine sont strictement comparables pour la tâche choisie. Dès lors, ces résultats suggèrent que les avancées effectuées dans un champ de recherche pourraient être utilisées dans l'autre champ de

recherche (et inversement). Etant donné que l'axe principal de cette thèse était la confiance interpersonnelle, l'état de l'art sur la confiance dans la machine présenté est relativement succinct. Il serait intéressant d'approfondir cet état de l'art afin de regarder les similitudes et différences, notamment en termes de comportement, obtenues dans les deux littératures. Cela pourrait ouvrir de nouveaux champs d'études ayant déjà des bases théoriques et expérimentales.

4. Apports théoriques de la thèse à la connaissance des caractéristiques propres au confiant

Les résultats obtenus lors des expérimentations 1 et 3 apportent des informations sur le rôle des caractéristiques du confiant tant au niveau de la mise en place du niveau de CI qu'au niveau des comportements engendrés par ces niveaux de CI. Dans l'expérimentation 1, les caractéristiques psychosociales du confiant (expérience dans le métier, métier, environnement de travail) ont été variées. Les résultats de cette expérimentation tendent à montrer que le niveau de confiance initial présent dans une relation ne dépend pas des caractéristiques psychosociales du confiant. Cependant, les résultats de cette expérimentation montrent que la modification comportementale engendrée par le niveau de confiance semble, quant à elle, dépendante des caractéristiques psychosociales du confiant.

Ce lien entre caractéristiques psychosociales du confiant, niveau de confiance interpersonnelle et comportement de l'individu semble aller à l'encontre des modèles existants. En effet, les différentes littératures sur la confiance indiquent un lien direct entre le niveau de confiance présent dans la relation et le comportement des individus, alors que les résultats des expérimentations 1 et 3 montrent l'existence d'un lien indirect pouvant être médié par différentes caractéristiques propres au confiant. Les caractéristiques étudiées ici sont l'expérience dans le métier, le métier lui-même, mais également l'environnement de travail du confiant. Les résultats des expérimentations 1 et 3 montrent, qu'à niveau égal de confiance interpersonnelle, les individus ont des comportements différents en fonction de ces différentes caractéristiques. Certains individus ont eu des comportements constants, soit totalement dépendants du niveau de confiance interpersonnelle présent dans la relation (élèves PN), soit sans aucun lien avec le niveau de confiance interpersonnelle présent dans la relation. Par exemple, des personnes avec un niveau de confiance en soi faible se comportaient comme si elles avaient toujours un niveau de confiance élevé envers leur coéquipier alors que d'autres individus (mécaniciens ayant fait des OPEX), se comportaient comme s'ils avaient toujours un niveau de confiance faible envers leur coéquipier (*Cf.*Tableau 31).

Tableau 31 : Matrice montrant, pour chaque groupe social, les comportements modulés par le niveau de CI dans l'expérimentation 1.
Les cases vertes indiquent que les comportements ont été significativement modulés par le niveau de CI présent dans la relation. Les cases orange montrent une absence de modulation significative

Variation du comportement en fonction du niveau de CI induit				
	Comportement de supervision	Comportement de gestion du temps	Comportement de modifications	Efficacité des supervisions
Elèves PN	V	V	V	V
Contrôleurs aériens	V	V	V	X
Mécaniciens (Base)	X	V	V	V
Mécaniciens (OPEX)	X	X	X	X
PN expérimentés	V	X	X	X

Les résultats de ces expérimentations montrent donc que, la prise en compte du niveau de confiance dans le comportement des individus n'est pas constante dans une population (ici l'aéronautique militaire) mais fonction des sous-populations étudiées (ici les élèves PN, les contrôleurs aériens, les différentes classes de mécaniciens et les PN expérimentés). Des grandes tendances ont été mises au jour notamment au niveau des métiers (les contrôleurs semblent avoir des comportements relativement stables), mais, les résultats suggèrent que le comportement est probablement multidimensionnel et lié à la tâche. Dans la première expérimentation nous avons considéré que tous les individus formant un même sous-groupe social avaient des savoirs, des savoir-faire et des traits de personnalité identiques propres à ce sous-groupe social (tous les individus ayant eu la même sélection et le même enseignement). Cependant, cela n'a pas été vérifié dans les différentes expérimentations présentées ici. Il est donc possible que certains traits de personnalités ou certaines caractéristiques puissent modifier le comportement de l'individu. Par conséquent, des expérimentations portant sur d'autres groupes sociaux ou prenant en compte d'autres facteurs spécifiques devraient être menées.

En plus de l'axe de recherche portant sur les caractéristiques psychosociales du confiant, un autre axe de recherche a été amorcé dans cette thèse. Cet axe de recherche provenant des travaux réalisés dans la littérature portant sur la CM visait à observer l'influence de la CS sur le comportement des

individus et a donné des résultats concluants. Cependant, le groupe social choisi pour cette expérience (les élèves ingénieurs) avait déjà des comportements spécifiques vis-à-vis du niveau de confiance (ce groupe social semblait superviser de manière équivalente quel que soit le niveau de confiance présent dans la relation). Ainsi, les résultats de l'expérimentation 3 suggèrent qu'il est possible de moduler le comportement des individus (sans moduler leur niveau de CI) en utilisant la méthode de renforcement positif ou négatif mais que le comportement est probablement également dépendant du groupe social.

L'ensemble des résultats montre que le modèle stipulant une relation directe entre le niveau de CI et le comportement doit être affiné. Pour une tâche donnée, il est mis en évidence que les conséquences de ce lien sur le comportement peuvent dépendre d'autres facteurs propres au confiant. Dans cette thèse, des facteurs tels que le groupe social d'appartenance ou le niveau de CS du confiant ont pu être isolés. Cependant d'autres recherches devraient être menées afin de déterminer d'autres facteurs pouvant moduler les conséquences comportementales engendrées par différents niveaux de CI. Ainsi, Il pourrait être intéressant d'investiguer sur le lien entre CI, caractéristiques du confiant et comportement dans d'autres contextes d'action et avec d'autres types de population ou en prenant en compte d'autres facteurs (traits de personnalités…).

5. Apports théoriques de la thèse a la connaissance des comportements engendrés par différents niveaux de confiance interpersonnelle

La littérature s'accorde sur le fait que la confiance est un modulateur de la performance de telle sorte qu'une augmentation du niveau de CI présent entre les membres d'une équipe, augmente la performance de l'équipe. Dans les différentes expérimentations réalisées dans cette thèse plusieurs mesures pourraient être considérées comme étant des mesures de la performance. C'est notamment le cas du temps mis par le participant à réaliser les tâches, du pourcentage de supervision contre-productives ou encore du pourcentage de mauvaises décisions (présente dans l'expérimentation 4). Les résultats des différentes expérimentations tendent à montrer que la confiance peut être un modulateur direct mais également indirect (*Cf.* résultats de l'expérimentation 4 portant sur la consistance des informations) de la performance. Cependant, la performance est par définition multifactorielle et dépendante de la tâche à accomplir. Par conséquent, les résultats des mesures de performance obtenus dans les différentes expérimentations ne peuvent pas être généralisés à d'autres tâches ou d'autres situations. Dans la tâche présentée ici nous avons déjà vu que le niveau de CI semblait moduler plus fortement la performance que la pression temporelle. Néanmoins, d'autres facteurs, tel que le stress ou encore le risque présent dans la prise de décision, pourraient moduler le lien entre CI et performance. Il serait donc intéressant d'effectuer de nouvelles expérimentations dans des tâches plus écologiques afin de regarder si d'autres facteurs permettraient, ou non, de moduler la performance plus fortement que le niveau de CI.

Outre ce lien entre confiance et performance, la littérature s'accorde sur le fait que la confiance est un modulateur de la supervision de telle sorte qu'une diminution du niveau de confiance entre un confiant et un mandant augmente le comportement de supervision du confiant. Dans la littérature, ce rôle de la confiance sur la supervision est couramment évoqué, cependant il est rarement étudié expérimentalement mais surtout rarement défini. La supervision peut être définie comme étant une action composée de deux facteurs distincts. Le premier facteur correspond à l'action de superviser et le deuxième facteur correspond au temps passé à superviser. La littérature actuelle sur la confiance semble confondre ces deux facteurs ce qui peut amener des problèmes d'interprétation des résultats. Par exemple, les conséquences, en termes de management, pourraient être tout à fait différentes selon que la confiance modifie « l'acte » de supervision ou le « temps » de supervision. En effet, une personne X peut superviser plus souvent une personne Y mais peut passer, en cumulé, moins de temps à superviser cette personne Y qu'elle en passe, à niveau de confiance égal, à superviser une personne Z. Au cours de cette thèse nous avons donc choisi d'analyser les deux comportements (acte de supervision et temps de supervision). Les résultats des expérimentations 1 et 2 tendent à montrer que le niveau de confiance module le pourcentage de supervision mais également le pourcentage de temps passé à superviser. Dès lors, ces résultats suggèrent qu'une diminution du niveau de confiance est liée à une augmentation du nombre de supervision mais, qu'en plus, ces supervisions sont temporellement plus longues.

Les résultats de l'expérimentation 1 montrent que cette double augmentation entraine un phénomène de compensation temporelle. La supervision semble venir non pas en « remplacement » mais en « complément » de la tâche principale des individus. Dans le contexte applicatif choisi, lorsque le niveau de confiance diminue les individus passent donc autant de temps à réaliser leur propre tâche mais vont plus superviser et passent plus de temps à superviser leur coéquipier ce qui fait que les individus passent, au global, plus de temps à travailler. Ce résultat semble assez important du fait que dans la littérature managériale (qui étudie le lien entre CI et supervision) la tâche de supervision est considérée comme l'une des tâches principale de l'opérateur (le manager). Ce résultat, non discuté dans la littérature sur la CI, peut poser question dans le contexte des STATs. Comme vu précédemment, dans les STATs, les membres de l'équipe sont généralement soumis à une forte pression temporelle et à une grande charge de travail. Dans certaines STATs militaires, dans lesquelles la survie des membres peut dépendre des compétences et actions des autres membres, une augmentation du nombre et du temps de supervisions de différents membres de l'équipe pourrait entrainer des conséquences extrêmement graves. Il semble donc fondamental de vérifier si les résultats obtenus sur le comportement de supervision pourraient être « retrouvés » dans un contexte écologique de STATs.

Enfin, les résultats de l'expérimentation 1 indiquent que le niveau de confiance module la prise en compte, par le confiant, des informations transmises par le mandant. Dans toutes les expérimentations, quel que soit le niveau de confiance induit la performance (transmettre au confiant le bon nombre d'aéronefs présent sur l'image) du mandant était équivalente et égale à 50%. Seulement, les résultats tendent à montrer que, malgré cela, le nombre de modifications effectuées par le confiant, sur les données envoyées par le mandant, augmentent lorsque le niveau de confiance diminue. La littérature s'accorde sur le fait que le niveau de confiance modifie la perception qu'à le confiant de la performance du mandant ; les résultats de cette thèse renforcent cet élément et montrent en plus que cette perception entraine probablement des mécanismes plus complexes.

Premièrement, cette perception semble entrainer un mécanisme de compensation qui se caractérise par le fait que le confiant modifie plus les informations transmises par le mandant lorsqu'il n'a pas confiance en lui. Deuxièmement, cette perception semble altérer la qualité de la supervision mise en place par le confiant qui est caractérisée, dans l'expérimentation 1, par la mesure du pourcentage de supervisions contre-productives. A notre connaissance, aucune étude n'avait montré le lien entre niveau de CI et comportements contre-productifs précis pour l'équipe.

Ce lien entre niveau de CI et comportements contre-productifs, s'il pouvait être prouvé dans d'autres champs disciplinaires, remettrait en cause le lien entre confiance et performance notamment dans les recherches managériales ; actuellement, dans cette littérature, c'est en grande partie la performance du mandant (e.g. le subordonné) qui caractérise la performance de l'équipe. La tâche du manager n'est pas d'agir sur la situation mais d'agir sur ses subordonnées afin qu'ils agissent au mieux sur la situation. Les résultats de cette thèse montrent que, lorsque le niveau de CI est faible, l'opérateur qui supervise l'autre « crée » ou « laisse passer » plus d'erreurs que lorsque le niveau de CI est élevé. Dès lors, il est possible qu'un manager, lorsqu'il n'a pas confiance en son subordonné, prenne des décisions contre-productives faisant baisser (involontairement) la performance de l'équipe.

6. Apports théoriques de la thèse a la connaissance du rôle de la situation dans la mise en place des comportements engendrés par différents niveaux de confiance interpersonnelle

Enfin, la dernière expérimentation de cette thèse s'est centrée sur le lien entre confiance, comportement et situation. Dans la littérature, la situation est uniquement caractérisée par sa notion de risque. Ainsi, dans la littérature managériale, plus le risque (d'échec par exemple) perçu dans une situation est élevé, plus le confiant a besoin du mandant pour réaliser une tâche. Dans la littérature économique, la relation de confiance est uniquement étudiée en termes de coût/bénéfice mais la caractéristique (risque) principale de la situation reste inchangée. Dans les différentes littératures c'est donc la notion de risque qui entraine la mise en place du niveau de confiance et les comportements qui en découlent. Dans cette thèse nous avons pris le parti d'analyser cette notion de risque comme une évaluation que le confiant fait des différents futurs possibles de la situation. Selon cette approche, si le confiant ne peut pas évaluer les différents futurs possibles de la situation il ne peut pas calculer le risque présent dans la situation. Dès lors, avec ce type d'approche, le niveau de confiance serait inutile car le risque serait incalculable. Afin de tester cette approche nous avons effectué une expérimentation (l'expérimentation 4) en plaçant le participant dans une situation dans

laquelle il lui était impossible de calculer une probabilité (réelle) quant à la survenue des évènements transmis par le mandant.

Les résultats de cette expérimentation tendent à montrer que, dans ce cas-là, le confiant essaye d'apposer une probabilité aux informations transmises par le mandant sur la base des évènements qu'il a lui-même perçu (quand bien même aucun lien ne serait présent entre les évènements). La prise en compte du niveau de confiance arrive alors en second plan. Ces résultats sont très intéressants dans l'étude des comportements des individus dans les environnements à forte incertitude, car ils indiquent que, dans ce type d'environnement, en l'absence d'information fiables portant sur la situation le confiant prendra des décisions sur la base de probabilités qu'il aura lui-même calculé et que, dans ce cas-là, le niveau de confiance ne sera pas la variable la plus importante dans la prise de décision.

7. Apport de la thèse à la RCPair

Au niveau opérationnel les résultats des différentes expérimentations apportent des informations utiles à la mise en place de la RCPair dans les C2air. Actuellement, les C2air sont en majorité constitués de contrôleurs aériens de formation qui sont en charge de créer une conscience de la situation Air. Les résultats de la première expérimentation indiquent que ces contrôleurs aériens ont des comportements (supervision, gestion du temps et acceptation des informations transmises par leurs coéquipiers) dépendants des niveaux de confiance présents dans la relation. La création et le maintien d'un niveau de confiance adapté au sein de l'équipe sera donc bien un levier permettant de favoriser le bon fonctionnement du C2air, tant dans le respect du rôle de chacun que dans la prise en compte de l'ensemble des informations pertinentes.

Le rôle premier des C2air repose sur le processus de prise de décision qui implique, de la part du décideur, une évaluation des futurs possibles de la situation. Il a été montré dans la quatrième expérimentation que lorsque les informations qui remontent au décideur sont consistantes et donc, se complètent ou se confirment entre elles, la décision est rapide et ne dépend pas de la confiance entre les acteurs. Par contre, quand ces informations ne sont pas consistantes entre elles la prise de décision est plus complexe et nos expérimentations montrent que, dans ce cas-là, le niveau de confiance entre les personnes a un impact sur la prise de décision. Dans le cas d'évènement cyber, la situation sera bien souvent celle de la confrontation d'informations non-consistantes provenant d'une part de la situation air et d'autre part de la situation cyber. D'après nos résultats, dans une telle situation la confiance entre les personnes impliquées aura donc toute son importance et devrait être un facteur qui influence tant le comportement des acteurs que la décision finale.

L'organisation des C2air utilisant la RCPair n'est actuellement pas figée. Le choix fait aura des répercussions sur le processus de prise de décision et sur l'importance relative de la confiance entre les opérateurs. Plusieurs possibilités sont maintenant explorées et il est proposé ici de leur associer quelques recommandations. Afin de faciliter la lecture, le C2air est étudié ici comme étant un CDC, ceci peut correspondre à une organisation de type *conflicted* ou *non conflicted C2*. Premièrement, le décideur final pourrait avoir, sur ses consoles, des informations air et des informations cyber. Dans ce cas-là, ce décideur final pourrait travailler sans lien direct avec l'opérateur de la RCP (*Cf.* « A » sur la figure 72) ou bien avoir quand même une communication dédiée avec le décideur cyber (*Cf.* « B » sur

la figure 72). Deuxièmement, le décideur final pourrait ne pas avoir d'informations cyber sur ses consoles. Dans ce cas-là, un décideur cyber, colocalisé ou non-colocalisé avec les autres opérateurs devrait communiquer les informations cyber au décideur final (*Cf.* « C » et « D » sur la figure 72). Il est à noter que dans tous les cas une communication directe existe avec le décideur air qui est physiquement présent dans le CDC.

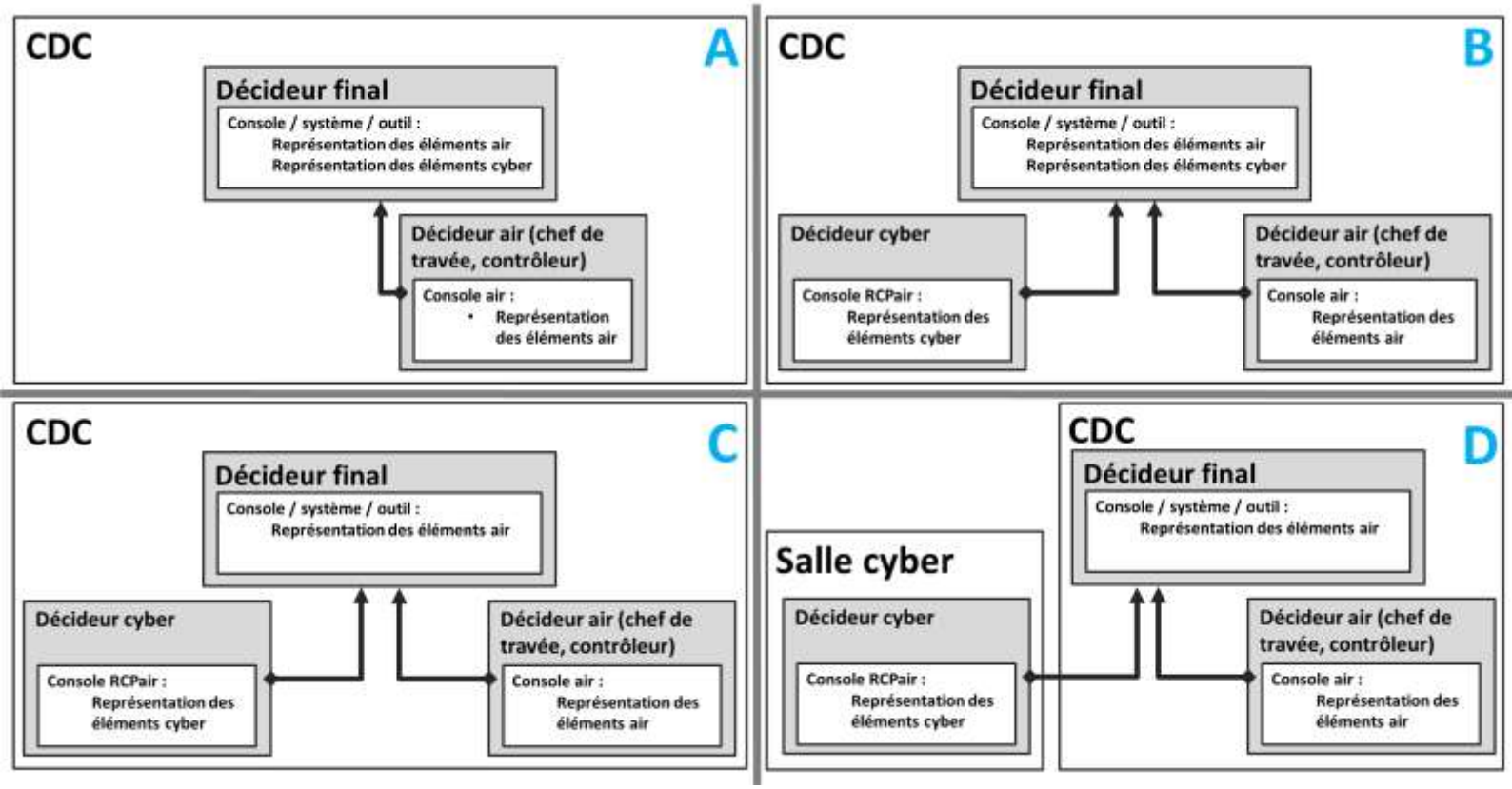


Figure 72 : Organisation possible des C2air utilisant la RCPair

Supposons que le système RCPair détecte une anomalie cyber, par exemple qu'une piste n'est probablement pas réelle mais simulée. Les informations air et cyber sont donc contradictoires. Les résultats des expérimentations indiquent que, dans ce cas-là, les différents niveaux de confiance présents dans la relation devraient avoir un impact sur la décision qui sera prise. L'enjeu premier est que l'information cyber, avec sa fiabilité et ses répercussions possibles, soit comprise par le décideur final afin de l'intégrer dans sa compréhension globale de la situation (la piste est réelle et constitue une menace directe, elle est fausse et sert de diversion pour focaliser l'attention et les moyens et permettre ainsi une intrusion à un autre endroit…). Dans ce cas-là, la question du partage, de la représentation et de la bonne prise en compte des informations cyber est double : d'abord au niveau du décideur final du CDC pour qu'il gère globalement la situation et les grandes décisions, ensuite au niveau de chaque opérateur (contrôleurs aériens…) afin qu'ils travaillent avec des données dont la fiabilité est modifiée par la situation cyber.

Dans le cas « A » illustré dans la figure 72, le fonctionnement est celui d'un C2air dont le décideur final est le chef du CDC. Celui-ci reçoit uniquement des informations provenant du décideur air (contrôleur aérien) puisqu'aucun décideur RCPair n'est présent. Sur sa console, le décideur final dispose des informations air mais également des informations cyber. Afin de prendre une décision, il devrait donc prendre en compte la donnée perçue comme ayant le plus haut niveau de confiance.

Dans ce cas-là, le décideur final, risque de prendre de manière préférentielle une décision allant dans le sens des informations air (une concordance étant présente entre les informations transmises directement par le décideur air présent dans le CDC et les informations air présentes sur la console air du décideur final). Afin de maximiser les chances que le décideur final puisse prendre en compte les informations provenant de la RCPair il serait nécessaire de le former aux risques cyber et au système RCPair. En effet, dans le cas « A », le décideur final aurait une formation de contrôleur aérien. Comme vu dans l'analyse du besoin, les contrôleurs aériens considèrent leurs consoles comme étant infaillible et n'arrivent pas à anticiper les problèmes liés à la cyber. Sans formation spécifique du décideur final au risque cyber et au fonctionnement de la RCPair (quelles données sont utilisées, que signifie une alarme…), une attaque cyber pourrait être mal interprétée ou sous-évaluée d'autant plus qu'elle correspondra nécessairement à un évènement rare. Une formation spécifique permettrait de rehausser le niveau de confiance qu'aura le décideur final dans les informations transmises par la RCPair et ainsi maximiser les chances que ces informations soient prises en compte dans la décision. Enfin, il pourrait également être possible d'optimiser la prise de décision en transférant, au décideur, des informations liées à la fiabilité et au risque d'une attaque cyber présente sur les données.

Dans le cas B illustré dans la figure 72, le fonctionnement est celui d'un C2air dont le décideur final est le chef du CDC. Celui-ci reçoit à la fois des informations en provenance du décideur de la RCPair et du décideur air (contrôleur aérien) qui sont tous deux dans la même structure. Sur sa console, le décideur final dispose également d'informations cyber et d'informations air. Dans ce cas-là, le décideur devrait prendre une décision basée sur les différents niveaux de confiance qu'il aura dans ses coéquipiers (décideur cyber et décideur air) mais également dans les informations transmises par la console (informations cyber et air). Afin de faciliter la prise de decision il est recommandé ici de s'assurer, dans un premier temps, que le niveau de confiance present entre le décideur final et le décideur cyber ne soit pas plus faible que le niveau de confiance présent entre le décideur final et le décideur air. En effet, en cas de différentiel de niveaux de confiance il est probable que la decision soit prise sur la base de l'information présentant le plus haut niveau de confiance. Dans un deuxème temps, il est recommandé de s'assurer que le niveau de confiance present entre le décideur final et les données cyber ne soit pas plus faible que le niveau de confiance présent entre le décideur final et les données air. Il a été vu que des informations sur le taux de fiabilité des données avaient un impact sur la confiance qui leur est associée. Il est donc recommandé que, dans ce type d'organisation, la transmission des informations de nature cyber entre la RCPair et la console du décideur final soit accompagnée de données complémentaires tant sur leur fiabilité que sur les risques associés. Ainsi, afin de faciliter la représentation de la situation, une piste ou des plots radars suspects, ou une piste « manquante » pourraient être directement affichés sur la console du décideur final assorties de ces informations complémentaires.

Dans les cas C et D illustrés par la figure 72, le fonctionnement est celui d'un C2air où il a été fait le choix de ne pas donner directement la console RCP ou les données cyber qui en sont issues au décideur final qui reste le chef du CDC. Celui-ci reçoit à la fois des informations en provenance du décideur de la RCPair et du décideur air (contrôleur aérien). Seulement, sur sa console, le décideur final ne dispose pas d'informations cyber, ces dernières n'ayant pas été intégrées dans sa console actuelle qui repose sur les éléments air. Dans le cas C, les résultats expérimentaux montrent qu'un des risques possibles de la colocalisation est que le décideur final cherche à contrôler les informations qui posent problème, en supervisant l'activité de celui qui les lui transmet. L'opérateur

cyber pourra alors justifier et argumenter ses informations afin de tenter de les « crédibiliser » auprès du décideur final. Cela pourrait permettre d'augmenter le niveau de confiance entre le décideur cyber et le décideur final, mais cela pourrait également inciter le décideur final à essayer d'analyser les informations cyber à la place du décideur cyber. Cette attitude légitime sera donc globalement contre-productive car le décideur cyber devrait être le mieux placé et le mieux formé pour évaluer la pertinence et la fiabilité des informations cyber. Dans le cas d'une cyberattaque, le temps mis par le décideur final à analyser la situation cyber ne serait pas utilisé pour agir sur la situation. Dans le cas D par contre, du fait de la non co-localisation du décideur final et du décideur cyber, il ne sera pas possible, pour le décider final, d'effectuer une supervision. Dans ce cas-là, le système de communication présent entre les deux décideurs et le niveau de confiance présent entre le décideur final et l'opérateur fournissant les éléments cyber seront fondamentaux pour la prise en compte des informations. Quel que soit le système de communication choisi il devrait être possible d'optimiser le fonctionnement du système sociotechnique en mettant en place des moyens permettant de donner au décideur final des informations sur la fiabilité des informations et la probabilité et les risques liés à l'évènement (*Cf.* conclusions des expérimentations 2 et 3).

Quelle que soit l'organisation utilisée, la transmission des informations air et cyber sera fondamentale afin d'optimiser la prise de décision. Cependant, le mode de transmission sera dépendant de l'organisation choisie. Ainsi, afin d'optimiser la prise de décision dans les C2air ayant une composante cyber il sera nécessaire, dans un premier temps, de déterminer si un décideur cyber sera ou non disponible. Une fois cela fait il sera nécessaire de déterminer les caractéristiques psychosociales des différents décideurs (air, cyber et final). Enfin, il faudra choisir des modes de transmissions de l'information adaptés à l'organisation et aux décideurs précédemment identifiés. En l'état actuel de nos connaissances, la première alternative (cas A sur la figure 72), ne nécessitant pas de recrutement particulier, semble être la plus simple à mettre en place. Seulement, du fait de l'absence de décideur cyber, dans cette alternative, les informations cybers risquent d'être sous évaluées par le décideur final. Afin que les informations cyber soient prise en compte il est préconisé qu'un décideur cyber puisse les transmettre directement au décideur final et que le niveau de confiance entre ces deux opérateurs soit élevé. Dans le cas où un décideur cyber bien indentifié peut communiquer avec le décideur final mais où il est impossible d'afficher des données cyber sur la console du décideur final, il pourrait être préférable, afin de limiter les risques liés à la supervision, qu'il n'y ait pas de colocalisation entre le décideur cyber et le décideur final.

8. Conclusions et perspectives

La littérature managériale déplore le manque d'études réalisées en laboratoire portant sur la confiance. En faisant un état de l'art de cette littérature on peut conclure que ceci est probablement dû à la complexité du phénomène de confiance qui demande pour être étudié, de prendre en compte les trois entités (le confiant, le mandant et la situation) et leurs interactions. Les différentes expérimentations présentées dans cette thèse contribuent à combler cette carence, dans la mesure où elles permettent d'étudier la confiance en isolant tour à tour chacune des trois entités dans un contexte précis. Les résultats des différentes expérimentations montrent qu'en induisant différents niveaux de confiance à différents confiant dans différentes situations, il est possible d'observer

certaines modifications comportementales. Etant donné qu'un seul facteur est « manipulé » dans chaque expérimentation (confiance interpersonnelle, confiance dans la machine ou confiance en soi), on peut conclure que ce facteur influe ou non sur le comportement (*Cf.* Figure 73). Certaines conclusions des expérimentations réalisées dans cette thèse vont dans le sens des observations déjà présentes dans la littérature (ceci est par exemple le cas du lien entre niveau de confiance interpersonnelle et comportement de supervision). Cependant, il semble que les conclusions des expérimentations effectuées dans les différentes littératures mais également des expérimentations présentées ici, pourraient être interprétées en utilisant un cadre théorique plus large. En effet, les conclusions présentées dans tous les champs de la littérature étudiant la confiance vont dans le sens de l'effet d'une seule « dimension » (confiance interpersonnelle, confiance dans la machine ou confiance en soi) de la confiance sur le comportement de l'individu. Dans la littérature portant sur la confiance interpersonnelle par exemple, c'est le niveau de confiance présent entre deux opérateurs humains qui modifie le comportement. Dans la littérature portant sur la confiance dans la machine, lorsque la machine est considérée fiable, c'est le niveau de confiance en soi de l'opérateur qui modifie le comportement. Dans cette même littérature, lorsque la machine est considérée comme pouvant être non fiable, c'est le niveau de confiance présent entre l'opérateur humain et le système automatisé qui modifie le comportement. Toutefois, la prise en compte de l'ensemble des résultats obtenus au cours de cette thèse montrent les limites de cette approche unidimensionnelle (un niveau d'une dimension de la confiance entraine un comportement) (*Cf.* Figure 73) et ouvrent le champ d'une approche multidimensionnelle de la confiance.

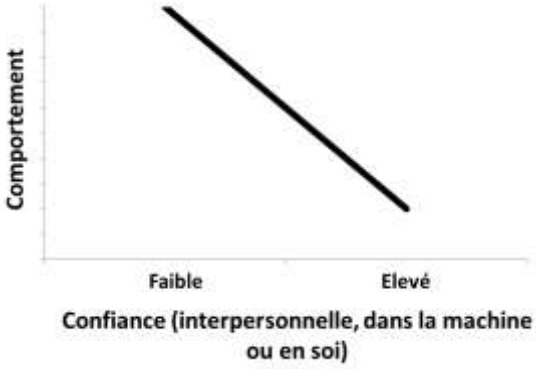


Figure 73 : Représentation de l'approche unidimensionnelle de la confiance.
Dans les expérimentations utilisant cette approche, l'expérimentateur observe si une modification du niveau d'une dimension de la confiance (interpersonnelle dans la machine ou en soi) module le comportement des participants

Les résultats de l'expérimentation 1 montrent que certaines caractéristiques propres au confiant modifient la prise en compte du niveau de confiance interpersonnelle dans son comportement. Ces résultats, analysés en utilisant une approche unidimensionnelle montrent un effet du niveau de confiance interpersonnelle sur le comportement de l'individu (en A sur la figure 74). Les résultats de l'expérimentation 2 montrent quant à eux qu'un niveau de fiabilité transmis par un système automatisé modifie le comportement de l'opérateur. Encore une fois, ces résultats, analysés avec une approche unidimensionnelle montrent un effet du niveau de confiance dans la machine sur le comportement de l'individu. En revanche, les résultats de l'expérimentation 3 ne peuvent pas être étudiés avec une approche unidimensionnelle et montrent, qu'en modifiant le niveau de confiance

en soi d'un confiant, il est possible de modifier sa prise en compte d'autres dimensions de confiance (ici la confiance interpersonnelle) dans son comportement (en B sur la figure 74).

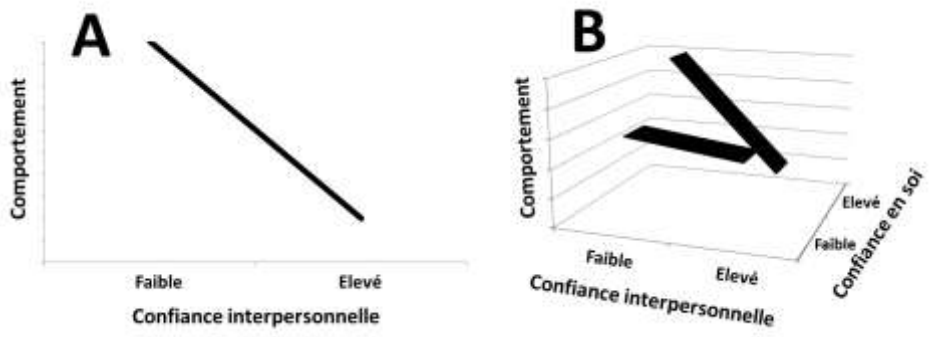


Figure 74 : Différences entre les approches unidimensionnelles (« A ») et multidimensionnelles (« B »).

Dans l'approche unidimensionnelle, une seule dimension de la confiance (interpersonnelle dans la machine ou en soi) est contrôlée. Dans l'approche multidimensionnelle, plusieurs dimensions de la confiance sont simultanément contrôlées. Dans cette deuxième approche, les différentes dimensions peuvent modifier le comportement, mais il est également possible, par exemple, qu'une dimension modifie la prise en compte de l'autre dimension. L'approche multidimensionnelle rend l'analyse des résultats plus complexe.

Dans les expérimentations réalisées dans les différents champs de la littérature (et dans les deux premières expérimentations de cette thèse) il est considéré, qu'entre un confiant et un mandant, il n'y a qu'une seule dimension de la confiance qui influe sur le comportement (celle modulée par l'expérimentateur) alors qu'il y en a en réalité, *a minima,* 2. La première correspond au niveau de confiance en soi du confiant et la deuxième correspond à celle qui est maitrisée par l'expérimentateur (confiance interpersonnelle ou confiance dans la machine). L'articulation de ces deux dimensions permet de moduler le comportement de l'individu. Cependant, cette articulation des confiances complexifie fortement l'analyse des résultats et leur interprétation. C'est pourquoi nous proposons ici le concept du « niveau de confiance intégrative » (le terme « intégrative » a été choisi afin de ne pas confondre ce concept avec d'autres comme celui de confiance générale qui correspond à « la perception que l'on peut compter sur les autres » (Siegrist, Keller, & Kiers, 2005)[46]).

Cette confiance intégrative correspond à une nouvelle « dimension » de la confiance prenant en compte l'articulation de toutes les dimensions de confiances présentes dans la relation. Cette confiance intégrative pourrait tout aussi bien être une somme, un ratio ou un produit des autres dimensions de confiance mais il est également possible que certaines dimensions (confiance dans la machine et confiance interpersonnelle par exemple) se combinent entre elles. Quoi qu'il en soit, selon cette approche, qui permet de faciliter l'analyse des résultats, c'est le niveau de confiance intégrative qui détermine le comportement de l'individu dans une situation donnée. La figure 75 représente une analyse de résultats unidimensionnelle (en A), bidimensionnelle (en B) et par confiance intégrative (C et D). Pour une situation donnée, des interprétations réalisées avec une approche unidimensionnelle peuvent être ré-analysées en prenant en compte l'intégralité des dimensions de la confiance. L'approche par confiance intégrative permet de passer d'une analyse à plusieurs dimensions à une analyse prenant en compte l'intégralité des dimensions de la confiance présente dans la relation. Enfin, en prenant en compte le facteur « situation » il est possible d'obtenir

[46] « the belief that other people can be relied on » (Siegrist, Keller, & Kiers, 2005)

une représentation des liens entre confiance intégrative comportement et situations (en D sur la figure 75). Dès lors, il parait nécessaire de clarifier comment les différentes confiances s'articulent afin de comprendre comment la confiance intégrative est mise en place et de pouvoir ainsi tester les différents comportements dans des tâches plus écologiques.

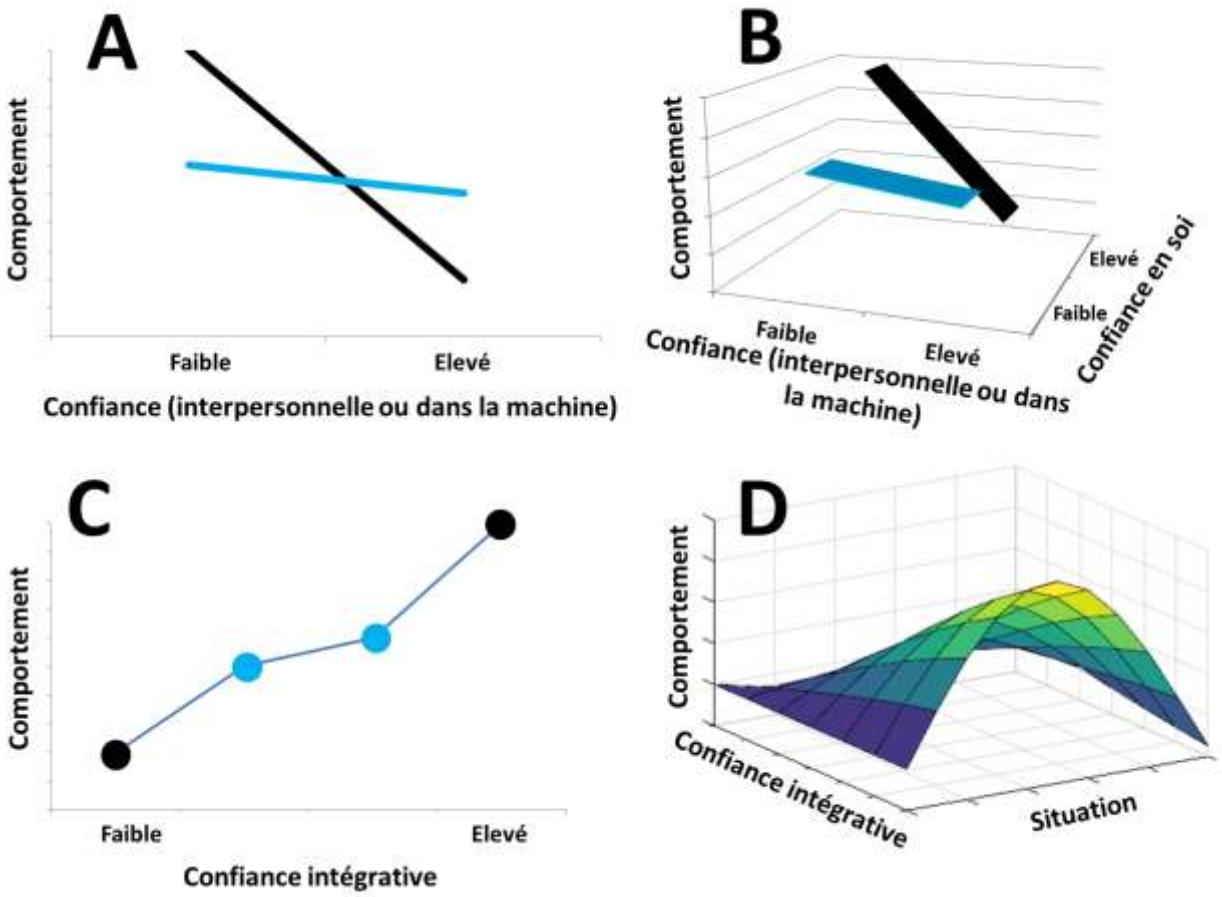


Figure 75 : Différentes possibilité d'analyse des comportements modifiés par le niveau de confiance.
En « A » l'approche unidimensionnelle qui est actuellement utilisée dans la littérature, montre une relation entre une dimension de la confiance et le comportement mais ne prend pas en compte les autres dimensions de la confiance qui peuvent pourtant avoir une influence aussi importante sur le comportement. Ces autres dimensions sont généralement non maitrisées ou non contrôlées dans ces expérimentations. En « B », l'approche bidimensionnelle permet d'analyser plus précisément les dimensions de la confiance modulant le comportement. Cependant, cette approche est complexe à mettre en place notamment pour la compréhension des résultats. En « C » l'approche par confiance intégrative permet d'observer distinctement le comportement modulé par différentes dimensions de confiances. En observant ce comportement dans un grand nombre de situation il devient possible d'obtenir une représentation plus « complète » (en « D ») du lien entre confiance comportement et situation.

Cette notion de confiance intégrative peut expliquer en partie pourquoi les résultats obtenus dans les différentes littératures semblent être parfois si différents, mais peut aussi permettre de mieux appréhender les résultats de l'expérimentation 1. Dans cette dernière, tous les participants, quel que soit leur groupe social, perçoivent l'induction des niveaux de confiance interpersonnelle mais ont des comportements différents. En analysant les résultats avec une approche unidimensionnelle, il semble que les caractéristiques du confiant modifient la prise en compte du niveau de confiance interpersonnelle dans son comportement. Cependant, en analysant les résultats selon l'approche de

la confiance intégrative, une conclusion différente peut émerger ; à niveau de confiance interpersonnelle perçue égal les différents groupes sociaux ont un niveau de confiance intégrative différent. Dès lors, les résultats comportementaux des PN expérimentés pourraient correspondre au fait que quel que soit le niveau de confiance interpersonnelle perçu (faible ou élevé) le niveau de confiance intégrative est toujours dans une plage faible (ce qui explique l'absence de différence comportementale). Les résultats obtenus auprès des élèves PN pourraient montrer la différence de comportement présente entre deux niveaux de confiance intégrative distincts (ici notés faible et élevé). Ainsi, en utilisant cette approche, on pourrait conclure que les résultats de l'expérimentation 1 montrent l'étendu des comportements sur une plage de confiance intégrative plus ou moins grande en fonction des groupes sociaux étudiés. Cependant, comme le niveau de confiance en soi et par conséquent le niveau de confiance intégrative, ayant entrainé les différentes modulations comportementales n'a pas été vérifié, il est impossible de connaitre l'étendue de cette plage de valeur. Les données obtenues en statistiques descriptives et inférentielles permettent de représenter schématiquement « l'emplacement » des différentes plages de valeurs des niveaux de confiance intégrative étudiées au cours de cette expérimentation (*Cf.* Figure 76).

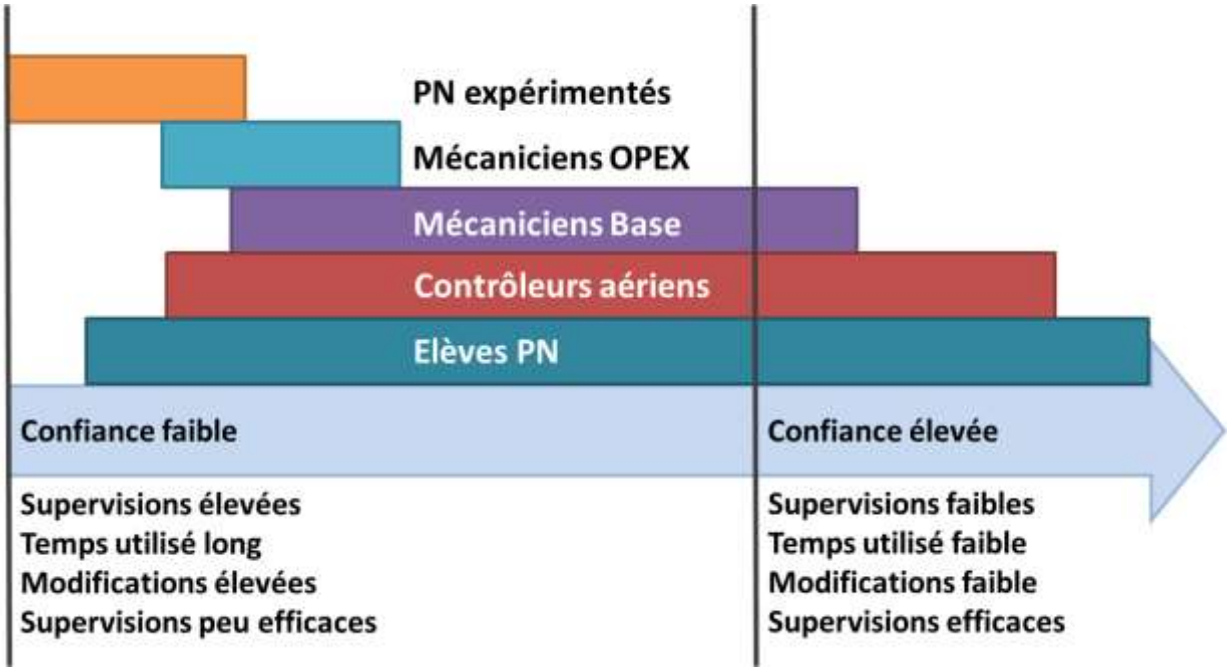


Figure 76 : Niveaux de confiance intégrative potentiellement étudiés dans chaque groupe social de l'expérimentation 1

En plus de cette notion d'intégration des dimensions de la confiance, une autre problèmatique issue de la forme des différents modèles, complexifie la mise en place d'études menées en laboratoires. L'ensemble des littératures décrivent que le confiant a besoin du mandant pour agir sur une situation ce qui peut être interprété de la manière suivante : « le confiant a besoin de percevoir que le mandant sera compétent pour agir sur la situation ». Ce fondement commun à toutes les études portant sur la confiance se caractérise par une dissociation entre les caractéristiques propres au confiant et les caractéristiques propres au mandant. Les caractéristiques propres au confiant correspondent à des « traits sociaux » (caractéristiques psychosociales qui influent sur sa disposition individuelle à faire confiance qui provient) alors que les caractéristiques propres au mandant correspondent à des compétences comportementales (habileté pour réaliser la tâche, intégrité et

bienveillance envers le confiant ou les institutions). Parallèlement, les compétences du confiant et l'influence des traits sociaux du mandant ne sont ni prises en considération, ni étudiées.

Dans les expérimentations réalisées de telle sorte à ce que le confiant et le mandant ne collaborent pas ensemble (les études réalisées en psychologie sur l'induction de confiance à l'aide de visages par exemple) cela ne devrait pas entrainer de biais. Cependant, dans les études réalisées en utilisant des tâches collaboratives, une prise en compte des compétences du confiant et des caractéristiques du mandant pourrait mener à de nouvelles conclusions. Par exemple, dans leur méta-analyse de 2016, De Jong et al. montrent que le lien entre confiance et performance se renforce avec l'interdépendance des tâches (Plus les tâches du confiant et du mandant sont dépendantes l'une de l'autre, plus le niveau de confiance modifie la performance de l'équipe)(De Jong et al., 2016) . Afin de montrer cela, De Jong et al. comparent des résultats obtenus dans des études réalisées dans des tâches fortement interdépendantes avec des résultats obtenus dans des études réalisées dans des tâches plus faiblement interdépendantes. Pour ces auteurs, la significativité obtenue sur cette comparaison montre un effet de l'interdépendance des tâches sur le lien entre confiance et performance. Cependant, si les compétences du confiant avaient été prises en compte, les résultats auraient pu montrer, par exemple, que le niveau de confiance module fortement la performance lorsque le confiant a les compétences pour agir sur les tâches du confiant.

Cette thèse a permis de montrer que les traits sociaux du mandant (autres que ses compétences supposées) étaient fondamentaux dans la mise en place du niveau de confiance interpersonnelle initial. Toutefois l'importance des compétences du confiant n'a pas été étudiée dans les différentes expérimentations présentées ici. A l'instar des études réalisées dans les différentes littératures une partie fondamentale de la confiance a été oubliée, à savoir sa réciprocité. En effet, dans la confiance, le confiant a besoin du mandant pour qu'il agisse sur une situation donnée mais la réciproque est souvent vraie ; si le mandant entre dans la relation de confiance c'est qu'il a besoin du confiant pour que ce dernier lui apporte quelque chose (agisse sur une situation, lui apporte des rétributions pécuniaires…). Dès lors, il est peut être nécessaire d'étudier conjointement les caractéristiques du confiant et du mandant afin d'avoir une vision plus exacte du processus de confiance. Cette intégration permet d'ajouter une composante comportementale aux caractéristiques propres au confiant, d'ajouter une composante sociale aux caractéristiques du mandant mais également de mieux appréhender la notion de confiance en soi. En effet, comme mentionné dans le cadre théorique (*Cf.* 2.5.A « a. caractéristiques propres au confiant »), la confiance en soi est une caractéristique propre au confiant qui a une composante sociale et une composante comportementale. De fait, il est relativement complexe de positionner cette confiance en soi dans les modèles actuels. En intégrant les caractéristiques du confiant et du mandant il devient possible d'intégrer la confiance en soi au nouveau modèle.

Ce nouveau modèle permet de faire apparaitre les différents liens et caractéristiques testés dans cette thèse (en noir sur la figure 77) mais permet également de voir les différents liens et caractéristiques qui devraient être testés afin de mieux étudier le processus de confiance (en couleur sur la figure 77). En analysant ce modèle il apparait que l'étude portant sur la mise en place du niveau de confiance intégrative vu plus haut, pourrait être utile pour tout type d'équipes. Ce niveau de confiance intégrative pourrait être le déterminant du comportement de l'équipe, quelle que soit son organisation (pyramidale ou non). Dans une organisation pyramidale, ce niveau de confiance intégrative pourrait dépendre uniquement des différentes dimensions de confiance propres au

confiant (le chef d'équipe ou le décideur) alors que dans des équipes organisées en grappe ce niveau de confiance intégrative pourrait dépendre de quatre (voire plus) dimensions de confiance différentes. En étudiant conjointement la dynamique de mise en place du niveau de confiance intégrative et le comportement associé à différents niveaux il serait possible d'anticiper le comportement (et donc les décisions) d'une équipe. Ceci permettrait, dans tout type d'environnement, de maximiser les comportements des individus en formant ces derniers aux conséquences comportementales engendrées par différents niveaux de confiance intégrative mais également en mettant en place des outils permettant de maximiser ces niveaux de confiance intégrative.

Comme vu dans les paragraphes précédents et comme le montre la figure 77, la mise en place de la confiance intégrative sera dépendante du lien présent entre les autres dimensions de la confiance et notamment dépendant de la confiance en soi du confiant. Toutefois, que ce soit au niveau de l'appellation (aucune appellation de la confiance en soi ne semble faire consensus dans la littérature anglophone), au niveau de sa mise en place ou encore au niveau de ses conséquences, la confiance en soi semble être un concept extrêmement peu étudié dans la littérature. Sur la base de ces observations, la dynamique de la confiance en soi et l'apport des différents niveaux de confiance à la mise en place de la confiance intégrative devraient être des champs d'études prioritaires.

La notion de confiance intégrative ne modifie pas le fondement même de la confiance qui est de faciliter et d'améliorer l'efficacité des décisions permettant d'agir sur une situation donnée. Sur cette base-là, les différentes littératures, et notamment celle portant sur les *STAT*s, laissent penser que le « besoin » de confiance présent dans une relation est dépendant du niveau de risque présent dans la mission ou la situation. Selon cette approche, plus la situation est risquée, plus le confiant a besoin de faire confiance au mandant. L'étude du modèle présenté à la figure 77 ne contredit pas cette affirmation mais y apporte une nuance fondamentale. En effet, même si le besoin de confiance est haut, le niveau de confiance intégrative est dépendant à la fois des caractéristiques et compétences du confiant et du mandant. Dès lors, même si la situation présente est extrêmement risquée, le niveau de confiance intégrative mis en œuvre pourrait être, en réalité, un niveau faible.

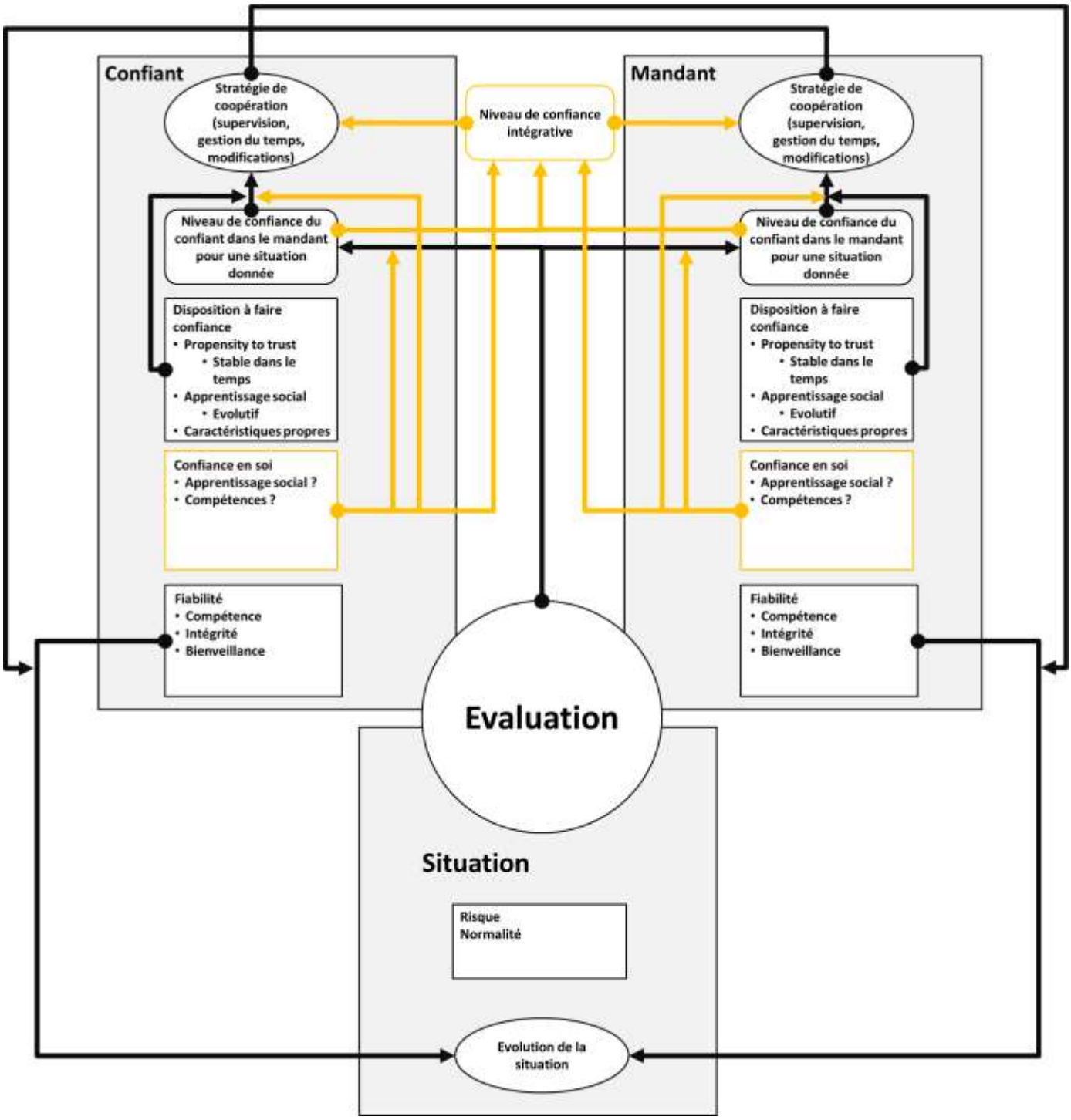


Figure 77 : Modèle représentant la mise en place du niveau de confiance intégrative en prenant en compte le principe de réciprocité.

L'intégration des différentes caractéristiques (*Cf.* Figure 77) permet de faire apparaitre un potentiel biais présent dans les différentes expérimentations menées dans les littératures sur la confiance, à savoir, celui de la « synchronisation ». En effet, comme le montre le modèle présenté à la figure 77, la supervision a pour but l'évaluation des actions effectuées par le mandant. Ainsi, pour que la

supervision soit efficace il est nécessaire qu'elle soit faite pendant que le mandant est en train de réaliser des actions sur la situation. L'effet de la confiance sur les supervisions contre-productives observé dans l'expérimentation 1 provient potentiellement de l'absence de synchronisation entre les actions du mandant et la supervision du confiant.

Les différentes expérimentations présentées dans cette thèse ont été réalisées sur la base d'un même protocole expérimental dans lequel le participant devait collaborer avec son coéquipier afin de réaliser une tâche donnée. Cependant, dans toutes les expérimentations présentées ici, le comportement ainsi que les erreurs faites par le coéquipier n'étaient pas « réels » mais pré enregistrés. Ceci a été rendu possible par le fait que les différentes expérimentations demandaient une collaboration asynchrone entre le participant et le coéquipier. Ce caractère asynchrone de l'expérimentation a possiblement créé des biais comportementaux. Il est par exemple possible que la supervision observée dans les différentes expérimentations soit en partie due à un choix du participant de « passer le temps » ou de « mettre à profit le maximum de temps imparti » ce qui expliquerait le pourcentage relativement élevé de supervisions contre-productives. Dans les différentes expérimentations, puisque le participant pouvait modifier le nombre total d'aéronefs comptés, une bonne supervision (compter le nombre d'aéronefs présents sur l'image du coéquipier), qu'elle soit faite au début, au milieu ou à la fin d'un essai donnait exactement les mêmes résultats. Pour éviter cela, il pourrait être intéressant de trouver une tâche demandant une collaboration synchrone du participant et du coéquipier afin de voir si les modulations comportementales observées durant cette thèse sont maintenues dans d'autres types de collaboration. Dans le cas d'une collaboration synchrone le participant devrait superviser « au bon moment » afin d'augmenter la performance d'équipe. Dans ce cas-là une supervision trop tardive ou trop en avance serait plus contre-productive que bénéfique à la performance d'équipe et pourrait donc modifier les différents niveaux de confiances présents dans la relation.

Afin de mettre en place une expérimentation avec collaboration synchrone il pourrait être nécessaire de regrouper les participants au même moment dans une ou plusieurs salles. Ceci pose le problème de la co-localisation des participants qui n'a pas été abordé dans cette thèse mais qui est également un possible biais des différentes expérimentations présentées ici. En effet, dans les trois premières expérimentations les participants étaient seuls devant leur ordinateur et les coéquipiers étaient simulés par cet ordinateur. Pour les expérimentations 4 et 5 en revanche, les participants étaient regroupés et avaient donc l'impression que les différents coéquipiers avec lesquels ils effectuaient l'expérimentation été présents au même moment. En comparant les données du nombre de supervision obtenues dans l'expérimentation 4 avec celles obtenues dans l'expérimentation 1, il apparait qu'il y a eu en moyenne, beaucoup plus de supervision dans l'expérimentation 1 (quel que soit le groupe social étudié) que dans l'expérimentation 4. Il est possible que cette différence soit due à la différence sociale entre les participants de ces deux expérimentations mais il est également possible que cette différence soit due à la co-localisation des participants. Afin de vérifier cela il pourrait être intéressant de passer une nouvelle fois l'expérimentation 1 avec des participants d'un des groupes sociaux ayant déjà passé cette expérimentation (élèves PN) en co-localisant les participants.

En comparant les données obtenues dans cette nouvelle condition expérimentale avec celles obtenues dans l'expérimentation 1, il pourrait ainsi être possible de voir si la co-localisation a un effet sur le niveau de confiance perçu ou sur le comportement. Observer le comportement des

individus dans une tâche asynchrone en co-localisation ou non co-localisation puis observer le comportement des individus dans une tâche synchrone en co-localisation ou non co-localisation pourrait apporter des informations sur la mise en place et le fonctionnement du niveau de confiance intégrative de l'équipe. Outre cela, un effet de la co-localisation sur le comportement des individus pourrait d'ores et déjà faire évoluer le cadre théorique de la confiance dans les STATs dont les membres peuvent être, dans certains cas, non co-localisés.

Rassembler les caractéristiques sociales et comportementales chez le confiant et le mandant permet également d'appréhender plus simplement les similitudes entre la confiance dans la machine et la confiance interpersonnelle. Actuellement ces deux littératures ne semblent pas se croiser. Cependant, en modifiant le modèle présenté à la figure 77 de telle sorte à ce que le mandant soit un système automatisé, aucun changement « fondamental » n'apparait. Ainsi, bien que cela soit probablement techniquement faisable, un système automatisé n'a en général pas de confiance en soi, ni de disposition à faire confiance ni même de niveau de confiance dans l'opérateur (ce qui enlève ces élèments du modèle) (*Cf.* Figure 78). Cependant, le système automatisé peut être défini par des caractéristiques qui lui sont propres (forme, taille, couleur, design…) mais également par les mêmes caractéristiques de la fiabilité qu'un opérateur humain. Un système peut, selon comment il a été codé, être plus ou moins intègre (transmettre la totalité des informations ou non à l'opérateur…) bienveillant (transférer des bons taux de fiabilité à l'opérateur ou modifier ces taux…) et compétent pour une tâche donnée. Dès lors, même si le système pouvait être « codé » afin de « rattraper » des erreurs commises par l'opérateur humain, la dynamique de la confiance devrait être similaire à celle présente dans une relation de confiance homme-homme (*Cf.* Figure 78). Les résultats de l'expérimentation 2 montrent déjà que dans une tache collaborative asynchrone, les comportements des opérateurs sont similaires qu'ils travaillent avec des coéquipiers humains ou avec un système automatisé. Ces résultats, s'ils étaient confirmés dans d'autres types de tâche mais également dans d'autres environnements, pourraient permettre de lier les deux types de confiance, et, à terme, servir les deux littératures.

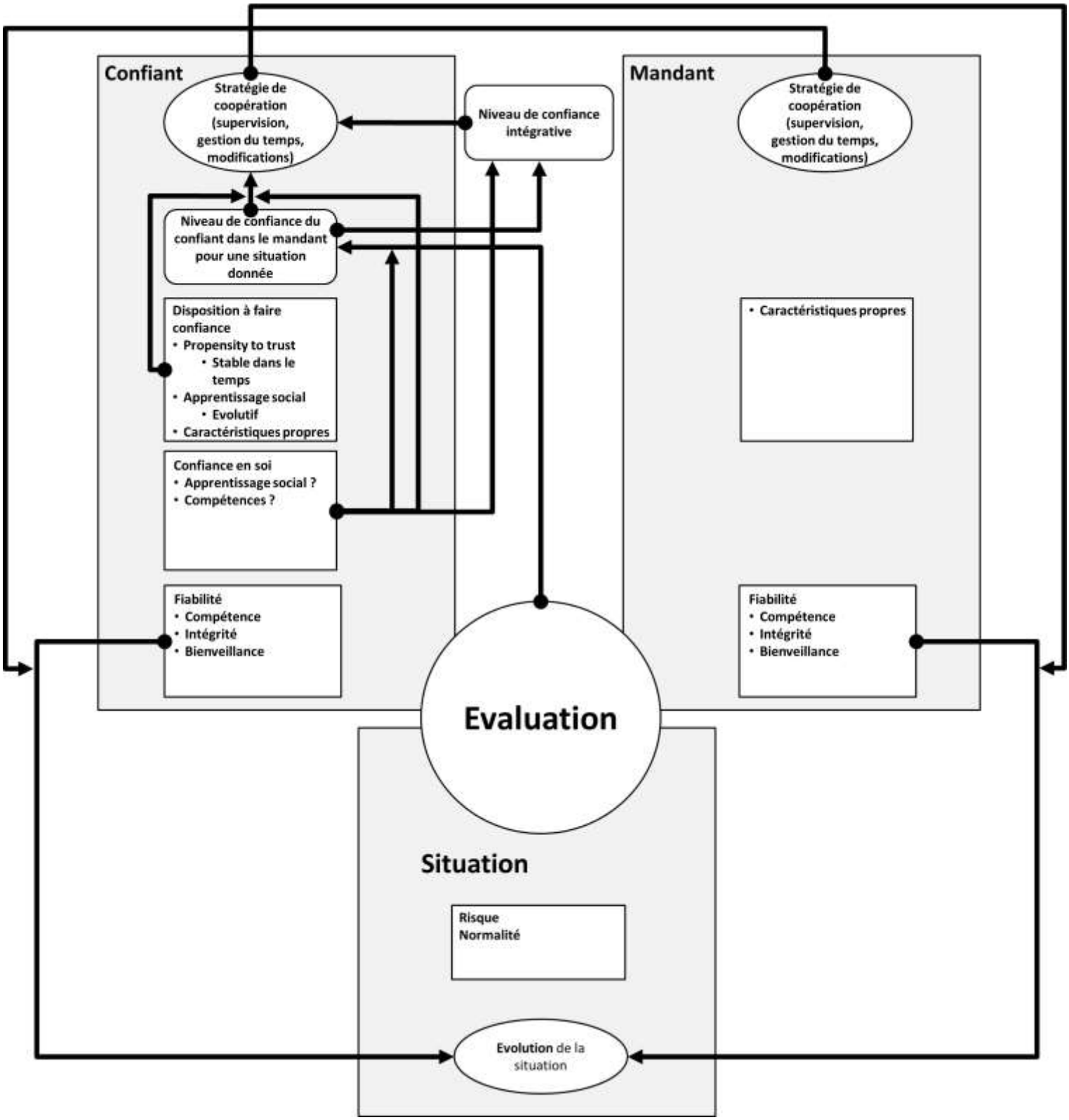


Figure 78 : Modèle, mis en place en se basant sur le principe de réciprocité, représentant la confiance dans la machine

Bibliographie

Bibliographie

Abric, J.C. (2003). *L'étude expérimentale des représentations sociales: Vol. 7e éd.* Presses Universitaires de France. https://www.cairn.info/les-representations-sociales--9782130537656-page-203.htm

Adali, S., Escriva, R., Goldberg, M. K., Hayvanovych, M., Magdon-Ismail, M., Szymanski, B. K., ... & Williams, G. (2010, May). Measuring behavioral trust in social networks. In *2010 IEEE International Conference on Intelligence and Security Informatics* (pp. 150-152). IEEE.

Adams, B. D., & Webb, R. D. (2002). Trust in Small Military Teams. *7th international command and control technology symposium*, 1‑20.

Adee, S. (2008). The Hunt For The Kill Switch. *IEEE Spectrum*, *45*(5), 34‑39. https://doi.org/10.1109/MSPEC.2008.4505310

Alarcon, G. M., Lyons, J. B., Christensen, J. C., Bowers, M. A., Klosterman, S. L., & Capiola, A. (2018). The role of propensity to trust and the five factor model across the trust process. *Journal of Research in Personality*, *75*, 69‑82. https://doi.org/10.1016/j.jrp.2018.05.006

Alberts, D.S., & Hayes, R. E. (2006). *Understanding command and control*. CCRP Publications.

Alberts, D.S., Huber, R. K., & Moffat, J. (2010). *NATO NEC C2 maturity model*. DoD Command and Control Research Program.

Alberts, D.S., & Hayes, R.E. (2003). Power to the Edge : Command...Control...in the Information Age. *OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE WASHINGTON DC COMMAND AND CONTROL RESEARCH PROGRAM (CCRP),* 297.

Alberts, D.S., Garstka, J. J., & Stein, F. P. (2000). *Network Centric Warfare : Developing and Leveraging Information Superiority*. https://apps.dtic.mil/dtic/tr/fulltext/u2/a406255.pdf

ANSSI. (2011). *Défense et sécurité des systèmes d'information Stratégie de la France*. https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

Armée de l'air. (2019). *Livret volfa*. https://www.defense.gouv.fr/content/download/569848/9793789/livret_volfa_BD_2019.pdf

Asenstorfer, J., Cox, T., & Wilksch, D. (2003). *Tactical data link systems and the australian defence force (ADF)-Technology developments and interoperability issues*. DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION SALISBURY (AUSTRALIA) INFO ….

Ashforth, B. E., & Mael, F. (1989). Social Identity Theory and the Organization. *The Academy of Management Review*, *14*(1), 20. https://doi.org/10.2307/258189

Ba, S., & Pavlou, P. A. (2002). Evidence of the Effect of Trust Building Technology in Electronic Markets : Price Premiums and Buyer Behavior. *MIS Quarterly*, *26*(3), 243. https://doi.org/10.2307/4132332

Bachmann, R., & Inkpen, A. C. (2011). Understanding Institutional-based Trust Building Processes in Inter-organizational Relationships. *Organization Studies*, *32*(2), 281‑301. https://doi.org/10.1177/0170840610397477

Baier, A. (1986). Trust and Antitrust. *Ethics*, *96*(2), 231‑260. https://doi.org/10.1086/292745

Ballew, C. C., & Todorov, A. (2007). Predicting political elections from rapid and unreflective face judgments. *Proceedings of the National Academy of Sciences*, *104*(46), 17948‑17953. https://doi.org/10.1073/pnas.0705435104

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational behavior and human decision processes*, *50*(2), 248–287.

Baud, M. (2012). La cyberguerre n'aura pas lieu, mais il faut s'y préparer. *Politique étrangère*, *Politique étrangère n° 2/2012*, 305–316.

Bélanger, M., Maupin, P., Berger, J., Boukhtouta, A., & Allouche, M. (2007). *Building a RAP from an R&D perspective*.

Bell, D. (1982). Regret in Decision Making Under Uncertainty. *Operations Research*, *30*, 961–81.

Bellman, R. E., & Zadeh, L. A. (1970). Decision-Making in a Fuzzy Environment. *Management Science*, *17*(4), B141–B164.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Éds.), *New Contributions in Information Systems and Technologies* (p. 311‑316). Springer International Publishing.

Boeke, S. (2017). National cyber crisis management : Different European approaches. *GOVERNANCE-AN INTERNATIONAL JOURNAL OF POLICY ADMINISTRATION AND INSTITUTIONS*.

Boies, K., Fiset, J., & Gill, H. (2015). Communication and trust are key : Unlocking the relationship between leadership and team performance and creativity. *The Leadership Quarterly*, *26*(6), 1080‑1094. https://doi.org/10.1016/j.leaqua.2015.07.007

Boin, A., Busuioc, M., & Groenleer, M. (2014). Building European Union capacity to manage transboundary crises : Network or lead-agency model? *Regulation & Governance*, *8*(4), 418‑436. https://doi.org/10.1111/rego.12035

Bollon, F., Maille, N., Marchand, A., & Blättler, C. (2019). Cyber-attaques : Organiser la confiance. *L'ergonomie et les nouvelles technologies*, 243‑250.

Borgman, C. L., & Furner, J. (2001). *Scholarly Communication and Bibliometrics*.

Brehmer, B. (2005). The Dynamic OODA Loop : Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control. *Proceedings of the 10th International Command and Control Research Technology Symposium*.

Burke, C.S., Sims, D. E., Lazzara, E. H., & Salas, E. (2007). *Trust in leadership : A multi-level review and integration*.

Burke, C. S., Stagl, K. C., Salas, E., Pierce, L., & Kendall, D. (2006). Understanding team adaptation : A conceptual analysis and model. *Journal of Applied Psychology*, *91*(6), 1189‑1207. https://doi.org/10.1037/0021-9010.91.6.1189

Chadwick, S. A. (2001). Communicating Trust in E-Commerce Interactions. *Management Communication Quarterly*, *14*(4), 653‑658. https://doi.org/10.1177/0893318901144009

Chi, M. T., Glaser, R., & Farr, M. J. (2014). *The Nature of Expertise*.

Claverie, B., & Desclaux, G. (2016). C2 - command and control : Un système de systèmes pour accompagner la complexité. *Communication et organisation*, *50*, 255‑278. https://doi.org/10.4000/communicationorganisation.5449

Coleman, J. S. (1990). Foundations of Social Theory. *Harvard University Press*.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity : A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, *92*(4), 909‑927. https://doi.org/10.1037/0021-9010.92.4.909

Cook, K. S., & Hardin, R. (2001). Norms of cooperativeness and networks of trust. In *Social norms* (p. 327‑347). Russell Sage Foundation.

Cooper, C. G. (2019). *NATO Rules of Engagement : On ROE, Self-Defence and the Use of Force during Armed Conflict*. BRILL.

Costa, A. C. (2003). Work team trust and effectiveness. *Personnel Review*, *32*(5), 605‑622. https://doi.org/10.1108/00483480310488360

Costa, A. C., Fulmer, C. A., & Anderson, N. R. (2018). Trust in work teams : An integrative review, multilevel model, and future directions. *Journal of Organizational Behavior*, *39*(2), 169‑184. https://doi.org/10.1002/job.2213

Crisp, C. B., & Jarvenpaa, S. L. (2013). Swift Trust in Global Virtual Teams : Trusting Beliefs and Normative Actions. *Journal of Personnel Psychology*, *12*(1), 45‑56. https://doi.org/10.1027/1866-5888/a000075

Davis, T. R. V., & Luthans, F. (1980). *A Social Learning Approach to Organizational Behavior*. 11.

De Cremer, D., van Dijke, M., Schminke, M., De Schutter, L., & Stouten, J. (2018). The trickle-down effects of perceived trustworthiness on subordinate performance. *Journal of Applied Psychology*, *103*(12), 1335‑1357. https://doi.org/10.1037/apl0000339

De Jong, B. A., Dirks, K. T., & Gillespie, N. (2016). Trust and team performance : A meta-analysis of main effects, moderators, and covariates. *Journal of Applied Psychology*, *101*(8), 1134‑1150. https://doi.org/10.1037/apl0000110

De Jong, B. A., & Elfring, T. (2010). How Does Trust Affect the Performance of Ongoing Teams? The Mediating Role of Reflexivity, Monitoring, and Effort. *Academy of Management Journal*, *53*(3), 535‑549. https://doi.org/10.5465/amj.2010.51468649

De Neve, A., & Henrotin, J. (2006). La Network-Centric Warfare : De son développement à Iraqi Freedom. *Strategique*, *N° 86-87*(1), 51‑73.

De Neys, W. (2006). Dual Processing in Reasoning : Two Systems but One Reasoner. *Psychological Science*, *17*(5), 428‑433. https://doi.org/10.1111/j.1467-9280.2006.01723.x

de Vries, P. W., Midden, C. J. H., & Bouwhuis, D. G. (2003). The effects of errors on system trust, self-confidence and the allocation of control in route planning. *International Journal of Human-Computer Studies*, *58*, 719–735.

Delhey, J., Newton, K., & Welzel, C. (2011a). How General Is Trust in “Most People”? Solving the Radius of Trust Problem. *American Sociological Review*, *76*(5), 786‑807. https://doi.org/10.1177/0003122411420817

Delhey, J., Newton, K., & Welzel, C. (2011b). How General Is Trust in “Most People”? Solving the Radius of Trust Problem. *American Sociological Review*, *76*(5), 786‑807. https://doi.org/10.1177/0003122411420817

Department of Defense. (1997). *C4ISR Architecture Framework Version 2.0*. 231.

Deutsch, M. (1973). The Resolution of Conflict : Constructive and Destructive Processes. *American behavioral scientist*, *17*(2), 248–248.

Deutsch, M. (1958). Trust and suspicion. *Journal of Conflict Resolution*, *2*(4), 265‑279. https://doi.org/10.1177/002200275800200401

Deutsch, M. (1960). The effect of motivational orientation upon trust and suspicion. *Human Relations*, *13*, 123‑139. https://doi.org/10.1177/001872676001300202

Dickinson, T. L., & McIntyre, R. M. (1997). *A Conceptual Framework for Teamwork Measurement*. Team Performance Assessment and Measurement. https://doi.org/10.4324/9781410602053-9

Dietz, G., & Den Hartog, D. N. (2006). Measuring trust inside organisations. *Personnel Review*, *35*(5), 557‑588. https://doi.org/10.1108/00483480610682299

Direction de la défense et de la sécurité civile. (2006). *Guide ORSEC départemental* (G.1). https://www.google.com/search?client=firefox-b-

d&ei=0nvsXpabCKmVlwTyxq5I&q=ORSEC+centre+commandement&oq=ORSEC+centre+commandement&gs_lcp=CgZwc3ktYWIQAzIECCEQFTIECCEQFToECAAQRzoCCAA6BQghEKABOgcIIRAKEKABUPcJWKwfYMQgaABwAXgAgAFTiAH1CpIBAjIwmAEAoAEBqgEHZ3dzLXdpeg&sclient=psy-ab&ved=0ahUKEwiWzOyiv43qAhWpyoUKHXKjCwkQ4dUDCAs&uact=5

Directive, N. I. S. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *OJ L*, *194*(19.7), 2016.

Dirks, K. T. (1999). The effects of interpersonal trust on work group performance. *The Journal of applied psychology*, *84*(3), 445‑455.

Dirks, K. T., & Ferrin, D. L. (2001). The Role of Trust in Organizational Settings. *Organization Science*, *12*(4), 450‑467. https://doi.org/10.1287/orsc.12.4.450.10640

Dirks, K. T., & Ferrin, D. L. (2002). *Trust in leadership : Meta-analytic findings and implications for research and practice*. https://elibrary.ru/item.asp?id=6247680

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the Influence of National Culture on the Development of Trust. *Academy of Management Review*, *23*(3), 601–620. https://doi.org/10.5465/amr.1998.926629

Driscoll, J. W. (1978). *Driscoll, J. W. (1978). Trust and participation in organizational decision making as predictors of satisfaction.* 44‑56.

Duncan, R. (1972). The characteristics of organizational environments and perceived environmental uncertainty. *Administrative Science Quarterly*, *17*, 313–327.

Elkins, A. C., & Derrick, D. C. (2013). The Sound of Trust : Voice as a Measurement of Trust During Interactions with Embodied Conversational Agents. *Group Decision and Negotiation*, *22*(5), 897‑913. https://doi.org/10.1007/s10726-012-9339-x

Evans, J. S. B. T. (2003). In two minds : Dual-process accounts of reasoning. *Trends in cognitive sciences*, *7*(10), 454–459.

Evans, J. S. B. T. (2011). Dual-Process Theories of Reasoning : Contemporary Issues and Developmental Applications. *Developmental Review*, *31*, 86‑102. https://doi.org/10.1016/j.dr.2011.07.007

Fanti, L., & Beach, D. (2002). NATO initial common operational picture capability project. *Battlespace Digitization and Network-Centric Warfare II*, *4741*, 80–89.

Farrell, P. S., Jobidon, M.-E., & Banbury, S. (2012). Organizational Agility Olympic Event Case Studies. *International C2 Journal*, *1*(1), 1–30.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23‑40. https://doi.org/10.1080/00396338.2011.555586

Ferrin, D. L., & Dirks, K. T. (2003). The Use of Rewards to Increase and Decrease Trust : Mediating Processes and Differential Effects. *Organization Science*, *14*(1), 18‑31. https://doi.org/10.1287/orsc.14.1.18.12809

Fiore, S. M., Salas, E., Cuevas, H. M., & Bowers, C. A. (2003). Distributed coordination space : Toward a theory of distributed team process and performance. *Theoretical Issues in Ergonomics Science*, *4*(3‑4), 340‑364. https://doi.org/10.1080/1463922021000049971

Foddy, M., Platow, M. J., & Yamagishi, T. (2009). Group-Based Trust in Strangers : The Role of Stereotypes and Expectations. *Psychological Science*, *20*(4), 419‑422. https://doi.org/10.1111/j.1467-9280.2009.02312.x

Gambetta, D. (1988). *Can We Trust Trust?*

Ghernaouti-Hélie, S. (2009). *La cybercriminalité : Le visible et l'invisible*. Collection le savoir suisse.

Godé, C., Hauch, V., Lasou, M., & Lebraty, J.-F. (2012). Une singularité dans l'aide à la décision : Le cas de la Liaison 16. *Systemes d'information management*, *17*(2), 9–38.

Goldberg, L. R. (1992). The development of markers for the big-five factor structure. *The development of markers for the big-five factor structure*, *4*(1), 26‑42.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud : An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *30*(4), 395‑410. https://doi.org/10.1109/3468.852434

Greenberg, P. S., Greenberg, R. H., & Antonucci, Y. L. (2007). Creating and sustaining trust in virtual teams. *Business Horizons*, *50*(4), 325‑333. https://doi.org/10.1016/j.bushor.2007.02.005

Hardin, R. (1993). The street-level epistemology of trust. *Politics & society*, *21*(4), 505–529.

Hardin, R. (2004). *Trust and trustworthiness*. Russell Sage Foundation.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2011). *The law of cyber-attack*. 76.

Hoff, K. A., & Bashir, M. (2015). Trust in Automation : Integrating Empirical Evidence on Factors That Influence Trust. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *57*(3), 407‑434. https://doi.org/10.1177/0018720814547570

Huff, L., & Kelley, L. (2003). Levels of Organizational Trust in Individualist Versus Collectivist Societies : A Seven-Nation Study. *Organization Science*, *14*(1), 81–90. https://doi.org/10.1287/orsc.14.1.81.12807

Jarvenpaa, S. L., Knoll, K., & Leidner, D. E. (1998). Is Anybody out There? Antecedents of Trust in Global Virtual Teams. *Journal of Management Information Systems*, *14*(4), 29‑64. https://doi.org/10.1080/07421222.1998.11518185

Jarvenpaa, S. L., & Leidner, D. E. (1999). Communication and Trust in Global Virtual Teams. *ORGANIZATION SCIENCE*, *10*(6), 25.

Jensen, C., Johansson, S., & Löfström, M. (2006). Project relationships – A model for analyzing interactional uncertainty. *International Journal of Project Management*, *24*(1), 4‑12. https://doi.org/10.1016/j.ijproman.2005.06.004

Johnston, D. A., McCutcheon, D. M., Stuart, F. I., & Kerwood, H. (2004). Effects of supplier trust on performance of cooperative supplier relationships. *Journal of Operations Management*, *22*(1), 23‑38. https://doi.org/10.1016/j.jom.2003.12.001

Jones, S. L., & Shah, P. P. (2016). Diagnosing the locus of trust : A temporal perspective for trustor, trustee, and dyadic influences on perceived trustworthiness. *Journal of Applied Psychology*, *101*(3), 392‑414. https://doi.org/10.1037/apl0000041

Kahneman, D., & Frederick, S. (2007). Frames and brains : Elicitation and control of response tendencies. *Trends in Cognitive Sciences*, *11*(2), 45‑46. https://doi.org/10.1016/j.tics.2006.11.007

Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise : A failure to disagree. *American Psychologist*, *64*(6), 515‑526. https://doi.org/10.1037/a0016755

Kahneman, D., & Tversky, A. (1972). Subjective probability : Judgment of representativeness. *Cognitive psychology*, *3*(3), 430–454.

Kahneman, D., & Tversky, A. (1979). Prospect Theory : An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263. https://doi.org/10.2307/1914185

Kantowitz, B. H., Hanowski, R. J., & Kantowitz, S. C. (1997). Driver Acceptance of Unreliable Traffic Information in Familiar and Unfamiliar Settings. *Human Factors: The Journal of the Human*

Factors and Ergonomics Society, *39*(2), 164‑176. https://doi.org/10.1518/001872097778543831

Karsenty, L. (2011). Confiance interpersonnelle et communications de travail—Le cas de la relève de poste. *Le travail humain*, *74*(2), 131‑155.

Karsenty, L. (2015). Comment maintenir des relations de confiance et construire du sens face à une crise ? *Le travail humain*, *78*(2), 141. https://doi.org/10.3917/th.782.0141

Kasarskis, P., Stehwien, J., Hickox, J., Aretz, A., States, U., Academy, A. F., & Wickens, C. (2001). Comparison of expert and novice scan behaviors during vfr flight. *In Proceedings of the 11th International Symposium on Aviation Psychology*.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce : The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544‑564. https://doi.org/10.1016/j.dss.2007.07.001

Klapper, A., Dotsch, R., van Rooij, I., & Wigboldus, D. H. J. (2016). Do we spontaneously form stable trustworthiness impressions from facial appearance? *Journal of Personality and Social Psychology*, *111*(5), 655‑664. https://doi.org/10.1037/pspa0000062

Komaki, J. L., Zlotnick, S., & Jensen, M. (1986). Development of an operant-based taxonomy and observational index of supervisory behavior. *Journal of Applied Psychology*, *71*(2), 260.

Koo, T. K., & Li, M. Y. (2016). A Guideline of Selecting and Reporting Intraclass Correlation Coefficients for Reliability Research. *Journal of Chiropractic Medicine*, *15*(2), 155‑163. https://doi.org/10.1016/j.jcm.2016.02.012

Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Information & Management*, *41*(3), 377‑397. https://doi.org/10.1016/j.im.2003.08.004

Kramer, R. M. (1999). Trust and distrust in organizations : Emerging perspectives, enduring questions. *Annual review of psychology*, *50*, 569‑598. https://doi.org/10.1146/annurev.psych.50.1.569

Kramer, R. M., & Carnevale, P. J. (2003). Trust and Intergroup Negotiation. In R. Brown & S. L. Gaertner (Éds.), *Blackwell Handbook of Social Psychology : Intergroup Processes* (p. 431‑450). Blackwell Publishers Ltd. https://doi.org/10.1002/9780470693421.ch21

Lee, J.D. (1992). Trust, Control Strategies and Allocation of Function in Human-Machine System. *Ergonomics*, *35*(10), 153–184.

Lee, J. D., & See, K. A. (2004). Trust in Automation : Designing for Appropriate Reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *46*(1), 50‑80. https://doi.org/10.1518/hfes.46.1.50_30392

Lee, J., Gore, B. F., & Campbell, J. L. (1999). Display Alternatives for In-Vehicle Warning and Sign Information : Message Style, Location, and Modality. *Transportation Human Factors*, *1*(4), 347‑375. https://doi.org/10.1207/sthf0104_6

Lee, J., & Moray, N. (1992). Trust, control strategies and allocation of function in human-machine systems. *ERGONOMICS*, *35*(10), 1243–1270.

Lee, J., & Moray, N. (1994). Trust, self-confidence, and operators' adaptation to automation. *International journal of human-computer studies*, *40*(1), 153–184.

Lee, M. K. O., & Turban, E. (2001). A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce*, *6*(1), 75‑91. https://doi.org/10.1080/10864415.2001.11044227

Levieux, F. (2005). La défense et les technologies de l'information et de la communication. *Réalités Industrielles*, 68.

Lewicki, R., & Bunker, B. (1995). *Trust in relationships.* 583‑601.

Lewicki, R., & Bunker, B. (1996). Developing and Maintaining Trust in Work Relationships. In R. Kramer & T. Tyler (Éds.), *Trust in organizations : Frontiers of Theory and Research* (p. 114‑139). Sage Publications.

Lewis, J. D., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces*, *63*(4), 967‑985. https://doi.org/10.1093/sf/63.4.967

Lieberman, J. K. (1981). *The Litigious Society*. Eweb:35438. http://dx.doi.org/10.2307/1288224

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. (2013). Measurable Resilience for Actionable Policy. *Environmental Science & Technology*, *47*(18), 10108‑10110. https://doi.org/10.1021/es403443n

Lo Monaco, G., Piermattéo, A., Rateau, P., & Tavani, J. L. (2017). Methods for Studying the Structure of Social Representations : A Critical Review and Agenda for Future Research: Methods and Structure of Social Representations. *Journal for the Theory of Social Behaviour*, *47*(3), 306‑331. https://doi.org/10.1111/jtsb.12124

Lowenstein, G. (2003). The Role of Affect in Decision Making. *Hanbook of Affective Sciences*, 619–642.

Luhmann, N. (1979). *Trust and Power (John A. Wiley and Sons, Chichester)*. NewYork.

Luhmann, Niklas. (1968). *Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität* (Verlag). F. Enke.

Marchand, A. (2013). Teamwork : Collaborative activities of French fighter pilots in joint operations. *Proceedings of the Human Factors and Ergonomics Society Europe Chapter 2013 Annual Conference*. http://www.hfes-europe.org/wp-content/uploads/2014/06/Marchand.pdf

Marzi, T., Righi, S., Ottonello, S., Cincotta, M., & Viggiano, M. P. (2014). Trust at first sight : Evidence from ERPs. *Social Cognitive and Affective Neuroscience*, *9*(1), 63‑72. https://doi.org/10.1093/scan/nss102

Mauchly, J. W. (1940). Significance test for sphericity of a normal n-variate distribution. *The Annals of Mathematical Statistics*, *11*(2), 204–209.

Maybury, M. (2013). Toward the Assured Cyberspace Advantage : Air Force Cyber Vision 2025. *IEEE Security Privacy*, *13*(1), 49‑56. https://doi.org/10.1109/MSP.2013.135

Mayer, R. C., & Davis, J. H. (1999). The effect of the performance appraisal system on trust for management : A field quasi-experiment. *Journal of applied psychology*, *84*(1), 123.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709. https://doi.org/10.2307/258792

Mayer, R. C., & Gavin, M. B. (2005). Trust in Management and Performance : Who Minds the Shop While the Employees Watch the Boss? *Academy of Management Journal*, *48*(5), 874‑888. https://doi.org/10.5465/amj.2005.18803928

McAllister, D. J. (1995). Affect and cognition based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, *38*(1), 24‑59. https://doi.org/10.2307/256727

McAllister, Daniel J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, *38*(1), 24‑59.

McCall, R. B., & Appelbaum, M. I. (1973). Bias in the analysis of repeated-measures designs : Some alternative approaches. *Child Development*, 401–415.

McIntyre, R. M., & Salas, E. (1995). Measuring and managing for team performance : Emerging principles from complex environments. *Team effectiveness and decision making in organizations*, *16*, 9–45.

Mckinney, E. H., Barker, J. R., Davis, K. J., & Smith, D. (2005). How Swift Starting Action Teams Get off the Ground : What United Flight 232 and Airline Flight Crews Can Tell Us About Team Communication. *Management Communication Quarterly*, *19*(2), 198‑237. https://doi.org/10.1177/0893318905278539

McKnight, D. H., & Chervany, N. (2000). What is Trust ? A Conceptual Analysis and an Interdisciplinary Model. *AMCIS 2000 Proceedings*, 827‑833. http://aisel.aisnet.org/amcis2000/382

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce : An Integrative Typology. *Information Systems Research*, *13*(3), 334‑359. https://doi.org/10.1287/isre.13.3.334.81

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial Trust Formation in New Organizational Relationships. *The Academy of Management Review*, *23*(3), 473. https://doi.org/10.2307/259290

Medeiros, J. (2019). *Protection renforcée : Le dispositif particulier de sûreté aérienne—Éduscol STI*. *718*, 18‑23.

Mercier, D. (2015). *Les opérations aériennes et le cyber : De l'analogie à la synergie*. *Res Militaris*(hors-série "Cybersécurité"). http://resmilitaris.net/ressources/10205/53/res_militaris_article_gaa_mercier_les_op_rations_a_riennes_et_le_cyber.pdf

Meyerson, D., Weick, K. E., & Kramer, R. M. (1996). Swift trust and temporary groups. In *Trust in organizations : Frontiers of theory and research* (p. 166‑195). Sage Publications, Inc. https://doi.org/10.4135/9781452243610.n9

Ministère des armées. (2018, mai 16). *Cyber Defence Pledge : « La France sera dans le premier cercle des nations en matière de cybersécurité »*. https://www.defense.gouv.fr/actualites/articles/cyber-defence-pledge-la-france-sera-dans-le-premier-cercle-des-nations-en-matiere-de-cybersecurite

Ministère des Solidarités et de la Santé. (2020, juin 19). *La gestion des alertes et des crises sanitaires*. Ministère des Solidarités et de la Santé. http://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/securite-sanitaire/article/la-gestion-des-alertes-et-des-crises-sanitaires

Ministry of Defense. (2017). *Joint Concept Note 2/17 Future of Command and Control*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643245/concepts_uk_future_c2_jcn_2_17.pdf

Moliner, P. (1988). Validation expérimentale de l'hypothèse du noyau central des représentations sociales. [Experimental validation of the hypothesis of a central nucleus of social representations.]. *Bulletin de Psychologie*, *41*(387), 759‑762.

Möllering, G. (2001). *The Nature of Trust : From Georg Simmel to a Theory of Expectation, Interpretation and Suspension*. 18.

Möllering, G., Bachmann, R., & Lee, S.H. (2004). Introduction : Understanding organizational trust – foundations, constellations, and issues of operationalisation. *Journal of Managerial Psychology*, *19*(6), 556‑570. https://doi.org/10.1108/02683940410551480

Muir, B. (1987). Trust between humans and machines, and the design of decision aids. *Int. Man-Machine Studies*, *27*, 527–539.

Muir, B., & Moray, N. (1996). Trust in automation. Part II. Experimental studies of trust and human intervention in a process control simulation. *Ergonomics*, *39*(3), 429–460.

NATO. (2006). *SAS-050 EXPLORING NEW COMMAND AND CONTROL CONCEPTS AND CAPABILITIES*. http://www.dodccrp.org/files/SAS-050%20Final%20Report.pdf

NATO. (2010). *AAP-15 NATO Glossary of Abbreviations Used in NATO Documents and Publications*. 346.

NATO. (2019). *AAP-6 NATO Glossary of Terms and Definitions*. https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf

Oosterhof, N. N., & Todorov, A. (2008). The functional basis of face evaluation. *Proceedings of the National Academy of Sciences*, *105*(32), 11087‑11092. https://doi.org/10.1073/pnas.0805664105

Opall-Rome, B. (2018). *Declassified : How an Israeli operation derailed Syria's nuclear weapons drive*. Defense News. https://www.defensenews.com/global/mideast-africa/2018/03/20/just-declassified-how-an-israeli-operation-derailed-syrias-nuclear-weapons-drive/

Parasuraman, R., Molloy, R., & Singh, I. L. (1993). Performance Consequences of Automation-Induced "Complacency". *THE INTERNATIONAL JOURNAL OF AVIATION PSYCHOLOGY*, *3*(1), 1–23.

Parasuraman, R., & Riley, V. (1997). Humans and Automation : Use, Misuse, Disuse, Abuse. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *39*(2), 230‑253. https://doi.org/10.1518/001872097778543886

Payne, J. W., Bettman, J. R., & Johnson, E. J. (1988). Adaptive strategy selection in decision making. *Journal of experimental psychology: Learning, Memory, and Cognition*, *14*(3), 534.

Pinto, J. K., Slevin, D. P., & English, B. (2009). Trust in projects : An empirical assessment of owner/contractor relationships. *International Journal of Project Management*, *27*(6), 638‑648. https://doi.org/10.1016/j.ijproman.2008.09.010

Posten, A., & Mussweiler, T. (2019). Egocentric foundations of trust. *Journal of Experimental Social Psychology*, *84*. https://www.sciencedirect.com/science/article/pii/S0022103118308886

Przegalinska, A., Ciechanowski, L., Stroz, A., Gloor, P., & Mazurek, G. (2019). In bot we trust : A new methodology of chatbot performance measures. *Business Horizons*, *62*(6), 785‑797. https://doi.org/10.1016/j.bushor.2019.08.005

Quéré, L. (2001). La structure cognitive et normative de la confiance. *Reseaux*, *no 108*(4), 125‑152.

Quéré, L. (2011). Confiance et reconnaissance. *Social Science Information*, *50*(3‑4), 375‑390. https://doi.org/10.1177/0539018411411020

Rateau, P., Moliner, P., Guimelli, C., & Abric, J. C. (2011). Social representation theory. *Handbook of theories of social psychology*, *2*, 477-497.

Ratnasingham, P. (1998). *The importance of trust in electronic commerce* [Text]. Emerald Group Publishing Limited. https://doi.org/info:doi/10.1108/10662249810231050

Reeves, B., & Nass, C. I. (1996). *The media equation : How people treat computers, television, and new media like real people and places.* Cambridge university press.

Rempel, J., Holmes, J., & Zanna, M. (1985). Trust in close relationships. *Journal of personality and social psychology*, *49*(1), 95–112.

Resnick, P., Zeckhauser, R., Swanson, J., & Lockwood, K. (2004). *The value of reputation on ebay : A controlled experiment*. 47.

Robert, L. P., Denis, A. R., & Hung, Y.-T. C. (2009). Individual Swift Trust and Knowledge-Based Trust in Face-to-Face and Virtual Team Members. *Journal of Management Information Systems*, *26*(2), 241‑279. https://doi.org/10.2753/MIS0742-1222260210

Rosenberg, M. (1965). Rosenberg self-esteem scale (RSE). *Acceptance and Commitment Therapy. Measures Package*, *61*(52), 159.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust1. *Journal of Personality*, *35*(4), 651‑665. https://doi.org/10.1111/j.1467-6494.1967.tb01454.x

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. *American Psychologist*, *26*(5), 443‑452. https://doi.org/10.1037/h0031464

Rotter, J. B. (1980). *Interpersonal Trust, Trustworthiness, and Gullibility*. 7.

Rousseau, D. M., & Sitkin, S. B. (1998). Introduction to special topic forum. Not so different after all : A cross-discipline view of trust. *Academy of Management Review*, 393–404.

Rule, N. O., Krendl, A. C., Ivcevic, Z., & Ambady, N. (2013). Accuracy and consensus in judgments of trustworthiness from faces : Behavioral and neural correlates. *Journal of Personality and Social Psychology*, *104*(3), 409‑426. https://doi.org/10.1037/a0031050

Sahaï, A., Desantis, A., Grynszpan, O., Pacherie, E., & Berberian, B. (2019). Action co-representation and the sense of agency during a joint Simon task: Comparing human and machine co-agents. *Consciousness and Cognition*, *67*, 44-55.

Salas, E., Goodwin, G. F., & Burke, C. S. (2008). *Team Effectiveness In Complex Organizations : Cross-Disciplinary Perspectives and Approaches*. Routledge.

Salgado, J. F. (2002). The Big Five Personality Dimensions and Counterproductive Behaviors. *International Journal of Selection and Assessment*, *10*(1 & 2), 117‑125. https://doi.org/10.1111/1468-2389.00198

Saritas, O., & Smith, J. (2011). The big picture-trends, drivers, wild cards, discontinuities and weak signals. *Futures*, *43*(3), 292–312.

Schilke, O., & Huang, L. (2018). Worthy of swift trust? How brief interpersonal contact affects trust accuracy. *Journal of Applied Psychology*, *103*(11), 1181‑1197. https://doi.org/10.1037/apl0000321

Schlenker, B. R., Helm, B., & Tedeschi, J. T. (1973). The effects of personality and situational variables on behavioral trust. *Journal of Personality and Social Psychology*, *25*(3), 419‑427. https://doi.org/10.1037/h0034088

Schmidt, S. M., & Cummings, L. L. (1976). Organizational environment, differentiation and perceived environmental uncertainty. *Decision Sciences*, *7*(3), 447‑467. https://doi.org/10.1111/j.1540-5915.1976.tb00692.x

Schneider, T. R., Dowling, P., Payton, G. M., & Stokes, C. K. (2009). *Experimental Evaluation of Collaborating Teams (EECT)* [Data set]. American Psychological Association. https://doi.org/10.1037/e504882010-001

Schul, Y., Mayo, R., & Burnstein, E. (2004). Encoding Under Trust and Distrust : The Spontaneous Activation of Incongruent Cognitions. *Journal of Personality and Social Psychology*, *86*(5), 668‑679. https://doi.org/10.1037/0022-3514.86.5.668

Sendjaya, S., & Pekerti, A. (2010). Servant leadership as antecedent of trust in organizations. *Leadership & Organization Development Journal*, *31*(7), 643‑663. https://doi.org/10.1108/01437731011079673

Shapiro, D. L. (1987). The Social Control of Impersonal Trust. *American Journal of Sociology*, *93*(3), 623‑658.

Shapiro, D., Sheppard, B., & Cheraskin, L. (1992). Business on a Handshake. *Negotiation Journal*, *8*(4), 365‑377. https://doi.org/10.1111/j.1571-9979.1992.tb00679.x

Siegrist, M., & Cvetkovich, G. (2000). Perception of Hazards : The Role of Social Trust and Knowledge. *Risk Analysis*, *20*(5), 713‑720. https://doi.org/10.1111/0272-4332.205064

Siegrist, M., Gutscher, H., & Earle, T. C. (2005). Perception of risk : The influence of general trust, and general confidence. *Journal of Risk Research*, *8*(2), 145‑156. https://doi.org/10.1080/1366987032000105315

Siegrist, M., Keller, C., & Kiers, H. A. (2005). A new look at the psychometric paradigm of perception of hazards. *Risk Analysis: An International Journal*, *25*(1), 211-222.

Simmel, G. (1950). *The Sociology of Georg Simmel*. Simon and Schuster.

Singh, I., Molloy, R., & Parasuraman, R. (1997). Automation-induced monitoring inefficiency : Role of display location. *International journal of human-computer studies*, *46*(1), 17–30.

Sirdeshmukh, D., Singh, J., & Sabol, B. (2002). Consumer Trust, Value, and Loyalty in Relational Exchanges. *Journal of Marketing*, *66*(1), 15‑37. https://doi.org/10.1509/jmkg.66.1.15.18449

Sirpa Air. (2010, octobre 12). *En direct du CNOA*. https://www.defense.gouv.fr/air/breves-migration/en-direct-du-cnoa

Sjoberg, L., & Drottz-Sjoberg, B.-M. (1991). Knowledge and Risk Perception Among Nuclear Power Plant Employees. *Risk Analysis*, *11*(4), 607‑618. https://doi.org/10.1111/j.1539-6924.1991.tb00650.x

Slepian, M. L., & Ames, D. R. (2016). Internalized Impressions : The Link Between Apparent Facial Trustworthiness and Deceptive Behavior Is Mediated by Targets' Expectations of How They Will Be Judged. *Psychological Science*, *27*(2), 282‑288. https://doi.org/10.1177/0956797615594897

Smith, R. E., Smoll, F. L., & Curtis, B. (1979). Coach Effectiveness Training : A Cognitive-Behavioral Approach to Enhancing Relationship Skills in Youth Sport Coaches. *Journal of Sport Psychology*, *1*(1).

Smoll, F. L., Smith, R. E., Barnett, N. P., & Everett, J. J. (1993). Enhancement of children's self-esteem through social support training for youth sport coaches. *Journal of Applied Psychology*, *78*(4), 602‑610. https://doi.org/10.1037/0021-9010.78.4.602

Solomon, L. (1960). The influence of some types of power relationships and game strategies upon the development of interpersonal trust. *The Journal of Abnormal and Social Psychology*, *61*(2), 223.

Tajfel, H. (1974). Social identity and intergroup behaviour. *Information (International Social Science Council)*, *13*(2), 65‑93. https://doi.org/10.1177/053901847401300204

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53‑55. https://doi.org/10.5116/ijme.4dfb.8dfd

Todorov, A., Olivola, C. Y., Dotsch, R., & Mende-Siedlecki, P. (2015). Social attributions from faces : Determinants, consequences, accuracy, and functional significance. *Annual review of psychology*, *66*, 519–545.

Van der Heijden, H., Verhagen, T., & Creemers, M. (2003). Understanding online purchase intentions : Contributions from technology and trust perspectives. *European Journal of Information Systems*, *12*(1), 41‑48. https://doi.org/10.1057/palgrave.ejis.3000445

Vilchenon, C. (2015). Recognized Cyber Picture de l'armée de l'air (RCP Air). *Penser les ailes Francaises*, *32*, 49‑56. https://doi.org/10.3917/sestr.019.0072

Walker, G. H., Stanton, N. A., & Jenkins, D. P. (2017). *Command and Control : The Sociotechnical Perspective*. CRC Press.

Watson, M. L. (2004). *Can There Be Just One Trust ? A Cross-Disciplinary Identification Of Trust Definitions And Measurement*. The Institute for Public Relations.

Webber, S. S. (2008). Development of cognitive and affective trust in teams : A longitudinal study. *Small group research*, *39*(6), 746–769.

Webster, G. D., Smith, C. V., Brunell, A. B., Paddock, E. L., & Nezlek, J. B. (2017). Can Rosenberg's (1965) Stability of Self Scale capture within-person self-esteem variability? Meta-analytic validity and test–retest reliability. *Journal of Research in Personality*, *69*, 156‑169. https://doi.org/10.1016/j.jrp.2016.06.005

Wildman, J. L., Fiore, S. M., Burke, C. S., Salas, E., & Garven, S. (2011). Trust in swift starting action teams : Critical considerations. *Trust in military teams*, 71.

Williamson, O. E. (1993a). Calculativeness, Trust, and Economic Organization. *The Journal of Law and Economics*, *36*(1, Part 2), 453‑486. https://doi.org/10.1086/467284

Williamson, O. E. (1993b). Calculativeness, Trust, and Economic Organization. *The Journal of Law and Economics*, *36*(1, Part 2), 453‑486. https://doi.org/10.1086/467284

Willis, J., & Todorov, A. (2006). First Impressions : Making Up Your Mind After a 100-Ms Exposure to a Face. *Psychological Science*, *17*(7), 592‑598. https://doi.org/10.1111/j.1467-9280.2006.01750.x

Wong, Y.-T., Ngo, H.-Y., & Wong, C.S. (2006). Perceived organizational justice, trust, and OCB : A study of Chinese workers in joint ventures and state-owned enterprises. *Journal of World Business*, *41*(4), 344‑355. https://doi.org/10.1016/j.jwb.2006.08.003

Zaheer, S., & Zaheer, A. (2006). Trust across borders. *Journal of International Business Studies*, *37*(1), 21‑29. https://doi.org/10.1057/palgrave.jibs.8400180

Zakay, D. (1993). The impact of time perception processes on decision making under time stress. In *Time pressure and stress in human judgment and decision making* (p. 59–72). Springer.

Glossaire

AA : Armée de l'Air Francaise

C2 : *Command and control*

CA : Contrôleurs aérien

CACC : Centre Air de Conduite Cyberdéfense

CDC : Centre de détection et de contrôle

CI : confiance interpersonnelle

CNOA : Centre National des Opérations Aériennes

CS : Confiance en soi

ESIOC : Escadron des systèmes d'information opérationnelle et de cyberdéfense

COP : *Common operational picture*

DPSA : dispositif particulier de sureté aérienne

IA : intelligence artificielle

IHM : Interface homme machine

L16 : Liaison 16

LID : Lutte informatique défensive

NCW : *Network Centric Warfare*

OPEX : Opérations extérieures

OTAN : Organisation du traité de l'Atlantique Nord

RAP : *Recognized Air Picture*

RS : Représentations sociales

PN : Pilotes et navigateurs

PT : *Propensity to trust*

PO : Permanence Opérationnelle

PPS : posture permanente de sureté

RAP : *Recognized air picture*

RCPair : *Recognized cyber picture*

SiTac : Situation tactique

STATs : *Swift starting action teams*

TIC : Technologies de l'information et de la communication

VD : variables dépendantes

VI : variables indépendantes

ANNEXE 1 : Exemple de questions posées et analyse du besoin de la RCPair

Analyse du besoin de la RCPair, type de questions posées

A qui /quoi rend le service

Qui est concerné par la mise en œuvre de la future RCP ?

- Quels sont les différents acteurs qui utiliseront la RCP ?
    - Responsable, services, opérateur, compétence, qualifications

Une fois la RCP mise en place qu'est ce qui pourrait la faire évoluer, existe-t-il de fortes chances de la voir évoluer ?

Quels sont les risques de la RCP ?

Une fois la RCP mise en place qu'est ce qui pourrait la faire disparaitre, existe-t-il de fortes chances de la voir disparaitre ?

Depuis quand avons-nous besoin d'une RCP ?

Quelle sera votre fréquence d'utilisation de la RCP ?

Sur qui/quoi agit la RCP

La RCP doit intervenir sur tous le spectre du cyber ?

- RCP indiquant l'état cyber de tous les systèmes Français ?
- RCP indiquant l'état cyber des systèmes nécessaires à la mission en court ?
- RCP indiquant l'état cyber des systèmes géographiquement distribués ?

La RCP doit pouvoir intervenir sur les systèmes physiques ?

- Envoie cyber de données de réparation ?

Dans quel but

Quel est l'état actuel de la situation ?

- Logiciels existants
- Systèmes envisagés

Obtenir des informations sur la situation cyber ?

- Reconnaissance ? (détection d'une intrusion)
- Identification ?

    - Identifier le type d'attaque
    - Identifier l'attaquant
    - Identifier la cause de l'attaque (but)

Obtenir des informations sur l'impact physique d'une attaque cyber ?

- Au présent (attaque en court)
- Au futur (impact en cas d'attaque sur un système ?)

Obtenir des informations sur l'évolution de la situation cyber ?

- Etat passé du système ?
- Etat présent du système ?
- Etat futur du système ?

Obtenir des informations sur les causes (pourquoi et comment) un problème cyber peut être ou est infecté ?

Obtenir des informations sur la qualité de l'information cyber collectée ?

- Véracité de l'information ?
- Validité de l'information ?

Obtenir les possibilités d'attaques cyber sur la base de la situation actuelle ?

Sur les fonctions principales et secondaires de la RCP

Quelles sont les caractéristiques de la RCP ?

- Quelles sont les fonctions principales de la RCP
- Quelles sont les fonctions secondaires de la RCP ?

Quelles sont les conséquences de la mise en place de la RCP ?

- Temps de mise en œuvre envisagé ?
- Coût ?
- Nombre de personnes pour la mise en œuvre ?
    - Qualifications
- Réorganisation ?
- Embauches ?

- Formation ?

Quels sont les risques ?

- Action, procédés, objets, méthode, opération

Ou la RCP s’applique-t-elle ?

- La RCP doit être physique ?
    - Lieu, local, distance, service, Park.
    - La RCP doit être déplaçable facilement ?
    - La RCP doit être fixe ?
- La RCP doit être dématérialisable ?
- Sur quelle machine ?
    - Ajout de fonctionnalité sur des machines existantes ? (outil)
    - Ajout de machines (unité centrale, écran…) (système)

26 juillet 2018 **Base Aérienne 701**

Analyse du besoin opérationnel des différentes unités Air concernées par la Recognized Cyber Picture

GT 16 – feuille de route Cyber

Florent Bollon & Anne Lise Marchand (Chaire Cyb'Air)

Introduction

De Novembre 2017 à Juillet 2018 une analyse du besoin sur la Recognized Cyber Picture (RCP) a été menée par des membres du centre de recherche de l'armée de l'air auprès :

- des équipes du centre air de conduite cyberdéfense, du commandant de base ainsi que du responsable cybersécurité de la base aérienne 113 de Saint-Dizier-Robinson ;
- du responsable cybersécurité de la base aérienne 133 de Nancy-Ochey ;
- des contrôleurs aériens de la base aérienne 705 de Cinq-Mars-La-Pile ;
- de l'Equipe de Marque Cyber (EM Cyber) sur la base aérienne 118 de Mont-de-Marsan ;
- de l'ESIOC sur la base aérienne 118 de Mont-de-Marsan ;
- du BSSI sur la base aérienne 118 de Mont-de-Marsan.

Cette analyse du besoin a donné lieu à la rédaction d'un compte rendu de réunion « Compte rendu de réunion – GT 16 Feuille de route » qui a été lu et approuvé par les différentes parties prenantes citées ci-dessus. Le compte rendu de réunion a ensuite été exposé et discuté auprès :

- du LCL Thierry KESSLER-RACHEL, chef du centre opérationnel de la cyberdéfense ;
- du Cdt Nicolas Schneider du CALID ;
- de Monsieur Olivier de BAYSER du CATOD.

Le présent document constitue le livrable final pour l'analyse du besoin Air de la RCP. Ce document a été rédigé sur la base du compte rendu de réunion modifié avec les données recueillies durant les 3 derniers entretiens listés ci-dessus.

I. La RCP

1. Définition

« La RCP est un outil d'aide à la compréhension et à la représentation de la situation cyber permettant d'améliorer la lutte informatique défensive et de faciliter la prise de décision des opérateurs ».

Une autre définition de la RCP, reprenant les mêmes idées, est présente dans la nouvelle version de la DIA 3.20

2. Concept général de la RCP

La RCP, telle qu'envisagée lors de ces réunions, est un Méta-Système matriciel alimenté par différents moyens matériels et humains et ayant pour sorties différentes Interfaces Homme-Machine (IHM) selon les besoins utilisateurs, qu'ils soient personnels Air ou Interarmées. La RCP ne sera donc pas une représentation partagée des états cyber de l'armée de l'Air mais un outil permettant, grâce à des IHM de sorties spécifiques, la représentation partagée des états cyber. Pour un fonctionnement optimal la RCP aura donc besoin d'un grand nombre de données d'entrée.

3. Flux d'informations de la RCP

A. Informations montantes

Pour un fonctionnement optimal la RCP devra être alimentée par des données matérielles (provenant par exemple de sondes de capteurs physiques ou électroniques) et humaines (toute personne travaillant au sein de l'armée) (*Cf.* Figure 1). Par ailleurs, certains logiciels et systèmes paraissent remplir des rôles importants pour les interlocuteurs. Afin de ne pas perturber le fonctionnement de la chaîne cyber actuelle, les bases de données (BDD) des systèmes suivants devront être récupérées pour alimenter la RCP :

- PAVENSIS
- TBHSSI
- SICLADE
- CAILLOU

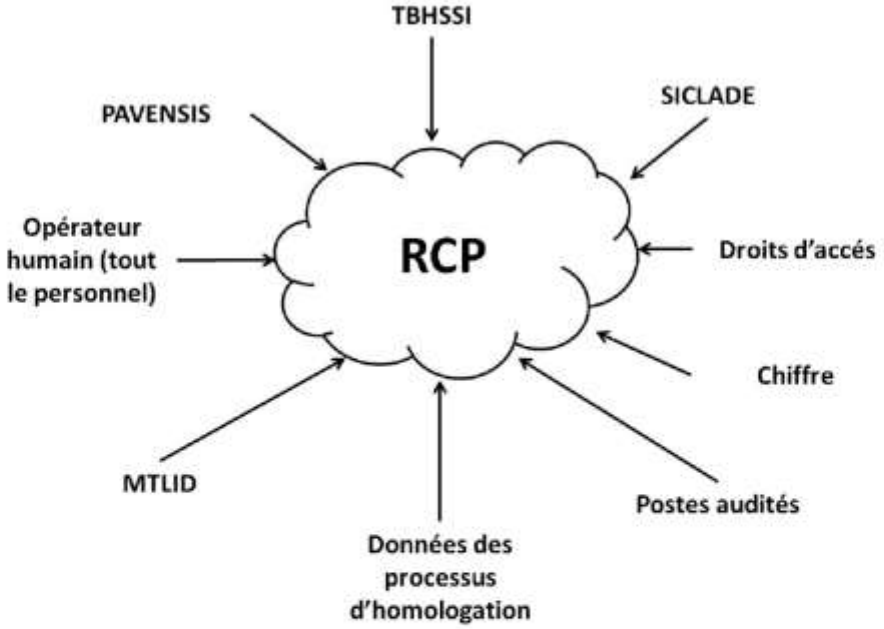


Figure 1 : exemple non exhaustif des sources pouvant alimenter la RCP

Selon la posture du COMCYBER il semblerait que les paradigmes de protection soient dépassés, et que, par conséquent, il devienne nécessaire de sécuriser de l'intérieur. A ce titre, il faudrait que chaque personne puisse être contributrice à la RCP. Tout le personnel devrait pouvoir faire remonter un dysfonctionnement ou une panne relevée sur son poste de travail (sous forme de tickets par exemple). Actuellement les problèmes cyber sont remontés avec l'aide de formulaires dénommé « FOURMIS » qui, bien qu'étant manuel, semble être difficile d'utilisation et qui n'est que peu connu en dehors des acteurs de la cybersécurité. Un dispositif simplifié, faisant automatiquement la distinction entre panne et menace cyber pourrait être mis en place afin que les personnes non expertes du domaine cyber puissent remonter des problèmes détectés. Par ailleurs, il est nécessaire que les opérateurs puissent faire remonter les dysfonctionnements ou les erreurs sans crainte de sanction, comme cela est fait pour la sécurité aérienne en vertu de la politique de dépénalisation de l'erreur instaurée par le GAA Abrial en 2006 (Abrial S. (2006), Bulletin de sécurité des vols, n°218, 2006/02).La RCP capitalisera ensuite toutes les informations provenant des opérateurs et des systèmes de sonde afin de garder une trace de tous les dysfonctionnements passés.

Il serait intéressant que la RCP soit également alimentée par les données recueillies lors du processus d'homologation (présentes notamment dans SICLADE) et notamment pendant la phase d'enrôlement des SI. Ceci permettrait d'avoir une vue de l'état initial d'un système et ainsi de quantifier les vulnérabilités coté terrain (avant la mise en place des systèmes l'équipe de marque cyber (EM cyber) identifie les risques macro en terme de conception et d'architecture). Pour l'EM Cyber la RCP devrait être alimentée par le recueil exhaustif de tous les postes audités afin de récupérer toutes les informations techniques et ainsi gérer l'historique des données existantes. L'ESIOC a besoin de moyens de récupération de données cybers permettant de renvoyer des données LID sur intradef. Actuellement, MTLID (moyens techniques de lutte informatique défensive) répond partiellement au besoin tactique. Cependant MTLID n'est ni ergonomique ni évolutif. Un des moyens d'alimenter et de se servir des données de la RCP serait de récupérer les couches MTLID et de rajouter (par-dessus) une couche IHM (possiblement développée par le GAIO).

Enfin, les données concernant l'homologation des systèmes, le chiffre ainsi que les droits d'accès devraient être pris en compte dans la RCP.

Afin de palier la problématique de la confidentialité de l'information il sera peut être nécessaire que les informations remontées soient gérées par niveau de classification. Ces RCP différentes se transformeront en une seule RCP après chiffrement des données et un passage par des « data diode » (*Cf.* Figure 2). En outre la RCP pourrait être découpé en deux espaces :

- Un espace collaboratif
- Un espace avec besoin d'en connaître

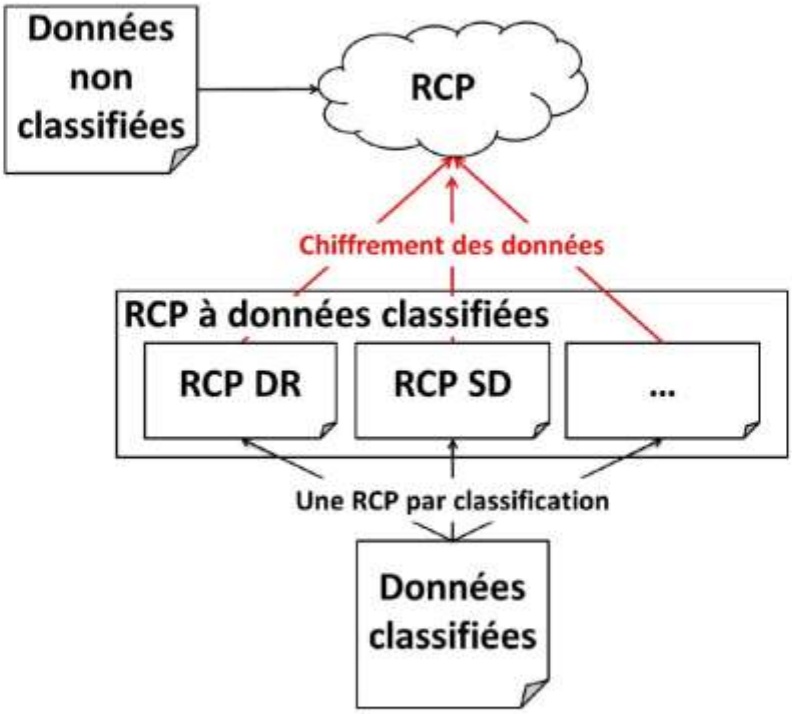


Figure 2 : Schéma représentant différentes RCP classifiées alimentant la base de données d'une méta-RCP

B. Traitement de l'information

Afin d'analyser, de traiter et de transférer au mieux les informations, la RCP devra possiblement allier une intelligence artificielle (IA) a des experts de la cybersécurité (*Cf.* Figure 3). En effet, une Intelligence Artificielle (IA) permettra de classer et d'analyser rapidement des informations déjà répertoriées, ou ressemblant à des informations connues, afin d'effectuer un stockage efficace (en terme de temps et de ressources) de ces informations. Seulement, du fait de l'évolution constante du monde cyber il sera nécessaire qu'un opérateur humain puisse intervenir à tout moment pour traiter les informations ambigües ou non utilisables par le système. Il serait donc préférable qu'une personne physique soit présente dans la boucle de la RCP.

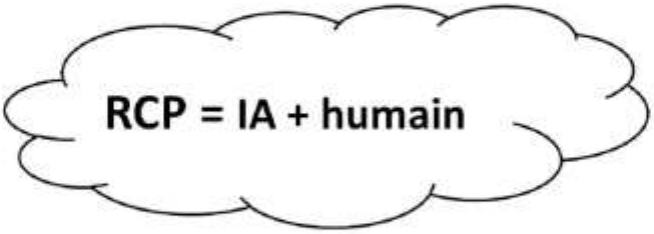


Figure 3 : Analyse et traitement de l'information dans la RCP

Les pannes ou problèmes redondants pourront être gérées automatiquement par l'IA afin d'éviter, à l'opérateur humain, la surcharge engendrée par une masse importante de données. Les pannes ou problèmes plus ponctuelles (n'arrivant pas en grand nombre) mais ressemblant à des données déjà vue pourront être traitées indépendamment par l'IA ou l'opérateur humain, voire de manière semi-automatique. Enfin, les pannes ou problèmes jamais répertoriés pourront être traités entièrement par l'opérateur humain (*Cf.* Figure 4).

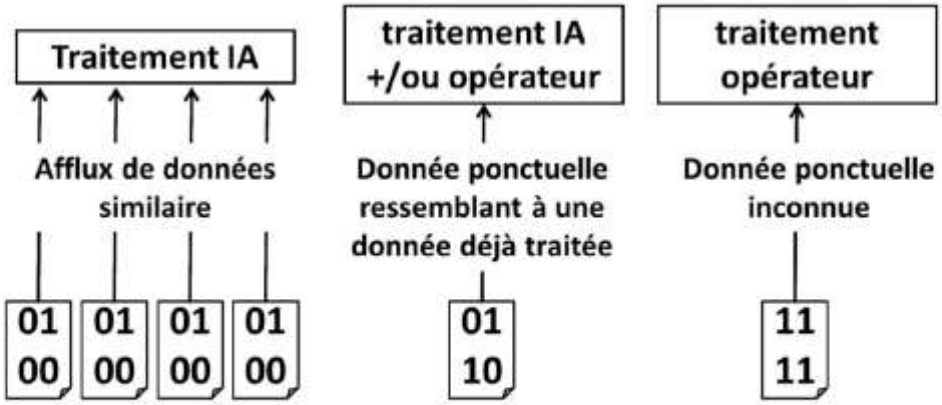


Figure 4 : Exemple de traitement de l'information dans la RCP

C. *Information descendantes*

Une fois les données traitées par la RCP elles devront être transmises aux différents opérateurs. Pour préserver une cohérence de travail les interfaces de PAVENSIS par exemple ne seront pas entièrement modifiées mais de nouvelles interfaces graphiques permettant le dialogue entre l'opérateur et la RCP (IHM ou Interfaces Homme-Machine) pourront être créées.

- Une interface axée contrôle aérien pour le CNOA et les CDC ;
- Pour le personnel non expert cyber ayant effectué une remontée d'information une IHM d'aide à la résolution du problème pourrait être envisagé. En effet, après avoir transmis le problème l'utilisateur aura besoin d'une assistance technique lui permettant, dans le meilleur des cas, de résoudre l'incident, ou, dans le pire des cas, de stopper la progression. Cette IHM pourrait prendre la forme d'une assistance par « chat » ou par « avatar » par exemple voire par documents à consulter ;
- L'EM cyber aurait potentiellement besoin d'une IHM axée sur le *big data* afin d'obtenir une matrice de connectivité et d'impact entre des systèmes semblants ne pas être reliés entre eux, et d'anticiper la propagation voire la survenue d'une infection ;
- Le CO-Cyber aurait besoin d'une IHM permettant de :
    - voir la matrice d'impact d'une attaque cyber ;
    - Planifier les actions ;
- Le CALID aurait besoin d'une IHM permettant :
    - de détecter les menaces les plus avancées ;

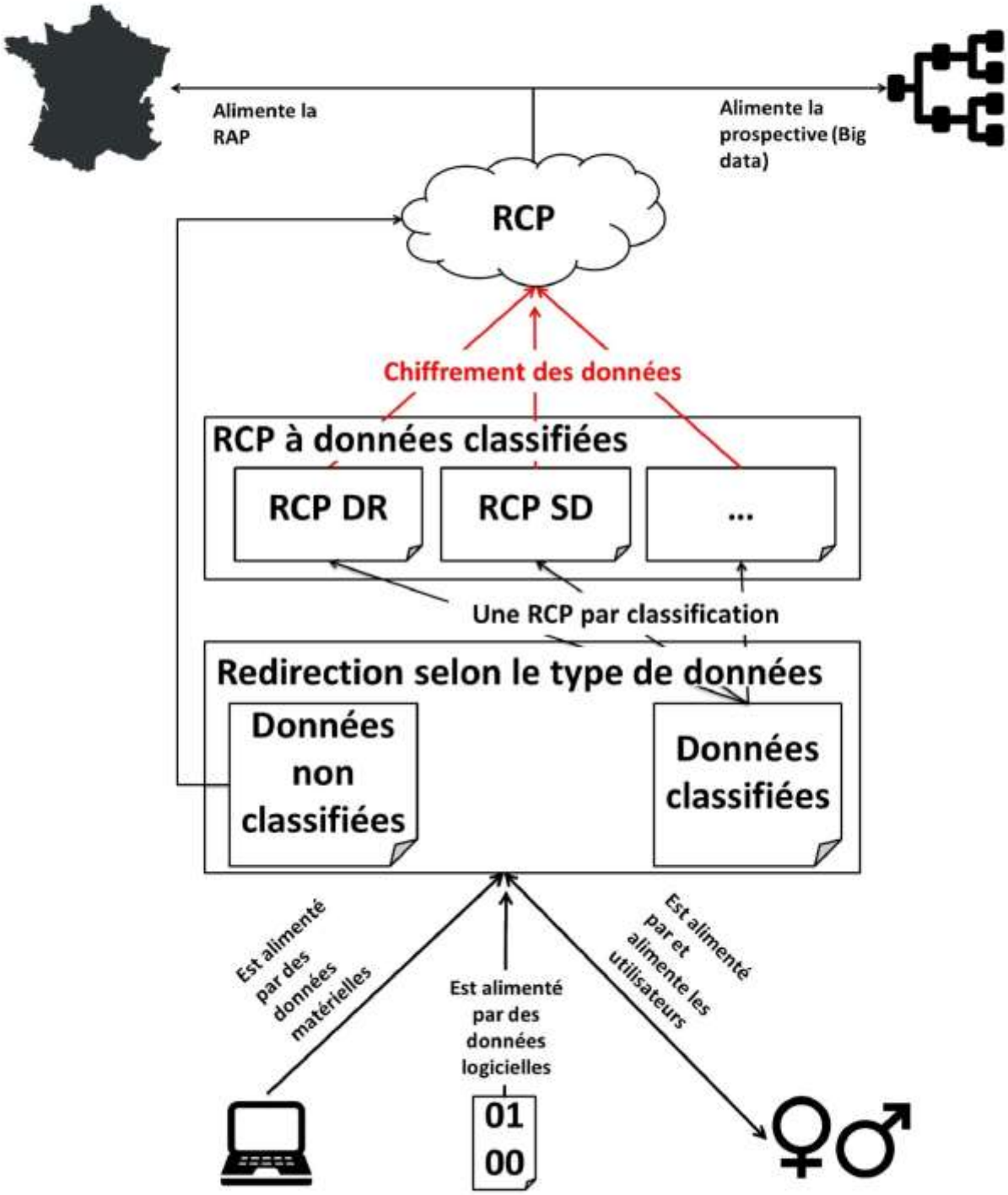
    - D'avoir une représentation partagée de la menace (avec le CO-Cyber notamment) ;
- Une interface pour l'entraînement pour créer facilement des scénarios possibles (*Cf.* infra « La RCP en entraînement et en retour d'expérience »);
- Une IHM représentant la cartographie de tous les SI.
- Etc.

4. Interactions entre les utilisateurs de la RCP

Afin de palier la rapidité du monde cyber le transfert d'information entre les opérateurs et la RCP devra se faire de manière directe sans passer par une chaîne hiérarchique de type pyramidale. De plus, il serait intéressant que la remontée d'information cyber dans la RCP se fasse sur le même principe de subsidiarité qu'entre les CDC et le CNOA, c'est-à-dire qu'il y ait une remontée d'information à l'échelon technique mais que la hiérarchie n'ait l'information que lorsqu'elle en a besoin.

5. Vue conceptuelle globale de la RCP

Le schéma ci-dessous représente une mise en commun des différents concepts de la RCP précédemment évoqués.



II. Processus utilisateurs de la RCP

Du fait du grand nombre de sorties possibles la RCP pourra être utilisée pour différents besoins. Une liste non exhaustive des utilisations est présentée ci-dessous.

1. RCP « prospective »

L'un des besoins de l'ESIOC est d'anticiper au mieux les évolutions du domaine cybers afin d'évaluer les impacts d'une menace sur les systèmes. En effet, étant donné le nombre de systèmes qui interagissent entre eux il y a un manque de vision global permettant de détecter, identifier et analyser les effets de bords intra et inter système, ce qui augmente la vulnérabilité globale. Pour l'ESIOC la RCP devrait permettre de cartographier les SI de l'armée et d'agir en anticipation en préparant les systèmes à affronter les agressions.

Le CO-Cyber aurait également besoin d'avoir la matrice des systèmes des différentes armées. Grâce à cela le CO-Cyber pourrait anticiper l'impact d'une menace et avoir, rapidement, la temporalité des risques liés à la propagation d'un incident.

De plus, grâce au grand nombre de données présentes dans la RCP (et en anonymisant ces dernières) il pourrait être envisagé d'utiliser des *data analyst* et *data scientist* afin de mettre au jour des analyses d'impact (La réalisation d'une analyse d'impact est obligatoire pour les traitements à grande échelle).

2. RCP « défense aérienne »

L'utilisation dans la défense aérienne pourrait correspondre aux besoins du CNOA (cela restant à vérifier) et des CDC (d'après le recueil de besoin effectué auprès des contrôleurs aériens de Cinq-Mars-La-Pile). Pour la défense aérienne, la RCP pourrait permettre de détecter une intrusion sur les écrans de contrôle, tel qu'une perte ou un ajout d'aéronef ou encore une multiplication d'IFF. Cette RCP pourrait être utilisée en opération extérieure ou dans le cadre de la PPS afin de détecter une intrusion cyber sur les systèmes de défense aérienne.

3. RCP « C2 »

Afin de pouvoir partager la situation et d'orienter les décisions la RCP pourrait être envisagée comme un C2. Ce type de RCP permettrait d'améliorer et de partager la visualisation d'un incident. Elle permettrait également de transformer, de synthétiser et de préciser les impacts techniques afin de les transformer en capacité opérationnelle. Enfin, grâce au partage de la situation, l'incident cyber pourrait être traité à différents échelons. Ce type de RCP pourrait être utile au CO-Cyber et au CALID.

4. RCP « entraînement et retour d'expérience »

Une RCP permettant de réaliser des entraînements de cybesécurité pourrait être utile au centre air de conduite cyberdéfense (CACC). Grâce aux données de la RCP des vulnérabilités des systèmes pourraient être mises en évidence afin de simuler des attaques cybers plus proches du réel. De plus, couplée à des systèmes de simulation la RCP pourrait être utilisé en retour d'expérience afin de montrer l'impact qu'aurait eu une attaque cyber sur le bon fonctionnement d'une mission. Ce fonctionnement de la RCP pourrait également être utile pour la formation des opérateurs, qu'ils

soient orientés vers le cyber ou non, en leur montrant les impacts potentiels d'une attaque sur les systèmes qu'ils utilisent.

III. Conclusion

Ce document ne constitue qu'une première version de l'analyse du besoin relative à la RCP. Des analyses plus précises des besoins de chaque acteur de la cyber sécurité seront primordiaux afin de concevoir plus précisément les fonctionnalités nécessaires à implémenter pour chaque acteur. Il est à noter que les figures présentent dans ce document ne sont que des schématisations qui ne donnent en aucun cas une idée de l'architecture de la RCP.

Enfin, Il pourrait être intéressant de transposer ce document aux domaines de commandement du COMCYBER qui n'a pas pu être visité lors de cette étude. La terminologie de la PIA-3.0.6 pourrait également être utilisée pour adapter le document.

ANNEXE 2 : Exemple de feuille de consentement et questionnaire utilisés dans les expérimentations effectuées sur les opérationnels de l'AA

Etude sur le travail collaboratif

Bonjour,

Vous allez participer à une expérimentation portant sur le travail collaboratif et les interactions médiées par ordinateur. Cette étude est menée par le Centre de Recherche de l'armée de l'air et l'ONERA se déroulera en deux parties. La première partie correspond à la saisie du questionnaire ci-dessous. La deuxième partie sera une tâche collaborative de comptage collaboratif avec un coéquipier et durera environ 45 minutes.

Vous pouvez interrompre l'étude à tout moment.

Les réponses au questionnaire et les données recueillies lors de l'expérimentation sont strictement anonymes, un numéro de passage vous sera attribué au début de l'expérimentation pour garantir cet anonymat.

Les résultats de l'étude ainsi que vos résultats personnels peuvent vous être transmis. Pour ce faire vous pouvez nous communiquer votre mail ou nous contacter directement (en nous donnant votre numéro de passage) à l'adresse suivante: florent.bollon@onera.fr

Cochez si vous souhaitez obtenir les résultats de cette étude ☐

Cochez si vous souhaitez obtenir vos résultats personnels ☐

Adresse Mail ☐

Questions générales

Age : ☐

Genre : Homme Femme

Pour les personnels navigants

Nombre d'heures de vol en opération extérieure : ☐

Nombre d'heures de vol total :

Qualifications (entourez l'élément correspondant) : « PO »« NO »« SCP »« SCN »« CP » « CN »

Pour les contrôleurs

Nombre approximatif de Control Event

Nombre d'OPEX (avec mission de contrôle)

Si possible nombre de CE en opération

Vous êtes : « CO » « PC » « MC »

Contrôleur : « CA » « DA »

A remplir par le participant :

J'ai lu et compris les renseignements ci-dessus et j'accepte de plein gré de participer à cette recherche.

Date :

L'équipe du Centre de Recherche de l'Armée de l'Air vous remercie de votre participation.

ANNEXE 3 : Expérimentation 1, Résultats des tests post-hocs

```
                                  Estimate Std. Error z value Pr(>|z|)
low.CA - high.CA == 0             0.141071   0.025104   5.620 2.87e-07 ***
medium.CA - high.CA == 0          0.111607   0.025104   4.446 0.000131 ***
high.Mec - high.CA == 0           0.138439   0.058455   2.368 0.268068
low.Mec - high.CA == 0            0.175000   0.058455   2.994 0.041338 *
medium.Mec - high.CA == 0         0.157143   0.058455   2.688 0.107741
medium.CA - low.CA == 0          -0.029464   0.025104  -1.174 1.000000
high.Mec - low.CA == 0           -0.002633   0.058455  -0.045 1.000000
low.Mec - low.CA == 0             0.033929   0.058455   0.580 1.000000
medium.Mec - low.CA == 0          0.016071   0.058455   0.275 1.000000
high.Mec - medium.CA == 0         0.026832   0.058455   0.459 1.000000
low.Mec - medium.CA == 0          0.063393   0.058455   1.084 1.000000
medium.Mec - medium.CA == 0       0.045536   0.058455   0.779 1.000000
low.Mec - high.Mec == 0           0.036561   0.025104   1.456 1.000000
medium.Mec - high.Mec == 0        0.018704   0.025104   0.745 1.000000
medium.Mec - low.Mec == 0        -0.017857   0.025104  -0.711 1.000000

low = niveau de CI faible
medium = niveau de CI moyen
High = niveau de CI élevé
CA = Contrôleurs aériens
Mec = Mécaniciens (Base)
```

Hypothèse 7 : Test post-hoc HSD de Tukey pour la variable dépendante %VDsup et pour les groupes contrôleur aérien et mécanicien n'ayant jamais fait d'OPEX.

```
                                 Estimate Std. Error z value Pr(>|z|)
low.exp - high.exp == 0           0.04851    0.02619   1.852 0.959751
medium.exp - high.exp == 0        0.03766    0.02619   1.438 1.000000
high.N_exp - high.exp == 0       -0.20268    0.04504  -4.500 0.000102 ***
low.N_exp - high.exp == 0        -0.01081    0.04504  -0.240 1.000000
medium.N_exp - high.exp == 0     -0.05891    0.04504  -1.308 1.000000
medium.exp - low.exp == 0        -0.01085    0.02619  -0.414 1.000000
high.N_exp - low.exp == 0        -0.25119    0.04504  -5.578 3.66e-07 ***
low.N_exp - low.exp == 0         -0.05933    0.04504  -1.317 1.000000
medium.N_exp - low.exp == 0      -0.10742    0.04504  -2.385 0.256055
high.N_exp - medium.exp == 0     -0.24034    0.04504  -5.337 1.42e-06 ***
low.N_exp - medium.exp == 0      -0.04847    0.04504  -1.076 1.000000
medium.N_exp - medium.exp == 0   -0.09657    0.04504  -2.144 0.480217
low.N_exp - high.N_exp == 0       0.19187    0.02619   7.326 3.56e-12 ***
medium.N_exp - high.N_exp == 0    0.14377    0.02619   5.490 6.04e-07 ***
medium.N_exp - low.N_exp == 0    -0.04809    0.02619  -1.836 0.994767

low = niveau de CI faible
medium = niveau de CI moyen
High = niveau de CI élevé
N_exp = Elèves PN
exp = PN expérimentés
```

Hypothèse 8 : Test post-hoc HSD de Tukey pour la variable dépendante %VDsup et pour les groupes PN expérimentés et élèves PN

```
                                 Estimate Std. Error z value Pr(>|z|)
low.exp - high.exp == 0          0.005636   0.008339   0.676 1.000000
medium.exp - high.exp == 0       0.009252   0.008339   1.110 1.000000
high.N_exp - high.exp == 0      -0.095429   0.019905  -4.794 2.45e-05 ***
low.N_exp - high.exp == 0       -0.046606   0.019905  -2.341 0.288188
medium.N_exp - high.exp == 0    -0.058978   0.019905  -2.963 0.045711 *
medium.exp - low.exp == 0        0.003617   0.008339   0.434 1.000000
high.N_exp - low.exp == 0       -0.101065   0.019905  -5.077 5.74e-06 ***
low.N_exp - low.exp == 0        -0.052242   0.019905  -2.625 0.130164
medium.N_exp - low.exp == 0     -0.064614   0.019905  -3.246 0.017554 *
high.N_exp - medium.exp == 0    -0.104681   0.019905  -5.259 2.17e-06 ***
low.N_exp - medium.exp == 0     -0.055858   0.019905  -2.806 0.075197 .
medium.N_exp - medium.exp == 0 -0.068230   0.019905  -3.428 0.009130 **
low.N_exp - high.N_exp == 0      0.048823   0.008339   5.855 7.16e-08 ***
medium.N_exp - high.N_exp == 0   0.036451   0.008339   4.371 0.000185 ***
medium.N_exp - low.N_exp == 0   -0.012372   0.008339  -1.484 1.000000


low = niveau de CI faible
medium = niveau de CI moyen
High = niveau de CI élevé
N_exp = Elèves PN
exp = PN expérimentés
```

Hypothèse 8 : Test post-hoc HSD de Tukey pour la variable dépendante %TempsTot et pour les groupes PN expérimentés et élèves PN

```
                                 Estimate Std. Error z value Pr(>|z|)
low.exp - high.exp == 0          0.003571   0.023045   0.155   1.0000
medium.exp - high.exp == 0       0.037500   0.023045   1.627   1.0000
high.N_exp - high.exp == 0      -0.031158   0.064850  -0.480   1.0000
low.N_exp - high.exp == 0        0.044643   0.064850   0.688   1.0000
medium.N_exp - high.exp == 0    -0.010714   0.064850  -0.165   1.0000
medium.exp - low.exp == 0        0.033929   0.023045   1.472   1.0000
high.N_exp - low.exp == 0       -0.034730   0.064850  -0.536   1.0000
low.N_exp - low.exp == 0         0.041071   0.064850   0.633   1.0000
medium.N_exp - low.exp == 0     -0.014286   0.064850  -0.220   1.0000
high.N_exp - medium.exp == 0    -0.068658   0.064850  -1.059   1.0000
low.N_exp - medium.exp == 0      0.007143   0.064850   0.110   1.0000
medium.N_exp - medium.exp == 0 -0.048214   0.064850  -0.743   1.0000
low.N_exp - high.N_exp == 0      0.075801   0.023045   3.289   0.0151 *
medium.N_exp - high.N_exp == 0   0.020444   0.023045   0.887   1.0000
medium.N_exp - low.N_exp == 0   -0.055357   0.023045  -2.402   0.2445

low = niveau de CI faible
medium = niveau de CI moyen
High = niveau de CI élevé
N_exp = Mécaniciens (Base)
exp = Mécaniciens (OPEX)
```

Hypothèse 9 : Test post-hoc HSD de Tukey pour la variable dépendante %VDmodif et pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX

```
                                 Estimate Std. Error z value Pr(>|z|)
low.exp - high.exp == 0         -0.009334   0.027463  -0.340   0.7339
medium.exp - high.exp == 0       0.039288   0.027463   1.431   0.1526
high.N_exp - high.exp == 0      -0.048472   0.062930  -0.770   0.4412
low.N_exp - high.exp == 0        0.019831   0.062930   0.315   0.7527
medium.N_exp - high.exp == 0    -0.034913   0.062930  -0.555   0.5790
medium.exp - low.exp == 0        0.048622   0.027463   1.770   0.0767 .
high.N_exp - low.exp == 0       -0.039138   0.062930  -0.622   0.5340
low.N_exp - low.exp == 0         0.029166   0.062930   0.463   0.6430
medium.N_exp - low.exp == 0     -0.025578   0.062930  -0.406   0.6844
high.N_exp - medium.exp == 0    -0.087760   0.062930  -1.395   0.1632
low.N_exp - medium.exp == 0     -0.019456   0.062930  -0.309   0.7572
medium.N_exp - medium.exp == 0 -0.074200   0.062930  -1.179   0.2384
low.N_exp - high.N_exp == 0      0.068304   0.027463   2.487   0.0129 *
medium.N_exp - high.N_exp == 0   0.013560   0.027463   0.494   0.6215
medium.N_exp - low.N_exp == 0   -0.054744   0.027463  -1.993   0.0462 *


low = niveau de CI faible
medium = niveau de CI moyen
High = niveau de CI élevé
N_exp = Mécaniciens (Base)
exp = Mécaniciens (OPEX)
```

Hypothèse 9 : Test post-hoc HSD de Tukey pour la variable dépendante %VDm_sup et pour les groupes mécaniciens ayant déjà fait des OPEX et mécaniciens n'ayant jamais fait d'OPEX

```
                                 Estimate Std. Error z value Pr(>|z|)
low.Mec - high.Mec == 0         -1.0062     0.2280  -4.414 0.000152 ***
medium.Mec - high.Mec == 0      -0.6498     0.2280  -2.851 0.065449 .
high.PN - high.Mec == 0          0.4534     0.4778   0.949 1.000000
low.PN - high.Mec == 0          -1.5350     0.4778  -3.212 0.019738 *
medium.PN - high.Mec == 0       -0.5290     0.4778  -1.107 1.000000
medium.Mec - low.Mec == 0        0.3564     0.2280   1.563 1.000000
high.PN - low.Mec == 0           1.4596     0.4778   3.055 0.033786 *
low.PN - low.Mec == 0           -0.5288     0.4778  -1.107 1.000000
medium.PN - low.Mec == 0         0.4772     0.4778   0.999 1.000000
high.PN - medium.Mec == 0        1.1032     0.4778   2.309 0.314235
low.PN - medium.Mec == 0        -0.8852     0.4778  -1.853 0.959250
medium.PN - medium.Mec == 0      0.1209     0.4778   0.253 1.000000
low.PN - high.PN == 0           -1.9884     0.2280  -8.723  < 2e-16 ***
medium.PN - high.PN == 0        -0.9824     0.2280  -4.310 0.000245 ***
medium.PN - low.PN == 0          1.0060     0.2280   4.413 0.000153 ***

low = niveau de CI faible
medium = niveau de CI moyen
High = niveau de CI élevé
Mec = Mécaniciens (Base)
PN = PN expérimentés
```

Hypothèse 10 : Test post-hoc HSD de Tukey pour la variable dépendante CertitudePartenaire et pour les groupes mécaniciens ayant déjà fait des OPEX et PN expérimentés

ANNEXE 4 : Feuille consentement et questionnaire utilisés dans les expérimentations 3 et 4

Travail collaboratif, en équipes éphémères, médié par ordinateur

But du projet de recherche

L'objectif principal de cette étude est d'évaluer le fonctionnement du travail collaboratif médié par ordinateur dans des tâches de très courtes durées.

Ce que l'on attend de vous

Lors de cette expérimentation, vous réaliserez une passation d'une durée totale de 2h. La passation comprendra un temps de familiarisation avec l'interface graphique, la passation d'une pré expérimentation et la passation de l'expérimentation finale (environ 30 minutes). Aucune pause ne pourra être effectuée durant l'expérimentation. Lors de cette passation, vous serez amené à effectuer une tâche de dénombrement d'aéronefs, avec différents coéquipiers, sur différentes images récupérées sur google maps.

Tout au long de chaque passation, nous enregistrerons informatiquement des données comportementales sans appareillage.

Afin de réaliser l'expérimentation dans de bonnes conditions, nous vous demanderons d'avoir une activité habituelle le jour même de l'expérience et d'avoir dormi normalement au cours des deux nuits précédant votre passation.

Vos droits de vous retirer de la recherche en tout temps

Vous êtes volontaire pour participer à cette étude. Vous êtes libre, à tout moment de l'étude de renoncer à votre participation sans aucun préjudice (personnel ou professionnel) et sans avoir à vous justifier. Votre retrait ne sera pas notifié au responsable des études de l'ENSC ni à aucun professeur, et n'aura pas de conséquences sur vos notes ni sur vos relations avec les enseignants et responsables pédagogiques de l'école.

Vos droits à la confidentialité et au respect de la vie privée

Les données obtenues seront traitées avec la plus entière confidentialité. Votre anonymat sera garanti à l'aide d'un numéro aléatoire chiffré pour toutes les données recueillies (physiologiques, questionnaires). Aucun renseignement ne sera dévoilé qui puisse révéler votre identité. Les données seront gardées dans un endroit sécurisé et ne seront jamais communiquées à une tierce personne étrangère au projet. Seul le responsable de l'étude y aura accès. Sur la durée de votre participation, conformément aux dispositions de la loi Informatique et Libertés, vous pourrez exercer vos droits d'accès et de rectification ou suppression auprès du responsable scientifique du projet. A l'issue de votre passation expérimentale, la procédure d'anonymisation rendra impossible la rectification ou la suppression des informations vous concernant. Les données personnelles ne seront conservées que le temps de l'expérimentation.

Bénéfices

Il s'agit lors de cette étude d'identifier l'impact de l'informatique sur les équipes éphémères.

Risques possibles

À notre connaissance, cette recherche n'implique aucun risque. Durant toute la durée de l'expérimentation.

Diffusion

Cette recherche fera l'objet de communications dans des congrès (nationaux et internationaux), et de publications dans des journaux académiques et des actes de congrès. Les résultats diffusés seront basés uniquement sur des analyses de groupe. Cette recherche servira aussi de point de départ à de futurs projets de recherche nationaux ou européens.

Vos droits de poser des questions en tout temps

Vous pouvez poser des questions au sujet de la recherche en tout temps en communiquant avec le responsable et les partenaires scientifiques du projet par courrier électronique à Florent Bollon (florent.Bollon@onera.fr) qui se trouve sur le site ONERA de Salon de Provence.

Consentement à la participation

En signant le formulaire de consentement, vous certifiez que vous avez lu et compris les renseignements ci-dessus, que nous avons répondu à vos questions de façon satisfaisante et que nous vous avons avisé que vous étiez libre d'annuler votre consentement ou de vous retirer de cette recherche en cours d'étude, sans préjudice.

A remplir par le participant :

J'ai lu et compris les renseignements ci-dessus et j'accepte de plein gré de participer à cette recherche.

Date :

Signature

Experimental Survey

1. One should be very cautious with strangers

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	○	●	○

2. Most experts tell the truth about the limits of their knowledge

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	○	●	○

3. Most people can be counted on to do what they say they will do

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	○	○	●

4. These days, you must be alert or someone is likely to take advantage of you

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	●	○	○	○

5. Most salespeople are honest in describing their products

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	●	○	○

6. Most repair people will not overcharge people who are ignorant of their speciality

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	○	●	○

7. Most people answer public opinion polls honestly

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	○	●	○

8. Most adults are competent at their job

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	○	○	●

9. If I had my way, I wouldn't let top management have any influence over issues that are important to me

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	○	●	○

10. I would be willing to let top management have complete control over my future in a company

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	●	○	○	○

11. I really wish I had a good way to keep an eye on top management

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	○	●	○

12. I would be confortable giving top management a task or problem which war critical to me, even if I could not monitor their actions

Disagree Strongly	Disagree	Neither agree nor disagree	Agree	Agree Strongly
○	○	●	○	○

13. I feel I am a person of worth, at least on an equal basis with others

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	○	●

14. I feel that I have a number of good qualities

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	●	○

15. All in all, I am inclined to feel that I am a failure

Disagree Strongly	Disagree	Agree	Agree Strongly
○	●	○	○

16. I am able to do things as well as most other people

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	●	○

17. I feel I do not have much to be proud of

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	●	○

18. I take a positive attitude toward myself

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	●	○

19. On the whole, I am satisfied with myself

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	●	○

20. I wish I could have more respect for myself

Disagree Strongly	Disagree	Agree	Agree Strongly
○	●	○	○

21. I certainly feel useless at times

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	●	○

22. At times I think I am not good at all

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	●	○

23. My opinion of myself tends to change a good deal instead of always remaining the same

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	●	○

24. I find that on one day I have on opinion of myself and on another day I have a different opinion

Disagree Strongly	Disagree	Agree	Agree Strongly
○	○	●	○

25. I change from a very good opinion from myself to a very poor opinion of myself

Disagree Strongly	Disagree	Agree	Agree Strongly
○	●	○	○

26. I have noticed that my ideas about myself seem to change very quickly

Disagree Strongly	Disagree	Agree	Agree Strongly
○	●	○	○

27. I feel that nothing can change the opinion I currently hold of myself

Disagree Strongly	Disagree	Agree	Agree Strongly
●	○	○	○