La prise de décision en situations extrêmes sous l'effet des nouvelles stratégies informationnelles : le cas des équipes militaires

Christine Dugoin-Clément

▶ **To cite this version:**

Christine Dugoin-Clément. La prise de décision en situations extrêmes sous l'effet des nouvelles stratégies informationnelles : le cas des équipes militaires. Gestion et management. Université Panthéon-Sorbonne - Paris I, 2020. Français. NNT : 2020PA01E038 . tel-03276190

HAL Id: tel-03276190

https://theses.hal.science/tel-03276190

Submitted on 1 Jul 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.

UNIVERSITE PARIS I- PANTHEON SORBONNE
Institut d'Administration des Entreprises de Paris

École doctorale de Management Panthéon-Sorbonne - ED 559
Equipe de Recherche GREGOR - EA 2474

La prise de décision en situations extrêmes sous l'effet des nouvelles stratégies informationnelles: le cas des équipes militaires

THESE
présentée et soutenue publiquement le **08/07/2020**
en vue de l'obtention du
DOCTORAT EN SCIENCES DE GESTION
par

Christine DUGOIN-CLEMENT

JURY

Directeur de recherche : **Monsieur Lamarque , Eric**
Professeur, IAE de Paris

Rapporteurs : **Monsieur Lebraty Jean-Fabrice,**Professeur agrégé des Universités, Université Lyon 3

Monsieur Danet Didier
Professeur- Directeur du MSc Cyber Defense, Université de Rennes 1 - Ecoles de Saint-Cyr Coëtquidan

Suffragants : **Monsieur Patrick, Gilbert**
Professeur, IAE Paris

Madame Chanut Véronique
Professeur des Universités, CIFFOP et Université de Paris II Panthéon-Assas

Général Castres, Didier
General d'Armée, sous chef Opération des Armées, Conseiller Sénior CEIS,

L'université de PARIS I – Panthéon Sorbonne n'entend donner aucune approbation ni improbation aux opinions émises dans les thèses ; ces opinions doivent être considérées comme propres à leurs auteurs

Table des matières

Table des matières 2

Remerciements 7

Liste des abréviations 8

Introduction 10

Références....29

CHAPITRE 1 : L'émergence de la question des valeurs et de la confiance dans les situations extrêmes....34

Introduction....35

1. Contexte cyber en Ukraine 37

1.1. Le cyber dans les conflits modernes : le cas ukrainien....40

1. 2. Potentialités du cyber....47

1. 3. Le cyber, facteur d'influence sur la confiance ? 49

2. Le rôle de la confiance dans le fonctionnement des équipes militaires....52

3. Potentiels opérationnels - l'utilisation de la dissonance cognitive....56

Conclusion : risques opérationnels et sanitaires pour les armées occidentales 60

Références....65

CHAPITRE 2 : Cadre théorique, approche épistémologique et méthodologique68

1. Un cadre théorique transdisciplinaire....69

1. 1. La dissonance cognitive....71

1. 2. La confiance....74

1. 3 . les situations extrêmes....78

1. 4 . La polémologie appliquée à la guerre informationnelle....84

2. La pertinence de l'approche abductive....90

3 . Méthodologie....96

3.1 Méthodologie générale....97

3.2. Contexte de la seconde vague d'entretiens 98

3.3- Traitements ou des outils d'analyse mobilisés dans la première phase de la seconde vague d'entretiens....100

3.4 – Traitements ou des outils d'analyse mobilisés dans la seconde phase de la seconde vague d'entretiens....105

3.5- Outillage technique pour exploiter ces entretiens....110

Références....113

CHAPITRE 3 : Confiance, altération de la confiance et rationalité de la prise de décision 117

I . The use of cyber activities as a weapon: the empirical case of Ukraine 120
Introduction.....120
1 - Literature Review and Definition of Terms.....121
1.1- Clarifying the Terms.....121
1.2- Existing Literature Review.....123
1.2.1- Cognitive Dissonance and Decision Making 123
1.2.2- Trust and Cohesion in Military Affairs.....128
1.2.3- Cyber Operations, Access to Information, and Changes in Trust.....129
2. The Case of Ukraine 131
2.1- Significance of the Case Study.....131
2.2- Data Collection and Research Methodology.....133
2.3- Survey methodology.....134
3- Analysis and Results.....135
Conclusion 140
II . La référence de la confiance comme cadre d'action en situation extrême 143
Introduction.....143
1. Confiance et gestion de coopération.....145
1.1. Confiance, efficacité et vulnérabilité 146
1.2. Confiance organisationnelle 149
1.3. La confiance au sein des organisations intervenant en situation extrême.....152
1.3.1. L'exercice de la confiance envers les différents niveaux.....153
1.3.2. La combinaison itérative de confiance comme atout de coordination156
2. Étude de cas 159
2.1- Méthodologie 161
2.1.1- Échantillon des sujets 162
2.1.2. Déroulé des entretiens et traitement des données 163
2.2. Données collectées.....166
3. Analyse des résultats.....166
3.1. Analyse des résultats du groupe d'étude A et B 167
3.2. Analyse des résultats du groupe C 171
3.3. L'émergence des déterminants potentiels de renforcement de la confiance ...172
3.4. Du basculement de l'équilibre de la dynamique de confiance vers l'incertitude : un virage cognitif ? 174

Conclusion 176
Références....179
CHAPITRE 4 : La problématique de l'information pour les organisations intervenant en situations extrêmes 185
Introduction....188
1. La communication sur Internet, les réseaux sociaux et les organisations 190
2. Typologie des réseaux sociaux 191
3. Réseaux sociaux, communication et information : quelles conséquences pour l'entreprise 194
3.1- Des usages, des générations et des terrains d'interventions 196
4. Enquête de terrain....199
4.1- Analyse des données 199
Conclusion 205
Références....207
CHAPITRE 5 : L'approche managériale des situations extrêmes: analyse et propositions préventives 208
Introduction....211
1. Values and military profession....212
1.1. Training and Values....213
1.2. From Instruction to Internalization....214
2. Discrepancy in Major Values....215
2.1. Consequences of Discrepancy in Values 215
2.2. Cognitive dissonance....216
2.3. Perception of Discrepancy in Values Provokes their Defence 217
3. Regulation of Discrepancies in Values Involving the Institution 218
3.1 . Discrepancy with the Institution: from inner conflicts to information warfare220
3.2 Field Experience 221
3.3. Media and information warfare 222
4. Overview of the Study....224
4.1. Method....225
4.1.1.Population and Sample 225
4.2. Content of interviews and identified variables....226
4.3. Staged observation part 227
5. Interview Results 228
5.1. Values and Self Perception 228

5.2. Trusts toward peers and Institution *229*
5.3. Reason of Mistrust *230*
5.4. Use and Confidence in Media *233*
5.5. Awareness Training and Perception of Being a Target *235*
6. Staged observation on Core Values targeting 236
6.1. Reactions to the provoked situation *236*
7. Discussion 238
7.1. Information Warfare and the Destabilization of the Organization *238*
7.2. Limitations and suggestions for further research *239*
7.3. Challenge for National Security *241*
7.4. Potential paths to prevent the risk *242*
Conclusion 244
References 246
CHAPITRE 6 : La hiérarchie des valeurs hiérarchiques et l'évolution de la confiance dans l'organisation 253
1. Introduction 255
2. Theoretical framework 257
2.1. Influence of values in organizational culture and identity *257*
2.2. Values influence in decision-making in extreme situation *259*
2.3. Values in specific context of organizations evolving in extreme situation *259*
3.Data collection and research proposal 262
3.1. Establishing proposal through exploratory Interviews *262*
3.2. Results of the exploratory interviews *264*
3.3. Trust and hierarchy values, an interaction *266*
4. Proposition validation through a second set of interview 270
4.1. Population and Data Collection *270*
4.2. Results *273*
4.2.1. Values hierarchy: organization ranking versus personal's ranking 274
4.2.1. Organization ranking vs. personal ranking based on time accorded to each values in interviews 275
4.2.1. Values hierarchy: discrepancy in between group members ranking 279
4.3. Trust : age influence in its meaning, and reasons of trust and mistrust in organization *283*
4.3.1. Meaning of cohesion and trust in peers 284
4.3.2. Reasons of mistrust in the organization 287

Conclusion 290
References 295
Conclusion 301
1. Principales contributions 301
2. Propositions managériales 309
3. Limites de la recherche 316
4. Perspectives de recherches complémentaires 317
Liste des graphiques et tableaux 321

Remerciements

Il sera difficile de remercier ici tous ceux qui m'ont aidé car c'est grâce à l'aide de très nombreuses personnes que j'ai pu mener cette thèse à son terme. Je voudrais d'abord remercier chaleureusement mon directeur de thèse, Eric Lamarque, pour son aide. Je suis ravie d'avoir travaillé avec lui, il a su me soutenir et me conseiller tout au long de mon parcours tout en m'offrant un précieux appui scientifique. Mes remerciements vont aussi à Jean-Fabrice Lebraty, Professeur à l'Université Lyon 3 et Didier Danet, Professeur à l'Université de Rennes 1 et aux Ecoles de Saint Cyr Coëtquidan, qui acceptèrent d'être rapporteurs de ma thèse, ils m'ont écouté avec bienveillance et leurs remarques ont permis d'enrichir mon travail. Je tiens à remercier Véronique Chanut, professeur à l'Université Paris II Panthéon-Assas et Patrick Gilbert, professeur à l'IAE, d'avoir été membre de mon jury de thèse et pour le temps qu'ils ont consacré à ma recherche. Merci aussi au Général Didier Castres pour l'honneur qu'il m'a fait d'être dans mon jury, pour son regard affuté et sa grande gentillesse. Je remercie également David Vaidis, Professeur à l'Institut de Psychologie de l'Université de Paris pour sa confiance, nous avons travaillé sur ce sujet et ses conseils m'ont été particulièrement précieux. Je tiens aussi à remercier Geraldine Michel et Frederic Noël, professeurs à l'IAE de Paris pour nos discussions et leurs conseils durant mon cursus. Il m'est impossible d'oublier Paola Berdugo pour son aide précieuse dans mon parcours de thèse. Elle a toujours fait son possible pour m'aider, je l'en remercie. A l'origine de tout, il y a ces hommes et femmes que j'ai eu la chance de rencontrer, en France et ailleurs, alors qu'ils faisaient leur métier dans des circonstances parfois sensibles, souvent dangereuses. Ils sont à l'origine de cette thèse, pour cela comme pour le reste, qu'ils soient remerciés. Mes remerciement vont particulièrement au Général Hervé Wattecamps, et au Général Hingray qui ont soutenu cette entreprise et ont autorisé les entretiens nécessaires à cette recherche. Je remercie aussi le Général Justel et le Général Vandenbussche qui m'ont toujours accompagnée dans ce travail de longue haleine. Je suis particulièrement touchée de la confiance témoignée par ceux que j'ai eu la chance d'entendre lors des entretiens qui ont permis la rédaction de cette thèse. Bien que l'exercice ne leur soit pas familier, ils ont su être sincères et ont accepté sans reserve de m'accorder de leur temps pour répondre avec patience aux questions parfois délicates dont je les accablais. Je ne peux les citer ici mais ils se reconnaitront et, je l'espère, recevront ma sincère gratitude. Messieurs, merci pour tout.

Au terme de ce parcours, je remercie enfin celles et ceux qui me sont chers et que j'ai dû un peu délaisser pour achever cette thèse. Leurs présences et encouragements m'ont accompagnée tout au long de ces années. Je pense avec emotion à ma famille, à mes enfants, Solane, Raphaël, Brann et Jade, à ma mère Odile, à mon père Xavier pour leur soutien, leur confiance, leur capacité à me faire rire et à me faire « revenir sur terre ». J'ai une pensée toute particulière pour mes collègues analystes qui sont surtout amis de tous temps et de tous terrains Mathieu Boulègue (la dream team) et Didier Chaudet, mais aussi pour les mains de Fanny, le sourire sans jugement de Joël (sauf sur les brewdogs), et les messages de Cop's. Enfin, une thèse est faite d'heures de travail qui n'auraient été les mêmes sans les musiques qui rendirent l'exercice moins solitaire, aussi, merci à Iron Maiden, Metallica, Beth Hart, Zoe Keatting, Florence+the machine, Anna Nalick les Foo Fighters et tant d'autres. Peut être aussi à Mulder et Scully: entendre que « la vérité est ailleurs », développa sans doute la curiosité nécessaire au travail de thèse. Merci à ceux qui m'ont dit que je n'arriverais pas au bout, vous fûtes une grande motivation.

Liste des abréviations

CCDCOE — NATO Cooperative Cyber Defence Centre of Excellence (Fr. Centre d'excellence coopératif de la cyberdéfense).

CDT — Cognitive dissonance theory

CERN-European Organization for Nuclear Research

HB — Heuristic and biases

INES — échelle internationale des évènements nucléaires

MISOC-Military Information Support Operations Command

MMM - Meaning Maintenance Model

NATO-North Atlantic Treaty Organization

NGW — New Generation War

OTAN – Organisation du traité de l'Atlantique Nord

PSA — predictability, susceptibility and awareness model

PSYOPS—psychological operations

RADA — Verkhovna Rada – national assembly of Ukraine

RuNEt — Russian Internet

SSA —Service de Santé des Armées

SSM—Self-Standard Model

SVR — Foreign intelligence service of Russia

TEA — Transit Europe-Asia terrestrial cable network (fr. dorsale Trans-Europe-Asie)

TEPCO — Tokyo Electric Power Company

TMT – Terror Management Theory

TRC – Theory of Rational Choice

TSOC—Theater of Special Operations Command

EU — European union

Introduction

La sécurisation de la prise de décision est une préoccupation majeure pour les organisations dont la croissance et l'existence dépendent souvent de la stratégie choisie, mais aussi de son bon déploiement. C'est tout particulièrement prégnant alors que les organisations sont amenées à évoluer dans un milieu de plus en plus concurrentiel et volatile, où l'information que la structure délivre à l'attention de ses membres est soumise à la concurrence forte constituée par une multitude de vecteurs extérieurs. Le développement d'Internet et de la consommation de données mobiles a fait croître cette préoccupation, qui dépasse le seul secteur privé pour s'étendre au domaine public. En effet, ces avancées technologiques et évolutions sociales de consommation de l'information ont permis le développement de nombreux canaux d'information, par là même, elles ont permis aux contenus diffusés par ces biais d'accéder à une grande « viralité », pouvant aller jusqu'à enclencher des réactions en chaîne pouvant toucher la prise de décision des membres d'une organisation. Ce risque apparaît d'autant plus fort en situations extrêmes qui sont encore sous contrôle ou dans une situation de crise qui échappent à tout contrôle des organisations qui perdent alors leur capacité d'initiative. Dans ces deux cas, de par la nature des situations, les perceptions pourront enclencher d'autant plus facilement des prises de décisions déviantes aux conséquences très lourdes, que ce soit pour l'organisation ou pour ses membres. En effet, dans ces situations, un système ordonné qui contraint les agents, où les comportements et les prises de décision sont régulés, sera prévisible par opposition aux systèmes désordonnés. Dans cette approche, un système complexe pourra toujours sembler ordonné et donc prévisible a posteriori, mais qu'en est-il a priori ? L'enjeu sera alors dans ce type de système complexe comparable à une entreprise ou une organisation qui connaît des interactions entre les agents et le système, de limiter les prises de décisions inadaptées au contexte et à la finalité poursuivit par l'organisation, et ce particulièrement pour

ceux intervenant en situations extrêmes ou de crise. Partant du principe selon lequel le système, l'organisation, est dépositaire d'un passé qui influencera son présent, et que chaque élément interagit avec l'environnement, alors il apparaît que développer un corpus de valeurs communes pourra permettre le développement d'un passé commun qui augmentera la probabilité d'action similaire des agents, limitant *de facto* le risque de décision déviante. Cette prévisibilité du comportement des agents tendrait à éviter une prise de décision inadaptée source de problèmes dont les conséquences pourraient s'avérer irréversibles pour l'organisation. Si les contextes complexes n'ont pas une seule «bonne réponse », mais bien plusieurs, l'enjeu sera de limiter la prise de décision qui serait par nature déficiente et emporterait des conséquences lourdes.

En ce qui concerne le secteur privé, rappelons les évènements du 11 mars 2011. À cette date, un tsunami déferle sur l'île de Honshu au Japon. L'amplitude imprévue de ce tsunami ravage 600 km de côtes touchant les infrastructures jusqu'à 10 km à l'intérieur des terres. Ce faisant, il impacte la centrale nucléaire de Fukushima-Daishii. Son gestionnaire TEPCO (Tokyo Electric Power Company) aura donc à affronter une situation extrême puis une gestion de crise dans un contexte à incertitude forte.

Les conséquences du tsunami sont désastreuses, les murs tombent, des systèmes électriques et les groupes électrogènes de secours sont inondés, des systèmes de refroidissement d'urgence de réacteurs par injection d'eau sont bientôt hors service. Rapidement, l'effondrement du cœur du réacteur 1 perce le fond de la cuve, et la TEPCO tente de refroidir le réacteur en envoyant des quantités massives d'eau de mer. Le 12 mars, l'unité 1 explose et les systèmes de refroidissement des unités 2 et 3 cèdent à leur tour. L'unité 3 explose le 14 mars et la fusion se confirme dans trois réacteurs. Les matériaux du cœur des réacteurs, dont le combustible radioactif, surchauffent et commencent à fondre, entraînant un risque de diffusion de radioacti-

vité qui se concrétisera dans les jours suivants. Le 12 mars 2011, la catastrophe de Fukushima est classée par l'agence japonaise de sûreté nucléaire au niveau 4 sur l'échelle INES (échelle internationale des évènements nucléaires) de gravité qui comprend 7 gradations.

Cette crise aura vu se succéder des épisodes dramatiques et des interventions dangereuses, improvisées sous la pression par le gestionnaire de Fukushima-Daichii, mais aussi par l'État japonais pris dans l'urgence qui aura parfois été amené à prendre des décisions dont la pertinence sera ensuite largement discutée. Sur place, le contrôle des informations sera accusé de minimiser l'ampleur du désastre pour faciliter l'acceptation de décisions douteuses alors que des hommes, rapidement baptisés par les médias « les 50 de Fukushima », se portent volontaires pour commencer les travaux de déblaiement. Les travaux sont particulièrement délicats et se déroulent dans des champs de radiation intense. Le nombre d'intervenants sur le site augmentera : 1000 personnes seront dénombrées le 23 mars, parmi lesquelles des pompiers et des militaires. Si les médias occidentaux ont gardé une image particulièrement héroïque de ces hommes sur site, les « 50 » critiquent des informations « incohérentes » reçues, et pointent le traitement hétérogène des données relatives à l'exposition aux radiations. Au-delà des critiques faites par la population japonaise à TEPCO concernant son inconséquence dans la gestion de la centrale, il apparaît que nombre des « liquidateurs » (personnels travaillant pour déblayer le site et le mettre en sécurité) seraient des travailleurs journaliers souvent mal informés de la mission à accomplir, en situation de grande précarité et recrutés par des intermédiaires (dont des yakuzas) sous-traitants pour TEPCO. Ce scandale sera dénoncé sous le terme de « gitans du nucléaire » dans plusieurs médias et rapports, dont celui du professeur Fukita de l'université de Keio, faisant de certains de ces hommes des héros malgré eux, voire des victimes.

Si une centrale nucléaire peut par nature envisager de se trouver dans une situation extrême, d'autres organisations, à première vue évoluant dans des milieux moins risqués, peuvent aussi connaître des situations extrêmes. Ainsi, toute organisation peut être confrontée à une situation extrême s'inscrivant dans un contexte d'incertitude élevée où les décisions et actions prises auront des conséquences fortes, tant économiques et stratégiques qu'humaines. Aussi, pouvoir mettre en place des systèmes visant à sécuriser le déploiement des stratégies afin qu'il ne fasse pas l'objet d'une application aléatoire due à une prise de décision déviante par les agents chargés de missions précises devient un enjeu crucial. En effet, cela participe à limiter fortement les risques d'évolutions problématiques de la situation, non anticipées par la structure, et qui pourraient avoir des effets délétères sur son avenir. Cette sécurisation des processus, qui est particulièrement importante dans des situations extrêmes et de crise, devient un sujet de majeur alors que les marchés sont de plus en plus ouverts à la concurrence et que le rythme de l'information s'accroît, permettant à chacun d'être témoin et juge des actions et « non-actions » choisies et mises en œuvre par les entreprises.

À ce titre, il apparaît que le milieu militaire est un sujet d'étude très approprié. En effet, leurs terrains d'intervention sont par nature des situations extrêmes, à savoir évolutives, potentiellement dangereuses et difficilement prévisibles où prévaut un niveau de tension fort. En outre, ces situations extrêmes peuvent facilement basculer vers des situations de crise échappant au contrôle. En raison de l'habitude qu'elles ont acquise de devoir gérer ce type de situations, les armées ont mis en place des systèmes ayant pour objet de sécuriser au maximum leurs modes d'action et processus, garantissant ainsi le bon déploiement de leurs stratégies. Aussi, l'observation des types interactions et des éléments pouvant se manifester comme des leviers de prise de décisions aléatoires et d'exécutions déviantes d'ordres par les agents, actions susceptibles d'engager l'avenir de leur organisation au sein de ces structures permet de bénéficier

d'un terrain d'observation de choix. En outre, étudier ce sujet au sein des armées permet d'obtenir des éléments de réponses à même de dépasser le seul cadre militaire et de s'appliquer aux organisations amenées à évoluer dans des situations extrêmes ou de crises à forte incertitude. En effet, si on pense naturellement à des organisations de type sécurité civile (telles que les pompiers ou les policiers), le contexte de situations extrêmes et de crise pourra également être perçu dans des structures plus classiques, que l'on parle de gestionnaires de flux de transports ou de systèmes d'énergies auront des conséquences environnementales importantes, voire irréversibles. On pourra également penser aux systèmes bancaires et financiers dont les défaillances peuvent engendrer des crises majeures pouvant dépasser largement les frontières d'un état. Dans ces différents cas, pour assurer le bon déploiement de leurs stratégies, sécuriser leurs processus et augmenter leur productivité et efficience, les organisations ont besoin de maîtriser la chaîne d'exécution des consignes définies par leur conseil de direction. Cela implique que le processus de « décision making », de prise de décision, de tous les membres de la structure soit stabilisé. Malheureusement, ce prérequis, qui reste un problème récurrent auquel se heurtent les organisations, peut aller jusqu'à mettre en danger la stratégie de développement définie. Cette sécurisation de l'exécution de la consigne et de la prise de décision peut voir sa complexité et sa délicatesse accrues si le contexte dans lequel les décisions doivent être prises et exécutées s'avère risqué, si les conséquences de ces décisions et actions sont porteuses de conséquences lourdes, tant pour la structure que pour l'individu ayant posé l'action. Cette problématique, si elle est facilement prise en compte par les décideurs et manager des organisations, doit aussi être appréhendée par les échelons intermédiaires, voire d'exécution, l'application incorrecte des ordres reçus pouvant conduire à un effondrement de la planification déployée par leurs organisations. Dans ce cadre, il est important de noter que ce travail ne fait pas fi des mécanismes de délégation, qui tendent à la responsabilisation des ac-

teurs de terrain. Néanmoins, dans le principe généralement admis et développé par Lagadec (1991) selon lequel la compétence primera sur le grade en situation de crise afin que la décision puisse être prise au plus près du terrain, ne se dispense pas du fait que la décision qui sera *in fine* posée doivent parfaitement correspondre aux attendus de l'organisation, servir l'effet final recherché comme défini par la structure et ne pas en dévier, sous peine de pouvoir engendrer des conséquences désastreuses.

Conscientes de ce risque, celles-ci ont souvent tenté d'en limiter la portée par différents processus. Aussi, afin d'avoir la visibilité et la maîtrise les plus précises sur le type d'actions effectuées par l'agent, beaucoup de structures ont développé un corpus de valeurs ayant vocation à être partagées avec leurs exécutants afin d'en justifier le bien-fondé. Ce corpus de valeurs permettrait de sécuriser l'organisation, mais aussi de faciliter le management. À ce titre, Barnard déclarera qu'il n'y aurait pas de management sans valeur (Barnard, 1938). Soulignons ici que cette question relative aux valeurs est également issue de la nécessité de donner une finalité et un sens à l'action des organisations qu'elles soient publiques ou privées. En effet, la nouvelle gouvernance publique place la promotion du bien public au titre de mission de l'action publique à l'égal de l'efficience et de la responsabilité (Chanut, Chomienne et Desmarais, 2015).

Avec les valeurs, on parlera alors de l'identité de l'organisation ou, selon le cas, de sa culture (Lemaître, 1987 ; Wittorski, 2010 ; Schield, 2004 ; Martin, Frost, Olivia O'Neill, 2006 ; Alvesson, 2011, Sveningsson et Alvesson, 2003 ; Larçon & Reitter, 1979, Alessandri, 2001). Ce corpus de valeurs a pour objectif d'être adopté par l'ensemble du groupe, au point d'engendrer une adhésion de nature à constituer un facteur de contrôle sur la nature des décisions arrêtées, d'améliorer l'exécution de consignes qui, si elles restent perçues comme servant l'organisation, s'inscriront également dans la droite ligne des valeurs admises par le personnel.

Bien sûr, il appartiendra aussi à l'organisation d'adapter le niveau des connaissances nécessaires à la meilleure exécution de la consigne ou à l'efficacité de la prise de décision en fonction du niveau de responsabilité des agents concernés. Ainsi, organisations et personnels partageant un socle de valeurs et de croyances communes, la confiance dans le bien-fondé de l'action voulue par la structure sera accrue. Par effet miroir, cette adhésion fera décroître les doutes et limitera l'émergence de décisions autonomes ou d'actions individuelles, par nature déviantes, au regard de celles définies par l'organisation. L'objectif sera donc de tisser un lien de confiance fort permettant de limiter les risques et, finalement, de sécuriser la stratégie organisationnelle, la structure concernée ayant pour cela au préalable défini et diffusé auprès de ses agents un ensemble de valeurs et de cognitions partagées.

Cette création d'un corpus commun de valeurs partagées intervient donc dans le but de prévenir une prise de décisions déviantes et l'exécution aléatoire, voire délétère, des consignes est un point récurrent pour toutes les organisations (Lemaître, 1987 ; Wittorski, 2010 ; Schield, 2004 ; Martin, Frost, Olivia O'Neill, 2006 ; Alvesson, 2011). Dans ce travail, la culture d'organisation est entendue comme pouvant être un levier de contrôle visant à obtenir une obéissance des décisions prises par le commandement ou la direction. Cette approche pourrait se voir opposer celle de l'*empowerment,* à savoir le processus par lequel les personnes ou les groupes amenés à intervenir ensemble pourraient développer leurs propres capacités d'action permettant leur émancipation (Bacqué, 2015). Si cette approche peut s'avérer pertinente en ce qu'elle est définie par Jouve (2006) comme opérationnelle sous réserve qu'elle bénéficie de la constitution de groupes amenés à être confrontés à une problématique commune, ce qui est le cas des équipes militaires, elle suppose néanmoins le développement de l'individualisation qui diffère de la nécessité du travail collaboratif inhérent à ce type d'équipe. Enfin en matière de ressources humaines, l'*empowerment* est généralement conceptualisé comme fondé sur

trois axes à savoir la vision, l'autonomie et l'appropriation. *De facto*, il apparaît que le premier point, la vision, se réfère au fait que le groupe ait une finalité qui ne peut s'entendre hors de la culture d'entreprise qui aura formé cette vision afin que l'autonomie du groupe soit tendue pour servir cette finalité qu'il se sentira légitime de servir (ce qui renvoie à l'appropriation). C'est dans ce contexte que nous avons pris le parti pris de penser la culture de l'organisation comme un moyen de sécuriser les processus et le déploiement de ses stratégies.

Cette problématique de sécurisation de déploiement des stratégies est commune à différents contextes à risque et dans des organisations très diverses. À ce titre, il convient ici de définir le risque comme étant un évènement qui sera perçu comme néfaste, mais qui ne s'est pas encore réalisé. Cependant, son apparition et ses conséquences délétères sont anticipées par la structure ou les individus, et peuvent aller de modérées à critiques. Cette approche correspond à une synthèse de différents travaux parmi lesquels ceux d'Azari et al. (2011), de Holzmann et Spiegler (2011) et de Wybo (2004), qui sont repris dans plusieurs études traitant des situations extrêmes (Lebraty, 2013).

Par ailleurs, si certains systèmes peuvent être confrontés à des risques dont les conséquences, certes importantes, restent circonscrites à leur seule structure, voire à leurs personnels, la réalisation de risques affectant d'autres entités peuvent avoir des effets beaucoup plus longs et toucher une structure macro de l'ampleur d'un État, allant jusqu'à affecter la sécurité nationale, voire l'équilibre financier mondial (i.e la faillite de la banque Lehman Brothers). Ainsi, le système bancaire est connu pour des risques financiers auxquels il est soumis. Ces risques doivent être envisagés, affrontés ou gérés par la structure. S'agissant des personnels confrontés à des situations extrêmes (Lièvre, 2004, 2009 ; Rivolier, 1998), les risques pouvant affecter l'intégrité physique ou la survenance de blessures mortelles peuvent devenir réels, voire omniprésents, et concerner un individu, voire l'ensemble du groupe. En outre, ce facteur de

risque immédiat peut s'étendre aux tiers présents sur la zone d'intervention, par exemple aux personnes présentes dans l'environnement proche.

Ce risque immédiat et tangible pourrait-il avoir un impact fort sur la prise de décision et l'exécution des consignes ? Il apparaît clairement que les organisations confrontées à ce type d'environnement s'attachent à développer un corpus solide de valeurs et qu'elles fondent une large part de leur communication et de leur formation sur la confiance entre individus et l'esprit d'équipe (Wittorski, 2008 ; Lemaitre, 1987). Les problématiques liées à la création d'un corpus de valeurs communes visant à renforcer la confiance des collaborateurs dans l'organisation pour en sécuriser la stratégie et des prises de décision individuelles seront l'objet de cette thèse. Ces problématiques se retrouvent donc tout naturellement dans les structures militaires telles que les armées.

En effet, les armées ont naturellement vocation à évoluer dans des situations extrêmes. Intervenant en tous lieux, les armées peuvent être confrontées à des environnements aux climats hostiles, inhospitaliers et inhabituels (altitude, profondeur, milieux tropicaux, désertiques ou glaciaires, terre, mer ou air). De même, la nature de leurs interventions les confronte à des adversaires dont l'objectif est leur destruction, tant au regard de la mission que de l'intégrité physique des personnels. Enfin, les actions de tous les membres du groupe auront un impact fort sur l'ensemble de la chaîne de décision responsable de la planification, du général de corps d'armée chargé de la planification au fantassin dont l'action fera, *in fine*, que la mission sera un succès ou un échec. Les conséquences pourront affecter les équilibres internationaux.

Les armées sont amenées à intervenir régulièrement en opérations extérieures (OPEX), voire sur le territoire national avec l'opération sentinelle mise en place depuis les attentats de 2015. Si ces interventions ne représentent pas la totalité de la vie des militaires, car les périodes d'OPEX ou de sentinelle sont alternées avec des périodes en caserne et donc or de situation

extrêmes, elles sont néanmoins une part considérable de la vie professionnelle de ces hommes et femmes. Or ces interventions se déroulent pour la plupart en situations extrêmes, soit dans des environnements où la constance de la tension permet de la qualifier d'« extrême », à la différence d'une situation de crise dont un évènement particulier serait l'origine (Wybo, 2004). Cependant, il est à noter qu'une situation extrême, de tension constante, peut être notoirement aggravée par la survenance d'un évènement déclencheur et alors devenir une situation de crise, échappant au contrôle et à la planification. À ce titre, il apparaît clairement que l'émergence d'une crise est très nettement plus probable dans une situation extrême caractérisée par un niveau inhérent de tension permanente.

Dans ce contexte, il apparaît donc que la communication développée, comme la gestion des informations diffusées, est essentielle dans des contextes de situations extrêmes. En effet, ces éléments peuvent amortir l'onde de choc due à l'apparition d'un « Black Swan » (Taleb, 1998) ou, au contraire, faire basculer la structure d'une situation de « routine » vers une situation « imprévue » ou « inattendue » (Godé, 2015) dans un contexte risqué de situation extrême.

Par ailleurs, l'explosion de tentatives et d'opérations de manipulation de l'information, dont les États et les sociétés civiles ont pu être des témoins tout autant que des cibles, prouve l'actualité du risque lié à la communication et à la diffusion d'informations susceptibles d'être altérées, modifiées ou crées à des fins d'instrumentalisation des acteurs. Plus encore, diverses pensées militaires envisagent que le domaine cognitif devienne, à court terme, un domaine de conflit au même titre que des domaines classiques de la guerre terrestre, maritime, aérienne, spatiale, électromagnétique et cybernétique (Wenzhe, 2019). Cette évolution incite à envisager l'utilisation du champ cognitif pour provoquer une prise de décision déviante comme étant un risque crédible.

À la lumière de ces éléments mêlant situation extrême et de crise, prise de décision pouvant altérer une stratégie globale et évolution de la pensée militaire et des stratégies offensives, il apparaît pertinent d'observer le contexte militaire. Ce dernier est tout particulièrement intéressant notamment en ce qu'il est un environnement où la situation est par nature paroxystique pour les hommes déployés en opération extérieures, mais également pour les États ordonnateurs d'actions dont les conséquences peuvent participer à la déstabilisation de nations. Enfin, les dernières évolutions technologiques, notamment la généralisation de l'Internet et de la consommation de données mobiles, ont profondément changé les vecteurs traditionnels de communication des organisations. Si elles pouvaient jusqu'alors maîtriser une communication faiblement exposée à une concurrence informationnelle extérieure, tel n'est plus le cas aujourd'hui. D'abord investi par la sphère privée, Internet est désormais largement utilisé par les entreprises qui recourent à une communication dématérialisée incluant les réseaux sociaux. Ainsi, la communication traditionnelle est désormais concurrencée par un milieu où elle a pris un retard notable en matière d'occupation de terrain, mais aussi de fluidité de transmission et donc de capacité de pénétration (Powell et Grodal, 2005 ; Antonelli, 2006). Ce constat prend un relief tout particulier alors que des affaires d'opérations d'influence informationnelle se font jour de toutes parts. C'est dans ce contexte, mêlant l'actualité du secteur privé et du secteur public, les enjeux géopolitiques et les relations internationales qu'il est apparu de première importance de s'interroger sur la possibilité de mettre en place des opérations informationnelles dont l'objectif serait d'altérer la confiance en ciblant les valeurs cœur des individus afin de déclencher une prise de décision déviante revenant à ne pas exécuter les ordres comme dispensés par l'organisation.

À cet égard, le conflit ukrainien aura permis une prise de conscience de la variété des opérations pouvant être engagées en temps de guerre par l'entremise d'une large variété de cyberat-

taques visant les systèmes et la captation de données, mais s'attaquant aussi à influencer les populations dans leur ensemble, tout autant que des groupes sociaux spécifiques. Ensuite, les campagnes de recrutement, notamment celles mises en place par l'État islamique (Bozorgmehri, 2018 ; Leander, 2016), ont renforcé cette prise de conscience. Il est également apparu que ces types d'opérations d'influence ne se cantonnaient pas aux périodes de guerre, mais pouvaient parfaitement être menées en temps de paix au sein de pays tiers, à l'insu des populations visées. À ce titre, plusieurs affaires ont crédibilisé ces hypothèses d'opérations d'influences. Citons notamment les soupçons d'influence apparus lors de l'élection de Donald Trump pendant la dernière élection présidentielle américaine ; ou encore l'influence déployée lors du référendum sur le Brexit, influence matérialisée par les révélations de l'affaire dite « Cambridge Analytica » où une société collectait les données des internautes pour ensuite définir des stratégies d'influences individualisées pour en accroître l'efficacité et influencer le vote de populations entières.

L'efficacité de ces manipulations de l'information semble ne plus faire débat, tout particulièrement dans des configurations de situations extrêmes. Il apparaît dès lors pertinent d'analyser les leviers qui permettent à ces opérations d'influence de se développer afin d'apprécier si l'instauration de valeurs communes au sein de groupes ou de structures leur permet de se préserver de ce type d'actions délétères, ou si, au contraire, elles y étaient plus sensibles. De fait, si ces organisations devaient se croire à l'abri de telles menaces, elles pourraient alors, s'appuyant sur un sentiment de sécurité erroné, abaisser leur niveau de vigilance au risque de déstructuration interne.

C'est dans ce contexte que le choix a été fait d'analyser la possibilité d'altération de la confiance liant une organisation intervenant dans des situations extrêmes à ses agents, altération créée dans le but d'impacter tant la prise de décision que l'exécution des ordres en résul-

Question de recherche	Dans un contexte de situations extrêmes soumis à une très forte pression de facteurs externes, en quoi la diffusion de certaines informations et le canal utilisé sont de nature à ne pas exécuter le ordre ou les décisions de la hiérarchie?	
Sous- problématiques	**Déclinaisons de la questions de recherche**	**Chapitre**
Altération de la confiance et prise de décision	Une organisation peut-elle utiliser des opération altérant la confiance des personnels à l'encontre d'une concurrente?	1-3
	Quelle serait la sémantique adaptable à ces nouvelles menaces ?	3
	Quelle est la nature de la confiance dans les organisations intervenant en situations extrêmes?	3
	Quels sont les apports des modèles théoriques issus de la théorie du choix rationnel ?	3
	La manipulation des informations peut-elle être appliquée dans le cadre militaire ainsi que pour d'autres organisations avouant en situation extrêmes?	3
	Quelle est la capacité d'alteration de la prise de décision d'informations centrées sur les valeurs professionnelles ?	5
Les valeurs et le renforcement de la confiance et des mécanismes de coopération	Les valeurs de l'organisation renforcent-elles les processus de coopération entre les différents agents?	3
	La présence de valeurs fortes protègent-elle les membres de l'organisation d'influences extérieures visant à altérer la prise de décision et la bonne exécution des consignes?	3-4-5
	Les valeurs sont-elles des failles de sécurité face à la diffusion d'informations dissonantes ?	5
	Les valeurs prônées par l'organisation restent-elles les même chez les agents ou varient-elles par l'entremise d'une sédimentation faite au sein des groupes de pairs ?	5-6
	L'attaque de valeurs des agents peut-elle engendrer une réactions outrepassant la formation à la prudence et à la prise de distance face aux sources peu fiables?	5
	Une difference dans la classification des valeurs entre l'organisation est les agents peut-elle être un risque à même d'engendrer une prise de décision déviante?	6
	Une difference de classification des valeurs peut-elle se faire en fonction de la classe d'âge (generation X,Y,Z)?	3- 5-6
La perméabilité aux informations divergentes de celles délivrées par l'organisation	La perception de l'organisation et de la hiérarchie peut-elle évoluer suite à la communication d'information aux personnels ?	1
	Quel impact du temps de consommation Internet?	3
	Internet peut-il être un vecteur efficace de ce type d'actions?	3 - 4
	Quelles résistances des informations délivrées par l'organisation face aux information extérieures?	4
	Pour les organisations intervenant en situations extrêmes, est-ce que l'impact des informations externes (particulièrement celles véhiculées par Internet) a des conséquences sur les pratiques quotidiennes de gestion des équipes ?	4
	Quelle influence de l'exposition aux situations extrêmes sur la confiance dans les différents niveaux de hiérarchie?	5
	L'ancienneté et le temps d'exposition en situation extrême participe à renforcer l'imperméabilité aux influences externes en accroissant la confiance entre les membres de l'organisation ?	5-6

tions ont constitué un ensemble d'expérimentations, il est légitime de supposer que les résultats de ces expériences ont fait l'objet d'une analyse destinée à améliorer le modèle dans l'hypothèse d'une utilisation future et optimisée permettant de perturber les cibles qui seraient

alors visées. En effet, l'altération de la confiance, par la manipulation des valeurs fortes des agents d'une organisation amenant à une déviance de la prise de décision, représente un risque majeur pour l'efficacité de la structure tant dans le déploiement de sa stratégie que dans la sécurisation de ses personnels. De manière générale, choisir des organisations intervenant en situation extrême permettait d'avoir des observations qui sont particulièrement parlantes et facilitent le travail d'analyse et de recherche. En outre, le contexte permettait d'interviewer des personnes qui avaient déjà été soumises à ce genre d'opérations, ce qui représentait un matériau précieux. Enfin, en raison de leurs spécificités, les sujets de la recherche répondaient parfaitement aux profils définis comme hypersensibles par la théorie (Aronson, 1968, 1992, 2019 ; Stone & Cooper, 2001) dans son développement fonctionnel de la conception de la dissonance cognitive initialement exprimée par Festinger (1957).

Dans le prolongement de l'analyse des premiers entretiens exploratoires de 2017, dont les résultats ont fait l'objet d'un article[1] qui sera présenté en chapitre 1, une seconde vague d'interviews a été réalisée en deux phases en 2018, afin de tester le modèle et valider les propositions élaborées. Le bilan tiré de la première vague d'entretiens a permis de définir le contenu de la seconde vague d'interviews (profils professionnels, âges des sujets, etc.) puis de construire et d'affiner la grille d'entretien. L'étude exposée dans l'article précité, menée initialement au titre de travaux d'analyse et d'audit hors contexte de recherches, a permis de définir et d'affiner la problématique, mais aussi de justifier l'engagement du travail de recherche plus large développé dans de cette thèse.

Tableau résumant la question de recherche, ses sous-problématiques afférentes et leurs déclinaisons et chapitres où elles sont abordées

[1] Article publié dans le revue Dynamiques Internationales en 2018

À la suite à la première phase de la seconde vague d'entretiens, menée en mai 2018, l'influence de la communication est apparue importante dans le processus de modification de la prise de décision par perte de confiance des agents dans les structures organisationnelles. En effet, les interviews portaient sur l'influence de la communication de l'organisation, sur sa résistance et son efficacité face aux influences extérieures. En d'autres termes, la communication verticale a été comparée à la communication transverse, non maîtrisée par l'organisation, à laquelle ses membres sont soumis. Cette analyse fait l'objet d'une communication qui, effectuée en septembre 2018, qui est présenté dans un des chapitres de cette thèse.

Étant entendu la nature du sujet, un article a abordé la problématique observée dans le cas ukrainien présenté dans le chapitre un, mais en l'abordant sous l'angle d'une approche cyber. En effet, le chapitre 1 retrace des observations menées hors contexte de recherche, dans une perspective orientée sur des objets techniques liés au conflit et aux opérations cyber. A contrario, l'article présenté en première partie du chapitre 3 et publié dans *The Journal of Intelligence and Cyber Security* en juin 2019, aborde la question des opérations cyber sous l'angle de l'influence et non dans une approche technique. Cette démarche a débouché sur des questions de ressources humaines et de psychologie liées à la perméabilité des acteurs, tout spécialement à la lumière des stratégies militaires développées notamment par la Fédération de Russie dans ce domaine particulier. Ce travail intègre la problématique de l'influence, en particulier l'étude visant à cibler la confiance des personnels militaires dans les stratégies mises en place à travers la New Generation War (NGW) par la Fédération de Russie, où l'influence des populations par l'entremise des différents canaux informationnels est un champ offensif à lui seul. En outre, cet article présente les résultats obtenus sous l'angle des théories Heuris-

tic and Biases (HB) développées Kanheman et Tversky (1977) dans le prolongement des théories du choix rationnel (Friedman, 1953; Simon 1965)**.** Cette analyse a mis en évidence l'importance de la confiance comme cadre d'actions en situation extrême. Ce sujet sera traité dans la seconde partie du chapitre 3 de cette thèse, au travers d'un second article qui analyse la nature de la confiance dans les situations paroxystiques. Cet article a fait l'objet d'une communication présentée lors des seizièmes journées de la collaboration scientifique entre les Écoles doctorales en gestion de l'Université de Paris I-Panthéon -Sorbonne et de l'Université Libre de Bruxelles de mars 2019. Ce travail s'appuie sur les interviews de la seconde phase de la deuxième vague d'entretiens, réalisée en octobre 2018. L'ensemble des interviews a permis d'appréhender la confiance comme « game changer », que cela soit dans la prise de décision ou dans l'exécution des ordres qui dans le cas particulier des armées, cas d'espèce transposable aux organisations intervenant en situation extrême. Dans ce cas précis, ce sujet est d'autant plus prégnant qu'il peut emporter des conséquences immédiates et irréversibles, qu'il s'agisse de la structure ou de ses personnels qui risquent leur vie en OPEX. Les concepts de confiance, leurs fondements et leur influence dans la prise de décision et l'exécution des consignes y ont été développés et analysés. Il en ressort que, intervenant dans la prise de décision comme dans l'exécution des ordres, la confiance est la pierre angulaire de l'efficacité de l'organisation et de la sécurisation des processus. Elle demeure indissociable des valeurs communément partagées par les agents de l'organisation, qu'il s'agisse de son identité ou de sa culture.

Les premières observations ayant mis en lumière l'intervention de canaux de communication dématérialisés, il semblait pertinent d'analyser le poids de la communication institutionnelle face à ce type de menace, car il apparaît que cette dernière représente un

moyen d'ampleur pour lutter contre le phénomène observé. Pour ce faire, nous nous sommes interrogés sur l'impact des nouveaux modes de circulation de l'information par Internet et sur les modes de gestion RH, en nous basant sur les entretiens de la première phase de la seconde vague. Ce travail a été soumis en conférence et fera l'objet du chapitre 4.

Traitant de la perception et de la nature de la confiance, un autre volet de ce travail de recherche prend appui sur un corpus théorique empruntant à la psychologie sociale, particulièrement à la dissonance cognitive (Cognitive Dissonance Theory—CDT). Dans une approche opérationnelle, une étude a été menée afin d'identifier les leviers susceptibles d'altérer la confiance et, par effet miroir, de s'en prémunir. En outre, lors de la seconde phase de la deuxième vague des entretiens, une observation dirigée de type expérimental a été réalisée afin de valider le modèle contenu dans les propositions formulées dans ce travail. Les résultats de cette expérimentation font l'objet d'une part importante de chapitre 5. Ce chapitre se fonde sur un article présenté à Revue Européenne de Psychologie, co-écrit avec David Vaidis et dont la rédactrice de cette thèse est l'auteure principale.

L'importance des valeurs a été clairement mise en avant dans les chapitres précités. Aussi, ce travail de recherche a porté sur l'influence de la hiérarchisation des valeurs dans la confiance. L'influence d'une hiérarchie de valeurs différentes entre l'organisation et ses membres a été analysée. Cette hiérarchisation a été examinée dans le cas, d'une part, d'une divergence de classement entre l'organisation et ses membres, entre les membres d'une même équipe de l'organisation, d'autre part. La nature et l'origine de ces hiérarchisations divergentes ont aussi été analysées. La première proposition était liée à l'âge des personnels étant rappelé que, lors des premiers entretiens exploratoires,

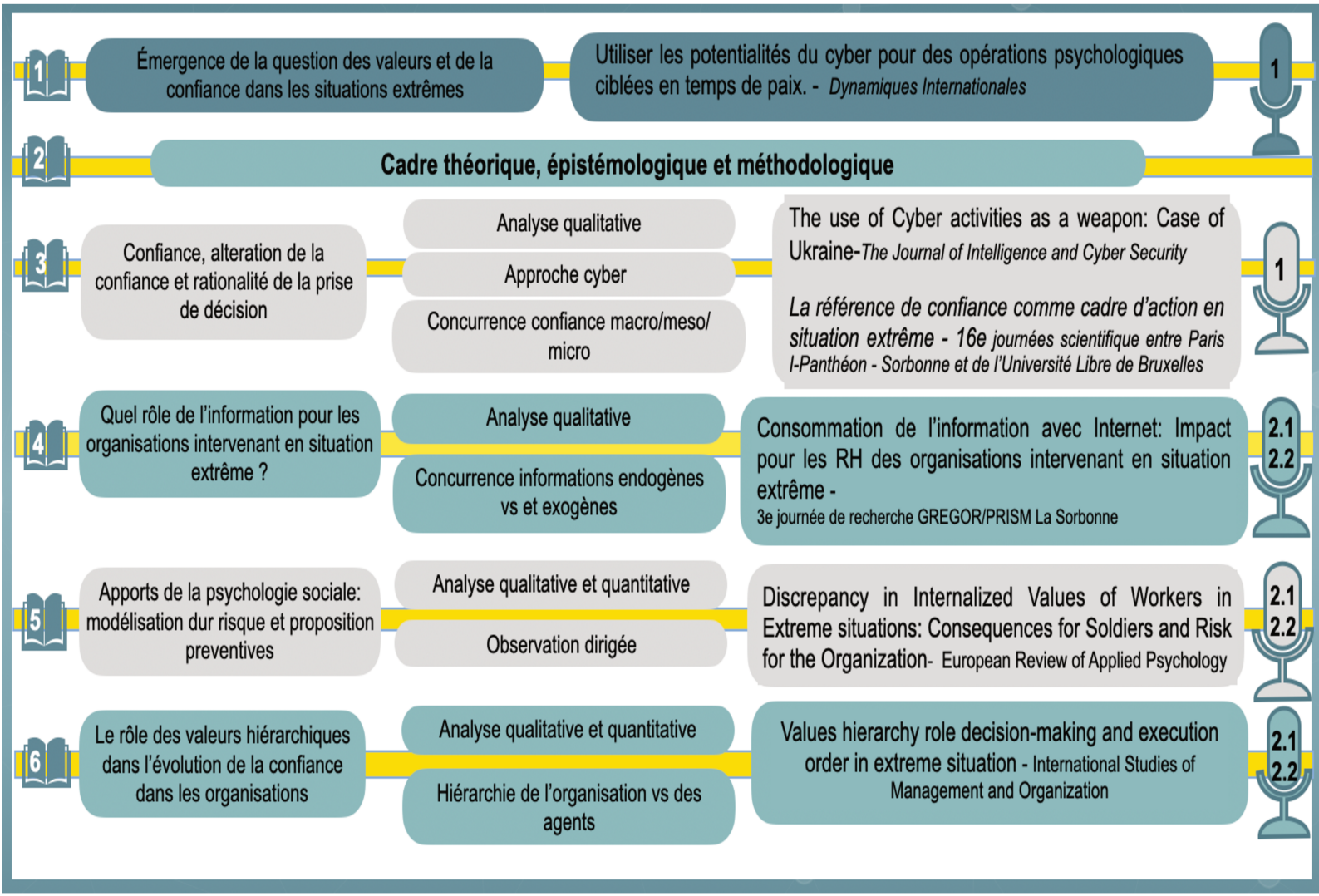
les modalités de consommation de données Internet avaient été analysées avec d'autant plus d'attention que la plupart des opérations belliqueuses visant à altérer la confiance avaient été menées sur des réseaux sociaux, des plateformes de broadcast et des blogs. Or la connectivité des individus est classiquement catégorisée au travers de générations qualifiées de « x », « y » et « z »[2]. Des résultats contre-intuitifs apparaissent quant aux motifs influant sur la hiérarchisation des valeurs[3]. Cet article sera présenté en chapitre 6 de cette thèse.

Ces travaux relèvent d'une démarche qualitative à base d'analyse d'entretiens et d'informations recueillies sur le terrain, en zones sensibles et de guerre, dans une logique interprétative. La suite de ce travail a été construite sur des entretiens exploratoires divisés en deux vagues et trois phases. Ces interviews étaient extrêmement peu dirigées, mais contenaient néanmoins une base de questions récurrentes permettant un double traitement des données, tant quantitatif que qualitatif. Les entretiens de février 2017 sont le résultat d'un travail mené sur le terrain depuis 2014 notamment au travers de différents entretiens préexploratoires. La seconde vague d'entretiens a été organisée à l'issue de l'analyse des interviews de 2017. Elle avait pour finalité de valider les propositions issues de l'analyse des premiers entretiens exploratoires.

---

[2] Generation X (nés entre 1965 et 1976), Generation Y (nés entre1977 et 1995) , Z generation (nés après 1996).

[3] Ce travail fait l'objet d'un article soumis en février 2020 encore en reviewing



Schema du design de la thèse par chapitre mentionné dans l'icône « livre », indiquant le titre du chapitre, la méthode employée dans l'article présenté dans le chapitre, le titre de l'article composant l'article et la vague et phase des entretiens utilisés dans l'article inscrit dans l'icône « micro ».

Références

Antonelli, Cristiano. 2006. “The Business Governance of Localized Knowledge: An Information Economics Approach for the Economics of Knowledge.” *Industry and Innovation* 13 (3): 227–61. https://doi.org/10.1080/13662710600858118.

Aronson, Elliot. 1968. “*The Cognitive and Behavioral Consequences of the Confirmation and Disconfirmation of Expectations.*”Application for research Grant submitted to the National Science Foundation, Harvard University.

Aubry, Monique, Lièvre, Pascal and Hobbs, Brian. 2010. “Project Management in Extreme Environments.” *Project Management Journal.* https://doi.org/10.1002/pmj.20185.

Barnard, Chester. 1938. *The Functions of the Executive.* Harvard University Press (1974 edition).

Bao, Jiefangjun. 2019. “OE Watch, Vol 09, Issue 12 December 2019 | Intercontinental Ballistic Missile | Submarines.” *Foreign Military Stufy Ofice OEWatch*. December 12th, 2019. https://fr.scribd.com/document/440394534/OE-Wa

Bozorgmehri, Majid. 2018. “Recruitment of Foreign Members by Islamic State (Daesh): Tools and Methods.” *Journal of Politics and Law,* 11 (4): 51. https://doi.org/10.5539/jpl.v11n4p51.

Chanlat, Jean-François, and Seguin, Françoise. (1987). *L’analyse Des Organisations Une Anthologie Sociologique.* Tome II : Les composantes de l’organisation, Montréal, Gaëtan Morin éditeur.

Chanut, Veronique., Chomienne, Hervé., & Desmarais, Céline. (2015). Pratiques valorielles et management public. *Revue Internationale Des Sciences Administratives,* 81(2), 235. https://doi.org/10.3917/risa.812.0235

Charles, Thierry. 2012. “Fukushima, Un an Après.” Institut de Radioprotection et de Sûreté Nucléaire. February 28th, 2012. https://www.irsn.fr/FR/connaissances/Installations_nucleaires/Les-accidents-nucleaires/accident-fuk

Duprez, Jean-Marie. 1982. “Larçon Jean-Paul et Reitter Roland, Structures de Pouvoir et Identité de l’entreprise.” *Revue Française de Sociologie* 23 (2): 321–22.

Demeriou Danielle. 2011. “Japan: Fukushima 50 Criticise ‘inconsistent’ Information—Telegraph.” *The Telegraph*. Avril 22cd, 2011.

Girin Jacques. 1995. “Les agencements organisationnels”, dans Charue-Duboc Florence [ed] Des savoirs en action. Contributions de la recherche en gestion, Paris, L’Harmattan, pp. 233-279.

Golène Mathieu. 2011. « Japon: Les Clochards Du Nucléaire » - L'Express." *L'express.* Avril 2cd, 2011.

Goudet Jean-Luc. 2017. "Fukushima : Retour Sur La Tragique Catastrophe Nucléaire." *Futura Planet.* Mars 12th, 2017.

Greenberg, Jeff, and Arndt, Jamie. (2012). "Terror Management Theory." In Handbook of Theories of Social Psychology: Volume 1, 398–415. SAGE Publications Inc. https://doi.org/10.4135/9781446249215.n20.

Greenberg, Jeff, Pyszczynski, Tom and Solomon, Sheldon. "The Causes and Consequences of a Need for Self-Esteem: A Terror Management Theory." In Public Self and Private Self, New York, Springer 1986. 189–212.. https://doi.org/10.1007/978-1-4613-9564-5_10.

Heine, Steven J., Proulx, Travis and Vohs, Kathleen D.. 2006. "The Meaning Maintenance Model: On the Coherence of Social Motivations." *Personality and Social Psychology Review,* 10 (2): 88–110. https://doi.org/10.1207/s15327957pspr1002_1.

Hogg Chris. 2011. "Japan Hails the Heroic 'Fukushima 50'—BBC News." BBC News. Mars 17th, 2011.

Holzmann, Vered, and Spiegler, Israel. 2011. "Developing Risk Breakdown Structure for Information Technology Organizations." *International Journal of Project Management,* 29 (5): 537–46. https://doi.org/10.1016/j.ijproman.2010.05.002.

Jinping, Xi. 2017. "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era." *Xinhua News*, 66, Avril 11th, 2017.

Jouve, Bernard. 2006. "Politiques Publiques et Empowerment : L'exception Française." *Économie & Humanisme,* 379, 99- 101

Karimiazari Amirreza, Mousavi, Neda ; Mousavi, Farid and Seyedbagher Hosseini. 2011. "Risk Assessment Model Selection in Construction Industry." *Expert Systems with Applications*, 38 (8): 9105–11. https://doi.org/10.1016/j.eswa.2010.12.110.

Lagadec, Patrick. (2011). *La gestion de crise outils de reflexions à l'usage des décideurs.* Paris: McGraw-Hill

Leander, Anna. 2017. "Digital/Commercial (in)Visibility." *European Journal of Social Theory,* 20 (3): 348–72. https://doi.org/10.1177/1368431016668365.

Lebraty, Jean-Fabrice. 2013. “SI et Situations Extrêmes.” *Systèmes d’information & Management,* 18 (1): 3-10. https://doi.org/10.3917/sim.131.0003.

Lemaître Nadine. 1987. *A propos… de la culture d’entreprise (un exemple d’écrit typiquement managérial)* Chanlat, Jean-François ; Séguin, Francine (dir) dans L’analyse Des Organisations, Une Anthologie Sociologique. Tome 2 : Les Composantes de l’organisation, Montréal/Paris, ESKA/Gaëtan Morin, 1987, 419–433.

Lièvre, Pascal, and Gautier, Anaïs. 2009. “Les Registres de La Logistique Des Situations Extrêmes : Des Expéditions Polaires Aux Services d’incendies et Secours.” *Management & Avenir,* 24 (4): 196. https://doi.org/10.3917/mav.024.0196.

Lièvre Pascal, and Rix-Lièvre Géraldine. 2004. “Le Management Des Expéditions Polaires.” *Management & Avenir ,* 24 (9): 1–12.

Lipietz, Alain. 2017. “L’empowerment, Une Pratique Émancipatrice, by Marie-Hélène Bacqué, and Carole Biewener.” *Rethinking Marxism,* 29(3):499-503. https://doi.org/10.1080/08935696.2017.1385323.

McGregor, Ian, Zanna, Mark P. ; Holmes, John G.; and Spencer, Steven J. 2001. “Compensatory Conviction in the Face of Personal Uncertainty: Going to Extremes and Being Oneself.” *Journal of Personality and Social Psychology,* 80 (3): 472–88. https://doi.org/10.1037/0022-3514.80.3.472.

McNaughton, Neil, and Jeffrey A. Gray. 2000. “Anxiolytic Action on the Behavioural Inhibition System Implies Multiple Types of Arousal Contribute to Anxiety.” *Journal of Affective Disorders,* 61 (3): 161–76. https://doi.org/10.1016/S0165-0327(00)00344-X.

Newby-Clark, Ian R., Ian McGregor, and Mark P. Zanna. 2002. “Thinking and Caring about Cognitive Inconsistency: When and for Whom Does Attitudinal Ambivalence Feel Uncomfortable?” *Journal of Personality and Social Psychology,* 82 (2): 157–66. https://doi.org/10.1037/0022-3514.82.2.157.

O’Neil Vincent. 2019. “199. ‘Intelligentization’ and a Chinese Vision of Future War | Mad Scientist Laboratory.” *Mad Scientist Laboratory.* December 19th, 2019.

Powell Walter, and Grodal, Stine (2005). *Networks and Innovators.* The Oxford Handbook of Innovation.Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199286805.001.0001

Proulx, Travis, and Inzlicht, Michael. 2012. “The Five ‘A’s of Meaning Maintenance: Finding Meaning in the Theories of Sense-Making.” *Psychological Inquiry,* 23 (4): 317–35. https://doi.org/10.1080/1047840X.2012.702372.

Randles, Daniel, Inzlicht, Michael ; Proulx, Travis; Tullett, Alexa M. and Heine., Steven J. 2015. "Is Dissonance Reduction a Special Case of Fluid Compensation? Evidence That Dissonant Cognitions Cause Compensatory Affirmation and Abstraction." *Journal of Personality and Social Psychology* ,108 (5): 697–710. https://doi.org/10.1037/a0038933.

Rivolier, Jean. 1998. Stress et situation extrême, *Bulletins de la psychologie*, 51, 6.

Schmeichel, Brandon J.; Gailliot, Matthew T. ; Filardo, Emily Ana; McGregor, Ian ; Gitter, Seth and Baumeister, Roy F.. 2009. "Terror Management Theory and Self-Esteem Revisited: The Roles of Implicit and Explicit Self-Esteem in Mortality Salience Effects." *Journal of Personality and Social Psychology* , 96 (5): 1077–87. https://doi.org/10.1037/a0015091.

Simon, Linda, Jeff Greenberg, and Jack Brehm. 1995. "Trivialization: The Forgotten Mode of Dissonance Reduction." *Journal of Personality and Social Psychology* , 68 (2): 247–60. https://doi.org/10.1037/0022-3514.68.2.247.

Simon H.A. (1965), Administrative behavior, 2nd edition, The Free Press, New York.

Snowden, D.J., Boone, M.J.,. (2007). A Leader's Framework for Decision Making, *Harvard Business Review*.https://hbr.org/2007/11/a-leaders-framework-for-decision-making

Steele, Claude. The psychology of self-affirmation: Sustaining the integrity of the self. In R. F. Baumeister (Ed.), Key readings in social psychology. The self in social psychology, Psychology Press, 1999, 372–390.

Stone, Jeff, and Cooper, Joel . 2001. "A Self-Standards Model of Cognitive Dissonance." *Journal of Experimental Social Psychology* , 37 (3): 228–43. https://doi.org/10.1006/jesp.2000.1446.

Sveningsson, Stefan, and Mats Alvesson. 2003. "Managing Managerial Identities: Organizational Fragmentation, Discourse and Identity Struggle." *Human Relations,* 56 (10): 1163–93. https://doi.org/10.1177/00187267035610001.

Thibodeau, Ruth, and Elliot Aronson. 1992. "Taking a Closer Look: Reasserting the Role of the Self-Concept in Dissonance Theory." *Personality and Social Psychology Bulletin,* 18 (5): 591–602. https://doi.org/10.1177/0146167292185010.

Wittorski. Richard. (1999). La notion d'identité collective dans Kaddouri Mokhtar, Lespessailles Corinne, Maillebouis Madeleine, Vasconcellos Maria (dir) *La question identitaire dans le travail et la formation : contributions de la recherche, état des pratiques et étude bibliographique,* Paris: L'Harmattan, 195-213, 2008

Wybo, Jean Luc. 2004. “Mastering Risks of Damage and Risks of Crisis: The Role of Organisational Learning.” *International Journal of Emergency Management,* 2 (1–2): 22–34. https://doi.org/10.1504/IJEM.2004.005228.

CHAPITRE 1 : L'émergence de la question des valeurs et de la confiance dans les situations extrêmes

Suite aux entretiens exploratoires de 2014, une première vague d'entretiens s'est tenue en février 2017 sur le terrain ukrainien. Cet ensemble d'entretiens exploratoires, menés sans cadre théorique prédéfini, a permis de faire émerger la question de recherche. Outre l'émergence de la problématique de la recherche, ces entretiens ont permis d'identifier les principaux concepts théoriques qui, préalables à la proposition d'un cadre, seront interrogés et testés dans la suite de ce travail. Lors de cette première étape, les questionnements portaient sur les conséquences d'une perte de confiance, notamment sur l'exécution de l'ordre, mais aussi sur les raisons de cette perte de confiance. Cette étude exploratoire, à vocation de sécurité militaire, met en évidence des questions de management transposables à d'autres milieux professionnels. C'est à la suite de ce constat qu'il est apparu pertinent de rapprocher ce travail des problématiques de management au sens large, plutôt que de le limiter au seul périmètre des affaires militaires et de sécurité. L'analyse de ces entretiens exploratoires a fait l'objet d'un article publié en juin 2018 dans le n°13 de la revue de Relations internationales Dynamiques Internationale.

Introduction

En novembre 2014, Viktor Ianoukovitch renonçait à un accord avec l'Union européenne à une semaine de sa signature. Ce moment avait pourtant été préparé très en amont, mais le Président préférait ne pas le signer afin, selon lui, de relancer ses relations économiques avec la Russie. L'accord d'association était attendu de longue date, par les partenaires européens qui l'avaient travaillé pendant plusieurs mois, mais également par la population ukrainienne, tout particulièrement par les étudiants de Kiev. La réaction en Ukraine fut immédiate, les étudiants descendirent dans la rue pour manifester leur désapprobation. Alors que le mouvement perdait en vigueur, la présidence prit la décision de faire charger les Berkuts. Cette opération violente eut pour effet de renforcer le mouvement de protestation : la population qui était jusqu'alors témoin des manifestations se déroulant sur la place Maïdan se joignit aux étudiants victimes de la répression violente des Berkuts. Ce qui devint alors « la Révolution du Maïdan » fut largement relayé par les médias, mais aussi par les réseaux sociaux et autres Twitter. Le mouvement gagna en vigueur, d'autres villes connurent aussi « leur » Maïdan et la tension monta jusqu'à un paroxysme atteint en février. À cette date, 80 personnes trouvèrent la mort à Kyiv, notamment à la suite des tirs de snipers. Le 22 février, Viktor Ianoukovitch quittait Kyiv et dans la foulée, un gouvernement provisoire s'installa sous la direction d'Alexandr Tourtchinov dans l'attente d'élections anticipées au mois de mai. Cependant, une partie de la population principalement dans l'est du pays (qui se trouvait aussi être le berceau du président déchu) s'opposa à la révolution du Maïdan et au gouvernement provisoire. Ainsi à partir du 23 février 2014, des manifestations « anti-maïdans » se développèrent dans plusieurs villes de l'est : Donetsk, Kramatorsk, Louhansk, Marioupol, Slaviansk, Kharkiv (seconde plus grande ville d'Ukraine). Elles

s'étendirent à Odessa, ville située au sud-ouest de l'Ukraine, et furent rejointes par d'autres protestations en Crimée. Ces mouvements d'opposition eurent plusieurs sources : si la crainte de la contagion de la violence en était une, la peur des oligarques locaux de voir leurs empires s'effondrer ou être financièrement captés par le nouveau gouvernement central en était une autre. Ce mouvement d'opposition trouva un prompt soutien exogène dans la Fédération de Russie où Viktor Ianoukovitch avait trouvé refuge. La Russie, au nom de la défense des peuples russes et du droit, refusa de reconnaître le gouvernement provisoire, accusé d'être illégitime, car fruit d'un coup d'État. Rapidement, la situation dégénéra : des échauffourées explosèrent dans l'est, et dégénérèrent rapidement en une insurrection armée. Les « séparatistes » du Donbass proclamèrent la création de la « République populaire de Donetsk » le 7 avril 2014, suivies par la proclamation de la « République populaire de Louhansk» le 11 mai.

Les séparatistes ne reconnaissant pas le gouvernement provisoire et étant acteurs de l'insurrection, ils furent rapidement qualifiés de « terroristes » par Kyiv, qui devint aux yeux des dits terroristes un gouvernement de « fascistes » et de « nazis ». À partir du 2 mai 2014, l'armée ukrainienne intervint dans l'est du pays donnant à l'insurrection armée le tour d'une vraie guerre fratricide, soutenue par une puissance exogène. Ce conflit (toujours en cours malgré les accords de Minsk 1 [de septembre 2014] et de Minsk 2 [de février 2015] qui avaient pour objet de faire revenir la paix sur le territoire) fut accompagné d'une vaste opération de cyberattaques visant les systèmes, mais aussi la population au travers de vastes opérations informationnelles.

1. Contexte cyber en Ukraine

Afin de comprendre de quelle manière le développement d'une vague massive d'opérations cyber fut possible, il convient de revenir sur le contexte du cyber dans le pays. Tout d'abord, rappelons qu'en 2011 l'Ukraine se classait au neuvième rang des 10 premiers pays connecté à Internet d'Europe, en affichant une pénétration du réseau de 33,9 % sur quelque 15,3 millions d'utilisateurs, pourcentage qui passait à 36,8 % en 2012. Avec un maillage plus fin, cela signifie que 48 % des Ukrainiens de plus de 15 ans avaient accès à Internet en 2012 et que 31 % d'entre eux se connectaient quotidiennement[4]. Concernant les connexions aux réseaux sociaux, on estime que Facebook avait 3 000 000 d'utilisateurs en Ukraine en 2013[5]. Concernant Twitter, qui fut très actif depuis le Maïdan, Google Analytics estime qu'en 2012 le nombre de visiteurs de la plateforme atteignait 120 000, même si GfK Ukraine[6] constatait que 28 % des utilisateurs ukrainiens de Twitter ne vérifiaient leurs comptes que de temps en temps. Le site le plus visité en Ukraine restait Vkontakte (l'équivalent de Facebook en russe) [7]: en février 2013, l'audience quotidienne de Vkontakte atteignait 9,35 millions soit 20,2 % du trafic mondial quotidien moyen du réseau.

Outre ces chiffres relatifs à l'utilisation d'Internet, il faut signaler d'autres points d'intérêt : historiquement, l'Internet ukrainien était majoritairement en russe (RuNEt) ce qui a eu une influence évidente dans les opérations à visée offensive menées par la Russie

---

[4] Internet Association of Ukraine

[5] Olga Minchenko « Вже 3 мільйони українців користуються Facebook »*Watcher*, 20 octobre 2013 watcher.com.ua". watcher.com.ua. 2013-10-25. Retrieved 2014-08-03.

[6] Société d'étude de marché

[7] Alexa « Top Sites in Ukraine »
https://www.alexa.com/topsites/countries/UA

dans le cyber espace. En outre, le développement de l'industrie IT sur le territoire a été très fort permettant à l'Ukraine de jouir de nombre de ressources humaines maîtrisant la technologie. Ce contexte a favorisé le développement d'un large réseau d'« Hacktivistes » qui décidèrent de se battre dans le cyber espace contre les hackers agissant pour les intérêts séparatistes.

Le développement de RuNet, l'Internet russe, a des racines historiques. Dans les années 90, le climat géopolitique ainsi que l'isolation de l'URSS puis de la Russie, de même que le mauvais état des liaisons internationales entre ces territoires et l'Europe ont été des facteurs qui ont poussé la Russie à développer ses propres compétences en matière de cyber, coupées et isolées des puissances occidentales. Par ailleurs, l'inter-connexion forte des infrastructures, notamment de télécommunications, entre la Russie et les anciennes Républiques de l'URSS a été autant de facilitateurs pour l'unité et le développement du RuNet. Enfin, l'explosion des marchés pétroliers a fourni la manne financière nécessaire à l'accroissement de RuNet. De facto, cette interconnexion, fruit de l'histoire, aura grandement facilité la pénétration informationnelle pro séparatiste en Ukraine notamment à la faveur du partage de la langue, de la culture et d'un réseau de communication commun. Cette interconnexion et le fait d'avoir dû développer leurs propres compétences laissèrent une longueur d'avance aux Russes, même si la création en 2005 de la dorsale Trans-Europe-Asie (TEA) a ouvert l'accès de ces territoires aux entreprises occidentales.

Afin d'avoir une vision d'ensemble du contexte et de la perception du cyber dans la région, il faut s'intéresser à la directive-cadre rédigée en 2000 en Russie intitulée « Doctrine de sécurité informationnelle de la Fédération de Russie »[8]. Dans ce texte fondateur

[8] http ://www.scrf.gov.ru/documents/5.html

et précurseur, les notions de « guerre informationnelle » sont abordées et décrites comme une « confrontation entre deux ou plusieurs États dans l'espace de l'information visant à endommager les systèmes d'information, les processus et les ressources, des structures "critiques", affaiblissant les systèmes politiques, économiques et sociaux. Action psychologique massive envers la population pour déstabiliser la société et l'État, ainsi qu'une influence forçant l'État visé à prendre des mesures dans l'intérêt du parti adverse ». Cette définition donne une importance primordiale aux actions orientées vers les populations, et donc aux opérations psychologiques de grande envergure. En 2011, la notion de guerre informationnelle est finalement clairement définie dans les « Concepts sur les activités des forces armées de la Fédération de Russie dans le cyberespace »[9] renforçant l'ébauche de 2000. On peut y lire : « Guerre informationnelle : confrontation entre au moins deux États dans le cyberespace (…) destinée à saper le système politique, économique et social, et à accomplir un lavage de cerveau massif de la population afin de déstabiliser la société et l'État. ».

Peu de temps après, le SVR (service de renseignement extérieur russe) diffusera des appels d'offres ayant pour objet la distribution massive de contenus dans des réseaux sociaux donnés dans le but de façonner l'opinion publique ». C'est dans ce contexte que se développe la guerre du Donbass.

[9] https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf

1.1. Le cyber dans les conflits modernes : le cas ukrainien

Concernant le volet relatif aux attaques cyber dans le conflit ukrainien, il apparaît clairement aujourd'hui qu'il est le fruit d'une stratégie globale, tant il toucha simultanément les structures en dur, le développement de cyber attaques sur des sites d'intérêts stratégiques, l'intervention de hackers suspectés d'être rattachés au pouvoir russe, mais aussi l'apparition de nombreuses opérations psychologiques plus subtiles visant à influencer différentes strates de la population.

Concernant les infrastructures en dur, rappelons que l'un des premiers objectifs après l'entrée des « petits hommes verts »[10] en Crimée, le 28 février 2014, et après la maîtrise des aéroports de Simferopol et Sébastopol, fut de prendre le contrôle des structures de télécommunication. Cette motivation se matérialisa au travers de la coupure des câbles à fibre optique reliant la Crimée à l'Ukraine. En mars, soit à peine un mois après l'annexion, Rostelecom[11] déployait un câble sous-marin à fibre optique de 46 kilomètres dans le détroit de Kertch, reliant directement les fournisseurs d'accès Internet (FAI) de Crimée à la Russie. Aujourd'hui, toutes les données sortant de Crimée transitent en premier lieu par la Russie. Dans le Donbass, les paquets de données des territoires détenus par les séparatistes transitent également par la Russie alors que ceux des régions frontalières sous contrôle ukrainien passent par les hubs de Kharkov ou d'Odessa. Cette ventilation des données a notamment été rendue possible par la multitude de FAI qui facilite largement ce découpage permettant ainsi aisément — et avec de moindres efforts — d'opérer une captation de données pouvant être mises au service d'opérations informationnelles servant des objectifs géopolitiques.

---

[10] Terme couramment employés pour décrire les hommes en armes ne portant pas d'identification nationale sur leur treillis qui débarquèrent en Ukraine au début de l'annexion.

[11] Entreprise russe de télécoms

S'agissant des menaces sur les sites et systèmes, le gouvernement ukrainien annonçait en décembre 2016 avoir subi 6 500 attaques pendant les seuls mois d'octobre et de novembre de la même année, et bien que le Président Porochenko ait accusé la Russie d'être à l'origine de ces offensives[12], l'impossibilité de fournir des preuves indiscutables de l'implication du Kremlin ne permit pas de donner des suites légales à ce qui restait des allégations.

Ces attaques, de même que celles qui les précédèrent et les suivirent, furent de différentes natures. Beaucoup utilisèrent des DDoS (déni de service distribué) sur des sites choisis, car ces attaques ont le double avantage d'être efficaces en ce qui concerne de désorganisation et de limiter le risque de contagion pour son créateur. À la différence des malwares et autres logiciels malveillants, qui, par l'interconnexion du réseau, pourrait revenir en boomerang vers le pays d'origine de leur initiateur, elles se cantonnent aux seuls sites visés. Cependant, le risque de contagion n'empêcha pas l'Ukraine d'être touchée par NotPetya qui a touché environ 20 % des structures administratives de l'État. Les attaques menées sur les centrales électriques en 2015 et 2016 restent également mémorables, la seconde ayant plongé Kyiv dans le noir pendant plus d'une heure[13]. Dans le cas précis de cette attaque, les soupçons se portent sur le groupe de hackers Sandworm, d'origine russe. Pour nombre d'experts dans le champ de la cyber sécurité, cette attaque pourrait tout à fait avoir été un test en prévision d'opérations de plus grande ampleur.

Du point de vue informationnel, de nombreux « leaks » ou fuites, hacks de mails et vols d'informations stratégiques furent réalisés comme, par exemple, le hack des communi-

---

[12] Natalia Zinets « Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar' », Reuters, 29 December 2016

[13] Reynald Flechaux « Nouveau black-out en Ukraine : encore une cyberattaque ? » Silicon, 21 décembre 2016.

cations de 800 personnalités ukrainiennes d'intérêt au moment même où des hommes en arme posaient le pied en Crimée. Cette opération précise fut revendiquée par les « CyberBerkuts », un autre groupe de hackers apparut dans le paysage du conflit ukrainien en avril 2014. Si ce groupe se prétendait autonome, il a été fortement soupçonné d'être en lien direct avec le Kremlin.

Concernant les opérations visant la population, qu'elle soit ukrainienne ou occidentale, de nombreux « bots » et « trolls » ont été identifiés alors qu'ils agissaient sur plusieurs réseaux sociaux et plateformes. À titre d'exemple, une étude de réseaux menée par Alexander Laurence[14] sur Twitter présentait une analyse basée sur des réseaux de comptes utilisant des phrases clefs révélatrices d'appartenance à des communautés plus importantes. L'analyse visait les métadonnées issues de quatre comptes fusionnés et les résultats montrèrent que sur un total de 17 590 comptes Twitter, la grande majorité était des bots : 93 % ne montraient aucun emplacement sur leur profil, 96 % n'avaient pas d'information sur le fuseau horaire et 97 % n'avaient aucun favori Twitter enregistré. Outre les actions menées par Twitter, qui visaient probablement tout autant les populations occidentales qu'ukrainiennes, de vastes opérations de « trolling » furent mises au jour qui s'attaquait aux conversations en ligne ou « chats » des réseaux sociaux qu'il s'agisse de Facebook ou de Vkontakte, notamment avant que le gouvernement ne décide de bannir de son territoire plusieurs sites russes, dont ce réseau social.

On a pu remarquer qu'un « ciblage » était effectué afin d'adapter le message et de toucher au plus près les individus visés par cette vague informationnelle. À ce titre, les combattants et militaires ukrainiens ne furent pas épargnés. Outre les messages reçus sur les téléphones portables les incitant par exemple à quitter leurs postes, des opéra-

[14] Laurence Alexander » Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign" Global Voices, 2 avril 2015

tions les visant (ou visant leurs proches) sur les réseaux sociaux furent mises en place. Certaines fois, les identités de soldats décédés au combat furent utilisées pour diffuser des informations alors que leur entourage ignorait encore leur mort. D'autres fois, des messages diffusés par de prétendus combattants ou par de simples quidams comportaient des éléments visant à avoir un impact psychologique sur ces hommes. Cette diversité de sources des messages perturbateurs pouvait tout à fait permettre, outre un ratissage large, de définir quelle était la voie de communication la plus efficace sur le plan de l'impact psychologique.

Point important à prendre en compte, si certains messages étaient clairement et immédiatement décelables comme antigouvernementaux ou suivant des opérations de « sappage » de moral ou de désinformation, d'autres étaient plus subtils. Ils commençaient par défendre des valeurs communément partagées par les soldats et les combattants avant de fournir des éléments liants des personnalités du gouvernement ou de la hiérarchie militaire à des comportements ou prises de décisions contraires aux valeurs prônées précédemment et partagées par une large majorité des militaires.

À la suite d'observations réalisées sur le terrain entre 2014 et 2017, plusieurs entretiens furent menés en Ukraine avec des militaires actifs et des vétérans, particulièrement en février 2017. Les soldats rencontrés pour cette analyse n'étaient pas également ventilés en matière de genre puisque principalement masculins (une seule femme). Les sujets avaient des profils socioprofessionnels et des parcours personnels variés, peu étaient des militaires de carrière, certains avaient été blessés, d'autres non, mais tous avaient été sur la ligne de front. Ces entretiens se déroulèrent alors qu'une flambée de violence avait

lieu dans la ville d'Adiivka où la population paya un lourd tribut[15]. L'ensemble des 30 entretiens est divisé en deux sections de 15 personnes chacune, une composée de soldats actifs, l'autre de vétérans tous blessés à des degrés divers et des moments différents (allant de la prise de l'aéroport de Donetsk en 2014 aux récentes batailles menées dans l'hiver 2016-2017). Tous les vétérans étaient encore en convalescence, que ce soit pour des traumatismes physiques ou psychologiques. Les entretiens étaient menés sous forme libre, notamment pour faciliter la mise en confiance et pour ne pas bloquer la parole des personnes entendues. Cependant, des questions récurrentes étaient posées en trame de fond afin de permettre de cadrer les entretiens. La durée moyenne était d'une heure, en fonction des réactions de chacun. L'objectif était, après s'être renseigné sur le temps passé quotidiennement sur Internet, de tenter de définir si la perception du gouvernement et de la hiérarchie avait évolué à la suite des informations prises sur Internet. Dans un second temps, la perception et la confiance accordée aux différents médias et canaux d'information étaient mises en question. Ensuite, il leur était demandé s'ils pensaient pouvoir être la cible de cyberattaques informationnelles en tant que militaire, pas seulement en tant qu'Ukrainiens et finalement, s'ils estimaient que leur vision et leur confiance dans les structures institutionnelles avaient été modifiées.

L'option choisie fut de se concentrer sur les grades allant de l'homme du rang au lieutenant et de ne pas interroger des officiers, susceptibles d'être plus préparés à ce genre d'attaque. La seconde raison militant pour le choix de cet échantillon était basée sur le constat selon lequel ce sont ces hommes qui agissent quotidiennement sur le front lors

---

[15] Sébastien Gobert, « Nouvelle escalade de violence sur le front ukrainien », Liberation, &er février 2017 http://www.liberation.fr/planete/2017/02/01/nouvelle-escalade-de-violence-sur-le-front-ukrainien_1545664

« Ukraine. Avdiivka à la veille d'une catastrophe humanitaire ? », Courrier International, 1er février 2017 https://www.courrierinternational.com/revue-de-presse/ukraine-avdiivka-la-veille-dune-catastrophe-humanitaire

Olivier Talles, « Adiivka, ville symbole de la guerre en Ukraine », La Croix, 31 janvier 2017

des combats et qu'à ce titre ils sont en eux-mêmes des éléments stratégiques ne se percevant pas toujours comme tels. Ces entretiens ont démontré que la chute de la confiance dans les médias officiels est proportionnelle à la confiance accordée aux réseaux sociaux et aux médias alternatifs. L'une des raisons principalement évoquées est la suspicion de liens entre le gouvernement (dans ce cas souvent perçu comme corrompu) ou des oligarques et les médias officiels alors que les sources alternatives sont supposées venir de gens plus proches des combattants, des « Ukrainiens de la rue ». Une différence était faite avec les organes reconnus comme étant de la propagande pro séparatiste. La confiance accordée aux personnes supposées partager le mode de vie des Ukrainiens ordinaires est encore renforcée si la personne délivrant l'information, ou la partageante est un militaire (actif ou vétéran) ou un combattant. Ainsi, concernant la confiance accordée aux différentes sources d'information, celles qui sont perçues comme les plus crédibles sont en lien directes avec des « frères d'armes » ou des volontaires, en d'autres termes avec des personnes partageant les mêmes valeurs ou, du moins, des valeurs identiques à celles des soldats.

Interrogés sur l'évolution de leurs comportements, si quelques-uns restent discrets, certains adoptent ouvertement une position antigouvernementale. D'autres encore disent ne pas avoir changé s'agissant de leurs « frères d'armes », mais affirment qu'ils ne risqueraient pas leur vie pour un ordre d'un chef lointain ou pour l'un de « ces hommes », même s'ils parlent de personnes représentant leur autorité hiérarchique directe. Enfin, il en est qui avouent avoir été tenté par un glissement vers la criminalité, tout en citant certaines de leurs connaissances qui ont déjà pris ce virage répréhensible.

En matière d'interaction entre l'évolution de leur comportement et leur consommation Internet, il semble que les hommes les plus touchés, ceux reconnaissant la plus grande

évolution dans leurs comportements, sont les consommateurs déclarant être connectés à Internet 3 heures et 4 heures par jour, particulièrement ceux de la tranche des 3 h quotidiennes. Les consommations d'Internet inférieures à 2 heures par jour ne semblent guère touchées, ce qui paraît logique, ces hommes déclarant utiliser Internet principalement pour consulter leurs mails ou communiquer avec leurs familles (notamment en utilisant Skype) et non pour « s'informer ». De même, les consommations supérieures ne semblent pas être plus affectées que le pic constaté parmi ceux déclarant une connexion journalière de 3 heures. Cependant, ce constat mérite d'être affiné, notamment en ce qui concerne les conditions de la consommation (privée, publique, etc.…).

Concernant la tranche d'âge, les membres de la « génération Y »[16] sont les plus sensibles et il semble que les grades de sergent et caporal soient plus touchés que les lieutenants.

Enfin, de tous les soldats interrogés, aucun ne se percevait comme pouvant être une cible en tant que militaire. Plusieurs raisons étaient évoquées de manière récurrente : tout d'abord, ils ne pensaient pas avoir un intérêt stratégique assez important pour pouvoir constituer des cibles ensuite, ils ne croyaient pas pouvoir être dupés, car « ils connaissent trop bien les séparatistes et leurs mensonges ». Ce point est particulièrement intéressant quand on le met en relation avec leur baisse de confiance dans les médias officiels qui, unanimement reconnue, laisse entendre qu'ils ont bien été impactés. Enfin, interrogée sur le point de savoir s'ils avaient changé de point de vue quant aux structures étatiques en s'informant, la réponse a été unanimement positive chez les caporaux et sergents consommateurs de 3 à 4 heures d'Internet par jour. Ceux-ci étaient pourtant

[16] Génération X: personnes nées entre 1966-1976 - Génération Y, baby-boomers ou millénaires: personnes nées entre 1977 et 1994 - Génération Z: personnes nées entre 1995 et 2012

convaincus de ne pas être dupes de stratégies informationnelles et ne pas en être des cibles.

1. 2. Potentialités du cyber

Le cyber est aujourd'hui un acteur incontournable dans les conflits modernes pour plusieurs raisons. Tout d'abord, en raison de l'interconnexion du réseau, il permet d'abolir les frontières physiques et géographiques connues jusqu'alors, et cette disparition de l'éloignement géographique a une conséquence matérielle immédiate : la diminution du coût d'actions menées loin du territoire donneur d'ordre. La plasticité du cyber, sa volatilité, permettent une adaptation extrêmement rapide aux contextes locaux et à leurs évolutions et, corrélativement, la modification sans délai de la perception d'un élément. Cette contraction temporelle reste cependant liée à la capacité de calcul disponible : l'analyse et le traitement efficace d'un volume important de données nécessitent la mobilisation d'une grande puissance de calcul. Cette contrainte peut aller jusqu'à nécessiter l'utilisation de super calculateurs, notamment pour obtenir des analyses en temps réel. Ces deux facteurs permettent d'atteindre un individu où qu'il se trouve, en temps réel, tous les jours de la semaine et à toute heure du jour et de la nuit. En outre, la multivectorialité du cyber est un avantage tactique énorme : si une source d'influence vient à être découverte, il est facile de la fermer et d'en ouvrir une autre, voire plusieurs autres, de façon simultanée. Cette possibilité de multiplication des sources participe à rendre les opérations psychologiques, menées sur Internet particulièrement difficiles à détecter : bien organisées et pensées par une même tête, elles peuvent utiliser différents axes qui ne font sens qu'une fois appréhendés dans leur globalité. Or cette vision globale, cette « big picture », peut devenir quasi impossible à atteindre lorsque les canaux d'influences

sont noyés dans le bruit du réseau, au cas particulier dans la masse des données et des sites consultés par la personne visée.

Autre point d'intérêt, Internet est une source d'information qui autorise la définition d'un profil pour une entité mal intentionnée. Avec l'analyse des données consultées, des sites visités et la mise en œuvre des méthodes d'ingénierie sociale, il est possible de glaner des informations permettant de définir le profil de la personne observée. Dans le cas ukrainien, les données des citoyens qui utilisent Yandex, Vkontakte et Mail.ru partent directement sur des serveurs moscovites. Cela constitue un problème majeur pour le gouvernement, car ces données représentent une source d'information très importante pour les renseignements russes sans même qu'il y ait la nécessité développer des stratégies de hacking. Enfin, le cyber a un avantage indéniable pour les opérations psychologiques, tout particulièrement quand elles sont menées par une structure tierce : il rend la traçabilité vers l'origine de l'attaque extrêmement délicate. Dans le cas ukrainien, si nombre de soupçons pointent vers le Kremlin, il reste cependant très difficile de réunir des éléments de preuves indiscutables en nombre suffisant pour permettre une mise en cause pénale de ce gouvernement. L'utilisation de groupes de hackers aura été un des éléments qui ont participé de cette complexité. En effet, si des groupes comme les CyberBerkuts, CozyBear, FancyBears ou encore Sandworm sont suspectés d'être liés à diverses agences gouvernementales russes, le lien indiscutable est délicat à établir. Ces groupes se présentent eux-mêmes comme totalement indépendants et déconnectés du Kremlin. Ce dernier fait écho à ces déclarations en annonçant ne pas avoir de prise sur les hackers, alors même que la puissance et l'importance de la guerre informationnelle ont été clairement formalisées au sein du ministère de la Défense russe depuis 2000. Enfin, si l'identité de certains hackers engagés par le FSB et le GRU est connue,

l'anonymat utilisé lors des opérations menées en Ukraine ne permet ni d'impliquer clairement ces individus ni de faire le lien avec le gouvernement. Quand bien même une connexion avec le gouvernement serait mise en évidence, encore faudrait-il prouver qu'ils n'ont pas agi de leur propre chef, sans ordre du gouvernement, de la même manière que les soldats russes capturés en Ukraine ont été déclarés comme ayant agi de leur propre initiative, pendant leurs congés, et non sur ordre gouvernemental.

Une fois que l'on a pris conscience de ce nuage de fumée permis par le cyber, il devient alors évident que ce type d'opérations peut être mené à loisir, notamment en temps de paix en prévision d'un conflit à venir, car le risque d'être démasqué et condamné reste minime.

1. 3. Le cyber, facteur d'influence sur la confiance ?

Dans l'analyse faite suite aux entretiens menés en Ukraine en 2017, il apparaît clairement qu'une des conséquences de l'influence informationnelle aura été l'érosion de la confiance portée par les soldats à diverses structures institutionnelles. Afin d'aborder cette analyse avec une vision plus globale il semble pertinent d'observer plus particulièrement l'influence du cyber sur la confiance portée aux informations de manière générale. Cette approche permettra de définir si cette inflexion était uniquement contextuelle ou si elle était plus générale et, par conséquent, si le cyber peut être utilisé de façon plus vaste pour servir une stratégie globale. Des observations de 2017, il ressort que les militaires interrogés accordaient majoritairement leur confiance aux informations — ou éléments d'information — données par d'autres militaires, par des personnes connues, ou par des personnes partageant leurs valeurs. Aussi, une recherche a été menée sur l'influence que peut avoir la personne diffusant, ou partageant une information sur l'indivi-

du la recevant. Diverses études ont été menées sur ce sujet, principalement aux États-Unis. Cependant, si le terrain de ces travaux n'était ni l'Ukraine ni la France les taux de pénétration d'Internet, assez proche entre l'Europe et les États-Unis, fournissent un premier socle solide à l'analyse. En effet, le taux de pénétration d'Internet est de 88 % en Europe de l'ouest et de 84 % aux États-Unis. En matière de pénétration des médias sociaux, les États-Unis affichent un ratio de 66 % contre 56 % dans l'Europe de l'Ouest en 2017.

Ces chiffres montrent que nous sommes nombreux à pouvoir être influencés par Internet. L'accroissement de la consommation de données mobiles ne fait qu'augmenter la possibilité d'atteindre n'importe qui à n'importe quel moment. Or, sur les 2,8 milliards d'utilisateurs de médias sociaux, plus de 91 % sont connectés grâce à des appareils mobiles. Parler d'une connexion tout au long de la journée n'est donc pas excessif : dans leur étude, Deloitte[17] montre que 16 % des Français consultent leurs smartphones dans les 5 minutes après le réveil (jusqu'à 35 % chez les 18-24 ans), et 42 % dans les 30 premières minutes, 59 % dans l'heure. 50 % d'entre eux dorment avec leurs smartphones à proximité et, parmi ceux qui sont réveillés par un message, 92 % assurent le consulter « toujours (ou presque), souvent ou parfois » et 79 % disent « répondre aux messages dès leur réception ». Ce n'est pas un phénomène local, au Royaume-Uni, une enquête menée par Omnibus Institut[18] montre que les 18-34 ans regardent leurs smartphones jusqu'à 100 fois par jour, soit toutes les 9 minutes 50 secondes. Les chiffres sont assez similaires pour les 25-34 ans avec un coup d'œil toutes les 9,55 minutes.

---

[17] Cabinet Deloitte « Usages Mobiles 2015: A Game of Phones » annual report, January 2016

[18] Omnibus Institut survey for Kana Software

Selon l'âge, le mode d'accès à l'information peut varier, mais il y a une tendance claire : de plus en plus de personnes utilisent Internet pour obtenir des informations. Avec une analyse fine, on remarque une augmentation de l'accès à l'information à travers les réseaux sociaux. Selon une étude de Harris Interactive, 58 % de la génération « Z » et 33 % de la génération Y utilisent les médias sociaux pour accéder à l'information, ces chiffres passent à 30 % et 41 % quand on parle d'accès à l'information via Internet au sens plus large. Au niveau européen en 2016, plus de 70 % des membres de la « génération Y » ont utilisé Internet pour lire des sites d'information en ligne et accéder à l'information, la « génération Z » est légèrement inférieure à ce chiffre. Ces deux tranches d'âge sont des utilisatrices de réseaux sociaux avec respectivement 65 % et 88 %.

Fort de ces chiffres en tête, il apparaît qu'une analyse de la confiance dans les informations reçues sur le web est pertinente pour déterminer si le cyber peut être utilisé pour influencer la confiance des personnes potentiellement ciblées par un adversaire.

Selon l'enquête de l'American Press Institute et de l'Associated Press-NORC Center for Public Affairs Research, la personne partageant une information à un effet majeur sur la confiance accordée au contenu diffusé. Ils remarquent que 51 % des personnes disent qu'un article publié est de qualité quand il est partagé par une personne de confiance. Seulement 34 % ressentent la même chose quand le même article est partagé par quelqu'un en qui ils n'ont pas confiance ou par un inconnu. Les chiffres sont les mêmes concernant la perception de la véracité des faits. Il semble que l'identité de celui qui partage influence également la perception relative à la représentativité des divers points de vue relatifs au sujet : 31 % des personnes sondées pensent que l'article présentait bien la pluralité des points de vue quand le document était fourni par une personne connue, seulement 22 % avaient ce sentiment lorsque le même document n'était pas

transmis par un « ami ». Enfin, si la même information est transmise par une personne de confiance et provenant d'une source connue, 52 % des internautes pensent que l'article a bien appréhendé les faits. Le même article non transmis par une personne de confiance, mais affichant la même source ne récoltait que 32 % de personnes estimant que les faits étaient correctement retranscrits. De même, 49 % des sondés pensent que l'histoire est vraie s'ils font confiance à celui qui l'a transmise, même si l'article est attribué à une source d'information fictive. Le même article transmis par un inconnu voit le chiffre tomber à 32 %. En ce qui concerne Facebook, 48 % des personnes interrogées disent que leur confiance dans la personne à l'origine de la publication influe sur le crédit qu'elles lui accordent. Dès lors, il apparaît clairement que l'identité de celui qui partage le message, le « post » ou l'information est plus importante que sa source originale. Considérant que la formation particulière des militaires développe « l'esprit de corps », il est possible que si la personne qui partage un contenu est supposée être un soldat, cela augmente d'autant la confiance accordée au contenu partagé.

2. Le rôle de la confiance dans le fonctionnement des équipes militaires

Selon Nicholas Negroponte, nous vivons dans un monde devenu numérique et les militaires ne font pas exception à ce constat. Non seulement ils sont aussi connectés que leurs concitoyens, mais de plus la « génération Y », qui est l'une des plus connectées, est fortement représentée parmi les grades allant de l'homme du rang au lieutenant. Ainsi, il ressort des différents travaux compilés qu'une large part de leur population appartient à la tranche d'âge la plus susceptible d'être exposée au cyber et à une altération de leur conscience. Si l'on part du postulat que la confiance peut être affectée par des opéra-

tions de « cyberwarfare », il devient alors nécessaire d'analyser l'importance et le rôle de la confiance dans le fonctionnement des équipes militaires.

Si nous traitons du fonctionnement militaire, il faut également évoquer le contexte dans lequel ils évoluent. Dans le cadre de leurs missions, les soldats interviennent dans des situations extrêmes au sens qui leur est donné par Lièvre (2005) pour qui une situation est extrême quand elle est évolutive, incertaine et risquée. Cet attendu est partagé par d'autres auteurs, parmi lesquels Rivolier (1998), qui affine la notion « d'évolutive ». Il explique qu'évolutive se réfère à une situation en rupture avec la vie quotidienne : la situation extrême présenterait un écart entre le quotidien — la situation « A » — et la situation « B » qualifiable d'extrême, qu'elle soit présente ou inscrite dans un futur proche. L'incertitude est ici entendue comme étant radicale et totale (Knight, 1923) c'est-à-dire qu'il sera difficile, voire impossible, de mesurer la probabilité qu'un évènement quelconque — mais le plus souvent à risque — apparaisse. En définitive, c'est une situation ou l'inattendu peut se faire jour à tout instant (Orlean, 1986).

Jean-Louis Moigne (1990) parlera d'un moment où l'impossible devient possible, voire probable. Quant au risque, il peut comporter plusieurs niveaux d'intensité, en matière de dommages subis, mais il n'exclut ni le risque de blessures ni le risque létal. Là encore, comme pour l'incertitude, l'échelle de risque n'est pas toujours précisément mesurable par les personnes qui y sont confrontées. En nous basant sur les trois critères, il apparaît clairement que les missions militaires totalisent toutes les caractéristiques permettant de les définir des situations de crises. Or, les soldats interviennent régulièrement dans de tels contextes qui ne devraient être qu'exceptionnels. En outre, en accord avec leurs spécificités intrinsèques, les situations extrêmes auront tendance à exacerber les comportements des intervenants, en faisant par là même des sujets d'observation privilégiés.

Dans le cas des militaires, les commandements ont parfaitement conscience que vivre et intervenir de façon récurrente dans de telles situations nécessite un conditionnement fort afin de contenir les risques et de tenter de faire diminuer l'incertitude. Si ce conditionnement, cet entraînement, s'avère efficace sur le terrain, il est plus que probable que les soldats se l'approprieront au point que ces éléments cognitifs, devenus affectifs et partie intégrante de leur personnalité, conditionneront indiscutablement le fonctionnement de leur système de pensée.

Il apparaît donc que l'incertitude est une pierre angulaire de la situation extrême ce qui amène logiquement à analyser le poids de la confiance dans le fonctionnement des équipes militaires ainsi que son traitement dans la littérature.

La confiance aurait un fondement à la fois cognitif et affectif (McAllister, 1995), et serait un facteur fort de cohésion à l'intérieur des groupes armés. Selon des études méta analytiques, il y a une relation positive entre la cohésion et la performance (Mullen & Cooper, 1994), l'un nourrissant l'autre, et chacun ne pouvant exister individuellement. Rapportée aux champs militaires, la performance pourrait être définie comme l'atteinte du but fixé par le commandement en subissant le moins de dégâts matériels et de perte humaine possible, nous parlerons donc d'efficacité des modes opérationnels. Ainsi, la confiance serait en relation directe avec la cohésion et l'efficacité des modes opérationnels. Dans d'autres travaux, la cohésion militaire est définie selon trois composantes principales : les relations avec les pairs, les relations entre supérieurs et subordonnés et la relation avec les forces armées et le gouvernement (Stewart, 1988, et Etzioni, 1961). Par conséquent, dégrader la perception du gouvernement dans l'esprit des soldats pourrait altérer la confiance et la cohésion. De même, une méfiance croissante envers les supérieurs détériorera la cohésion et par construction l'efficacité des modes opérationnels

de l'équipe, ce qui augmentera le facteur de risque pour le succès de la mission. Dans le cas présent, on préférera parler de modes opérationnels plutôt que de performance qui apparaît être un terme trop générique. Si la confiance est citée comme un facteur majeur pouvant permettre ou compromettre la réussite d'une opération elle apparaît comme un concept nécessitant un éclaircissement. Selon Bhattacharya & al (1998), la confiance serait la somme des résultats positifs de l'espérance basée sur les actions attendues d'une autre partie dans une interaction basée sur l'incertitude. Une autre définition parle d'un état psychologique comprenant l'intention d'accepter la vulnérabilité sur la base d'attentes positives quant aux intentions ou au comportement d'un autre (Rousseau et al, 1998). Une dernière définition est celle de Mayer, Davis et Schoorman (1995) pour qui de la confiance est « une volonté d'être vulnérable envers un autre parti lorsque ce parti ne peut être contrôlé ou surveillé ». La « loyauté » est également identifiée comme un mot-clé lorsqu'il s'agit de confiance (Adams, 2003). À la lumière de ces définitions, et parce que les équipes militaires interviennent couramment dans des situations extrêmes, des notions comme l'acceptation de la vulnérabilité prennent un tour très réaliste, les soldats pouvant être blessés ou même tués lors des opérations. La définition précédente de la confiance décrit l'incertitude comme un « game changer » et, par effet miroir, la confiance comme une pierre angulaire du quotidien des soldats. Ainsi, altérer la confiance des soldats dans l'une des trois strates décrites par Stewart et Etzioni pourrait avoir des conséquences immédiates pouvant aller jusqu'à l'échec de la mission avec son corollaire de dommages subis par l'équipe intervenante. Au-delà de leur propre mission, avec un échec, c'est la crédibilité et la fiabilité du gouvernement donneur d'ordre qui peuvent être touchées que ce soit dans la relation entretenue avec les citoyens (par exemple, si les soldats sont blessés ou tués) ou dans les relations interalliés. Par consé-

quent, l'érosion de la confiance des soldats peut avoir un effet énorme non seulement sur le terrain, mais aussi sur la politique et la stabilité du gouvernement. Or, influencer la stabilité d'un État, infléchir ses prises de décisions sans que cela soit manifeste ou détectable, correspond en tous points aux objectifs affichés de la théorie du chaos dirigé, chère à un certain nombre de puissances.

3. Potentiels opérationnels - l'utilisation de la dissonance cognitive

En croisant les potentiels liés à l'altération de la confiance des soldats avec les observations de terrains, il apparaît que nous sommes confrontés à une technique de manipulation psychologique destinée à modifier le comportement connu depuis les années 50 : la dissonance cognitive. Cette théorie a été réutilisée et repensée à l'aune des moyens modernes capables d'en décupler l'efficacité. En effet, selon la théorie, une cognition forte est confrontée à une autre cognition, générant ainsi un inconfort psychologique. Pour retrouver l'état de quiétude précédent, le sujet soumis à cette opposition entre des cognitions opposées, dites « inconsistantes » (Festinger, 1956), aura tendance à agir, à poser une action pour affirmer son choix premier et se dégager de la situation inconfortable induite par la confrontation. C'est ce que l'on appelle des stratégies de réduction de la dissonance cognitive. Selon la théorie, plus grande est l'amplitude entre les cognitions inconsistantes, plus forte sera la pression pour mettre en place des stratégies de réduction. Cette dernière pourra prendre des formes variées : la modification des éléments prenants part dans l'inconsistance, l'ajout d'éléments consistants permettant d'invalider une des deux cognitions générant la dissonance et l'inconfort, ou encore la diminution de l'importance des éléments inconsistants avec la cognition la plus résistante. Ce sont là les fondements de la théorie de la dissonance cognitive développée initialement par

Léon Festinger (1956). Selon ce sociologue, la dissonance cognitive est un état d'inconfort psychologique motivationnel ressenti par un individu dès lors que deux cognitions, dites « inconsistantes », opposées, s'affrontent. Afin de diminuer le ressenti dû à la dissonance, le sujet victime mettra en place des stratégies de réduction permettant de revenir à un état psychologique de confort. Cet enchaînement modifiera donc le comportement de la cible, faisant de l'état de dissonance cognitive un phénomène orienté vers l'action (Harmon-Jones, 2002-2003).

En revenant sur les observations de terrain, si les soldats ukrainiens n'ont jamais cessé de croire en la cause qu'ils défendaient (se battre pour l'Ukraine), leurs doutes envers le gouvernement ont augmenté progressivement et, pour certains d'entre eux, se sont cristallisés sur la personne du président. Leur perception d'eux-mêmes était fortement liée à leur identité de soldats (cela même s'ils n'étaient pas des militaires de carrière et exerçaient d'autres professions avant le déclenchement du conflit). Cette identité, ces valeurs étaient étroitement liées à la lutte patriotique pour leur pays. De plus, ils utilisaient pour se décrire des termes faisant référence à des valeurs souvent associées au monde militaire, donnant à penser qu'ils adoptaient ces éléments cognitifs (appris par la formation, le conditionnement dû à la nature même de leur métier), se les appropriaient comme faisant partie d'eux-mêmes, de leur affect et de leur personnalité intime. Le glissement vers l'émotionnel de ces éléments, initialement cognitifs, se renforce par le test in situ de leur bien-fondé, à savoir l'expérience empirique : leur formation les aidant à sauver leur vie, elle a été testée avec succès et est devenue intégralement indiscutable. Cela peut être un facteur qui explique que la plupart d'entre eux ne peuvent accepter que quiconque utilisant la force pour servir les valeurs morales auxquelles ils adhèrent — par exemple la protection de la famille — ait maille à partir avec les tribunaux au cas

où leur action, considérée comme légitime, voire digne d'éloges, par les soldats, provoquerait des dommages physiques pour l'agresseur. La réaction provoquée par cet exemple, qui peut être radicale et aller jusqu'au rejet du jugement rendu et de ceux qui l'ont prononcé, fonctionnerait sur le modèle d'une action réflexe, émotionnelle, étrangère au filtre de la pensée : c'est une réaction sans réflexion. En s'appuyant à nouveau sur les méthodes décrites dans les théories de la dissonance cognitive, ces éléments pourraient tout à fait être utilisés à des fins de déstabilisation d'une organisation. Cette opération pourrait intervenir de façon assez discrète, avant le déploiement des militaires, et ne prendre tout son sens qu'une fois les hommes arrivés au plus fort de la situation extrême, par exemple sur un théâtre d'opérations.

Cette hypothèse de stratégie d'influence et le mode de fonctionnement observé chez les militaires incitent à explorer la variante fonctionnelle de la théorie de la dissonance cognitive présentée dans les travaux d'Elliott Aronson (1968, 1992). Cet auteur a explicité le concept de l'« autoconsistance » selon lequel la dissonance résulte de la contradiction entre le comportement ou l'action des individus et leur perception d'eux-mêmes. C'est donc le soi qui sera à l'origine de la dissonance quand il est confronté à une idée ou à un comportement inconsistant (Girandola 2000, 2001). Selon cette théorie, plus la perception de soi est positive, plus le sujet ressentira l'effet de la dissonance cognitive (Thibodeau et Aronson, 1992). De même, les individus dont la mortalité est saillante sont plus sensibles à la dissonance cognitive (Jonas, Greenberg et Frey, 2003). Or, les soldats sont formés sur la base de valeurs unanimement perçues comme hautement positives, telles que le sacrifice pour le bien commun, le service de la Nation, concepts généralement liés à la mythologie du héros. De plus, ils mettent régulièrement leur vie en danger faisant de leur propre mort un compagnon de route. En conséquence, ils ont les

profils parfaits pour être particulièrement sensibles à la dissonance cognitive. Remarquons que la dissonance peut survenir même si le comportement engagé n'est pas immoral ou n'a pas de conséquence irréversible (Harmon-Jones, Brehm, Greenberger, Simon et Nelson, 1996), mais qu'elle sera d'autant plus ressentie si les conséquences sont irrévocables. Une autre évolution de la théorie initiale de Festinger est le modèle intégratif de Stone et Cooper (1999), le Self Standard Model (SSM). Dans cette proposition, les éléments cognitifs qui pouvant être touchés par la dissonance cognitive peuvent relever de normes personnelles (on parlera d'excitation idéographique) ou de standards normatifs (l'excitation nomothétique). Dans le cas des soldats, les standards normatifs se transforment parfois en normes personnelles comme vues ci-dessus. Sur ces bases, les militaires apparaissent à nouveau comme étant théoriquement particulièrement sensibles à la dissonance cognitive, et donc à une attaque cognitive utilisant leurs propres standards pour susciter la dissonance — soit l'inconfort motivationnel — afin de les faire changer de comportement. Cette attaque psychologique sera probablement très réussie si elle diminue la confiance dans les esprits, puisque la confiance est, comme vus plus haut, une des pierres angulaires du bon fonctionnement des opérations militaires. Dans le contexte actuel, le cyber offre la possibilité, grâce à ses caractéristiques propres, de soumettre les hommes à des éléments inconsistants à même de déclencher de la dissonance avec un rythme jamais atteint ni même envisagé jusqu'alors. Toujours dans le cas des soldats ukrainiens, il serait simpliste de penser que les personnes visées n'ont été victimes que d'envois de cognitions inconsistantes sans « préparation» préalable. Dans certains cas, ils ont été en contact avec des groupes ou des personnes virtuelles partageant leurs points de vue, le faisant savoir et ayant même tendance à réaffirmer les valeurs communément partagées par le corps militaire, renforçant d'autant les

cognitions auxquelles les cibles adhéreraient déjà. Ensuite seulement venait une « information » inconsistante, le plus souvent reliée à une personnalité ou à une institution. En rejetant l'élément inconsistant, moins solide et résistant que les valeurs du soi comme décrites dans la théorie de l'autoconsistance, les « victimes » se retrouvaient dans une situation délicate vis-à-vis de la structure mise en cause. S'ils ne pouvaient pas totalement la rejeter (dans le cas du gouvernement ou de leur commandement par exemple), la confiance placée dans ces mêmes structures se trouvait fortement endommagée. En fin de compte, pour pouvoir garder indemne la cognition relative à leur soi, ils auront tendance à affaiblir systématiquement ce qui se rapporte à l'information inconsistante ou à ses corollaires, y compris la structure mise en cause, cela pouvant se traduire par une méfiance voire une perte de confiance systématique. La mise en œuvre de la dissonance cognitive, reposant notamment sur la masse d'informations à laquelle la cible peut être soumise, a été rendue possible par la plasticité et l'adaptabilité du cyber. Dans les faits, pour peu que le stratège utilisant cette méthode ait une connaissance assez fine du conditionnement reçu et donc des éléments déclencheurs de l'inconfort psychologique, il pourra soumettre les cibles choisies à un feu roulant d'attaque cognitive.

Conclusion : risques opérationnels et sanitaires pour les armées occidentales

En partant du principe que l'Ukraine aura servi de laboratoire expérimental pour de nombreuses méthodes d'attaques cyber, incluant les opérations psychologiques, il convient de se demander quelles seront les utilisations faites des données collectées. En

toute logique, les méthodes utilisées seront analysées et participeront à une amélioration des processus dans la perspective d'utilisations ultérieures envers d'autres structures, parmi lesquelles des entités occidentales pourraient être ciblées. En se basant sur les éléments ci-dessus développés, il apparaît que plus une cible sera conditionnée, plus elle sera théoriquement « piégeable » par des méthodes de dissonance cognitive. L'armée ukrainienne a dû se recomposer à partir de 2014, soit avec l'explosion du conflit, notamment en faisant appel à la conscription, et, malgré ce conditionnement relatif, la dissonance cognitive utilisée via le cyber a connu des résultats « positifs ». Dans le cas des armées occidentales, l'organisation est très huilée et ne recourt pas à la conscription, mais à une armée de métier, professionnalisée. La force de cette organisation repose notamment sur ce professionnalisme, sur des compétences acquises au fil de l'entraînement et donc du conditionnement. Or, dans la théorie évoquée dans cet article, plus une personne sera conditionnée et entraînée, plus elle sera prévisible en ce qui concerne les réactions possibles face à des éléments cognitifs inconsistants. En d'autres termes, ce qui est un des éléments fondamentaux de la force des armées occidentales pourrait devenir une faiblesse au regard des attaques psychologiques véhiculées par Internet et informationnelles. En outre, ces opérations seront difficilement détectables par l'encadrement, notamment parce qu'elles peuvent mobiliser simultanément plusieurs canaux (réseaux sociaux, articles de blogs, « cyber bait », discussions de groupes, plateforme de broadcast type YouTube, native advertising, médias d'information alternatifs, etc.), que la consommation de données intervient sans que le commandement le voie et que la cible ne se sentira pas attaquée, car, dans la plupart des cas, l'attaque utilisera les valeurs prônées dans la formation reçue. Enfin, il n'est pas nécessaire que la cible de cognitions inconsistantes soit acteur de la mise en contact pour qu'il y ait éveil de la disso-

nance, une exposition accidentelle pourra être tout aussi efficace (Vaidis & Gosling, 2011). Notons qu'une attaque englobant des membres de la famille de la cible n'est pas non plus inenvisageable.

Dans l'hypothèse où ces méthodes seraient utilisées dans le cadre d'une stratégie globale, il serait tout à fait possible qu'en profitant de la complexité à remonter jusqu'à l'origine de l'attaque, des opérations soient menées en temps de paix dans la perspective d'un éventuel conflit ultérieur, voire d'un conflit planifié. Dans ce cas, les hommes pourraient être attaqués « en avance de phase », et ne pas jouir de 100 % de leurs capacités au moment du déploiement sur le terrain. En effet, en accroissant le doute envers des structures institutionnelles ou dans une partie de la chaîne de commandement, le soldat impacté pourrait modifier son comportement qui ne sera alors plus en adéquation avec celui attendu par le commandement. Que cette modification soit une hyperréaction (action hors du cadre défini par les ordres) ou une hyporéaction (manque de réactivité, temps de latence, ou mise en retrait), elle sera également dangereuse quant au bon déroulement de la mission confiée : on parlera alors de « désengagement » au sens où l'action ne correspond pas à celle comprise dans l'engagement des soldats. Si les personnels visés font partie d'équipes spécialisées avec des savoir-faire longs à acquérir, ils seront d'autant plus difficiles à remplacer. Enfin, les armées occidentales ayant restreint leurs effectifs, les hommes tendent à intervenir en équipes plus réduites que par le passé. Or si, 3 hommes sont touchés dans une équipe de 6 personnes, c'est en réalité 50 % de la capacité opérationnelle du groupe qui sera atteinte, ce qui représente un risque fort quant au résultat de la mission confiée.

Enfin, si les hommes ciblés par une attaque cyber utilisant la dissonance cognitive résistent à l'inconfort psychologique engendré par l'affrontement de cognitions et ne mo-

difient pas leur comportement, il n'est pas certain que la stratégie à l'origine de l'attaque soit un échec. En effet, plusieurs études ont mis en avant l'effet produit par la dissonance au niveau neuronal. Or la stimulation perpétuelle des zones activées lors de l'éveil de la dissonance comme le cortex antérieur cingulaire (Van Veen, Krug, Schooler, Carter, 2009), le cortex frontal (Colosio, Shestakova, Nikulin, Blagovechtchenski and Klucharev, 2017), plus particulièrement le cortex frontal médial connu pour jouer un rôle important dans la prévention des résultats aversifs qui est un instinct de survie intégré (Buckley, 2017) ne pourrait-elle pas avoir des conséquences sanitaires ? Si tel devait être le cas alors, outre la problématique opérationnelle, l'utilisation de la dissonance cognitive pourrait devenir un problème de ressources humaines au regard de la santé des personnels. Enfin, outre les conséquences induites par l'hyperstimulation de zones cérébrales, la persistance d'un inconfort psychologique pourrait mener à des conduites addictives tendant à faire décroître l'inconfort. Dans tous les cas, sur le long terme la personne ciblée sera fragilisée et potentiellement instable alors que la mission exige une efficience optimale et une stabilité sans faille.

En conclusion, ces diverses observations on fait émerger la question générale de recherche évoquée en introduction et une base conceptuelle pour pouvoir y répondre. Cela a justifié sa déclinaison en plusieurs dimensions qui ont conduit à se lancer dans un véritable travail de recherche plus large. Ce travail était destiné à vérifier les effets de la dissonance cognitive sur les personnes conditionnées, mais également à tenter de cerner les facteurs cognitifs propres à susciter de la dissonance cognitive afin d'atteindre la confiance, de développer l'incertitude et par construction, d'engendrer le désengagement.

Dès lors, cet article présente une étude préalable qui a fait émerger des problématiques et a conduit à l'engagement d'un travail de recherche allant au-delà de ce que la démarche exploratoire pouvait proposer. En effet, il apparaît clairement que dans un contexte de situation extrême la dissonance observée est un facteur de risque que les organisations concernées doivent intégrer dans leur approche de la situation et dans les stratégies appelées à se dérouler dans ce type de contexte. Une des premières questions était alors l'exploitation de ce type de risque par des organisations concurrentes. Dans le cas des armées, il apparaît pertinent d'analyser la prise en compte de ces attaques dans la stratégie militaire récemment élaborée. Ce questionnement a conduit à interroger la place et le rôle donné a ce nouveau risque émergeant.

Références

Adams Barbara;, and Robert D.G. Webb. 2003. “Trust Developpement in Small Teams.” Recherche et développement pour la défense du Canada -Toronto. RDDC, N° CR 2003-016, 22

American Press Institute. 2017. “What Makes People Trust and Rely on News?” Survey Research. https://www.americanpressinstitute.org/publications/reports/survey-research/trust-news/.

Bhattacharya, Rajeev, Timothy M. Devinney, and Madan M. Pillutla. 1998. “A Formal Model of Trust Based on Outcomes.” *The Academy of Management Review ,*23 (3): 459. https://doi.org/10.2307/259289.

Buckley, Thea. 2015. “What Happens to the Brain When We Experience Cognitive Dissonance?” *Scientific American Mind ,* 26 (6): 72–72. https://doi.org/10.1038/scientificamericanmind1115-72b.

Cabinet Deloitte. 2015. “Usages Mobiles Les Français et Le Smartphone En 2016 : Une Relation Fusionnelle.”

Colosio, Marco, Anna Shestakova, Vadim V. Nikulin, Evgeny Blagovechtchenski, and Vasily Klucharev. 2017. “Neural Mechanisms of Cognitive Dissonance (Revised): An EEG Study.” *Journal of Neuroscience,* 37 (20): 5074—83. https://doi.org/10.1523/JNEUROSCI.3209-16.2017.

Courier International. 2017. “Ukraine. Avdiivka à La Veille d’une Catastrophe Humanitaire ?” *Courrier International*, February 1st, 2017.

Eurostat. 2016. “Internet Activities in the Past Three Months by Age Group EU-28, 2016 (% of Internet Users).”

Etzioni, Amitai. 1961. *A Comparative Analysis of Complex Organizations On Power, Involvement, and Their Correlates*. The Free P. New York.

Festinger, Léon. 1957. *Cognitive Dissonance*. Stanford University Press. Stanford u. Stanford. https://doi.org/10.7312/columbia/9780231175081.003.0017.

Girandola, Fabien. 2000. “Le Soi et La Théorie de La Dissonance Cognitive.” *Revue Internationale de Psychologie Sociale,* 13 (2): 115–47.

Gobert, Sebastien. 2017. “Nouvelle Escalade de Violence Sur Le Front Ukrainien.” *Liberation,* February 1st, 2017.

Harmon-Jones, Eddie, Brehm, Jack W.; Greenberg, Jeff ;Simon, Linda and Nelson David E.. 1996. “Evidence That the Production of Aversive Consequences Is Not Necessary to Create Cognitive Dissonance.” *Journal of Personality and Social Psychology,* 70 (1): 5–16. https://doi.org/10.1037/0022-3514.70.1.5.

Harmon-Jones, Eddie, Jack W. Brehm, Jeff Greenberg, Linda Simon, and David E. Nelson. 1996. “Evidence That the Production of Aversive Consequences Is Not Necessary to Create Cognitive Dissonance.” *Journal of Personality and Social Psychology,* 70 (1): 5–16. https://doi.org/10.1037/0022-3514.70.1.5.

Jonas, Eva, Greenberg, Jeff and Frey, Dieter. 2003. “Connecting Terror Management and Dissonance Theory: Evidence That Mortality Salience Increases the Preference for Supporting Information after Decisions.” *Personality and Social Psychology Bulletin,* 29 (9): 1181–89. https://doi.org/10.1177/0146167203254599.

Knight, Franck. (1923). *Risk, Uncertainty and Profit.* Lanham, National Book Network, 1923, 448.

Lièvre, Pascal, and Rix-Lièvre Géraldine. 2004. “Le Management Des Expéditions Polaires.” *Management & Avenir,* 24 (9): 1–12.

Le Moigne, Jean-Louis. 1990. *La modélisation des systèmes complexes.* Paris, Dunod.

Mayer, Roger. C., Davis, James. H. and Schoorman, David F.. 1995. “An Integrative Model of Organizational Trust.” *Academy of Management Review,* 20 (3): 709–34. https://doi.org/10.5465/amr.1995.9508080335.

Minchenko, Olga. 2013. Вже 3 мільйони українців користуються Facebook. *Watcher*. Watcher.com.ua. 2013-10-25. Retrieved 2014-08-03.

Mullen, Brian, and Carolyn Copper. 1994. “The Relation between Group Cohesiveness and Performance: An Integration.” *Psychological Bulletin,* 115 (2): 210–27. https://doi.org/10.1037/0033-2909.115.2.210.

Orléan, André. 1986. Hétérodoxie et incertitude. Épistémologie et Autonomie, *Les cahiers du CREA*, n° 5, École Polytechnique, Paris.

Rivolier, Jean. 1998. Stress et situation extrême, *Bulletins de la psychologie*, 51, 6

Rousseau, Denise M., Sitkin, Sim B.; Burt, Ronald S. and Camerer, Colin. 1998. “Not so Different after All: A Cross-Discipline View of Trust.” *Academy of Management Review*.23, 3, 393-404. https://doi.org/10.5465/AMR.1998.926617.

Kinzer Stewart, Nora. 1988. *South Atlantic Conflict of 1982: A Case Study in Military Cohesion.* Research Institute for the Behavioral and Social Sciences: Alexandria.

Stone, Jeff, and Joel Cooper. 2001. "A Self-Standards Model of Cognitive Dissonance." *Journal of Experimental Social Psychology,* 37 (3): 228–43. https://doi.org/10.1006/jesp.2000.1446.

Thibodeau, Ruth, and Aronson, Elliot. 1992. "Taking a Closer Look: Reasserting the Role of the Self-Concept in Dissonance Theory." *Personality and Social Psychology Bulletin,* 18 (5): 591–602. https://doi.org/10.1177/0146167292185010.

Thalles Olivier. 2017. "Adiivka, Ville Symbole de La Guerre En Ukraine." La Croix, January 31, 2017.

Veen, Vincent Van, Marie K. Krug, Jonathan W. Schooler, and Cameron S. Carter. 2009. "Neural Activity Predicts Attitude Change in Cognitive Dissonance." *Nature Neuroscience,* 12 (11): 1469–74. https://doi.org/10.1038/nn.2413.

We are Social. 2018. "We Are Social. Digital, Social, Mobile: Les Chiffres de 2017." https://wearesocial.com/fr/blog/2017/01/digital-social-mobile-les-chiffres-2017.

CHAPITRE 2 : Cadre théorique, approche épistémologique et méthodologique

Le chapitre 1 a repris les premières observations de terrain qui ont fait l'objet d'un premier article. Ce travail retrace l'expérience ukrainienne menée hors d'un contexte de recherche, l'approche qui y était développée correspondant à l'analyse d'objets techniques liés aux conflits se déroulant dans la partie est du territoire, le Donbass. Ainsi, la présente recherche trouve son origine dans une approche initiale de terrain d'où a émergé la problématique de recherche à savoir en quoi la diffusion de certaines informations et le canal utilisé dans un contexte de situations extrêmes soumis à une très forte pression de facteurs externes sont de nature à ne pas exécuter l'ordre ou les décisions de la hiérarchie. Cette problématique contient en elle-même trois ramifications principales, à savoir, le rôle de l'altération de la confiance et prise de décision, le rôle des valeurs dans le renforcement de la confiance et des mécanismes de coopération et la perméabilité des personnels aux informations divergentes de celles délivrées par l'organisation.

Afin de travailler à la compréhension des phénomènes observés , j'ai procédé à un retour au cadre théorique avant de poursuivre l'investigation, notamment par la mise en place d'entretiens visant à les valider, ou, au contraire, à les invalider les propositions formulées à la suite de la revue de littérature et à la création d'une observation dirigée. Ces allers-retours entre le terrain et la théorie caractérisant la démarche abductive, cette dernière s'est tout naturellement imposée à cette thèse. Enfin, au regard des modalités d'accès aux informations et aux données on ne se situera pas dans une logique de vérifi-

cation d'hypothèses, mais plutôt de formulation de propositions, validées sur la base d'étude de cas.

1. Un cadre théorique transdisciplinaire

Cette thèse par articles propose un design original, mais non unique en science de gestion. Dans ce contexte, les articles devaient répondre à des logiques propres, par conséquent les cadres théoriques sont présentés individuellement. Ce chapitre s'attache donc à synthétiser l'ensemble des cadres théoriques mobilisés dans cette recherche.

La nature même du sujet appelle un cadre théorique pluridisciplinaire et transverse. Les premières observations mettaient en lumière l'utilisation de méthodes exploitant la dissonance cognitive afin d'altérer la confiance au point d'engendrer une prise de décision aléatoire de personnels évoluant en zones sensibles et en zones de guerre. Ces terrains sont par nature représentatifs des situations extrêmes, voire de crises (qui se différencient de la situation extrême en ce que l'initiative et le contrôle échappent aux acteurs qui sont confrontés à ladite situation). À ce titre, ils répondent à des règles particulières. Il en va de même pour les personnes appelées à y intervenir. Néanmoins, si l'armée demeure une structure verticale agissant dans des situations paroxystiques, elle n'en est pas moins une organisation confrontée à des problèmes structurels susceptibles d'altérer la mise en œuvre de sa stratégie et son efficience. En cela, elle est comparable en cela à toute autre organisation. En effet, une altération de la prise de décision ou une exécution déficiente des consignes constituent une problématique récurrente pour tous les types d'entreprises. À ce titre, il s'agit d'un domaine d'étude naturellement inscrit dans le pé-

rimètre des sciences de gestion, particulièrement des organisations et des ressources humaines, ces dernières constituant le matériau privilégié de ce travail.

Néanmoins, au vu de la spécificité des missions et des interventions de l'armée, le traitement d'un tel sujet nécessite de s'attacher aux champs théoriques de la polémologie, autrement dit, des « war studies ».

Par ailleurs, travaillant sur des personnes et sur leurs réactions, notamment quant à la confiance qu'elles accordent, qui peut être considérée comme pouvant être d'une importance première dans le comportement qu'elle induit, c'est tout naturellement qu'une large part de ce travail a pris appui sur la psychologie sociale.

Enfin, les dernières analyses conduites dans le cadre de cette recherche exigent, pour obtenir la vision la plus exhaustive possible, de se pencher sur le champ des « computer science » et de la neuroscience. Cette perception globale permet de mieux cerner les propositions envisageables pour prémunir efficacement les organisations confrontées aux situations extrêmes contre les risques identifiés comme susceptibles d'avoir un impact sur la confiance, la prise de décision et l'exécution des ordres et, pour finir, sur l'efficacité de la structure.

Avec une granularité plus fine, les observations réalisées lors des entretiens exploratoires, menés entre 2017 et 2018, s'attachent à plusieurs axes principaux, à savoir, la dissonance cognitive qui est la méthode mise en œuvre pour obtenir l'effet recherché, la confiance qui est l'objet que l'on cherchera à altérer afin de déclencher une prise de décision déviante, le cadre théorique relatif aux situations extrêmes qui représentent la particularité du cas observé et permettront de mieux saisir le sujet, et enfin la polémologie, à même de traiter de ce type d'attaques. De manière générale, les cadres théoriques

ont été utilisés pour construire des propositions permettant de comprendre et d'expliquer les phénomènes observés initialement, mais aussi au travers de leur formulation, grâce à l'apport du vocabulaire spécifique à ces mêmes cadres. Ces propositions ont ensuite été validées, ou invalidées, à la lumière de ces cadres théoriques, permettant ainsi d'en définir le degré de pertinence dans la recherche menée.

1. 1. La dissonance cognitive

Selon Festinger (1956), la dissonance cognitive est un état d'inconfort psychologique motivationnel ressenti par un individu dès lors que s'affrontent deux cognitions dites « inconsistantes », soit opposées. Afin de diminuer cet inconfort, le sujet ressentant de la dissonance cognitive aura tendance à mettre en place des stratégies de réduction afin de revenir à un état psychologique de confort tel que connu antérieurement. Cet enchaînement, fruit de l'éveil de la dissonance cognitive induira donc un changement de comportement. Selon Harmon-Jones (2002-2003), l'état de dissonance cognitive est orienté vers l'action ce qui fait écho au volet « motivationnel » précédemment décrit. Toujours selon Festinger, plus l'amplitude est grande entre les cognitions inconsistantes, ou dissonantes, plus la pression ressentie pour mettre en place des stratégies de réduction sera forte. Celle-ci pourra prendre plusieurs formes comme une modification des éléments constituant l'inconsistance, ou l'ajout d'éléments consistants. Ces stratégies auront pour objectif d'invalider une des deux cognitions à l'origine de la dissonance. Depuis Festinger, différents courants de la théorie de la dissonance cognitive sont apparus. Aronson et Carlesmith (1960, 1962) proposent une variation fonctionnelle qui semble particulièrement éclairante dans le cadre de cette recherche.

Ils y développent l'idée de l'importance de « l'autoconsistance » (self-consistency theory) dans la dissonance cognitive. Aronson (1968, 1969, 1992) se livre donc à une refonte de la théorie de Festinger. Pour ce chercheur, le développement de la dissonance est engendré par un écart entre le comportement (ou l'information reçue) et son concept du soi, ses standards personnels, en d'autres termes, l'idée que le sujet a de lui-même. Ainsi un comportement ou une action allant notoirement à l'encontre de l'image que le sujet a de lui-même déclencherait un ressenti de dissonance, un inconfort psychologique motivationnel.

Dans cette logique, tout individu ayant reçu une formation, un conditionnement, fort, ayant eu pour effet d'exacerber les valeurs morales et sa perception de soi à la lumière d'idiomes inculqués, serait particulièrement sensible à une attaque de dissonance cognitive. Or, nos sujets (de même que la majorité de ceux intervenant en situation extrême) reçoivent un conditionnement fort dont l'objet est de les aider à donner du sens aux situations chaotiques auxquelles ils sont confrontés. Dans certains cas, ce conditionnement se fonde sur des valeurs morales socialement acceptées et majoritairement perçues comme positives. En outre, Aronson signale également que la validation empirique des cognitions aura une réelle plus-value de renforcement.

Dans le cas présent, cette validation empirique du bien-fondé de la formation, et donc du conditionnement reçu, reçoit une traduction pratique. La force des savoirs acquis et des apprentissages assimilés participant à la préservation de l'intégrité physique des sujets ayant suivi la formation conditionnante, à savoir les soldats. Quant aux valeurs traditionnelles qui sont enseignées puis adoptées par un grand nombre de soldats, elles sont généralement socialement considérées comme positives (la défense de la population par exemple). À ce titre, elles permettent aux soldats d'accéder à un concept du soi positif

(statut de guerrier magnifié, du héros, valeur des honneurs, glorification du sacrifice). Or, selon Thibodeau et Aronson (1992), une conception positive de soi est un pré requis pour le déclenchement des effets de la dissonance cognitive.

S'il n'est pas question de limiter le champ de la dissonance à la seule autoconsistance, il semble que dans le cas présent et compte tenu de la nature particulière des sujets observés, elle puisse être particulièrement intéressante.

Stone et Cooper (2001) propose une autre réécriture à prendre en compte : le modèle des standards du soi (Self Standard Model — SSM). Il s'agit d'une théorie intégrative selon laquelle l'éveil de la dissonance est relié avec l'estime de soi, en lien direct avec les règles de conduite accessibles dans la mémoire de l'individu. On parlera alors d'éveil idéographique de la dissonance s'il est issu d'une inadéquation avec les standards personnels (proche de l'autoconsistance) ; et d'éveil homothétique si ce sont les standards normatifs de jugements qui sont mobilisés. Se pose alors la question de savoir si, dans le cas de militaires fortement conditionnés, les volets idiomatiques et homothétiques ne s'entremêlent pas, tant les valeurs auxquelles ils associent leurs personnalités propres touchent aux valeurs normatives.

Ce modèle sera analysé à la lumière des entretiens menés et de l'analyse des données collectées afin de vérifier s'il s'adapte en totalité, partiellement, ou pas du tout à la situation observée, mais aussi s'il intervient seul dans l'altération de la confiance due à des pressions exogènes ou s'il s'adosse à d'autres théories de psychologie sociale.

Ce travail analyse donc les facteurs internes et externes pouvant participer à l'altération de la confiance, structurée sur les valeurs que l'organisation développe et communique à ses agents. Ces valeurs ont pour objet de sécuriser le développement de la stratégie

organisationnelle par la stabilisation des prises de décision des personnels, de leur façon d'exécuter les ordres, afin que ces dernières restent en adéquation avec les attentes de la hiérarchie.

À la lumière de ce cadre théorique, on pouvait s'attendre à ce que les valeurs de l'organisation renforcent les processus de coopération entre les différents agents, et renforcent également la confiance dans les différentes strates de la hiérarchie de l'organisation. De même, la présence de valeurs fortes était supposée protéger les membres de l'organisation d'influences extérieures visant à altérer leurs prises de décisions et la bonne exécution des consignes, clefs du déploiement de la stratégie de l'organisation.

À l'analyse des éléments exposés, il apparaît que les propositions formulées dans le tableau présenté précédemment s'appuient sur un cadre théorique adapté.

À titre d'exemple, alors qu'il était attendu que l'ancienneté et l'exposition en situation extrême participent à renforcer cette imperméabilité en accroissant la confiance entre les membres de l'organisation, l'analyse des données contredit cette proposition. C'est sur la base de ces présupposés, issus d'un cadre de théories transdisciplinaires, que la grille d'entretien a été construite comme indiqué dans le chapitre relatif à la méthodologie.

1. 2. La confiance

La confiance est un champ qui a été étudié par de nombreux chercheurs, à travers différentes spécialités. S'intéresser à la confiance dans le cadre des opérations militaires est en phase avec les recherches menées en gestion sur ce thème. En ce qui concerne la confiance, les années 1990 ont été marquées par l'essor des recherches relatives aux problématiques mêlant la confiance au contrôle et à la coordination. Ces thèmes se recoupent avec l'étude menée ci-dessous où la confiance et l'incertitude seront des fac-

teurs déclenchants de problématiques potentiellement lourdes de conséquences pour l'organisation.

Néanmoins, la confiance reste un terme protéiforme auquel plusieurs définitions ont été données. Pour McAllister (1995), elle a un fondement à la fois cognitif et affectif, elle est un facteur de cohésion à l'intérieur des groupes armés. Pour Bhattacharya & al (1998), la confiance est la somme des résultats positifs de l'espérance basée sur les actions attendues d'une autre partie dans une interaction basée sur l'incertitude. Selon une autre définition, elle serait un état psychologique comprenant l'intention d'accepter la vulnérabilité sur la base d'attentes positives quant aux intentions, ou au comportement, d'un autre (Rousseau et al, 1998). Pour Mayer, Davis et Schoorman (1995), la confiance est « une volonté d'être vulnérable envers un autre parti lorsque ce parti ne peut être contrôlé ou surveillé ». Enfin, pour d'autres auteurs, la « loyauté » est également identifiée comme un mot-clé (Adams, 2003).

Bernoux et Servet (1997) mettent quant à eux en avant l'incertitude et la vulnérabilité. Selon eux, la confiance est la « condition d'une personne, d'un groupe ou d'une institution à un moment donné, fondée sur des éléments affectifs, intuitifs, ou sur un ensemble d'informations et de croyances, de préjugés et par des processus d'apprentissage face à un objet, un mécanisme, un animal, un environnement physique, un individu, un groupe de personnes ou une organisation de toute nature, et dont la connaissance permet d'anticiper avec un degré plus ou moins élevé d'incertitude leur devenir ou leur réaction ou comportement dans telle ou telle situation ».

Sous l'angle de la gestion des organisations, la confiance met en exergue une augmentation potentielle du risque d'opportunisme, particulièrement en cas de constitution de ré-

seaux de confiance horizontaux au sein de la structure organisationnelle, comme, par exemple cela pourrait être observé entre soldats.

Transposée dans le domaine militaire, la confiance est pensée comme en relation directe avec la cohésion et l'efficacité des modes opérationnels. Ainsi, certains travaux définissent la cohésion militaire selon trois composantes principales : les relations avec les pairs, les relations entre supérieurs et subordonnés et la relation avec les forces armées et le gouvernement (Stewart, 1988, et Etzioni, 1961). De facto, dégrader l'une des perceptions relatives à ces structures dans l'esprit des soldats pourrait altérer la confiance et la cohésion. Par parallélisme, une méfiance croissante envers les supérieurs altérera la cohésion et donc l'efficacité des modes opérationnels du groupe dans le sens de l'atteinte de ses objectifs, augmentant d'autant le risque quant au succès de la mission et complexifiant également la gestion de l'organisation et du déroulement de la mission pour l'organisation.

À la lumière de ces définitions et en raison de la nature des tâches confiées aux personnels visés par cette étude, les notions relatives à l'acceptation de la vulnérabilité prennent rapidement un aspect très réaliste, les soldats risquant d'être blessés ou tués lors des opérations où ils sont déployés. Dans plusieurs définitions de la confiance, il apparaît que l'incertitude est un « game changer ». Par effet miroir, la confiance apparaît bien comme étant un fondement du quotidien des soldats et, de facto, un axe requérant toute l'attention de l'organisation.

Enfin, il semble que la confiance ressentie et accordée par les soldats est souvent ternaire en ce qu'elle mobilise trois axes. Le premier serait de nature principalement instinctive, reliée au niveau macro représenté par le Gouvernement. Il s'agirait là d'une

confiance quasi intuitive due à l'appartenance originelle permettant, par principe et a priori, d'avoir une confiance plus élevée dans son pays que dans un tiers.

Le second axe serait structuré autour de la confiance nouée entre l'organisation et l'individu adhérant aux règles supérieures de l'entité. Il s'agirait là d'une confiance organisationnelle de type wébérienne basée sur une interaction cognitive, nourrie des apprentissages délivrés par l'organisation et allant parfois jusqu'à permettre le développement d'une culture commune.

Le troisième axe serait fondé sur une confiance dans les « frères d'armes », comme le développe Ouchi (1980). On parlera alors de confiance clanique.

Cette confiance clanique est à mettre en perspective avec les théories de Meyerson & al (1996) pour qui des personnes, même dissemblables, accorderont plus rapidement leur confiance à ceux à qui elles attribuent de la bonne volonté au regard du but recherché par le groupe. Le développement de la mythologie du héros prend là tout son sens, en ce qu'il permet aux soldats de s'identifier à des figures tutélaires communes, à des codifications comportementales facilitant le développement de la confiance. Enfin, une fois que l'affect associé à un groupe social est déclenché par le processus de catégorisation (i. e. par la reconnaissance de valeurs communes), il peut immédiatement influencer l'état affectif général et avoir un effet non conscient sur les jugements (Dovido & Gaertner, 1991, Olson & Zanna, 1993), permettant l'accroissement de la confiance clanique.

Selon la littérature, la confiance interpersonnelle, donc clanique, limiterait les risques d'opportunisme, en raison de la dépendance affective de l'individu à son « clan ».

Selon McAllister (1995), la confiance interpersonnelle à une double origine cognitive et affective, mais elle s'appuie surtout par la volonté d'un individu de se rendre vulnérable aux actions d'une tierce personne. Selon cette définition, accroître l'incertitude dans le cadre des actions militaires où se place cette recherche serait particulièrement dangereux. En effet, la nature spécifique de ces professions particulières donne au risque une réalité particulièrement tangible et parfois quotidienne. En effet, si un soldat doute, il n'acceptera plus, ou tout du moins bien plus difficilement, d'accroître sa vulnérabilité au-delà de ce à quoi le contexte l'y contraint. Enfin, la confiance clanique étant dans cette hypothèse toujours intacte et forte, un effet de contagion au sein de ce groupe pourrait être observé. La conséquence serait un essaimage de l'incertitude, une diffusion de la perte de confiance, renforçant la fracture entre structures horizontale et verticale. À terme, cette évolution pourrait fortement handicaper les modes opérationnels, voire la survie de l'organisation, tout particulièrement quand celle-ci est appelée à intervenir dans un contexte de situation extrême.

Par construction, l'altération de la confiance des soldats dans l'une des trois strates telles que décrites par Stewart et Etzoni pourrait engendrer des conséquences immédiates pouvant aller jusqu'à l'échec de la mission, assorti de son corollaire de dommages subis que cela soit par l'organisation ou par l'équipe intervenante. Cette analyse de la revue de littérature justifie donc parfaitement une des hypothèses que le travail de thèse s'applique à étudier. Au-delà de leur propre mission, un échec pourrait entacher la crédibilité et la fiabilité de l'organisation elle-même.

1. 3 . les situations extrêmes

Parler du fonctionnement militaire nécessite d'évoquer le contexte dans lequel il s'inscrit. Dans le cadre de leurs missions, les militaires évoluent dans des situations extrêmes

au sens qui leur est donné par Aubry, Lièvre, & Hobbs (2010), et par d'autres chercheurs (Bouty et al., 2012 ; Godé, 2015 ; Godé & Lebraty, 2015). Selon ces auteurs, une situation est considérée comme extrême quand elle présente trois caractéristiques principales : être évolutive, incertaine et risquée.

Selon Godé (2015) il faut comprendre l'incertitude comme intimement liée à l'imprévu. Clegg et al (2006) y attacheront également l'idée de surprise puisqu'un évènement de cette nature ne peut pas, par essence, faire l'objet d'un contrôle absolu, ce que rappellent Perrow (1994) et Tsoukas (2005). Ainsi l'incertitude peut se comprendre comme l'apparition d'un ou de plusieurs évènements imprévus à même de créer la surprise : c'est ce type d'évènement que Taleb (1998) baptisera « Black Swan ». Dans le même ordre d'idée, Rivolier (1998) expliquera qu'« évolutive » se réfère à une situation en rupture avec la vie quotidienne, ainsi la situation extrême représenterait un écart entre le quotidien, la situation « A », et la situation « B » qualifiable d'extrême, qu'elle soit présente ou à venir dans un futur proche. L'incertitude est ici entendue comme étant radicale et totale (Knight, 1923) c'est-à-dire qu'il sera difficile, voire impossible, de mesurer la probabilité qu'un évènement quelconque — mais le plus souvent à risque — apparaisse. En outre, l'origine des évènements provoquant l'incertitude peut être difficile à anticiper, leur origine pouvant tenir à des éléments extérieurs comme à des facteurs internes à la structure concernée par cette incertitude. En somme, c'est une situation où l'inattendu peut se manifester à tout instant (Orlean, 1986) ; Moigne (1990) parlera d'un moment où l'impossible devient possible, voire probable.

Quant au risque, il peut être entendu à plusieurs niveaux en matière de dommages subis, mais il n'exclut ni le risque de blessures ni le risque mortel. Là encore, comme dans l'incertitude, l'échelle des risques n'est pas toujours précisément mesurable par les per-

sonnes ou organisations qui y sont confrontées. Enfin, selon la complexité de la situation extrême rencontrée, les acteurs pourront être confrontés à des risques multiples.

En nous basant sur ces trois caractéristiques, il apparaît clairement que les missions militaires revêtent toutes les caractérisant des situations extrêmes.

Plusieurs chercheurs (Hällgren et al., 2018) considèrent cependant qu'il existe différents types de situations extrêmes. Leurs travaux se réfèrent à trois catégories définies comme suit :

– **Les contextes risqués (risky contexts)** : dans ce cas, les acteurs (qu'ils soient des personnes physiques ou morales) sont exposés ponctuellement à des situations considérées comme extrêmes en ce qu'elles sont imprévues et emportent des conséquences potentiellement graves. Envisageant cette possibilité, ces structures ou acteurs développent des stratégies de protection fondées sur des « routines » propres à assurer la fiabilité des systèmes mis en place afin de se prémunir contre les conséquences de ces imprévus. Parce que la situation a été anticipée, acteurs et structures ont élaboré des processus qui leur permettront de réagir à ces imprévus, le cas échéant en improvisant.

– **Les contextes d'urgence (emergency contexts)** : dans ces situations, le risque, imprévu, mais constant, fait peser une pression habituelle sur les acteurs. Cette permanence du risque autorise donc les acteurs à l'intégrer, particulièrement s'il fait partie de leur activité principale et que les conséquences peuvent devenir très rapidement catastrophiques (Shrivastava, Mitroff, Miller, & Miclani, 1988). Selon Weick (1993), la capacité de donner du sens à la situation rencontrée sera nécessaire pour que les acteurs puissent y réagir correctement.

– **Les contextes perturbés (disrupted contexts)** : Ici, les évènements imprévus sont externes à l'activité habituelle et principale des acteurs alors que, dans les deux autres cas, ils peuvent également être induits par des évènements internes. Parce que les évènements sont externes, inattendus, nouveaux et non anticipés par les acteurs, ils ne seront pas catégorisables (Christianson, Farkas, Sutcliffe, & Weick, 2009 : 846).

Godé (2015) présente une catégorisation relative aux modes de gestion applicables en situation de crise où des évènements peuvent s'enchaîner, dégradant d'autant la situation générale. En premier lieu, elle développe la « routine » dans laquelle les principales caractéristiques de la situation extrême, à savoir le risque et l'incertitude, sont faibles. Comme dans le contexte risqué, les acteurs peuvent s'appuyer sur des procédures déjà mises en place par l'organisation qui aura anticipé ce type de situation. Dans la pensée de Godé, la situation de routine peut devenir la situation « imprévue » ou « inattendue » qui représente alors le second niveau de sa catégorisation.

Pour que ce basculement s'opère, il faut qu'un ou plusieurs évènements inattendus apparaissent, créant un effet de surprise, voire de sidération chez des acteurs qui ne pourront dès lors plus se référer à leur routine. Dans ce cas, ceux-ci devront faire preuve de réactivité face à l'évènement inattendu, ou à la succession d'évènements inattendus (Bouty et al., 2012 ; Godé, 2015). Cette créativité pourra alors prendre la forme d'un « bricolage socio-cognitif » (Bechky & Okhuysen, 2011), pouvant déboucher sur des stratégies issues de l'improvisation « bottoms up » parfois appuyées sur les éléments cognitifs ou affectifs fondateurs des acteurs impliqués dans l'action, tels que leurs propres valeurs.

Dans le cas où les évènements inattendus n'ont jamais été anticipés et résultent de causes totalement inconnues, la situation peut dégénérer en situation de crise. Celles-ci sont rares et se caractérisent par une amplitude qui dépasse totalement les capacités des acteurs en présence. En fonction de l'ampleur de son incertitude et des risques encourus, la situation de crise impliquera un mode de gestion spécifique dans lequel les acteurs et les organisations en présence seront appelés à modifier significativement leur mode de raisonnement (Roux-Dufort & Ramboatiana, 2008).

Dans la catégorisation proposée par cette auteure, il est important de noter qu'une situation extrême ne renvoie pas nécessairement à une situation de crise. En effet, la capacité d'anticipation et de renouvellement des procédures, fondées sur un regard critique et proactif, pourra permettre à une structure, même familiarisée aux situations extrêmes, de ne pas glisser vers la catégorie de crise précédemment décrite (Carroll, Rudolph, & Hatakenaka, 2002 ; Weick & Sutcliffe, 2006), tant celle-ci se caractérise par le dépassement de la capacité des acteurs à y faire face.

Au cas particulier de l'étude, les soldats interviennent de façon régulière dans des situations extrêmes qui, bien que sous contrôle, sont marquées par une pression temporelle forte, ne devraient être qu'exceptionnellement vécues par le reste de la population. Si ce contexte, qui est lié à leur activité principale, a fait l'objet de procédures précises, comme dans le contexte d'urgences, la situation peut rapidement prendre un tour plus radial au cas où des rebondissements totalement imprévus feraient appel à des méthodes, tactiques ou stratégies totalement inédites. Ainsi, les situations extrêmes qu'ils rencontrent peuvent évoluer et passer du contexte d'urgence au contexte de crise à partir du moment où il n'y a plus de contrôle. À titre d'exemple, en se penchant sur la cinéma-

tographie dédiée le film « Black Hawk Down » de 2001 dépeint le passage d'une situation extrême à une situation de crise. Ce film, tiré du livre livre *Black Hawk Down : A Story of Modern War* écrit par Mark Bowden, relatant les combats ayant eu lieu en 1993 à Mogadiscio où dix-neuf militaires américains trouvèrent la mort, de même que de nombreux somaliens. Au début du film, les milices de la faction d'Aidid abattent deux hélicoptères UH-60 Black Hawk ce qui sera le début de l'histoire développée ensuite. Lors du crash des hélicoptères Black Hawk en zone ennemie, un des protagonistes annonce « nous avons perdu l'initiative ». À ce moment précis, une situation extrême, préalablement sous contrôle, devient une situation de crise, qui par nature échappe à tout contrôle.

Dans le cas des soldats, les commandements sont conscients que vivre et intervenir de façon récurrente dans des situations extrêmes exige un conditionnement fort afin de minimiser les risques et tenter de faire décroître l'incertitude tout en participant à donner du sens à la situation vécue, comme décrite par Weick. Dans cette vision, un comportement déviant des exécutants, imprévu par la hiérarchie chargée de la stratégie, peut être en soi un « black swan », et peut faire basculer la situation extrême vers une situation de crise.

Il apparaît donc que l'incertitude est une constituante fondamentale de la situation extrême, puis de crise. C'est à ce titre que la pertinence d'analyser la nature de la confiance dans le fonctionnement des équipes militaires s'est fait jour.

1. 4 . La polémologie appliquée à la guerre informationnelle

La confiance, étudiée dans le cadre des équipes militaires, sera développée dans le chapitre qui lui est consacré. Cependant, la nature même du sujet qui traite des opérations cherchant à influencer la confiance et, par voie de conséquence, à modifier le comportement a été reprise dans les théories militaires, tout particulièrement depuis une décennie.

À ce titre, si le terme « cyberwarfare » est souvent employé, d'autres terminologies, notamment « cyber opération », « opération informationnelle », mais aussi « guerre hybride » sont communément reprises par le monde politique, militaire, mais aussi dans les médias. Cependant, le terme de « guerre hybride » soulève un certain nombre de problèmes conceptuels. En effet, beaucoup de chercheurs estiment avec justesse qu'il s'agit d'un « mot-valise » issu du vocabulaire biologique (l'hybridation biologique) qui ne correspond pas, au vu du contexte et des opérations menées dans le Donbass depuis la révolution du Maïdan, à la nature profonde de ce type d'opérations menées conjointement à une guerre traditionnelle. Ce débat a pris énormément de vigueur depuis 2014.

Le terme s'est répandu en 2009 sous la plume de Franck Hoffmann dans un article intitulé « The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War ». Il y reprenait l'analyse du Général Charles Krulak, décrivant les conflits à venir comme les descendants de la guerre de Tchétchénie. Il les définissait comme un mélange d'opérations régulières et irrégulières, conventionnelles et non conventionnelles. Le terme fut également utilisé pour décrire les méthodes employées par le Hezbollah pendant la guerre du Liban en 2006, avant d'être défini comme l'exploitation de tout le spectre des moyens offerts par la guerre moderne en ne se restreignant pas à la guerre conventionnelle.

Apparaît ici le premier problème : de facto, toute menace pourrait être considérée comme « hybride » dès qu'elle ne se limite pas à une forme et à une dimension unique de la guerre. À la lumière de l'évolution des techniques développées notamment par le complexe militaro-industriel (CMI) et de l'évolution des conflits lorsqu'une menace ou un recours à la force est défini comme hybride, le mot perd aussitôt sa valeur et crée de la confusion au lieu de clarifier la « réalité » de la guerre moderne.

En outre, le terme de guerre hybride a souffert d'un effet de « trend mark », notamment après que les médias l'ont associé à ce qui fut rapidement appelé la « doctrine Guerassimov » d'après le nom du chef d'état-major russe. Cette supposée « doctrine » se référerait à une théorie expansionniste des conflits, parfois reprise comme une approche de guerre totale. La réalité est tout autre. Cette appellation trouve son origine dans une déclaration de 2013 du Général Valery Guerassimov, qui n'est pas un théoricien des conflits. Dans une intervention, il expliquait qu'« un État parfaitement prospère peut, en quelques mois et même quelques jours, se transformer en une arène de conflits armés féroces, devenir victime d'une intervention étrangère et sombrer dans un tissu de chaos, de catastrophe humanitaire et de guerre civile. » Cette déclaration a été reprise dans un blog tenu par Marc Galeotti, chercheur renommé et spécialiste de la Russie qui, pour avoir un effet d'annonce renforcé, baptisera l'article de son blog la « doctrine Guerassimov ». Malgré les explications que l'auteur a données ensuite, où il insistait sur le fait qu'il ne s'agissait pas d'une doctrine, le terme est resté et la « doctrine Guerassimov » est devenue un des piliers de la guerre hybride comme stratégie pensée et structurée. Or, dans cette intervention, le Général Guerassimov évoquait la manière dont Moscou comprenait les évènements survenus lors du « Printemps arabe » et des « révolutions de couleur » à l'encontre des régimes pro russes. En d'autres termes, il s'agissait d'un constat

amenant à s'interroger sur la façon de lutter contre ce type de mouvements et non d'une doctrine militaire au sens où la Russie peut traditionnellement l'entendre. Les explications de Marc Galeotti (Galeotti, 2018) sur ce point, qui tentaient de clarifier la situation, n'auront pas suffi à contrecarrer l'expansion de cette terminologie qui permettait de mettre des mots sur une angoisse montante et qui, par certains aspects, miroitait parfaitement avec les évènements qui devaient se dérouler en Ukraine les années suivantes.

Le risque induit par la diffusion de cette vision doctrinale est qu'elle ne correspond pas à la réalité de l'approche russe, notamment en ce que la pensée offensive ne repose pas sur une seule pensée organisée aux mains d'une seule et même organisation, mais que l'objectif reste largement politique, fondé sur de grands items de démoralisation, de diversion et de distraction s'autorisant l'opportunisme au point de parfois pouvoir paraître contradictoire dans les rhétoriques employées. Enfin, ce qui, en Occident, est défini comme « guerre hybride » ne trouve pas d'équivalent *stricto sensu* dans la stratégie russe et ne revêt pas forcément un caractère particulièrement innovant. En effet, rompre la chaîne de commandement, attiser les insurrections locales, brouiller les communications sont des méthodes connues de longue date (appelées des « mesures actives » par la Russie). Ce sont seulement les innovations massives qui ont marqué leurs vecteurs applicatifs qui ont rendu ces mesures sensiblement plus efficaces. Si ces procédés sont considérés comme l'avant-garde d'un conflit armé classique, elles peuvent également constituer une alternative à la guerre cinétique. En effet, dans la vision russe, l'OTAN est un ennemi, mais un ennemi puissant avec lequel il serait difficile de rivaliser de manière frontale, tant d'un point de vue technique qu'économique. Il paraît donc plus pertinent et efficace de retourner les normes des institutions démocratiques ennemies

contre elles-mêmes afin d'ouvrir ou d'élargir les lignes de faille existantes qui représentent autant d'opportunités de travailler à les neutraliser par le biais de comportements opportunistes. C'est l'idée qui sera développée par Kennan (1948), l'un des principaux penseurs de la politique américaine de la guerre froide, qui explique que tous les moyens autres que la guerre qui sont à la disposition d'un État peuvent être mis en œuvre pour atteindre l'objectif politique fixé. Il poursuit en définissant la « guerre politique » comme des opérations à la fois évidentes et secrètes, pouvant aller d'*« actions évidentes telles que des alliances politiques, des mesures économiques… Et de la propagande "blanche" à des opérations secrètes telles que le soutien clandestin à des éléments étrangers "amis", une guerre psychologique "noire" et même l'encouragement de la résistance souterraine dans des États hostiles ».*

Ainsi la subversion ne serait pas une composante de la guerre, mais une guerre en elle-même.

Enfin, le terme de guerre hybride fait référence à un nouveau format de conflit, ce qui est discutable. En effet, comme noté par Gray (2015) la guerre du futur serait principalement identique, dans sa nature profonde, à celles connues par le passé, mais en différerait principalement, les moyens techniques utilisés permettant d'en exploiter d'autres dimensions. La permanence des méthodes fondamentales et des objectifs poursuivis rendrait caduque la mise en œuvre d'une nouvelle terminologie conceptuelle.

À ce titre, l'OTAN elle-même ne parvient pas à une définition claire de ce que serait la « guerre hybride », aucun consensus ne pouvant être trouvé parmi les 28 membres. Ainsi l'organisation a édité une note de Van Puyvelde (2015), où il était préconisé aux décideurs occidentaux d'oublier « tout ce qui est "hybride" et de se concentrer sur la spécificité et l'interdépendance des menaces auxquelles ils sont confrontés. La guerre, qu'elle

soit ancienne ou moderne, qu'elle soit hybride ou non, est toujours complexe et ne peut être assimilé à un seul adjectif. Toute stratégie efficace doit prendre en compte cet environnement complexe et trouver des moyens de le gérer sans trop simplifier. » Aussi, fort de ce constat, la terminologie de « guerre hybride », bien que souvent utilisée dans les médias et dans des contextes spécifiques ne sera pas utilisée dans ce document.

Ce travail sémantique réalisé, nous avons continué l'exploration de la littérature. Schaap (2009) définit le cyberwarfare, ou la guerre cybernétique comme l'utilisation des capacités réseau d'un État pour perturber, nier, dégrader, manipuler ou détruire des informations contenues dans les ordinateurs et les réseaux, d'un autre État ». Pour Clarke (2010), il s'agira d'« actions d'un État-nation visant à pénétrer dans les ordinateurs ou les réseaux d'un autre pays dans le but de causer des dommages ».

Le Centre d'excellence coopératif de la cyberdéfense (CCDCOE) de l'OTAN adopte une approche large, selon laquelle la cyber guerre serait « l'utilisation de capacités cybernétiques dans le but principal d'atteindre des objectifs dans ou par l'utilisation du cyberespace ». Cette définition est suffisamment large pour englober les cyber psyops dans un contexte de guerre, ce qui est en totale adéquation avec notre sujet tant les experts s'accordent à penser que l'Ukraine était et est toujours un laboratoire d'essais pour les opérations de cyberguerre ainsi que pour les opérations psychologiques ou « psyops » (Greenberg, 2017). À cet égard, il est important de définir le terme « psyops ». De manière générale, une psyops est une opération visant à influencer l'état d'esprit de l'ennemi par des moyens non combatifs. À cette fin, les psyops peuvent utiliser des informations ou des indicateurs choisis pour influencer les émotions, les pensées et les réactions des individus. Le terme « psyops » apparaît en 1965, mais l'expression « Opérations de soutien à l'information militaire » (Military Information Support Operations

— MISO), apparu plus récemment l'a souvent remplacé notamment aux États-Unis. Bien que les psyops soient définies comme essentielles aux succès militaires américains, que cela soit en temps de guerre ou en temps de paix, le terme a été jugé trop menaçant par le Département de la Défense (DOD). Aussi en 2010 il ordonna à l'armée de le remplacer par une autre terminologie : MISO (Cowan & Cook, 2018). À la suite à ce pivot sémantique, un commandement dédié lui a été assigné sous la forme du commandement des opérations d'appui à l'information militaire (Military Information Support Operations Command MISOC) dont la mission est de fournir un soutien à l'information militaire (MIS) des combattants, mais aussi des ambassades et d'autres agences afin de synchroniser les plans et actions et d'exécuter des activités d'information et d'influence (IIA) dans toute la gamme des opérations militaires. Mis en œuvre en 2011, le MISOC, a pour objet d'unifier les efforts déployés par la mie en œuvre des MISO envisagées à l'échelle mondiale, tout en en augmenter la capacité d'intervention. Pour cela, il vise à s'investir dans les différents pilotages des théâtres d'opérations spéciales (Theater of Special operations command — TSOC). Les phénomènes observés qui paraissent se rapporter à des psyops menées par l'intermédiaire du cyber seront qualifiées de cyber opérations dans le cadre d'une guerre informationnelle d'influence.

En effet, sur le front de l'information ukrainienne, différents canaux ont été utilisés pour faire correspondre les profils psychologiques des cibles, et l'armée n'a pas fait exception à la règle. En ce qui concerne les soldats, des opérations subtiles ont été menées notamment sur Internet, en particulier sur les réseaux sociaux et les forums de discussion. Ces opérations ont joué sur la confiance dans des groupes de pairs pour générer des doutes et de l'incertitude à l'endroit des membres des gouvernements ou de la hié-

rarchie des cibles. Les combattants actifs ont été visés tout autant que les anciens combattants.

Cependant, ce travail ne se cantonne pas aux seuls champs de bataille, mais envisage la possibilité d'opérations visant à affaiblir la confiance des agents dans l'organisation à laquelle ils appartiennent afin de générer chez eux une prise de décision altérée, dont la conséquence serait une modification de leurs comportements et des conditions d'exécution des consignes données, détériorant par là même sérieusement la stratégie et l'organisation de la structure visée. Or ce type de travail peut être mené en temps de paix. Il peut également ne pas se limiter à des structures militaires, mais s'étendre à d'autres organisations amenées à intervenir en situations extrêmes ou à forte incertitude. En procédant à ce type de modélisation abstractive, il apparaît clairement que la confiance est l'objet visé par la détérioration ce qui amène logiquement à procéder à une revue de la littérature sur ce thème.

2. La pertinence de l'approche abductive

D'un point de vue épistémologique, ce travail s'inscrit dans l'observation de faits surprenants constatés sur le terrain et qui ont soulevé un premier questionnement, qui fut confirmé ensuite par les premiers entretiens exploratoires menés sur le terrain. Ces derniers auront permis la définition d'une problématique ouvrant sur la recherche de l'orientation théorique et conceptuelle à donner à cette problématique — qui s'avère ici transdisciplinaire —, puis à la formulation de propositions. Afin de valider ces propositions, d'autres entretiens exploratoires de collecte de données ainsi que la tenue d'une observation dirigée de type expérimental ont été réalisés et analysés avec une approche qualitative à visée compréhensive. Ces analyses ont

permis de procéder à une étape d'invalidation/validation des propositions émises pour ensuite rechercher les fondements théoriques auxquels ces dernières pouvaient se rapporter.

Ce travail est donc parti d'une observation empirique qui a généré une analyse et une tentative d'ordonnancement des éléments constatés. Au-delà, cette première phase exploratoire aura permis d'ouvrir une seconde phase de recherche et d'analyse de fond qui est l'objet de cette thèse. L'objectif a été de remettre en question les propositions formulées depuis la base théorique en y introduisant un facteur nouveau, en les confrontant à une seconde vague d'entretiens, elle-même scindée en deux phases et incluant un volet expérimental.

Cette seconde vague, et la mise en œuvre de l'observation dirigée qu'elle comporte avaient notamment pour objectif de tester la reproductibilité et la stabilité des propositions avancées. Ici, la préconisation n'est pas présente a priori, mais émerge des données de terrain — d'un étonnement — pour faire ensuite l'objet d'une phase de vérification. C'est en effet, l'observation d'un fait « surprenant » — la modification des comportements des militaires — parce que « nouveau » — premières observations à ce niveau d'amplitude — et « anormal » — les hommes ne sont pas censés douter de leur hiérarchie, ce qui correspond aux items développés par Aliseda (1998). Enfin, cette recherche s'attachera à faire émerger une proposition à même d'expliquer la situation, en d'autres termes, de limiter, voire de faire disparaître l'étonnement, face aux faits initialement ressentis comme surprenants.

Ce travail a été mené au moyen d'une démarche abductive, elle-même issue de la philosophie pragmatique décrite par Pierce (1958) qui, ayant travaillé sur l'abduction pendant près de cinquante ans, déclarait « si vous examinez attentivement la question du pragmatisme, vous verrez que ce n'est rien d'autre que la question de la logique de l'abduction ». Cependant, si définir l'abduction dans le cadre d'une recherche qualitative ne peut pas se résumer à évoquer

un courant philosophique, il est courant de se référer à Pierce pour tenter de la définir et, notamment, à cet extrait où A représente une hypothèse :

« La forme d'inférence […] est: le fait surprenant, C, est observé. Mais si A était vrai, C serait une évidence.

Par conséquent, il y a une raison de suspecter que A est vrai. Ainsi, A ne peut être conjecturé de manière […] abductive tant que son contenu n'est pas entièrement déjà présent dans la prémisse, « Si A était vrai, C serait une question ».

Dans ce texte, il apparaît donc que le fait surprenant du début est un élément fondamental de la démarche abductive puisqu'il permet le continuum des étapes successives. En outre, ce fait surprenant peut être unique ou multiple, être une anomalie ou au contraire une nouveauté en ce qu'il permet, selon Dumez (2012) "de formuler des hypothèses nouvelles ce qui renvoie bien sûr à la recherche qualitative. Cet auteur ajoute d'ailleurs « qu'une fois que le fait surprenant est repéré, l'abduction peut intervenir ». D'autres auteurs comme Dubois et Gadde (2002) qualifient ces anomalies ou faits surprenants de « données actives » intimement liées à la découverte, et émanant d'observations qui ne pourraient pas être trouvées grâce à la recherche.

En l'espèce, le fait surprenant, une réaction imprévue, a été repéré à plusieurs reprises et a en effet permis d'engager le travail de recherche. Dans le travail développé ici, il a fallu effectuer une sorte de retour en arrière, une fois le fait surprenant observé. En effet, la démarche a consisté à formuler des propositions sur les origines de ce fait étonnant, sur les raisons pouvant l'expliquer, en se fondant sur un cadre théorique qui donnait des points d'éclairage, mais n'expliquait pas tout.

À ce point de la démarche abductive, Aliseda (2006) fait remarquer que les formes peuvent varier, allant des règles établissant des liens de causalité aux théories nouvelles permettant la

compréhension du fait surprenant en passant par de simples faits explicatifs. Cette auteure conclut en expliquant que ces options peuvent également coexister. Pour Dumez (2012), plusieurs critères relatifs aux hypothèses formulées peuvent permettre de qualifier une démarche abductive de « réussie », à savoir : il faut que l'hypothèse jouisse d'un pouvoir explicatif ; qu'elle puisse être testée ; que cette hypothèse soit en mesure d'expliquer le plus de faits possible tout en étant la plus simple possible et la plus facile à tester ; enfin, l'hypothèse créée par abduction se doit de ne pas bloquer les possibles à venir, ce qui implique qu'elle ne soit pas définitive. C'est ce à quoi le travail présenté ici s'est attaché lors de l'émergence des propositions. Enfin, ce travail de recherche s'inscrit dans le champ des sciences de gestion et du management. Or, pour Dumez (2012), le management stratégique est la pensée de l'action. En cela, un travail de recherche dans ces disciplines doit s'attacher à faire émerger les acteurs en tant qu'être pensant, agissant et interagissant. Cette particularité due à la nécessité de l'action implique de mettre en lumière les stratégies d'action afin de les comprendre. C'est ce qui a été réalisé dans ce travail au travers la validation de différentes propositions pouvant contribuer à comprendre la construction et les motivations de ces stratégies d'actions, dont les origines peuvent être multiples, conformément à la pensée d'Aliseda. En outre, chercher à comprendre les modes d'action des acteurs observés, notamment dans le champ de la prise de décision et de l'exécution de la consigne à la lumière de la confiance, peuvent parfois se heurter à devoir observer l'inobservable. Aussi, la méthode qualitative a permis de remonter de l'observable vers l'inobservable par l'étude des acteurs, de leurs propos et actions dans une vision dynamique globale.

Outre l'observation d'un fait surprenant et la construction de propositions, ce travail de recherche se compose d'une multiplicité de phases ou l'abduction domine sans pour autant être

exclusive rejoignant en ceci la vision de David (1999) appliquée aux sciences de gestion. Pour ce chercheur, l'abduction s'entend dans des dimensions épistémologiques tout autant que logiques, car étant à l'origine d'un processus qu'il qualifie de « boucle ». Selon David, l'abduction, en tant que méthode de recherche, se compose de boucles combinant dans des processus récursifs les différents types d'approches (abductif, déductive et inductive). Ainsi, pour cet auteur 'la déduction permet de générer des conséquences (C) ; l'induction d'établir de règles générales (A) ; et l'abduction de construire des hypothèses (B) […] La plupart des raisonnements, et en particulier les raisonnements scientifiques, combinent les trois formes de raisonnement' (1999). Il ajoute qu'une fois les premières hypothèses validées ou invalidées, il faut 'reformuler — par abduction — de nouvelles hypothèses explicatives [ou compréhensives], et le cycle recommence'.

On retrouve ici le lien avec Pierce pour qui l'abduction prend naissance dans l'étonnement engendré par un évènement inexplicable. Concernant les processus développés par David dans ses boucles, Pierce nous explique que la déduction tire des conséquences d'une hypothèse, que l'induction détermine une valeur et que l'abduction peut introduire une nouvelle idée. Ainsi, il écrit que « la déduction prouve que quelque chose doit être ; l'induction montre que quelque chose est réellement agissant ; l'abduction suggère simplement que quelque chose peut être ».

Dans la pratique, cette recherche, qui a démarré à la suite d'un « étonnement », a ensuite débouché sur une première étude exploratoire où des orientations théoriques ont été dessinées, permettant l'élaboration de propositions. Par la suite, le volet théorique (ici transdisciplinaire) a été développé pour conforter les propositions. Ayant franchi cette phase avec succès, ces dernières ont d'abord été soumises à de nouveaux entretiens qui ont permis le recueil de

data, puis à une mise à l'épreuve de la validité des propositions dans la seconde vague de la 2. Cette séquence a autorisé la réalisation d'une analyse fine qui a débouché sur l'édition de règles, mais aussi sur la définition des limites de l'exercice. Ce séquençage du travail permet de mettre l'accent sur les travaux qu'il serait pertinent de poursuivre par la suite, fermant ainsi la « boucle » décrite par David. Concernant la mise à l'épreuve par le moyen d'une observation dirigée menée lors des entretiens de la phase 2 vague 2 des interviews, la grande difficulté de la démarche tenait à ce que l'étude vise des phénomènes sociaux qui, par nature, se manifestent dans des systèmes ouverts rendant ainsi leur reproduction en laboratoire, milieu artificiellement clos, délicate, voire impossible. Ce contexte spécifique justifie d'autant plus l'approche qualitative choisie pour cette étude.

Néanmoins, si la recherche qualitative avec une approche abductive paraît la plus logique, compte tenu de la nature du terrain de recherche, force est de reconnaître que coexistent nombre de protocoles de recherche qualitative dont la motivation est épistémologique. Certains d'entre eux sont motivés par un cadre post-positiviste, d'autres, par un cadre réaliste-critique ou encore constructiviste-pragmatique. Le travail présenté ici s'appuie sur la qualité d'inférences permettant d'identifier des causes et, plus encore, de modéliser des compréhensions possibles ainsi que les éléments sous-jacents aux phénomènes au cœur de la recherche, comme dans le paradigme épistémologique constructiviste pragmatique. Pour autant, la première étape de ce travail, qui s'est attachée à identifier des similitudes, des répétitions (patterns), au moyen de l'induction rappelle largement l'approche post-positiviste. En ce sens, on peut rappeler les travaux de Martinet (1990) qui appelait à un pluralisme méthodologique et à l'abolition de frontières rigides. Cependant, la seconde approche suivie dans la recherche s'écarte sensiblement de celle des positivistes pour se recentrer sur le constructivisme pragmatique, le chercheur ayant dû formuler ses suppositions sur les mécanismes observés en uti-

lisant sa créativité (Bhaskar, 1998), en accord avec la démarche abductive (Avenier, Parmentier et Cajaiba, 2012). C'est dans cette approche que la méthodologie des entretiens et de l'encodage des données, qui ont permis de bâtir le processus de recherche, seront expliqués, dans le respect cependant de la nécessaire prévenance due à la nature de la profession des sujets entendus et à la sensibilité de leurs cadres d'emploi. C'est également la raison pour laquelle les prochains chapitres présenteront des verbatim, issus des matériaux bruts, et leurs interprétations adossées aux constructions théoriques qui ont permis l'élaboration du développement progressif de l'abstraction.

Enfin, Pierce (1958) explique que l'abduction est le rapprochement entre le fait surprenant observé avec quelque chose de différent. Pour Dumez (2012), la pensée de Pierce pourrait alors être rapprochée de la répétition d'éléments provenant de différentes sources appuyant le raisonnement. Ainsi, la validité d'une proposition serait d'autant plus probante qu'elle serait corroborée par des observations consécutives au fait surprenant initial et aux différentes sources recueillies par le chercheur.

3 . Méthodologie

Cette partie sur la méthodologie présente une synthèse où sont explicitées les caractéristiques principales de la méthodologie en terme générique d'abord puis dans les particularités propres à chaque vague d'entretiens menée. Ces caractéristiques sont néanmoins reprises dans les articles qui, ayant fait l'objet de publication, devaient obéir à une cohérence propre.

3.1 Méthodologie générale

Ce travail prend appui sur deux vagues d'entretiens, la seconde vague ayant été divisée en deux phases. Si la méthode générale était similaire est clairement ancrée dans une approche qualitative dans les deux vagues ainsi que dans les deux phases de la seconde vague, certaines différences substantielles nécessitent d'être explicité en détail.

La première vague a été développée dans le chapitre 1. Il s'agissait d'entretiens exploratoires qui ont été menés à visée d'analyses et d'audits militaires. Ces entretiens ont été à l'origine de la motivation de l'auteur pour pousser la recherche plus avant dans le cadre d'un travail de thèse en sciences de gestion et de ressources humaines.

La première phase de la seconde vague d'entretiens est, quant à elle, le produit d'un désir de pousser la réflexion plus avant dans le cadre d'une recherche organisée sous forme de thèse. À cette fin, les entretiens ont été pensés à partir d'une grille de questions fondées sur une base théorique analysée en amont.

De manière générale, un tableau a été conçu afin de reprendre, en ordonnée, les propositions issues des problématiques à même d'expliquer le fait surprenant et de les soumettre, et en abscisse, les différentes sources trouvées (entretiens, documents, etc.) ayant permis de valider ou d'invalider les propositions. On aura alors cherché à valider les propositions par un ensemble de sources, la lettre « V » correspondant à la validation de la proposition par une source du type spécifié, « NV » signifiant que la source n'a pas permis la validation de la proposition.

Ainsi, à titre d'exemple, on observe que les quatre premières propositions sont largement validées alors que les autres le sont moins nettement. Il en découle que ces dernières pourraient légitimement faire l'objet de recherches ultérieures.

La seconde phase de la seconde vague d'entretiens s'est structurée autour d'une base de questions similaires, mais a permis d'ajouter une observation dirigée systématique qui aura servi à finaliser la validation des propositions.

Chaque chapitre amènera des éléments de démonstration et des exemples pour montrer que la source de donnée valide la proposition, que ce soit par l'intermédiaire de verbatim, d'extractions issues de l'analyse sémantique réalisée avec le logiciel Nvivo, de traitement statistique issu des déclarations, ou encore des résultats de la soumission à l'aveugle de verbatim ciblés en fonction du sujet à un groupe de personne servant de contrôle. Cette méthode ayant amené à la validation de propositions sera mise en avant dans l'introduction de chaque chapitre au travers la présentation d'un tableau reprenant la nature des sources (observations, entretiens ou documents) ayant permis de valider la proposition.

3.2. Contexte de la seconde vague d'entretiens

Les premiers entretiens exploratoires ont fait l'objet d'un article initial qui a permis de présenter le contexte dans lequel les données ont été collectées, ainsi que la méthodologie utilisée à cette fin. À noter que ces entretiens ont été menés à la suite d'observations de terrain et non à la lumière du cadre théorique, à la différence des entretiens des deux phases de la seconde vague. Ces premières interviews exploratoires ont permis de procéder à une recherche théorique et de faire émerger des propositions. Les résultats obtenus ainsi que les problématiques qui en découlaient ont été présentés à la Direction des Ressources Humaines de l'Armée de Terre (DRH-AT), dans l'objectif d'obtenir les autorisations nécessaires au déroulement d'une seconde vague d'entretiens exploratoires

nécessaires à la poursuite de la recherche, étant entendu que les expérimentations menées en Ukraine pouvaient être le prélude à des opérations similaires menées en Occident. En outre, s'il était possible de cibler une autre organisation évoluant en situations extrêmes, les premiers entretiens exploratoires permettaient déjà l'identification de profils supposés particulièrement sensibles dans le cadre précis des structures militaires.

Enfin, pour des raisons évidentes de sécurité, il était préférable de demander ces autorisations à l'armée française plutôt qu'à une armée tierce pour laquelle mon statut d'étrangère aurait représenté un obstacle majeur pour la délivrance d'habilitation de sécurité. Après plusieurs rendez-vous avec le Général Hervé Wattecamps, la DRH-AT a accordé sa confiance à ce projet et autorisa la réalisation des entretiens envisagés.

Afin de pouvoir travailler dans un climat de confiance et de pouvoir avoir des entretiens francs avec les militaires entendus, il a été possible de leur assurer un anonymat complet et de ne pas avoir à transmettre la retranscription des entretiens. En contrepartie, les éléments recueillis ne devaient pas être communiqués à l'extérieur. Cependant, l'obtention des habilitations comprenant une enquête de sécurité relativement longue, la seconde vague d'entretiens n'a pu être réalisée que 15 mois après la première[19].

À la suite de l'analyse de la première phase d'interviews, il a été décidé de procéder à une seconde phase d'entretiens exploratoires. Ces entretiens bénéficieraient de la même grille d'entretien que la première phase afin de ne pas corrompre les données.

Ce travail a ensuite fait l'objet d'un retour à la DRH-AT, alors même que le directeur avait changé suite aux nouvelles affectations de l'été ; le Général Wattecamps ayant été remplacé par le Général Hingray.

[19]La première vague d'entretiens s'est tenu en mai 2018, et à fait l'objet d'un compte rendu au DRH-AT en juillet.

3.3- Traitements ou des outils d'analyse mobilisés dans la première phase de la seconde vague d'entretiens

La première vague d'entretiens a eu lieu au printemps 2018. Elle a porté sur des personnels disposant majoritairement d'une expérience forte en situation extrême, âgés de 23 à 44 ans. Il avait également été demandé de pouvoir entendre des personnels n'ayant pas été confrontés à des situations extrêmes, ce qui impliquait un âge moyen plus faible, les hommes engagés ayant vocation à être envoyés en situation extrême dès leur formation parfaitement complétée et achevée. La première phase de la seconde vague d'entretiens a sollicité des personnels appartenant à différents groupes, mais homogènes s'agissant de leurs missions et de leurs expériences afin de ne pas altérer les résultats de la recherche. Les autorisations ont été données aux chefs de corps, et le contact a été pris avec eux afin d'organiser les entretiens. Pour ce faire, les profils recherchés ont été transmis aux chefs de corps afin qu'ils puissent sélectionner des personnels. Par souci de transparence, une trame globale des thèmes abordés leur a aussi été fournie. Il leur a également été précisé qu'en accord avec la DRH-AT, aucun compte rendu ne leur serait transmis sur les dires de leurs hommes.

Les militaires correspondant aux profils recherchés ont été informés par leur hiérarchie de la venue du chercheur et de la nature générique du travail poursuivi avant qu'un appel à volontaire ne soit réalisé. La nature même de la recherche n'a pas été clairement définie auprès des candidats, elle est restée floue à dessein afin de ne pas influencer les personnes appelées à être entendues et à composer le corpus de données analysées ce qui aurait corrompu les données collectées. Une fois dans les unités, le chercheur était présenté aux militaires par leur hiérarchie, ils étaient alors encouragés à parler en toute

liberté et confiance. Avant chaque entretien, le chercheur informait les sujets de l'étude qu'un anonymat complet leur était garanti, et qu'aucune donnée issue des entretiens ne serait transmise à qui que ce soit, que seule l'analyse de l'ensemble serait l'objet d'un retour auprès de la seule DRH-AT. Ce point a été d'une importance cruciale pour nombre de soldats qui s'en sont réassurés plusieurs fois au cours de l'entretien.

Là encore, comme pour la première vague, les entretiens se sont déroulés sous forme semi-directive, en tête-à-tête. Des questions récurrentes étaient posées (notamment pour obtenir des données chiffrées), et les thèmes forts de la recherche étaient systématiquement abordés (tableau 2). Néanmoins, les personnels entendus étaient libres de développer un point ou un autre, en s'appuyant sur des exemples s'ils le souhaitaient, ou, au contraire, de s'abstenir de répondre à certaines questions.

Nous tenons ici à insister sur le fait que tous furent particulièrement coopératifs. Les entretiens avaient vocation à prendre la forme d'un échange libre, les militaires entendus pouvant aussi poser des questions au chercheur. Il était néanmoins précisé que certaines questions ne seraient traitées par le chercheur qu'à la fin de l'entretien pour ne pas altérer les réponses que les interviewés pourraient faire suite à ces réponses. De même, les personnels entendus quittaient le site où avait eu lieu leur entretien sans être mis en contact avec les autres volontaires, et en ayant pris l'engagement ne communiquer avec leurs collègues devant être entendus qu'une fois que tous les entretiens seraient terminés. Cette mesure a été mise en place afin de ne pas corrompre les données collectées.

La première phase de la seconde vague représente un ensemble de 17 personnels, tous masculins. Trois ne disposaient pas d'expérience en situation extrême. La durée des en-

tretiens était comprise entre 45 minutes et 2 h 15. Tous ont été enregistrés, puis retranscrits et traités avec un encodage réalisé avec Nvivo 13.2. Sur la base ces données et analyses qualitatives, un travail permettant de quantifier les données obtenues a été réalisé.

Concernant l'encodage par Nvivo, les entretiens transcrits ont été analysés à la lueur du cadre théorique mobilisé. Ainsi, les champs de la confiance ont notamment été traités. Concernant la confiance, différents champs ont été interrogés : hiérarchiques, bien entendu, mais également la confiance accordée aux médias.

Chacun de ces axes a été subdivisé en « positif » ou « négatif ». Enfin, une granularité plus fine a été mise en œuvre quand la raison de cette confiance ou défiance était développée par les sujets entendus, notamment quand elle s'appuyait sur des valeurs. Les raisons de l'engagement et du réengagement ont également été encodées, en « positif » ou en « négatif ». Les réponses relatives aux questions posées sur les dernières informations ayant fait réagir les personnes auditionnées ont également été encodées quant à la raison profonde de la réaction.

Des caractéristiques ont également été attribuées aux interviewés, notamment l'âge, le grade, le temps passé en opérations extérieures et le temps passé quotidiennement sur Internet.

À titre d'exemple, des phrases comme « *si c'était à refaire, je ferais tout pareil, je ne changerais rien* » ont été encodées dans « *réengagement -> positif* », alors que « *j'ai hâte de partir, je suis fatigué, j'en peux plus de les voir faire n'importe quoi avec nous… la seule chose qui me ferait changer, peut-être, ce serait un peu plus de considération… on n'est pas considéré… et la paie aussi* » a été relié au nœud « *réengagement -> négatif »* pour la première partie, puis à *réengagement -> négatif ->manque considération/*

respect pour la seconde partie. Autre exemple, une citation comme *« le groupe, oui on bosse avec les gars, mais après est-ce que je leur fais confiance ? Je ne dirais pas… Non. En même temps est-ce qu'on peut jamais faire confiance à quelqu'un ? Mais non je dirais pas confiance, je sais qu'ils vont faire le boulot, mais c'est tout* » a été encodée à : *confiance groupe -> négative*. De même, un encodage a été créé pour les personnels estimant que leurs valeurs professionnelles et personnelles étaient entremêlées et indissociables ou a contrario qu'elles divergeaient afin de pouvoir procéder au plus grand nombre de requêtes exploratoires possible.

Axes abordés dans les entretiens

Axes abordés :

- Positionnement des sujets (âge, grade, spécialité, temps passé en opération extérieure [OPEX], temps d'engagement, blessures, situation familiale, background professionnel) ;

– Raison de l'engagement, perception de celui-ci ;

– Nature de la confiance/défiance dans le groupe. Évolution de la confiance dans le temps, développement de raisons à l'origine de cette évolution ;

- Question sur les valeurs. Valeurs professionnelles sont-elles différentes des valeurs personnelles ? Utilité ? Raison de la foi en ces valeurs…
- Nature de la confiance/défiance dans l'institution. Évolution de la confiance dans le temps, développement de raisons à l'origine de cette évolution, sur quoi repose-t-elle, etc. Lien avec les valeurs
- Nature de la confiance/défiance dans le gouvernement. Évolution de la confiance dans le temps, développement de raisons à l'origine de cette évolution, lien avec les valeurs ;
- Raison de la confiance/défiance dans les différents médias (mainstream, alternatifs, réseaux sociaux, broadcast) médias. Évolution de la confiance dans le temps, développement de raisons à l'origine de cette évolution , lien avec les valeurs;
- Nature de la recherche dans les informations (quels objectifs, quelles attentes, quelles méthodes utilisées par les sujets) ;
- Mise en situation d'influence par l'intermédiaire d'« informations » ou de contenus
- Position face à un réengagement. Position face au choix initial de carrière (satisfaction regret), raison de ce sentiment. Quels éléments pourraient modifier cette perception (en bien ou en mal)…
- Dernières informations ou contenus ayant provoqué une réaction (positive et négatives) et pourquoi ;
- Perception d'être une cible, et raisons de la réponse ;

Questions dirigées

- Demande de cotation de la confiance dans le groupe ;
- Demande de cotation de la confiance dans l'institution ;
- Demande de cotation dans le gouvernement ;
- Demande de cotation dans les médias *mainstream ;*
- Demande de cotation de confiance dans les médias alternatifs ;
- Demande de cotation de confiance dans les réseaux sociaux ;
- Demande si le point de vue et/ou la confiance dans les structures gouvernementales et institutionnelles ont changé suite à des informations vues ou lues ;
- Temps passé sur Internet par jour

Tableau 2 : synopsis des entretiens de la première phase, vague 2

Concernant l'analyse quantitative, les données récoltées pendant les entretiens ont été ensuite codifiées afin de pouvoir être exploitées. Ainsi les réponses positives ont été traitées par « 1 » et négatives par « 0 ». Les données en temps ont été rapportées en mois, etc.

Enfin, afin de fiabiliser les notes déclarées par les intervenants concernant le degré de confiance qu'ils accordaient aux trois niveaux de l'organisation (à savoir le groupe, l'institution et le gouvernement), un groupe de 5 personnes servant de contrôle a été composé. Les verbatim relatifs à ces trois niveaux de confiance ont été présentés à l'aveugle à ce groupe qui avait pour mission de noter la confiance du narrateur envers les niveaux visés sur la même échelle de Likert à 5 degrés. Ce groupe était composé de personnes entre 19 et 62 ans, trois hommes et deux femmes afin de permettre une ventilation harmonieuse et d'éviter des biais dus à un profil socioprofessionnel particulier ou à une classe d'âge. Les membres du groupe n'ont pas pu consulter les estimations données par leurs collègues afin que leurs appréciations ne puissent pas être influencées. Les résultats de ce groupe ont été confrontés aux notes déclarées par les sujets de la recherche.

3.4 – Traitements ou des outils d'analyse mobilisés dans la seconde phase de la seconde vague d'entretiens

La seconde phase de la seconde vague d'entretiens a été décidée par l'armée de terre. Néanmoins, et pour la cohérence de la recherche, les profils choisis étaient comparables à ceux ciblés dans la phase 1, tant en âge qu'en exposition aux situations extrêmes ou au niveau de

responsabilité. Seule la spécialité professionnelle différait. Cette seconde phase était composée de 21 sujets, tous issus de l'appel à volontaires réalisé par la hiérarchie. La mise en œuvre et la présentation du chercheur ont suivi le même mécanisme que dans la phase 1, à savoir une présentation de l'objet de la recherche aux hommes répondant aux profils demandés au sein de différents groupes. Les volontaires se sont ensuite manifestés et les dates d'entretiens ont été planifiées en accord avec leur hiérarchie.

De même que dans la phase 1, ces entretiens portaient exclusivement sur des hommes. Cela dit, il convient de rappeler qu'il ne s'agissait là nullement d'un choix de l'organisation ou du chercheur, mais d'un simple reflet de la composition de la structure. En effet, le bilan social de l'armée de terre française de 2017 fait état d'un taux de féminisation de 15,5 % concernant les personnels militaires. Il était donc logique que le pourcentage de femmes soit particulièrement faible d'autant plus que le public cible de cette étude était composé de personnels militaires ayant une expérience forte en situations extrêmes.

La méthodologie appliquée fut strictement la même que pour la première phase afin de ne pas fausser les résultats obtenus grâce à ce corpus (tableau 3). Néanmoins, comparativement à la première phase, les 21 sujets disposaient d'un vécu fort en situations extrêmes, aucun ne disposait d'aucune expérience en la matière à l'image des 3 sujets entendus lors de la phase 1.

Cependant, une différence majeure a été introduite lors des entretiens. Suite à l'analyse de la première phase, une expérimentation a été mise en œuvre afin de vérifier une des propositions formulées. À ce titre, un « fake » a été imaginé afin de tester les réactions des personnes entendues dans le cas où leurs valeurs principales seraient ciblées afin de générer une éventuelle altération de la confiance. Pour ce faire, un screen d'une page de Facebook a été composé. Y apparaissait une communication d'un prétendu groupe de militaires. Ce groupe « forwardait » une publicité pour le recrutement composé par le SIRPA (département chargé de la communi-

cation au ministère des armées) de l'armée de terre. Ces publicités bien connues des militaires représentent des instants forts de la vie de soldats, avec une mise en scène très flatteuse, des images léchées et élégantes, et la mise en scène de matériel de dernière génération parfaitement neuf. Le supposé groupe avait ajouté un commentaire cynique : « Jolie publicité, dommage que le militaire qui a alerté sur l'état réel du matériel sur le terrain est actuellement sous sanctions disciplinaires ». Ce fake visait les valeurs principales du métier de militaire à savoir l'honnêteté (de la réponse du militaire), la justice (ici un traitement injuste : le militaire a juste dit la vérité), et le professionnalisme (alerter sur du matériel défectueux permet de le remplacer afin de pouvoir effectuer la mission au mieux). Enfin, cette situation fait appel à une expérience empirique : les militaires comme tous les professionnels, ont eu à un moment ou à un autre de leur carrière à travailler avec du matériel dont l'état ne correspondait pas parfaitement à leurs attentes. En revanche, tout militaire de carrière sait qu'une mise sous sanction pour la simple mention d'un état matériel moyen, voire mauvais, est hautement improbable, voire grotesque.

Ce fake était présenté après 45 à 55 minutes d'entretiens en fonction des cas, après que les personnels aient été interrogés sur leur confiance dans les différents médias, notamment les réseaux sociaux, et qu'ils aient noté cette confiance en la justifiant. Il leur avait aussi été demandé s'ils avaient suivi les formations de sensibilisation aux risques induits par Internet, y compris par les réseaux sociaux, question à laquelle tous ont répondu par l'affirmative. Après quelques échanges de transition, le chercheur leur disait avoir vu passer une publication récemment, et dans la perspective des entretiens, un screenshot en avait été fait sur lequel elle aimerait avoir leur sentiment. Il leur était précisé que la source n'avait pas du tout été vérifiée, pas plus qu'aucun des éléments présents sur le screenshot. Notons ici que l'expérimentation menée suivait un protocole pensé en adéquation avec les propositions soutenues de manière à

les valider avec suffisamment de stabilité pour être exploitables. Néanmoins, nous ne disposions pas des conditions d'un laboratoire. Au demeurant, il est fort possible que le seul fait de réaliser cette expérimentation en laboratoire (qu'il conviendrait donc mieux de qualifier d'observation dirigée) aurait probablement faussé les résultats étant entendu la spécificité des sujets interrogés. En effet, la désirabilité sociale ressentie par les personnes interrogées, ajoutée à un environnement de laboratoire, aurait probablement inhibé les réactions.

L'ensemble des résultats a été encodé sur les mêmes bases que ceux de la première phase des entretiens, que ce soit d'un point de vue qualitatif ou quantitatif. Les résultats de l'expérimentation ont fait l'objet d'un traitement qualitatif (notamment concernant les raisons données à la réaction), mais aussi quantitatif (afin de pouvoir tester des corrélations entre variables).

Axes abordés dans les entretiens

Axes abordés :

- Positionnement des sujets (âge, grade, spécialité, temps passé en opération extérieure [OPEX], temps d'engagement, blessures, situation familiale, background professionnel) ;

– Raison de l'engagement, perception de celui-ci ;

– Nature de la confiance/défiance dans le groupe. Évolution de la confiance dans le temps, développement de raisons à l'origine de cette évolution ;

- Question sur les valeurs. Valeurs professionnelles sont-elles différentes des valeurs personnelles ? Utilité ? Raison de la foi en ces valeurs ;
- Nature de la confiance/défiance dans l'institution. Évolution de la confiance dans le temps, développement de raisons à l'origine de cette évolution, sur quoi repose-t-elle, etc. Lien avec les valeurs.
- Nature de la confiance/défiance dans le gouvernement. Évolution de la confiance dans le temps, développement de raisons à l'origine de cette évolution, lien avec les valeurs ;
- Raison de la confiance/défiance dans les différents médias (mainstream, alternatifs, réseaux sociaux, broadcast) médias. Évolution de la confiance dans le temps, développement de raisons à l'origine de cette évolution, lien avec les valeurs ;
- Nature de la recherche dans les informations (quels objectifs, quelles attentes, quelles méthodes de recherche mobilisées par les sujets) ;
- Mise en situation d'influence par l'intermédiaire d'« informations » ou de contenus
- Position face à un réengagement. Position face au choix initial de carrière (satisfaction regret), raison de ce sentiment. Quels éléments pourraient modifier cette perception (en bien ou en mal) ;
- Dernières informations ou contenus ayant provoqué une réaction (positive et négatives) et pourquoi ;
- Perception d'être une cible, et raisons de la réponse.

Questions dirigées

- Demande de cotation de la confiance dans le groupe ;
- Demande de cotation de la confiance dans l'institution ;
- Demande de cotation dans le gouvernement ;
- Demande de cotation dans les médias *mainstream ;*
- Demande de cotation de confiance dans les médias alternatifs ;
- Demande de cotation de confiance dans les réseaux sociaux ;
- Demande si le point de vue et/ou la confiance dans les structures gouvernementales et institutionnelles ont changé suite à des informations vues ou lues ;
- Temps passé sur Internet par jour.

Observation dirigée

Tableau 3 : synopsis des entretiens de la seconde phase, vague 2

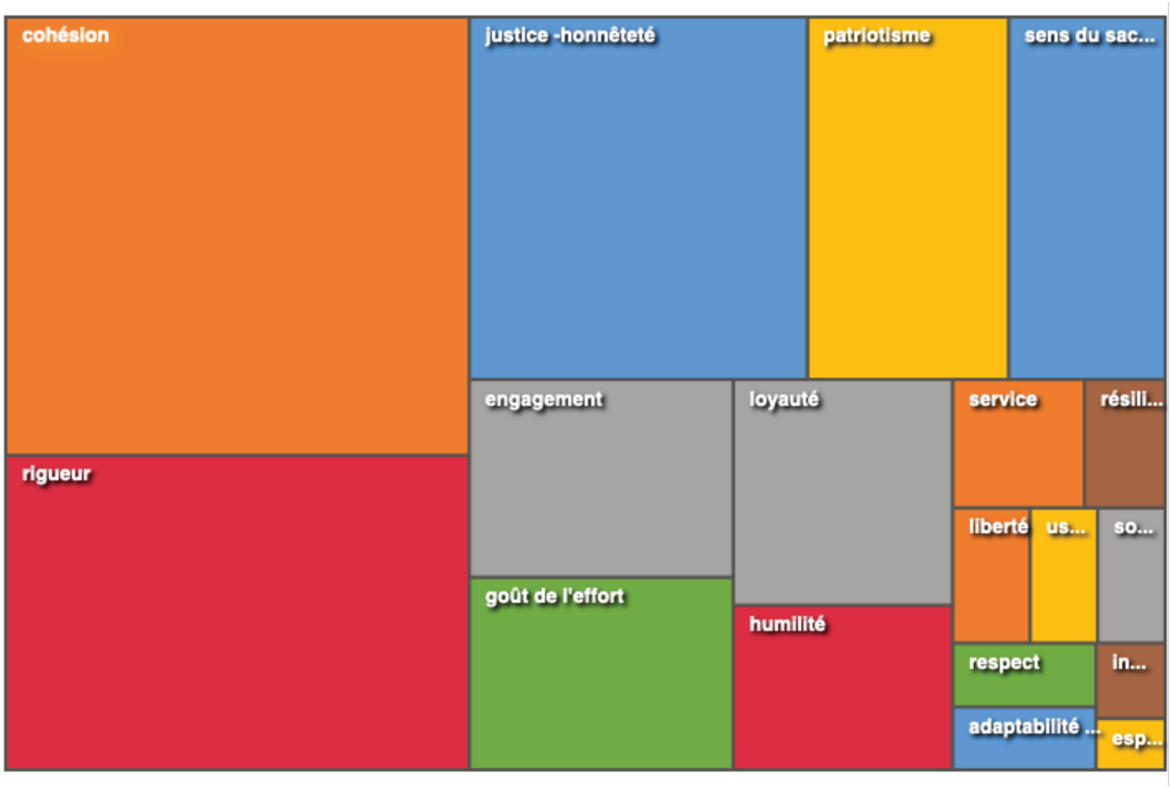
3.5- Outillage technique pour exploiter ces entretiens

La retranscription des entretiens a abouti à une masse importante de données de plus de 400 pages de données. C'est alors posé la question de la méthode et de l'outil à utiliser pour effectuer l'encodage le plus efficace, permettant l'analyse qualitative informatisée la plus adaptée. Plusieurs logiciels sont couramment utilisés dans les recherches qualitatives afin de permettre de procéder à un encodage efficace. L'objectif étant de faire émerger le sens, de pouvoir analyser un document à la lumière des questions suivantes : « quel est le sujet dans ce document, de quoi parle-t-on ? » ; « Que dit la personne écoutée ? ». Ces interrogations permanentes permettent ensuite de dégager les grandes idées des documents analysés, et, ce faisant, de mieux en dégager le sens. Dans le cas présent, un travail de recherche ayant été effectué préalablement et des propositions formulées, il s'agissait de pouvoir rattacher les éléments collectés aux idées maîtresses de ces propositions afin de les valider ou de les invalider. Appuyée sur une analyse thématique, cette approche est particulièrement adaptée à l'utilisation du logiciel Nvivo qui permet un encodage rapide et intuitif, aidant à mettre en lumière le sens des propos tenus par les différents intervenants. En outre, Nvivo permet de faire ressortir les récurrences liées à une thématique, ce qui facilite la validation des propositions faites, voire, aide à qualifier des résultats quantitatifs comme cela a été mis en œuvre dans le chapitre 5 et 6. En outre, Nvivo permet de procéder à une « décontextualisation » des données collectées lors d'un entretien, en le découpant par unité de sens et non plus par suite chronologique et contextuelle (Tesch, 1990).

Exemple d'un encodage sur le nœud : valeur -> adaptabilité/rusticité ». Il apparaît que peu d'éléments s'y rapportent. (Pour des raisons de confidentialité, les extraits de textes sont systématiquement obscurcis).

De plus, l'utilisation de ce logiciel autorise à un encodage qualifiable de riche. En d'autres termes, il est possible de rattacher un extrait à plusieurs nœuds ce qui permettra alors une analyse en profondeur. Par exemple, si une des valeurs est dans la même citation associée à une confiance forte dans le groupe, elle pourra être attachée aux différents nœuds *« valeur x »* et « *confiance* ». Enfin, il est également possible de procéder à des croisements, à l'analyse d'intersections entre plusieurs nœuds.

En outre, Nvivo permettait de réaliser un traitement graphique du codage particulièrement utile dans le cas présent.



Exemple d'un graphique reprenant le nombre d'encodages par valeur qui a été utilisé dans le chapitre 6 de ce travail.

Cette thèse est originale de par sa forme qui s'appuie sur la présentation d'essais publiés, présentés ou en cours d'évaluation dans des revues ou des colloques. En effet, cette structure est peu fréquente en dehors des champs de la finance ou du marketing. Si cette présentation a été préférée à une structure plus classique, c'est qu'elle traduit le parcours de recherche suivi, et plus particulièrement l'engagement dans un processus de recherche entrepris après avoir déjà mené plusieurs investigations de terrain. C'est pourquoi il est logique de retrouver dans les chapitres suivants, des tableaux, des éléments d'analyse ou des commentaires faits dans ce chapitre qui avaient pour vocation de proposer une présentation plus développée des aspects conceptuels et méthodologiques que l'on ne peut raisonnablement faire dans le nombre limité de pages autorisé pour un article de revue ou de communication.

Références

Aliseda Atocha (2006) “What is abduction? Overview and Proposal for Investigation” in Aliseda Atocha Abductive Resaoning. Logical Investigation into Dicovery and Explanation, Dordrecht, Springer, Synthese Library, Studies in Epistemology, Logic, Methodology, and philosophy of Science, vol. 330, Chapter 2, pp. 27-50.

Aubry, Monique, Lièvre, Pascal and Hobbs, Brian. 2010. “Project Management in Extreme Environments.” *Project Management Journal,* 41, 3, 2-3. https://doi.org/10.1002/pmj.20185.

Bechky, Beth A., and Okhuysen, Gerardo A.. 2011. “Expecting the Unexpected? How Swat Officers and Film Crews Handle Surprises.” *Academy of Management Journal,* 54 (2): 239–61. https://doi.org/10.5465/AMJ.2011.60263060.

Bouty, Isabelle; Godé, Cécile, Drucker-Godard, Carole; Lièvre Pascal, Nizet Jean, and Pichault François. 2012. “Coordination Practices in Extreme Situations.” *European Management Journal,* 30 (6): 475–89. https://doi.org/10.1016/j.emj.2012.03.015.

Carroll, John S., Rudolph, Jenny W. ; and Hatakenaka, Sachi. 2002. “Learning from Experience in High-Hazard Organizations.” *Research in Organizational Behavior,* 24 (January): 87–137. https://doi.org/10.1016/s0191-3085(02)24004-6.

Cowan, David, and Cook, Chaveso. 2018. “What’s in a Name? Psychological Operations versus Military Information Support Operations and an Analysis of Organizational Change.” *MilitaryReview.* Online exclusive article, mars 2018.

Christianson, Marlys K., Farkas, Maria T. ; Sutcliffe, Kathleen M. and Weick, Karl E.. 2009. “Learning through Rare Events: Significant Interruptions at the Baltimore & Ohio Railroad Museum.” *Organization Science,* 20 (5): 846–60. https://doi.org/10.1287/orsc.1080.0389.

Clegg, Stewart R.; Cunha, Miguel Pina , and Kamoche, Ken. 2006. “Surprises in Management and Organization: Concept, Sources and A Typology.” *British Journal of Management,* 17 (4): 317–29. https://doi.org/10.1111/j.1467-8551.2005.00470.x.

David Albert. 1999. “Logique, Épistémologie et Méthodologie En Sciences de Gestion.” dans Actes de La VIIIe Conférence de l’Association Internationale de Management Stratégique, edited by AIMS. Chatenay-Malabry, mai 1999.

Dubois, Anna, and Lars Erik Gadde. 2002. “Systematic Combining: An Abductive Approach to Case Research.” *Journal of Business Research,* 55 (7): 553–60. https://doi.org/10.1016/S0148-2963(00)00195-8.

Galeotti Mark. 2018. “’I’m Sorry for Creating the ’Guerassimov Doctrine’.” *Foreign Policy,* March 5th, 2018.

Galeotti, Mark. 2016. “Hybrid, Ambiguous, and Non-Linear? How New Is Russia’s ‘New Way of War’?” *Small Wars and Insurgencies,* 27 (2): 282–301. https://doi.org/10.1080/09592318.2015.1129170.

Barney, Glaser, and Strauss Anselm. (1967). *The Discovery of Grounded Theory*. Adline. Chicago.

Godé, Cécile. 2011. “Construire Le Sens Par Le Retour d’expérience : Le Cas de l’Equipe de Voltige de l’Armée de l’air.” *Management & Avenir,* 41 (1): 416. https://doi.org/10.3917/mav.041.0416.

Godé, Cécile. (2015). *La Coordination Des Équipes En Environnement Extrême*. Londres, ISTE Éditions. 2015.

Godé, Cécile. (2015). *Team Coordination in Extreme Environments: Work Practices and Technological Uses Under Uncertainty*. Wiley and son, London. 2015.

Godé, Cécile, and Lebraty., Jean-Fabrice. 2015. “Experience Feedback as an Enabler of Coordination: An Aerobatic Military Team Case.” *Scandinavian Journal of Management,* 31 (3): 424–36. https://doi.org/10.1016/j.scaman.2015.02.002.

Gray, Colin. (2015). *The futur of strategy.* Polity, Cambridge, 2015.

Guerassimov, Valeryi. 2013. “Ценность Науки в Предвидении,.” February 26, 2013, *VPK.-News.*

Hällgren, Markus, Rouleau, Linda and De Rond, Mark. 2018. “A Matter of Life or Death: How Extreme Context Research Matters for Management and Organization Studies.” *Academy of Management Annals,* 12 (1): 111–53. https://doi.org/10.5465/annals.2016.0017.

Hartshorne, Charles, Paul Weiss, Arthur W. Burks, and Charles Sanders Peirce. (1931). *The Collected Papers of Charles Sanders Peirce.* Harvard University Press, Harvard, 1931.

Hoffmann, Franck G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac institute for Policy Study, Arlington, 2007.

Hoffman, Frank. 2015. “The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War.” *Index of US Military Strength*, no. 1991: 25–36.

Kahneman, Daniel., & Tversky, Amos. (1982). Intuitive Prediction: Biases and Corrective Procedures. https://doi.org/10.1017/CBO9780511809477.031

Kahneman, D., & Tversky, A. (1982). The Simulation Heuristic. https://doi.org/10.1017/CBO9780511809477.015

Kennan, George F. 1948. ’The Inauguration of Organized Political Warfare' [Redacted Version],” April 30, 1948, History and Public Policy Program Digital Archive, Redacted final draft of a memorandum dated May 4, 1948, and published with additional redactions as document 269, 'FRUS, Emergence of the Intelligence Establishment.'

Martinet Alain-Charles, and Pesqueux Yvon. (2013). *Grandes Questions Épistémologiques et Sciences de Gestion. Épistémologie et Sciences de Gestion*. Vuibert, Paris, 2013.

Ministère de la Défense. 2018. “Bilan Social de l’année 2017.” Paris.

Pierce Charles Sanders. (2006). Ecrits Logiques, Oeuvres Philosophiques. Volume 3. Cerf. Paris 2006.

Perrow, Charles. 1994. “The Limits of Safety: The Enhancement of a Theory of Accidents.” *Journal of Contingencies and Crisis Management,* 2 (4): 212—20. https://doi.org/10.1111/j.1468-5973.1994.tb00046.x.

Roux-Dufort, Christophe, and Sanjy Ramboatiana. 2008. “Crise et Sentiment, Le Cycle d’incompétence Habile.” *L’Expansion Management Review,* N° 128 (1): 120. https://doi.org/10.3917/emr.128.0120.

Shrivastava, Paul, Ian I. Mitroff, Danny Miller, and Anil Miclani. 1988. “Understanding industrial crisis.” *Journal of Management Studies,* 25 (4): 285–303. https://doi.org/10.1111/j.1467-6486.1988.tb00038.x.

Taleb Nassim Nicholas. (2007). *The Black Swan: The Impact of the Highly Improbable.* Penguin,Westminster, re-Issue 2006.

Tesch, Renata. (1990) *Qualitative Analysis Programs Basic Structures and Functions*. London, Falmer, 1990. https://doi.org/10.4324/9781315067339.

Tsoukas, Haridimos. (2005). *Complex Knowledge: Studies in Organizational Epistemology. Management Learning.* Oxford University Press, Oxford, 2005. https://doi.org/10.1108/00220410710759048.

Van Puyvelde, Damien. 2015. “Hybrid War — Does It Even Exist?” *NATO Review Magazine*, 2015–17.

Weick, Karl E. 1993. “The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster.” *Administrative Science Quarterly,* 38 (4): 628. https://doi.org/10.2307/2393339.

Weick, Karl E., and Kathleen M. Sutcliffe. 2006. “Mindfulness and the Quality of Organizational Attention.” *Organization Science,* 17 (4): 514—24. https://doi.org/10.1287/orsc.1060.0196.

CHAPITRE 3 : Confiance, altération de la confiance et rationalité de la prise de décision

Le constat résultant des premières observations menées en Ukraine montrait des actions visant les militaires. Cependant, ces constatations appelaient un travail plus en profondeur s'agissant des doctrines mises en œuvre dans l'objectif de militariser Internet, notamment dans le cadre d'opérations psychologiques. C'est cette approche, tournée vers l'utilisation de l'outil Internet en lien avec la pensée militaire, notamment russe, qui sera présentée en partie I de ce chapitre au travers un article publié au Journal of intelligence and cyber security en juin 2019.

L'examen de ces attaques psychologiques fondées sur l'utilisation d'Internet et visant la confiance amène naturellement à les analyser et à en mesurer les impacts d'un point de vue managérial. C'est cet axe de la problématique qui sera abordé dans la partie II de ce chapitre, au travers l'analyse de la référence de confiance comme cadre d'action en situation extrême. Cette analyse est le produit d'une communication présentée lors des seizièmes journées de la collaboration scientifique entre les Écoles doctorales en gestion de l'Université de Paris I-Panthéon - Sorbonne et de l'Université Libre de Bruxelles qui se sont tenues en mars 2019.

En termes méthodologiques, ce chapitre s'attache à valider ou invalider plusieurs propositions relatives à deux des sous-problématiques abordées dans ce travail à savoir l'altération de la confiance et prise de décision et la perméabilité aux informations divergentes de celles délivrées par l'organisation en s'appuyant sur diverses sources de données comme précisées dans le tableau proposé ci-dessous.

Si deux publications ont été regroupées dans ce chapitre, c'est parce que le travail de recherche a débouché sur deux types de développements intimement liés. À ce titre, la première publication s'inscrit dans le prolongement de celle présentée en chapitre I. Cependant, si le chapitre 1 présente des propositions globales et analyse la réaction des sujets interrogés hors con-

texte de recherche, la publication présentée ici s'intéresse à l'inscription des problématiques soulevées dans le cadre des dernières stratégies militaires et à la lumière des théories développées par Kahneman et Tversky. Ainsi, un travail de clarification des termes employés a été mené, participant ainsi à définir la nature précise des actions menées sur le champ de l'information. Cette définition est suffisamment délicate pour être encore matière à controverses dans le champ de la stratégie militaire. En outre, cet article met en perspective les théories développées, notamment par des membres de l'armée de la Fédération de Russie, avec les actions et effets observés sur le terrain. Dans un second temps, il les met en perspective avec les modèles théoriques se rapportant au choix rationnel qui, apportant un nouvel éclairage sur cette problématique, devient un sujet crucial pour les armées du monde entier. L'importance prise par ce sujet tient, notamment, à ce qu'il peut altérer l'action appelée à être menée dans une situation extrême. De plus, les armées occidentales fondent la fiabilité de la prise de décision sur le triptyque confiance - cohésion - performance, aussi s'interroger sur la référence de la confiance comme cadre d'action en situation extrême apparaissait primordial. C'est l'objet de la communication qui est présenté dans la partie II de ce chapitre, et qui découlait directement des conclusions explicitées dans l'article présenté en première partie de ce chapitre. Enfn, en matière de méthodologie, ce chapitre permet de tester des propositions lien avec les sous-problématiques de l'altération de la confiance et prise de décision, et de la perméabilité des cibles aux informations divergentes de celles délivrées par leur organisation. Ces deux volets découlant de la question principale de recherche principale, à savoir dans un contexte de situations extrêmes soumis à une très forte pression de facteurs externes, en quoi la diffusion de certaines informations et le canal utilisé sont de nature à ne pas exécuter l'ordre ou les décisions de la hiérarchie. Le tableau ci-dessous présente les différentes sources de données qu'il s'agisse des entretiens, d'observations ou d'analyse de documents, qui auront ou n'au-

ront pas permis de valider (V pour validé, NV pour non validé) les propositions inhérentes à ces problématiques et questions de recherche.

Question de recherche	**Dans un contexte de situations extrêmes soumis à une très forte pression de facteurs externes, en quoi la diffusion de certaines informations et le canal utilisé sont de nature à ne pas exécuter le ordre ou les décisions de la hiérarchie?**			
DONNEES DE RECHERCHE				
Sous-Problématiques	**Déclinaisons**	Entretiens	Documents	Observations
Altération de la confiance et prise de décision	Une organisation pourrait-elle utiliser des opération altérant la confiance des personnels à l'encontre d'une concurrente?	V	NV	V
	Peut-on définir les attaques visant à alterer la confiance des personnels dans une organisation	V	V	V
	La confiance comme facteur de coopération	V	V	V
	Il existe différents niveaux de confiance	V	NV	V
	Les différentes strates de confiance rentrent en concurrence au lieu de déclencher un mode itératif vertueux à même de renforcer la confiance et les processus de coopération	V	NV	V
	Il y a différentes dynamiques selon les niveaux de confiance, et différentes combinaisons itératives de confiance intervenant à la croisée des fondement de la confiance (affectif, cognitif, intuitif) et des différents niveaux hiérarchiques	V	NV	V
	La confiance, pierre angulaire de la gestion de la coopération au sein des équipes en situation extrême	V	V	V
	Les cibles potentielles de ce type d'attaque n'ont pas conscience de pouvoir être visée	V	NV	V
La perméabilité aux informations divergentes de celles délivrées par l'organisation	Quand une information est partagée ou transmise par un « pair », ou un supposé pair pensé comme partageant les mêmes valeurs, la confiance dans le contenu est accrue	V	NV	V
	Internet et un vecteur efficace des opérations d'alteration de la confiance	V	V	V
	Le temps sur Internet influence sur l'efficacité des opération d'influence	NV	V	NV

I . The use of cyber activities as a weapon: the empirical case of Ukraine

Introduction

Since the Maidan revolution in late 2013, Ukraine has faced war on its eastern territories in Donbass. This ongoing war is not only 'kinetic' but has also included a large cyber warfare component. According to President Poroshenko, Ukraine faced 6,500 cyberattacks on 36 Ukrainian targets between November and December 2017 alone. The attacks included classical intrusions on private and professional emails of persons of interest, as well as Distributed Denial of Service attacks (DDoS) of websites (including government). Larger scale operations were also conducted, such as an attack on the electronic system used for the presidential election (May 2014) or power cuts affecting 225,000 people in 2015 and the Kiev blackout of December 2016. Numerous operations targeting human psychology were conducted against Ukraine, notably on soldiers. Some of these operations used multifaceted tools to interfere with the robust cognition acquired by soldiers during training and to weaken trust in their hierarchy and government. The aim was to influence the subjects' behavior unbeknownst to them, a key issue this article will address. In 2017, we conducted field interviews with active soldiers and veterans. The aim was to conduct a qualitative analysis in the light of cognitive dissonance theories (self-consistency and SSM model), a decision driven by the nature of the field and the specific profile of the subjects studied. Based on the 2017 interviews, we considered the question of whether Ukrainian soldiers' trust had been affected by cognitive dissonance deployed in Internet-based operations. In other words: had their perceptions

changed and uncertainty increased enough due to Internet consumption to modify their behaviors? Another key question was to define whether they were aware of being potential targets or not. Part 1 of the paper reviews the literature and defines some of the terminology, such as psyops, etc., and explains the theories used in the analysis, such as cognitive dissonance, and trust in military affairs and in the Internet. Part 2 presents the Ukrainian case study, its methodology, the data collected, and our analysis.

1 - Literature Review and Definition of Terms

Terms such as ‘cyber warfare’ and ‘psyops’ are often loosely defined due to their cross-disciplinary nature. As such, before presenting the theoretical framework we start the paper by defining relevant terms. This will help shed light on the data collected and analyzed, to be presented in Part 2.

1.1- Clarifying the Terms

For Schaap, « cyber warfare » is « the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and networks themselves, of another state » (Schaap 2009). Other definitions invoke ‘actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption’ (Clarke 2010). Still others divide cyber warfare into two types: strategic and operational. Strategic is explained as ‘a campaign of cyberattacks one entity carries out on another,’ while operational ‘involves the use of cyberattacks on the other side’s military in the context of a physical war’ (Libicki 2009). For

the purpose of this paper, we use Schaap's definition of cyber warfare, as Libicki's refers to physical war by an identified adversary and as such is not applicable here.

In our case, although suspicions fall on Russia, final attribution of cyber operations is not absolutely defined. And while Clarke's definition involves a 'nation-state,' Ukraine faces both a separatist movement and cyberspace struggle against structures that are not all officially linked to a nation-state. Furthermore, the present paper addresses cyber operations having psychological effects on military staff rather than effects on computers or networks. Accordingly, we use the term 'cyber operation' instead of 'cyberwarfare.' Moreover, our choice accords with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). This seems wise, given that the Ukraine conflict is linked to Russia's geopolitical strategy. The CCDCOE's definition (found in the Tallin Manual on the International Law Applicable to Cyber Warfare) denotes a broad approach and is defined as 'the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace.' Moreover, as the Tallinn manual is the result of a transnational study group, it makes sense to use its terminology[20]. Applied to the present subject, the CCDCOE's definition is large enough to embrace cyber psyops in a context of war, which matches our subject perfectly.

There is agreement among experts today that Ukraine was – and is – a test lab for cyber warfare operations and 'psyops,' or psychological operations (Greenberg 2017). When talking about psyops, we refer to operations aimed at influencing an enemy's state of mind through non-kinetic means. For this purpose, psyops can use chosen information or indicators to influence people's emotions, thoughts, and reactions. Targets will

[20] The Tallinn manual (Tallinn Manual on the International Law Applicable to Cyber Warfare, published in 2013 and followed by an updated version in 2017) was written on the invitation of the CCDCOE by a transnational group of IT experts and legal scholars. It deals with international law applications in cyber operations conducted by and directed against states, in cyber conflict and cyber warfare; as such, it had to define the terms covered by laws in this field.

consequently change their minds and behaviors and, as fallout, the behavior of governments, organizations, or groups can also be changed. The word ‘psyops’ first appeared in 1965 although the expression ‘Military Information Support Operations’ (MISO) may also be used. On the Ukrainian information front, when addressing psyops, various channels were used to match the psychological profiles of targets, and the military was no exception. Concerning soldiers, stealth operations were conducted through the Internet, particularly social networks and chat forums. These operations targeted active fighters as well as veterans and used peer group trust to generate doubt and uncertainty toward the government and military hierarchy.

1.2- Existing Literature Review

By its very nature, the subject of the paper is at the crossroads of various theoretical frameworks. Due to their make-up, the operations studied require three different approaches. The methodology is based on cognitive dissonance and heuristic biases; the effects observed involved trust in military teams and military psychology; and the way messages are disseminated are essentially Internet-based, requiring channel-based trust.

1.2.1- Cognitive Dissonance and Decision Making

Although cyber operations use new technology, the methods of influence, such as persuasion or psychological destabilization, have been used before. Cyber tools, with their speed and opacity, are a way to designate a strategy, here based on cognitive dissonance. Developed in the 1950s by Léon Festinger, cognitive dissonance theory postulates that when two cognitions are opposed (said to be ‘irrelevant’) in someone’s mind, he or she will experience a ‘motivational psychological discomfort.’ The discomfort is ‘motiva-

tional' because in order to feel comfortable again, the subject will behave in such a way as to reinforce or weaken one of these cognitions. Aronson (1968, 1992) improved this theory by casting it in a more functional light. He developed the 'self-consistency' variation, in which dissonance arises in people from contradictions between individual behavior/action and their perception of themselves. In this theory, the more people's perception of themselves is positive, or whose values are socially considered as positive, the more they will feel cognitive dissonance. And individuals whose lives are at risk are also more sensitive to cognitive dissonance (Jonas, Greenberg, & Frey 2003).

It seems clear that subjects such as soldiers match these prerequisites perfectly. Effectively, soldiers are associated with values perceived as highly positive, such as sacrifice for the greater good (related to heroic mythology), regularly putting their lives at risk, and facing extreme situations (that is, situations that are unpredictable, risky, and subject to rapid change). Further, empirical experience strengthens cognition. Since it helps soldiers stay alive, training is validated by field experience and external operations (EOs). Training is therefore internalized, and soldiers follow it completely, consistent with Festinger (1956), for whom a cognition can be the result of past experience. In the case of soldiers, a cognition is initially learned during training, then later reinforced through validation by everyday life experience in extreme situations. According to theory, the more the cognition linked with their values is strengthened, the greater their reaction toward inappropriate behavior will be, functioning as an emotional reaction by-passing the thinking filter: more a reaction than a reflection.

Another relevant development of the theory is the Self-Standard Model (SSM) of Stone and Cooper's integrative model (1999). In this version, the cognitive elements

affected by dissonance may be personal standards (idiographic arousal) or normative standards (nomothetic arousal). In the case of soldiers, normative standards can turn into personal ones. On this basis, theoretically, they are highly sensitive to cognitive dissonance and thus to a potential cognitive attack. Indeed, cognitive dissonance incurred by psyops mobilizes soldiers' own standards to arouse dissonance – motivational discomfort – and make them change their behavior. These operations are highly effective when they decrease trust and certainty in soldiers' minds, thereby weakening the cornerstone of a properly functioning military, as we shall see in Part 2.

With regards to the self-consistency model and Self-Standard Model theory, the more a target is trained and conditioned, the more it can merge its professional values and self perception, combining idiomatic and nomothetic standards. Consequently, training gives serious indicators on how soldiers think and react, thus helping in profiling. If the target is conditioned enough, we can postulate that this kind of profiling could be very effective and close to what a personal profile can be. Moreover, when reacting to a psyop built on cognitive dissonance, the target will not even be aware he had been influenced, as he changed his behavior according to what he perceived as the very values and elements which are part of his personality, as highlighted by our interviewees' responses to their perception of being a target. Consequently, in professional settings, compromised personnel will not be easily detected because they are still loyal to the overall pattern of what must be defended and what is worth fighting for.

It seems clear that the risk component of a deterioration in trust is a change in behavior based on a change in decision-making. But making a realistic prediction of what the agent behavior could be in order to secure an organization strategy (i.e., being sure that orders are going to be executed without modification) implies the supposition

that decision making is based on rationality. The 'rational choice model' refers to theories of action in this area of research. Developed initially by Friedman (1953), the Theory of Rational Choice (TRC) is based on a holistic approach and has achieved paradigmatic status in economic sciences. More specifically, the TRC states that individuals act according to two criteria: maximization and coherence, in which rationality is a link between information and individual preference. While this theory helps predict expected decision results, some authors (Elster & Gerschenfeld 1986; Bourdon 2004; Allais 1955) highlight its lack of realism. TRC does not in fact take account of environmental factors, or of the subjects' experiences and intuition, and thus has certain inherent limitations.

In response to these, Kahneman and Tversky (1977) developed a decision model that departs from the theory of rational choice and attempts to define the mechanisms leading to individual and collective decision-making. Basing their theory on a heuristic approach that privileged heuristics and biases (HB), Kahneman and Tversky proposed decision-making as the product of mechanisms of interaction between the automatic system and the reflected system. In HB, mental process is constituted by two different systems: the automatic system (System I) based on immediately available knowledge, always able to generate an answer, and the reflexive system (System II) producing judgments and able to rationalize the ideas produced by System I.

More concretely, System I is based on innate abilities and makes quick associations between ideas (Morewedge & Kahneman 2010). It is known for translating emotion into impulsion, given that emotion is understood as a psychological and physical reaction to a situation. As such, System I may lead individuals to act suddenly (by reflex) without thinking about the consequence (Baratt 1993). System II uses memory and requires at-

tention and effort to work (Beatty & Kahneman 1966; Kahneman, Tursky, Shapiro, & Crider 1969). Consequently, when this system is called into play, it becomes difficult for the individual to perform multiple actions at once (Kahneman 2012). In practice, System I generates suggestions (feelings or intuitions) when a new situation arises and submits them to System II, which decides to launch actions. But the two systems may conflict (Gilovich, Griffin, & Kahneman, 2002). In this case, automatic reaction coupled with the intention of correcting a situation may cause problems.

As to our subject of interest, cyber operations may attempt to change System I in order to produce unexpected behavior in the targeted organization's agents. Effectively, changing System I will generate biased suggestions and result in a change of actions triggered by System II based on System I data. Moreover, intuition – managed by System I – comes from emotions and thus from the affective domain. Here, military values may switch from cognitive to affective and be reinforced by individual experience, modifying the intuition. According to Klein (1999) intuition also comes from experience, and military personnel usually develop strong intuition in their own field of action. According to Kahneman's theory, the efficiency of cyber operation as described could be particularly important.

As such, this study examines the possibility that cognitive-dissonance-based psyops can change both soldiers' trust and behavior, as we will see in the presentation of data and analysis. Failure of frontline soldiers to carry out orders properly could endanger an entire operation. To cause this, cognitive dissonance must change a soldier's trust and decision-making. Accordingly, prior to proceeding we must look at the literature on trust and cohesion in military affairs.

1.2.2- Trust and Cohesion in Military Affairs

Trust seems to be the cornerstone of military cohesion and performance. According to McAllister (1995), trust has cognitive and affective underpinnings and is a factor of cohesion. Some meta-analytic studies show a positive relationship between cohesion and performance (Mullen & Cooper 1994). In military matters, performance means achieving the goal of a successful mission with as little loss as possible. Other sources propose three main components of military cohesion: relations between peers, relations between superiors and subordinates, and relations between the armed forces and the government (Stewart 1988; Etzioni 1961). Hence for soldiers, degrading the perception of government and increasing mistrust in superiors will deteriorate cohesion and performance, increasing the risk factor in mission success.

While trust is primordial, it remains a nebulous concept that needs clarifying. Bhattacharya et al. define it as 'the expectancy of positive outcomes that one can receive based on the expected action of another party in an interaction characterized by uncertainty' (Bhattacharya et al. 1998). Another definition from Rousseau et al. (1998) indicates a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another. Lastly, Mayer, Davis, and Schoorman (1995) define trust as 'a willingness to be vulnerable to another party when that party cannot be controlled or monitored.' These definitions are particularly apt here because our subjects live and act under extreme situations. Accepting vulnerability is very real in that they can be wounded or even die in action.

Previous definitions of trust described uncertainty as a game changer. For Rivolier (1998), extreme situations are fast-changing with high levels of uncertainty for participants. To be considered extreme, a situation must also be risky (Lièvre 2014). In milita-

ry parlance, vulnerability is a recurrent keyword in the definition of trust. Given that soldiers operate in extremely risky situations, it seems clear that trust is a cornerstone in achieving their tasks. In the event of failure, over and above their own mission is the government's credibility and trustworthiness. This can be diminished in its citizens' eyes (if soldiers come home wounded or die in battle, for example) and possibly its allies' too. So, eroding the trust of soldiers may have considerable effects not only on the battlefield but also on the government's policy and stability.

1.2.3- Cyber Operations, Access to Information, and Changes in Trust

Finally, in terms of literature review, in the case of Ukraine, the target of cyber operations was information. Based on our observation of increased uncertainty resulting from cyber operations, a comprehensive update on research into this issue seems appropriate. According to Negroponte (1995), we live in a digital world, and military personnel are no exception: they are as connected as anybody else. Many of the soldiers we surveyed are 'Generation Y;"[21] judging by Internet and mobile data consumption figures, this generation is among the most highly connected in history. A survey conducted by Omnibus Institute in the United Kingdom showed that 18 to 34-year-olds look at their smartphone up to 100 times a day, in other words every 9 minutes and 50 seconds. The growth of smartphones has caused a major shift in how we inform ourselves. As far as social media consumption is concerned, mobile usage grew by 30 percent from 2015 to

[21]Generation X refers to people born between 1966–1976; Generation Y, or Echo Boomers or Millennials, to people born between 1977–1994; Generation Z to people born between 1995–2012.

2016, an increase of 581 million. Over 91 percent of the 2.8 billion people on social media are connected via mobile devices, and soldiers are no different.

Cyberspace, being a vector of information, changes how people inform themselves, and therefore influences their trust. Although information access may vary depending on age, the trend is clear: more and more people use the Internet to get information, many through social networks. Only two soldiers in our sample were not connected to social networks. So, people can easily be targeted in cyberspace by 'information' created for the need of a psyops strategy using cognitive processes. Given that all the soldiers interviewed owned smartphones and said they use them for surfing the web and social networks, analyzing the trust attributed to web-sourced information seems important in understanding how it can be used by an adversary to influence soldiers' perceptions. According to the American Press Institute and the Associated Press-NORC Center for Public Affairs Research (2016), the person sharing a post was considered more important than the original source of information. The survey results showed that the individual sharing the information had a major effect on how trustworthy the information was considered: 51 percent of people said an article was well reported when shared by a person they trust. With Facebook, 48 percent of the interviewees said how much they trusted the person posting the article influenced how much they trusted the information in question.

As to the military, given the special training and resulting team spirit, we postulated that if information is posted by a soldier, or someone sharing the same values (volunteer,

etc.), a soldier's trust in the content will increase. The analysis of data in Part II vindicate this.

2. The Case of Ukraine

Ukraine has been facing the biggest deployment of cyber operations against a country ever seen. In light of the literature presented in Part 1, we examined the possibility that the trust of active and veteran Ukrainian soldiers had been affected by cognitive methods of Internet-based attacks. The purpose was to see whether their perceptions had altered and uncertainty increased in relation to their Internet consumption, and if so whether the effect was significant enough to modify their behavior. Another key question was whether they were aware of being potential targets or not.

2.1- Significance of the Case Study

Before answering these questions by means of data analysis, we discuss the value of Ukraine as an example. In Ukraine, the kinetic conflict was accompanied by massive waves of cyberattacks of many kinds. While Russia had already used such methods against Estonia and Georgia, the case of Ukraine is unprecedented in its magnitude. For many experts (Greenberger 2017; Weedon, 2015), it was a blueprint for testing various methods and estimating their effects. For NATO's CCDCOE, the use of cyberattacks by (in all appearance, Russia) was part of a broader strategy of information warfare (Geers et al. 2015).

Specific to Ukraine, cyberattacks included psyops cyber operations intended to affect as many people as possible and weaken the central government and country. We found that

various channels were used in order to match the psychological profiles of targets and that the military was no exception, quite the contrary. Many military personnel received text messages on their mobile phones, encouraging them to stop fighting, go back home, or leave their positions. Meanwhile, more subtle operations were conducted through the Internet. We found that the soldiers we interviewed had received fraudulent messages. For example, the profiles of dead soldiers were used to send Facebook chat messages and spread 'information' to sow doubt and mistrust toward state institutions. The soldiers explained that since they didn't know their 'brothers in arms' were actually dead they were more inclined to believe these messages. This is paramount as such operations used soldiers' in peer-group trust to sow doubt about members of government or commanding officers.

Active fighters were not the only targets: a vast operation was also conducted on veterans. Veterans are ideal targets, as they exemplify an ideal of heroism for the general population, occupy a special position as thought leaders or national symbols, and have been trained in firearms handling. Many of them are young and thus part of the labor force and have political weight as voters and/or potential political leaders. Moreover, their past in EO makes them a potentially explosive social group. The way they feel can therefore have a profound influence on people's perceptions.

Except for certain occasions – tactical war phases, for example – the final goal seems to be to increase uncertainty in the minds of soldiers and fighters. To this end, some information media such as blogs or social networks were used (Weedon 2015). These practices are in accordance with Russian cyber warfare strategy such as developed by General Gareev (2015), or Colonel Chekinov and Lieutenant General Bogdanov (2011,

2013). According to them, information is a component of New-Generation War (NGW). As such, subversive operations involving information can be used to create chaos and provoke various kinds of disturbance, including weakened state resilience. Russian cyber warfare strategists have even recommended the use of mass media to stir up chaos and confusion in government but also in military management, particularly command and control. This matches the desired results of operations conducted in Ukraine. As a mirror effect, their recommendations for safeguarding Russia from such operations can be reversed for devising battle plans. For instance, their proposals included keeping sources of domestic (Russian) information out of reach of adversarial influence; yet in Ukraine, information channels were penetrated by exogenous influence.

Last but not least, Russian cyber warfare strategists have advised that information, including psychological warfare, should predominate in NGW, and be used extensively. The effect on the human psyche targeted is clearly to misinform, as well as encourage discontent and unlawful acts. Analysis of the data collected in Ukraine thus seems to suggest a global military strategy, since loss of trust resulting in disengagement and changes to soldiers' behavior can be assimilated with unlawful acts based on discontent. Further, the result of these operations upon the execution of orders is clearly disruptive of military management, and command and control.

2.2- Data Collection and Research Methodology

Since 2014, we have made several trips to Ukraine, during which we witnessed cyber operations on various population levels. The data collection presented is based on research into the literature and field observations, static and dynamic, on and off the battlefield.

The goal of the research trip in February 2017, during the battle of Avdiivka, was to interview soldiers and veterans and establish whether their uncertainty had changed according to their Internet consumption, specifically according to a certain type of content. For context, the government had been vigorously promoting military values since the beginning of the conflict in Ukraine. Travel was initially planned to Avdiivka. However, due to the battle that broke out in the city, safe access was not assured, and we traveled instead to Poltava and Kremenchuk. Poltava has a hospital where many wounded soldiers were treated for physical and psychological trauma. Kremenchuk has a military school and a large part of its population was affected by the war. In addition, many soldiers were based in these cities to ensure turnover on the front line, ensuring ease of access to interview subjects.

2.3- Survey methodology

After local contacts had introduced the researchers to various groups, thirty active soldiers and veterans were interviewed after being divided into two groups, one of fifteen veterans (all wounded physically or psychologically) and one of fifteen active soldiers. The soldiers were assured of their anonymity and that the interviews would be neither transmitted nor published, as much for reasons of national security as to increase their trust in the researchers. The surveys used a qualitative approach designed to obtain as much information as possible.

Concerning the question set, the interviews were not strictly directed but many questions were recurrent, thus allowing an analytical framework to be defined. For instance, the soldiers were asked to quantify their trust in various structures (group, institution, and government) on a Likert scale from 0 to 5, as well as their confidence in various

kinds of media (radio, television, social networks, and alternative media such as blogs and nongovernmental information websites). They were also invited to explain their Internet habits and how they get their information. They were surveyed on how they felt about their institution and government before and after operations and also asked about the various media they listen to and why. The subjects were thus interviewed to ascertain whether their trust and perception of the government and their military hierarchy could have been influenced by cyber content and/or their Internet consumption. Lastly, they were asked about their perception of being or not being a potential target for psyops on the Internet. They were asked to elaborate on their answers. The interviews were sometimes followed by discussions on Skype or by email at the soldiers' discretion. Several of them used these discussions to send material, especially fake profiles they had spotted, or blog posts that particularly interested, impressed, or influenced them.

3- Analysis and Results

The qualitative data were processed with Nvivo 12; some data were extracted using Excel in order to express results as percentages, allowing us to perform the analysis presented here.

Analysis of the data collected from interviews with soldiers in Ukraine sheds light on several points. First, their daily consumption of Internet data was very diverse (from 0.5 to 6 hours). Nonetheless, it seems that the ones who changed their mind the most were those Journal of Intelligence and Cyber Security 55 connected two to four hours per day, in other words, it was not the biggest consumers who were the most influenced.

However, we need to look more deeply into this observation, especially when it comes to the data consumption environment (private or public, etc.). Second, in terms of age, it seems that soldiers belonging to 'Generation Y' were more responsive and increased their uncertainty level toward institutions and government most. Some of them went so far as to say they had changed their behavior enough to not strictly obey a direct order. As justification, they explained that they had discovered details revealing that some of their commanders were not as 'trustworthy' as they expected them to be. One of them explained that 'I won't risk my life for someone who shows no respect for us, the sons of Ukraine, and for our wounded.' Here, we also noticed the development of a gap between 'us' the soldiers, and 'they,' 'the others,' in other words, the military hierarchy or members of government.

The interviewed soldiers' experience and participation in kinetic operations seemed to give them the feeling that they were more legitimate than the government in judging the merit of an action. For instance, one explained, 'I believe less and less in people who do not have their hands in grease, who had never been on the field'; another told us that 'there are too many people talking about what they do not know … it's getting on my nerves.' Yet another soldier concluded that 'they are wearing figures just for the pictures, reality is that they don't know anything.' At the same time, one thing we observed in a focus group of Ukrainian soldiers was that they never stopped believing in the core of their cause ('fighting for Ukraine') but have gradually dissociated it from Ukraine's government. One explained, 'I believe less and less in our government and its capacity to help us. I only believe in Ukraine, those who fight. Those who do not stop fighting.'

Indeed, the growing mistrust of the 'others' has ratcheted up doubt in their government and, for some, President Poroshenko in particular. As to their level of trust in various

media, they mainly seemed to trust social networks and alternative media more than official ones, which are perceived as tied too much to government or oligarchs. For instance, one explained to us that 'the newspapers, the big media belong to men who serve politics, so it's not the truth that they want us to believe.' Another said, 'when you are not paid for your publication you are more honest, so I think blogs and social networks lie less than big media.'

In explaining this gap in trust, soldiers argued that they mostly trusted their brothers in arms' and volunteers because they had similar experiences and fought for the same cause. It also seemed quite clear that their self-perception was strongly linked to their soldier's identity (even if they had other professions before the war) and patriotic fight for their country. Furthermore, they described themselves using military values and vocabulary (like patriotism, honor, and loyalty). It seems that they adopted these cognitive data (learned by training, the very nature of their job) as part of themselves, of the way they perceive themselves: these cognitive elements have become personal and affective ones. The cognitive components of their training and conditioning eventually became part of their personality.

According to the research we conducted, the soldiers we interviewed and surveyed seem to have been targeted by multi-step operations. Firstly, strong cognitions inherited from training were reinforced. In a military environment, this was easy to achieve since the targets believed their contact (the writer of the papers they read or sharer of the information seen or heard, etc.) was involved in military operations and therefore shared the same values. This was indicated by the use of expressions such as 'brother in arms,' 'sons of Ukraine,' 'we,' or 'us.' Furthermore, since this concerns values of importance to soldiers, the agent involved appears increasingly trustworthy. Consequently, an ad-

versary can send misinformation to his target, linking this cognition with the field in which he wants to sow doubt.

For instance, soldiers showed us articles associating a member of government or a superior with the disrespectful treatment of veterans or wounded fighters who, in a soldier's belief system, deserve military honors. As the information is completely opposed to the way soldiers want to see themselves and their values, this content was rejected. This example is no exception, and this kind of reaction is founded on soldiers' self-perception, even if it is based on cognitions resulting from training and conditioning. We thus noticed that some soldiers' strong cognitions were reinforced, particularly via Internet chats with apparently fake profiles or through the fraudulent use of deceased soldiers' profiles. Other strong cognitions were increased through blogs forwarded by 'friends' or by other soldiers, sometimes real but sometimes created on purpose.

Thanks to mobile data, interactions between the targets and psyops agents can occur every day. Some may encourage targeted persons to perform specific actions at specific times, but this is very unlikely. It would require the conjunction of two complicated phenomena: an exact action and an exact time. When the focus group was asked whether they thought they could be a target of interest, the answer was unanimously 'no.' The explanation given was that, in their opinion, they were not strategic targets because they were not officers and did not hold strategic information or data. They particularly did not feel they could be strategic targets themselves. On the other hand, the focus group agreed they could be targeted by propaganda, but as Ukrainians and not as soldiers. Were it to happen, however, they thought it wouldn't work on them as they 'knew separatists' and Russian lies too well to be fooled.' Yet, the focus group only referred to

‘higher’ propaganda and not its most subtle forms, i.e., the use of cognitive dissonance. One counterintuitive result is that soldiers felt they were not affected by cyber operations, all the while acknowledging that their opinion about the government and military command had changed as they ‘learned’ more about them, largely through information obtained online.

The implications here are important. If the perpetrator of an attack were to obtain an increase in uncertainty among a large enough proportion of a military team, this could increase his ability to cause the operation to fail. With increased levels of doubt and uncertainty, military personnel may not behave as they are supposed to. This is very dangerous as mission planning is built on the basis that soldiers will obey orders without variation and relies on behavioral stability. In the end, the nature of behavioral change does not matter. What does is that overreaction could be as dangerous for the conduct of a mission as under reaction. By under reaction, we understand a weaker response than expected, such as not executing an order or taking more time to carry it. In all cases, targeted soldiers do not accord with their conditioning and engagement. It is this ‘disengagement’ that can jeopardize the mission. These operations and their observed effects are related to trust in military teams, and to military psychology. Using cyber operations could be particularly advantageous for an adversary. Their efficiency can be significant on two levels, first from a practical point of view, in other words, on efficiency, and second in terms of the interest to the organization using these kinds of operations, in other words, on strategy. Concerning efficiency, many people use the Internet to get information, in other words, cognitive elements. Cognitive dissonance can thus be used to trigger a psychological motivational discomfort and attempt to change the behavior of any subject. In addition, the Internet can be used all day long to affect people, which means

they can be subjected to several phases of cognitive dissonances, thereby increasing the rate of success in behavior change. Moreover, in accordance with the theories of Aronson (1968, 1992, and 1999) and Cooper & Stone (1999), cognitive dissonance can be deployed if a target's training is known and the values learned have become part of their personality, as occurs in the military. The Ukrainian case seems to validate this theory.

Conclusion

Based on the above observations, it appears that cognitive dissonance through misinformation circulated on the Internet can be used as an efficient tool for psyops to affect trust. If Ukraine were indeed a blueprint for Russian destabilization operations, the methods used were presumably worked out beforehand. In agreement with the concept of cognitive dissonance, the more the cognitive and affective dimensions are merged, the easier it should be to influence somebody using methods discussed in this theory. In the case of soldiers, since training and personal values merge in accordance with self-consistency theory, an adversary can easily obtain the profile of a military team, including soldiers' self-perceptions. In other words, the more someone is trained and conditioned, the more he can become a target. This holds the possibility of many practical consequences. First, using the training and conditioning of military personnel as key component of these cyber operations, the assailant does not need to send agents into the field, close to targets, to perform individual psychological profiles. It is not only safer, decreasing the risk of being unmasked, but also less expansive, as long as the training and values inculcated have been studied enough. Looked at cynically, using this me-

thod, part of the work is done by the victim, not by the assailant, thereby reducing the latter's work. Further, as the target changes his behavior in accordance with the values he believes in and the training he received, he will not realize he is acting under someone else's influence. In our study, soldiers stated they couldn't be targeted and, even if they were, wouldn't be affected. Finally, we may suspect that when a soldier is subject to long-term cognitive dissonance, even if he does not change his behavior, he will feel psychological discomfort, for cognitive dissonance affects brain activity, in particular the prefrontal cortex and anterior cingular cortex (Gehring et al, 1993; Amodio, et al, 2004; Harmon-Jones et al, 2008). This in turn becomes a human management issue during both the short and long terms for the assaulted person. On the strategic level, the benefit of this kind of weaponization means that it will be very complicated to prove the involvement of the head of operations, and just as complicated to detect the attack itself. In the Ukrainian case, even if president Poroshenko points the finger at Russia for many of the Volume 2, Issue 1: June 2019 60 cyber-attacks and cyber operations his country has faced since 2014, actually proving Russian involvement is very complicated. Given the wide range of people and events involved, it would be very difficult to link attacks conducted via multiple channels with an overall state strategy. Concerning Ukraine, various hacker groups are known to be involved in the war, such as CyberBerkuts, Cozy Bears, FancyBears, or SandWorm. However, despite strong suspicion, no sufficient proof has ever been brought to a court of law. Consequently, any government might find it useful to hide behind seemingly autonomous hacker groups to target another country without fear of falling under the scope of international law, military or otherwise. Alternatively, those attacked can hardly respond in kind if they wish to respect the law. Further, since either detecting or attributing these cyber operations is complicated, assai-

lants could more than likely apply them during peacetime. The high level of Internet penetration and the fact that cyber's multi-channel nature can be used to generate cognitive dissonance and affect System I enough to upset its relation with System II is extremely interesting, particularly because no commitment is needed for the outbreak of information dissonance (Vaidis and Gosling ; 2011). Thus, if information that appeared on a smartphone can trigger dissonance, the target does not need to have sought the information for a reaction to be emulated. Moreover, the rapid growth of 5G will probably play its role in future developments, revolutionizing our relationship with technology and information. As such, the present results are probably just the first step in further research, as operations like this are likely to increase in importance as time progresses.

II . La référence de la confiance comme cadre d'action en situation extrême

Introduction

Nombre d'organisations intervenant dans des situations extrêmes (Lièvre 2005, 2009 ; Rivolier, 1998) rapportent que la confiance entre les intervenants est la condition sine qua non de la réussite des opérations. À ce titre, la performance d'une équipe, à l'aune de la bonne exécution de l'ordre donné par la hiérarchie, serait en lien direct avec la confiance exprimée au sein du groupe dans lequel les agents interviennent — donc dans les coéquipiers — de même qu'avec celle éprouvée envers la hiérarchie, puis dans le gouvernement. À la lumière de ces éléments, nous préférons donc parler de modes opérationnels plutôt que de performance. Dans le cas d'organisations en situations extrêmes, la cohésion apparaît comme un élément permettant d'accroître l'efficacité des modes opérationnels et donc de sécuriser les stratégies de la structure. La confiance conduisant au renforcement des liens de coopérations entre les agents, elle participe au développement de la cohésion au sein des groupes. Du point de vue de la recherche scientifique, différentes études, notamment la méta analyse réalisée par Mullen et Cooper (1994), ont travaillé à mettre en évidence le lien entre la cohésion et la performance des modes opérationnels.

La confiance étant considérée comme un élément fondateur de la réussite d'une opération menée en situation extrême (Lièvre 2005 ; Arena, Oriol et Pastorelli, 2013 ; Auger & Reynaud, 2007), certaines organisations ont observé la manière dont s'articulaient les différents niveaux de confiance — les différentes strates — afin de travailler à leur renforcement mutuel en vue de sécuriser l'exécution de leur projet. Une telle démarche,

menée sur la dynamique entre les différentes strates de confiance entre les différents niveaux hiérarchiques, pourrait alors servir de protection pour leurs agents et collaborateurs, les préservant du doute et de l'incertitude, notamment de ceux que pourrait déclencher l'intervention d'éléments exogènes. Or, des organisations intervenant en situation extrême soumettent quotidiennement leurs équipes à des environnements particulièrement incertains. En effet, la théorie identifie une situation extrême par la réunion de trois critères : elle est changeante, imprévisible et risquée. De facto, la création d'un système de forte confiance sera d'autant plus importante qu'elle permettra de développer des schémas de coopération qui participeront à contrebalancer l'incertitude liée au contexte où se déroulent les interventions et actions décidées par l'organisation. C'est pourquoi les contextes de situations incertaines offrent un terrain privilégié d'étude pour qui s'interrogeant sur les conséquences de la confiance au sein des équipes, dans la hiérarchie, mais aussi dans la structure gouvernementale.

En d'autres termes, une dynamique créée et entretenue entre les différents niveaux de confiance, entre ces différentes strates de confiance, pourrait assurer une protection contre le doute à même d'altérer la stratégie de gestion de l'entité. Or, sur la base des observations réalisées, la question de l'efficacité de cette dynamique se pose. Si une réponse négative devait y être apportée, c'est toute la stratégie de gestion de l'organisation qui pourrait être mise en situation d'instabilité dangereuse.

Dans ce contexte, cet article s'attachera à identifier les dynamiques interagissant entre les différents niveaux de confiance (celle portée au niveau horizontal d'une équipe (niveau micro), celle dans l'organisation (niveau méso) puis celle dans la superstructure étatique (niveau macro) se renforcent ou, au contraire, tendent à s'opposer. Selon le cas, les leviers mis en évidence seront analysés. L'objectif de cet article est, à partir d'un tra-

vail empirique, d'analyser l'articulation entre ses différents niveaux de confiance et d'observer si un de ces niveaux, une des strates, prend le pas sur l'autre. Pour ce faire, le cadre théorique de la confiance sera abordé au travers du lien entre confiance et la gestion de la coopération au sein des équipes puis, plus généralement, de la confiance organisationnelle avant de recentrer, en premier lieu sur l'analyse des organisations intervenant en situation extrême et, dans un second temps, de s'attacher à observer le fonctionnement de la confiance entre les différents niveaux hiérarchiques. La seconde partie présentera l'étude de cas et sa méthodologie. Enfin, la troisième partie fournira la somme de l'analyse des entretiens menés auprès de personnels d'une organisation intervenant en situation extrême.

1. Confiance et gestion de coopération

Dans le prolongement des travaux effectués sur la confiance par les sciences sociales (Zucker, 1986) pour le volet institutionnel, pour le volet interpersonnel (Shapiro, 1987) et en psychologie (Deutsch, 1962 ; Rotter, 1967), les sciences économiques puis de gestion ont également investi ce champ de recherche. L'influence de la confiance sur le fonctionnement de l'organisation a été examinée, notamment dans le contrôle et dans la coordination des membres de la structure agissante. À ce titre, des travaux comme ceux de Zand (1972) mettent en lien la confiance et l'efficacité dans la réalisation des projets. Cette analyse est en accord avec la méta analyse de Mullen et Cooper citée ci-dessus. Cependant, si la confiance semble régulièrement liée à l'incertitude, il convient d'approfondir l'analyse de ce qui constitue la nature même de ces deux concepts — i.e. la

confiance et l'incertitude — afin de définir quel cadre conceptuel sera utilisé au cours de ce travail.

1.1. Confiance, efficacité et vulnérabilité

Au cours de cet article, nous chercherons à évaluer si l'incertitude du milieu, autrement dit sa volatilité, accroît l'importance de la confiance, si ces contextes spécifiques la rendent garante de l'exécution efficace des missions par les équipes chargées de la réalisation des consignes données par l'organisation. Les situations extrêmes sont définies comme changeantes et imprévisibles, mais également comme risquées pour les personnes ayant à y intervenir. Cette omniprésence du risque et de l'incertitude fait de la confiance, comprise comme levier de coopération, la clef de voûte de la sécurisation de la stratégie de l'organisation : pour être contrebalancée, l'incertitude doit avoir des contrepoints forts, à savoir la confiance.

Le lien entre incertitude et confiance apparaît aussi dans la littérature. En effet, plusieurs définitions de la confiance font directement référence à l'incertitude : ils utilisent notamment des termes comme « vulnérabilité » qui renvoient directement à l'aspect périlleux des situations extrêmes. En ce sens, la définition de Bidault et Jarillo (1995) met en corrélation la confiance avec une « situation imprévue » qui rappelle également les caractéristiques des situations extrêmes. Deutsch (1962) parlera lui de la confiance comme d'une « action qui augmente la vulnérabilité d'un individu face à un autre individu ». Pour Zand (1996), il s'agira de la volonté d'un individu d'augmenter sa vulnérabilité face aux actions d'un autre individu dont le comportement ne peut être contrôlé. On notera ici le lien évident entre vulnérabilité et manque de contrôle. Or le contrôle peut s'entendre également comme la capacité à prévoir les actions à venir, soit à de la

connaissance. Ainsi, le manque de contrôle se rapproche de l'incertitude alors que la confiance aurait une base cognitive forte.

Cette même idée ressort clairement chez Mayer et al. (1995), pour qui la confiance serait une « volonté délibérée d'être vulnérable aux actions d'une autre partie fondée sur l'espérance que celle-ci accomplira une action importante pour la partie qui accorde sa confiance, indépendamment de la capacité de cette dernière à surveiller ou contrôler l'autre partie ». Enfin, citons la définition de Bernoux et Servet (1997) selon lesquels la confiance serait la « condition d'une personne, d'un groupe ou d'une institution à un moment et en un lieu donné, fondé sur des éléments affectifs, intuitifs ou sur un ensemble d'informations et de croyances, de préjugés et par des processus d'apprentissage face à un objet, un mécanisme, un animal, un environnement physique, un individu, un groupe de personnes ou une organisation de toute nature, et dont la connaissance permet d'anticiper avec un degré plus ou moins élevé d'incertitude leur devenir ou leur réaction ou comportement dans telle ou telle situation ». Cette définition souligne clairement l'aspect cognitif de la confiance.

Dans ce cadre, la confiance permettrait au groupe de garder la capacité d'agir tant individuellement que collectivement. Il est à noter que l'amplitude de l'incertitude peut varier, allant d'une incertitude relative, à une incertitude radicale, telle que conceptualisée par Knight (1921), c'est-à-dire échappant au calcul probabiliste. On peut formuler l'idée que plus l'incertitude est forte, voire radicale, plus la confiance joue un rôle primordial dans la capacité de l'organisation à agir avec pertinence et efficacité.

Cependant, si l'incertitude est par nature imprévisible, la confiance peut également sembler irrationnelle, a minima à l'origine. Or si cette dernière est une condition impérative d'efficience des organisations, particulièrement pour celles intervenant dans des situations extrêmes et donc incertaines, l'enjeu sera de rationaliser ce lien. Ainsi, l'organisation pourrait maîtriser l'émergence d'une confiance « utile » et en assurer le maintien sur le long terme. Cette approche semble primordiale puisque la confiance, en lien avec l'efficacité des modes opérationnels, devient de facto une variable de gestion de l'organisation.

Ainsi pour réduire l'incertitude et augmenter la confiance, il faudra maîtriser les bases sur lesquelles se construit cette confiance. Outre les éléments fournis par Bernoux et Servet d'autres chercheurs, dits « conventionnalistes » et issus des sciences économiques, ont appuyé leurs travaux relatifs à la confiance sur la « convention ». Ainsi pour Orléan (1994) la convention permettrait de réguler les comportements des individualités compris dans un ensemble partageant une situation commune et se conformant aux attentes que chacun place dans l'autre. La régulation des comportements faciliterait le développement de la confiance ce qui aurait pour effet de mieux coordonner les comportements réciproques. Dans cet esprit, Gomez (1995) déclare que « chaque homme porte sa confiance en un certain nombre de valeurs, de représentations et de systèmes de justifications qui situent ses propres calculs et ses propres jugements ». Pour Giddens, la confiance se diviserait en deux catégories : la confiance interpersonnelle, exprimée envers les individus et la confiance dans les systèmes experts qui fourniraient des garanties suffisantes pour l'établissement de la confiance. Outre cette forme de confiance, Zucker a recensé trois différents modes de construction de la confiance : celle fondée sur les processus (process-based trust), la confiance basée sur l'expérience personnelle,

la confiance adossée à des obligations normées dans l'interaction d'individus disposant d'une similitude sociale, pouvant être tant socioprofessionnelles qu'ethnique (characteristic-based trust), et la confiance liée à une structure ou une organisation susceptible de pouvoir garantir les attributs de l'individu (institutional-based trust).

1.2. Confiance organisationnelle

La confiance organisationnelle dans la littérature renvoie principalement à Shapiro et al. (1992), Rousseau et al. (1998) et Lewicki et Brunker (1996). Selon ces auteurs, la confiance reposerait sur trois piliers, la dissuasion, le calcul et le relationnel.

Dans le premier cas, les agents obéiraient par peur de la punition.

Dans le second, la confiance, et l'action qui en découle, seraient fondées sur le calcul (ou knowledge based pour Shapiro), à savoir la connaissance, voire la certitude, que la partie tierce agira dans un sens favorable à l'agent. Il s'agirait donc d'un choix rationnel en partie fondé sur la réputation et sur un ensemble d'informations crédibles et accessibles concernant ce tiers. À noter que ce mode de confiance aura besoin de communications et d'un flux régulier d'informations de nature à accroître la connaissance et donc la prévisibilité de l'action supposée favorable. En outre, les théories relatives au choix rationnel ont pu être discutées par des chercheurs mettant en avant les limites de la rationalité (Simon, 1964; Chanut, Guibert, Rojot et Dubois 2011).

Dans le troisième cas, la confiance relationnelle s'apparenterait à de la confiance affective. Elle pourrait d'ailleurs se fonder sur l'identité, comme évoqué par Lewicki et Brunker (1996). In fine, MacAllister (1995, 1997) présentera deux formes de confiance interpersonnelle, la confiance affective, d'une part, la confiance cognitive, d'autre part. Alors que, dans le premier cas, la confiance s'appuie sur des liens émotionnels entre les

individus, elle résulte, dans le second, de choix rationalisés fondés sur la certitude que porte la personne dans le sérieux ou la fiabilité de celui en qui il place sa confiance.

Enfin, en science de gestion, d'autres auteurs se sont intéressés aux aspects de la confiance. Un point important serait que l'autre ne tirera pas profit de sa situation, ou de la situation générale, au détriment de l'agent : au contraire, le souci du bien-être de l'agent exclurait un comportement opportuniste (Barber, 1983 ; Ouchi, 1981 ; Mishra, 1996). Un autre aspect propre à susciter la confiance tiendrait à la fiabilité et à la cohérence, notamment entre le déclaratoire et les actions posées (McGregor, 1967) : il s'agit de ce que Kirkpatrick et Locke (1991) qualifient de « crédibilité ».

Dans toutes ces définitions, on retrouve la pluridimensionnalité de la confiance, qu'il s'agisse de ses causes ou de ses manifestations. Cependant, il apparaît clairement qu'elle sera toujours le pendant de l'incertitude et, plus précisément, la réduction de cette dernière. Que cette réduction se fonde sur des éléments cognitifs (positifs ou négatifs, i.e. dissuasion ou connaissance) ou affectifs, elle permettra d'accroître la prévisibilité de l'action des parties engagées ce qui, pour une organisation intervenant en situation extrême, prend une importance tout particulièrement aiguë.

Se pose alors la question des bases sur lesquelles développer une confiance efficacement mobilisée dans l'action. À ce titre, si l'incertitude figure dans la définition de Bernoux et Servet, elle présente également les vecteurs sur lesquels la confiance prendrait racine : des données affectives, intuitives, ou encore des facteurs résultant d'un ensemble d'informations et de processus d'apprentissage. Cette définition permet de regrouper les éléments précités à partir des travaux de différents auteurs. En outre, elle

pourrait parfaitement faire référence aux éléments acquis lors d'une formation ou d'un entraînement et, par là même, à des éléments cognitifs. Par ailleurs, en illustrant le lien direct existant entre l'individu ou le groupe social et une autre structure ou organisation, elle dépasse la simple relation interpersonnelle et transhumaine.

Ainsi dans cette approche, la confiance est entendue comme s'exprimant particulièrement dans une situation extrême où l'incertitude est forte, voire radicale. De même, pour exister, la confiance s'appuiera sur une base de cognitions communes composée « d'un ensemble d'informations et de croyances, de préjugés et par des processus d'apprentissage » pouvant donc comprendre des valeurs. Enfin, ces éléments pourraient être fournis par l'une des parties prenantes de la relation de confiance aux autres, au début de leur interaction, afin de sceller les bases d'une relation ultérieure.

Cette dernière définition de la confiance est la plus en phase avec la nature du terrain de recherche, à savoir la confiance dans les organisations intervenant en situations extrêmes. En effet, l'émergence de la confiance dans l'organisation est impérative compte tenu de la vulnérabilité et des risques inhérents aux situations dans lesquelles les agents évoluent. Cette interaction apparaît notamment dans les travaux de Lièvre (2004, 2008) et d'Arena, Oriol et Pastorelli (2013), qui ont analysé des organisations travaillant dans un contexte à forte incertitude (i.e. les expéditions polaires, les traders en salle de marché, la prise de décision dans le milieu aéronautique, le milieu de l'alpinisme).

En outre, comme l'ont développé Bernoux et Servet (1997), la confiance pourra s'entendre comme « fondée sur des éléments affectifs et intuitifs ou sur un ensemble d'informations et de croyances, et par des processus d'apprentissage face à un environnement physique, un individu, un groupe de personnes, ou une organisation, et dont la

connaissance permet d'anticiper avec un degré plus ou moins élevé d'incertitude leur devenir ou leur réaction ou comportement dans telle ou telle situation ». C'est la définition qui sera retenue pour la suite de la présente étude.

Il apparaît que certaines organisations, pour renforcer leur efficacité, leur contrôle sur les agents et se protéger des influences extérieures, cherchent à maîtriser différents niveaux de confiance. Cette démarche semble s'apparenter à une tentative de maîtrise des trois processus développés par Zucker, à savoir le process-based trust, le characteristic-based trust et l'institutional-based trust. Dans ce travail, la résistance et l'efficacité d'une combinaison itérative des confiances seront étudiées, en matière de protection des agents. Il y aura donc lieu de présenter l'organisation de la structuration et de l'architecture de cette combinaison itérative, de cette superposition de confiance.

1.3. La confiance au sein des organisations intervenant en situation extrême

Ces différents éléments constitutifs de la confiance ont été perçus par nombre d'organisations. C'est notamment le cas de celles dotées d'une longue expérience d'interventions dans des situations extrêmes où l'incertitude est forte, et où la vulnérabilité peut se concrétiser tout particulièrement en portant atteinte à l'intégrité physique.

Aussi, pour sécuriser leurs opérations, certaines organisations cherchent-elles à agir sur l'interconnexion des différents niveaux de confiance. Des entretiens menés au sein de l'organisation en amont de cette étude ont montré une superposition des strates de confiance entre les différents niveaux hiérarchiques. Il apparaît que l'emboîtement des niveaux hiérarchiques crée une dynamique susceptible d'impacter la confiance accordée

par les agents à leurs groupes ainsi que la confiance accordée à l'institution et au Gouvernement. Tout particulièrement, cette interdépendance est censée renforcer la confiance globale et agir comme un bouclier contre des interventions extérieures à même d'altérer le lien de confiance par l'apparition d'éléments cognitifs divergents. L'objectif serait donc de protéger grâce à cet emboîtement les strates raisonnées et surtout irrationnelles de la confiance, donc cognitives et affectives comme développées par Shapiro (1992), MacAllister (1995, 1997), Lewicki et Brunker (1996), Rousseau et al (1998) et reprises dans la définition de Bernoux et Servet (1997).

1.3.1. L'exercice de la confiance envers les différents niveaux

Pour sécuriser leurs processus et le mode d'intervention de leurs équipes, certaines organisations ont travaillé à développer cette combinaison itérative de la confiance. Il apparaît que deux niveaux s'y croisent, à savoir les principes sur lesquels se fondent la confiance et les niveaux hiérarchiques constitutifs des strates de confiances (voir tableau 1). Leurs traductions avec leurs corollaires de niveaux hiérarchiques seraient la suivante :

– Une première strate serait construite sur l'aspect affectif, basée sur les liens interpersonnels, et renforcée par la validation de l'expérience empirique et d'un vécu commun qui pourraient tout autant renforcer des cognitions communes. Cela renvoie clairement à des liens affectifs, comme exposé dans les écrits doctrinaux relatifs à la confiance. Il s'agirait pour l'organisation d'une vision micro se rapportant au groupe.

– Une seconde strate serait fondée sur les éléments cognitifs notamment acquis au cours de la formation se rapportant à l'institution même. Ces éléments participeraient à construire non seulement une identité commune, mais encore une base permettant

d'anticiper l'action de l'autre, comme présenté dans les définitions précitées. En outre, ces données cognitives fournies par l'organisation permettraient de construire une base commune à partir des éléments choisis et, par conséquent, plus facilement mobilisables par la suite. Il s'agirait là d'une vision méso touchant la hiérarchie, et par continuum, l'organisation.

– Une troisième strate s'appuiera sur le volet intuitif de l'individu, en se rapportant à la confiance donnée intuitivement à la superstructure d'appartenance comprise au sens de l'État. En effet, la confiance sera plus facilement accordée à une structure connue dès l'origine, dans laquelle l'individu pourra se retrouver grâce à des facteurs aussi prégnants que, par exemple, la reconnaissance linguistique. Cette assertion s'appuie notamment sur les recherches réalisées en psychologie sociale desquelles il ressort que les individus appartenant à une même catégorie sont spontanément plus loyaux envers les autres membres de leur groupe d'appartenance qu'avec des individus qui y sont extérieurs.

De prime abord, il sera donc plus facile d'avoir foi en son pays que dans un État étranger. En ce sens, ce niveau de confiance fait écho aux travaux d'Offe pour qui les institutions génèrent — ou a minima facilitent — la confiance, car, tous les intervenants vivant dans le même cadre institutionnel, ils sont imprégnés de normes communes auxquelles ils adhèrent. Ils peuvent donc s'engager en leur faveur et s'obligent mutuellement à s'y conformer. De facto, chacun parie sur l'adhésion des autres, même sans les connaître individuellement. Parce que ces normes sont partagées (et diffusée par l'institution) l'individu peut partir du principe que cet attachement commun fait de chacun un partenaire potentiel digne de confiance. Il s'agit là d'une vision macro référant à la superstructure représentée par le volet étatique.

Dans certaines organisations, le volet micro peut même faire l'objet d'une subdivision supplémentaire. Dans cette configuration, les personnels de l'organisation sont supposés jouir d'une forte confiance en eux notamment à la lumière de la sélection très exigeante subie pendant leur recrutement, que ce soit sur le plan de connaissances ou d'aptitudes physiques.

Dans l'idéal, les différentes strates de confiance auraient pour résultat de se renforcer mutuellement. De fait, cette « superposition » permettrait non seulement de ne pas donner de prise à l'incertitude et au doute ; elle pourrait également servir de ressort en cas d'actions à mener dans des situations extrêmes. Ainsi, l'organisation serait sécurisée dans l'accomplissement de sa mission et dans le déploiement de sa stratégie. En faisant écho aux définitions précédemment citées, cette combinaison itérative renforcerait la volonté délibérée d'être vulnérable aux actions d'une autre partie, notamment parce que ces strates permettraient de transformer l'espérance, évoquée par Mayer & al, en la certitude du bien-fondé de l'action choisie. En effet en renforçant une base commune d'éléments cognitifs et affectifs, tels qu'identifiés par Bernoux et Servet (1997), la confiance serait mécaniquement et proportionnellement également renforcée.

Enfin, si ces différentes strates partagent un ensemble de valeurs communes, les organisations peuvent légitimement espérer que la vulnérabilité décrite par Zand (1972) et Deutsch (1962) ne sera pas perçue comme un facteur de dissension, mais, au contraire, comme un vecteur de cohésion fondé sur la compréhension et une culture mutuelle. Cela permettrait de donner l'impression d'un réel souci du bien-être de l'agent (puisque reconnu comme identique à la hiérarchie) tout en réduisant l'éventualité des comportements opportunistes, tels que ceux décrits par et Barber (1983), Ouchi (1981) et Mishra

(1996). De même si le discours officiel se structure autour d'éléments discursifs communs, alors l'impression de fiabilité et de cohérence sera renforcée, augmentant ainsi la crédibilité définie par Kirkpatrick et Locke (1991).

Le présent article s'attachera à vérifier cette proposition relative à des strates, des combinaisons itératives, intervenant à la croisée des fondements de la confiance (affectif, cognitif et intuitif) et des différents niveaux hiérarchiques.

	Niveau micro (groupe)	Niveau meso (institution)	Niveau macro (gouvernement)
Affectif	**X**		
Cognitif		**X**	
Intuitif			**X**

Tableau1. Représentation de la structuration de la confiance. Source : C. Dugoin-Clement

1.3.2. La combinaison itérative de confiance comme atout de coordination

Le sujet de la confiance a été investi par les sciences de gestion avec un engouement fort, tout particulièrement en ce qu'elle était perçue comme un vecteur potentiel de coordination de coopération. Pour Thompson (1967), la confiance pourrait être une méthode efficace pour gérer les interdépendances grâce aux ajustements mutuels qu'elle

autorise. Elle pourrait alors suppléer aux règles et méthodes traditionnelles de coordinations dont l'efficacité décroît avec la montée de l'interdépendance (Thompson, 1967 ; Wicks & al, 1999). À ce titre, on peut relever que la dissuasion pourrait décroître — au moins partiellement — avec la montée de l'indépendance des agents. En effet, l'indépendance affaiblit le contrôle nécessaire à la mise en place de potentielles punitions en cas de manquement à la règle.

Cet éclairage permet donc de penser que la confiance est particulièrement efficace en terme organisationnel dans une structure où la relation interpersonnelle, mais aussi informelle, est forte, par exemple dans les structures claniques au sens d'Ouchi (1980).

Pour autant, la relation informelle garantit-elle la naissance de la confiance ? Selon Aoki (1988) et Lazega (2001), cela ne serait pas suffisant, et le contrôle de la communauté resterait nécessaire. Rapporté à notre propos, et au cercle de la confiance micro, relatif au groupe, il faudrait donc un contrôle du groupe lui-même. Dans le cas où les différents membres de ce groupe disposent d'une certaine autonomie et sont appelés à travailler dans des milieux stressants et incertains, comme des situations extrêmes, cette volonté de rétrocontrôle pourrait être encouragée par la nécessité de protéger tant son intégrité physique propre que celle des autres. En outre, le partage de valeurs communes socialement considérées comme positives pourrait être un facteur permettant de reconnaître en l'autre un semblable, et d'accroître d'autant la possibilité de nouer une confiance personnelle et affective avec lui : la confiance clanique permettrait d'exercer une « une domination douce » (Courpasson, 2000). De plus, si ces valeurs sont inculquées dans le cadre d'une formation, se référant donc à la sphère cognitive, il est probable qu'elles puissent faire l'objet d'une appropriation par celui à qui on les a ensei-

gnées. À ce titre, elles pourraient même devenir parties intégrantes de la perception que le sujet a de lui-même et se muer en éléments affectifs et non plus cognitifs.

Il reste que l'organisation — surtout si elle est importante d'un point de vue numéraire — ne peut pas uniquement se reposer sur des leviers ayant en commun de s'appuyer sur une coopération non contrainte par des instruments formels dans l'exécution de tâches complexes, exigeantes et pouvant intervenir dans un créneau de temps très contraint. En effet, ce mode de gestion présenterait un risque bien trop important pour la bonne exécution de consignes à exécuter dans un ordre précis et avec un chronométrage strict ne laissant aucune place à un temps d'hésitation causé par un doute ou une incertitude. A minima, ce mode de contrôle pourrait être en contradiction relative avec la mise en place d'une tactique précise et minutée, donc conçue sur la base de règles strictes, voire inamovibles. Cela sera encore plus patent dans le cas d'une planification stratégique à long terme impliquant un grand nombre d'acteurs. Pour autant, intervenir dans des situations extrêmes ne permet pas de faire l'économie de la confiance.

Fort de ce constat, une tentative de mise en place de confiance dans un cadre plus strict et directif est mise en place par nombre d'organisations afin d'optimiser la coordination. Le développement de la confiance s'appuie alors sur des apprentissages et connaissances apprises. Le fil d'Ariane de cette méthode consiste à s'appuyer sur un ensemble d'éléments cognitifs communs qui deviendront progressivement des éléments affectifs constitutifs de la personnalité des membres du groupe micro, où se retrouvera une confiance clanique.

Enfin, dans le but de sécuriser l'exécution des tâches confiées, l'organisation pourra inscrire ses éléments cognitifs forts dans une suite de symboles et d'éléments supérieurs permettant instinctivement de créer un lien de confiance. À ce titre, les éléments et

symboles fédérateurs en lien avec la Nation pourront être de réels facilitateurs. En outre, ces éléments étant également socialement considérés comme positifs et à l'origine de certaines des valeurs déclinées dans les éléments cognitifs transmis, puis devenus affectifs, on peut supposer que cette juxtaposition de strates s'apparentera à une spirale positive. Ainsi, par la superposition de strates de confiance, l'organisation pourrait s'assurer à la fois de la bonne coordination de l'exécution des ordres en situation extrême. En outre, cela assurerait l'acceptation par le groupe de stratégies globales pensées par l'organisation et impliquant l'édiction de règles strictes, contraignantes, comprenant le cas échéant un volet coercitif. Au-delà de l'acceptation de règles, cette superposition des confiances pourrait permettre d'éradiquer les doutes quant au bien-fondé des décisions prises. Enfin, cette superposition, où toutes les couches se renforcent mutuellement par effet d'entraînement, aurait pour effet de protéger les membres de l'organisation de l'influence d'informations extérieures pouvant altérer la coordination des opérations. Dans cette hypothèse, une information dissonante par rapport à la stratégie globale ne pourrait être reçue positivement et serait corrélativement dans l'impossibilité d'engendrer une rupture de confiance entre l'individu et sa hiérarchie. La seconde proposition de cet article est que la combinaison itérative des confiances, cet enchevêtrement de strates de confiance, permettrait à l'organisation d'assurer à la fois le maintien de la coordination en son sein et la sécurisation de l'exécution des ordres dans des situations extrêmes.

2. Étude de cas

Une étude a été menée sur une organisation évoluant en situation extrême. Ce choix a été fait, car ce type de structure est un terrain idéal pour vérifier les phénomènes de su-

perposition et de renforcement de la confiance au vu de la nécessaire coordination des équipes que cela soit pour assurer le bon déroulement de la stratégie de l'organisation ou pour assurer leur propre sécurité. En effet, la définition de la situation extrême exige que celle-ci soit non seulement imprévisible et changeante, mais également risquée. Dans le cas où le risque est physique, la perception de ce dernier est encore augmentée auprès des agents qui y sont confrontés ce qui rend leurs réactions d'autant plus fortes. L'objet de ce travail n'était pas été de réaliser une mesure de la confiance. Non seulement les mesures sont encore sujettes de débats — certains la considèrent comme une variable unidimensionnelle (Tsui et al. 1997 ; Robinson et Rousseau, 1994), d'autres multidimensionnelle, - mais encore il n'y a pas de consensus sur le nombre d'aspects à retenir pour mesurer la confiance. Certains auteurs, comme McAllister (1995), retiennent deux aspects alors que d'autres en préconisent 52 comme Clark et Payne (1997). L'objet de cette étude exploratoire, qui s'inscrit dans un processus de recherche plus large est, au travers d'entretiens qualitatifs, de définir si cette superposition de confiance, cette combinaison itérative, mise en œuvre par l'organisation, atteint ses objectifs de renforcements mutuels, renforçant ainsi la sécurisation des personnels et des stratégies mises en œuvre par l'organisation. Un autre objectif est de définir si ce contexte participe à l'accroissement de la coordination ou si, au contraire, ces confiances superposées en concurrence, voire en conflit entre elles, pourraient provoquer les effets opposés à ceux initialement recherchés.

2.1- Méthodologie

Pour évaluer si la superposition des confiances décrites ci-dessus peut être à la fois harmonieuse dans la coexistence des confiances et efficace en matière de protection face à l'apparition du doute et de l'incertitude engendrés par l'exposition à des informations extérieures et d'optimisation de la coordination, des entretiens ont été menés auprès des membres d'une organisation évoluant en situation extrême.

Pour ce faire, plusieurs interviews semi-dirigées ont été conduites au sein de l'armée française dont les personnels sont couramment appelés à intervenir dans des situations extrêmes. Le choix de conduire une étude qualitative répondait à la nécessité de rentrer dans une granularité fine au regard de la définition de la confiance. En effet, il s'agissait d'atteindre un niveau de détail permettant de faire la différence entre le discours relatif à la confiance et les pratiques s'y rapportant chez les sujets interrogés. Il est apparu que des entretiens longs et semi-directifs, laissant beaucoup de liberté aux personnes entendues pour illustrer leur propos avec des exemples précis, permettaient d'aller au-delà des conventions sociodiscursives régissant les façons culturellement et socialement acceptables de parler d'individus ou d'institutions. Partant du principe que ces conventions ne sont vraisemblablement pas en lien avec les pratiques de la confiance et de la défiance, un échange long permettait de contourner ce biais.

En outre, la première strate de confiance revêtant un aspect affectif, il semblait cohérent de travailler sur la base d'échanges aussi libres que possible, car ils sont plus aptes à créer un lien de confiance entre l'auditeur et les personnes interrogées. Dans ce même objectif et pour pouvoir obtenir des échanges francs, le respect d'un anonymat strict et l'engagement de ne pas communiquer les échanges ont été assurés aux personnes interviewées. Ces entretiens ont été encodés avec le logiciel Nvivo. Cet encodage a permis

de mettre en exergue, au travers du rattachement à des nœuds issus de l'analyse du cadre théorique, le sens profond des entretiens et de conforter les propositions en en vérifiant certains aspects, voire de participer à en qualifier les résultats.

2.1.1- Échantillon des sujets

L'option retenue étant de s'attacher à des définitions de la confiance en lien direct avec l'incertitude et le risque, le choix a été fait de sélectionner une organisation évoluant en situation extrême par nature. Concernant les 17 sujets interrogés, afin que les résultats soient le plus probants possible, il a été demandé de rencontrer des personnels disposant tous d'une expérience forte en situation extrême. Leurs vécus étaient comparables : les missions auxquelles ils avaient pris part étaient quasiment similaires et avaient eu lieu dans des théâtres d'opérations de même nature. Il reste que, si nous avons choisi d'interroger des sujets disposant d'expériences similaires et représentatives dans des situations comparables, il existe cependant un effet type des situations extrêmes à partir du moment où l'incertitude est forte, la prédictibilité faible et que le risque est réel et présent.

Le thème de la recherche a été présenté de façon collective puis les entretiens se sont tenus individuellement. Afin de correspondre à des profils sensibles au développement de la confiance horizontale ou clanique, le profil des sujets échantillonnés était homogène au regard de leurs fonctions, tous appartenant au niveau de l'exécution ou au management de proximité.

En ce qui concerne l'âge des personnes interviewées, le panel comprenait 3 membres de la génération « x » disposant d'une expérience opérationnelle forte (ils représentent l'échantillon du groupe A) et quatorze personnes appartenant à la génération « y » dont

11 avaient une expérience en situation extrême (ces 11 sujets représentent l'échantillon du groupe B). Enfin, présupposant que l'action dans des situations extrêmes où l'incertitude est forte pouvait avoir un impact fort sur les confiances, un échantillon de 3 personnes n'étant pas intervenues en situation extrême, représentant la génération « y », a également été utilisé comme contrôle (ces trois sujets sans expérience opérationnelle représentent l'échantillon du groupe C). Si l'échantillon de contrôle paraît numériquement faible pour une recherche quantitative, il est rappelé que la représentativité statistique n'est pas recherchée dans un travail qualitatif (Borges da Silva, 2001). En effet, l'objectif n'est pas d'avoir une représentation moyenne de la population, mais d'obtenir un échantillon de sujets ayant vécu des expériences particulières ou possédant une caractéristique précise à analyser.

2.1.2. Déroulé des entretiens et traitement des données

Les entretiens n'étaient que semi-directifs : ils comprenaient des questions génériques et ouvertes, définies en accord avec le cadre conceptuel développé précédemment (voir tableau 2). L'objectif était d'apprécier si les propositions faites étaient validées ou invalidées par le déclaratif de sujets non influencés par l'auditeur ou la formulation de ses questions. Ainsi, au cours de ces entretiens semi-directifs, certaines interrogations étaient formulées de façon récurrente afin de permettre un traitement optimal des données recueillies. À ce titre, plusieurs questions relatives à la nature des différentes confiances éprouvées étaient posées (i.e. dans le groupe, dans l'institution et dans le gouvernement). En outre, les militaires interrogés ont été invités à noter leurs confiances dans les différents niveaux précédemment définis sur une échelle de type Likert graduée de 0 à 5.

L’étude s’interrogeait également sur le degré de résistance qu’une dynamique harmonieuse des confiances pouvait créer face à des influences extérieures. Celles-ci pouvant intervenir par différents canaux, notamment dématérialisés, les sujets étaient invités à préciser la nature de leur mode de consommation de l’information et la confiance qu’ils leur accordaient. Il leur était également demandé de dire s’ils estimaient que leur point de vue ou leur confiance avait pu évoluer après qu’ils ont pris connaissance d’une information. Ils étaient également priés de noter ces différents médias, toujours sur une échelle de Likert. Enfin, les sujets étaient appelés à s’exprimer sur un éventuel changement dans l’appréhension de leur métier, des missions qui leur étaient confiées et de leur organisation après avoir été en contact avec des informations.

Tableau 2. Thèmes abordés dans les entretiens et échelle d'évaluation de la confiance

Les thématiques recouvraient une grande variété d'échanges en fonction des sujets, l'entretien n'étant que semi-dirigé. En outre, les entretiens oscillaient entre 45 min à 2 h démontrant la variété de l'amplitude des réponses collectées.

1— Motivation pour le choix professionnel initial (présupposé sur la nature de l'emploi des relations au sein de la structure…)
2— Confiance au niveau micro/relation au sein du groupe (avec demande de quantification sur échelle de Likert, description de la nature de la confiance si la confiance est évoquée, utilité de celle-ci. Si la thématique des valeurs est abordée par le sujet, quelles sont-elles, description, utilité)
3— Confiance au niveau méso/relation à l'institution (avec demande de quantification sur échelle de Likert, description de la nature de la confiance si la confiance est évoquée, utilité de celle-ci, si la thématique des valeurs est abordée par le sujet, quelles sont-elles, description, utilité)
4— Confiance au niveau macro/relation aux structures gouvernementales, hors perception partisane l'institution (avec demande de quantification sur échelle de Likert, description de la nature de la confiance si la confiance est évoquée, utilité de celle-ci, si la thématique des valeurs est abordée par le sujet, quelles sont-elles, description, utilité)
5— Rapport à l'information (canaux utilisés, raison de ces choix, explication de la motivation. Interaction entre information et différents niveaux de confiance. Puis demande de quantification de la confiance dans les différents canaux médiatiques consultés sur une échelle de Likert de 0 à 5)
6— Interaction entre éléments extérieurs et différents niveaux de confiance (changement de point de vue, de confiance accordée aux différents niveaux, si oui pour quelles raisons, perception de changement de point de vue)
7— Quels moments forts de la carrière (nature, changement suite à cet évènement dans la confiance, si oui, de quelle nature)
8— Question sur le choix professionnel à l'instant « T » (par l'intermédiaire de questions du type « aujourd'hui feriez-vous les mêmes choix ? », « avez-vous envisagé de changer de carrière ? ». Selon les cas, quelles sont les motivations pour ce choix)
9— Derniers éléments à avoir engendré une réaction affective, quelle que soit sa nature

Quantification de la confiance : À chaque fois qu'il leur était demandé de quantifier la confiance dans les trois groupes cités ci-dessus, il était précisé que « 5 » représente la confiance la plus forte et « 2,5 » correspond à « ni méfiant ni confiant ». Afin de rentrer dans le détail, il était demandé de préciser, de qualifier cette confiance, en laissant l'opportunité de s'appuyer sur des exemples.

Tableau des thèmes abordés dans les entretiens et échelle d'évaluation de la confiance

L'objectif était de vérifier la réalité des différentes strates présentées supra. Il s'agissait également de voir si celles-ci avaient une dynamique vertueuse et concouraient à se renforcer mutuellement pour accroître la confiance. En outre, cette étude s'interrogeait sur le renforcement possible de la combinaison itérative comme facteur de coordination accrue. Les éléments ainsi collectés ont été traités avec Nvivo 12 et avec Excel.

2.2. Données collectées

Les interviewés ayant été divisés en trois groupes distincts l'analyse est restituée en fonction de cette subdivision, et en relation avec les interrogations concernant le renforcement mutuel des confiances comme acteur d'efficience, de coordination et de résistance à de potentielles influences extérieures.

3. Analyse des résultats

Les résultats ont été analysés avec Excel pour les données quantitatives, et avec Nvivo 12 pour les données qualitatives. Pour ce faire, un encodage en relation avec les thématiques traitées dans cet article a pratiqué. À titre d'exemple, des nœuds ont été créés sur les différents niveaux de confiances abordés, à savoir micro pour le groupe, méso pour l'institution et macro pour le gouvernement. Ces nœuds comprenaient une subdivision « positive » et « négative ». De même, les valeurs évoquées ont été encodées lorsque ce point a été abordé par les sujets. Les raisons motivant le choix professionnel des militaires entendues ont été encodées, ainsi que celles qui leur feraient refaire le même choix de carrière au moment de l'entretien ou qui, a contrario, les en dissuaderaient. À titre d'exemple, des phrases telles que *« Nos dirigeants ont peur de*

prendre leurs responsabilités » ou *« j'ai hâte de partir. J'ai pas envie de partir complètement blasé d'ici. »* ont été encodées comme une confiance négative. A contrario des phrases comme *« mon groupe, c'est vraiment une deuxième famille. Je donnerai tout pour eux, les yeux fermés* » ou « *Je veux dire si j'ai un problème quelconque dans ma vie, je sais que j'aurai des gens qui seront présents pour moi* » ont été codées au nœud « confiance micro -> positive ».

3.1. Analyse des résultats du groupe d'étude A et B

L'analyse des différents entretiens fait apparaître des écarts importants entre les confiances accordées aux différents corps structurels (à savoir, le groupe, l'organisation et l'État). Si le niveau micro correspond à l'hypothèse de départ et révèle une confiance de type clanique et affective, la symbiose espérée avec les niveaux méso – cognitif — et macro - strate intuitive — ne valide pas la proposition sur laquelle l'organisation a fondé son mode de management.

Dans le cas de la confiance micro accordée au groupe, il apparaît que les individus sont attachés à un socle cognitif commun insufflé par l'organisation.

Cependant, le lien interpersonnel, la coopération et l'évolution en situation extrême ont tendance à modifier la perception de ce socle constitué, notamment, de valeurs devenues parties intégrantes de la personnalité des sujets. Ainsi on observe une mutation d'éléments qui, initialement cognitifs, deviennent progressivement des éléments affectifs intimement intégrés à la personnalité des sujets interrogés. En ce qui concerne la notation, la confiance reste dans l'ensemble assez haute dans le groupe A, confortant ainsi le descriptif opéré pendant l'entretien, où des termes comme « famille » et « confiance absolue » reviennent de manière récurrente.

A contrario, la relation de confiance ressentie vis-à-vis de l'organisation ne soulève pas d'autant d'enthousiasme que celle du niveau micro. Si des facteurs tels que l'éloignement sont logiquement cités, ils sont négativement renforcés par la comparaison avec l'interconnexion forte entretenue au sein du groupe micro avec des phrases comme « *ils sont complètement déconnectés. C'est mon point de vue. On est dans le nôtre, ils sont dans le leur. Ils essayent peut-être de nous comprendre de temps en temps, mais ils n'y arriveront jamais. Parce qu'ils ne vivent pas ce qu'on vit, c'est tout…… Ils ne sont pas là, ils ne vivent pas avec nous.* »

Le concept de valeurs a naturellement émergé des entretiens alors qu'ils n'étaient pas une clef d'entrée de l'étude. À ce titre, alors que l'organisation pense qu'en inculquant ses valeurs aux individus elle obtiendra une identification du micro au méso - soit du groupe à l'institution, à la hiérarchie — les mots employés par les sujets pour parler de ces deux niveaux, tant dans le groupe A que B, fait au contraire apparaître une nette dissociation, tant dans la description analytique que dans le vocabulaire utilisé. Ainsi, les sujets parleront de « nous » pour le groupe par opposition à « eux », ou « ils » pour se référer aux membres de l'organisation des niveaux de management supérieurs. Leur faire remarquer que beaucoup des membres de leur hiérarchie ont un jour occupé la place qui est la leur à ce jour ne semble pas influencer leur jugement. Il semble qu'une barrière, qui peut aller jusqu'à être vécue comme une trahison, soit élevée dès la sortie du groupe.

Si les éléments cognitifs communs aux groupes micro et méso participent à un lissage, ils deviennent aussi facteurs de jugement. Alors mobilisée en termes de crédibilité (comme développé par Kirkpatrick et Locke) toute prise en défaut retentira fortement

sur la confiance accordée au niveau méso. A contrario, tout élément perçu comme étant en adéquation avec ces notions sera pris comme un facteur de renforcement de la confiance. Cependant, là où le premier niveau est affectif, le second niveau de confiance reste principalement structurel et assis sur le respect du cadre réglementaire, potentiellement coercitif, des contractualisations et conventions collectives.

En outre, l'impact des interventions en situations extrêmes semble renforcer l'autorisation que s'octroie le groupe pour juger l'organisation. En effet, en raison de la spécificité de leur nature, notamment à cause du danger encouru, les situations extrêmes vécues par les membres du groupe leur donnent le sentiment d'être les « vrais » dépositaires des valeurs communes, eux seuls — ou eux principalement — les ayant testées et validées en situation. Ainsi l'expérience empirique, doublée du glissement affectif, donne le sentiment aux membres du groupe micro d'être en capacité de juger avec justesse du respect de valeurs annoncées comme communes, creusant corrélativement un fossé grandissant avec le niveau méso.

Concernant le niveau macro, la confiance accordée est de nature bien évidemment différente en raison de la distance le séparant des sujets. Cependant, la distance physique, et l'inévitable manque de proximité sont acceptés. Mieux, elles peuvent même parfois devenir une justification, une excuse raisonnable expliquant des décisions parfois estimées en décalage avec la réalité de terrain. Enfin, le niveau d'exigence sera moins élevé en ce qui concerne les attentes de compétences techniques.

L'organisation est considérée par les membres du groupe comme constitué d'individus qui, par leur formation et leur parcours professionnel, ont une connaissance fine des besoins, des contraintes et des attentes des personnels d'exécution. Aussi, tout ce qui pourrait être considéré comme un manquement au niveau méso sera jugé bien plus durement

et ne bénéficiera pas de la compréhension qui profiterait au niveau macro, perçu comme non spécialiste par principe.

Cela se traduit dans la notation attribuée aux différentes confiances où les écarts sont bien moins importants entre le niveau macro et le niveau micro qu'entre le niveau méso et le niveau micro. Les résultats du groupe A donnent une note moyenne de confiance de 4 pour le micro, de 3 pour le méso et de 2 pour le macro, le groupe B lui obtient les moyennes de 5 pour le groupe, 3 pour l'institution et 2 pour le gouvernement.

Cependant, si la note du groupe A, relative au niveau micro, est plus faible que celle du groupe B, elle revêt une qualité supérieure et moins individualiste. En effet, là où le groupe A utilisera des termes comme, « confiance familiale », « confiance absolue » et tout le registre sémantique relevant de l'intime et de la famille, le groupe B parlera plutôt d'une utilité du groupe pour l'individu et d'une confiance contrainte par la nécessité de maintenir son intégrité physique et sa sécurité lors des missions confiées.

De manière générale, il apparaît que les valeurs que l'organisation a transmises dans la perspective de servir de liant entre les groupes passent à côté de l'objectif s'agissant de fidélisation et d'accroissement de la confiance. Bien plus, il semble qu'une « concurrence des confiances » se crée. La confiance micro devient une référence absolue, même si elle est parfois considérée comme perfectible notamment par les jeunes (cf. infra). Ainsi, les actions, décisions et prises de position de l'organisation et de l'État sont-elles analysées au travers du spectre de la confiance affective, toujours estimée supérieure tant qualitativement que quantitativement.

Pire, tout élément qui n'apparaît pas comme immédiatement positif pour le groupe, ou pour un de ses membres, peut potentiellement se traduire par une altération de la confiance accordée aux deux strates supérieures, la plus proche accusant le déficit le

plus important en raison de sa proximité. Enfin, la compétence et le partage des valeurs, supposés plus prononcés entre le niveau micro et la strate méso, amène à des jugements réciproques d'autant plus durs que l'excuse de l'éloignement n'existe pas. Cette perception négative peut aller jusqu'à un sentiment de trahison à l'encontre de l'individu, voire du groupe auquel il se sent appartenir.

Le tout premier niveau de confiance présupposé par l'organisation, à savoir la confiance en soi assurée par la sélection subie par ses subordonnés, ne semble pas davantage répondre aux attentes, tout particulièrement auprès des jeunes. Un des éléments qui revient de manière récurrente est que ces tests et le choix de cet emploi étaient justement un moyen de se prouver à eux-mêmes qu'ils disposaient d'une compétence et de capacités dont ils doutaient jusqu'alors.

3.2. Analyse des résultats du groupe C

Le groupe test était composé de militaires souvent de moindre ancienneté dans l'organisation et qui, à ce titre, n'avaient pas encore été confrontés à des situations extrêmes. La confiance qu'ils accordent au groupe s'écarte sensiblement de celle exprimée dans l'échantillon A et se rapproche de celle affichée par l'échantillon B (cf. supra). La note de confiance dans le niveau méso est comparable à celle ressortant des groupes A et B avec une moyenne de 4.

En revanche, ce groupe test affiche une différence très nette dans la perception qu'il a du niveau micro par rapport groupe A. Même si, à l'instar de l'échantillon B, le groupe reste le mètre étalon de la confiance sa nature, telle que la décrivent les qualificatifs qui lui sont attribués, diffère sensiblement. Dans ce groupe test, le collectif est perçu au travers de ce qu'il peut apporter à l'individu, et non à l'inverse. Il semble donc que l'indi-

vidualisme prenne le pas sur le collectif. Par contre, le fait notable est que la confiance dans l'institution continue d'égaler celle accordée au groupe, soit une moyenne 4, alors qu'elle est plus basse pour les groupes A et B. Dans l'échantillon C, seule la confiance dans le gouvernement est plus faible avec une moyenne 3. Sur ce dernier point, l'étude montre que les deux confiances accordées aux niveaux méso et macro sont en moyenne plus élevées que dans les groupes A et B. En effet, bien que le niveau macro reste lointain, comme cela avait été observé pour les groupes A et B, il bénéficie néanmoins d'un a priori favorable.

Concernant la confiance en soi des personnes entendues, le présupposé de l'organisation apparaît moins fiable que pour la catégorie précédente. S'ils estiment qu'on ne leur demandera pas de faire quelque chose qu'ils ne seraient pas en mesure de réaliser, il revient de manière récurrente qu'ils attendent de tester leurs qualités *in situ* pour peut-être affermir ou asseoir leur confiance en eux. À ce titre, leur perception du groupe est intéressante et se confond avec celle du troisième groupe dont il a semblé pertinent de reporter l'analyse au paragraphe suivant.

3.3. L'émergence des déterminants potentiels de renforcement de la confiance

L'analyse des entretiens fait apparaître un élément non envisagé avec précision dans les propositions initiales. Si les valeurs participent à la construction des différents niveaux de confiance, elles diffèrent en fonction de plusieurs facteurs tels que l'âge ou l'ancienneté. Ainsi c'est à la fois la perception des valeurs et leur partage qui peut être sujet aux plus grandes variations. Cette différence peut constituer une faille, un potentiel point de basculement.

En ce qui concerne la variable de l'âge, les échantillons étaient composés selon les générations « x » et « y » en présupposant qu'une sensibilité aux médias pourrait apparaître comme facteur d'influence de la confiance dans les résultats de ces groupes. Un troisième groupe était composé d'individus ayant suivi les mêmes formations, mais n'ayant pas encore été confrontés à des situations extrêmes. Une différence entre ce dernier groupe et les autres tient à ce que sa confiance dans l'institution est plus forte, ce qui peut signifier que la confrontation au terrain a un impact immédiat sur la confiance.

Cependant, un autre élément ressort de l'étude, à savoir la perception du groupe. S'il bénéficie toujours de la confiance la plus forte, il semble que la nature en est différente. Cet écart apparaît dans les groupes B et C rapportés au groupe A : la situation extrême ne pourra pas constituer un déterminant puisque le groupe B y a été confronté et non le groupe C. Pour ces deux groupes (B et C), la perception de la strate micro se fait au travers d'un prisme où l'individualité prend une place significative : le groupe est perçu comme un levier pour des intérêts personnels.

À titre d'exemple, interrogé sur l'aide représentée par le groupe dans la gestion du stress, et tout particulièrement sur le point de savoir si le groupe pouvait être un levier de diminution du stress, un des sujets a déclaré, de façon assez représentative des autres, que le fait de savoir que d'autres étaient plus stressés que lui, représentait pour lui une aide et que la circonstance que d'autres disposaient d'une moindre compétence au sein du groupe le rassurait. Apparaît ici clairement un effet pervers du groupe, loin de la cohésion imaginée dans la théorie d'Ouchi par exemple.

Ce trait se retrouve fortement dans le groupe C où, si les sujets estiment que le groupe est une nécessité absolue notamment pour réaliser les missions confiées à l'équipe, le

lien interpersonnel y est plus ténu et plus réduit. Ainsi dans les groupes C et B la différenciation entre « nous » et « eux » peut apparaître au sein même de leur groupe et ne plus être uniquement réservé à l'institution et à la hiérarchie. À titre de comparaison, si les membres des groupes A et B, qui affichent des confiances négatives dans les trois niveaux de confiance étudiés (soit une évaluation comprise entre 0 et 2,5 sur l'échelle à 5 degrés), ont un résultat comparable à l'égard de l'institution (donc du niveau méso), les membres des groupes B et C sont deux fois plus nombreux que ceux du groupe A à avoir une confiance horizontale négative (16 % contre 37 %).

3.4. Du basculement de l'équilibre de la dynamique de confiance vers l'incertitude : un virage cognitif ?

L'analyse des données présentées dans cette étude exploratoire met en avant un conflit entre les différentes strates de confiance chez les membres de groupe d'agents d'exécution placés dans des situations extrêmes. L'hypothèse de nombreuses organisations est que la combinaison itérative de plusieurs strates de confiances liées aux différents niveaux hiérarchiques (macro, méso et micro), fondée sur un partage de valeurs communes, permet d'accroître la fidélisation de leur membre et de sécuriser leurs processus, notamment en cas de situations extrêmes. Ce présupposé semble battu en brèche : loin d'assurer une pérennisation, ce schéma conduit à une situation paradoxale. En effet, l'équilibre parfait ne pouvant être atteint, l'une des strates prend le pas sur les autres, devenant alors la référence. Le fait que seule la confiance micro ait pu être testée de manière empirique par les personnes interrogées participe certainement au renforcement de cette dernière au détriment des autres. Cette théorie est en accord avec la vision d'Aronson et Thibodeau (1992) et de Stone Cooper (1999) selon laquelle les cognitions

d'un individu seront d'autant plus fortes qu'elles auront été validées par l'expérience, permettant ainsi d'en faire des éléments constitutifs de leur personnalité. De facto, le basculement du cognitif vers l'affectif des éléments forts sur lesquels s'est fondée la confiance représente un virage qui, survenu au fil du temps et à la faveur de l'expérience acquise par les membres du groupe, serait un des facteurs constitutifs de la mise en concurrence des confiances. Ce phénomène serait surtout à l'origine de l'émergence d'un mètre étalon défini au niveau micro, permettant de juger les autres strates et tout particulièrement l'échelon intermédiaire que représente l'organisation. Or la dynamique de renforcement des confiances, prise ici en défaut, était censée jouer un rôle de protection envers des éléments d'informations auxquels les membres de l'organisation pourraient être soumis, ou pourraient se soumettre (par exemple par l'entremise des médias alternatifs et autres sources accessibles sur Internet). Dans la configuration observée il est probable que cette fonction de protection soir inopérante.

En outre, au cas où des exécutants seraient assaillis par le doute, on peut légitiment redouter que les prescriptions de l'organisation ne soient pas suivies, ou le soient moins bien, ou encore dans un temps en inadéquation avec la planification. Pour s'assurer la parfaite exécution des consignes transmises, les organisations adoptant ce type de superposition de confiance parient sur l'effet cumulatif du respect de la règle, du contrat, d'un cadre potentiellement coercitif et de la confiance clanique et affective accordée au groupe. Cet ensemble serait au service d'une superstructure macro adoptant les mêmes codes et normes que les niveaux méso et micro. Or, si une des structures prend le pas sur l'autre et se pose en juge en se référant à sa propre échelle de valeurs, l'analyse critique qui sera faite des actions et demandes de la hiérarchie permettra l'instillation d'un doute ou d'une incertitude.

Conclusion

Bien que l'analyse qui vient d'être présentée s'inscrive dans un périmètre de recherche plus large, l'objectif de cet article était multiple. Il s'agissait d'abord de valider la proposition selon laquelle les différents niveaux de confiance entretenaient bien un lien en lien avec leur emboîtement. Ensuite, il convenait d'évaluer la mesure dans laquelle une dynamique entre ces différents niveaux de confiance permettait d'assurer leur coopération. Enfin, dans l'optique d'analyser les modalités de construction de la confiance sur la base d'un corpus de valeurs,

Cet article s'intéresse au phénomène du basculement de la confiance résultant de perceptions et de partages des valeurs différents en fonction de l'âge et de l'ancienneté.

Les données collectées auprès de militaires faisant partie d'équipe d'exécution, en prise directe avec les situations extrêmes, mettent en avant l'existence d'une dynamique des différentes strates de confiances. Cependant, elle met à mal la proposition selon laquelle cette dynamique participerait à un renforcement global. Au contraire, l'analyse des entretiens révèle l'apparition d'une concurrence des confiances en lieu et place d'une dynamique de renforcement. Pire encore, cette concurrence pourrait constituer un facteur d'aggravation du doute envers la strate intermédiaire, le niveau méso. En outre, au premier niveau — la strate du groupe — il semble qu'il y ait une évolution au regard de la perception et de la confiance que ses propres membres lui accordent. In fine, le fait d'intervenir en situation extrême paraît de nature à renforcer la confiance micro au détriment de la confiance méso.

Cette recherche permet également d'éclairer le lien entre les différents fondements de la confiance (affectif, cognitif et intuitif) et les niveaux hiérarchiques (du groupe, de l'institution et de l'État). En outre, s'il apparaît que la confrontation à des situations ex-

trêmes constitue un facteur d'accroissement de la confiance micro, une nouvelle catégorie est apparue de manière inattendue au sein du groupe. En effet, une tranche d'âge présente une mutation dans la nature de la confiance accordée au groupe, sans que cela soit en lien direct avec la participation à des situations extrêmes. À la suite de ces résultats, une analyse a été réalisée afin d'identifier les éléments cognitifs susceptibles d'amener des modifications comportementales chez les membres d'un même groupe. Par ailleurs, la corrélation entre la concurrence des confiances et la probabilité d'un changement d'opinion a été mise en lumière. Par extension, il serait pertinent d'engager une étude relative à l'identification des éléments cognitifs extérieurs susceptibles de jouer un rôle dans le renforcement de la supériorité de la confiance accordée par la strate micro au niveau méso.

À terme, ces diverses évolutions, renforcements ou affaiblissements de confiance, pourraient avoir un impact fort sur l'exécution des missions confiées à ses personnels par l'organisation sans que cette dernière ait pris la pleine mesure d'un risque dont elle s'estimerait protégée par la superposition de strates de confiance.

Enfin, un des objectifs d'une dynamique de renforcement des confiances était de prémunir les agents de l'organisation des influences extérieures. À ce titre, les résultats des entretiens concernant la possibilité d'interactions entre information et altération de la confiance sont intéressants : il a été demandé aux sujets s'ils pensaient avoir changé d'opinion et/ou de perception concernant leur métier suite à des informations qu'ils auraient vues ou lues. Or, sur l'ensemble de ceux qui ont répondu par l'affirmative, près de 37,5 % appartenaient au groupe B.

Enfin, les réponses des interviewés, aux interrogations portant sur leurs habitudes de consommations d'informations et de médias, montrent que s'ils regardent majoritaire-

ment la télévision pour y avoir les grandes lignes de l'information, tous vérifient l'exactitude du contenu des médias *mainstream* télévisuels sur Internet, notamment sur des blogs alternatifs et des plateformes de broadcast. Ces données confirment la pénétration de ce type de médias dans cette strate de population.

Enfin, parmi la majorité de ceux qui disent ne pas avoir confiance dans les réseaux sociaux, beaucoup les citent néanmoins pour confirmer la véracité de leurs réponses aux questions de l'auditeur utilisant, par exemple, des phrases telles que : « *on voit bien que c'est partout pareil, il n'y a qu'à regarder sur les réseaux sociaux* ». Ce point fait ressortir la contradiction profonde qui existe entre l'affirmation, appuyée par des arguments structurés, d'une confiance très limitée à l'égard des réseaux sociaux et, par ailleurs, le discours qui indique que ces mêmes médias sont utilisés pour avérer la réalité des faits. À la lumière de ces éléments et de la proposition concernant le phénomène de construction de la confiance, il apparaît qu'un affaiblissement du corpus fondateur pourrait entraîner un déclin de la confiance. Une telle évolution accroîtra la perméabilité de l'organisation à des phénomènes extérieurs (notamment informationnels véhiculés par l'intermédiaire des réseaux sociaux, de blogs ou de contenus dématérialisés) susceptible d'affecter très négativement l'exécution d'un ordre. Ce constat appelle à approfondir la recherche au regard des risques encourus, s'agissant de leur ampleur et dans leurs natures profondes.

Références

Avenier, Marie Jose, and Aura Parmentier Cajaiba. 2012. “The Dialogical Model: Developing Academic Knowledge for and from Practice.” *European Management Review*, 9: 199—212. https://doi.org/10.1111/j.1740-4762.2012.01038.x.

Adams Barbara;, and Robert D.G. Webb. 2003. “Trust Developpement in Small Teams.” Recherche et développement pour la défense du Canada -Toronto. RDDC, N° CR 2003-016, 22

Allais, Maurice. (1955). *Fondements d’une Théorie Positive Des Choix Comportant Un Risque et Critique Des Postulats et Axiomes de l’Ecole Americaine.* Paris, Imprimerie Nationale, 1955. https://doi.org/10.2307/2342890.

Amodio, David M., Harmon-Jones, Eddie ;Devine, Patricia G. ; Curtin, John J. ; Hartley, Sigan L. and Covert, Alison E. 2004. “Neural Signals for the Detection of Unintentional Race Bias.” *Psychological Science ,* 15 (2): 88–93. https://doi.org/10.1111/j.0963-7214.2004.01502003.x.

Aoki Masahiko. (1988). *Information, Incentives, and Bargaining in the Japanese Economy.* New York: Cambridge University Press, 1988.

Arena, Lise, Oriol, Nathalie and Pastorelli Ivan. 2013. “Systèmes d’information et Gestion Du Couple Performance/Sécurité : Trajectoires Comparées de Trois Situations Extrêmes.” *Systèmes d’information & Management*, 18:87–123. https://doi.org/10.3917/sim.131.0087.

Aronson, Elliot. (1968). *The Cognitive and Behavioral Consequences of the Confirmation and Disconfirmation of Expectations*.” Harvard, Harvard University Press, 1968.

Aronson, Elliot. 1992. “The Return of the Repressed: Dissonance Theory Makes a Comeback.” *Psychological Inquiry,* 3 (4): 303–11. https://doi.org/10.1207/s15327965pli0304_1.

Auger, Pascale, and Reynaud Emmanuelle. 2007. “Le Rôle de La Confiance Dans La Gestion Du Risque d’incendie.” *Revue Française de Gestion,* 33 (175): 155–70. https://doi.org/10.3166/rfg.175.155-170.

Barratt, Ernest S. 2004. Impulsivity: Integrating cognitive, behavioral, biological, and environmental data. In W. G. McCown, J. L. Johnson, & M. B. Shure (Eds.), *The impulsive client: Theory, research, and treatment*. Washington, American Psychological Association. 2004, 39—56. https://doi.org/10.1037/10500-003

Bernoux Philippe, Servet Jean-Michel. (1998). *La Construction Sociale de La Confiance*. Paris Montchrestien, Association d’économie financière, 1998, 484.

Bhattacharya, Rajeev, Timothy M. Devinney, and Madan M. Pillutla. 1998. “A Formal Model of Trust Based on Outcomes.” *The Academy of Management Review* ,23 (3): 459. https://doi.org/10.2307/259289.

Boudon, Raymond. 2012. “Théorie Du Choix Rationnel Ou Individualisme Méthodologique ?” *Sociologie et Sociétés*, 34 (1): 9-34. https://doi.org/10.7202/009743ar.

Cabinet Deloitte. 2015. “Usages Mobiles Les Français et Le Smartphone En 2016 : Une Relation Fusionnelle.”

Chanut, Véronique, Guibert, Nathalie, Rojot, Jacques et Pierre-Louis Dubois.(2011) Les limites de la rationalité limitée? Un essai de reflexion en science de gestion. *Management et Avenir,* n°49, 97-117

Chakravarti, Ashok. (2013). *The Nature and Content of Aid. In Aid, Institutions and Developmen*t. Cheltenam/Northampton, Edward Elgar, 2013.https://doi.org/10.4337/9781845425524.00008.

Clarke Richard D. (2011). Cyber war: the next threat to national security and what to do about it. New York, Harper Collins, 2011, 304. https://doi.org/10.22456/2178-8839.20585.

Courpasson, David. (2000). *L’action Contrainte.* Paris: Presses Universitaires de France, 2000.

Department of Defense (US). 2010. “JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (As Amended Through 15 February 2016).” http://www.dtic.mil/doctrine/dod_dictionary.

Deutsch, Morton. (1962). Cooperation and Trust: Some Theoretical Notes. In M. R. Jones (Ed.), Nebraska Symposium on Motivation 275-319. Lincoln, NE: University of Nebraska Press, 1962.

Dumez Hervé. 2012. “Qu’est-Ce Que l’abduction, et En Quoi Peut-Elle Avoir Un Rapport Avec La Recherche Qualitative ?” Libelio D’aegis, 8-3, 3-9.

Elster, Jon & Gerschenfeld, Abel. (1986). *Le laboureur et ses enfants : deux essais sur les limites de la rationalité.* Paris : Les Éditions de Minuit, 1986, 208.

Etzioni, Amitai. 1961. *A Comparative Analysis of Complex Organizations On Power, Involvement, and Their Correlates*. The Free P. New York.

Eurostat. 2016. “Internet Activities in the Past Three Months by Age Group EU-28, 2016 (% of Internet Users).”

Festinger, Léon. (1957). *Cognitive Dissonance.* Stanford , Stanford University Press, 1957.

Friedman, Milton. (1953). The Methodology of Positive Economics In Daniel M Haussmann (eds) *The Philosophy of Economics: An Anthology*, Madison: Cambridge university Press, 1953.

Gareev, Makhmut. 2016. « How Does One Develop a Modern Army? » November 2016, *Krasnaya Zvezda* On line.

Geers, Kenneth Giles; Keir.; Wirtz, James .J; Lewis, James.A; Lebicki, Martin; Koval, Nikolay; Pakharenko, Glib; Weedo, Jen, et al. (2015). Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn, CCDCOE, 2015.

Gehring, William J., Goss, Brian ; Coles, Michael G. H.; Meyer, David E. and Donchin, Emanuel. 1993. "A Neural System for Error Detection and Compensation." *Psychological Science,* 4 (6): 385–90. https://doi.org/10.1111/j.1467-9280.1993.tb00586.x.

Giddens, Anthony. (1990). *The Consequences of Modernity*. Stanford, Stanford University Press, 1990.

Gilovich, Thomas; Griffin, Dale; Kahneman. Daniel. (2002). *Heuristic and biases: the psychology of intuitive judgement.* New York, Cambridge University Press, 2002, 882.

Godwin James B, Kulpin Andrey, Rauscher Karl Frederick, and Yaschenko Valery. (2014). *Critical Terminology Foundations 2 Chief Editors*. New York, The EastWest Institute, 2014, 76.

Greenberg Andy. 2017. "Hunting the Hackers: How Ukraine Became Russia's Test Lab for Cyber-war." *The Sydney Monring Herald*, June 20, 2017.

Harmon-Jones, Eddie, Brehm, Jack W. ;JGreenberg,eff ; Simon, Linda and Nelson, David E.. 1996. "Evidence That the Production of Aversive Consequences Is Not Necessary to Create Cognitive Dissonance." *Journal of Personality and Social Psychology ,* 70 (1): 5–16. https://doi.org/10.1037/0022-3514.70.1.5.

Harmon-Jones, Eddie, Harmon-Jones, Cindy ; Fearn, Meghan ; Sigelman, Jonathan D. and Johnson. Peter. 2008. "Left Frontal Cortical Activation and Spreading of Alternatives: Tests of the Action-Based Model of Dissonance." *Journal of Personality and Social Psychology,* 94 (1): 1–15. https://doi.org/10.1037/0022-3514.94.1.1.

Hootsuite, and We Are Social. 2017. "Special Reports Digital in 2017: Global Overview (Special Report)."

Jonas, Eva, Greenberg, Jeff and Frey, Dieter. 2003. "Connecting Terror Management and Dissonance Theory: Evidence That Mortality Salience Increases the Preference for Supporting Information after Decisions." *Personality and Social Psychology Bulletin,* 29 (9): 1181–89. https://doi.org/10.1177/0146167203254599.

Kahneman, Daniel., & Tversky, Amos. (1982). Intuitive Prediction: Biases and Corrective Procedures. https://doi.org/10.1017/CBO9780511809477.031

Kahneman, D., & Tversky, A. (1982). The Simulation Heuristic. https://doi.org/10.1017/CBO9780511809477.015

Kahneman, Daniel, and Beatty, Jackson. 1966. “Pupil Diameter and Load on Memory.” *Science,* 154 (3756): 1583–85. https://doi.org/10.1126/science.154.3756.1583.

Kahneman, Daniel; Tursky, Bernard, Shapiro David, and Crider Andrew. 1969. “Pupillary, Heart Rate, and Skin Resistance Changes during a Mental Task.” *Journal of Experimental Psychology ,* 79 (1 PART 1): 164–67. https://doi.org/10.1037/h0026952.

Kinzer Stewart, Nora. 1988. *South Atlantic Conflict of 1982: A Case Study in Military Cohesion.* Research Institute for the Behavioral and Social Sciences: Alexandria.

Klein, Gary.A. (1999). *Source of power how people make decisions*. Cambridge, MIT press, 2000, 352.

Lazega, Emmanuel. 2000. “Rule Enforcement among Peers: A Lateral Control Regime.” *Organization Studies,* 21 (1): 193–214. https://doi.org/10.1177/0170840600211003.

Lewicki, Roy J., and Barbara Benedict Bunker. (1996) Developing and Maintaining Trust in Work Relationships. In Kramer, R.M. and Tyler, T.R., (Eds.), *Trust in Organizations: Frontiers in Theory and Research*, Thousand Oaks, Sage Publications, 1996, 114-139. http://dx.doi.org/10.4135/9781452243610.n7

Libicki, Martin. (2009). *Cyberdeterrence and Cyberwar.* Washington, RAND Corporation, 2009, 214.

Lièvre, Pascal, and Anaïs Gautier. 2009. “Les Registres de La Logistique Des Situations Extrêmes : Des Expéditions Polaires Aux Services d’incendies et Secours.” *Management & Avenir,* 24 (4): 196. https://doi.org/10.3917/mav.024.0196.

Lièvre, Pascal. 2014. « Management Des Situations Extrêmes » In 25e Congrès de l’Association Francophone de Gestion Des Ressources Humaines, 12 mai 2014

Mayer, Roger. C., Davis J.ames. H., and Schoorman. David F. 1995. “An Integrative Model of Organizational Trust.” *Academy of Management Review,* 20 (3): 709–34. https://doi.org/10.5465/amr.1995.95080803

McAllister, Daniel 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/10.5465/2567

McAllister, Daniel J. 1997. “The Second Face of Trust: Reflections on the Dark Side of Interpersonal Trust in Organizations.” *Research on Negotiation in Organizations,* 6: 87-111.

Mishra Aneil K. (1996). Organizatinal response to crisis , the centrality of trust In T. R. Kramer, R. M., Tyler(Eds) *Trust in Organizations: Frontiers of Theory and Research*, London: SAGE Publications, 1996, 430. https://doi.org/10.2307/3857331.

Morewedge, Carey K., and Kahneman Daniel. 2010. » Associative Processes in Intuitive Judgment ». *Trends in cognitive sciences*. 14. 435-40. 10.1016/j.tics.2010.07.004.

Mullen, Brian, and Copper. Carolyn 1994. "The Relation between Group Cohesiveness and Performance: An Integration." *Psychological Bulletin,* 115 (2): 210–27. https://doi.org/10.1037/0033-2909.115.2.210.

Negroponte, Nicolas. (1995). *Being Digital.* New York: Alfred A Knops, 1995, 272.

Offe Claus. (1999). How Can We Trust Our Fellow Citizens? In *Institutionen, Normen, Bürgertugenden*. Cambridge, Cambridge Press University, 1999, 147-190.

Orléan, André. 1985. Hétérodoxie et incertitude, *Cahiers du CREA*, n°5, juin 1985, Ecole Polytechnique, 247-275.

Ouchi, William G. 2019. "Markets, Bureaucracies, and Clans." *In Management Control Theory*, 25:343—55. Taylor and Francis. https://doi.org/10.2307/2392231.

Rivolier, Jean. 1988. Stress et situation extrêmes. *Bulletins de la psychologie*, pp. 6-20

Robinson, Sandra L., and Rousseau. Denise M. 1994. "Violating the Psychological Contract: Not the Exception but the Norm." *Journal of Organizational Behavior,* 15, *245*—.259. https://doi.org/10.1002/job.4030150306

Rotter, Julian B. 1967. "A New Scale for the Measurement of Interpersonal Trust1." *Journal of Personality,* 35 (4): 651–65. https://doi.org/10.1111/j.1467-6494.1967.tb01454.x.

Rousseau, Denise M., Sitkin, Sim B.; Burt, Ronald S. and Camerer, Colin. 1998. "Not so Different after All: A Cross-Discipline View of Trust." *Academy of Management Review*.23, 3, 393-404. https://doi.org/10.5465/AMR.1998.926617.

Schaap, Arie J. 2009. "Cyber warfare operations: development and use under international law." *Air Force Law Review*, vol. 64, 121

Shapiro, Susan P. 1987. "The Social Control of Impersonal Trust." *American Journal of Sociology,* 93: 623–58. https://doi.org/10.2307/2780293.

Shapiro, Debra L., Sheppard Blair H., and Cheraskin Lisa. 1992. "Business on a Handshake." *Negotiation Journal,* 8 (4): 365–77. https://doi.org/10.1111/j.1571-9979.1992.tb00679.x.

Stone, Jeff, and Cooper Joel. 2001. "A Self-Standards Model of Cognitive Dissonance." *Journal of Experimental Social Psychology,* 37 (3): 228–43. https://doi.org/10.1006/jesp.2000.1446.

Thibodeau, Ruth, and Aronson Elliot. 1992. “Taking a Closer Look: Reasserting the Role of the Self-Concept in Dissonance Theory.” *Personality and Social Psychology Bulletin,* 18 (5): 591–602. https://doi.org/10.1177/0146167292185010.

Thompson James D. (1967). *Organizations in action.* New York: Mc Graw-Hill, 1967, 192.

Tsui, Anne S., Pearce, Jone L. Porter Lyman W., and Tripoli Angela M.. 1997. “Alternative Approaches to the Employee-Organizational Relationship: Does Investment in Employees Pay Off?” *Academy of Management Journal,* 40 (5): 1089–1121. https://doi.org/10.2307/256928.

Vaidis David, and Gosling Patrick. 2011. “Is Commitment Necessary for the Arousal of Informational Dissonance?” *Revue Internationale de Psychologie Sociale,* 23: 33–63.

Weedon, Jen. (2015). Beyond ‘Cyber War’: Russia’s Use of Strategic Cyber Espionage and Information Operations in Ukraine In Geers Kenneth (Eds) *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCDCO. Talinn, NATO CCDCOE, 2015.

Wicks, Andrew C., Berman Shawn L., and Jones. Thomas M. 1999. “The Structure of Optimal Trust: Moral and Strategic Implications.” *The Academy of Management Review,* 24 (1): 99. https://doi.org/10.2307/259039.

Zand, Dale E. 1972. “Trust and Managerial Problem Solving.” *Administrative Science Quarterly,* 17 (2): 229. https://doi.org/10.2307/2393957.

Zucker, L.G. 1986. “Production of Trust: Institutional Sources of Economic Structure, 1840-1920.” *Research in Organizational Behavior,* 8: 53–111.

CHAPITRE 4 : La problématique de l'information pour les organisations intervenant en situations extrêmes

Le chapitre précédent s'est attaché à analyser l'importance de la confiance appliquée aux organisations militaires amenées à intervenir en situations extrêmes. Ce chapitre pose la question de l'interaction, positive ou négative, pouvant exister entre l'organisation de structures confrontées à des situations extrêmes et l'information extérieure, non maîtrisée par la structure, mais à laquelle ses agents et personnels ont quotidiennement accès. En fonction du sens de la réponse, il s'agira alors d'en mesurer les impacts sur la gestion des ressources humaines de ces structures, tant en ce qui concerne l'appréciation du risque que l'efficacité des méthodes envisagées pour assurer la stabilité organisationnelle. En effet, il apparaît que, pour ce type de structure, la confiance est une condition déterminante de l'efficacité des modes opérationnels, entendus au sens de succès des missions confiées et de réalisation des objectifs assignés. À ce titre, ce chapitre est en lien direct avec des propositions formulées dans le chapitre 2 de ce travail[22]. Dans les premières observations exploratoires, il apparaissait que la confiance pouvait être altérée par les informations auxquelles les militaires étaient soumis.

Les organisations agissant en situation extrême élaborent leurs propres stratégies de communication à l'attention de leurs agents. L'objectif est notamment de développer des vecteurs porteurs de sens pouvant être un recours dans des situations qui, par la rapidité et l'imprévisibilité de leurs évolutions, et par les risques susceptibles d'en résulter, peuvent sembler manquer de lisibilité, être privées de sens et paraître chaotiques pour les person-

---

22. Les propositions sont respectivement:
7. L'impact des informations externes (particulièrement celles véhiculées par Internet) a des conséquences sur les pratiques quotidiennes de gestion des équipes des organisations évoluant en situations extrêmes
9. Impact de l'information sur la confiance et les valeurs
10 Valeurs comme protection des influence extérieur / garant de l'exécution conforme des consignes

nels y intervenant. Ce travail analyse si la communication de l'organisation est toujours aussi efficace que par le passé. Pour ce faire, cet article s'appuie sur diverses sources (observation, entretiens et documents) qui auront permis de valider ou d'invalider des propositions découlant des sous-problématiques traitées dans ce travail de recherche, comme présenté dans le tableau ci-dessous.

Avec l'arrivée d'Internet et des réseaux sociaux, les modes de consommation de l'information ont notablement évolué, modifiant en profondeur l'écosystème connu jusqu'alors. À la lumière de ce constat, ce chapitre pose la problématique de la protection que peuvent apporter les sites développés dans la communication institutionnelle. Il s'interroge également sur la capacité de résistance de cette communication verticale, sur son maintien de crédibilité face aux autres canaux de communications présents dans l'écosystème informationnel où évoluent les personnels, écosystème susceptible de devenir un réel « game changer ». Dans cet esprit, cette communication, présentée lors de la troisième journée de recherche organisée par le GREGOR et par le PRISM Sorbonne sur le thème de « La transformation digitale, ses enjeux pour les organisations et pour la recherche en management » le 11 septembre 2018, s'applique à analyser les impacts que les nouveaux modes de consommation d'informations peuvent avoir sur la gestion des ressources humaines d'organisations agissant en situations extrêmes.

Question de recherche	Dans un contexte de situations extrêmes soumis à une très forte pression de facteurs externes, en quoi la diffusion de certaines informations et le canal utilisé sont de nature à ne pas exécuter le ordre ou les décisions de la hiérarchie?			
DONNEES DE RECHERCHE				
Sous-Problématiques	Déclinaisons	Entretiens	Documen	Observations
Altération de la confiance et prise de décision	Il existe différents niveaux de confiance	V	NV	V
	Les cibles potentielles de ce type d'attaque n'ont pas conscience de pouvoir être visée	V	NV	V
Les valeurs et le renforcement de la confiance et des mécanismes de coopération	Les valeurs sont une protection contre des influence extérieures, elles sont garantes de l'exécution conforme des consignes	NV	V	NV
La perméabilité aux informations divergentes de celles délivrées par l'organisation	Internet et un vecteur efficace des opérations d'alteration de la confiance	V	V	V
	Le temps sur Internet influence sur l'efficacité des opération d'influence	NV	V	NV
	Les information venant de l'organisation résistent aux informations extérieures	NV	V	NV
	La communication institutionnelle de l'organisation n'est aussi efficace sur ses personnels que dans le passé	V	NV	V
	L'impact des informations externes (particulièrement celles véhiculées par Internet) a des conséquences prises en compte dans les pratiques quotidiennes de gestion des équipes des organisations évoluant en situations extrêmes	NV	V	NV
	L'ancienneté et l'exposition aux situations extrêmes participent à renforcer l'imperméabilité en accroissant la confiance entre les membres de l'organisation	NV	V	NV
	Il y a un impact de l'information sur la confiance et les valeurs	V	NV	V

Tableau représentant les sources utilisées pour valider ou invalider les propositions présentées dans le chapitre 4

Introduction

L'apparition d'Internet a changé nombre de paramètres dans la société. L'un d'entre eux touche directement à notre rapport au monde et à l'information. Depuis l'apparition en ligne du premier site lancé par le CERN en 1993, la toile s'est considérablement étendue. La naissance de Facebook en 2004, puis de YouTube en 2005, ont été des virages importants tant dans la communication que dans la perception de ce qu'est une information. Dans le sillage des réseaux sociaux et des plateformes de broadcast vinrent les blogs qui traitent une infinité de sujets. À titre d'exemple, lancer une recherche dans le navigateur Google avec les simples mots « blogs d'information » amène quelque 757 000 000 résultats. Cette déferlante dématérialisée a grandement modifié les canaux traditionnels, dit « mainstream » comme la télévision, la presse et la radio. De ce fait, ces canaux mainstream, outre leur production traditionnelle, ont ouvert des sites afin de pouvoir concurrencer l'afflux d'informations, ou d'éléments perçus comme tels, qui mettaient à mal leur modèle économique. Cependant, cet effort a-t-il été suffisant pour leur permettre de rester leaders dans la transmission d'informations ? Il semble que non si on se réfère à la confiance accordée aux médias traditionnels. En effet, selon le baromètre Kantar, moins d'un français sur deux utilise la télévision pour s'informer (48 %) au bénéfice d'Internet et seulement 41 % estiment que les journaux télévisés présentent les faits en conformité avec la réalité. Il en va de même pour les chaînes d'information en continu dont le crédit a chuté de 14 points pour ne plus atteindre que 30 %. Cependant, le web bénéficie d'un rapport ambigu en ce qui concerne la confiance et l'information. Ainsi 73 % des Français disent ne pas avoir confiance dans les informations qui circulent sur Internet. Ce vecteur reste néanmoins la principale source d'information

pour plus de 25 % des personnes interrogées, en hausse de 4 points par rapport à 2016[23]. Si on considère qu'une part non négligeable de la population estime que les sites d'informations alternatives, les blogs et les plateformes de broadcast sont fiables, il semble clair que la perception de l'information a subi une mutation profonde.

Enfin, la consommation de données mobiles réalisée avec les smartphones a permis d'accéder en tout temps et tout lieu à ces canaux d'informations, tout particulièrement pour les personnes des générations « Y »[24] et « Z »[25].

Rapporté aux organisations, ce changement implique que la traditionnelle communication descendante n'est plus la seule voie ni la seule vérité. À ce titre, les informations que l'organisation donne à ses membres — tant en ce qui concerne ses objectifs et motivations que la légitimité des méthodes employées pour réaliser les missions qui en résultent — peuvent venir en concurrence avec d'autres éléments d'information, le cas échéant en totale contradiction avec leur ligne interne de communication et leur stratégie RH globale. Dans ce contexte, la gestion RH de ces structures peut-elle être perturbée par une communication concurrente représentant une influence externe ? Au contraire, les campagnes classiques de prévention destinées à mettre en garde les membres de l'organisation envers Internet sont-elles suffisantes ? Cette supposition se verrait-elle renforcée pour les structures employant des personnels majoritairement jeunes (de la génération Y) et intervenant en situation extrême ?

---

[23] Baromètre 2017 de la confiance des français dans les médias, Kantar Public, Janvier 2018

[24] La génération Y est constituée de l'ensemble des personnes nées entre 1980 et l'an 2000. Elle est perçue comme ayant des comportements propres notamment en termes de consommation Internet et de caractéristiques.

[25] La génération z succède à la génération Y, on l'appelle aussi la nouvelle génération silencieuse ou génération C (pour Communication, Collaboration, Connexion et Créativité)

En effet, l'exercice professionnel en situation extrême présente plusieurs particularités. La première est liée à la nature même de ces situations : elles sont changeantes, imprévisibles et dangereuses (Lièvre, 2004, 2009). À ce titre, les personnels y intervenant doivent agir selon les consignes des organisations, sans avoir le moindre doute quant au bien-fondé des ordres transmis. Aussi une perturbation extérieure pourrait avoir des conséquences immédiates et délicates à absorber pour ce type d'organisation.

Enfin, si ces organisations interviennent régulièrement en situation extrême, les informations extérieures — particulièrement de celles véhiculées par Internet — auront-elles un impact sur les modes habituels de management et de gestion des équipes ?

À travers une série d'entretiens menés auprès de personnes correspondant aux caractéristiques mentionnées ci-dessus, l'article interroge ces propositions.

1. La communication sur Internet, les réseaux sociaux et les organisations

Avec l'arrivée d'Internet tel que nous le connaissons, nous sommes les témoins d'un fait innovant : la société civile est en avance, en termes d'usage du web, sur le monde de l'entreprise. En effet, les réseaux sociaux professionnels, initiés par des entreprises n'ont vu le jour que bien après ceux d'origine privée. Il en va de même pour les blogs et autre Twitter. Les premières organisations à avoir investi ce territoire sont les entreprises à but commercial. En effet, ce champ est rapidement devenu le prolongement de la relation client et l'occasion de mieux cerner la cible. Outre cette entrée dans le domaine d'Internet à visée de promotion de leurs produits, les entreprises ont eu à travailler sur les retours positifs, mais aussi — voire plus régulièrement — sur les retours négatifs reçus par l'intermédiaire des réseaux sociaux. Dès lors, ces entreprises se trouvaient

dans une posture de réaction, où elles pouvaient au mieux tenter de comprendre les raisons de ces réactions et manifestations.

On est ici bien loin de la traditionnelle communication d'entreprise qui avait pour objet de diffuser un message extrêmement contrôlé dans des médias choisis, ce qui permettait non seulement de maîtriser le contenu et la cible du message, mais en outre de ne pas se retrouver en concurrence avec d'autres messages potentiellement dissonants comme c'est aujourd'hui quotidiennement le cas.

Dans le cas de structures n'ayant pas un but commercial, mais de service ou d'intérêt général, la problématique est encore plus prégnante. En effet, la concurrence ne sera pas alors monétaire, mais quasi philosophique, et pouvant avoir des conséquences importantes quant à la gestion des ressources humaines et au management.

L'entreprise ou l'organisation devra rentrer en concurrence avec des réseaux déjà existants, fonctionnels et jouissants d'une fidélité de leurs utilisateurs qui véhiculent des idées ou des notions avec lesquelles la communication de l'organisation devra jouer.

2. Typologie des réseaux sociaux

Cet état de fait force à s'interroger sur la motivation qui pousse un individu à rentrer dans un réseau social. Selon certaines théories (Balagué Fayon, 2016), il s'agira d'un besoin d'appartenance à un groupe, quel qu'il soit. À ce titre, on pourra reconnaître différents réseaux sociaux plus ou moins spécialisés sur des centres d'intérêt ou des caractéristiques reconnues, par les consultants, comme représentatifs de leurs sensibilités. D'autres réseaux regrouperaient leurs membres sur des finalités partagées, il s'agira alors des réseaux plus généralistes de type Facebook, VKontacke. Enfin, appartenir à un

réseau social permet aussi de tendre à une certaine reconnaissance comme le fait remarquer Mercklé (2011) pour qui alors que l'individualisme ne cesse de se développer, les individualités sont face à un besoin de reconnaissance de plus en plus fort, que cela soit d'une communauté dématérialisée ne changeant pas le fait que le tout puisse avoir une valeur supérieure à celle de l'ensemble des parties.

Ces motivations peuvent permettre une approche facilitée pour des entreprises commerciales. En effet, une marque pourra tenter d'intervenir en créant des « fans » de son produit phare, ce qui, par là même, peut permettre de récolter des avis positifs en activant une dynamique de contagion « *bottom up* » et non plus *« top to bottom* ». En revanche, cette approche sera plus délicate à mettre en place pour une structure traitant avec de l'immatériel. Cela peut même s'avérer d'autant plus délicat si les champs d'action de ces organisations impliquent des changements irrévocables sur leurs milieux, notamment au niveau humain. Cependant, certaines de ces organisations ont créé une page Facebook pour gagner en lisibilité quant à leur popularité, notamment auprès de leurs employés adhérant à leur page ou choisissant de *« liker* » leurs nouvelles et leurs « *posts* ». Cependant, les motivations des « followers » pour ce type de structure, pourront largement différer de celles des 9 560 000 fans de Madonna.

Si, dans le cas d'une vedette, la motivation est principalement fondée sur l'engouement et la recherche d'information visant à satisfaire la curiosité provoquée par cet attrait, dans le cadre d'entreprises ou de structures, on pourra voir s'affronter différentes motivations. *In fine*, la participation à ce groupe pourrait venir nourrir une sorte de contrôle par l'internaute ayant pour objet de vérifier la concordance entre le propos publique-

ment porté par l'entreprise à laquelle il appartient et son vécu interne en tant que membre de cette structure.

A contrario, si l'objectif de l'organisation est de gagner en notoriété, par exemple dans l'idée de faciliter une campagne de recrutement, la toile de diffusion sera relativement complexe à appréhender. En effet, plusieurs théories ont cours : notamment celle du petit monde et celle des « hubs » des systèmes complexes.

La première fait référence aux travaux de Milgram en 1967. Lors d'une expérimentation, ce chercheur avait demandé à 296 personnes de transmettre à une seule et même cible un ensemble de documents en ne passant que par un réseau de connaissances. Au résultat, 217 personnes envoyèrent le dossier, 64 atteignirent la cible choisie en passant par une chaîne d'une longueur moyenne de 5,2 intermédiaires. En ressortit une théorie selon laquelle avec le petit nombre de six intermédiaires, on peut relier n'importe qui dans le monde (six degree theory). Si en 1967 la théorie essuya quelques critiques, le développement d'Internet relança cette théorie et les travaux de Barasbasi & Albert (2002) restreignirent le nombre de nœuds entre deux sommets à 4 en ce qui concerne les réseaux complexes non finis comme Internet. Dans leur travail, les auteurs notèrent que plus de 80 % des pages montraient moins de 4 liens alors qu'elles étaient moins de 0,01 % à en avoir plus de 1000. Fort de ce constat la recherche fut poursuivie et il apparut un effet de « hub » relié à de très nombreux sommets de nœuds, ce qui exclut une théorie aléatoire dans la création des réseaux.

Rapportées à la communication d'une organisation ou d'une entreprise, la démultiplication des ramifications des réseaux, leur intrication et leur ancienneté rendent difficile l'appréhension de l'effet que pourra avoir une action de communication dictée par une

stratégie globale visant l'atteinte des objectifs fixés, passant notamment par l'optimisation des ressources humaines dont l'organisation dispose.

3. Réseaux sociaux, communication et information : quelles conséquences pour l'entreprise

Avec les réseaux sociaux et plateformes de broadcast, c'est la circulation même des connaissances et informations qui ont été modifiées. Préalablement fruit d'un acte intentionnel (Powell et Grodal, 2005), les informations ou connaissances s'échangent et se diffusent maintenant par l'entremise de plateformes d'échanges libres et de partages volontaires sans même qu'il n'y ait obligatoirement de demande pour relier au contenu diffusé. Ainsi les connaissances deviennent des biens non plus individuels, mais collectifs prenant racine dans les divers réseaux qui leur permettent de se diffuser, voire de créer de nouvelles connaissances issues de la compilation et de l'entrecroisement des bribes d'informations comprises dans les différents réseaux (Antonelli, 2006).

L'objectif premier des réseaux sociaux est de répondre à cinq questions principales, à savoir : « Qui es-tu ? », « où es-tu ? », « que fais-tu ? », « pourquoi fais-tu ça ? » et « comment le fais-tu ? ». Ces réponses liées à l'activité individuelle et humaine doivent être saisies par des personnes morales dans une visée de communication, voire de fédéralisation autour de valeurs communes permettant le développement d'une cohésion de ses « employés followers » visant, par exemple, à accroître l'efficacité des modes opérationnels, donc l'atteinte des objectifs fixés par la direction.

Ainsi les entreprises se trouvent face à un dilemme complexe. Non seulement elles sont projetées dans un monde où l'efficacité de l'habituelle communication hiérarchique se délite au bénéfice d'une communication transverse, mais en plus elles n'ont que très peu de prise sur la contagion de l'information. Pire, leur communication et leurs actions peuvent être jugées à l'aune d'informations parallèles fournies à leurs personnels par des canaux tiers bien difficiles à reconnaître pour pouvoir en identifier les ressorts.

À titre d'exemple, si une campagne promotionnelle de recrutements est trop décalée de la réalité perçue par les membres de l'organisation qui suivent l'activité « on-line » de communication de l'organisation, le ressenti négatif de ces employés peut, par contagion au sein de leurs propres réseaux, atteindre d'autres membres de l'organisation. La conséquence pourrait être d'engendrer un mécontentement important dans le personnel vis-à-vis de l'employeur. Ce mécontentement né dans le monde dématérialisé « *on-line* » pourrait potentiellement avoir une traduction dans le monde bien réel « *offline* », par exemple par une « grève du zèle », ou un accomplissement des tâches confiées ne présentant plus la qualité attendue et précédemment connue.

Enfin, un autre problème peut tout à fait se faire jour et prendre une ampleur très gênante pour les organisations : il s'agit d'une diffusion non maîtrisée d'informations considérées comme sensibles. En effet, l'interconnexion des réseaux et des briques d'informations qu'ils transitent, issues du partage volontaire par des internautes de différents éléments, peut être à l'origine de « fuites » ou « leaks » d'information. Ce qui — exception faite des secrets de fabrication — peut avoir un effet bénéfique pour une entreprise commerciale, qui pourrait alors créer du « buzz » sur un nouveau produit, pourra avoir un tout autre effet sur une organisation étatique ne tenant pas à diffuser tout ou

partie de son activité notamment dans le cas de dossiers encore en gestations et loin d'être prêts pour une communication externe.

Autre cas de figure tout aussi délicat : comment percevoir l'influence que pourrait subir leur personnel sur Internet ? Comment connaître la nature des faiblesses pouvant en découler ? Il faudrait pour cela être en capacité d'auditer les usages de consultations de données ce qui irait à l'encontre de la réglementation en vigueur et en outre représenterait un travail de suivi et de traitement de données colossal. Afin de remédier à ce risque, nombre d'organisations ont créé des « guides de bonne utilisation » d'Internet à l'attention de leurs membres. Cependant, bien souvent, il s'agit là de simples conseils de bon sens, et le référentiel individuel de l'usage d'Internet aura tendance à influencer sur l'appréciation de ce type de document, pouvant souvent être perçu comme désuet, infantilisant ou coercitif.

3.1- Des usages, des générations et des terrains d'interventions

Parler de l'habitude quasiment native de l'utilisation des réseaux sociaux et autres plateformes numériques fait immédiatement penser à cette tranche de la population qualifiée de « natif numérique ». Il s'agit là de personnes nées et ayant grandi dans un environnement numérique, soit entre la fin des années 80 et le début des années 1990 et ayant baigné dans le « web social » proposé par les réseaux susmentionnés. Il n'est pas question d'ouvrir ici le débat sur les différenciations, en discussion, quant à cette terminologie. Le terme sera simplement employé pour caractériser des personnes jouissant d'une certaine fluidité dans l'utilisation des nouvelles technologies, et pouvant s'avérer être des « naïfs du numérique », conformément à la qualification de Le Deuff dans son blog (2009). Par ce terme, il vise des personnes certes nées au contact de la technologie, mais

qui n'en estiment pas avec justesse les enjeux qu'ils soient purement numériques ou d'information. Cette population se révèle, en outre, être plus souvent composée d'utilisateurs un peu « bricoleurs » que des techniciens fins de l'informatique.

Cependant, dans ce qui nous occupe ici, une chose semble importante à prendre en compte, il s'agit de la consommation de données que peuvent faire ces générations plus précisément la génération « y » — aussi appelée « *génération millennale » ou « millennials »* —, qui regroupe les individus âgés de 18 à 37 ans. Plus cette consommation sera importante, plus elle aura tendance à les faire devenir, tour à tour, acteur de diffusion d'information (sans parfois en avoir conscience) ou cibles d'information visant à modifier leurs comportements qu'ils soient personnels ou potentiellement professionnels. De plus, leur consommation itinérante de données, par l'intermédiaire des smartphones, décuple la potentielle influence de canaux externes pouvant impacter l'organisation pour laquelle ils travaillent. En effet, selon une étude publiée par le Statistica dans leur GlobalWebIndex relatif à la consommation Internet, la consommation de données mobiles chez les « *millennials* » n'a cessé d'augmenter depuis 2012 ou la moyenne atteignait 107 minutes par jour pour arriver à 223 minutes en 2017. Là où la consultation moyenne des smartphones était de 43 fois par jour en 2014, elle s'est faite en 2017 avec une périodicité de 9 minutes 55 secondes, selon le cabinet Deloitte. Ces mêmes *millennales* comptent en moyenne 250 amis sur Facebook contre 200 pour la génération « x » en 2013.

Dans la même étude publiée par SDL, il apparaît que pour les *millennales* les trois canaux de prédilections pour accéder à de l'information seraient Facebook, Twitter et YouTube, loin devant les sites des canaux d'information traditionnels. Or, ces trois canaux de prédilections s'avèrent être totalement libres de tout contrôle, par là même ils

s'affranchissent de toute déontologie relative aux informations, permettant à tout à chacun de publier ce que bon lui semble quelle que soit la motivation à l'origine de cette publication.

Or, les organisations intervenant dans des situations extrêmes soit dites imprévisibles, dangereuses et en perpétuelles évolutions donc incertaines (Lièvre, 2005 ; Rivolier, 1998) auront tendance à faire intervenir sur le terrain une population d'employés jeunes, en raison de la nature même de la situation. Ainsi, ce seront principalement des *millennales* qui seront potentiellement amenés à effectuer les missions confiées par l'organisation, soit la population la plus connectée et ayant pour principales sources d'information des canaux libres et non contrôlés par des autorités de l'audiovisuel. Or c'est précisément cette même population qui est la plus encline à mobiliser une communication transverse en lieu et place de la communication hiérarchique traditionnellement utilisée par les entreprises et organisations. De plus, leur habitude d'usage d'Internet aura tendance à rendre les consignes de sécurité diffusées par l'entreprise relativement peu efficace, dans le cadre de ce qu'ils estiment être leur consommation privée. Enfin, le fait d'intervenir dans des terrains délicats et potentiellement dangereux, en raison de la localisation de la mission confiée ou de la nature de cette dernière, aura tendance à renforcer chez eux l'enracinement de la perception du bien-fondé de leur point de vue en ce qu'il sera basé sur une expérience empirique intense.

4. Enquête de terrain

Dans ce cadre, plusieurs entretiens ont été menés avec des employés d'organisation appelée à intervenir dans des situations extrêmes, dont l'âge était compris entre 23 et 45 ans afin de pouvoir procéder à une ventilation en deux groupes, un groupe d'étude regroupant les personnes âgées de 23 à 36 ans (groupe A) et un autre groupe témoin âgé de plus de 37 ans (groupe B). Une autre subdivision a été opérée avec un groupe n'étant jamais intervenu en situation extrême afin de tester si ce vecteur avait ou non une influence, mais appartenant à la génération milléniale (groupe C). Les entrevues abordaient plusieurs sujets, dont leurs usages de consommation Internet, leurs perceptions de la communication de leur employeur et leurs potentielles évolutions de point de vue vis-à-vis de ce dernier. Afin de pouvoir avoir des données sincères, un anonymat strict a été respecté.

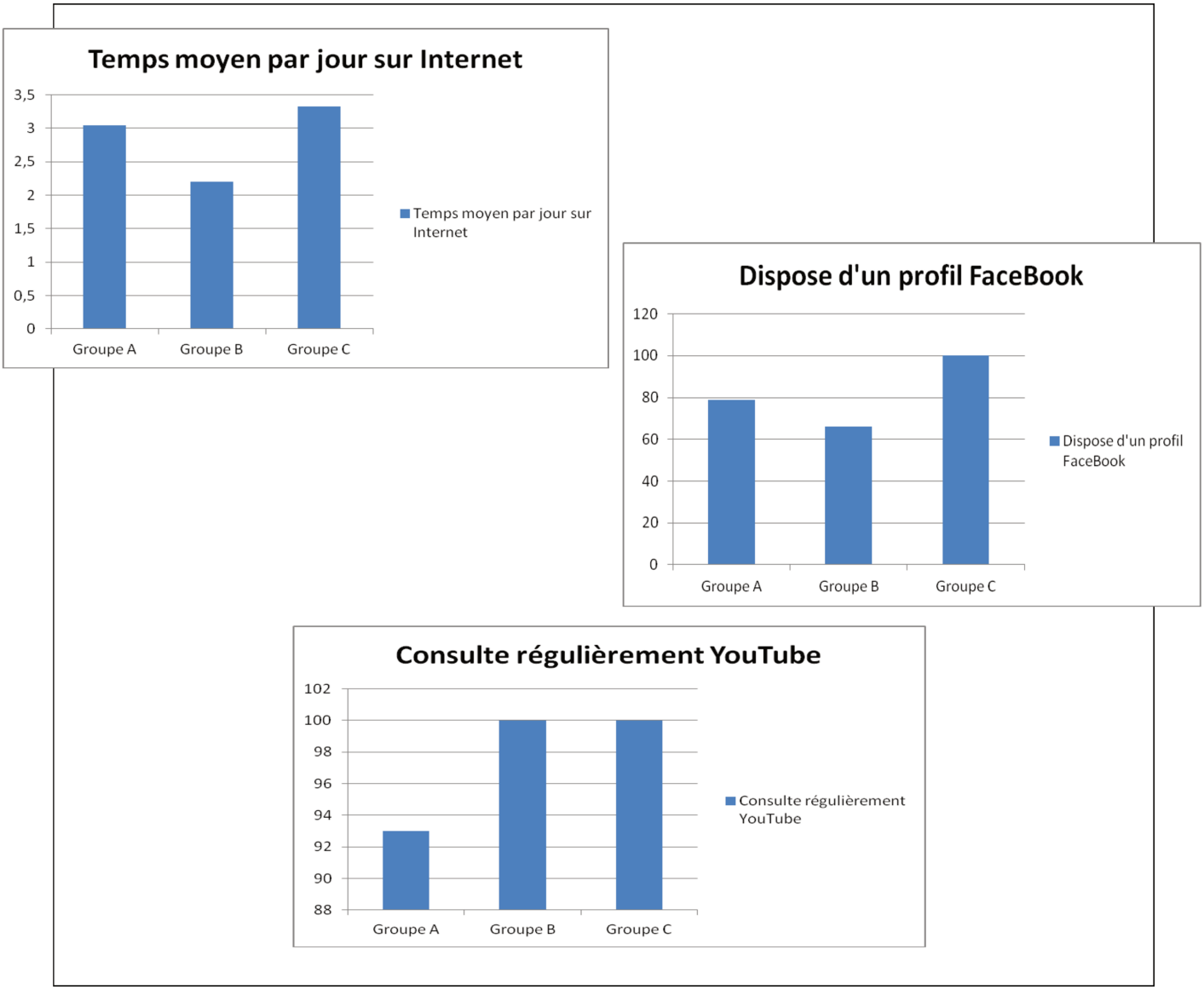
4.1- Analyse des données

L'approche de terrain confirme les données annoncées préalablement quant à l'usage d'Internet généralement fait par les sujets. Ainsi, la plupart consultent Internet par l'intermédiaire d'un smartphone, leur permettant de rester perpétuellement connectés. Concernant l'usage des réseaux sociaux, 76,47 % des personnes interrogées déclarent avoir un profil Facebook et 94,11 % consultent régulièrement YouTube. Ventilé sur les différents groupes, 79 % du groupe A ont un profil Facebook, et 93 % consultent régulièrement YouTube. Concernant le groupe B, les deux tiers ont un profil Facebook, ce chiffre monte à 100 % pour le groupe C n'ayant jamais travaillé en situation extrême. Rapporté à YouTube — référencé parmi les trois principales sources d'information dans l'étude de SDL, — la totalité des membres des groupes B et C consultent ce média.

Concernant le temps de consommation, il est en moyenne de 3,05 heures pour le groupe A, de 2,20 heures pour le groupe B et de 3,33 heures pour le groupe C.

Un décalage significatif existe entre le groupe A et le groupe C, pourtant, tous deux composés de millénnials, quant au temps quotidien moyen passé sur Internet et à la possession d'un profil. Interrogés sur ce point précis, il apparaît que les membres du groupe A auraient une conscience plus aiguë, que ceux du groupe C, de l'empreinte numérique et de ces conséquences. En outre, concernant le temps passé sur Internet, ceux ayant travaillé dans des situations sensibles affirment avoir pris conscience de la nécessité d'être préparés au mieux afin de pouvoir s'adapter à toutes évolutions pouvant intervenir lors de leur travail.

Cette prise de conscience est ressentie par beaucoup comme une motivation pour consacrer plus de temps à leur travail, ce qui pourrait être un des facteurs entrant en ligne de compte dans cet écart. Il semble donc bien qu'il y ait un premier lien entre exposition aux situations extrêmes et consommation Internet.

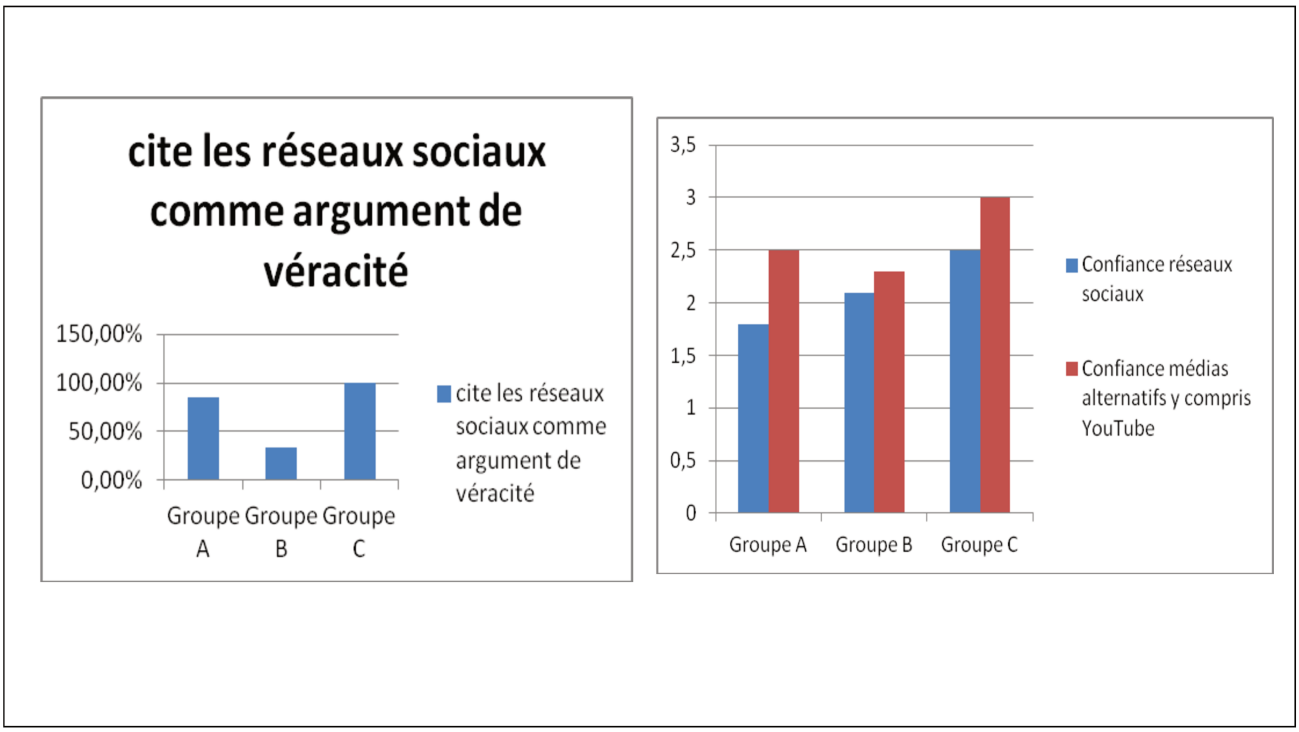


Graphiques relatifs à l'usage d'Internet sur la population auditionnée. Source : C. Dugoin-Clément

Dans le rapport de confiance accordé aux réseaux sociaux, le groupe C arrive en tête avec une moyenne de 2,5 (sur une échelle de Likert à 5 degrés), suivi du groupe B avec une note moyenne de 2,1 et enfin du groupe A avec une note moyenne de 1,8, soit une confiance très faible alors que près de 80 % d'entre eux disposent d'un profil.

Cependant, interrogés sur cette même confiance accordée aux canaux alternatifs comprenant YouTube, les moyennes évoluent pour atteindre 3 pour le groupe C, et réduire l'écart entre les groupes A et B dont les moyennes respectives sont de 2,3 et 2,5. Plus intéressants et surtout plus révélateurs, malgré ce taux de confiance assez bas, ils sont 85,71 % du groupe A à citer les réseaux sociaux comme preuve de véracité, notamment par des expressions du type « on voit bien que c'est partout ainsi, il n'y a qu'à regarder les réseaux sociaux pour savoir, pour s'en rendre compte ». Concernant le groupe B ce chiffre tombe à 33 %, mais monte à 100 % pour le groupe C.

Ainsi, il semble y avoir un véritable écart entre la confiance déclarée et la pénétration des éléments lus et vus sur les réseaux sociaux. Interrogés sur la raison de leur défiance dans les réseaux sociaux, tous évoquent la sensibilisation reçue sur ce point, notamment dans leur cadre professionnel. Il semble donc que si la communication hiérarchique faite par l'entreprise vers ses personnels a été entendue, elle n'atteigne pas encore le résultat escompté dans la réalité.



Graphiques comparés de la confiance portée aux réseaux sociaux et médias alternatifs et de l'appui sur les réseaux sociaux comme élément probant de la véracité d'un fait ou d'une situation. *Source : C.Dugoin-Clément*

Cependant, concernant la perception de la communication mise en place par leur employeur, elle est généralement mieux perçue par le groupe n'ayant pas travaillé en situations extrêmes. En termes de perception qualitative, les groupes A et B font émerger un ratio entre leur expérience professionnelle et l'image véhiculée par la communication hiérarchique. Cette dernière est alors souvent perçue comme éloignée de la réalité, ne représentant pas leur quotidien. Ainsi, il y a un effet de jugement de ces populations notamment à l'échelle de leur propre vécu : plus il a été intense, plus il est estimé comme

maître étalon probant, justifiant le bien-fondé de l'avis posé sur la communication hiérarchique.

L'écart le plus marqué et le jugement le plus dur se retrouvent vis-à-vis des campagnes de recrutements qui sont assimilées à de la publicité, en y associant tous ses travers, notamment le côté mensonger.

La communication hiérarchique devient donc de plus en plus sujette à caution et il y a une concurrence accrue entre les messages qu'elle diffuse et ce qui est capté par d'autres canaux, y compris interpersonnels. En se référant à la théorie du petit monde, cet accroissement de la sensibilité aux informations perçues par des canaux personnels faciliterait l'influence, sur ces personnels, d'intervenants tiers. Ainsi 52,94 % des interviewés déclarent recouper et vérifier les informations transmises par la hiérarchie par l'intermédiaire de leurs propres sources, voire, pour certains, accorder plus de confiance dans leurs propres sources que dans la communication hiérarchique. 35,29 % préfèrent ne pas répondre à la question et seulement 11,81 % affirment une confiance absolue dans la communication de leur entreprise. Rapporté au groupe A, 35,7 % sont dans la première situation quand 50 % ne se prononcent pas. Et les deux tiers du groupe C annoncent revérifier les informations par leurs propres canaux, canaux comprenant les réseaux sociaux.

Enfin, quand on interroge l'échantillon de sujets pour savoir si leurs perceptions ou avis concernant leur employeur ont pu changer suite à des éléments d'informations vues, lues ou entendues, ils sont 70,58 % à répondre par l'affirmative, sans que le changement soit forcément négatif. Cette tendance monte à 71 % dans le groupe A et représente les deux tiers du groupe B.

Conclusion

En conclusion, il apparaît suite à l'étude menée dans cet article que si la sensibilisation menée par les organisations à l'attention de leurs employés visant à leur faire prendre une certaine distance vis-à-vis des réseaux sociaux a bien été diffusée, elle n'a cependant qu'un effet relatif. En effet, si le déclaratif a tendance à afficher une confiance très relative dans les médias sociaux (avec une note moyenne 1.93 sur les 5 degrés proposés), 82,35 % des sujets entendus s'appuient tout de même sur les réseaux sociaux pour asseoir la véracité des propos véhiculés par leur hiérarchie. Concernant l'influence de l'exercice de l'emploi dans des situations extrêmes, il aurait tendance sur la population auditionnée à être un régulateur de la consommation Internet. En effet, ces expériences, notamment en raison de la prise de conscience du risque, auraient tendance à renforcer la volonté de se préparer au préalable de la mission confiée. Par système de vase communicant, les sujets auraient donc tendance à être plus focalisés sur leur travail préparatoire se dispersant moins dans une consommation de données.

Néanmoins, il apparaît aussi que si la consommation est plus réduite dans les groupes A et B, leur perception de la communication de leur organisation est également moins positive.

Enfin, concernant l'évolution de leur perception de la communication produite par leur employeur suite à des éléments d'information ou des communications reçues par des canaux n'émanant pas de la communication hiérarchique, les résultats se montrent largement positifs. Si le changement de perception n'a pas forcément été négatif pour tous les sujets déclarant avoir changé de point de vue, cela reste néanmoins un élément sensible. En effet, cette capacité pour des tiers à influencer la vision que des employés ont de leur organisation engendre un vrai risque pour l'organisation et sa gestion RH. En

effet, en cas de pression forte, directe ou indirecte, sur les membres de l'organisation afin de dégrader l'image de leur employeur, peut influencer directement leur travail avec des conséquences immédiates pour la structure, notamment si la confiance des personnels dans leur hiérarchie est altérée.

Fort de ses éléments, il semble que la recherche doit être poursuivie notamment concernant l'influence que pourraient avoir ses canaux d'information parallèle sur la confiance portée dans l'organisation et, de facto, dans l'incertitude ressentie par ses membres.

Références

Antonelli, Cristiano. 2006. “The Business Governance of Localized Knowledge: An Information Economics Approach for the Economics of Knowledge.” *Industry and Innovation* 13 (3): 227–61. https://doi.org/10.1080/13662710600858118.

Balagué Christine & Fayon David. (2016). *Facebook, Twitter et Les Autres...: Quels Réseaux Sociaux Pour Votre Entreprise*. Paris: Pearson France, 2016, 256.

Cabinet Deloitte. 2015. “Usages Mobiles Les Français et Le Smartphone En 2016 : Une Relation Fusionnelle.”

Le Deuff, Olivier, 2009. “Le Guide Des Égarés.” *Blog d’Olivier Le Deuff*. 2009.

Lièvre Pascal, and Rix-Lièvre Géraldine. 2004. “Le Management Des Expéditions Polaires.” *Management & Avenir,* 24 (9): 1–12.

Mercklé. Pierre. (2016) “Un Nouveau Paradigme Sociologique ?” dans *La Sociologie Des Réseaux Sociaux. Paris,* La Découverte, 2016, 95–104.

Milgram, Stanley.,1967. ‘The Small World Problem’, *Psychology Today*, 61−67

Pew Research Center. (2013) *Internet & Technology.* Washington, Pew Research Center, 2013.

Réka Albert & Barabási Albert-László. 2002. “Statistical Mechanics of Complex Networks.” *Reviews of Modern Physics,* 74 (1): 47—97. https://doi.org/10.1103/RevModPhys.74.47.

Rivolier, Jean. 1998. « Stress et situation extrêmes », *Bulletins de la psychologie*, vol 51, *51*, 6-20.

Statista . 2018. « Worldwide: globalWebIndex : 2012 to 2017: 18 to 32 years » *Satista,* 2018.

SDL. (2014). *Five truths for futur marketers*. Maidenhead, SDL publication, 2014

CHAPITRE 5 : L'approche managériale des situations extrêmes: analyse et propositions préventives

Il apparaît clairement que la confiance est un des « game changer » de l'efficacité des modes opérationnels lors d'interventions en situations extrêmes. Les chapitres précédents ont montré l'influence de l'information sur le degré de confiance qui peut être accordé soit à des paires, soit à l'organisation. Il convient maintenant, pour approfondir l'analyse afin de pouvoir avoir une approche managériale à même de pouvoir formuler des propositions anticipatives, correctrices et curatives à des opérations informationnelles telles que décrites dans les chapitres précédents. Pour ce faire, je me suis interrogé sur les leviers psychologiques qui interviennent dans l'accroissement ou la diminution de la confiance afin d'en identifier les motivations profondes.

Ce chapitre s'attache donc à analyser le modèle et à comprendre les ressorts sur lesquels des opérations destinées à altérer la confiance pourraient jouer pour amoindrir la confiance, déstabiliser la cible et in fine affaiblir notablement l'organisation. À cet effet, un article a été rédigé conjointement avec le Professeur David Vaidis. Néanmoins, afin de ne pas alourdir ce chapitre 5 avec une méthodologie relevant purement de la psychologie sociale, il a été décidé de ne pas présenter l'article dans sa globalité, mais de procéder à une extraction des éléments qui y sont présentés et qui permettent de se concentrer sur l'approche managériale du sujet. Toujours en ce qui concerne la méthodologie, ce chapitre s'attache à traiter plusieurs propositions issues de la problématique centrale. Pour ce faire, il s'appuie sur plusieurs sources de données (entretiens, observation et documents consultés) ayant permis de valider (« V ») ou de ne pas valider (« NV ») les propositions de recherches comme présentées dans le tableau suivant.

Question de recherche	Dans un contexte de situations extrêmes soumis à une très forte pression de facteurs externes, en quoi la diffusion de certaines informations et le canal utilisé sont de nature à ne pas exécuter le ordre ou les décisions de la hiérarchie?			
DONNEES DE RECHERCHE				
Sous-Problé-matiques	Déclinaisons	Entretiens	Documen	Observation
Altération de la confiance et prise de déci-sion	La confiance comme facteur de coopération	V	V	V
	Il y a différentes dynamiques selon les niveaux de confiance, et différentes combinaisons itératives de confiance intervenant à la croisée des fondement de la confiance (affectif, cognitif, intuitif) et des différents niveaux hiérarchiques	V	NV	V
	La confiance, pierre angulaire de la gestion de la coopération au sein des équipes en situation extrême	V	V	V
	Les cibles potentielles de ce type d'attaque n'ont pas conscience de pouvoir être visée	V	NV	V
	La manipulation de l'information peut altérer la confiance	V	V	V
	Différents leviers psychologiques interviennent dans l'évolution de la confiance	V	NV	V
Les valeurs et le renforce-ment de la confiance et des méca-nismes de coopération	Les valeurs sont une protection contre des influence extérieures, elles sont garantes de l'exécution conforme des consignes	NV	V	NV
	La hiérarchisation des valeurs divergent entre les différentes strates hiérarchique de l'organisation	V	NV	V
	La hiérarchisation des valeurs divergent entre les différentes classes d'âge	V	V	V
	Il y a un impact des valeurs sur la prise de décision et les proces-sus de coopération entre les agents	V	V	V
	Le partage supposé des valeurs prévaut sur la sensibilisation à la prudence (notamment sur Internet)	V	NV	V
	Les valeurs sont des failles de sécurité face à la diffusion d'infor-mations dissonantes	V	NV	V
La perméabili-té aux infor-mations diver-gentes de celles déli-vrées par l'or-ganisation	Le temps sur Internet influence sur l'efficacité des opération d'in-fluence	NV	V	NV
	L'ancienneté et l'exposition aux situations extrêmes participent à renforcer l'imperméabilité en accroissant la confiance entre les membres de l'organisation	NV	V	NV
	Il y a un impact de l'information sur la confiance et les valeurs	V	NV	V

Tableau 9 - Sources utilisées pour valider ou invalider les propositions présentées dans le chapitre 5

Ainsi ce chapitre présente les données collectées lors de la seconde phase d'entretiens (vagues 1 et 2), analysées sous l'angle qualitatif ainsi que quantitatif, et présente plusieurs propositions et remèdes aux attaques pouvant altérer la confiance et ainsi engendrer des prises de décisions déviantes risquant de faire basculer une situation extrême en

situation de crise échappant à tout contrôle et pouvant avoir des conséquences lourdes tant pour l'organisation que pour les personnels y travaillant. L'article présenté ici est en reviewing auprès de la revue européenne de psychologie appliquée sous le titre « Discrepency in internalized values of workers in extreme situation: consequences for soldiers and risk for the organization ».

Introduction

Some people, including soldiers have to work in extreme situations, defined by Rivolier (1998) as situations that differ from everyday life and are risky, volatile and unpredictable. Unpredictability is here defined as radical as in Knight's (1923) vision where the probability of occurrence of an event is not measurable (Orlean, 1986). People facing these situations try to cope with them by relying on their personal values. For these reasons, military personnel are both physically and psychologically trained to enter combat situations. This training includes the adoption of strong and central values such as *patriotism*, *bravery*, *loyalty*, *respect for authority*, *cohesion*, *courage*, *justice*, and *honesty*. These shared values contribute to group cohesion and the development of trust (Evans, & Dion, 1991). In addition, many have shown that cohesion and trust are directly linked with performance in military teams (see Mullen & Cooper, 1994 ; Oliver, Harman, Hoover, Hayes, & Pandy, 1999). More broadly, Fuller, Mayer, and Pike (2008) posit trust as a critical enabler of team success). Thus, in the military field, the organization performance is largely associated with mission success and linked to team success. However, because these values are fundamental for efficient work, their alteration could strongly impact the execution of orders that could consequently represent a risk for the mission success and thus, for the organization's strategy and efficiency. An influence operation targeting these specific values could then perturb their trust in the military institution, with dire consequences.

As an organization operating regularly in extreme and risky situations, the Army needs to rely on values. These values are inculcated in soldiers' minds through their military training. Considering these values' importance, military personnel can theoretically be particularly sensitive to influence operations mobilizing these values. They are central and relevant for their ingroup, and consequently any threat to them could be perceived as a direct attack to soldiers self. We thus argue that specific information threatening these values is likely to produce strong reactions that could

interfere with the superordinate goal of accomplishing their mission. In addition, we consider that because these values support their self-image and generate strong emotional reaction, military personnel could be less vigilant about the reliability of the source of information when they feel closer to it, and responsible for its access, as it could be when using social networks.

In this paper the value system of the military was examined through general models of social psychology. Using interviews, with both quantitative and qualitative methodologies, the link between values and trust was examined and specific hypotheses concerning the consequences of discrepancy between participants' core values and the way their institution deals with them were developed. Finally, a staged observation was conducted to illustrate with empirical data the founding principles of this mechanism.

1. Values and military profession

From the beginning of its initial training of new recruits, the Army highlights the importance of values. For instance, official communications usually stress specific values such as *trust*, *team spirit*, *self-help*, *respect*, *courage*, *will*, *perseverance*, *merit* and *patriotism*. These values are supposed to be shared by all soldiers and enrich them throughout their lives. In armies, cohesion is described as essential and is reinforced by the necessary confidence and the daily sharing of the demands and risks of the job. This idea is corroborated by Dasgupta (1988), who argues that without risk there is no need of trust. Because military teams are usually at risk, they require strong confidence in the organization. This trust is not only dedicated to their peers, but also to their superiors giving orders and supplying materials, even if these hierarchy members are not close to the battle field. The distance between soldiers and their hierarchy makes trust particularly relevant, as trust can be substituted for control in relationships (Aulakh, Kotabe, & Sahay, 1997). Trust is essential

because their everyday life as soldiers involves risk, and following orders may sometimes increase that risk.

1.1. Training and Values

For these reasons, army as an institution recognized long ago the benefits of inculcating desired values in soldiers' minds (Huntington, 1957). Perpetuation of values is justified by their necessity for the effectiveness of the military institution. Similarly, according to Schweisguth (1978), organizations try to establish control over their members by imposing norms whose justification implies reference to a symbolic system. In the army's case, due to its very function, this is particularly effective since the mission may require soldiers to sacrifice themselves for the general interest. Furthermore, values shared by team members are a guarantee that they will do all their best to assure the security for the individuals and for the group (Cvetkovich & Löfstedt, 1999). As said by Siegrist, Cvetkovich,and Roth (2000, p. 360) "a strategy reducing this risk is to rely on those individuals who we sense will follow what we consider to be appropriate guidelines and general principles for setting goals and procedures—those with similar salient values." Concerning the institution, these values limit the reassessment and questioning of orders by reinforcing trust. In this sense, the military's symbolic system is built on chosen values which are a fundamental element of the trust in and functioning of the institution. In sum, values serve the army as building blocks for the integration of norms supporting an active ideology. They are crucial elements to motivate the soldiers, to give meaning to their military activities and thus to help the organization deploy its strategy.

1.2. From Instruction to Internalization

After months of training, the strengthening and internalization of army values gets solidified when the newly enlisted soldiers are deployed to their units on the field, specifically through External Operations (EO). During these EOs, personnel share with their group a daily life and a common confrontation of risks. There, because what they learnt turns to be applied every day, the values are strengthened and cohesion is reinforced. Deployment in EOs also confronts them with the risk of death and injury while performing their missions. This participation to military operations and this confrontation to risk reinforcing cohesion, namely trust in peers (Adams & Webb, 2003). Moreover, trust helps to secure collective meaning maintenance that may contribute to going through the crisis to its resolution (Karsenty, 2015). Logically, other values are equally reinforced through field deployment as well as everyday life, but trust in peers is essential and particularly strong during risky EOs, as it serves an adaptive purpose. Groups and the associated trust in peers thus becomes central. Barrois (1993) maintains that the group becomes a true homeland to kill or die for. In the same vein, De Richoufftz (1999) postulates that soldiers are not giving their lives for nation or institutions, but for their brothers in arms. In line with this suggestion, Godé (2011) showed that debriefings reinforce common values and culture in military teams. Altogether, trust in peers turns out to be a foundational component of the values soldiers are most attached to.

Finally, even if the institution promotes a package of values, the ones soldiers favour could be different from the ones expected by the hierarchy. While trust in the hierarchy and respect for orders are essential for efficient functioning of the military institution, one could postulate that the most deeply rooted trust ultimately lies in the group. This is because the factual establishment of values takes place in units, close to other soldiers and far from the institution's commanding officers.

2. Discrepancy in Major Values

The military institution also promotes chosen values to control their agent's behaviour especially during mission execution. But the training initially given by the institution is then achieved in their units through socialization with their peers and during the execution of missions. Consequently, we hypothesize, soldiers' experience may lead them to prioritize trust in their peers over trust in their institution. Moreover, once soldiers have developed their own scale of values enriched by empirical experimentation in EO and socialisation in their units, indeed, some authors postulate that military values and commitment is directly influenced by military socialisation (Francke & Heinecken, 2001). Consequently, they can legitimately think they are the ones who know best what these values really mean, that they are the one who really applied them correctly. Thus, they can judge the way the military hierarchy deals with the same values. This could be particularly relevant because soldiers' values learnt during training and then tested on the ground often become part of their personality. As such, some authors postulate that military values and commitment is directly influenced by military socialisation (Francke & Heinecken, 2001). As a result, these values are central, and confronting peers and the institution may have important consequences for the general organization and specifically with regard to respect for authority.

2.1. Consequences of Discrepancy in Values

Different psychological models suggest that the discrepancy in values between members of an organization and the organization as an institution has disruptive consequences on behaviours, perceptions and reactions. Soldiers are not exceptions. More specifically, we assume that cognitive dissonance theory (CDT; Festinger, 1957; Harmon-Jones, 2019; Vaidis, 2014), attitude ambivalence theory (McGregor, Zanna, & Holmes, 1998; McGregor, Zanna, Holmes, & Spencer, 2001), terror management theory (Greenberg, Pyszczynski, & Solomon, 1986), and finally, the meaning mainte-

nance model (MMM; Heine, Proulx, & Vohs, 2006; Proulx & Inzlicht, 2012) provide relevant understanding of soldier behaviour perturbation based on values discrepancies that could affect the expected course of the institution.

2.2. Cognitive dissonance

When we consider that confronting values can be hazardous in soldiers' case, we refer to CDT and more specifically to the self-consistency revision (Aronson, 1968, 1992, 2019; Stone & Cooper, 2001). According to Festinger (1957), when there is inconsistency between two cognitions, the individual experiences a state of cognitive dissonance, a motivational discomfort, and tries to reduce it. The main strategy for doing so that has been studied has been attitude change to reduce discrepancy with an attitude-inconsistent behaviour. Smith (1965) showed how soldiers rationalized an attitude-discrepant behaviour (i.e., eating grasshoppers) with a positive change in attitude when they had no justification for doing it, but not when they had several justifications. Unfortunately, the means used to cope with unwanted information or a behaviour perceived as discrepant with values are not necessary rational. Dissonance-reducing efforts could lead to reinforcement of the said values, to their weakening, or to disengagement, depending on several parameters (see McGrath, 2017; Vaidis & Bran, 2018).

For the current purpose, it appears relevant to focus on Self-Standard Models of dissonance (SSM), as developed by Aronson (1968, 1992) and then further by Stone and Cooper (2001). According to these models, dissonance specifically arises from contradictions between individuals' behaviour and their self-perception. In the case of soldiers, this self-perception is closely linked to the aforementioned values. According to the SSM, the more people's self-image is positive, the more they feel cognitive dissonance when they feel they have not lived up to their personal standards. Soldiers' self is strongly linked to the military values which motivated them to fight for the

greater good. Soldiers' values initially learnt during training are validated and strengthened by everyday life experience in extreme situations. Consequently, because these values are strong and linked to their self-concept, behaviours that are discrepant with their standards will be considered as a direct threat, thus generating strong dissonance.

2.3. Perception of Discrepancy in Values Provokes their Defence

The specific setting of agents evolving in extreme situations is a fertile ground for the observation of cognitive dissonance and more generally of meaning threat. This is obviously the case for military personnel. Soldiers are confronted with death and professionally stand alongside it. Additionally, being prepared to cause death falls within their job description: while killing of other humans is generally forbidden by law, religion and, broadly speaking, morality, they are the official executioners of nations. Because their profession exposes them to moral dilemmas and mortality, soldiers, sponsored by the military institution, develop efficient coping based on professionalism and bolstering and strengthening of central values of their job. This fits with the general strategic pattern of the institution's expectancies, and justifies the reinforcement of chosen values in soldiers' minds. Indeed, this bolstering of values is a standard regulation for informational dissonance (see Burris, Harmon-Jones, & Tarpley, 1997, Festinger, Singer, & Schachter, 1956; Vaidis & Gosling, 2011). Consequently, mortality salience bolsters central values, but it also probably leads soldiers to engage in more general worldview defences. Many of these worldviews could be associated with their profession (i.e. promoting a secure world and protection). This general context supposes soldiers have strongly internalized values that are central to their self-concept. In accordance with CDT and MMM, these values should be very sensitive to inconsistency. Thus, we assume that perception of discrepancy between their values and their professional environment should provoke a disturbed state that requires regulation.

3. Regulation of Discrepancies in Values Involving the Institution

Inconsistency amongst central values is supposed to readily trigger regulation processes (Kruglanski et al., 2018). In addition, important values are also resistant to change and thereby cannot be directly targeted by the regulation (Eisenstadt & Leippe, 2005; Simon et al., 1995; Vaidis & Bran, 2018). As "believers" cannot accept changing core beliefs (e.g., Batson, 1975; Burris et al., 1997), individuals with strong grounded values are more likely to reinforce these values (Festinger et al., 1956), by rejecting the external information (Batson, 1975; Bochner & Insko, 1965), to reorganize their knowledge (e.g., Leippe & Eisenstadt, 1994), or to denigrate another group (e.g., Cooper & Mackie, 1983). In soldiers' case, values are strong and can serve as resources to buffer threat. Amongst these values, the ones related to trust in peers are likely to be the strongest ones. One could thus assume this prevalence of trust in peers is a double-edged sword when the soldiers are confronted to a discrepancy between the military institution and these values.

As discussed previously, soldiers should be highly sensitive to inconsistency aiming their personal values. Thus, if there is a salient discrepancy in two clusters of cognitions, one involving confronting professional values, soldiers should not endanger their perception of their self but rather should derogate the other cognitions. As derogating the other cognitions protects not only their perception of themselves, but also their worldview coherency, it is more likely in this situation. But what if the discrepancy involves trust in peers and trust in the institution? Because the group is central, individuals are likely to derogate the weaker source of trust, namely the military institution. Consequently, one could hypothesize that when the inconsistency is related to trust in peers and trust in the military institution, the more likely outcome is a reduction of confidence in the institution.

One could argue that other means can be employed to regulate this conflict. For instance, the individual could be inclined to reject the source of information generating discomfort instead of modifying core values. Several authors have argued that people are inclined to reject the source of information when it does not fit with their expectancies (Batson, 1975; Bochner & Insko, 1965; Vaidis & Gosling, 2011). Indeed, information suggesting high discrepancy in expectations is likely to be rejected (i.e., discredited). According to Bochner and Insko, information coming from a non-expert source will not modify the recipient's attitude but will be discredited. Similarly, for Batson, most believers will not consider disconfirmatory information to be true. This idea also fits with the general process of confirmation bias and selective exposure (e.g., Hart et al., 2009).

Nevertheless, these forms of regulation are unlikely in soldiers' case for two reasons. First, the discrepancy involves self-relevant values, reinforced by their training and experience. Confronting these values is similar to a direct threat and soldiers should react as if they were personally attacked, or as if their close relatives were threatened. In such a situation, the individuals could be inclined to react without fully processing the arguments of the message, as strong emotions are likely to alter information processing (e.g., Bodenhausen, Sheppard, & Kramer, 1994; Moons & Mackie, 2007; Rydell, et al., 2008; Witte, 2009). Second, some evidence could suggest that soldiers hold both positive and negative attitudes toward the military. In this case, army hierarchical structure and soldiers field experience should favor ambivalent attitudes toward the institution, which in turn would facilitate its derogation. Finally, as previously hypothesized, even if formed through the prism of the institution, foundational aspects of their values should rely on trust in peers, not in the institution per se. Altogether, without other means offered by the situation, soldiers should be more likely to derogate their trust in the institution when it conflicts with their trust in their peers. This derogation is a source of decrease of results for the institution as it could interfere

with obedience to orders, and thus present a risk for the organization strategy. Moreover, in regard to information warfare, this situation presents a potential breach likely to be used by opponents.

3.1 . Discrepancy with the Institution: from inner conflicts to information warfare

In the previous paragraphs, we explained how a salient discrepancy between values can disturb the value system of military personnel. Information stressing the discrepancy between core values concerning the institution, hierarchy members and soldiers could be involved in undermining trust. In the present section, we stress what could be the sources of discrepancies involving peers and the institution, and their implications for the organization. In the final part of this section, we develop the new strategies of information warfare that are now considered as part of modern conflicts.

The institution is a moral entity that is primarily incarnated in the hierarchy. Members of the hierarchy are the frontline of the institution. A strong situation of discrepancy occurs when soldiers perceive a gap between their expectations of the hierarchy and its actual behaviour. For instance, soldiers can perceive that officers are distant from soldiers, not conscious of field reality, and even careless about soldiers' lives. Military personnel can believe that officers are focused on using soldiers' skills and lives to advance their career instead of serving superior values. Moreover, if considered to be very different and far from soldiers' reality, officers can be thought of as not as competent as they ought to be. More concretely, if soldiers face a situation where they judge an officer to be dishonest, they will experience expectancy violation. Because honesty is a central value, this will lead to derogation of the officer, undermining trust in the military institution. This decreased trust can in turn lead to a decline in performance and, in the worst case, disobeying orders.

This situation is what we call here a *hierarchical split*, a circumstance in which the discrepancy involves the relationship between the management of the institution (i.e., officers), on one

side, and enlisted personnel on the other side. A hierarchical split is a critical situation, because contrary to other situations, in this circumstance it is more difficult for soldiers to conjure up cognitive filters to ignore the discrepancy. When exposed to hierarchical split, people cannot ignore the information because, first, the information is relevant for them and required for adapted reactions in their environment. Second, when official, they cannot avoid or minimize the exposure to such information. The personnel are thus forced to face the gap between the professed values of the hierarchy and their actions, and could hardly avoid processing this source of discrepancy. Two main vectors of discrepancy with the institution are field experience and communication exposure through media.

3.2 Field Experience

The experience of real situations in EO can be a strong generator of doubt. For instance, remembering tine information they were given during training or conferences and realizing that it is intentionally not representative of what empirical experience reveals can be a strong cognitive dissonance trigger. Confrontation with death is obviously also a trigger of expectancy violation and a factor in intensification of reactions (Greenberg & Arndt, 2012; Proulx & Inzlicht, 2012).

When analysing the effects of an observed gap between training or briefings and reality, one symptom of doubt could be a search for information from peers regarding what was said in official briefings. People are inclined toward selective exposure to information, and when exposed to circumstances that do not fit with their conceptions of reality, they search for consistent information to bolster their initial commitment (D'Allessio & Allen, 2006; Jonas, Schulz-Hardt, Frey, & Thelen, 2001; Fischer et al., 2011). In soldiers' case, the result of this kind of search could simultaneously involve both a loss of trust in hierarchy because they doubt previously provided information and an increase in trust in peers because they rely on them to found support.

The field experience can also be vicarious: the confrontation does not come from the individual's experience but from a peer's. It could even come from soldiers or people the individual does not know personally but perceived as reliable: social media for instance provide access to people sharing common values and similar professional backgrounds even if they are not physically known, nor verified profiles. So-called soldiers met on the Internet may thus irrationally be considered as relevant for official briefing checking.

3.3. Media and information warfare

Information channels provide access to content from different parts of the world, and thus from different theaters of operation. Therefore, media, including social media, provide many opportunities to make salient a gap between everyday experience and what soldiers initially committed for. Smartphones and the Internet access makes available a large array of media any time, anywhere. Moreover, media contents initially perceived as unreliable could be regarded more positively if recommended by a brother in arms or an appreciated contact (i.e. an evaluative conditioning; see De Houwer, Thomas, & Baeyens, 2001). For instance, social networks promote opinions and individuals through posts, comments, links, or activities with "likes," thumbs up, and sharing. Because algorithms rely on profiling, individuals are more likely to be exposed to information shared by individuals who are presumed to be similar to them.

Obviously, field experience and media exposure may work together. For instance, individuals could be exposed to discrepancies on social networks via reported peer experiences of hierarchical violations of central values. In this case, the experience is reported by a third party via social media. There is the rub: some media content could be designed for a specific goal, including to serve geopolitical strategies from other organizations or countries. These tactics belong to information warfare.

Overall, information warfare relies on the use of information and communication technologies to take advantage over the opponents in a conflict. If these tactics seem classical in modern conflicts, the advances in computational sciences and Internet technologies suggested new developments and broader uses. In recent times, due to the blowup of new technologies, these operations have been included in some military strategies such as the *New-Generation War* (NGW). This strategy has been developed by three Russian officers, Gareev (2015), Chekinov and Bogdanov (2011, 2013) and put information as a main component of the current strategy for 21st-century conflicts. In the NGW, information-based subversive operations can be created to provoke different kinds of disturbances, including weakened state resilience and organizational processes. This kind of process has already been applied in several places including the Ukrainian war since the blowup of Donbass conflict and Crimea annexation in 2014. This kind of attack has been at the origin of some report from the *Cooperative Cyber Defence Centre of Excellence* (Giles, 2015).

In light of NGW, the use of social media to disturb the agent's efficiency and thus indirectly the military institution is very likely. Here lies a main evolution: contrary to former use of information material which could be perceived as an influence attempts, the use of social media could be more subtle because it gives the perception of control and freedom in the exposure to information. Indeed, even if militaries are trained to be vigilant towards Internet, social media holds specific features that, associated with individual involvement, could reduce this vigilance. Indeed, individuals are likely to feel agency in their search for information when they use the Internet, and thus feel responsible for the information they are exposed to. When not perceived as advertisements, information shared on the Internet will not be perceived as an influence attempt. In addition, as discussed previously, because the individual could feel a threat to the self, such information could be sufficient to trigger reactive behaviour that undermines trust in the military institution. In

regard to the psychological models we developed previously, one could consider that these strategies could use soldiers core value in order to modify their behaviour in the field and way to orders.

4. Overview of the Study

We presented a theoretical background pertaining to what could lead to military personnel disengagement. We discussed the potential critical consequences such as decreased trust and a global undermining of efficiency.

More specifically, in light of previous sections, we postulate that if soldiers' values are nested in a message, this content could reinforce these values and make them salient. When the message stresses discrepant information concerning peers and the Institution, this is likely to generate strong reactions because it violates the inner attitudes and expectancies of the individuals (Kruglanski et al., 2018; Vaidis & Gosling, 2011). Because the information is based on central values and stresses a pre-existing ambivalence toward the institution, it should be consistent with some existing priors and favour a confirmation bias. The soldiers could then be inclined to process the message less deeply, the arguments and the source, leading them to overestimate the content and not protecting them from an attempt to influence. Thus, regardless of whether individuals have been trained to be cautious about the information source, the presence of such values overwhelms usual caution and vigilance. Finally, because the values relative to peers are highly resistant to change, they should guide regulation attempts (McGrath, 2017; Vaidis & Bran, 2018) and lead to reinforcement of values linked to the group and undermine trust in the institution. Consequently, endangerment or flouting of core values could push soldiers to bolster their trust in peers, even if it implies derogation and ultimately destabilization of the organization.

To evaluate the suggested processes we discussed in the first part, we relied on qualitative and quantitative data obtained from individual interviews. These interviews were complemented by a staged observation for a second set of participants. The interview purpose was to collect confirmatory information concerning the soldiers core values, to evaluate their trust toward the peers and institution, and their relation with media. A qualitative approach was chosen because of the specificity of the topic and because accessing honest responses requires achieving a trusting relationship. Quantitative analyses were also performed in order to test some variables and hypotheses, especially concerning trust perception and values ranking. Concerning the stage observation, it was designed in a second time to evaluate an important proposal in our model concerning soldiers' strong emotional reaction to discrepancy with their core values. This permitted to assess the soldiers in an ecological situation and to estimate their processing of a message threatening their values.

4.1. Method

4.1.1.Population and Sample

Thirty-eight interviews with active duty male soldiers[1] were conducted. With permission from their commanding officers, interviewees volunteered and were assured complete anonymity. They all belonged to the same type of units of highly experienced soldiers regularly exposed to extreme situations and sensitive operations. This sample has been completed in two periods with 17 interviewees in the first set and 21 in the second one. All the participants of the second set participated in the staged observation. The interviews were audio recorded with participants' full agreement, and they were assured that the recordings would be destroyed and the data would be only used for scientific purposes. The interviews were conducted by a female investigator, one of the authors. They took place in different military bases over several consecutive days. The investigator had time

to gain the trust of the units; moreover, she was trained and experienced in EO, which allowed her to engage in ice-breaking. The interviews lasted between about 45 minutes and two hours. Although introduced to them by their commanding officer, the interviewer had no legitimate power over the participants. The quite long length of the interviews indicates the level of comfort and rapport the interviewer developed with the participants.

Most of the interviewees had been deployed in a war zone (from 4 to 96 months; median of 18.5 months); only three men were not and were excluded from analyses related to EO experience. Participants were between 23 and 45 years old (median age of 30 years old).

4.2. Content of interviews and identified variables

The interviews were semi-structured, and conducted so as to grasp the essence of the interviewees' thinking and experiences without influencing the answers. The discussions also contained a series of recurring topics focused on the variables studied such as trust in peers, the military institution, and the media. On these items, participants were invited to assess their trust on a scale from 0 (no trust at all) to 5 (absolute trust). Subsequently, they were asked to explain the nature of this trust, eventually giving examples to refine their declarations.

The interviews also assessed the participants' values, commitment, past behaviours and their professional project. Participants were asked to discuss which values they perceived as the most important both in their job and personal lives. Concerning their enlistment, they were questioned regarding their initial motivations and whether they had ever considered leaving the Army If they had, they were encouraged to explain the reasons why they considered leaving the military and why they did not act on it. Finally, they were asked whether they had had doubts—or not—about orders they had been given, and whether they had ever thought about disobeying them or had actually done so.

4.3. Staged observation part

A key proposal of the model is that highly trained military personnel could be inclined to overreact to information threatening their values. More specifically, it was hypothesized that mobilizing central values through the media should provoke a negative reaction and mistrust in soldiers' hierarchy, even if the "information" was not reliable. Because one could consider this proposal bold and because it could have crucial implications for the military institution, confrontation was made through a staged observation. During the interviews, after asking about their trust or mistrust in media and social networks and the reasons for it, and after discussing the training by the institution on the necessary distrust towards social networks, a screenshot of a fake Facebook page was presented to the participants of the second set of interviews. We relied on the interviews of the first set to create the informational content.

The sample was composed of the 21 participants of the second set. There was no selection in the participants and all the second set's participants were included.

The material was created to stress some core values and confront participants with a reaction of the institution discrepant from the one they expected. More specifically, it emphasized *Professionalism* (i.e., proper equipment is a necessity to achieve mission) and made available in memory past experiences (i.e., most soldiers dealt at some point with improper equipment). The second part of the message highlights the alleged institutional reaction that sanctioned a soldier for telling the truth (*Justice/ and Honesty* values).

This fake message was an alleged publication from a group of "friends" of a unit containing a reshare of recruiting advertisement for the army showing bright new materials. The sharing was adjunct with a cynical comment: "*Nice advertising; too bad that the 'whistle blower' about the current state of equipment in EO is now facing sanctions from his commanding officers."* If the picture used was an extract of recruitment material, it appeared clear that it was reshared by a self-de-

cleared group of friends. These kinds of groups are unofficial, and the message was clearly not official neither according to its tone and meaning. Moreover, in the current case, saying that material on the field is not roadworthy is quite common and happens every day without implying sanctions, which makes the statement unrealistic. The goal was to see if they doubted the truthfulness of the comment and the source, and if this piece of information provoked a reaction towards the institution even if the content was not realistic.

5. Interview Results

Qualitative data were analyzed with *Nvivo 12.3.0.* Comments concerning trust in peers and in the institution were submitted to 5 independent judges blind to the situations. Judges, who did not know participants' reported ratings of trust, scored participants' comments regarding trust toward peers and institution (each on the same scale from 0 to 5). These evaluations presented good reliability (Standardized Cronbach's $\alpha_{peer} = .85$; $\alpha_{institution} = .87$) and were averaged to compose two indexes.

5.1. Values and Self Perception

Participants were asked to describe the most important values in their job and personal life. Most of them (80%, $n = 30$) said they were unable to dissociate their personal and professional values: they declared these values were all part of their personality. The most reported values were largely consistent amongst the sample. *Cohesion* took the first place (73%) followed by *Justice/Honesty* in second (58%). *Merit/Professionalism* came in at third place (37%), then *patriotism and sense of sacrifice* were next (26%). Other values such as *love of effort*, *loyalty*, *humility*, *bravery* were far from this top rating with less than a quarter citing them.

Comparing the ranking of values based on soldiers' declarations, and according to the number of sentences referring to these same values, it appears that the declared ranking is not exactly identical with the amount of time spent talking about them; it seems that if they made a ranking, some are more important to them, at least important enough to talk more about them. Nevertheless, no matter the ranking methodology (ratings or numbers of quotes), *Cohesion* is always the top-ranked value, followed by *Justice/honesty*. These results support the assumption that professional and personal values are merged. This outcome fits with the idea that professional values are relevant to the self and involve the individual's self-definition.

5.2. Trusts toward peers and Institution

During the interviews, soldiers were asked about trust. They were asked to assess their trust in several actors in their organization, mainly their group and the military the military institution. Then, they were asked to discuss the nature of this trust. Judges evaluated the transcriptions of soldiers' declarations of this part.

In accordance with the literature, participants expressed more confidence in their peers (M = 4.36, SD = .67; 95% CI [4.14; 4.57]) than in the institution (2.78, SD = 1.04; 95% CI [2.44; 3.12]). This difference is statistically significant (paired t-test : t (37) = 8.12, ps < .01, Cohen's d = 2.67). Trust in peers is very high, with a 1st quartile at 4 (on 5) and a minimum rating assigned to trust in peer on the open scale is 2.5. The mode was 5 (42%, n = 16). Results for the judges' evaluation were similar to those for the self-reports (M_{peers} = 4.12, SD = 0.70; 95% CI [3.89, 4.35]; $M_{institution}$ = 2.33, SD = 0.82; 95% CI [2.06, 2.60]). Judges' evaluation of participants' trust toward their group was significantly higher than for the institution (paired t-test: t (37) = 11.31, p < .01, d = 3.72). The correlation between the judges' evaluations and the self-reported scores was high (respectively, r_{peers} = .50; $r_{institution}$ = .69; all ps < .01). Comparisons of the self-report and judge evalua-

tions were performed and revealed a significant trend for self-report scores to be higher for peers (M = +0.24, 95% CI [0.01, 0.46]; t (37) = 2.13, p = .04) and institution (M = +0.44, 95% CI [0.19, 0.69]; t (37) = 3.5, p < .01).

Regarding the distribution of scores, compared to trust in peers, trust in institution is low both for the self-reports (Mdn = 3.00) and according to judges (Mdn = 2.35). In conclusion, the reported evaluations seem rather honest considering the likely social desirability of the answers. The upward trend concerning institution could be considered as fitting with respect due to hierarchy learnt in training. The examination of the quotes suggests an ambivalence toward the institution: all interviewees made some statement reflecting a lack of confidence, as expressed in follow-up quotes.

5.3. Reason of Mistrust

Complementary analysis were performed to further examine the nature of and the reason for the mistrust. For participants reporting scores below the midpoint of the scale (less than 3.00, n = 14), the explanations were linked with the declared most important values. Common reasons for mistrust were lack of sincerity of the hierarchy and the fact it was perceived as distant (e.g., "*Even if they try to understand us, they can't because they are to different from us*"). Similarly, leaders are perceived as not aware of EO reality and soldiers' life. A participant explained: "*They are cut off from reality.*" Another declared he doubted the information chain and even the interest of leaders, saying that "*I sometimes wonder if all the reports of our experience are really taken into account when I see what we are asked to do. And sometimes we wonder if they take into account the information they get from EO. Even sometimes I have the impression, I wonder ... do they read them?".* *A*nother one explained: *"it is not because they are badly informed that they are disconnected... I*

think they.... [Silence]. *Yes that's it, they think at their level and not for us… I'm not in their heads but that's what I feel. They give orders like that and don't think about the impact for us.*"

Other reasons mentioned for mistrust are lack of professionalism, bravery and honesty. One declared that "*they became fearful chickens.*" Another stated: *"Our leaders are afraid to get involved, to take responsibility.*" Others explained that they have doubts concerning the intellectual honesty of some institutional hierarchy members, or doubts about the relevance of their choices: "*they try but…* [Silence]. *It is just for the show. They try because they are forced to*". Always on *honesty*, some deplored the institution's official communication they have to be part of, and explained "*this spread an image that is a little...* [hesitation] *...which is false* [silence] *which is artificial. And I hate that. We should never be forced to lie* [pause] *particularly on our jobs*". One recurrent reported reason for mistrust was that the institution does not really care about them, because the hierarchy is more interested in operational success. Participants reported not being highly regarded, declaring "*for them, we are just a number in an Excel page*". They also suggested that officers are more interested in their own career, saying"*leaders are more career-minded than able to be brave and take risks to help us.*"

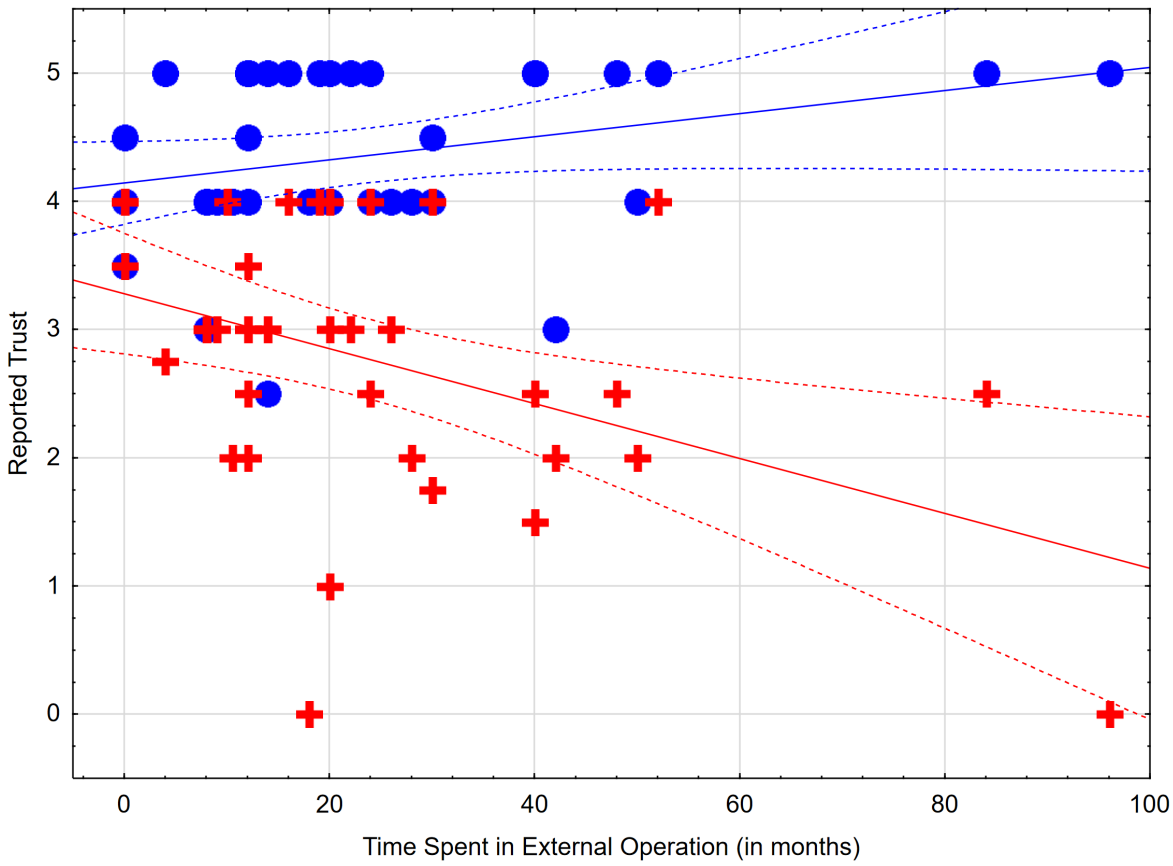
On these bases, mistrust appeared to be a vicious circle. Soldiers felt they are not trusted (and considered) by their leaders and as a mirror effect, they lose their trust in their institution, as explained by one interviewee "*The problem is that our leaders do not trust us any more, they have less confidence in subordinates, and not only the big bosses ."* Consequently, some said that they question orders. Basically, the major reasons for the mistrust are directly linked with the core values discussed previously, namely *Cohesion*, *Honesty/Justice*, and *Merit/Professionalism*.

To investigate the origin of trust and mistrust, quantitative exploratory analyses were performed. The different trust indexes were regressed on soldiers' age, years of engagement and time past on EO. In accordance with the previous paragraphs, only the time in EO is negatively correla-

ted with trust in institution (r = -.43, p < .01), while in the same time, it tends to be positively correlated with trust in peers (r = .28, p = .08) (see Figure 1). These two trust indexes do not correlate together (r = .06, *ns*).

In light of these elements, it appears that most participants do not doubt the military values they reported at the beginning of the interview. But these same values are also the root of their decreased trust in the institution. For the enlisted, it appears unacceptable to observe the non-application of these values and to catch their institution red-handed. We assume values importance increases with EO experience, that can give a beginning of explanation to the above chart. Their experience in extreme situations makes them the most suitable persons to judge the good application of these values, values that are the core of military identity.

Figure 1. Trust in peers (in dark) and in military institution (in light) as function of months spent in External Operations. The dark dots and the light cross represent the associated observations. The dotted lines represent 95% CI.



Finally, in this part of the interview, they were asked about doubts they felt concerning orders. Participants with EO experience (n = 35) were asked if they ever had doubts about the reason why they were deployed, and secondly, if they had doubts about the manner in which they were asked to act. They reported having no doubt on the *Why*. In sum, they approve and accept the general idea of being the "good guys" fighting the "bad guys." But they were more dubious considering the reasons motivating their deployment, explaining that "*sometimes we know that we are not sent into a combat zone just to protect people and save lives but because there are other,* less respectable *interests.*" When addressing the subject of agreement with the *How*, reactions were clear: 80% of this sample confessed that they already experienced doubts. These doubts were important enough that they reported they had already "adapted" an order in accordance with what they thought was really right for the situation. Under cover of anonymity, some said that they had already disobeyed a direct order (e.g., "missing" a shot). This kind of disobedience could have a deleterious impact on operations success and thus presents a risk for the institution strategy. For instance, the refusal to shoot a target could have deadly consequences if the target is part of a terrorist headquarters planning a terror attack aiming civilians. Finally, doubts concerning the institution could have secondary serious consequences, as it is likely to promote disengagement which is particularly costly for the organization. In the present sample, 83% had already considered a career change.

5.4. Use and Confidence in Media

We hypothesized that external information such as media and social media could influence trust in institution or peers. Participants were asked about their use of and confidence in media. They were also asked if they had been warned about Internet risks, and information manipulation, such as giving information inadvertently to adversaries through social network publications

(i.e., localization of units). Considering the average age of the subjects, given that young people are known for their hyperconnectivity (Deloitte, 2017), special attention was paid to Internet use.

Concerning soldiers with EO experience, they mostly used mainstream TV—including web TV—blogs and broadcast platforms such as *YouTube*, to get information, no matter the topic. They mainly (84%) reported having a *Facebook* profile but said they were not using it to inform themselves, explaining that they doubt the data's reliability. Concerning *YouTube*, they all declared that they were regular users, except two who said they did not use *Youtube*.

When asked about the confidence they accord to the different media, as expected considering the training made by their institution, they gave the lowest score for social networks. On a scale from 0 to 5, the highest scores for reported trust are for alternative media (e.g., blogs) (M = 2.73, SD = 1.35), broadcast platforms (e.g., *YouTube*) (M = 2.65, SD = 1.03), then mainstream media (e.g., major TV channels and daily newspapers) (M = 2.28, SD = 1.17) and finally, social networks (e.g., *Facebook*) (M = 1.84, SD = 1.33). Social network was the only one to be statistically differentiated from the others (paired t-test: ts > 3.54, p < .01; d > 1.15). Results are globally low; the best rating was accorded to alternative media. Paradoxically, even if they said they did not trust social media, 84% referred to it in the interview as an argument to convince, using sentences such as "*that's true, just have a look on Facebook if you don't believe me!*"

Time spent on the Internet is not statistically linked to any other variable (all rs < |.30|), but tended to be correlated with trust in peers (r = -.30, p = .08). Finally, whatever the source, 79% said they were more confident in information coming from peers than from the institution, and 89% reported clicking on pop-ups and cyberbait when web surfing.

To assess their reactivity to topics, participants were asked to report the last information watched or read in the media that provoked a reaction, from laughter to anger, no matter the subject,

with a preference for information not linked with their profession. The huge majority of reported information provoking negative reactions was linked to information inconsistent with their core values. *Individualism* (i.e., an antagonist to *cohesion*) caused reaction like "*they do not care about the others, like WE do in our jobs*". Other reactions were linked to unfair criticism of the military from media and/or civilians. For instance, talking about a case of child murder, a participant said that journalists like to stress that a suspect was military personnel: "*This guy* [the child murderer]*, journalists want to show that HE IS a soldier because he is a serial killer, even though he was fired from the army. It is very negative and unfair for us who are fighting to protect people.*" Thus, here the lack of *honesty* and *justice* are triggers. The organization's lack of courage was also mentioned, as well as the lack of patriotism and lack of merit of some people in charge. On that topic, one explained: "*I don't understand why our officers accept playing a part in that sick game, this cowardly game*."

A large majority of participants (85%) reported questioning official information -particularly using alternative media and broadcast platforms- sometimes bypassing their hierarchy. Personal networks composed of other soldiers they personally knew were used as well as networks of people they know only through acquaintances. They argued that people expressing themselves on broadcast platforms had nothing to gain; the apparent altruism of the action was thought of as a reliability guarantee. In their search for information, it appears they are both looking for elements "consistent" with their cognitions and for confirmatory elements.

5.5. Awareness Training and Perception of Being a Target

Soldiers are supposed to receive specific training when deployed on EO about the use of Internet and social network in particular; 95% of the participants reported having performed such training. Near the end of the interview, they were asked if they thought that they could be a target

for Internet information operations intended to influence their behaviour. The interviewer had to re-explain the question regularly because participants generally understood that the aim would be to obtain information from them. Once this point was made clear, only 5% say that they could be a target of influence; 24% said that they could probably be a target but it would not be efficient because they believed they would resist the influence attempt. Finally, the majority (71%) said that they could not be a target and that if this occurred it would not work on them. When they were asked the reasons for their certainty, some did not believe that these operations were achievable, while others said that they would obviously see the attempt at influence. Another reason evoked was they are too sure of themselves and of their values to be subject to influence by these kinds of operations.

6. Staged observation on Core Values targeting

In order to test the strength of the model whereby the entrenchment of the values allows triggering of an expectancy violation, we presented participants with a contrived information situation. This took place at the end of the interview, after all the previous topics were discussed.

Participants were invited to give their opinion of a screenshot of a fake Facebook page. As explained in the Method section, this screenshot was specifically created to target *Professionalism* and *Honesty/justice* values. Additionally, the interviewer explained that she did not check the source or reliability of this comment. She also explained that she just wanted to get their perceptions and feelings concerning this page.

6.1. Reactions to the provoked situation

On the 21 participants, only one reserved his judgment concerning the screenshot. All the others (95%) directly reacted to it, sometimes with strong emotional reactions. The majority (57%) expressed *disgust* or deception. One stated: "*they don't realize, and when something is beyond them*

like that, that's their way to react... anyway they don't care about us at all…" One declared: *"it is maybe the only way we have to make them change, because they are more interested in their face-saving face and image than in the real problems. They are more preoccupied by the form than by the content.*" About 33% of the sample who declared they do not trust hierarchy also expressed a reaction close to *anger*, such as one explaining this was a shame that this situation still happens but that this was particularly indicative of the way the Institution treats them daily. Another explicitly said "*I am really angry at them*!"

None expressed clear doubt about the validity of the source, although two (10%) declared that it was exactly the reason why they did not want to look at social networks, because this kind of information has an effect on their morale and on their faith in their institution. For them, it did not matter if it was true or not, because in their opinion, it *could* be true. The others declared that they were not surprised. One explained that "*he can only be right, that guy, frankly*"; and another said that "*It is true obviously, and yes, things have to be said!*" Another concluded with: "*I am not surprised of that content [...] They don't realize the consequences for us—and they don't care—here we go! But they cannot fight against the freedom of expression of that guy who posted that.*"

When the interviewer specifically asked if they were not surprised that a man was sanctioned just for a statement, they were mostly not (90%). One explained: "*we know the system, you know what we say, 'never surprised, always f*****'*"; another said *"I could have been surprised in the past, but not any more given my experience.*" They globally did question the veracity of the information. In their argumentation, they referred to their own vision of what the military institution should be like—namely based on the values they care for—and on their own experience or peers' experiences.

7. Discussion

The aim of this research was to address the likely consequences of salient discrepancy between the soldiers' core values. The inconsistency models we rely on suggested consequences for the soldiers that could promote risks for the organization. Theoretically, we suggested that the soldiers embedded values presented a risk for the organization if they were exposed to information that confront their peer values to their institution values. We suggested that because the institution trust is less resistant, the expected regulation should favour mistrust toward their Institution, favour disobedience, and thus potentially threaten the organisation performance.

In accordance with the literature, interviews confirmed participants' strong attachment to internalized values based on *Cohesion*, *Justice/Honesty*, and *Merit/Professionalism*. We provided support for the idea that the development and deepening of soldiers' values relies on the experience acquired through EO and that paradoxically, if the institution was the former promoter of the said values, it could be the object of mistrust. Indeed, we showed that trust toward peers was very strong, while trust for the institution is somewhat ambivalent. Lastly, the role of media was examined and we stressed their use and underestimation of the extent to which they are a possible source of information. Ultimately, we gather support from interviews that the mistrust toward the institution is likely to present a risk for the organization, while a large part of the sample of well-trained soldiers already indirectly questioned the order and disobeyed.

7.1. Information Warfare and the Destabilization of the Organization

Finally, in accordance with NGW, and most generally with the rise of information warfare in modern conflicts, a specific goal of this study was to examine if an influence based operation through the Internet could overwhelm the training received concerning Internet use and information

manipulation, and provoke mistrust in the institution. In light of the results, we think we provided some evidence in support of this assumption.

More specifically, we presented participants with fake information that promoted a hierarchical split. It was designed to stress *professionalism* and *rigor* values and it made salient an inconsistency regarding *Justice* and *Honesty* values. We consider the situation was unfavourable to obtain strong effects as the previous interview specifically stresses the importance of media and the awareness training about countering influence attempts, and the interviewer explained the information was not verified. However the results are unequivocal with only one expressed suspicion in our sample and strong emotional reactions from the overwhelming majority. The present observations showed strong reactions linked to mistrust. It thus appears that these kinds of operations are realistic and can obtain results in accordance with the developed models.

The literature underlines the essential role of trust in military teams (e.g., Etzoni, 1961 ; Mullen & Cooper 1994 ; Stanton, 2004) and while the previous interviews already stressed an existing ambivalence toward the Institution, one could easily consider that this kind of operation information will favor disobedience to given order, or at least a decreased efficiency in order execution. The ultimate consequence is the destabilization of the organisation and a decrease of its performance. For Army, the potential consequences are at the level of the importance of its strategic goals: potentially the efficiency of external operations and internal security.

7.2. Limitations and suggestions for further research

To our knowledge, the current study was the first to propose an explication and a controlled observation of these assumptions. However, to bolster future research, some limitations can be stressed. We here considered methodological improvements that could improve both internal and external validity.

First, while the interview sample size was respectable for this population, the staged observation would merit a larger sample. Additionally, while it holds ecological features in the current case, the evaluation of such an important proposal should be subject to an experimental design with a control group and extensive measures. If this reduced the ecological aspects, it could bolster the validity of the conclusions.

Second, a limitation could stem from the studied population. One could indeed wonder if the current observation is generalizable to all the corps and to all the countries. Concerning the military units, one could wonder it the structure of values are the same in the navy or in the air force. We cannot firmly disconfirm this assumption because the whole sample came from the ground force. However, while the participants had various sociological profiles with different experiences, ages and social backgrounds, they all held the same value structures with a similar reaction to its threat. We could thus consider that if they are constrained by the same elements (i.e. trust in peers, potential hierarchical split), they are likely to experience the same consequences. In the same vein, concerning the international generalization and potentially cultural variations, one could obviously consider that there could exist variation in the held values and their importance. Nonetheless, because we rely on a low-level psychological process and because in many cases, the organisation efficiency is based on the unity adhesion to values including trust in peers, we could expect that the process is fundamentally the same, with minor variations on the regulation.

Altogether, the current methodology could be refined. However, according to the literature and in the specific context of military personnel, the validity of this assumption is very likely. In addition, the reactivity of this topic involving security of nations suggests that these findings should be taken very seriously. The present study brings to light a possible way for exogenous influence attempts to destabilize an organization which is based on psychological processes. We consider this as a critical security breach for the institution and we call for complementary studies.

Considering the likelihood of the underpinning process and the importance of the topic for national security strategies, we conclude the paper with some suggestions to limit the risks for the organization and protect them from influence operations.

7.3. Challenge for National Security

In our study, we relied on some media contents that were used for a specific goal. The outburst of new media on the Internet, of mobile data consumption, and the new way people use to inform themselves reinforce the possibility of using these methods to influence special targets in a specific goal. Computer science is already working on software to model individual behavior and factors that influence it manage influence the individual behavior influence and. On another hand the current war strategies suggest using cyber to improve behavior influence is suggested by the current war strategies. One has to expect an increase of influence strategies by foreign powers attempting to destabilize a national institution in the coming years. In the present perspective, influence operations resting on aims central values could be implemented at a massive level with critical consequences for organizations. Consequently, disposing of general models to limit, control and prevent these risks is an essential challenge for national security.

One important raising model from computer science is the Predictability Susceptibility Awareness model (PSA; Santos, 2017). This model argues that there are three important aspects to understanding the behavior of an insider (i.e. a member of a restricted group or organization who has special or secret knowledge or influence). First is Predictability, which is the ability to predict an insider's reaction to a message or situation that can be created in order to influence him. Second is Susceptibility, which is the tendency of an individual to be implicated in any kind of actions that can affect his organization, directly or indirectly and due to internal or external influence. Finally, Awareness is the ability to identify manipulative intent behind false and/or partial information. In

this light, the present data could provide clues concerning elements of the expected outcomes of Susceptibility that can be influenced by the Internet. Indeed, our research helps in understanding dynamic factors (i.e. emotional triggers based on values) that will probably impact the PSA, and consequently the potential insider threat type. Our work contributes to suggested PSA emotional influences from both a psychological and organizational point of view. It helps in defining the previously developed model on aspects of Awareness, namely trust, empathy and through false identity. More exactly, it appears that the internalized professional values can reinforce the first two variables developed by Santos, namely Predictability and Susceptibility, and decrease Awareness.

7.4. Potential paths to prevent the risk

In light of the precedent elements, we think a dedicated training including immersive scenarios and assessment can be created to educate potential targets on the risk they have to face. This proposal will be in accordance with the results of Santos and Hale (2017), considering that situational factors had a much larger impact than dispositional factors. This emphasizes the usefulness of training to improve security, and in our case, trust and cyber security. During training participants can realize they are targeted. Moreover, software tracking the increase in suggestion and reception of values-based information could be useful.

Generally speaking, to prevent organization from these risks, it seems necessary to bolster trust in military hierarchy to secure the organization, to preserve its efficiency and ensure personal safety. Based on our work, we consider that recommendations are of two types: one concerning the human relationship, the other dealing with information technologies. They can also be categorized as three different types of remedies: namely, prevention, detection and correction.

It appears that mistrust can rest on the perception of institutional verticality: As observed, while soldiers perceived the peers as part of their group, and the lack of trust is focused on the hie-

rarchy, which is viewed as an out-group. Here may lie some reasons for the strong distinction between enlisted personnel and officers can be responsible for intergroup relationship perturbations (see Yzerbyt & Demoulin, 2010). Obviously it seems obvious that the Army is not inclined to reduce its the verticality because it is considered an essential part of the organization's structure. Nevertheless, we consider that some suggestions could help to cope with this issue. For example, a dedicated awareness training to prevent this hierarchical split may be taken into account by the Institution's head management. Similarly, increasing the length of time of the middle management positions could favor the both the officers to care more about their men's preoccupations and decrease of their suspicions about officers' intentions. Secondly, concerning detection, psychological tests may be developed to specifically identify men whose trust is affected enough to modify their behaviours. Then, to correct mistrust, developing procedures to increase confidence by building a bridge between enlisted soldiers and commanding officers may be created, for example, by building a stereotypes deconstruction module and elements reinforcing mistrust that could rely on the strong experience of social psychology in the field of intergroup relations.

Another point of reflection could focus on helping soldiers in their second career. To do so, dedicated units composed of former peers specially trained to support soldiers if they decide to change careers could be developed. One virtuous would be that soldiers who decide to stay in the institution are motivated to do so intrinsically, and not because they feel trapped or forced, or because of the cost of disengagement (see Meyer & Allan, 1990). This program could not be implemented under the direction of middle management without raising suspicion, and the institution would have to think carefully about how to implement such a project.

Another work-stream is dealing with information technologies and their management. The current research highlighted that soldiers were not aware of the potential effectiveness of a manipulation carried out over the Internet, and that they were also not aware that they could be targe-

ted as an active agent of information, and. By nature, this unawareness weakens their ability to prevent it. This observation echoes the commonly accepted fact that humans are the weakest link in any cyber system. But denying them access to the Internet would be neither efficient nor realistic. Indeed, the attacks can happen during private time, such an interdiction would appear to be a restriction of freedom, generating rejection and mistrust (e.g. Brehm, 1965). Moreover, as the attacks are not circumscribed to times outside of operation or training moments, denying some access during work hours or on the bases will probably fail to expunge the risk. With this in mind, it seems relevant to develop means of helping soldiers to realize they are targeted by content dealing with their core values. To achieve this goal, specific software programs may warn them when specific content deal with some core military values. In addition, giving them freedom in their use of such devices will reinforce their responsibility as well as trust in the institution. Thus, this tool could serve a dual preventive purpose, both helping them to acknowledge the risk and leading them to realize that their commanding officers trust and support them.

Conclusion

Throughout this paper, we stressed the importance of values in military personnel. From promoted values to internalized values, we showed that they are a central factor in soldiers' trust that plays a central role in their personal development as well as in their daily job. However, these values are also the cause of possible security breaches which can be used by likely malevolent individuals or enemies, especially in times when information war methods developed by various schools of thoughts around the world are increasing, and used during war time as well as during peacetime. Indeed, when a discrepancy is made salient between values promoted by the institution, the latter can suffer from mistrust which could have dramatic consequences for the obedience of agents, thus in mission accomplishment, and can be exploited by adversaries.

In the discussion section, we described the conclusion of these studies that highlight the risk reality of using these methods aiming at trust alteration, we also noticed its limits and expressed why some further research has to be led in order to make other recommendations than the ones exposed here to prevent institution from these risks as it appears clear that mistrust in the military institution by military personnel is a crucial issue. Because the observed rejection of the institution relied on an existing lack of trust which may be emphasized by the enemy's attack, we consider that the means has to involve bolstering trust in the institution and to address the existing gap between soldiers and their hierarchy. We consider that this trust alteration represents a real risk for the organization (i.e. mission success and accomplishment and personnel security). Taking into account the context, namely the risk propagation throughout new technologies such a mobile data consumption, we consider that recommendations that may be done to prevent institution rely both on human management, information management and computer science. For information technologies, the design of tools respecting individual freedom and protecting mental integrity have to be developed. Altogether, these means could address an important issue for national security. For management issues, some proposals have been made in order to improve institution protection towards these kinds of risks.

Finally, one has to admit that the values package including *Trust*, *Respect* and *Honesty* is a blessing and a curse for the army. On the one hand, they are the motivation for soldiers to fulfill their duty, bolstering their morale on the field and their pride in being part of the family. In several weeks of training, individuals integrate values which are becoming central for them and hold the power to accompany them for their whole life. But, on the other hand, these values-based models require great responsibility, as the institution has to be able to exemplify them every day. As a consequence, if possible hypocrisy from the institution is pointed out, these same values become the breach through which adversaries can instil doubt which could shake the whole edific

References

Adams Barbara;, and Robert D.G. Webb. 2003. “Trust Developpement in Small Teams.” Recherche et développement pour la défense du Canada -Toronto. RDDC, N° CR 2003-016, 22

Alter, Norbert. 1993. “La Crise Structurelle Des Modèles d’organisation.” *Sociologie Du Travail,* 35 (1): 75–87. https://doi.org/10.3406/sotra.1993.2109.

Aulakh, Preet S., Kotabe Masaaki, and Sahay Arvind. 1996. “Trust and Performance in Cross-Border Marketing Partnerships: A Behavioral Approach.” *Journal of International Business Studies,* 27 (5): 1005–32. https://doi.org/10.1057/palgrave.jibs.8490161.

Barry Jennifer L. 2013. “A Few Good (Wo)Men: Gender Inclusion in the United States Military.” JIA SIPA. 2013. https://jia.sipa.columbia.edu/online-articles/few-good-women-gender-inclusion-united-states-military.

Bond David. 2018. “UK Military Lifts Ban on Women in Close Combat Roles | Financial Times.” *Financial Times*, October 25th , 2018.

Bruner, Jerome S., and Postman Leo. 1949. “On the perception of incongruity: a paradigm” *Journal of Personality,* 18 (2): 206–23. https://doi.org/10.1111/j.1467-6494.1949.tb01241.x.

Bryon-Portet, Céline. 2011. “Les Pratiques Rituelles de l’École de l’air.” *Communication et Organisation*, 40: 141–62. https://doi.org/10.4000/communicationorganisation.3597.

Chandler, Michael J, Lalonde Christopher E, Sokol Bryan W, and Hallett Darcy. 2003. “Personal Persistence, Identity Development, and Suicide: A Study of Native and Non-Native North American Adolescents.” *Monographs of the Society for Research in Child Development,* 68 (2): 100-138.

Chakravarti, Ashok. (2013). *The Nature and Content of Aid. In Aid, Institutions and Development*. Cheltenam/Northampton, Edward Elgar, 2013. https:/ doi.org10.4337/9781845425524.00008.

Corbin, Juliet M., and Strauss Anselm. (2008). *Basics of Qualitative Research : Techniques and Procedures for Developing Grounded Theory.* London, Sage publication, 2008, 456.

De Richoufftz, E.(1999). *Pour qui meurt-on ?* Paris, De Guibert, 1999, 203.

Cabinet Deloitte. 2015. "Usages Mobiles Les Français et Le Smartphone En 2016 : Une Relation Fusionnelle." Cabinet Deloitte.

Crelley. 2011. "Threat and Selective Exposure: The Moderating Role of Threat and Decision Context on Confirmatory Information Search After Decisions." *Journal of Experimental Psychology: General,* 140 (1): 51–62.

Crene, Yves. 1999. Directive relative aux comportements dans l'armée de terre. Paris, Ministère de la Défense, 1999.

Cvetkovich, George. (1999). The Attribution of Social Trust In *Social Trust and the Management of Risk*, London, Routledge, 1999, 53–61.

D'Alessio, Dave, and Allen Mike. (2013). The Selective Exposure Hypothesis and Media Choice Processes In Preiss Raymond, Gayle Barbara May, Burell Nancy, Allen Mike, Briant Jennings (Eds) *Mass Media Effects Research: Advances Through Meta-Analysis*, New York/ London, Routledge, 2007, 103–118.

Drevets, Wayne C., Price Joseph L, Bardgett Mark E., Reich Theodore, Todd Richard D., and Raichle Marcus E.. 2002. "Glucose Metabolism in the Amygdala in Depression: Relationship to Diagnostic Subtype and Plasma Cortisol Levels." *Pharmacology Biochemistry and Behavior,* 71 (3): 431–47. https://doi.org/10.1016/S0091-3057(01)00687-6.

Dugoin-Clément, Christine. 2018. « Utiliser Les Potentialités Du Cyber Pour Des Opérations Psychologiques Ciblées En Temps de Paix ? » *Dynamiques Internationales,* 13: 1–21.

Evans, Charles R., and Dion Kenneth L.. 1991. « Group Cohesion and Performance: A Meta-Analysis. » *Small Group Research,* 22 (2): 175–86.

Etzioni, Amitai. 1961. *A Comparative Analysis of Complex Organizations On Power, Involvement, and Their Correlates*. The Free P. New York.

Festinger, Léon. (1957). *Cognitive Dissonance.* Stanford , Stanford University Press, 1957.

Fischer, Peter, Andreas Kastenmüller, Tobias Greitemeyer, Julia Fischer, Dieter Frey, and Crelley David. 2011. « Threat and selective exposure: The moderating role of threat and decision context on confirmatory information search after decisions ». *Journal of Experimental Psychology: General,* 140(1), 51–62. https://doi.org/10.1037/a0021595.

Forray, Gilbert. 1990. Charte de l'exercice de l'autorité dans l'Armée de Terre. Paris, Ministère de la Défense, 1990.

Franke, Volker, and Heinecken Lindy. 2001. « Adjusting to Peace: Military Values in a Cross-National Comparison. » *Armed Forces and Society,* 27 (4): 567–95.

Fuller, Mark A., Roger C. Mayer, and Ronald E. Pike. (Eds) *Media and familiarity effects on assessing trustworthiness: "What did they mean by that? »* Hershey, IGI Global, 2008, 19. https://doi.org/10.4018/978-1-59904-495-8.ch005

Gareev, Makhmut. 2016. How Does One Develop a Modern Army*? Krasnaya Zvezda Online,* 11. Unofficial retranscription of speech.

Giles Keir. (2015). Russia and Its Neighbours: Old Attitudes, New Capabilities In Giles Keir (Eds) *Cyber War in Perspective: Russian Aggression against Ukraine,* Talllinn, CCDCOE NATO, 2015.

Greenberg, Jeff, and Arndt, Jamie. (2012). “Terror Management Theory.” In Handbook of Theories of Social Psychology: Volume 1, 398–415. SAGE Publications Inc. https://doi.org/10.4135/9781446249215.n20.

Godé, Cécile. 2011. “Construire Le Sens Par Le Retour d’expérience : Le Cas de l’Equipe de Voltige de l’Armée de l’air.” *Management & Avenir ,* 41 (1): 416. https://doi.org/10.3917/mav.041.0416.

Goffman, Erving. (1959). The presentation of self in everyday life In Newman David , o’brain Jodi (Eds) *Socilogy, exploring he everyday life > readings*, London, Sage ublications, 2008 (7th edition), 46–61.

Harmon-Jones Eddy, and Mills Judson. (1999). Washington, American Psychological Association, 424.

Hart, William, Albarracín Dolores, Eagly Alice H., Brechan Inge, Lindberg Matthew J., and Merrill Lisa. 2009. “Feeling Validated Versus Being Correct: A Meta-Analysis of Selective Exposure to Information.” *Psychological Bulletin ,* 135 (4): 555–88. https://doi.org/10.1037/a0015701.

Heine, Steven J., Travis Proulx, and Kathleen D. Vohs. 2006. “The Meaning Maintenance Model: On the Coherence of Social Motivations.” *Personality and Social Psychology Review,* 10 (2): 88–110. https://doi.org/10.1207/s15327957pspr1002_1

Huntington, Samuel P. (1957). *The Soldier and the State: The Theory and Politics of Civil-Military Relations*. London, Harvard University Press, 1957, 550.

Jonas Eva, Schulz-Hardt Stefan, Frey Dieter, and Thelen Norman. 2001. “Confirmation Bias in Sequential Information Search after Preliminary Decisions: An Expansion of Dissonance Theoretical Research on Selective Exposure to Information.” *Journal of Personality and Social Psychology,* 80 (4): 557–571. https://doi.org/10.1037//0022-3514.80.4.557

Karsenty, Laurent. 2015. “Comment Maintenir Des Relations de Confiance et Construire Du Sens Face à Une Crise?” *Travail Humain,* 78 (2): 141–64.

Knight, Franck. (1923). *Risk, Uncertainty and Profit.* Lanham, National Book Network, 1923, 448.

McGregor Ian, Zanna Mark P., Holmes John G., and Spencer Steven J.. 2001. “Compensatory Conviction in the Face of Personal Uncertainty: Going to Extremes and Being Oneself.” *Journal of Personality and Social Psychology,* 80 (3): 472–88.

Ministry of Defence. (2018). Defence Statistic 2017. UK Armed Forces Biannual Diversity Statistics 1 October 2017. London, MoD, 2018

Ministère des Armées. (2018). *Bilan social 2017.* Paris, Ministère des Armées, 2018

Ministère de la Défense. (2002). Brochure Armée de terre 2002, document diffusé aux officiers généraux et aux chefs de corps par l’État-Major de l’Armée de Terre en avril 2000. Paris, Ministère de la Défense, 2002.

Moons, Wesley G., and MacKie Diane M.. 2007. “Thinking Straight While Seeing Red: The Influence of Anger on Information Processing.” *Personality and Social Psychology Bulletin,* 33 (5): 706–20. https://doi.org/10.1177/0146167206298566.

Mullen Brian, and Copper Carolyn. 1994. “The Relation between Group Cohesiveness and Performance: An Integration.” *Psychological Bulletin,* 115 (2): 210–27. https://doi.org/10.1037/0033-2909.115.2.210

Myers, Michael D. (2008). *Qualitative Research in Business & Management*. London, Sage publication, 2008, 296.

Oliver Laurel W., Harman Joan, Hoover Elizabeth, Hayes Stephanie M., and Pandhi Nancy A.. 1999. “A Quantitative Integration of the Military Cohesion Literature.” *Military Psychology,* 11 (1): 57–83. https://doi.org/10.1207/s15327876mp1101_4

Orléan, André. 1985. Hétérodoxie et incertitude, *Cahiers du CREA,* n°5, juin 1985, Ecole Polytechnique, 247-275.

Price, Joseph L., and Drevets Wayne C.. 2010. "Neurocircuitry of Mood Disorders." *Neuropsychopharmacology,* 35 (1): 192–216. https://doi.org/10.1038/npp.2009.104

Price, Joseph L., and Drevets Wayne C.. 2012. "Neural Circuits Underlying the Pathophysiology of Mood Disorders." *Trends in Cognitive Sciences,* .61-71. https://doi.org/10.1016/j.tics.2011.12.011

Rivolier, Jean. 1998. Stress et situation extrêmes. *Bulletin de Psychologie, 51*, 6-20.

Ross, Michael. 1989. "Relation of Implicit Theories to the Construction of Personal Histories." *Psychological Review,* 96 (2): 341–57. https://doi.org/10.1037/0033-295X.96.2.341

Rydell, Robert J., MacKie Diane M., Maitner, Angela T., Claypool Heather M., Ryan Melissa J., and Smith Eliot R.. 2008. "Arousal, Processing, and Risk Taking: Consequences of Intergroup Anger." *Personality and Social Psychology Bulletin,* 34 (8): 1141—52. https://doi.org/10.1177/0146167208319694

Santos, E. (2017). A social, cultural and emotional basis for trust and suspicion manipulating insider threat in cyber intelligence & operations. *BRI: Cyber Trust and Suspicion*. El Paso: University of Texas.

Santos, E., & Hale, J. (2017). Targeted interventions derived from biomarkers of cyber trust. *BRI: Cyber Trust and Suspicion.* El Paso: University of Texas.

Schweisguth, Etienne. 1995. "La Montée Des Valeurs Individualistes." *Futuribles* 200 (Juillet-Août): 131–160.

Schweisguth, Etienne. 1978. "L'institution Militaire et Son Système de Valeurs." *Revue Française de Sociologie,* 19 (3): 373. https://doi.org/10.2307/3321050

Siegrist,M.,Cvetkovich, G.,Roth, C. (2000). Analysis Salient Value Similarity, Social Trust, and Risk/Benefit Perception. *Risk Analysis*, Vol. 20, 3, 353-362.

Steele, Claude. The psychology of self-affirmation: Sustaining the integrity of the self. In R. F. Baumeister (Ed.), Key readings in social psychology. The self in social psychology, Psychology Press, 1999, 372–390.

Vaidis David, and Gosling Patrick. 2011. "Is Commitment Necessary for the Arousal of Informational Dissonance?" *Revue Internationale de Psychologie Sociale,* 23: 33–63. https://www.researchgate.net/publ

Yzerbyt, Vincent & Demoulin Stéphanie. (2010). Intergroup Relations In *Handbook of Social Psychology.* Hoboken, John Wiley & Sons, Inc.1024-1083. https://doi.org/10.1002/9780470561119.socpsy002028

CHAPITRE 6 : La hiérarchie des valeurs hiérarchiques et l'évolution de la confiance dans l'organisation

Dans le chapitre précédent, la notion de valeurs est clairement apparue comme un des éléments constitutifs de la confiance ou comme étant a contrario capable de participer à son altération. Les valeurs ayant une influence à ce point prépondérante dans la constitution de la confiance et, partant, dans la fiabilisation de la structure organisationnelle, il est nécessaire de s'interroger sur le rôle potentiel de la hiérarchisation de ces dernières, dans l'évolution de la confiance et dans la sécurisation des stratégies de l'organisation. Aussi, ce chapitre s'attache à analyser l'incidence de la hiérarchie des valeurs fondatrices de la confiance dans la prise de décision. Plus particulièrement, il propose un décryptage de son implication éventuelle dans le mécanisme intellectuel pouvant aboutir à un acte déviant se traduisant par une action en désaccord avec la stratégie que l'organisation veut appliquer sur le terrain de son activité principale. Un des axes de réflexion consistera à analyser si un écart entre la hiérarchie des valeurs de l'organisation et celle de ses agents peut constituer un facteur d'amélioration ou de dégradation de la coopération. Dans ce chapitre, comme dans les précédents diverses sources (entretiens, observation, documents) ont été utilisé pour valider ou invalider les propositions découlant de la problématique.

Ce travail a fait l'objet d'un article intitulé « values hierarchy role decision-making and execution order in extreme situations », soumit à la revue European Management Journal.

Le tableau ci-dessous présente les sources utilisées pour valider ou invalider les propositions présentées dans ce chapitre, propositions découlant de la question de recherche centrale et de ses subdivisions en sous-problématiques auxquelles elles sont rattachées.

Question de recherche	Quelle possibilité de mettre en place des stratégies informationnelles dont l'objectif serait d'altérer la confiance en ciblant les valeurs coeur des individus afin de déclencher une prise de décision déviante revenant à ne pas executer les ordres comme dispensés par l'organisation?			
DONNEES DE RECHERCHE		Entretiens	Documen	bservatior
Sous-Problématiques	**Déclinaisons**			
Altération de la confiance et prise de décision	La confiance comme facteur de coopération	V	V	V
	La confiance, pierre angulaire de la gestion de la coopération au sein des équipes en situation extrême	V	V	V
	La hiérarchisation des valeurs influence l'évolution de la confiance	V	NV	V
Les valeurs et le renforcement de la confiance et des mécanismes de coopération	La hiérarchisation des valeurs divergent entre les différentes strates hiérarchique de l'organisation	V	NV	V
	La hiérarchisation des valeurs divergent entre les différentes classes d'âge	V	V	V
	Un écart dans la hiérarchisation des valeurs de l'organisation et de ses agents constitue un facteur de dégradation de la coopération	V	NV	V

Tableau présentant les sources utilisées pour valider ou invalider les propositions présentées dans le chapitre 6

1. Introduction

In order to be efficient organizations have to secure the systems that will support their overall strategy. This cornerstone of organization's management is recurrent no matter the activity sector they are dealing with. One of the main problems faced when deploying their strategies is the deviant execution of the guidelines. Indeed, their employees do not always react as expected by their hierarchy. By deciding not to strictly execute the organization's guidelines, employees may participate in a disorganization motion that may have direct consequences. If it is a recurrent issue, the consequences can be particularly devastating for organization working in extreme situations, namely, unpredictable, risky and evolving (Girin, 1990, Lièvre, 2005, Lebraty, 2013). Consequently, for armies that are particularly representative of this king of organizations, if the gap is too wide between organization expectation and order execution, consequences may endanger human-being lives and national security. With this in mind, it appears particularly relevant to define which factors may be at the origin of this gap between the deployment target and its implementation in practice.

Considering armies, they are organizations basing their identity on a strong package of values, shared and even taught to their personnel. Some authors developed a field of research on values in organizations, the way they influence team spirit, behavior and decision-making. Edgar Schein (2004) postulate that values are used as a part of organization culture by many managers. He explained that organization culture based on values helps understanding the personnel behaviors as well as the interactions taking place in between the groups, because its members identify themselves and recognize each other as a peer in the light of these common elements. Considering values as a part of organization culture, we understand that these elements are not only shared, but also stable in time. Moreover, the rooting of these elements

have to be deeply implemented to be considered as cultural; lastly, culture has to be pervasive, to irrigate all the spectra of the institution. Consequently, values that composed organizational culture may be supposed to be an element helping to avoid a decision-making implying a distorted order execution by creating a social control helping perceive people or manipulating their thoughts and even feelings (Kunda, 1992). Accepting the statement that values are an obedience guarantee of teams address the question of the consequences of discrepancies in values hierarchy between the institution and personnel on organization efficiency in terms of order execution reliability.

We postulate that studying armies will be particularly relevant because, as working in extreme situations, observation should be facilitated because the reactions and perception should be paroxystical. This is in line with Schein's culture theory in which he explained that to observe deep assumptions that are part of cultural values, the better way is to try to observe and understand perceptions and feeling arising in critical situations. If these theory on organization values are right, it may be interesting to observe if a different hierarchy ranking in hierarchy may be observed between organization and its employees, as well as in between the group members. The goal is here to observe if these discrepancies in values hierarchy may have an influence in decision-making and thus in order execution that is one of the main issues for organizations.

This study is based on dedicated theoretical framework stems from a first sample of exploratory observations and based on the relations of values and organizations. Consequently, a first part will deal with the theoretical approach before exposing the exploratory observations and the resultant hypothesis. Then this paper will present the second sample of interviews led in order to test these hypotheses, before concluding this study.

2. Theoretical framework

The theoretical framework refers to the role of values in the management of organizations. In our context of taking decisions and respect orders in extreme situations, we refer to the possible influence of values on organizational culture and identity building. The impact on the decision-making process and more generally on organizational behavior face to this kind of situation should be considered.

2.1. Influence of values in organizational culture and identity

Organizational cultures and thus the values on which it is built is a major topic in organizational studies. But it is regularly overwhelmed by the research on organizational identity based on discourse and communications of firms. Nonetheless organization's culture is widely perceived as a key tool in management and thus on efficiency (Schield, 2004; Martin, Frost, Olivia & O'Neill, 2006; Alvesson, 2011). But the term of culture itself is a subject of debate. We here are focused on the values that composed it, so we refer to the Kunda vision (1992) for whom culture is the result of shared rules governing cognitive and affective aspect of membership in an organization, and the means whereby they are shaped and expressed', Smircich (1983) talked of a shared system of meanings that won't be reinterpreted constantly. This is in adequacy with our research subject; indeed, armies built a large part of their culture on shared values the organization taught to its staff. As in Smircich and Kunda's visions, this set of values may be taught and not primarily in the employee's minds. Similarly, according to Alvesson (2011) culture may be defined as a shared and learned set of experiences, meanings, values and understandings. As for Schein, Alvesson exposed that this set has to be stable. In our case, armies postulate that its set of values is unique and represents an overall and unquestionable package of meanings, values that once diffused by the head of the organization will re-

sult in a sense of hierarchy and of priority shared by all the elements of the organization. This vision is quite close to Schein's (1985) but maybe field observations may highlight that this is not as homogenous as presented here. Some theories defend the possibility of ambiguity and fragmentation (Martin, 2000; Martin & al, 2006) in organizational culture, thus in values diffused through. According to these authors, differences will emerge from competing groups, often vertically structured, which behavior is manly led by domination or resistance, which apparently will not fit with our research field. Fragmentation theory is developed as an unavoidable state as long as the organization reality is dynamic.

Nonetheless, it is commonly accepted that an organization that won't be able to master a moderate level of common meaning and understanding will probably not be able to perform in a competitive environment and may even not survive. If this is the case in the business world, it will probably be even obvious to organizations dealing with extreme and risky situations. Because these kinds of risks must be eradicated because they already have to face extremely complicated and risky situations. This is why this organization, to secure its process, worked to reinforce its culture in the minds of its employees, conferring these values to identity. In transforming these cultural elements, namely values, in part of the identity, the Institution expects to merge organizational identity, social identity and self-identity what will make employees' behavior and way to decide predictable, and thus secured, as developed by Gioia & Thomas (1996). Moreover, according to Alvesson and Empson (2008), it seems that armies may benefit from a strong identity as it is constructed as very distinct, generally based on values considered as highly positive and significant for the organization employees. Another point reinforcing this idea that armies can easily be portrayed through few characteristics, and many of the personnel define themselves primarily through their institution (Dutton & al, 1994). If research had been realized on these concepts in everyday organization's life and in

business competition environment, they do not study on the peculiar context that extreme situations are, which is the target of this paper is.

2.2. Values influence in decision-making in extreme situation

The role of values in decision-making had been studied in different research fields, including management. Many works questioned the role of personal values in professional decision-making (Green, 1998), other questioned the role of emotions and affects in a usual context (Loewenstein & Lerner, 2003). Other studies are focused on decision-making in medical context, and most of the literature is focused on the leadership decision-making or middle management level. Other studies observing the decision-making in risky situations are focused on an economic approach and not in the context of extreme situations (Gollier, Hilton & Raufaste, 2003; Kahneman & Tversky, 1979). Considering the context of armies, studies deal with the ethical influences of orders, or on the decision-making in commandments and control (Bryant, Webb, McCann, 2003). But these studies are mainly based on headquarters or management level. Observing the recent increase of operations aiming manipulation at large scale on populations (and military personnel) observed in Ukraine, and considering the direct consequences of an affected order's execution led by a deviant decision-making of soldiers it appears relevant to work on this special case.

2.3. Values in specific context of organizations evolving in extreme situation

Generally speaking, as explained in the previous paragraph, organizations try to establish coherency between their activities and behavior socially considered as acceptable. To do so, they can try to develop and settle a package of values that can be read as a trigger for their actions, and linked with the social acceptability (Dowling & Pfeiffer, 1975). Consequently, if organi-

zations succeed in creating a congruence between this two systems, values and social acceptability, it helps create their own legitimacy. Focusing on organizations evolving in extreme situations (Lievre, 2009) like the Army, building legitimacy can be paramount to be ensured of personnel loyalty if they have to face direct and personal risks, or to act in a way that society usually reprobates. This is indeed particularly obvious in armies whose action can be socially not accepted when soldiers have to wound or killed adversaries. Observing extreme situations, we notice that because of their uncertainty, they do not possess the structure allowing rational believing as explained by Viviani (1994). Thus in order to maintain a rational behavior and decision-making, organization can use values as a 'behaviour insurance' of their personnel. As armies are by nature used to work in an extreme situation, and as there is evidence that military experience affects the life course (Settersten, 2006; Ludtke, Trautwein, & Husemann, 2009; Robins, Fraley, Roberts & Trzesniewski, 2001; Thoemmes & al., 2012) it appears relevant to observe how soldiers deal with the army's values as a case subject.

As context elements, British army (2008) exposed that 'Values and Standards directly contribute to the Army's ethos and to fighting power. They are a moral requirement and have functional utilities. Upholding them is the collective responsibility of all members of the Army. (…) If any one of them is lacking, the team and the mission are threatened.' Here appears clearly how values can be used in a functional way to secure the mission and efficiency of the mission and thus the efficiency of the organization. Similarly, this highlights they are linked to one of the first necessary values, namely cohesion. Concerning the values developed by the British army, we can quote selfless commitment, courage, discipline, integrity, loyalty and respect for others. These values seem to be quite widespread. Indeed, the French Army developed a close panel of values including trust, team spirit, self-help, respect for oneself and others, courage, will, perseverance, merit and patriotism; as well as US Army who synthesize

them through the acronym LDRSHIP (Loyalty, Duty, Respect, Selfless service, Honor, Integrity, Personnel courage).

If we can notice these values are pretty close independently of the armies' nationality, we can also observe that they are quite similar to those diffused by past armies. Nonetheless, armies realized a long time ago the necessity of values for their effectiveness. Not only they help soldiers accept the risks and the possibility of the 'ultime sacrifice', but it helps face these eventualities without deviating from the execution of the orders. This echoes Huntington theory (1957) in which military values would depend neither on the time nor the place as well as the definition of organizational culture as though by Schein (i.e. stable). In the image of the military profession values would be the intellectual expression. On another hand, for Schweisguth (1978) institution tries to establish control on its members by imposing norms whose justification implies the reference to a symbolic system. He also noticed that in the case of the military institutions, this is particularly effective as the profession requires soldiers to defer themselves to the general interest. Another aim of value diffusion is the limitation of reassessment and questioning of the orders. In other words, it is a way to increase the soldier's reliability and obedience, to avoid a random execution order due to a personal decision-making deviates from the one expected by the organization. With this in mind, it appears that values are a keystone in armies' organization. As their activities take place in an extreme situation which has a considerable potential of crisis emergence (Lebraty, 2013). Moreover, due to the nature of constant tension known in extreme situations, crisis happening there may have even more disastrous consequences than intended in the economic field. Studies on values hierarchy are not numerous. Schwartz and Bardi (2001) realized a work on school teacher values. In this study it appears that value hierarchies presented a widespread consensus even if some differences appeared to depend on normative cultural baseline. We point out that beside the cultu-

ral differences, school teachers are not commonly confronted with extreme situations as soldiers are. This lack of research on that topic was an invitation to dig in that matter, to define is values hierarchy of soldiers and of the organization are the same, and possibly if these values created some typical behavior, routines or reflexes. To do so, the first set of exploratory interviews were led in Ukraine, a country at war, in 2017, and a second in France in 2018.

3.Data collection and research proposal

Values, organizational behavior, decision-making processes are phenomena which suppose to observe and have the feedback of people inside the organization. A qualitative methodology was developed to collect data able to help us to generate proposals applied to the specific context of extreme situations.

3.1. Establishing proposal through exploratory Interviews

In order to observe the role and hierarchy of values in extreme situations, interviews were led in Ukraine in 2017. For this purpose 30 soldiers were questioned, some were in active duty, others were veterans because of injuries, all had a recent fire experience. They were not equally ventilated in gender, on the 30 subject only one was a woman, but they were equally dispatched between veterans and active-duty soldiers. Their ages varied between 21 and 59. Some of them have an experience in the military field but biggest part taken up arms with the rise of the Donbass war in early 2014. The survey takes place in two different cities. The original planned place was at this exact time facing a very violent battle and it was not possible to go safely there. Consequently, it was decided to go in those cities, also located in the east of Ukraine. One is known for its high quality hospital and a military school is settled in the other. Both of these cities were strategic fall back points; consequently many soldiers could be met there.

Local contacts introduced the searcher in the hospital of one city and in a center where soldiers were used to go to meet each other in the other city. It was explained that people who want to be part of this inquiry had to come back at a specific date in order to proceed to the interview with the help of a translator. Soldiers were ensured of their anonymity and that the interviews would not be transmitted nor published, equally for national security motives than to increase their confidence with the researcher. Surveys were not directed but used recurring questions allowing defining a guideline pattern and used a qualitative approach in order to get as much information as possible and to help subjects to relax and be as natural and honest as possible, considering the context and the sensitiveness of the questions asked. Nonetheless, some queries were asked in recurring way in order to obtain a question set. These interviews sometimes led to follow up discussions, using Skype or emails, at the soldier's initiative. Concerning values topics, subjects were not submitted to any listing of values, when they choose to mention values it was from their own and not under incitation.

Even if interview guidelines may not be communicated according to the engagement taken and already explained, we can expose the main point addressed during surveys. In a first part they were questioned about their identity, namely, age, time of service, ranking, if they took up arms recently or if they already were professionals. They were questioned about the reason of their engagement, and in this part, they often talked about their values. They were also questioned on the trust they accorded to their group, to their commandment and to their government, and they were invited to develop the reason for their rankings. They were also asked what they want to do next, namely knowing that the conflict was still raging, and even after when peace will have returned.

3.2. Results of the exploratory interviews

During the interviews, some value appears clearly as recurring, namely patriotism, sense of sacrifice, courage, honor and honesty. Most of them use as punctuation the expression ‘Slava Ukrainy !’ meaning ‘ To Ukraine! » Many of them explained that they make this particular choice to take up arms and risk their own lives because they have to defend their homeland and to protect their family and child. As if their patriotism can help them face, everything and was a motivation to face their everyday war zone life. This appears in active duty soldiers as well as in veterans’ interviews. As well courage and honor appears as clearly linked and were recurrently quoted.

In discussion they talked naturally of their commandment and government, and it appears that they did not appreciate them. When asking if they trust their commandment, those who accept to answer the question – namely 12 – confessed a lack of trust (ranking it between 0 and 1). When asking why they were not trusting their hierarchy, they explained that because they had no values or, not the same values they were not trustable. And they highlight their statement with some example of the field reality. As an example one explained to us that, *‘they are not true patriots, they go to hide in Kiev, but they are not courageous.’* Another explained, ‘*they are wearing figures for the cameras, but they are not real patriots! We are. We will die for our country and our family, Slava Ukrainy*!» Another recurrent element was their sense of sacrifice. They regularly quote that they did not regret their wounds because they accept to sacrifice as the one who already faced several operations due to the same wound ‘ *If I had to do it again, I will. I do it for my country and for my girl, I want her to be proud of me.”* By mirror effect they reproach the lack of sense of sacrifice to their commandment. None of them refers clearly to cohesion.

On another hand when talking with some officers met in these cities and not included in the

exposed set, it appears that if patriotism was always ubiquitous, honesty was also regularly quoted. One based in Kyiv and in the city to visit the wounded explained, *'The more important is the honesty of the approach of people who get involved in that war. The fact that they decide to fight or to participate in the war effort for good reasons.'* Some also explained that it was paramount to defend their country which directly refers to patriotism, but sense of sacrifice was not as present as in the survey's set.

After analyzing the Ukrainian soldiers, it appears that all the values set deployed by armies and exposed previously was not quoted. As an example compared to the values developed by the US Army, namely, Loyalty, Duty, Respect, Selfless service, Honour, Integrity, Personnel. Loyalty respect and integrity were never quoted or evoked through illustrations. Compared to French pattern (trust, team spirit, self-help, respect for oneself and others, courage, will, perseverance, merit and patriotism) self-help, respect for oneself and others and merit were absent. Analyzing the delta with British standard (selfless commitment, courage, discipline, integrity, loyalty and respect for others), discipline, integrity, loyalty was not quoted. As after mentioning, western armies are often built on the same pattern particularly considering their values and Ukraine is no exception, so we could expect to find the same values, which is not. Another observation is that their trust in their commandment appeared as deeply impacted. If the organization of armies is well known and had been the subject of many research, the possibility to affect trust in the institution by targeting the army values as not yet been fully studied. In this work, we analyzed the interviews in encoding the positive and negative assertions towards the institution. Both positive and negative assertions were also linked to the values interviewees referred to in order to justify their answer when they did it.

3.3. Trust and hierarchy values, an interaction

Looking to the results of the interview, concepts which emerge were related to the role of trust and values in this extreme situation. Trust is the generally considered as the cornerstone of military cohesion and thus of performance of military teams. The issue of trust is prevalent in academic literature dealing with military affairs.

According to some authors, trust has cognitive and affective underpinnings (McAllister, 1995), and it is a cohesion factor. Some meta-analytic studies show a positive relationship between cohesion and performance (Mullen & Cooper, 1994). Considering the military field, performance means achieving the goal of the success of the mission with the least possible loss. Thus, trust is linked with cohesion and performance. According to other sources, there are three main components in military cohesion: peer relationships, relation between superiors and subordinates, and relation towards the armed forces and the government (Stewart, 1988; Etzioni, 1961). Therefore, for soldiers, degrading the perception of government and increasing mistrust in superiors will deteriorate cohesion and performance.

If trust is considered as essential, it remains a nebulous concept that needs to be clarified; indeed many works gave different definitions of this concept. Referring to Bhattacharya & al, it is '*the expectancy positive outcomes based on the expected actions of another party in an interaction based on uncertainty*' (Bhattacharya & al, 1998). Another definition talks about psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another (Rousseau & al, 1998). A last definition of trust is by Mayer, Davis and Schoorman's as '*a willingness to be vulnerable to another party when that party cannot be controlled or monitored*' (Bayer, Davis and Schoorman, 1995). 'Loyalty,' has also been identified as a keyword when dealing with trust (Adams, 2003). These definitions are particularly relevant in military affairs because it is a field where people evolve in

extreme situations. Consequently, the acceptance of vulnerability takes a realistic turn as soldiers can be wounded or even die in operation. Previous definitions of trust described uncertainty as a game changer. If thinking these concepts with Rivolier (1998) and Girin's (1990) definition of extreme situations, though as evolutive, with a high rate of uncertainty for people involved in, trust appears as a key element. Some authors even describe extreme situations as a moment when the unexpected can appears (Orléan, 1986). To be considered extreme, a situation must also be risky (Lièvre, 2014). These theoretical literature on trust explains the interest of organization working in extreme situations to develop a dedicated culture and identity based on a strong set of values. The necessity of trust is clearly paramount in armies and needs to be found on stable and deeply rooted values exactly as described by Schein. Considering these elements and the previous observation during the exploratory interviews we can logically posit scheme proposals, namely :

1. There is a discrepancy in hierarchy values between military personnel and their commandment
2. There is no discrepancy in hierarchy values in between the member of a military personnel groups
3. When this gap in value is identified, it is linked to the age of personnel
    1. Sub-proposal the X, Y and Z generations are a segregating effective factor
    2. Sub-proposal this division is shaped by the service time, and can be reinforced by the time passes in exterior operation
4. Values are main actors in lack of trust: when institutions members are caught red hand in default of these values, trust is altered
5. A change in the hierarchy of values have an impact on decision-making and consequently in order execution.

Theoretical framework	Concepts mobilized	Propositions
Organizational culture	Institution tries to establish control on its members by imposing norms, in the case of the military institutions, this is particularly effective as the profession requires to soldiers to defer themselves to the general interest (Schweisguth, 1978) Organization culture (i.e. values and beliefs of an organization) commands how individuals interact with each other and behave with people outside the organization (Schiele, 1980; Schield, 2004) In transforming values in part of the identity, the Institution merge organizational identity, social identity and self-identity what will make employees' behavior and way to decide predictable, and thus secured (Gioia & Thomas, 1996)	N°1- There is a discrepancy in hierarchy values between military personnel and their commandment; N°2- There is no discrepancy in hierarchy values in between the member of a military personnel groups; N°3-When this gap is identified, it is linked to the age of personnel (with sub proposal N°1 & 2); N°5- A change in hierarchy of values have an impact on decision-making and consequently in order execution.
Values hierarchy	Value hierarchies presented a widespread consensus (Bardi & Schwartz, 2001)	N°1- There is a discrepancy in hierarchy values between military personnel and their commandment; N°2- There is no discrepancy in hierarchy values in between the member of a military personnel groups.
Trust	Trust is '*the expectancy positive outcomes based on the expected actions of another party in an interaction based on uncertainty*' (Bhattacharya & al, 1998), or '*a willingness to be vulnerable to another party when that party cannot be controlled or monitored*' (Bayer, Davis and Schoorman, 1995) Trust is the generally considered as the cornerstone of military cohesion and thus of performance of military teams There are three main components in military cohesion/trust: peer relationships, relation between superiors and subordinates, relation towards the armed forces and the government (Stewart, 1988; Etzioni, 1961).	N°3-When this gap is identified, it is linked to the age of personnel (with sub proposal N°1 & 2); N° 4 -Values are main actors in lack of trust: when institution's members are caught red hand in default of these values, trust is altered.
Extreme situation	For organizations evolving in extreme situations building legitimacy can be paramount to be ensured of personnel loyalty and trust if they have to face direct and personal risks, or to act in a way that society usually reprobates (Lievre, 2009; Lebraty, 2013)) In extreme situations, because of uncertainty, people involved do not possess the structure allowing rational believing as explained by Viviani (1994). Thus in order to maintain a rational behavior and decision-making, organization can use values as a 'behaviour insurance' of their personnel.	N° 4 -Values are main actors in lack of trust: when institution's members are caught red hand in default of these values, trust is altered; N°5- A change in hierarchy of values have an impact on decision-making and consequently in order execution.

Summary table of the theoretical framework and concepts mobilized in the proposals.

4. Proposition validation through a second set of interview

The coming part will present a case study helping to validate or invalidate the proposal in a first step and, in order to go beyond to define a grid of interpretation based on a theoretical framework able to be applied and to give comprehension key to others extreme situation context.

For this purpose we choose the subjects' profiles in accordance with the results of the first interviews and the element from the theoretical framework. The current research relies on interviews allowing qualitative data collection. Qualitative approach was chosen because of the specificity of the topic and because accessing honest responses requires to achieve a trust relationship. Moreover, it seems more relevant particularly as one aim was to encode the answers and explanations concerning values meaning to observe if it was in accordance with the declared ranking. Additionally, as Maxwell said (2005), qualitative approach is very powerful when focused on people and phenomena, which is exactly the case here. It allows relevant observations when studying the subject in depth when considering personal topics (Myers, 2008). Thus, our subject deals with professional values potentially merging with personal ones so deeply that they become part of people self-construction. For these reasons, interviews were led in 2018 with 38 subjects of organization working in extreme situations, namely, the Army.

4.1. Population and Data Collection

Thirty-eight one-to-one interviews with soldiers (all male) in active duty were led. Military hierarchy informed them and the interviewees volunteered with the assurance of complete

anonymity. Even if the interview were audio recorded with their full agreement, they were assured that recording would be destroyed after de-identified transcriptions and that data or transcriptions would not be transmitted to anyone. The interviews were performed by a female investigator, one of the authors. They took place in different military bases during several consecutive days. The investigator had time to acquire confidence from the units. The interviews lasted between 45 minutes to two hours, depending on the participants. Most of the interviewees were deployed in a war zone from 4 to 96 months with a median time in operation of 18.5 months, only three men were never deployed and used as a control sample. Considering their experiences, they were comparable in their nature. Indeed, the missions were almost similar and involved in comparable theaters. Except for the sample group, they had an operational experience in war zones. They were all males between 23 and 45 years old ventilated as such: 3 were of the Generation X (born between 1965 and 1977), 24 of Generation Y (born between 1978 and 1990) and 11 of the Z-generation (born after 1990).

The interviews were open and not directed even if some theme were systematically covered. Indeed, the discussions contained a series of recurring questions focused on topics studied such as values and trust given in peers and in commandments.

Nonetheless, it seems more efficient to choose a free approach to grasp the essence of the interviewees' perceptions and appreciations of their professional and personal values. Additionally, long time and free interviews illustrated with examples from interviewees allowed going beyond the socio-discursive conventions governing culturally and socially acceptable ways of talking about individuals or institutions. Assuming that these conventions are unlikely to be linked to the practices of trust and distrust, a long exchange using examples and illustrations helped to circumvent this bias.

They were both questioned on professional and personal values without any quotation of the army package from the investigator. They were invited to quote the values they perceived as the most important in their profession and to expose the reasons for their ranking.

To obtain qualitative data, they were also invited to explain the reason why they think these values are so important and to clarify their very meaning, involving examples if necessary.

Concerning trust, they were invited to grade to their confidence in peers and in their institution. As in the trust approach, they were encouraged to explain their ranking. On this item, they were invited to give their grade using a 5-degree Likert scale. It was clearly explained that 2.5 was 'no distrust but no trust either,' as a middle, neutral point.

For a second time, they were asked to explain the very nature of these trusts, potentially giving examples. These explanations and illustrations were particularly relevant to refine their first quantitative declarations. Indeed, according to their job and its necessity of obedience, the goal of this double interrogation was to avoid an 'agreed upon answer' not representative with their real perceptions. Re-transcription of the interviews were analyzed with Nvivo 13 based on a coding in link with the hierarchy of values, namely encoding discourse in adequacy with quoted values, with trust and with decision-making and order execution applied by the interviewees.

Finally, the transcription of the interviews were studied and coded with Nvivo 13. The coding was made on nodes based on the theoretical framework. The classification of the value was made through two different methods. One only based on the interviewees declared ranking, the other one was made according to the time people spend talking of these values. For instance, sentences as ' for me, the most important thing is the relation I have with my colleague, we are very linked … something as a family, this is cohesion and it is the most important va-

lue for me in my job' were linked with the node 'cohesion in peers—> positive', and integrated in the calculation of the time spend talking of cohesion. As another example quote like 'for them, we are just a number in an Excel page' was coded in 'trust in the hierarchy—> negative', some other quotes may be coded in different nodes such as '*our leaders are afraid to get involved, to take responsibility*' have been coded in 'trust in the hierarchy—> negative', and in 'value—> courage', and 'sense of responsibilities'.

In the end, some data were exploited by Exel to obtain percentage.

4.2. Results

As explained, it appears quickly that values and trust are intimately linked. Indeed, most of the surveyed define cohesion as a trust-based values, build on a package of common values and experiences. If the results allowed us to validate and invalidate our proposals, they also provide elements helping to develop a comprehension grid of trust alteration and its consequences in decision making in extreme situations. This comprehension grid stems from the theoretical framework and the validation and invalidation of our proposals.

4.2.1 : Results about values hierarchy

For clarification, this part has to be divided in four subparts dealing respectively with the organization ranking versus personal's ranking in value hierarchy, with the organization ranking versus personal rankings based on time accorded to each values in interviews, with discrepancy in between group members value ranking and with the influence of age -on discrepancy in between group members ranking.

4.2.1. Values hierarchy: organization ranking versus personal's ranking

Participants were questioned on what was in their opinion the most important values in their job, and then in their personal life. In our sample, cohesion took the first place followed by Justice/Honesty in second position. Merit/Professionalism came in third place (see table 1), then Patriotism and Sense of sacrifice arrived at the follow-up. Other values such as Love of effort, Loyalty, Humility, Bravery were far from this top rating with less than a quarter quoting them.

Value	Rate of déclarations
Cohesion	68.42 %
Justice/Honesty	50%
Merit/professionalism	34.21 %
Patriotism	31.58%
Love of effort	28. 95 %

Table 1. Ratio (in percentage) of values ranking according to self-declaration. Source: C.Dugoin-Clement

As explained previously the institution promotes its values to control its personnel efficiency, decision-making and execution order. Thus the evolution of value perception between institution and employees may result in misunderstanding between these two entities. If the values meaning of the organization differs from the personal one, they can feel betrayed by several actions, such as official speeches, or promotion operations.

Here comparing the value hierarchy declared by the soldier and the set developed by the French army (namely trust, team spirit, self-help, respect for oneself and others, courage, will, perseverance, merit and patriotism), we can observe an important gap (See Table 2). Indeed, even if we decide to consider that trust and team spirit exposed by the organization may be

merged in the cohesion quoted by the military personnel, Will may not be correlated with Love of effort.

Thus, this first observation seems to answer positively to the discrepancy in values hierarchy between the organization and military personnel.

Value ranking declared by interviewees	Organization value ranking
Cohesion	Trust
Justice/Honesty	Team spirit
Merit/professionalism	Self help
Patriotism	Respect
Love of effort	Courage
	Will

Table2. Comparison between army values hierarchy and personal values hierarchy. Source: C. Dugoin-Clement

We can notice discrepancies between organization values hierarchy and personal's one. A first discrepancy appears when comparing the interviewee's declarations and the institution ranking, but the interview was also composed of a qualitative part considering the values that seems interesting top also analyze.

4.2.1. Organization ranking vs. personal ranking based on time accorded to each values in interviews

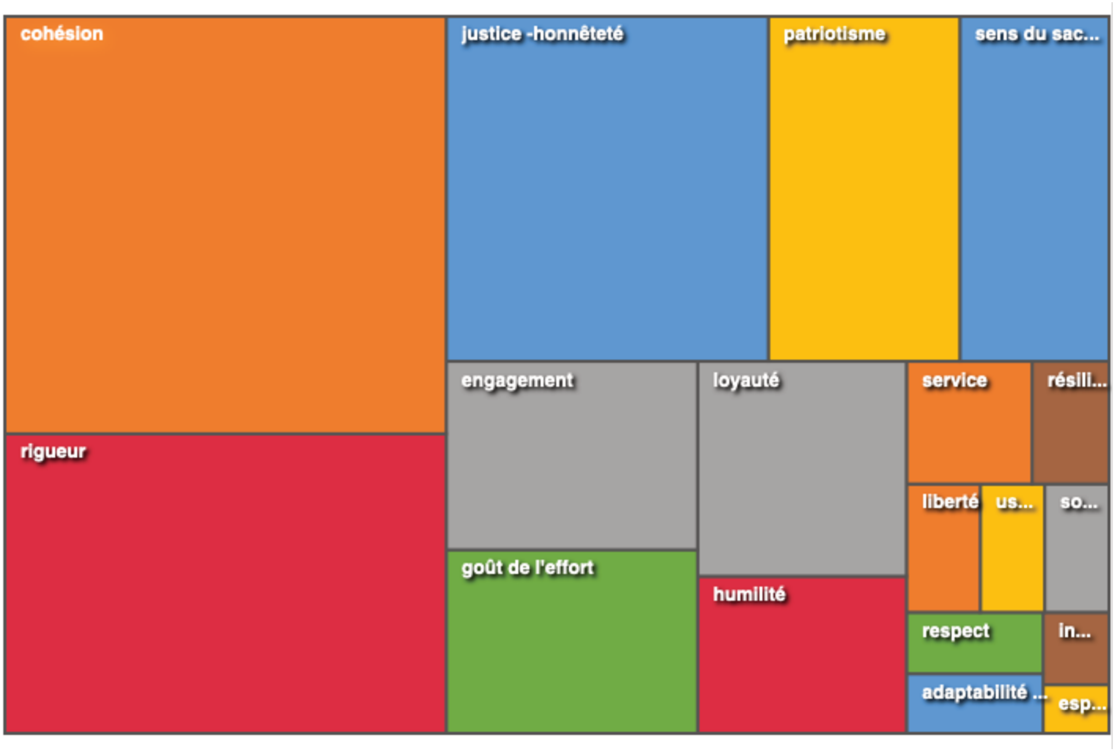
The interviews contents have been encoded with Nvivo in order to proceed to a study the complexity of the corpus in a dynamic approach. With this in mind, each value quoted has linked to a node, and each part referring to this value had been encoded at the corresponding node. This encoding system of all the interviews was also linked with the characteristic of each subject, namely, age, time of service, ranks and gender, to be able to realize some matrix

later.

As values were clearly named the thematic encoding is not subject to discussion on the encoder subjectivity, so the referential function of the language, also called the ‘theme’, namely what we are talking about, is clearly defined. Considering the descriptive function of language, the ‘rheme’, namely what we say about the theme, the link can thus easily be made with the theme of the different values because of the stability of the representation of values has an encoded system. Concerning the stability of the corpus, the sample was homogenous considering is socio-professional profile, all the subjects were talking in their own names and these encoded interviews were not mixed with other types of discourse such as official communications. Moreover, the interviewees’ anonymity helps to weaken the risk of discursive strategy. According to the coding related to values, it appears that some value nodes or types, namely the grouping of elements realized on the basis of their identity and sense, present a larger mass than others. For some searchers, the repetition in a speech of a word or of items helps to become aware of what is insisting through the speech, in other words, of elements of interest for the speaker (Gauzente & Peyrat-Guillard, 2007). Moreover, if in a second time we decide to analyze the influence of behavior of values hierarchy, we have to remember that for Damasio (1994), ‘The ability to express and feel emotions is essential to the implementation of rational behaviors’.

Here we are dealing with the time accorded to develop some subject, remembering that the interviewees were not influenced. Indeed, the questions asked were ‘concerning the values you declared as important in your job, could you please explain what they mean to you? Can you define them? » Thus subjects should logically have been spoken more on the values at the top of the aforementioned hierarchy, but differences appear. If the three top values are the same as in hierarchy declaration, we can notice that they are

even more developed (see table 3). Pragmatically, 267 encryption is related to cohesion and trust, 196 to Merit and professionalism, 188 to justice and honesty, 105 to patriotism and 88 to sense of sacrifice.



Graphic one the number of encryption related to values of the whole sample.Source: C.Dugoin-Clement

But concerning the fifth values, they differed, the declarations referred to Love of effort, when the speech highlighted Sense of sacrifice and Duty which did not appear in the declarative hierarchy. Nonetheless, in both of these analyses of the hierarchy, difference appears with the organization ranking.

We proceed to two different evaluation of the values hierarchy of military personnel: through statements and via the time they spent to talk about these values. With both methods, we noticed a disparity between the organization's values hierarchy and personal one.

Value hierarchy according to time spend talking about	**Value hierarchy based on interviewees declarations**	**Organization value ranking**
Cohesion	Cohesion	Trust
Justice/Honesty	Justice/Honesty	Team spirit
Merit/professionalism	Merit/professionalism	Self help
Patriostism	Patriotism	Respect
Sens of sacrifice/duty	Love of effort	Courage

Table 3. Ratio (in percentage) of the values the most quoted by the participants.

We postulate that an explanation may lie in the rooting of values. Indeed, values will particularly freeze in units and even more in the field when personnel share with their group daily life and a common confrontation with conflicts, namely an exterior operation in the war zone. Because in that context values are applied every day and sometimes helps save their integrity, they benefit of the empirical validation helping a deep rooting in soldiers' minds. In a symmetrical pattern, values can help soldiers to save their lives or their 'brother in arm' ones. As such, it explains the group may become something close to a 'true homeland, they are ready to kill or die for' (Barrois, 1993).

Consequently, the socialization in units with other soldiers would be a huge part of development and understanding of values. It will evolve incrementally with missions, but also with the return of experience (Retex). Thus, risk and cohesion – and trust – would be closely linked, because the second helps avoid the first. With this in mind, it appears that among all values, cohesion would seem to be the keystone of the others. Besides, this link between risk and trust is described in Schoorman (1995) theory of trust. According to him, trust is based on

the acceptance of being vulnerable to another whose actions cannot be monitored or controlled. In armies case, common values could be a way to decrease uncertainty concerning actions of other soldiers, facilitating trust birth, in other words, values can be the nest of trust. This is in the line of the observations of Godé (2011). After analysing how the members of the Aerobatic Team of French Air Force are led to collectively construct and maintain a sense to the situations they face, she showed return of experience reinforces common values and culture.

But if we notice a discrepancy between organization and personal values hierarchy, the previous elements exposed did not give hints concerning a potential disparity in between military personal values hierarchy. In the next paragraph, we focused on this specific point.

4.2.1. Values hierarchy: discrepancy in between group members ranking

As we observed a discrepancy between organization values hierarchy, we supposed that maybe some other divergence may be found in between the group members. Because the sample presents a large array of age, we took into account the age of the individual. One proposal was that hierarchy values may have been influenced by the subject's Internet consumption often described as a characteristic of the young generation usually called as the millennials. For that purpose a work was led on values hierarchy in group members according to their generations, to observe is some significant elements rise up. According to the classical classification, the X generation included western people born between 1965 and 1979, generation 'Y' included people born between 1980 and 2000 and finally generation 'Z' also called millennials, is composed of people born after 2000. But the results were inconclusive: no clear difference appeared with this classification.

But an unexpected result appears. Indeed, particularly when comparing the time spent to speak of values, another age division comes out when observing a difference in values hierar-

chy: a first group in between 23 to 34 years old presented a common value hierarchy that differed from those of a second group composed of the people over 35 years old.

4.2.1.d. Values hierarchy: age influence on discrepancy in between group members ranking

In this light, observations were made on values ranking for these groups categorization. If there was no difference concerning the first quoted values – namely Cohesion, Justice/Honesty, and Merit/Professionalism – but fourth position and followers differ (see table 4). Indeed, older declared a package of equal importance in the fourth place, when younger interviewees give on items as well as for the fifth and sixth rank. More, the values chosen by the younger groups at fifth and sixth place are absent from the older ranking. As a mirror effect, three of the values quoted by the older are not mentioned by the younger (namely: Patriotism, Appetence for effort, Humility).

As for the complete sample, when comparing the number of quotes used to talk about their main values, the ranking results change (see table 5).

Considering people under 34 years old, classification results are first Cohesion, second Honesty/Justice, third Professionalism/Merit, then Loyalty, Patriotism and Love of effort. For older subjects – over 35 years old – the results were: Cohesion, Professionalism/Merit, Justice/Honesty, Sense of Sacrifice, and engagement, then Patriotism and Love of effort and then Humility.

Hierarchy values based on declaration according to ages groups	
From 24 to 34 years old	**Over 35 years old**
Cohesion	*Cohesion*
Justice/Honesty	*Justice/Honesty*
Professionalism/merit	*Ex aequo* *Professionalism/merit* *Patriotism* *Appetence for effort* *Humility* *Sense of sacrifice*
Love of effort	
Sense of sacrifice	

Table 4. Difference in values hierarchy between peers according to age

Values hierarchy discrepancy in group (by ages) based on time spend talking of those values		
Complete sample	**From 23 to 34 years old**	**35 years old and over**
Cohesion	Cohesion	Cohesion
Justice / Honesty	Justice / Honesty	Professionalism/Merit.
Professionalism/Merit	Professionalism/ merit	Justice / Honesty
Sense of sacrifice	Loyalty	*Ex aequo* Sense of sacrifice ; Engagement
Love of effort	Patriotism	*Ex aequo* Love of effort; Patriotism
	Love of effort	Humility

Table 5. Values hierarchy discrepancy based on time spend talking of them (green are values appearing only in younger interviewee's hierarchy; pink are the ones only appearing in older interviewee's hierarchy).

As the second group is made with more experienced men, we supposed that the difference in rankings can be linked with the time passed in operation, where people expe-

rience risk and mortality salience. This proposal may have influenced their choice considering sense of sacrifice, because some of them had probably already experienced risking their lives and maybe considered paying the ultimate sacrifice for the general interest.

Another observed thing, Loyalty that appears in youngest ranking is far from the top for the older men. During the interviews they explained that Cohesion referred to their peers – i.e., soldiers they were working with every day – and Loyalty to the organization.

Similarly, older are talkative concerning Humility – even if they did not declare it in their first hierarchy – but this value did not appear in the younger interviews.

Comparing the ranking of values according to their declaration, on the one hand, and according to the number of quotes on another hand; it appears that the declared ranking is not exactly identical with the one based on time spend talking of these same values.

A proposal for the explanation of this disparity observed between declaration and time passed speaking about some values – thus between them and rheme – may be the effect of conditioning. Indeed, when asking a direct question, interviewees may be tempted to answer with a preconditioned answer, thus with some learnt answers, but when digging in emotional and personal perception through explanation and explication, they may express a more personal perception. But this proposal has to be controlled in further works.

Considering the discrepancy observed in values hierarchy in between people between 23 and 34 years old and the ones over 35 years old, the explanation may be linked with their service time. Indeed, the older group was composed of soldiers with quite a long

career, namely about 10 years, mainly corresponding at a couple of 5-years-contract, when the younger were mostly in their first contract course.

Nonetheless, no matter the choice made to realize ranking (on declared values or on a number of quotes related), Cohesion is always the prime value, followed by Justice/Honesty and the rest of the chart still diverge from the organization values hierarchy.

As we showed the link between values in the organization and the necessary development of trust in personnel minds to ensure a decision-making and execution order in accordance with the organization's strategy, it seems relevant to work on this item. To do so, we studied personnel trust in their peers and in their organization in the light of their values hierarchy but also the trust that can be accorded to the data collected during their interviews.

4.3. Trust : age influence in its meaning, and reasons of trust and mistrust in organization

The interviewees were all questioned on the trust they accord to their peers as well as to their institution. But these questions were a bit sensitive and they could have been tempted to rearrange their answers.

Thus, knowing that self-declarations may always be the subject of doubt concerning the reliability of the respondents, it was decided to realize a control test with a group of control. For that purpose, extractions and quotes were submitted to a control group composed of 5 independent people blind to the situations and to the participant's values hierarchy or ranking of their trusts. The goal was to define if interviewees were trustable in their notation, not because doubting of their honesty but because knowing the risk of

answers influenced by a social desirability. Thus, on the basis of the only given text of the interview, the control group had to score participants trust in peers as well as in the institution on the same five degree scale.

It appears that these evaluations presented a good reliability. Indeed, the average of soldiers trust in peers ranking was 4.24 when juries average was 3.84. Concerning the trust in organization, self-declared ranking average is 3.18 when juries average is really lower with only a grade of 2.81. These results are consistent with the fact it seems complicated to confess a lack of trust in your own institution especially as the result are not that good, namely with the social acceptability of an answer. Nonetheless, the difference between self-declaration and jury estimation are consistent and allowed us to rely on the military personnel declarations.

As the declared rating are not good concerning the organization, it seems relevant to inquiry on two different axes to get a better understanding. One will be what respondent means by trust in peers and in their organization and in a second time to understand the reason of their mistrust, particularly to observe if they are directly connected to the values declared as the most important.

4.3.1. Meaning of cohesion and trust in peers

As explained, trust is considered as a keystone for the organization efficiency, a part of the triangular virtuous interrelation defined as Cohesion – Trust – Performance. As when observing the values hierarchy, a clear difference appears in the meaning of trust in peers according to the ages.

The older group used vocabulary related to the family, described their relation like close to clanic trust (Ouchi, 1980). They explained their trust is over their job necessity that

they are always in close relation with their former 'brother in arms,' including in their personal lives. One explained, '*It is like a second family, a stronger one. I know that if I am in trouble, it is with these guys that I am going to talk, to ask for help. You see, we are more than colleagues. Some of them know better my underwear than my wife!* » They also explained that this cohesion helps them in a hard time on the field because the interest and safety of the group are more important than their own; consequently it helps going over-emotional complicated situations. To summarize, we can quote this participant who said, '*it is a family trust, we are brothers of arms, and it is even beyond the family. "Brothers of arms" is not an s hollow word…*'

The younger had not the same perception. They referred more to '*forced cohesion*' a '*constrained trust*' necessary to the success of their mission and their self-perception. Some expressed cohesion useful for themselves and not placing the group at the first place. A respondent explained that cohesion was useful because they '*know that in a group there is obviously some that are weaker than I of more afraid than I am. And it helps me feel more in confidence and comfortable*.' In this quote it appears clear that the group is useful for the individuals and not for the whole population composing the group. In this quote, the group is not overtaking self-priority of the interviewee.

In comparison with the interpersonal relations described by the older group, a member of the younger sample declared that '*In combat, I trust them… But telling them all my personal life or to lending them money… No, definitely no!* » This declaration is in perfect adequacy with what was explained by another, '*for me it is just a job. I don't want to pass all my life with them, even if the elderly reproached that. But for me I end my job at 5 p.m., so at 5:15 p.m., I am on the road back home to have time with my wife and relatives*.'

In the same mindset, an interviewee explained that they do commando courses and that '*during these 2–3 weeks, we see that people are not at all cohesive — it's funny because they are cohesion internships. It's a hypocritical cohesion. That is to say in the tests, people help themselves and support each other but it's fake, it's toxic … even if it cannot be seen from the outside. That is to say, the guy who is going to encourage you on the basis of 'go ahead!', in fact, this person does it for … it's to reinforce him, in reality he doesn't really think about the person he is promoting. It's a way to show that they are better, to take the lead, to show off by pretending to encourage. In their mind it is "if I encourage you, it is to show the others that I do cohesion, it is not for you. It is to show that 1 – I am good, 2 — I have still enough energy to do it and 3 – you are not as good as I am.' By the same token, we were explained that 'you know, all that staff … cohesion, it's what you see in the pictures, and it does not exist any more*.' The average age of those making these kinds of statements on cohesion and trust in peers is 28.9 years old.

However, this mindset change can be useful for maintaining the competition in peers, and to sustain the research of excellence necessary for the perpetual skills improvement required for these kinds of jobs. As said a member of the older group '*Well, it's not a mass sport. There is necessarily a competition that is done there is inevitably leadership that is done … but it's a balance that can be fragile … if there's too much competition between guys, it could become very negative.'*

Consequently, it appears that the meaning of the more important value differed between the younger member of the sample and the older one.

Nonetheless, both groups gave the best ranking to trust in the group and, generally speaking, institution trust is quite low (for memory, according to the jury's results are 2.81, thus hardly over the average of 2.5, level explained as 'no distrust but no trust ei-

ther'). Knowing that trust and cohesion are the cornerstone of the organization efficiency, it appears interesting to analyze the reasons evoked to explained mistrust in the institution that can be a game changer in decision-making and order execution in adequacy with what the organization expected to be a good strategy deployment. These analyses will help compare if these reasons are linked with values formerly exposed. It also will enlighten if the division between elders and younger is still apparent.

4.3.2. Reasons of mistrust in the organization

Using qualitative analysis to refine the reasons of trust or of mistrust, it appears that people with low trust in institution justification of this rating is linked with values declared as the most important.

But we noticed that if the same reasons were evoked by all the interviewees, some are more developed by the younger than by the elders. As such, some great categories appears in the reasons of mistrust. Were quoted by the interviewees: the lack of sincerity of the hierarchy, the fact they perceived them as distant from them (e.g. 'they don't know us, they are different. Even if they try to understand us, they can't because they are too different from us').

But if older talked about it with resignation as a fact that cannot be changed, younger obviously are still revolted. As one explained, '*In fact they* [hierarchy] *are at years light away from what we do, what we are!!*' Hierarchy is predominantly perceived as not aware of field reality, of real soldiers life as explained with resignation by an interviewee over 35 '*yes it's two different world*s [soldiers and officers one] *that are ... different. They are cut off from reality*.'

Graph 1. Comparative graphics of reasons of mistrust in organization exposed by respondents. Source: C.Dugoin-Clement

Another reason regularly exposed by the older interviewees for the mistrust, that was the lack of professionalism, and bravery. As such, some declared that '*they* [hierarchy] *became fearful chickens*'. When another considered: '*Our leaders are afraid to get involved, to take their responsibilities*.'

Here appears a huge difference between the two groups. Indeed, the younger group mainly thinks its hierarchy is not coward but not well informed. As an example, a participant explained that '*I think they want to do well, but middle management doesn't tell them everything, so they do not necessarily have all the keys…'*. Another in the same

mindset explained, '*For me they are not well informed!* » This appears in the graphic (see Graph 1) realized from the qualitative encoding of the interviews.

Some explained that they have the feeling that institution managed an '*organized opacity on purpose*' to force them not to change of professions or not to understand institution real intentions and motives. This was quoted by all those who mistrust the institution but mainly by the younger.

Concerning distance of the leadership, both old and young quoted it. But concerning the reasons for this distance, point of view differs. The older are tougher and more radical. They explained it as evidence and don't take a long time to analyze the reasons, like if it is an unquestionable fact with explanations as '*they are not in the same world. They just don't live in my world'* or '*for me they are far, far away*.'

Obviously, the major reasons for the mistrust are directly linked to the core values exposed previously, namely cohesion (that cannot be felt with distant and different people, with some that do not care for you), Honesty/Justice, and Merit/Professionalism.

With this in mind and in the light of the age division previously observed that was not in adequacy with the classic X, Y and Z generations, exploratory analysis was performed. We postulated that time in service may be the game changer in values hierarchy as well as in differences observed concerning trusts (in ratings and meanings). Thus, a negative correlation appears between time passed in exterior operations and trust in institutions ($b^* = -.43$, $p < .01$; $b = -.02$); meanwhile it increases the trust in peers ($b^* = .28$, $p = .08$; $b = .01$). These results are in adequacy with our proposals concerning the division observed in the values ranking. Indeed, after 10 years of service, trust in the peer's in-

crease, similarly values are more deeply rooted, thanks to the group socialisation effect, and not to the organization teaching influence.

Conclusion

According to these results, it appears that our proposal number one is validated as there is a discrepancy in the hierarchy values of the organization and the one of its personnel. Indeed, even if values are initially diffused by the organization, it appears that personal values hierarchy differed from the one defines in the organization culture and identity. These results invalidate the theory of Bardi & Schwartz (2001) for whom value hierarchies presented a widespread consensus.

More, it also appears that the values hierarchy is not completely homogenous in between the peers contrary to our second proposal. This according to Schiele (1980) and Schield (2004) theories, it will me more complicated to predict how individuals interact with each other and behave with people outside the organization because they are not sharing the exact same set of value composing the organization identity.

Our third proposal supposed that discrepancy in value hierarchy would be directly linked to ages of people. The result validates that proposal. Indeed, a disparity appears and can be linked with ages. But an unexpected result was that this discrepancy is not ventilated according to the classical ‘x’, ‘y’ and ‘z’ generation but between the 23–34 years old and the over 35-year-old as supposed in the sub-proposal number 1.

We made a second sub-proposal advancing that this division is shaped by the service time, and can be reinforced by the time passes in exterior operation, possibly in the battlefront. This sub-proposal seems borne out by the quantitative analysis led through a

regression that highlights the increase of trust in peers with time passed in exterior operations which proportionally decrease trust in the organization.

Concerning the fourth proposal advancing that values are main actors in lack of trust, it appears that the reason of mistrust is clearly linked with the values quoted as the more important by the respondent, no matter the methods used to rate the values hierarchy (by declarations or through the time spent speaking of these values, in a more psycholinguistic approach). Thanks to the use of a control group, it also appears that respondents were trustable events if they were overestimated their rating trust in organization probably for social acceptability of their answer. We find that even if the perception of trust in peers may vary between the respondents, peers stay nonetheless the better rating trust. Indeed, no matter the age, trust in peers is always the top-rated one. More, the trust in peers presented a positive trend with time of service, especially with time passed in the field.

Considering the fifth proposal, namely that a change in the hierarchy of values have an impact on decision-making and consequently in order execution, we observed that a discrepancy appears between personnel and organization and that this gap may be problematic because it provokes a decrease in trust. Indeed the same values are directly correlated with a weak trust in the organization. Knowing that trust is one of the guarantees of a controlled decision-making assuring the good execution of the organization orders, in other words, the guarantee of the safe deployment of the organization strategy, such a vulnerability may appear to be a main failure trigger.

In the continuation of the invalidation of proposal number 2 (there is no discrepancy in hierarchy values in between the member of a military personnel group) it appears that according to soldiers ages commitment time and exterior operation experiences, values

do not have the same meaning or importance? It seems that it could be a real human resource management issue for the organization if it has to face a two-level values hierarchy discrepancy. Indeed, besides the risk of an altered orders execution, if an awareness-raising effort is not developed within units, a gap could appear in between soldiers and provoke misunderstood and affect trust and cohesion, which are efficiency and safety guarantees when operating in extreme situations. In further research in order to evaluate this evolution's potential consequences, it could be interesting to realize a comparative analyze of the operational results between units composed of soldiers mainly sharing the same meaning of trust and cohesion, and another unit where personnel perception is more divided. If the results are similar, thus it will reinforce the theory according to which this evolution is not a risk in itself.

If that hierarchy values may be implied in organization trust or mistrust and knowing the rise of psychological operation aiming at inflecting people perception as in Ukraine (Dugoin-Clement 2018), we can wonder what is the risk for soldiers to be influenced by online media. Especially if these media play their core values in cognitive dissonance based operation to alter trust and consequently provoke divergent decision-making and altered execution of orders. Moreover, maybe a team's division based on meaning of values and affecting trust quality may weaken the usual soldier's defense against exogenous influence that can endanger the organization good functioning.

This study showed the role of values hierarchy in evolution of trust in the organization and, consequently, highlighted the risk of altered decision-making and organization directive execution dues to this discrepancy. Indeed, thanks to the literature review, it has been exposed that trust is a guarantee in control of the organization on personal behavior. Consequently, the more this trust is altered – here by a discrepancy in values hie-

rarchy – the more the risk of deviant action increase, expanding the probability of a deleterious action decided by the soldiers that will have dire consequences for the organization. But this study did not succeed in quantifying the weight that the vector constituted by discrepancy in values' hierarchy would have in the deployment's strategy of the organization. That seems to be a limit of this exercise.

Moreover another question emerged from this study. Considering the heuristics theory of decision-making, such as firstly developed by Kahneman and Tversky (1974) and particularly the decision in situation theory developed by Rasmussen et al. (1991) and Amalberti (1996). Indeed, according to these theories, the decision makers must integrate the context in his decision-making process. When this decision takes place in a managerial field, they have to deal with situations described as unstable, often irrevocable and implies many individuals' action (Lebraty, 2004). In this situation, the way decision is taken is based on the use decision maker made of their knowledge and expertise. In other words, to be efficient, they may have to save their cognitive resources, that implies to devolve a piece of cognitive functioning to automatisms. Actually if they don't, they won't have enough cognitive resource available to face a degraded situation such as a crisis. Practically to do so, they are constantly arbitrating between what they understand and what they accept not to understand. As this is a dynamic approach, to be efficient it needs to be regularly updated. The update includes a set of elements allowing sorting out what confirm or infirm the context they are evolving in. If their update is based on false elements such as the values hierarchy that trigger their personnel decision-making, leaders may probably not be able to make the right decision. If we refer to Amalbreti who explained that the real matter of understanding is not to build a representation but to properly updating the context's representation already available, so, hierar-

chy values is not only a matter of personnel's trust and decision-making, it may also have consequences on leaders decision-making, particularly in extreme situations and in crisis context.

References

Alter, Norbert. 1993. “La Crise Structurelle Des Modèles d’organisation.” *Sociologie Du Travail,* 35 (1): 75–87. https://doi.org/10.3406/sotra.1993.2109

Alveson, Mats. (2011) Organizational culture: meaning, discourse and identity in Ashkanasy, Neal M. , Wilderom Celeste P. M. and Peterson Mark F. (Eds) *Handbook of organizational culture and Climate*, Thousand Oaks, Sage Publication, 2011, 11-28. https://doi.org/10.4135/9781483307961.n2

Alvesson, Mats, and Laura Empson. 2008. “The Construction of Organizational Identity: Comparative Case Studies of Consulting Firms.” *Scandinavian Journal of Management,* 24 (1): 1–16. https://doi.org/10.1016/j.scaman.2007.10.001

Amalberti, René. (2001). *La Conduite de Systèmes à Risques.* Paris, Presses universitaires de France, 2001, 239.

Aubry, Monique, Lièvre, Pascal and Hobbs, Brian. 2010. “Project Management in Extreme Environments.” *Project Management Journal,* 41, 3, 2-3. https://doi.org/10.1002/pmj.20185.

Barrois, Claude.(1993). *Psychanalyse Du Guerrier.* Paris, Hachette Litterature, 1993, 322.

Bechky, Beth A., and Okhuysen Gerardo A.. 2011. “Expecting the Unexpected? How Swat Officers and Film Crews Handle Surprises.” *Academy of Management Journal,* 54 (2): 239—61. https://doi.org/10.5465/AMJ.2011.60263060

Bouty Isabelle, Godé Cécile, Drucker-Godard Carole, Lièvre Pascal, Nizet Jean, and Pichault François. 2012. “Coordination Practices in Extreme Situations.” *European Management Journal,* 30 (6): 475—89. https://doi.org/10.1016/j.emj.2012.03.015

Christianson, Marlys K., Maria T. Farkas, Kathleen M. Sutcliffe, and Karl E. Weick. 2009. “Learning through Rare Events: Significant Interruptions at the Baltimore & Ohio Railroad Museum.” *Organization Science* 20, 5,835-939. https://doi.org/10.1287/orsc.1080.0389

Clegg Stewart R., Cunha Miguel Pina, and Kamoche Ken. 2006. “Surprises in Management and Organization: Concept, Sources and a Typology.” *British Journal of Management,* 17 (4): 317–29.

Courpasson, David. (2000). *L’action Contrainte.* Paris: Presses Universitaires de France, 2000.

Crene, Yves.1999. Directive relative aux comportements dans l’armée de terre, comportant en annexe le « Code du soldat », et le « Guide du comportement». Paris, Ministère de la Défense, 1999.

Damasio António (1994). *L'erreur de Descartes, la raison des émotions*. Paris, Odile Jacob, 1994, 397

Desportes Vincent. 2018. « Décider Dans l'incertitude » Réunion Mensuelle de l'ANDRH, 6 février 2018, Toulouse.

Dowling, John, and Jeffrey Pfeffer. 1975. "Organizational Legitimacy: Social Values and Organizational Behavior." *The Pacific Sociological Review,* 18 (1): 122–36. https://doi.org/10.2307/1388226.

Dutton, Jane E., Dukerich Janet M., and Harquail Celia V.. 1994. "Organizational Images and Member Identification." *Administrative Science Quarterly,* 39 (2): 239. https://doi.org/10.2307/2393235.

Dugoin-Clément, Christine, 2018. "Utiliser Les Potentialités Du Cyber Pour Des Opérations Psychologiques Ciblées En Temps de Paix ?" *Dynamiques Internationales* 13: 1–21.

Festinger, Léon. 1957. Cognitive Dissonance. Stanford University Press. Stanford u. Stanford. https://doi.org/10.7312/columbia/9780231175081.003.0017.

Gauzente Claire & Peyrat-Guillard Dominique. (2007). *Analyse Statistique Des Données Textuelles En Sciences de Gestion.* Paris, EMS Editions, 2007, 200.

Gioia, Dennis A., and Thomas James B.. 1996. "Identity, Image, and Issue Interpretation: Sensemaking during Strategic Change in Academia." *Administrative Science Quarterly,* 41 (3): 370–403. https://doi.org/10.2307/2393936.

Godé, Cécile. 2011. "Construire Le Sens Par Le Retour d'expérience : Le Cas de l'Equipe de Voltige de l'Armée de l'air." *Management & Avenir,* 41 (1): 416. https://doi.org/10.3917/mav.041.0416

Godé, Cécile. (2015). *La Coordination Des Équipes En Environnement Extrême*. Londres, ISTE Éditions. 2015.

Godé, Cécile. (2015). *Team Coordination in Extreme Environments: Work Practices and Technological Uses Under Uncertainty.* London, Wiley and son, 2015, 300.

Godé, Cécile, and Jean Fabrice Lebraty. 2015. "Experience Feedback as an Enabler of Coordination: An Aerobatic Military Team Case." *Scandinavian Journal of Management,* 31 (3): 424—36. https://doi.org/1

Gollier Christian, Hilton Denis, and Raufaste Eric. 2003. “Daniel Kahneman et l’analyse de La Décision Face Au Risque.” *Revue d’économie Politique,* 113 (3): 295-307. https://doi.org/10.3917/redp.133.0295.

Green, Bruce. 1997. “Role of Personal Values in Professional Decision making” *Georgetown Journal of Legal Ethics,* 11, 19-39.

Hällgren, Markus, Rouleau Linda, and De Rond Mark. 2018. “A Matter of Life or Death: How Extreme Context Research Matters for Management and Organization Studies.” *Academy of Management Annals,* 12 (1): 111–53. https://doi.org/10.5465/annals.2016.0017

Huntington, Samuel P. (1957). The Soldier and the State: The Theory and Politics of Civil-Military Relations. London, Harvard University Press, 1957, 550.

Jackson, Joshua J., Felix Thoemmes, Kathrin Jonkmann, Oliver Lüdtke, and Ulrich Trautwein. 2012. “Military Training and Personality Trait Development: Does the Military Make the Man, or Does the Man Make the Military?” *Psychological Science,* 23 (3): 270–77. https://doi.org/10.1177/0956797611423545

Kahneman, Daniel, and Amos Tversky. 2013. « Prospect Theory: An Analysis of Decision Under Risk » *Econometrica*, 47, 2, 263-292. https://doi.org/10.2307/1914185

Kahneman, Daniel., & Tversky, Amos. (1982). Intuitive Prediction: Biases and Corrective Procedures. https://doi.org/10.1017/CBO9780511809477.031

Kahneman, D., & Tversky, A. (1982). The Simulation Heuristic. https://doi.org/10.1017/CBO9780511809477.015

Kunda, Gideon. 1995. “Engineering Culture: Control and Commitment in a High-Tech Corporation.” *Organization Science,* 6 (2): 228—30. https://doi.org/10.1287/orsc.6.2.228

Lamizet, Bernard. (1998). *La Médiation Politique*. Paris, L’Harmattan, 1998, 417.

Lampel, Joseph, and Shapira Zur. 2001. “Judgmental Errors, Interactive Norms, and the Difficulty of Detecting Strategic Surprises.” *Organization Science,* 12 (5): 599–611. https://doi.org/10.1287/orsc.12.5.599.10094

Lebraty, Jean-Fabrice. 2004. “Biais Cognitifs : Quel Statut Dans La Prise de Décision Assistée ?” *Systèmes d’information et Management,* 9 (3): 1–27.

Lièvre, Pascal, and Anaïs Gautier. 2009. “Les Registres de La Logistique Des Situations Extrêmes : Des Expéditions Polaires Aux Services d’incendies et Secours.” *Management & Avenir,* 24 (4): 196-216. https://doi.org/10.3917/mav.024.0196

Lowenstein Georges, and Lerner Jennifer S. (2000). The Role of Affect in Motivation In *Handbook of Affective Sciences,* 81:. Oxford: Oxford University Press, 2000, 582–585

Maxwell Joseph Alex. (2019). Qualitative Research Design In Paul Atkinson, Sara Delamont, Alexandru Cernat, Joseph W. Sakshaug & Richard A. Williams (Eds) London, SAGE Publications, 2019. https://doi.org/10.4135/9781526421036788354

Mayer, Roger. C., J.ames. H. Davis, and David F. Schoorman. 1995. “An Integrative Model of Organizational Trust.” *Academy of Management Review,* 20 (3): 709–34. https://doi.org/10.5465/amr.1995.95080803

Ministry Of Defense, Values and Standards of the British Army. (2008). [MOD, The Army Leadership Code: An Introductory Guide, 1st Edition, SO2 Leadership. Sandhurst, Royal Military Academy, 2008.

Mullen, Brian, and Carolyn Copper. 1994. “The Relation between Group Cohesiveness and Performance: An Integration.” *Psychological Bulletin,* 115 (2): 210–27. https://doi.org/10.1037/0033-2909.115.2.210

Myers, Michael D. (2008). *Qualitative Research in Business & Management*. London, Sage publication, 2008, 296.

O’neill, Olivia A. (2004). Organizational Culture: Beyond Struggles for Intellectual Dominance In S. Clegg, C. Hardy, W. Nord, and T. Lawrence (Eds) *Handbook of Organization Studies* London, Sage Publications, 2004 (2cd edition), 725. https://doi.org/10.4135/9781848608030.n26

Ouchi, William G. 2019. “Markets, Bureaucracies, and Clans.” *Administrative Science Quarterly,* 25, 1, 129-141. https://doi.org/10.2307/2392231

Perrow, Charles. 1994. “The Limits of Safety: The Enhancement of a Theory of Accidents.” *Journal of Contingencies and Crisis Management,* 2 (4): 212–220.

Robins, Richard W., R. Chris Fraley, Brent W. Roberts, and Kali H. Trzesniewski. 2001. “A Longitudinal Study of Personality Change in Young Adulthood.” *Journal of Personality,* 69 (4): 617–40. https://doi.org/10.1111/1467-6494.694157

Robinson, Paul. 2007. “Magnanimity and Integrity as Military Virtues.” *Journal of Military Ethics,* 6 (4): 259—269. https://doi.org/10.1080/15027570701755364

Roux-Dufort, Christophe, and Sanjy Ramboatiana. 2008. “Crise et Sentiment, Le Cycle d’incompétence Habile.” *L’Expansion Management Review,* 120-128 (1): 120. https://doi.org/10.3917/emr.128.0120

Schein, Edgar H. 1986. Organizational Culture and Leadership. *The Academy of Management Review,* 11, 4, 677-680. https://doi.org/10.2307/258322

Schwartz, Shalom H., and Anat Bardi. 2001. “Value Hierarchies Across Cultures.” Journal of Cross-Cultural Psychology 32 (3): 268–90. https://doi.org/10.1177/0022022101032003002.

Schweisguth, Etienne. 1995. “La Montée Des Valeurs Individualistes.” *Futuribles* 200 (Juillet-Août): 131–160.

Schweisguth, Etienne. 1978. “L’institution Militaire et Son Système de Valeurs.” *Revue Française de Sociologie,* 19 (3): 373. https://doi.org/10.2307/3321050

Settersten, Richard A. 2006. “When Nations Call: How Wartime Military Service Matters for the Life Course and Aging.» *Research on Aging*, *28*(1), 12–36. https://doi.org/10.1177/0164027505281577

Shapiro, Susan P. 1987. “The Social Control of Impersonal Trust.” *American Journal of Sociology,* 93: 623—58. https://doi.org/10.2307/2780293

Shrivastava, Paul, Ian I. Mitroff, Danny Miller, and Anil Miclani. 1988. “Understanding industrial crisis” *Journal of Management Studies,* 25 (4): 285–303. https://doi.org/10.1111/j.1467-6486.1988.tb0

Strauss, Anselm L. & Corbin Juliet (2015). *Basics of Qualitative Research : Techniques and Procedures for Developing Grounded Theory.* London, Sage publication, 2015 (3rd edition), 272..

Thompson James D. 1967. Organizations in action . New York: Mc Graw-Hill

Tsoukas, Haridimos. (2005). *Complex Knowledge: Studies in Organizational Epistemology. Management Learning*. Oxford University Press, Oxford, 2005. https://doi.org/10.1108/00220410710759048.

Tversky, Amos, and Daniel Kahneman. 1974. “Judgment under Uncertainty: Heuristics and Biases.” *Science,* 185, 1124-1131.

Van Daele, Agnès and De Keyser Véronique. (1991). Distributed Decision Making and Time in the Control of Continuous Processes in Jens Rasmussen, Berndt Brehmer, and Jacques Leplat

(Eds). *Distributed Decision Making: Cognitive Models for Cooperative Work*. Chichester, John Wiley & Sons, 1991, 416.

Viviani, Jean-Laurent. 1994. “Incertitude et Rationalité.” *Revue Française d’économie,* 9 (2): 105–46. https://doi.org/10.3406/rfeco.1994.954

Weick, Karl E. 1993. “The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster.” *Administrative Science Quarterly,* 38 (4): 628. https://doi.org/10.2307/2393339

Zand, Dale E. 1972. “Trust and Managerial Problem Solving.” *Administrative Science Quarterly,* 17 (2): 229-239. https://doi.org/10.2307/23939

Conclusion

Cette recherche a permis d'analyser les fondements et l'évolution de la confiance, d'en étudier l'influence sur la coopération développée entre les membres d'une organisation évoluant en situations extrêmes voire dans des environnements hostiles où les groupes sont soumis à des contraintes physiques très fortes avec un enjeu vital avéré.

1. Principales contributions

Ce travail met en avant le rôle de la confiance dans les mécanismes de prise de décision et dans l'exécution des ordres et consignes reçues par les personnels. Par ailleurs, si le développement de valeurs au sein de l'organisation apparaît comme indéniable, il n'est cependant clairement pas un remède absolu qui immuniserait les agents contre des prises de décisions déviantes quant aux consignes reçues, ou contre des influences extérieures, contrairement aux théories de Schiele (1980) et Schield (2004). Cela repose notamment sur le fait que contrairement aux travaux de Bardi & Schwartz (2001) les valeurs ne sont pas unanimement partagées par l'ensemble de l'organisation dans toutes les strates hiérarchiques.

En outre, cette capacité des organisations à peser sur la construction du socle des valeurs participe en elle-même en leur insuffisance à créer la confiance sur laquelle repose l'engagement des individus. En effet, la capacité de l'organisation à enraciner des valeurs auprès de ses agents, à construire de la confiance à travers l'adhésion à des valeurs apparaît être un objet de compétition entre l'institution militaire et les organisations combattantes adverses.

Cette recherche tend à ne pas discuter la question de l'affirmation des valeurs, mais bien plus à en comprendre la nature, la construction et le développement afin de tenter de trouver des méthodes permettant de protéger ces valeurs contre les influences externes.

Il apparaît qu'une des failles permettant la perméabilité à des influences extérieures semble être que l'appropriation de ce corpus de valeurs développé par l'organisation connaît son enracinement au sein des unités de terrain, éloignées des organes de décision. Ainsi, la sédimentation des valeurs peut échapper pour une part non négligeable à la tête de la structure. Dès lors, l'organisation peut perdre la maîtrise absolue de cet ensemble de valeurs alors même qu'elles deviennent des éléments constitutifs de l'identité sociale et individuelle des membres de l'organisation. De ce fait, les valeurs, différemment appréhendées par les agents peuvent diverger de celles prônées par la hiérarchie, voire devenir un référentiel parallèle sur lequel l'organisation elle-même et ses dirigeants seront jugés par les exécutants. La conséquence de ce jugement de la hiérarchie pourra les pousser à une prise de décision déviante concernant l'exécution des ordres donnés. Ce constat va à l'encontre des théories de Gioia et Thomas (1996) pour qui l'institution, lorsqu'elle fait des valeurs un élément constitutif de son identité organisationnelle, fusionne cette dernière avec l'identité sociale et l'identité de l'individu, ayant pour effet de rendre le comportement et la prise de décisions des employés prévisibles et donc sécurisés.

En outre, cette perte de maîtrise peut participer à l'affaiblissement des messages qui seraient mal ciblés avant d'être délivrés par l'organisation vers ses membres ratant par là même leur cible. En effet, la classification différenciée des valeurs emporte des conséquences sur la communication de l'organisation : orientée sur la mobilisation de valeurs

qu'elle pense déterminantes pour les personnels, elle peut s'avérer inefficace, voire néfaste, si celles-ci ne sont plus primordiales dans l'esprit des agents de terrain. Le message que la structure entend porter sera alors, a minima, brouillé. Toujours en termes de communication, la présente étude aura mis en lumière la sous-estimation des dommages pouvant être causés par l'exposition des soldats aux informations que ce soit par les intéressés ou par l'Institution. Enfin, cette recherche a mis en lumière que la communication de l'organisation est généralement mieux perçue par les agents n'ayant pas travaillé en situations extrêmes.

Ceci participe à dessiner les contours d'éléments à même de pouvoir faciliter la perméabilité de soldats aguerris à des influences extérieures émanant d'adversaires qui auraient cerné la hiérarchisation des valeurs ayant pris corps au sein des unités. Il ne serait alors pas question qu'une influence extérieure se substitue en totalité à celle de l'institution, mais qu'elle utilise les fondements dispensés par l'institution pour les retourner ensuite contre elle, particulièrement auprès de sujets plus sensibles.

Un autre apport de cette recherche se porte sur les valeurs en lien avec la confiance. Si les valeurs restent des éléments constitutifs de la confiance, la hiérarchisation différenciée de ces dernières par les diverses strates de la structure pourra devenir un facteur de défiance entre les niveaux opérationnels et fonctionnels. En mettant en lumière la possibilité d'une entrée en concurrence de ces strates de confiances au lieu d'un renforcement mutuel, ce travail représente un apport aux théories de Stewart (1988) et Etzioni (1961), qui expliquent que la confiance dans le milieu militaire comprend trois composantes principales (les relations avec les pairs, les relations entre supérieurs et subordonnés, les relations entre l'armée et le gouvernement). En effet, au travers ce travail,

on a pu observer un effet de « clanisation » entre les agents qui, partageant les mêmes valeurs, se font plus naturellement confiance alors qu'ils se défieront des autres échelons hiérarchiques, perçus comme « différents ». Cette « clanisation » pourra en ce sens être rapprochée de la cohésion en ce qu'elle est conçue par la sociologie militaire comme construite par opposition à l'extérieur du groupe. Or, si la cohésion est généralement reconnue comme un facteur primordial dans la réussite des unités militaires, il y a ici le risque que cette construction ne dévie et ne passe de « au service de la mission » à « contre son environnement » et « au service de valeurs incarnées par le groupe », particulièrement si ce groupe perçoit une trahison de ces mêmes valeurs au sein de sa hiérarchie donneuse d'ordre. Il s'agit là d'une question complexe qui, si elle n'est pas nécessairement négative par nature, doit néanmoins être envisagée à la lumière des stratégies d'influence par l'information telles que développées ces dernières années et déployées sur les récents théâtres d'opérations.

Par ailleurs, si l'exposition à des situations extrêmes consolide l'enracinement de valeurs communes entre ceux qui y sont confrontés, elle entraîne un effet pervers qui se traduit par un renforcement du sentiment d'altérité par rapport aux autres strates hiérarchiques. Enfin, l'intériorisation des valeurs apparaît être à double tranchant. En effet, lorsque les personnels se sont complètement approprié ces valeurs, celles-ci leur seront d'un précieux secours pour donner du sens à un environnement chaotique dans lequel ils pourraient être amenés à intervenir. Elles seront aussi utiles en ce qu'elles participeront à les faire agir de façon cohérente avec les attendus de la mission. Cette intériorisation sera d'autant pus forte chez les agents qui ont connu des situations extrêmes, conformément aux théories de Batson (1975) et Burris et al. (1997) pour qui les individus dis-

posant de valeurs fortes, particulièrement si elles ont été testé empiriquement en situation extrême, changeaient difficilement d'avis. En accord avec les théories de Festinger (1956) et avec les variantes fonctionnelles développées par Aronson (2004), ils semblent plus susceptibles de renforcer ces dernières notamment en cherchant des éléments confirmatoires (Fischer, Kastenmüller, Greitemeyer, Fischer, Frey, & Crelley, 2011), ou en rejetant une cognition différente même étayée par des faits (Batson, 1975; Bochner & Insko, 1965). La recherche a aussi mis en lumière un abaissement de la méfiance face à des informations conformes aux valeurs fortes des individus, ce qui s'inscrit dans les résultats présentés par Vaidis & Gosling (2011). Ce seuil de méfiance s'abaisse encore si la personne transmettant l'information est reconnue comme un pair, car elle bénéficiera alors d'un *a priori* de confiance. En outre, à la lumière des éléments présentés par cette recherche, il apparaît que les valeurs fortes des soldats présentent un risque pour l'organisation lorsqu'ils sont exposés à des informations mettant en évidence un conflit entre les valeurs partagées avec leurs pairs et l'institution.

Par ailleurs, l'enracinement des valeurs amène un glissement du cognitif vers l'affectif : les valeurs professionnelles deviennent personnelles, finissant par faire partie intégrante de la personnalité des agents. Si ce glissement apparaît inévitable au vu de la nature de l'emploi, nécessaire pour le bon déploiement de la stratégie de l'organisation, mais aussi du fonctionnement du groupe, de l'unité, il doit, être pris en considération comme pouvant représenter une faille de sécurité à même d'être exploitée par des adversaires. En effet, ces mêmes valeurs intériorisées peuvent devenir des leviers d'influence efficaces pour des stratégies concurrentes, au détriment de la confiance entre les niveaux hiérarchiques.

La conséquence peut alors être l'altération de la coopération et l'accroissement corrélatif du risque de prise de décisions divergentes, d'exécution déviante des ordres (ce qui a pu être constaté à travers les entretiens menés en phase 2). Ces conséquences de la perte de confiance font échos aux travaux de Mullen & Cooper (1994) et Stanton (2004) qui soulignent le rôle essentiel de la confiance au sein des équipes militaires, tout en les affinant par la définition des valeurs la constituant.

Par ailleurs, une modification de la perception et de l'affect attaché à ces valeurs entre les membres du même groupe est également à prendre en considération. Au cours des entretiens menés, il est apparu que, selon l'âge et surtout le temps d'engagement, la perception de la confiance, voire de la cohésion, pouvait être très différente. Le sujet n'est pas ici de juger la pertinence de cette évolution et encore moins de procéder à un jugement de valeur, mais de mettre en lumière qu'une différence notable peut apparaître et que la vigilance doit être de mise afin que cet écart ne représente pas un fossé pouvant devenir un écueil au sein des groupes.

Dans le cas où ces valeurs devenues affectives viendraient à être attaquées, la réaction des individus sera émotionnelle, plus immédiate. Elle outrepassera les règles de prudence, même si ces règles font partie d'un programme spécifique de sensibilisation ou d'entraînement. Une telle réaction risque de porter gravement préjudice à la stratégie de l'organisation. Cette proposition a été vérifiée au cours de l'observation dirigée réalisée à la suite des entretiens précédents sur la base des valeurs centrales recensées.

Dans le prolongement de ces constats il a été observé que, les facteurs influençant la confiance au point de se traduire, le cas échéant, par des décisions et actions déviantes, peuvent résulter d'informations ou de contenus auxquels les personnels seraient soumis

par l'intermédiaire d'Internet. Ces conclusions quant aux raisons ayant participé à modifier le comportement des sujets s'inscrivent dans la lignée d'un modèle récent traitant de la déstabilisation organisationnelle: le Predictability Susceptibility Awareness model (PSA; Santos, 2017). Développé dans le champ des sciences informatiques, il suggère que trois facteurs peuvent expliquer le comportement d'un insider (c'est à dire d'un individu susceptible de perturber le fonctionnement de son organisation en raison d'une influence externe). Le premier facteur est la prévisibilité, soit la capacité de prédire la réaction d'une cible à un message pouvant être créé afin de l'influencer. Le deuxième facteur est la sensibilité, soit la tendance d'un individu à être impliqué dans des actions pouvant affecter son organisation, directement ou indirectement, et en raison d'une influence interne ou externe. Le troisième facteur est la sensibilisation, soit la capacité pour la cible d'identifier l'intention de manipulation derrière des informations reçues pouvant être fausses ou partielles. Les modèles psychologiques développés dans cette recherche contribuent à faciliter la compréhension des processus sous-jacents du PSA et affinent la perception du lien entre ces facteurs. Plus précisément, les valeurs professionnelles intériorisées pourraient renforcer la prévisibilité et la sensibilité et diminuer la sensibilisation.

Précisons ici que la prise de décision déviante est comprise dans ce travail comme certes contraire à l'ordre donné, mais surtout comme ne permettant pas d'atteindre l'objectif fixé. En effet, de même que la loi peut s'interpréter dans son esprit, un ordre pourra l'être également dans la mesure où une large part d'autonomie est donnée aux membres de l'organisation. Une prise de décision déviante sera alors considérée comme contraire à l'ordre initial et à la finalité de celui-ci et non comme n'étant pas parfaitement iden-

tique à la consigne initialement donnée. Un exemple patent, bien que simpliste, serait un tir volontairement raté sur une cible donnée. Au titre d'exemple plus complexe, citons une prise de décision qui impliquerait une priorisation d'objectifs différente de celle initialement fixée et décidée par la hiérarchie, et qui, *in fine,* ne permettrait pas d'atteindre l'effet final recherché par l'organisation commanditaire.

Concernant les décisions et actions déviantes pouvant résulter d'informations ou de contenus auxquelles les personnels seraient soumis par l'intermédiaire d'Internet, notons que la concurrence entre la communication verticale de l'organisation et les autres canaux d'informations sera d'autant plus efficace que les agents pourraient considérer que ces dernières émanent de leurs pairs. Le risque est d'autant plus prégnant que les sujets qui pourraient être visés n'ont pas conscience d'être des cibles potentielles. Au contraire, convaincus d'avoir construit leur personnalité autour de valeurs fortes, testées empiriquement et en situations extrêmes voire de crise, ils se pensent immunisés contre des opérations d'influences exogènes. Pourtant, c'est précisément en jouant sur ces valeurs que la manipulation aura la plus grande efficacité. Cette absence de prise de conscience du risque auquel elles sont exposées accroît fortement la vulnérabilité des cibles potentielles.

À l'inverse de ce que l'hyper connexion des plus jeunes, démontrée par l'américain press Institut, aurait pu le laisser penser, l'étude montre que l'âge n'est pas un facteur de sensibilité accrue aux informations extérieures. En effet, plus que l'âge des agents, c'est davantage le temps passé dans l'organisation, particulièrement en situations extrêmes,

qui se révèle avoir l'impact le plus significatif matière de vulnérabilité au risque de manipulation.

2. Propositions managériales

Ce travail a permis de faire émerger différentes propositions visant à limiter le risque de survenance de décisions déviantes à l'origine d'une exécution inappropriée des instructions pouvant donner un résultat contraire aux attentes de l'organisation.

Ces propositions concernent les différentes étapes de la vie professionnelle des agents (le recrutement, la formation, le déroulé de parcours professionnel et la transition intervenant en fin de carrière).

Au titre des propositions managériales relevant de la prévention, un premier travail pourrait être mené lors du recrutement afin de détecter les profils particulièrement sensibles à certaines des valeurs qui seront amenées à être ensuite développées par l'organisation. En effet, comme expliqué précédemment, ces valeurs et leur internalisation sont nécessaires à l'organisation, néanmoins, elles sont à double tranchant et peuvent également représenter une faille en ce que les personnels y seront hyper réactifs. Dans les faits, cette sensibilité accrue pourra avoir des conséquences sur la perception de contenus qu'ils pourraient être amenés à consulter autant que sur les sources les diffusant: cette sensibilité, de nature émotionnelle, pourra les pousser à faire fi des règles de prudence appliquées usuellement quant aux sources du message reçu ainsi qu'au contenu véhiculé. Dans le cas de personnels ayant déjà un attachement fort à ces valeurs, il est possible qu'ils soient d'autant plus réactifs, avoir connaissance de ce point pourrait permettre d'effectuer un suivi plus fin. Cette proposition pourrait également s'adapter à

une organisation civile ayant construit son identité sur des valeurs fortes et évoluant en situation extrême.

Dans le même ordre d'esprit, et dans la prolongement des sas de décompression mis en place à Chypre, des tests prenant en compte ce risque et l'altération de la confiance par l'entremise des valeurs pourraient être mis en place au cours de la carrière afin de percevoir si un personnel est impacté avant de le redéployer.

Un autre axe repose sur la perception du risque. Il est clairement apparu, notamment au travers des résultats de l'observation dirigée, que si une formation est réalisée au sein des armées, les résultats en sont largement perfectibles. Les personnels ne percevant que peu ce type de risque d'influence: s'ils sont conscients que l'on peut vouloir leur extorquer des informations, ils perçoivent moins qu'on puisse vouloir influencer leur comportement en leur soumettant des contenus prenant l'apparence d'une information. Par nature, ce manque de conscience affaiblit leur capacité à se prémunir du risque. En outre, ils pensent généralement que leurs valeurs les protègent de ce type d'action alors qu'elles sont justement le point d'appui de ces dernières comme vu dans les études de terrain. Ainsi une formation plus finement ciselée, appuyée sur des méthodes d'inoculation pourrait être d'une grande aide. En restant dans le champ de la prévention, une sensibilisation dédiée comprenant des scénarios immersifs et une évaluation pourrait être créée pour sensibiliser et éduquer les cibles potentielles sur le risque auquel elles sont confrontées. Cette proposition est en accord avec les résultats de Santos et al (2017), qui considèrent que les facteurs expérimentaux ont un impact beaucoup plus important que les facteurs dispositionnels. Ces formations pourraient participer activement à améliorer

la sécurité et, dans notre cas, la confiance et la cybersécurité. Il est à noter que les personnels entendus lors de cette recherche semblent tout à fait favorables à ce type d'approche. Cette problématique touche également les organisations intervenant dans le secteur civil, aussi, cette proposition de sensibilisation et de formation ciselées permettant de mieux comprendre le risque pourrait être particulièrement adaptée à un large spectre d'entreprises confrontées à ce risque d'influence pouvant altérer le déploiement de leurs stratégies.

Il est également apparu que les moyens de communication moderne déployés sur Internet et pouvant être consultés en tout temps et en tous lieux grâce notamment aux smartphones représentaient un axe pouvant être mobilisé lors d'opération d'influence. Se prémunir de ce risque devient donc un sujet important. Une vision simpliste serait de refuser l'accès à Internet au personnes pouvant perte ciblées. Mais cela ne sera ni efficace ni réaliste. Premièrement, parce que les attaques peuvent se produire pendant le temps passé dans la sphère privée, ensuite parce que cette interdiction serait probablement perçue comme une restriction de liberté, générant le rejet et la méfiance (Brehm, 1965). De plus, comme l'attaque n'est pas circoncise aux temps de projection en OPEX ou aux périodes d'entraînement, interdire l'accès pendant les heures de travail ou sur les bases échouera probablement à éliminer ce risque. Par contre, il serait envisageable de créer un système permettant de suivre les sollicitations visant les valeurs cœur reçues par les personnels par l'intermédiaire de leurs consommations Internet. L'idée ne serait pas d'avoir une approche coercitive assimilable à un proxy, mais d'avoir un système d'alerte informant l'utilisateur qu'il a reçu un pourcentage plus élevé de sollicitations visant telle ou telle valeur (par exemple par l'intermédiaire de l'apparition de fenêtres

pop up ou de propositions de vidéos YouTube, etc.). Cet outil pourrait être proposé aux personnels après avoir qu'ils aient été sensibilisé à ce risque spécifique conformément à la troisième proposition managériale. Le principe serait une installation sur la base du volontariat sur les appareils de connexion (téléphones portables, ordinateurs, etc.) sans rétrocontrôle auprès de la hiérarchie. Le système avertirait son utilisateur lorsqu'ils feraient l'objet d'une augmentation de sollicitations abordant des sujets ayant trait à ses valeurs centrales, contenus à même de renforcer ces dernières et de rendre les cibles potentiellement hyper réactives à une seconde vague d'informations tentant d'enclencher un éveil de dissonance cognitive visant à altérer la confiance accordée à la hiérarchie ou à l'organisation. Le message ainsi délivré par l'organisation qui fournirait cet outil serait qu'elle estime ses personnels assez responsables pour faire le tri dans les contenus auxquels ils sont soumis pour peu qu'ils en soient avertis. Ce message, doublé de l'adoption de cet outil sur la base du volontariat et de l'absence de retour des informations au commandement, permettrait de renforcer la confiance tout en accentuant la prise de conscience de la possibilité de ces opérations ciblées. Ce type de propositions est transposable au-delà du cadre militaire dans des secteurs d'activité plus classiques.

Partant du principe selon lequel les données véhiculées par la communication peuvent impacter la confiance des personnels, particulièrement si elles touchent (avec plus ou moins d'exactitude) les valeurs dont l'organisation est porteuse et qu'elle transmet à ses personnels, il paraît important de mieux cibler la communication interne.

En ce qui concerne le management RH proprement dit, la présente recherche a mis en avant que la perte de confiance peut s'appuyer sur la perception de la verticalité institu-

tionnelle doublée à une scission entre les catégories professionnelles. Les soldats percevaient leurs pairs comme faisant partie de leur groupe, le manque de confiance se concentrant plus facilement sur leur hiérarchie, notamment intermédiaire, qui est alors considérée comme un groupe externe. La distinction faite entre ces deux catégories est souvent responsable des perturbations des relations intergroupes (voir Yzerbyt et Demoulin, 2010). Certaines suggestions pourraient aider à résoudre ce problème en affaiblissant quelques points sur lesquels les personnels s'appuient pour justifier cette distinction entre les groupes. À ce titre, le temps d'affectation du management de proximité semble jouer un rôle fort. Perçu comme bref par les personnels, ces derniers sont plus enclins à estimer que les officiers pensent prioritairement à leur carrière personnelle plus qu'au bien de l'unité et des hommes qui la composent sur le long terme. Un accompagnement visant à démystifier cette croyance ainsi qu'un allongement de la période d'affectation pourrait être une piste.

Un autre point participant à renforcer la perte de confiance dans la hiérarchie consistait en une perception d'un traitement différencié entre sous-officiers et soldats d'un côté et officiers de l'autre, notamment en fin de carrière. Plusieurs se sentaient abandonnés alors qu'ils avaient connaissance de systèmes d'accompagnement visant à aider la transition professionnelle de membres de leur hiérarchie, notamment des officiers généraux. Pire, certains se sentaient coincés dans leur emploi, craignant de ne pouvoir intégrer le secteur privé (qu'ils ne connaissaient pourtant pas pour la plupart puisque s'étant engagés au tout début de leur vie professionnelle), ils ont l'impression d'être tenus dans une relative captivité par l'organisation. Dans le même ordre d'idée, certains confient avoir du mal à confier leurs nouvelles aspirations professionnelles. Cette crainte a plusieurs

motivations qui se retrouvent pour certaines dans le manque de confiance accordée aux soignants du secteur psychologiques. Ainsi, la crainte de ne pouvoir être parfaitement compris par un tiers n'ayant pas partagé leur vécu opérationnel est un point systématiquement évoqué. Un autre volet et la crainte de représailles de la part de leur hiérarchie directe, notamment dans les missions qui pourraient leur être confiées (par exemple en les excluant de celles plus rémunératrices) s'ils venaient à connaître leurs doutes et leurs potentielles aspirations de changement de carrières.

Un moyen de contourner cet a priori serait de mettre en place une structure dédiée à la reconversion de ces personnels. Afin d'éviter l'écueil de la confiance, partant du potentat qu'ils ne peuvent l'accorder à des personnes n'ayant pas un vécu commun avec les cibles, cette structure pourrait être composée principalement d'anciens d'unités actives. Ces personnels devraient alors recevoir une formation dédiée tant dans la reconversion professionnelle que dans le coaching. Cette structure devrait également être rattachée à l'état-major du ministère des Armées et non au chef de corps afin de court-circuiter la crainte de représailles évoquée lors des entretiens. En outre, ce rattachement permettrait aux personnels de prendre conscience de l'intérêt sincère que leur porte leur institution, ne les considérant pas uniquement comme « des cases dans un tableau Exel », ce qui permettrait mécaniquement de renforcer la confiance. Cette approche est droite ligne avec le « Plan Famille » voulu par Madame la ministre des Armées. Cette structure aurait pour mission de se déplacer dans les unités afin d'avoir un contact direct avec les personnels y compris ceux s'interrogeant sur leur avenir professionnel. Il est probable que cette démarche n'engendrerait pas pour autant une hémorragie des forces vives des armées, mais elle permettrait d'aider les personnels qui le souhaitent vraiment à partir à le faire dans de bonnes conditions. Par ruissellement, les personnels qui feraient le choix

de rester dans leur emploi ou de renouveler leur engagement le feraient pour de « bonnes raisons » et non pas avec un sentiment de contrainte propre à altérer leur confiance. En outre, réduire le nombre de personnels aigris aura pour conséquence de limiter la potentielle viralité au sein du groupe de sentiments délétères à l'encontre de la structure, viralité qui ouvrirait une brèche patente et encore plus exploitable par des opérations informationnelles ciblées. De manière plus insidieuse, le passage des membres de cette structure pourrait représenter un premier pas dans la détection de mal-être des personnels dus, par exemple, à des syndromes de choc post-traumatique dont certaines victimes n'auraient pas voulu parler aux professionnels de santé mis à leur disposition par le Service de Santé des Armées (SSA). Notons ici qu'une préconisation serait de renvoyer sur le terrain les membres de cette structure tous les deux à trois ans minium. En effet, il est apparu que les personnels ont tendance à estimer que même des individus ayant partagé un vécu semblable au leur en oublient les réalités quand ils en restent trop longtemps éloigné. La durée serait à estimer plus finement, mais les entretiens recueillis permettent de dégrossir cette durée de supposée péremption entre deux et trois ans. Outre les effets mentionnés ici en ce qui concerne le renforcement de confiance entre les personnels et la haute hiérarchie, ce travail permettrait de capitaliser en matière d'image des armées, en faisant la démonstration l'intérêt porté à leurs personnels au-delà de leur passage en son sein, en droite ligne avec les valeurs de loyauté et de sens de l'honneur porté par cette organisation. On pourrait soutenir que le coût de laisser des soldats formés quitter l'établissement est trop important, cependant analyser ce coût à la lumière de celui que représente des soldats dysfonctionnels permettrait de modérer cet argument.

3. Limites de la recherche

Cependant, ce travail de recherche n'est qu'une première étape et il a, à ce titre, rencontré un certain nombre de limites qui pourraient faire l'objet d'un approfondissement. Cet approfondissement nécessiterait notamment de mener une analyse qualitative adossée à un recueil de données plus massif que ce qu'il a pas été possible de réaliser dans le temps imparti, et sans moyen matériel et temporel autre que ceux dont disposait l'auteure de ce travail. Dès lors, les volets applicatifs sont ici ébauchés, mais méritent encore d'être approfondis.

Il conviendrait également d'affiner les granularités relatives aux facteurs qui peuvent déclencher la défiance et la confiance ce qui permettrait de pouvoir définir des stratégies plus précises quant à la détection, la prévention et la correction des effets délétères induits par des opérations visant l'altération de la confiance au sein d'équipes intervenant en situations extrêmes.

Une autre limite aura été de poursuivre la recherche dans d'autres milieux intervenant en situation extrême afin d'observer si les leviers sont bien les mêmes ou s'ils diffèrent en fonction du champ d'activité de l'organisation. Cet axe permettrait d'affiner la transposabilité des résultats présentés ici.

Enfin, pouvoir croiser avec plus de finesse les résultats obtenus avec d'autres champs de recherche comme les computer science aurait sans doute permis de mettre en lumières d'autres éléments. En effet, cette discipline a étudié des problématiques liées à l'influence pouvant être mise en oeuvre afin de modifier le comportement humain, l'objet de ces recherches étant notamment de pouvoir modéliser les méthodes afin de développer des logiciels aptes à les détecter avec une grande célérité. Mais là encore le temps et

les moyens dont disposait l'auteure ne permettaient pas de pousser plus avant la recherche dans cette direction.

4. Perspectives de recherches complémentaires

Cette recherche n'étant que le premier volet d'un programme bien plus large, elle ouvre sur plusieurs perspectives de recherches complémentaires.

À ce titre, il serait intéressant de conduire une étude plus approfondie à partir des travaux en neurosciences selon lesquels la dissonance cognitive emporte des effets physiologiques ce qui n'a pas pu être réalisé ici. Cette approche permettrait de penser un traitement plus efficace des conséquences sanitaires de ces manipulations, ainsi que de développer des méthodes permettant d'adapter le management des personnels pouvant être ou ayant été l'objet de ce type d'opérations. En effet, plusieurs études montrent les conséquences comportementales lourdes que l'exposition à la dissonance cognitive peut avoir. Certains de ces troubles pouvant même être associés à certains effets liés au syndrome de choc post-traumatique. Travailler plus en profondeur sur ces points pourrait permettre une meilleure prise en charge des effets induits par une exposition prolongée et faciliter la prise en charge avant que les personnels ne soient victimes de dégâts trop importants.

La présente recherche a fait émerger des points clefs s'agissant de la compréhension des mécanismes pouvant amener à des prises de décisions déviantes de la stratégie définie par l'organisation, et aura permis de formuler quelques propositions managériales. À ce titre, en s'appuyant sur les travaux de Santos et al (2017) notamment, il serait intéressant de modéliser les signes physiques de la confiance, analysables de manière non invasive (mouvements rétiniens par exemple), lorsqu'un individu est face à un contenu,

informatique ou papier. En effet, les travaux évoqués ci-dessus montrent que les mouvements rétiniens peuvent être modélisés et mis en relation avec les zones stimulées au sein du cerveau (visibles par imagerie médicale). On pourrait alors en définir une cartographie. Affiner cette cartographie pourrait permettre d'avoir une idée précise du degré de confiance accordé à un contenu type. Une fois le recensement effectué, il serait alors envisageable de tester la confiance accordée à un contenu visant à altérer la confiance dans l'organisation pouvant ainsi potentiellement modifier le comportement de l'individu visé. Selon les résultats, il pourrait alors paraître pertinent de ne pas déployer un personnel sans avoir préalablement travaillé avec lui à renforcer la confiance qu'il accorde à la structure. Ce travail aurait nécessité un partenariat avec des laboratoires en biologie médicale et en imagerie médicale, partenariat qu'il n'a pas été possible de mettre en œuvre lors de ce premier travail.

Il apparaît également que l'identification des causes de ces dysfonctionnements de la confiance amenant à une exécution déviante des consignes est capitale, celles-ci pouvant emporter des conséquences délétères, tout particulièrement dans le cas d'organisations intervenant dans des contextes à forte incertitude où la pression exercée sur les individus est élevée. Or, de tels environnements sont de plus en plus fréquents, indépendamment du secteur d'activité dans lequel évolue la structure, serait-elle publique ou privée.

Si ce travail s'est particulièrement attaché à l'analyse de ce risque dans les structures militaires, on peut néanmoins postuler que ces enseignements pourront s'appliquer à d'autres organisations civiles. Plusieurs arguments plaident en la faveur de cette transposabilité. Tout d'abord les contextes similaires ou comparables à ceux développés ci-dessus, à savoir soumis à une tension forte, dans des contextes évolutifs, dangereux (le

risque pouvant ne pas être physique, mais compris comme touchant au champ psychologique, environnemental ou économique) et à imprévisibilité forte (ce qui peut par exemple ramener aux systèmes complexes tels que développés par Snowden (2011)). Si les secteurs interagissant avec la sécurité civile tels que les policiers et les pompiers viennent immédiatement à l'esprit, car leurs caractéristiques et contextes de déploiement sont très proches de ceux étudiés dans le cas des forces armées, on ne peut faire l'exclusion d'autres secteurs d'activité évoluant également dans des situations qualifiables d'extrêmes et porteurs des valeurs fortes. À ce titre, divers secteurs de l'énergie pourraient tout à fait être ciblés, que l'on pense du nucléaire ou de l'extraction pétrolière (notamment en haute mer), au même titre que des laboratoires pharmaceutiques dépositaires de la santé humaine tout en étant des entreprises à but commercial dont les produits, s'ils sont mal conçus, peuvent avoir des conséquences graves, irréversibles, voire létales. Les secteurs de la finance sont également aux prises avec la gestion de situations extrêmes en ce que les marchés sont souvent évolutifs, que la prédiction en est parfois aléatoire et que les risques sont réels. La perte de plusieurs millions peut non seulement engendrer la fermeture d'entreprises créant une vague massive de licenciements dans une zone géographique qui s'en verra déstabilisée d'autant, mais le développement des banques dites systémiques aura pour conséquences qu'une crise financière pourra facilement s'étendre au-delà des frontières de l'État qui l'aura vu naître pour devenir une crise mondiale. La sécurisation de la prise de décision est d'ailleurs un sujet d'intérêt majeur dans ce secteur spécifique.

Enfin, il apparaît également que ces secteurs pourraient tout à fait représenter de véritables enjeux pour des concurrents tant ils évoluent dans des domaines très concurrentiels et très évolutifs. Ces domaines professionnels pourraient également avoir un intérêt

tout particulier pour des adversaires étatiques en ce que ces organisations et entreprises représentent souvent des enjeux stratégiques.

Aussi, nous pensons que ces résultats pourraient être transposables, néanmoins, la cartographie des valeurs et leur mode d'internalisation analysée ici nécessiteraient être étudiés selon les secteurs d'activités choisis afin de pouvoir en avoir une lecture fine et optimisée.

Liste des graphiques et tableaux

- Tableau 1 - Tableau résumant la question de recherche, ses sous-problématiques et déclinaisons chapitres où elles sont abordées…….……. ….p.22
- Graphique 1- Design de la thèse ……..….p.28
- Tableau 2 - Sources de données disponibles ayant servies à valider (« V ») ou ne permettant pas de valider (« NV ») les propositions de recherches présentées dans les différents chapitres. Les thèmes abordés reflètent les questions de recherches issues des problématiques..…….……..…p.97
- Tableau 3 - synopsis des entretiens de la première phase, vague 2……..…… . p.104
- Tableau 4 - synopsis des entretiens de la seconde phase, vague 2…….….p.109
- Graphique 2 - Exemple d'un encodage sur le nœud : valeur ->adaptabilité/ rusticité »…….…… p.111
- Graphique 3 - Exemple d'un graphique reprenant le nombre d'encodages par valeur qui a été utilisé dans le chapitre 6 de ce travail…….…..p.112
- Tableau 5 - Sources utilisées pour valider ou invalider les proposition présentées dans le chapitre 3…….p.118
- Tableau 6 - Représentation de la structuration de la confiance.……..…p.156
- Tableau 7 - Thèmes abordés dans les entretiens et échelle d'évaluation de la confiance…….p.165
- Tableau 8 - Sources utilisées pour valider ou invalider les proposition présentées dans le chapitre 4…….p.187
- Graphique 4 - Graphiques relatifs à l'usage d'Internet sur la population auditionnée. …….p.201
- Graphiques 5 - Graphiques comparés de la confiance portée aux réseaux sociaux et médias alternatifs et de l'appui sur les réseaux sociaux comme élément probant de la véracité d'un fait…… …….p.203
- Tableau 9 - Sources utilisées pour valider ou invalider les proposition présentées dans le chapitre 5…….p.209
- Graphique 6 - Trust in peers (in dark) and in Institution (in light) as function of months spent in External Operations. The dark dots and the light cross represent the associated observations. The dot lines represent 95% CI…….…….p.232

- Tableau 10 - Sources utilisées pour valider ou invalider les proposition présentées dans le chapitre 6…….p.253
- Tableau 11 - Summary table of the theoretical framework and concepts mobilized in the proposals…….…….……p.268
- Tableau 12 - Ratio (in percentage) of values ranking according to self-declaration……p.273
- Tableau 13 - Comparison between army values hierarchy and personal values hierarchy……..…p. 274
- Graphique 7—Graphic one the number of encryption related to values of the whole sample.……..…..p. 276
- Tableau 14—Ratio (in percentage) of the values the most quoted by the participants. ……..…..p. 277
- Tableau 15—Difference in values hierarchy between peers according to age……p. 280
- Tableau 16 - Values hierarchy discrepancy based on time spend talking of them (green are values appearing only in younger interviewee's hierarchy; pink are the ones only appearing in older interviewee's hierarchy).……p. 280
- Graphique 8—Comparative graphics of reasons of mistrust in organization exposed by respondents…….p. 287

La prise de décision en situations extrêmes sous l'effet des nouvelles stratégies informationnelles: le cas des équipes militaires

Résumé: Cette recherche étudie l'altérer la confiance au sein d'équipes évoluant en situations extrêmes, ici les militaires. Elle s'attache à analyser l'influence de cette altération sur la prise de décision relative à l'exécution des ordres donnés et aborde le rôle à double tranchant des valeurs. Cette recherche repose initialement sur des observations conduites en situation extrême, en zone de guerre, en Ukraine, puis sur 38 entretiens menés en France et sur une observation systématique réalisée avec 21 participants. Ce travail trans-disciplinaire s'appuie sur des modèles de psychologie sociale, sur la polémologie, les sciences de la gestion, et sur l'analyses des situations extrêmes. Il suggère un modèle expliquant comment la différence de valeur peut avoir un impact sur la confiance et sur le comportement d'un agent pouvant déstabiliser l'organisation. Dans une approche abductive, il propose qu'une exposition à des informations confrontant les valeurs fondamentales, notamment par Internet, déclencherai une réaction forte, affaiblissant la prudence envers la source, pouvant aller jusqu'à modifier la confiance dans l'organisation.
Enfin cette recherche analyse les conséquences de ce mécanisme, insiste sur la nécessité fondamentale de le prendre en compte et propose quelques suggestions qui pourraient être faites pour le gérer.

mots clés : Confiance, cyber, influence, prise de décision, situations extrêmes, personnels militaires, valeurs, dissonance cognitive, dissonance informationnelle, sécurité nationale

Decision making in extreme situations under effect of new informational strategies: the military teams case

Abstract : This research addressed the possibility of trust alteration in teams working in extreme situations- namely soldiers- through the Internet, and its influence on decision-making and order execution. It also observes the double-edged role of values among army personnel. It focuses on how trust alteration and value discrepancy may impact personnel behaviour and destabilize the organization.
This study is firstly based on observations led in extreme situations, in a war zone, in Ukraine, then on 38 interviews led in France and on a directed observation on 21 subjects. This trans-disciplinary work is based on social psychology models, in war studies, management sciences, and in extreme situations theories. It suggests an exposition to information which confronts the core values, especially through the Internet, should trigger an overwhelming reaction, weakening caution towards the source, and could finally modify the trust in the organization. Finally, this research focused on the consequences of this mechanism, the fundamental necessity of taking it into account and suggests proposals which could be made to cope with it.

Key words :Trust, cyber, influence, decision making, extreme situations, military personnel, values, cognitive dissonance, informational dissonance, national security