De la Network Centric Warfare à la Recognized Cyber Picture, la confiance interpersonnelle comme facteur de gestion des crises cyber

Florent Bollon, Nicolas Maille, Anne-Lise Marchand, Laurent Chaudron

De la *Network Centric Warfare* à la *Recognized Cyber Picture*, la confiance interpersonnelle comme facteur de gestion des crises cyber

Florent BOLLON, Nicolas MAILLE
Office National d'Etudes et de Recherches Aérospatiales (ONERA), France
Florent.Bollon@ensc.fr, Nicolas.Maille@onera.fr

Anne-Lise MARCHAND
Centre de Recherche de l'Ecole de l'Air (Crea), France
anne-lise.marchand@ecole-air.fr

Laurent CHAUDRON
Theorik-Lab, France
laurent.chaudron.1981@polytechnique.org

Résumé

Les premières attaques informatiques de grande envergure ont entrainé une prise de conscience sur la vulnérabilité des systèmes interconnectés. Afin de prévenir la présence d'un dysfonctionnement causé par une cyber attaque un système nommé « Recognized Cyber Picture » est envisagé par l'armée Française. Cependant, cette RCP sera potentiellement affectée par la perte de confiance des opérateurs dans la fiabilité des nouvelles technologies de l'information et de la communication. Il devient donc nécessaire de s'intéresser aux différents facteurs permettant la gestion d'une crise cyber, dont la communication directe entre les différents opérateurs. Cet article propose, en se basant sur des études de cas survenus dans l'aéronautique militaire et les résultats d'expérimentations, de regarder le champ relatif à la confiance interpersonnelle.

Mots-clés : guerre réseau-centrée, Recognized cyber picture, Technologie de l'information et de la communication, confiance interpersonnelle, confiance rapide

Abstract

In order to prevent the increase in both the number and the strength of cyber-attacks, military cyber operations centers are settings up by States. The French ministry of defense is own system, called "Recognized Cyber Picture", dedicated to monitor the state of systems and information flows. As cyber-attacks potentially corrupt the ICT, the use of this system could be affected by the level of trust in the resulting information. Direct communication between first line operators could be used to manage the crisis. In this paper we look at the impact of interpersonal trust through operational situations and experimental results.

Keywords: Network centric warfare, Recognized cyber picture, Information and Communication Technologies, interpersonal trust, swift trust

Introduction

La notion de guerre réseau-centrée (*Network Centric Warfare* - NCW), apparait en 1998 en s'inspirant des transformations du monde économique de l'époque dans lequel le développement des réseaux informatiques modifiait profondément les organisations, la productivité et la réactivité des entreprises (De Neve & Henrotin, 2006). Cette nouvelle organisation des opérations

militaires a fait prendre une place prépondérante aux technologies de l'information et de la communication (TIC), permettant une augmentation des liens entre les différentes entités coexistant dans une zone de combat. Ainsi, en 1999, pendant la guerre au Kosovo, la mise en place de la NCW a permis des prises de décision faisant intervenir, par le biais de communications satellites, de fibre sous-marines et de radio fréquence une dizaine d'acteurs de pays et d'unités différentes. Durant cette guerre la NCW a aussi démontré sa capacité à améliorer la coordination en permettant une intervention des troupes aériennes moins d'une heure après une demande de tir. La prépondérance des TIC, que ce soit dans l'observation des informations présentes, dans l'orientation des actions, dans la décision de la stratégie ou encore dans le passage à l'action (Levieux, 2005) a même permis de réduire ce temps à moins de vingt minutes durant la guerre de 2003 en Irak (De Neve & Henrotin, 2006).

Afin de bénéficier pleinement des avantages de cette organisation réseau-centrée, en 2006 la France commence à équiper ses chasseurs d'une liaison de données tactiques nommée « Liaison 16 » (L16). L'implémentation de la L16 entraine un changement d'échelle dans la NCW en permettant les communications au-delà de la ligne d'horizon et une standardisation au sein des troupes alliées. En effet, afin d'implémenter au niveau OTAN le concept de la NCW, la L16 a été pensée comme un outil d'aide à la décision centré réseau, interopérable (Godé & all, 2012). Toutes les unités, quel que soit leur pays et leur armée, peuvent, si elles sont équipées de liaison de données tactiques interopérables, aider à la création d'une représentation partagée de la situation tactique (SITAC). Cette pluralité des sources d'information et de leur provenance constitue la force du système mais rend aussi le processus plus complexe. Pour le pilote ou l'opérateur engagé dans les opérations, ces changements l'obligent à passer de l'utilisation d'une SITAC relativement limitée, alimentée par ses proches et sa hiérarchie, à une SITAC plus complète mais dont il ne connait pas l'ensemble des sources d'information. Du fait de la fiabilité des TIC et du nombre d'informations recoupées pour créer une SITAC, le système semblait fonctionner correctement. Cependant, des nouvelles menaces provenant du cyberespace apparaissent, comme en Estonie en 2007, en Géorgie en 2008 ou encore en Iran en 2010 (Farwell & Rohozinski, 2011) et remettent en cause précisément la fiabilité des TIC et la confiance que l'on peut avoir dans les données échangées.

En 2009 par exemple, le virus « Conficker » infecte le département américain de la défense, le ministère de la défense britannique et empêche, pendant 2 semaines, le décollage des Rafale de l'aéronavale française (Baud 2012). La virulence de cette première cyber-attaque de grande envergure touchant les infrastructures militaires a entrainé une prise de conscience sur la vulnérabilité des systèmes de défense. En entrainant une remise en cause de la confiance qu'ont les opérateurs dans les systèmes informatisés (eg. la SITAC créée par la NCW) ces cyber-attaques ont amené les états à mieux définir leurs besoins et leurs stratégies de gestion de la cyber sécurité. Afin d'accélérer le processus décisionnel et de coordonner au mieux les actions en cas d'attaque provenant du cyberespace il devient nécessaire d'avoir une représentation partagée de l'état cyber du réseau, qu'il soit passé, présent ou futur (Vilchenon,

2015). Pour garder une souveraineté nationale sur les systèmes de cyberdéfense, la France décide de mettre au point son propre système. Au sein des forces françaises, le système ou l'outil, actuellement en cours de développement, pensé pour permettre cette représentation se nomme la « Recognized Cyber Picture » (RCP).

La RCP sera un système militaire entièrement français, qui sera déployé à différents niveaux hiérarchiques pour surveiller et gérer la cyber sécurité des systèmes d'information, de communication et de défense français. Elle sera potentiellement utilisable en opérations extérieures, et, dans ces cas-là, devant apporter des informations utiles aux membres de la coalition. De fait, dans le cas où la RCP permet de détecter une faille sur les systèmes de communication d'un appareil équipé de L16 et effectuant une intervention dans le cadre d'une coalition internationale les différents acteurs du réseau devraient en être informés, que ce soit au sein des forces françaises ou au sein des forces alliées. La transmission d'une telle information qui pourrait être classée comme sensible pose un problème de fond à résoudre. En effet, du fait de la perversion possible du réseau de communication lors d'une cyber attaque il devient dangereux d'utiliser ce même réseau afin de prévenir les autres utilisateurs. De plus, ces utilisateurs risquent de douter de la véracité de l'information transmise s'ils ont connaissance par un autre moyen de l'attaque en cours. De ce fait, si une défaillance potentielle sur un réseau de communication est détectée, le recours à un travail sans utilisation des TIC modernes pourrait être une des solutions à court terme pour lever une alerte et soutenir les premières décisions. Ainsi, il semble probable que d'autres systèmes de communications tels que la radio puissent être utilisés pour pallier les potentiels problèmes de fonctionnement des TIC modernes. Un des éléments clé pour les opérateurs sera la confiance que l'on peut avoir dans les informations reçues et à partir desquelles des décisions vont être prises. La NCW et la RCP étant des systèmes sociotechniques cette confiance peut se bâtir à partir de la connaissance du système mais également des informations provenant des autres opérateurs.

Nos travaux visent à mieux comprendre l'impact des relations entre les personnes dans le système sociotechnique de la RCP et les facteurs qui influent sur les performances globales. En cas de cyberattaque et de compromission des données transmises par le système, cette communication interpersonnelle pourrait être le facteur clef de la viabilité des TIC. Dans la partie 2 de cet article nous regardons comment la radio, paraissant être un système archaïque de communication en comparaison aux systèmes de liaison de données tactique, pourrait jouer un rôle dans la fiabilisation des informations transmises par les systèmes électroniques. Si tel en était le cas la force de cette fiabilisation sera certainement liée au niveau de confiance interpersonnelle (CI) entre les divers acteurs de la RCP. Ceci nous amène à étudier les différents types de confiance interpersonnelle (CI) ainsi que leur fonctionnement. La partie 3 se base sur une revue de littérature pour identifier les mécanismes permettant la construction de la CI. Enfin, la partie 4 s'intéresse à l'impact que peut avoir un niveau de confiance plus ou moins important pour l'utilisation de la RCP.

Fiabilisation de l'information

Dans cette partie, nous nous intéressons à l'activité d'opérateurs dans des situations opérationnelles en prêtant une attention particulière aux échanges d'information. Notre premier cas d'étude est celui de la réaffectation d'objectifs pour les missions d'appui feu au profit de troupes au sol. Celui-ci consiste à modifier la mission d'un ou de plusieurs appareils déjà engagés sur le théâtre d'opération quand une demande d'appui feu est émise par des troupes au sol. Le réseau-centrage de la coalition, par le biais notamment de la L16, permet d'obtenir une représentation partagée de la situation tactique et va jouer un rôle prépondérant dans le processus. Grâce à la NCW il est aujourd'hui possible de déterminer rapidement l'aéronef le plus à même de réaliser cette tâche d'appui feu, même si cet appui feu ne fait pas partie de ses missions initiales et de lui transmettre les éléments nécessaires pour cette nouvelle mission (position des troupes ami et ennemies…). Si l'utilisation de la NCW a permis des gains importants en termes de réactivité ou d'adaptation, des études de l'activité des opérateurs montrent que son introduction n'a pas pour autant fait disparaître le besoin de la transmission d'information entre les opérateurs par d'autres vecteurs de communication. Ainsi, bien que la L16 soit réputée « imbrouillable » les retours d'expériences pour les tâches d'appui feu montrent que la communication par radio est toujours utilisée. En particulier, plus le pilote se rapproche d'une cible transmise par un personnel au sol, plus le nombre de communications radio augmente (Jansen& Soeters, 2017).

Ces éléments suggèrent qu'en dépit de la puissance que semble avoir la NCW grâce aux TIC, la communication interpersonnelle par le biais de la voix semble être préférée dans certaines tâches à fort risque vital. Ceci peut être lié au fait que la radio entraine la présence d'indices sur les personnes émettrices de l'information. En effet, la grammaire, la sémantique ou encore la variation linguistique sont des vecteurs langagiers de l'identité sociale. La voix et la manière de parler d'une personne transmettent aussi des informations importantes sur son état de stress et plus généralement sur son état émotionnel (Sherer, 1986). Tout porte donc à croire que, dans ces situations de coopération étroite pour un appui feu, les opérateurs aient besoin de ces indices supplémentaires. D'ailleurs, des analyses montrent que l'utilisation combinée de la L16 et de la radio améliore les performances en termes de compréhension et de rapidité de la prise de décision (Gonzales & all, 2005).

La criticité de l'information vis-à-vis de ses conséquences semble être un élément qui influe sur les canaux de transmission privilégiés par l'utilisateur, mais on peut penser que ce n'est pas le seul facteur pouvant modifier le comportement de l'opérateur. La confiance dans le système qui génère l'information pourrait aussi être un élément important. A ce titre, l'incident relaté en 2013 dans le Bulletin de liaison de l'association nationale du transport aérien militaire (ANTAM) est significatif. Il repose sur le problème de la confiance des opérateurs dans la radiosonde, qui est un système permettant de connaître la hauteur de l'aéronef par rapport au terrain. Cet instrument est particulièrement utile dans les vols à basse altitude car il génère une alarme lorsque l'appareil passe en dessous d'une hauteur sol fixée à l'avance par l'équipage. La particularité de ce système est le niveau de confiance qui lui est attribué au sein

de l'armée de l'air. En effet, suite à de nombreux dysfonctionnements la radiosonde a, depuis longtemps, la réputation d'être non fiable a d'ailleurs été considérée comme une des causes de 2 accidents de Mirage 2000. De manière simplifiée, cet incident à eu lieu pendant une mission d'entrainement au largage autonome à l'aide d'un avion de transport. Pour cette mission l'équipage comprenait de deux personnes novices, une personne plus expérimentée et une personne très expérimentée qui était présente afin de superviser la mission. Durant cet entrainement de vol en basse altitude l'alarme de la radiosonde se déclencha. A cause d'un faible niveau de confiance dans cette alarme son déclenchement n'entraina aucune mesure de la part de l'équipage. Cependant, le pilote moniteur commandant, soit la personne la plus expérimentée de la cabine, ordonna au pilote stagiaire une remontée en altitude immédiate. Une fois la manœuvre enclenchée l'équipage constata que l'alarme avait eu un fonctionnement normal et adapté, et que le crash n'avait été évité que grâce à la communication orale initiée par le superviseur. La confiance accordée à l'information et sa prise en compte pour ajuster son comportement peut donc être fortement lié au canal de transmission de cette information.

Ces deux exemples tirés de situations opérationnelles permettent de mettre en valeur le rôle de la radio, ou d'une autre communication interpersonnelle directe, dans la fiabilisation des informations transmises par des systèmes électroniques. Dans le cas de la RCP, lors de la suspicion d'une attaque cyber, les opérateurs auront besoin de transmettre des informations critiques et les réseaux informatiques auront perdu de leur fiabilité. L'opérateur se retrouvera ainsi dans un cas typique où il devrait ressentir le besoin de confirmer ces informations par un lien direct avec la personne avec qui il doit coopérer. La communication interpersonnelle non médiées par les TIC sera un candidat naturel pour pallier la méfiance dans les systèmes automatisés en cas d'attaque cyber. Il est donc probable que le transfert d'information au sein de la RCP, mais aussi entre la RCP et le réseau interallié et interarmes utilise plusieurs supports et que la performance globale soit liée au niveau de confiance dans les sources d'informations mais aussi entre les différents acteurs. Nous allons donc maintenant nous pencher sur ce qu'est la confiance interpersonnelle et les éléments qui favorisent sa mise en place.

La confiance interpersonnelle

La confiance interpersonnelle (CI) est un processus mis en jeu dans les activités à risque (Karsenty, 2015) afin de réduire l'incertitude (Luhmann, 2006). Elle nécessite, pour être mis en place, trois conditions minimales : (1) la présence d'un **confiant**, qui est la personne initiatrice du lien de confiance, (2) la présence d'un **mandant**[1], c'est-à-dire la personne sujette au lien de confiance, et (3) une situation à risque pour laquelle une réduction de la complexité est nécessaire. Cette réduction de l'incertitude correspond à une simplification des possibles et l'acte d'avoir confiance peut être définit comme le

[1] Le confiant est appelé en anglais « *trustor* » et le mandant « *trustee* ». Ces termes sont parfois réutilisés en français.

fait de « *vivre comme si certains évènements rationnellement possibles n'allaient pas arriver* » (Lewis & Weigert, 1985 : libre traduction). Ainsi, avoir confiance en un autre opérateur permet de se baser principalement sur les informations qu'il donne et, par conséquent, de faciliter la prise de décision. L'utilisation fréquente de la communication radio lors des phases à risques d'une mission permettrait donc d'augmenter le niveau de CI en minimisant les problèmes potentiels liés à la technologie.

La CI n'a que très peu été étudiée en laboratoire (De Jong, Dirks, & Gillespie, 2016) mais les résultats des études, issus de questionnaires ou d'expérimentations tendent à valider la définition liant la confiance à la réduction de l'incertitude. Ainsi, dans la littérature managériale, le lien est fait entre confiance et prise de risque de telle sorte qu'un fort niveau de confiance entraine une plus grande prise de risque (Mayer, Davis, & Schoorman, 1995). De manière plus fine, cette modification comportementale entrainant la prise de risque correspond à une diminution de la supervision et du monitoring. Ainsi, lorsque le niveau de confiance est fort entre deux individus, toutes leurs ressources sont mises à effectuer la tâche. Cependant, lorsque le lien de confiance est plus faible, le confiant utilise des ressources afin de superviser les résultats transmis par son partenaire (Colquitt, Scott, & LePine, 2007). Outre cette modification comportementale la force du lien de confiance pourrait avoir des conséquences sur la performance d'équipe. Lorsque le niveau de confiance entre deux individus est fort, la performance est élevée. Ce résultat, largement répendu dans la littérature est également largement débattu. En effet, ne serait-ce que par la définition même de la performance (calcul de points, temps…) ou de par son recueil (qualitatif, quantitatif, de manière auto-déclarative ou par observation) des résultats différents peuvent être obtenus. La mesure de la performance est donc largement sujette à différents biais qui entrainent des résultats non généralisables.

Toujours est-il que dans la RCP comme dans tous systèmes utilisés en TIC, et par extension dans la NCW, le niveau de CI que le système sociotechnique permet de bâtir devrait avoir des implications sur les comportements des individus voire potentiellement sur la performance du système global. La CI étant dépendante des caractéristiques du confiant, du mandant et de la situation, il est nécessaire de se pencher sur la culture d'organisation de l'armée et sur la littérature concernant la mise en place et l'évolution de cette CI. Au sein des forces armées françaises il est possible de distinguer deux types d'organisations différentes, qui impliquent des contextes différents pour les personnes qui doivent interagir : (1) l'organisation des forces de défense sur le territoire national, basée sur un modèle hiérarchique et qui est relativement stable dans le temps, et (2) l'organisation en opération hors du territoire national qui comprend les opérations extérieures (OPEX) d'une part et les forces de souveraineté nationale ou de présence à l'étranger d'autre part. En dehors du cas des OPEX, très peu de mouvements sont présents à l'intérieur d'une cellule opérationnelle. Ces changements sont limités aux changements d'unité, de base de rattachement ou les montées en grade. En ce sens, les liens de confiance interpersonnelle à l'intérieur des unités présentes ont le temps de se former et d'évoluer.

Les OPEX par contre sont des actions plus limitées dans le temps, liées à un conflit et décidées par le président de la république. Elles sont, pour la grande majorité, issues de collaborations internationales, et, par conséquent possiblement formée d'équipes éphémères agissant dans un contexte de NCW. Ce type d'équipe peut avoir une durée de vie de l'ordre d'une dizaine de minutes dans le cas de l'appui feu et peut comporter des membres de différentes armées et de différentes nations qui ne se sont jamais vu, qui n'interagiront plus jamais ensemble mais qui doivent réaliser une tâche à fort risque vital. Ce type d'équipe éphémère, nommé « *swift starting action team* » (STAT) (Mckinney, Barker, Davis, & Smith, 2005) est courant en OPEX et ne cesse d'augmenter avec les capacités d'interactions apportées par les TIC dans la NCW. Le nombre croissant d'OPEX emmène la problématique liée à la possibilité de créer un lien de confiance dans ces équipes éphémères, c'est-à-dire n'ayant pas le temps d'apprendre à se connaitre.

La formation et la fluctuation des niveaux de confiances dans les équipes soudée et éphémères ont été étudiées indépendamment dans la littérature. La CI entre les membres d'une équipe travaillant ensemble pendant un temps très long, telle que les équipes des forces de défense sur le territoire national, est étudié dans le champ littéraire relatif à une confiance évolutive. Pour les équipes de type STAT, un champ de la littérature, portant sur une confiance dite rapide[2] est présent (cf. figure 1).

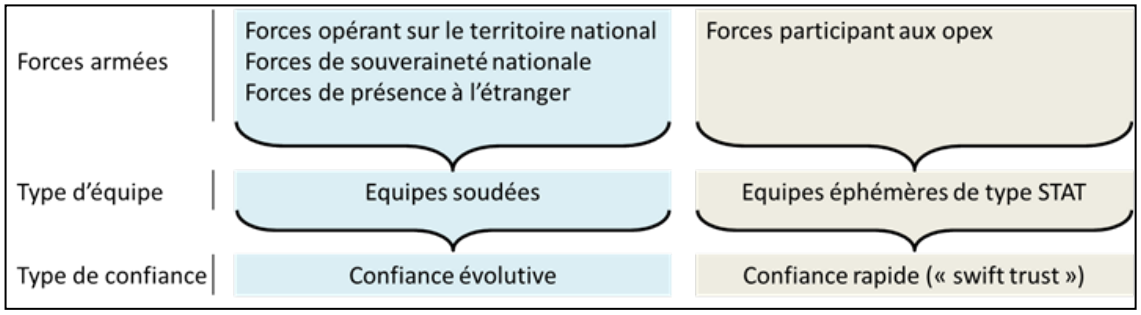

Figure 1. Type d'équipe et type de confiance associée correspondant aux différentes opérations de l'armée française

Nous allons maintenant étudier succinctement ce que la littérature nous dit de ces deux types de confiance.

Confiance évolutive

La confiance évolutive est la forme de confiance la plus étudiée en psychologie, sociologie et management. Cette théorie de la confiance prône une modification, au cours du temps, des liens de confiance entre le confiant et le mandant. Dans le champ de la littérature sur la confiance évolutive le niveau de confiance est fonction de la tâche. Ainsi, entre deux individus, différents

[2] Le terme anglais « *swift trust* » reste le plus utilisé.

niveaux de confiance peuvent exister au même moment. En fonction du nombre, de la qualité et de la résultante des interactions sur une tâche donnée, le niveau de confiance va évoluer de manière positive ou négative. Les études sur la confiance évolutive reposent généralement sur des concepts issus du modèle de Shapiro (Shapiro, Sheppard & Cherastin, 1992) qui identifie trois sources principales permettant de générer la confiance et dont leur influence va évoluer avec le temps. Ces trois moteurs de la confiance sont :

- La **dissuasion** : le confiant accorde sa confiance au mandant car si ce dernier n'agit pas comme souhaité, il pourra le punir. Cette notion est étendue dans son versant positif au fait de pouvoir récompenser le mandant si son comportement correspond à ce qui est attendu (Lewicki & Bunker, 1995). On parle alors de confiance **calculée**. C'est le plus faible niveau de confiance et correspond à ce qui s'établit au départ d'une relation, et qui peut perdurer.

- La **connaissance** : la confiance repose sur le fait que le confiant est capable de prédire de manière assez fiable ce que son partenaire va faire. Cette confiance peut s'établir sur la base des premières interactions entre les personnes et va amener un niveau de confiance plus fort que dans le cas de la dissuasion.

- L'**identification** : le confiant et le mandant se sont appropriés les désirs et les intentions de leur partenaire et agissent en vue de leur bien commun. Ceci correspond au dernier niveau de confiance interpersonnelle qui peut apparaître quand des personnes interagissent régulièrement et que ces relations confortent ce lien de confiance.

Pour ces auteurs, la force du lien de confiance entre individus, groupes ou institution va évoluer au cours du temps en fonction des conséquences de leurs interactions et met en jeu au moins trois composantes : cognitive, de réputation et affective (Shapiro, 1987 ; Lewicki & Bunker, 1995). La composante cognitive de la confiance est un processus de discrimination permettant de classer des personnes comme étant, plus ou moins dignes de confiance ou de la méfiance (Lewis & Weigert, 1985), en fonction de connaissance que l'on a sur leur caractéristique, que ce soit sociale, culturelle, ethnique, ou sur des éléments plus institutionnels comme, par exemple, des titres professionnels (McAllister, 1995). Grâce à l'observation des comportements de différents partenaires dans différents contextes, le confiant se crée une représentation des personnes qui sont pour lui digne de confiance. Cependant, pour qu'un mécanisme de confiance se mette en place il est souvent nécessaire qu'il y ait une redondance d'interaction ou qu'une troisième personne (différente du confiant ou du mandant) se porte garante du mécanisme de confiance. La réputation de l'institution peut jouer le rôle du médiateur de confiance. L'émergence de cette confiance, utilisant la réputation des institutions, est notamment facilitée lorsque les directeurs des institutions, qu'ils soient chef d'entreprise ou simples recruteurs, sont en mesure de créer des familiarités entre les personnes devant travailler ensemble (Shapiro, 1987). De plus, l'adoption de normes, structures et procédures connues et partagées dans l'institution permet une orientation des comportements des individus qui la composent et est garante de la relation de confiance (Bachmann & Inkpen, 2011). La composante affective de la confiance

quant à elle se base sur des investissements émotionnels (McAllister, 1995) et est généralement limitée aux interactions fréquentes et aux relations étroites (Lewis & Weigert, 1985).

Le niveau initial de confiance se fait principalement par des composantes cognitives, basées sur des stéréotypes que le confiant impute au mandant. Ces stéréotypes peuvent provenir de lien de confiance antérieur avec des individus ressemblant au mandant mais peuvent être également médié par l'institution que le mandant représente. Au cours de la relation le niveau de confiance va évoluer en fonction des comportements du mandant mais également grâce à des éléments plus affectifs liés à la qualité et la quantité des échanges entre les différents acteurs. Ainsi, pour étudier la résilience basée sur la confiance d'une RCP utilisée uniquement en intra France ce modèle évolutif de la confiance pourrait être le bon. Cependant, pour comprendre le rôle de la confiance lors de l'utilisation de la RCP en interarmes, voire en interallié, dans le cas d'une OPEX entrant dans une organisation de type NCW, il est fondamental de s'intéresser aux résultats que donne la littérature sur la confiance rapide.

Confiance rapide

La plupart des recherches et des théories s'intéressent à la confiance qui évolue avec le temps et est construite à travers un processus nécessitant un grand nombre d'interactions. Cependant, il existe aussi des cas où la relation entre les individus ne perdure pas dans le temps, mais où une relation de confiance est bien présente sur une période de temps courte, nécessaire à l'action commune. C'est le cas des systèmes et équipes temporaires qui sont soumis à un processus appelé confiance rapide et qui infère généralement un fort niveau de confiance interpersonnelle (Meyerson, Weick & Kramer, 1996).

Selon Crisp, la confiance rapide se bâtit à partir des composantes normatives et cognitives (Crisp & Jarvenpaa, 2013). Les règles et les rôles de chaque organisation pourraient être considérés comme étant la composante normative fournissant des preuves sociales et des mécanismes de sureté. Cette composante peut être rapprochée de la composante institutionnelle vue précédemment dans la confiance évolutive. La composante cognitive quant à elle, correspond à une évaluation, principalement sur la base de stéréotype, de la fiabilité du mandant. Il est intéressant de remarquer que dans cette approche toutes ces composantes qui fondent la relation de confiance sont imputable au mandant lui-même ou en tout cas à la représentation que le confiant en a. Pourtant des études qui s'intéressent aux mécanismes sous-tendant les relations de confiance au sein des organisations font parfois apparaître une composante directement liée au confiant, généralement nommée **prédisposition** individuelle à faire confiance (Kramer, 1999). En rassemblant les éléments de ces diverses études, on peut admettre que le mécanisme de confiance rapide repose sur les composantes cognitive et normative qui caractérisent la perception que le confiant à du mandant, ainsi que sur une composante propre au confiant, la prédisposition. Ainsi, bien que la confiance rapide permette d'attribuer, entre les personnes de groupes temporaires, des perceptions basées sur les stéréotypes personnels et professionnels provenant d'interactions du passé, la prédisposition de chaque individu à faire confiance et

sa personnalité vont aussi entrer en compte pour établir cette relation de confiance (Hyllengren & all, 2011).

Les théories sur la confiance rapide s'intéressent à des personnes dont les interactions sont sur une période de temps limitée. Elles considèrent que pendant l'exécution de la tâche en équipe le niveau de confiance entre les individus n'évolue pas. Par contre, ces théories montrent que les facteurs générant la confiance (e.g. les facteurs relatifs aux composantes cognitives et normatives) évoluent grâce à l'expérience du confiant. L'expérience faite au sein d'une équipe éphémère va conduire chaque membre à revoir son évaluation de la confiance qu'il peut accorder aux différents types de personnes avec qui il est amené à coopérer. Ce résultat est classique dans les recherches en psychologie sociale ou les notions de groupe et de stéréotype sont des processus dynamiques. Par exemple, bien que les personnes aient au départ tendance à favoriser les membres de leur groupe plutôt que ceux de l'extérieur, des expériences de coopération avec des personnes éloignées de leur groupe d'appartenance et des contacts réguliers avec un groupe étranger peuvent limiter cet effet si la coopération est productive (Delhey & Welzel, 2012). Il est montré que ces interactions régulières aident à obtenir des informations sur ce groupe, et à individualiser des membres. L'individualisation peut cependant mener à la stigmatisation qui correspond à la possession d'une caractéristique évaluée négativement par des membres d'un sous-groupe (Kurzban & Leary, 2001). Le nombre et le type d'interaction qu'un individu a déjà eu avec certains groupes de personnes peuvent donc faire évoluer le niveau initial de confiance rapide qu'il pourra accorder à une nouvelle relation.

Les expérimentations sur la confiance

Dans la méta-analyse portant sur la confiance et la performance d'équipe, 16 études en Laboratoire sont dénombrées (De Jong, Dirks & Gillespie, 2016). En étudiant ces dernières il ressort que dans la majorité d'entre elles le niveau de confiance interpersonnelle n'est pas un des facteurs contrôlé de l'expérimentation. En d'autres termes, un niveau de CI particulier n'est pas induit par la condition expérimentale, mais c'est le niveau de CI atteint qui est recueilli. En effet, après avoir réalisé la tâche qui est au cœur de l'expérimentation, le plus souvent en groupe ou devant un ordinateur, les participants évaluent, grâce à différentes échelles, le niveau de confiance ressenti en leur partenaire. Afin de pouvoir étudier l'effet de la CI sur les stratégies et les performances, il peut être important d'être capable de maîtriser ce niveau de CI. Quelques expérimentations en laboratoire ont adopté cette approche et ont étudié la CI en induisant, chez les participants des niveaux de CI faible ou forts (Dirks, 1999 ; Ferrin & Dirks, 2003). Dans ces deux études la CI était induite sur la base de données transmises par l'expérimentateur relatives à la fiabilité des autres membres, soit directement, soit à travers un rapport manuscrit relatif à une première tâche réalisée avec ce partenaire. Les tâches étant interactive, le niveau de CI pourrait se modifier au cours du temps en fonction de l'évaluation successive de la fiabilité des collaborateurs. Ainsi, le niveau de CI réellement induit tout comme le CI final ne semble pas être totalement maitrisé dans ces expérimentations.

Il en résulte que la littérature sur la confiance propose des théories tant sur la confiance rapide que sur la confiance évolutive mais que les résultats s'appuient rarement sur des expérimentations où le niveau de confiance induit est contrôlé de manière rigoureuse et son impact sur les performances ou sur le comportement évalué à travers des mesures objectives. Afin de contribuer à combler ce manque, une méthodologie d'induction de niveau de confiance initial, dans un contexte applicatif donné, a été développée et mise en œuvre afin d'observer expérimentalement l'impact de la CI sur le comportement des opérateurs (Bollon & all 2019, Bollon & all 2020). Les résultats de ces études, focalisées sur le cas des équipes éphémères de type STAT ayant des activités proches de celles des opérateurs de la future RCP, seront abordés au paragraphe suivant.

RCP et niveau de confiance initial

En utilisation quotidienne, le transfert d'information à l'intérieur de la RCP sera effectué par des membres d'une même équipe évoluant ensemble durant un laps de temps assez long. Dans ce type d'équipe le lien de confiance sesera construit au cours du temps, et ne devrait pas entrainer de biais quant à l'utilisation de la RCP. En effet, même si le niveau de confiance est bas entre deux membres de l'équipe, le transfert d'information pourra se faire par le biais d'un tiers qui sera garant d'un lien de CI élevé, au sein de l'armée ce tiers est souvent représenté par le plus haut échelon hiérarchique de l'unité.

Dans le cadre d'une utilisation en coalition internationale la RCP sera soumise aux problématiques d'équipes éphémères formées de personnes ne se connaissant pas tel que ceci est vue dans les OPEX. La littérature sur la confiance indique que dans une équipe éphémère évoluant dans un contexte de confiance rapide, un niveau de CI fort se met automatiquement en place. Cependant, très peu d'expérimentations ont été effectuées pour valider cette assertion et dans le domaine militaire les retours d'expérience des opérationnels laissent penser qu'un niveau de CI faible peut parfois intervenir. Par exemple, des témoignages de personnels navigants ayant effectués des OPEX indiquent que pendant des missions en équipe éphémère la supervision du partenaire augmente fortement, ce qui tend à montrer une baisse de la confiance entre les individus. Nous allons nous appuyer sur l'étude d'une situation particulière, qui a eu lieu dans le cadre d'une opération interalliée de 2013, pour mettre à jour des facteurs pouvant influencer ce niveau de CI.

Pour cela, nous analysons le retour d'expérience d'un Forward Air Controller (FAC), qui est un personnel militaire au sol, placé au plus près de la zone de combat, et qui transmet les informations d'une cible au pilote d'un aéronef devant réaliser une tâche d'appui feu au profit des forces amies au contact avec l'adversaire. Du fait de leur faible nombre les FAC sont mis au service de l'ensemble des forces présentes sur le théâtre d'opération. Fortement spécialisés ils font partie des militaires les plus susceptibles de travailler avec des personnes qu'ils ne connaissent pas, qu'ils ne reverront probablement jamais, provenant d'autres pays que le leur (Jansen, Soeters, 2017). Au début de cette mission le FAC est héliporté, seul, au milieu du désert avant d'être

rejoint par un groupe de 18 personnes inconnues. Le FAC décrit qu'aux premiers moments de la relation « *la panique s'installe. Je ne connais pas cette meute aguerrie et nous allons pénétrer cette vallée déjà mortelle et je cache mon stress* ». Les détails de la mission décrivent des comportements, jugés comme étant anormaux par le FAC lui-même, et pouvant être dues à ce niveau faible de confiance ressenti par le FAC. Cependant, ce niveau de confiance semble être plus élevé envers certaines personnes, et notamment ceux qui partagent la même spécialité : « *Un FAC de la marine se trouve à bord et je sais qu'il m'aidera. La communauté FAC est petite et soudée quelle que soit l'armée d'appartenance.* » Ce récit montre que dans un même contexte opérationnel il peut y avoir des niveaux de confiance différents en fonction des personnes engagées dans la relation de type confiance rapide. En particulier le narrateur identifie que les différences de nationalité ou d'arme sont plutôt des facteurs qui font baisser le niveau de confiance alors que le fait de partager une même expertise est un facteur fort pour rehausser cette CI.

Ce cas d'étude, basé sur des équipe éphémères de type STAT, apporte quelques éléments de réflexion sur le fonctionnement de la confiance rapide. Contrairement au consensus présent dans la littérature il semblerait que cette confiance rapide ne soit pas toujours associée à un niveau élevé de CI. De plus, cet exemple montre qu'on ne peut pas considérer que ce soit uniquement la situation qui module le niveau de CI. Différents facteurs, tels que la nationalité, l'expérience ou la spécialité pourraient influencer fortement cette CI, même dans le contexte d'opérations faisant intervenir cette confiance rapide.

De récentes études (Bollon & all 2019, Bollon & all 2020) confirment qu'il est possible d'induire des niveaux de confiance rapide différents entre des coéquipiers qui vont réaliser une tâche collaborative pour un temps restreint. D'autre part, elles montrent que ce niveau de CI a un impact direct sur la stratégie de supervision du partenaire : lorsque le niveau de confiance diminue, le temps de supervision augmente. Par ailleurs, la deuxième expérimentation indique que dans le cas où une décision doit être prise alors que les informations disponibles sont partiellement incohérentes, le niveau de confiance dans le partenaire va influencer la décision prise : plus le niveau de confiance dans le partenaire est fort, plus le décideur aura tendance à prendre en compte son point de vue même s'il est en contradiction avec les éléments dont il dispose personnellement. Le propre d'une attaque cyber pouvant être d'introduire des incohérences dans les données disponibles (fausses informations, suppression d'information…) la compréhension des liens entre le niveau de CI et les décisions prises est un point important à explorer.

Discussion et perspectives

La notion de guerre réseau centrée, mise en place afin d'augmenter les capacités des coalitions en temps de guerre, amène une plus grande dépendance vis-à-vis des systèmes d'information et de communication. Ainsi, l'intégration des liaisons de données tactiques, définies par l'OTAN, dans les systèmes d'armes français permet à nos forces d'agir conjointement avec d'autres alliés en partageant les données tactiques recueillis par les différents

membres du réseau. Ceci a entrainé une augmentation du nombre d'informations reçues mais pose aussi la question de la confiance que l'on peut accorder à ces données, du fait de la multiplicité des sources possibles mais aussi du transfert de ces données. Ce partage d'information qui est au départ une force et amène un gain d'efficacité, peut devenir une vulnérabilité si l'ennemi arrive à pénétrer ces réseaux, pervertir les informations qui transitent ou bloquer le système. La montée des cyber-attaques montre que cette menace est réelle. Dans ce contexte de mondialisation de l'information la nécessité d'avoir un outil qui permette de surveiller l'activité des réseaux, l'intégrité des données et de détecter des attaques n'est plus à démontrer. La RCP doit jouer ce rôle afin que la France garde la souveraineté de ses systèmes numériques, tout en restant interopérable avec les systèmes équivalents de nos alliés.

La RCP sera un système sociotechnique qui devra permettre de détecter des cyber-attaques et de prendre des décisions. Un point important sera la fiabilisation des informations sur l'état de la situation qui vont circuler et remonter vers les décideurs. Comme nous l'avons vu au paragraphe 2, tout porte à croire que la fiabilisation de ces échanges utilisera au moins partiellement des vecteurs de communications autres que les réseaux où l'attaque est suspectée. Les échanges directs entre personnes seront très certainement privilégiés par les opérateurs et doivent donc être pris en compte dès la conception de cette RCP. Un cas critique à considérer est celui de l'engagement des forces sur des conflits hors du territoire français. Il amène plus de risque pour le personnel militaire qui peut être pris à partie par les forces ennemies et donne un cadre d'échange plus complexe, ces opérations étant généralement effectuées dans des coalitions internationales. Dans ces conditions opérationnelles, il est à prévoir que les différents acteurs intervenant au sein de la RCP pour gérer une crise ne se connaitrons pas et devront agir sur un temps court. De par son contexte d'utilisation la communication orale, si elle est utilisée dans la RCP ne sera établie que lorsqu'une anomalie sera détectée par le système. De ce fait, les interactions entre les personnes seront ponctuelles et c'est pourquoi il est pertinent de s'intéresser au fonctionnement des équipes éphémères. La manière dont la confiance est générée dans ce type d'équipe correspond au cadre théorique de la confiance rapide.

Bien que la littérature sur la mise en place de la confiance rapide dans des équipes éphémères stipule un niveau de confiance élevé, les retours opérationnels dans les opérations militaires tant à montrer que ce n'est pas toujours le cas. Afin de pouvoir discuter de manière plus étayée (1) ce qui contribue à générer cette confiance rapide, (2) le niveau de confiance établit et (3) son impact sur le comportement des utilisateurs, une méthodologie permettant de contrôler de manière expérimentale le niveau de confiance dans un contexte opérationnel donné a été développée. Elle a montré qu'il est effectivement possible de créer, même dans des équipes éphémères, des niveaux de confiance distincts en jouant sur les caractéristiques du mandant. D'autre part ces différences de niveau de confiance entrainent bien des modifications comportementales du confiant, tant dans sa stratégie de supervision que dans sa prise de décision.

Afin de mieux cerner l'impact opérationnel des choix qui peuvent être fait concernant le personnel utilisé pour gérer la RCP et les moyens sociaux-techniques de fiabilisation des informations échangées, cette méthodologie expérimentale devra être réutilisée pour évaluer dans des expérimentations contrôlées l'impact sur la confiance rapide des facteurs de nationalité, spécialité et expertise. L'ensemble de ces résultats amènera des éléments objectifs pour orienter les choix nécessaires à la mise en place de la RCP dans les forces. La prise en compte de l'impact de la confiance pour optimiser le fonctionnement de ce système sociaux-technique est important car un niveau de CI mal ajusté peut amener les différents opérateurs à s'écarter du fonctionnement prévu, à mettre en place (ou supprimer dans le cas de la sur-confiance) des stratégies de contrôle qui peuvent nuire à l'efficacité de la RCP. Enfin, la problématique de l'équilibre entre la confiance dans les partenaires et celle dans les informations provenant des systèmes devra être aussi abordée de manière expérimentale.

Bibliographie

Bachmann, R. & Inkpen, A. C., 2011, « Understanding institutional-based trust building processes in inter-organizational relationships », *Organization Studies*, vol. 32, n° 2, pp. 281-301.

Baud, M., 2012, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, vol. 2, pp. 305-316.

Bollon F., Maille N., Marchand A.-L. & Blätter C., 2019, « Cyber-attaques : Organiser la confiance », pp. 243-250, *in* : *Actes du dixième colloque de Psychologie Ergonomique – EPIQUE 2019*, Lyon, ARPEGE.

Bollon F., Marchand A.-L., Maille N., Blätter C., Chaudron L. & Salotti J.-M., 2020, « Interpersonal trust to enhance cyber crisis management », pp. 161-174, *in* : de Waard D & all, *Proc. of the HFES Europe Chapter 2019 Annual Conf.*, Nantes.

Colquitt, J. A., Scott, B. A., & LePine, J. A., 2007, « Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance », *Journal of applied psychology*, vol. 92, n°4, pp. 909-927.

Crisp, C. B. & Jarvenpaa, S. L., 2013, « Swift trust in global virtual teams: Trusting beliefs and normative actions », *Journal of Personnel Psychology*, vol. 12, n° 1.

De Jong, B. A., Dirks, K. T. & Gillespie, N., 2016, « Trust and team performance: A meta-analysis of main effects, moderators, and covariates ». *Journal of Applied Psychology*, Vol. 101, n°8, pp. 1134-1150.

Delhey, J. & Welzel, C., 2012, « Generalizing trust: How outgroup-trust grows beyond ingroup-trust. »

De Neve, A. & Henrotin, J., 2006, « La Network-Centric Warfare: de son développement à Iraqi Freedom », pp 51-73, *Stratégique*, vol. 1.

Dirks, K. T., 1999, « The Effects of Interpersonal Trust on Work Group Performance », *Journal of Applied Psychology*, vol 84, pp. 445–455.

Farwell, J. P. & Rohozinski, R., 2011, « Stuxnet and the future of cyber war ». *Survival*, vol. 53, n°1, pp. 23-40.

Ferrin, D. L. & Dirks, K. T. (2003), « The use of rewards to increase and decrease trust: Mediating processes and differential effects ». *Organization science*, vol. 14, n°1.

Gonzales, D., Hollywood, J., Kingston, G., & Signori, D., 2005, « Network-centric operations case study: air-to-air combat with and without link 16 », Rand Corporation.

Godé, C., Hauch, V., Lasou, M. & Lebraty, J. F.,2012, « Une singularité dans l'aide à la décision: le cas de la Liaison 16 », *Syst. d'info. & management*, vol. 17, n°2, pp. 9-38.

Hyllengren, P., Larsson, G., Fors, M., Sjöberg, M., Eid, J. & Kjellevold Olsen, O., 2011, « Swift trust in leaders in temporary military groups », *Team Performance Management: An International Journal*, vol. 17, n° 7/8, pp. 354-368.

Jansen, W. & Soeters, J., 2017, « Dutch forward air controllers in Uruzgan », pp. 120-136, *in* : Glicken Turnley J. & all, *Special Operations Forces in the 21st Century: Perspectives from the Social Sciences*, Routledge.

Kramer, R. M., 1999, « Trust and distrust in organizations: Emerging perspectives, enduring questions », *Annual review of psychology*, vol. 50, n°1, pp. 569-598.

Karsenty, L., 2015, « Comment maintenir des relations de confiance et construire du sens face à une crise ? », *Le travail humain*, vol. 78, n°2, pp. 141-164.

Kurzban, R. & Leary, M. R., 2001, « Evolutionary origins of stigmatization: the functions of social exclusion », *Psychological bulletin*, vol. 127, n°2.

Levieux, F., 2005, « La défense et les technologies de l'information et de la communication », *Réalités Industrielles*, vol. 68.

Lewicki, R. J. & Bunker, B. B., 1995, « Trust in relationships », *Administrative Science Quarterly*, vol 5, n°1, pp. 583-601.

Lewis, J. D., & Weigert, A., 1985, « Trust as a social reality », *Social forces*, vol. 63, n°4, pp. 967-985.

Luhmann, N., 2006, « La confiance: un mécanisme de réduction de la complexité sociale », Economica.

Mayer, R. C., Davis, J. H., & Schoorman, F. D 1995, « An integrative model of organizational trust », *Academy of management review*, vol. 20, n°3, pp. 709-734.

McAllister, D. J., 1995, « Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations », *Academy of management journal*, vol. 38, n°1, pp.24-59.

Mckinney Jr, E. H., Barker, J. R., Davis, K. J., & Smith, D., 2005, « How swift starting action teams get off the ground », *Management Communication Quarterly*, vol. 19, n°2, pp. 198-237.

Meyerson, D., Weick, K. E. & Kramer, R. M., 1996, « Swift trust and temporary groups », pp. 166-195, *in* : Kramer, R.M. & Tyler, T.R., *Trust in organizations: Frontiers of theory and research*, Sage.

Shapiro, S. P., 1987, « The social control of impersonal trust », *American journal of Sociology*, vol 93, n°3, pp. 623-658.

Shapiro, D. L., Sheppard, B. H. & Cheraskin, L., 1992, « Business on a handshake », *Negotiation journal*, vol 8, n°4, pp. 365-377.

Scherer, K.R., 1986, « Voice, Stress and Emotion », pp. 157-179, *in* : H. Appley & all, *Dynamics of Stress: Physiological and Psychological Social Perspective*, Plenum.

Vilchenon, C., 2015, « Recognyzed Cyber Picture de l'armée de l'air (RCP Air) la RAP cyber des aviateurs », *Penser les ailes françaises*, n°32.