Cyber attaques : Organiser la confiance

Bollon Florent, Maille Nicolas, Anne Lise Marchand, Blättler Colin

Cyber attaques : Organiser la confiance

Bollon Florent
ONERA, BA 701, 13661, SALON cedex AIR
Florent.bollon@onera.fr

Maille Nicolas
ONERA, BA 701, 13661, SALON cedex AIR
Nicolas.maille@onera.fr

Marchand Anne-Lise
CReA, BA 701, 13661, SALON cedex AIR
Anne-lise.marchand@ecole-air.fr

Blättler Colin
CReA, BA 701, 13661, SALON cedex AIR
Colin.blattler@ecole-air.fr

Catégorie de soumission : communication longue

RÉSUMÉ

L'augmentation constante du nombre d'attaques par virus informatique a entrainé la nécessité pour l'Armée de l'Air Française, de développer un outil nommé « Recognized Cyber Picture » (RCP) permettant une visualisation globale de l'état cyber de ses systèmes interconnectés. Dans un tel système sociotechnique, bien que les enjeux techniques soient colossaux, les problématiques humaines, notamment en termes de transfert d'information entre les différents opérateurs, le sont tout autant. Cet article propose d'étudier une partie du volet social de la RCP et plus particulièrement le rôle de la confiance interpersonnelle, entre deux opérateurs humains qui ne se connaissent pas, dans la réalisation d'une tâche collaborative médiée par ordinateur.

MOTS-CLÉS
Confiance interpersonnelle, cyber-sécurité, travail collaboratif, supervision

1. PROBLEMATIQUE ET HYPOTHESE

La montée des opérations militaires inter-nations ou inter-armées et la complexification des théâtres d'opération changent profondément la collaboration des forces en présence. Des interactions fortes, pour des opérations ponctuelles, avec des troupes alliées que l'on rencontre pour la première fois ne sont pas rares. Afin de favoriser leur succès les armées mettent en place des processus de standardisation et développent leur résilience (Amalberti, 2013). L'usage des nouveaux modes de communication utilisant des réseaux informatisés se généralise et permet des gains importants en efficacité et en rapidité des échanges d'information. Jusqu'au début des années 2000 ces transferts d'informations réseaux centrés paraissaient être sécurisés. Toutefois, avec l'explosion du nombre de systèmes interconnectés, des nouvelles menaces provenant du cyberespace apparaissent et touchent, dans un premier temps, des réseaux civils, comme en Estonie en 2007 ou encore en Géorgie en 2008 (Farwell et Rohozinski, 2011). Rapidement, la menace cyber s'étend aux

infrastructures des armées comme aux Etats-Unis, en Angleterre et en France en 2009 (Baud, 2012) et des sites et des réseaux protégés comme en Iran en 2010 (Farwell et Rohozinski., 2011). Ces premières cyber-attaques ont entrainé une remise en cause de la confiance qu'ont les opérateurs dans leurs systèmes informatisés et ont amené les Etats à mieux définir leurs besoins et leurs stratégies de gestion de la cyber-sécurité.

Il est en particulier reconnu qu'il est nécessaire d'avoir une représentation partagée, au sein de la chaine de commandement, de l'état cyber du réseau, qu'il soit passé, présent ou futur (Vilchenon, 2015). Ceci implique de pouvoir, sur la base de l'activité observée, identifier les systèmes et les informations qui pourraient être corrompus ou dans des états dégradés, afin d'anticiper au mieux l'impact des anomalies observées sur l'état futur du réseau de communication. Actuellement, aucune visualisation globale ne permet de rassembler et représenter les failles détectées, puis d'identifier et d'analyser les effets de bord intra et inter systèmes. Dans les années à venir l'Armée de l'Air Françaises devra donc se doter d'un outil permettant de superviser et cartographier les liens entre les différents systèmes d'information et d'agir en anticipation en préparant les systèmes à affronter les agressions. C'est sur la base de cette représentation que les décisions pourront être prises et coordonnées. Pour l'Armée de l'Air Française, l'outil permettant cette représentation se nomme la « Recognized Cyber Picture » (RCP) et sera alimentée tant par des analyses automatiques des activités sur les différents réseaux que par des opérateurs identifiant des anomalies. L'outil n'est pas encore déployé mais il est fort probable qu'un tel dispositif, complexe et nouveau, impactera les activités des différentes équipes en charge de la gestion de la cyber-sécurité, que ce soit dans leur fonctionnement ou dans leur organisation.

Le principe des attaques cyber pouvant être de falsifier de supprimer voire d'insérer des données ou encore de rendre des services indisponibles pour bloquer les échanges, la confiance dans les données observées semble être un des fondements de cette RCP. Cependant, comme dans tout nouveau système sociotechnique complexe le fonctionnement social du transfert d'information devra être pris en compte. En effet, telle qu'envisagée aujourd'hui, la RCP sera alimentée par des sources humaines et logicielles (intelligence artificielle) et gérée par plusieurs personnes, ayant des informations différentes sur leurs écrans et devant prendre des décisions conjointes. Ainsi la qualité du transfert d'information entre ces différents opérateurs pourrait être un point clef de l'efficience de la RCP.

Les retours d'expérience de militaires partis en opérations extérieures montrent déjà que dans les situations critiques, le transfert d'information et, plus particulièrement, la question de la confiance interpersonnelle (CI) entre différents partenaires est un des éléments clé pour la performance et la réussite de l'équipe. Dans le cas de la gestion de la sécurité cyber où les informations numériques risquent d'être corrompues, nous faisons l'hypothèse que les relations directes entre les opérateurs seront utilisées dans la RCP pour fiabiliser l'appréciation que l'on se fait de l'état cyber du réseau, et que, par conséquent, la CI aura un rôle prépondérant. Ceci rejoint des résultats de la littérature qui indiquent déjà que la CI joue un rôle essentiel dans les activités collaboratives (De Jong et Dirks, Gillespie, 2016), plus particulièrement comme étant un modulateur de la performance d'une équipe (Dirks, 1999). Ainsi, les résultats d'études, pour la plupart qualitatives, montrent qu'une CI faible au sein d'une équipe entraine une diminution de la performance (De Jong et al, 2016). Il apparaît que ce lien entre CI et performance n'est pas direct mais peut être médié par d'autres facteurs tels que la supervision (De Jong et Elfring, 2010) de telle sorte qu'une augmentation du niveau de CI entraine une diminution du temps de supervision. Cependant, ce lien entre confiance et supervision n'a actuellement été étudié qu'entre opérateur humain et système technique (Parasuraman, Molloy et Sing, 1992) et non entre deux opérateurs humains. Ainsi, il parait possible que selon la catégorie sociale des différents opérateurs le lien entre confiance et supervision ne soit pas constant.

Dans cet article nous proposons d'étudier expérimentalement le lien entre CI et supervision dans le cadre d'une activité collaborative entre opérateurs humains socialement différents. Plus particulièrement, nous faisons l'hypothèse que les opérateurs augmentent leur temps de supervision lorsqu'ils ont moins confiance en leur partenaire mais que cette stratégie est dépendante du groupe social auxquels ils appartiennent.

2. MILIEU D'IMPLANTATION ET METHODE

Une analyse du besoin de la RCP réalisée dans le cadre de cette campagne d'étude met en évidence une possible utilisation de l'outil par les personnels navigants (pilote et navigateur officier système d'arme) (PN) et les contrôleurs aériens (CA). Il apparaît aussi que pour la gestion d'une crise cyber le processus de collaboration doit se faire rapidement et entre des personnels qui ne se connaissent pas. Afin que notre étude puisse répondre aux problématiques de la RCP nous avons donc choisi d'effectuer nos travaux avec des personnels militaires représentatifs des potentiels utilisateurs finaux visés et de créer un micro monde permettant de réaliser des expérimentations contrôlées sur des tâches simples mais représentatives des activités d'équipes où les interlocuteurs ne se connaissent pas.

2.1 Participants

Un ensemble de 40 personnes composé de 20 PN (0% de femmes et 100% d'hommes) d'âge moyen 33.05 ans (SD : 5.14 ans) et de 20 CA (20% de femmes et 80% d'hommes) d'âge moyen 34.15 ans (SD : 8.53 ans) a participé à cette étude. Tous les participants sont des opérationnels de l'armée de l'air ayant un niveau d'expertise équivalent et ayant tous effectué des missions inter alliées.

2.2 Matériel et méthode

2.2.1 Introduction

La tâche à réaliser est une tâche de comptage collaborative sur ordinateur qui consiste à repérer et dénombrer les aéronefs présents sur deux images différentes. Le travail est réalisé par une équipe de deux personnes composée du participant et d'un partenaire fictif, c'est à dire dont le comportement est en fait simulé par ordinateur et donc entièrement contrôlé pour l'expérimentation. Dans cette tâche le rôle du participant est de donner le nombre d'aéronefs présents sur son image puis de valider le nombre d'aéronefs présents sur l'ensemble des deux images. Chaque membre de l'équipe est en charge du comptage des aéronefs présents sur une image différente. Cependant, le participant, qui est également le chef d'équipe, peut à tout moment visualiser l'image traitée par son partenaire et éventuellement ajuster le résultat donné par ce partenaire.

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

Méthode d'induction de la confiance dans le partenaire

L'objet de l'expérimentation étant d'étudier l'impact de la confiance sur l'activité de supervision du chef d'équipe, un mécanisme permettant d'induire un niveau de confiance plus ou moins haut dans son partenaire est utilisé. Ce processus, construit sur les méthodologies des Représentations Sociales (notamment Abric, 2003) mobilise l'utilisation de paires de mots décrivant le partenaire. Ces paires de mots ont été identifiées dans une étude préliminaire menée auprès de 373 aviateurs ayant travaillé en opération interalliée. Dans cette pré-étude il était demandé aux participants de produire 5 expressions ou mots qui leur faisaient penser à une personne digne de confiance en opération interalliée. Parmi tous les mots recueillis 49 ont été cités plus de 3 fois, parmi ces 49, 18 ont été caractérisés comme étant les plus susceptibles d'induire de la confiance pour des opérationnels de l'Armée de l'Air. Ces 18 éléments ont ensuite été associés en paires afin de créer :

- 30 paires de mots censés induire un niveau de confiance élevé dans le partenaire (e.g. « Opérationnel » et « Loyal », « Fidèle » et « Honnête »…) ;
- 30 paires de mots censés induire un niveau de confiance intermédiaire (e.g. « Hypocrite » et « Professionnel », « Méprisant » et « Fiable »…). Ces paires de mots étaient constitués d'un mot devant induire un niveau de confiance élevé et d'un antonyme d'un des autres mots induisant de la confiance ;
- 30 paires de mots censés induire un niveau de confiance faible (e.g. « Méprisant » et « Hypocrite », « Négligent » et « Désinvolte »…). Ces paires de mots étaient constituées des antonymes des mots associés à un niveau de confiance élevé.

Enfin, ces 90 paires de mots ont été testées auprès de 32 aviateurs et les 42 paires de mots les plus représentatives (14 paires représentatives d'un niveau de CI élevé, 14 paires représentatives d'un niveau de CI médian et 14 paires représentatives d'un niveau de CI faible) ont été utilisées afin d'induire les différents niveaux de CI dans l'expérimentation.

2.2.2 *Protocole expérimental*

L'expérimentation est découpée en 42 essais comprenant chacun trois phases successives (*cf.* figure 1). Pour la mise en œuvre expérimentale, le participant a toujours le rôle de chef d'équipe. Le partenaire étant fictif, la tâche de comptage du partenaire est automatisée. Les résultats transmis par le partenaire peuvent être modifiés par le participant mais le partenaire ne modifie, ni ne peut modifier, dans aucun cas, les résultats transmis par le participant.

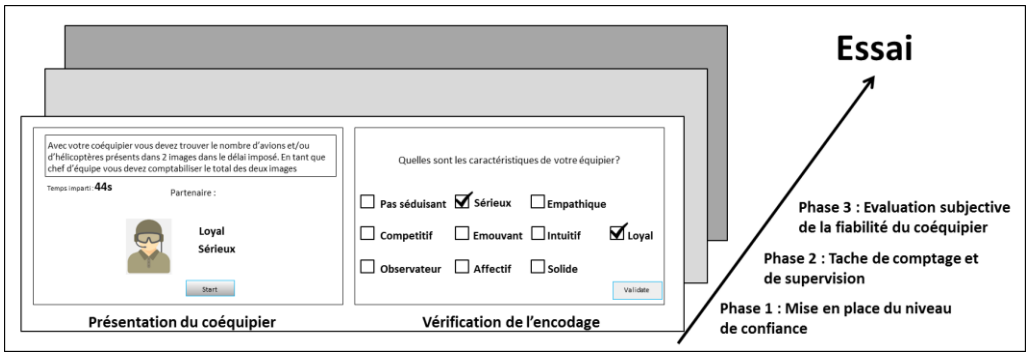

Figure 1 :L'expérimentation se compose de 42 essais différents de 3 phases chacun. Chaque essai est effectué avec un partenaire différent représenté par une paire de mots en phase 1. Les paires de mots correspondent à celles obtenues dans la pré expérimentation.

La première phase comprend deux affichages distincts et correspond à la mise en place du niveau de confiance. Sur un premier affichage la paire de mot caractérisant le partenaire est présentée au participant. Dans un tiers des cas ces paires de mots induisent un haut niveau de confiance interpersonnelle dans le partenaire, dans un tiers des cas les paires de mots induisent une confiance intermédiaire et dans le tiers restant les paires de mots induisent une confiance faible. Afin de s'assurer que le participant ait encodé les caractéristiques du partenaire, il lui est demandé, sur le second affichage de retrouver la paire de mot parmi 8 distracteurs. Une fois cela fait la deuxième phase commence.

La deuxième phase comprend trois affichages différents et correspond à la phase de comptage collaboratif et de supervision (cf. figure 2). Au début de la deuxième phase le participant se trouve devant un affichage de contrôle (cf. figure 2 « A ») sur lequel lui est présenté le score total (somme des aéronefs comptés par le participant et par le partenaire) et deux boutons. Le premier bouton permet au participant d'afficher une interface présentant son image (cf. figure 2 « B ») et ainsi effectuer sa tâche de comptage. Lorsque le participant valide le compte des aéronefs présents sur son image l'affichage de contrôle réapparait automatiquement (cf. figure 2 « A »). Le participant peut

alors soit valider le score total correspondant au dénombrement des aéronefs dans les deux images et passer à la troisième phase, soit cliquer sur le bouton lui permettant d'afficher de nouveau son image (cf. figure 2 « B »), soit cliquer sur le deuxième bouton lui permettant d'afficher l'image du partenaire (cf. figure 2 « C ») et ainsi superviser. Sur l'affichage de supervision l'image sur laquelle le partenaire a effectué le comptage ainsi que le score transmit par le partenaire sont présentés. Lorsque le participant estime que la somme des aéronefs présents sur les deux images est la bonne, il peut terminer la phase 2 et passer à la phase 3. Cependant, si le participant ne valide pas la somme des aéronefs présents sur les deux images dans le temps imparti (temps calibré en phase de test pour permettre de compter convenablement les aéronefs présents sur les deux images) le test est considéré comme étant échoué et une nouvelle paire d'image est tirée à la fin de l'expérimentation, avec un partenaire de même niveau de confiance.

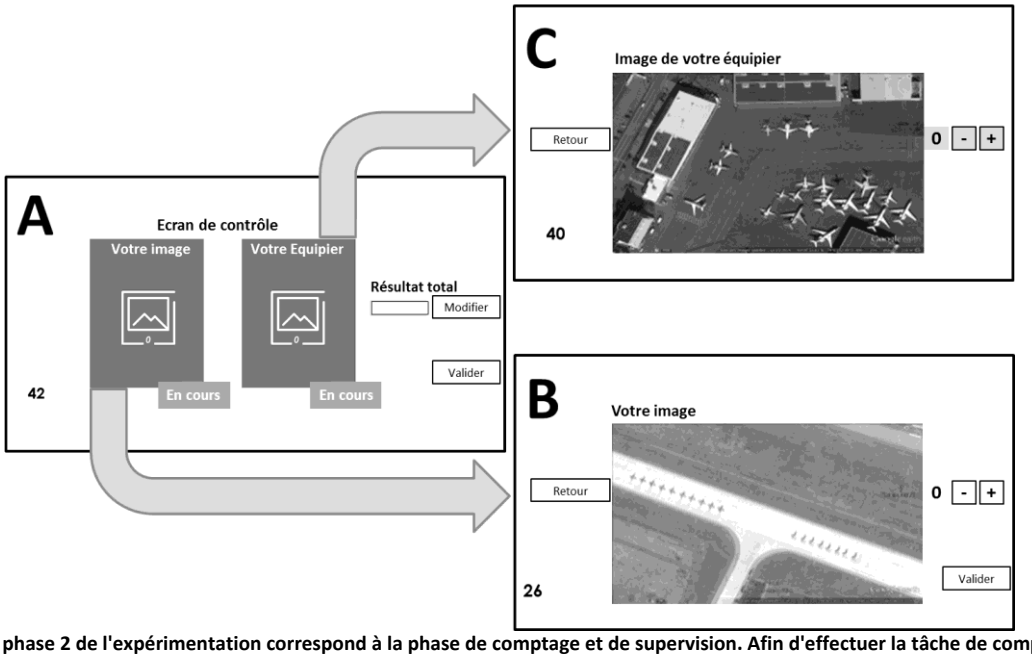

Figure 2 : La phase 2 de l'expérimentation correspond à la phase de comptage et de supervision. Afin d'effectuer la tâche de comptage le participant initialement en « A » doit afficher l'interface « B ». S'il souhaite superviser le partenaire, le participant doit afficher l'interface « C ».

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

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

Enfin, lorsque le participant renseigne les différentes échelles de la phase 3, il finit la tâche liée à cette image et doit réaliser une nouvelle série de 3 phases, avec une nouvelle paire de mot inductrice de niveau de confiance. Chaque participant réalise ainsi 42 fois la tâche avec des partenaires fictifs toujours différents caractérisés par différentes paires de mots. L'hypothèse principale est que l'augmentation du niveau de confiance doit s'accompagner d'une réduction du temps de supervision du partenaire mais que cet effet est dépendant de la population; la variable principalement étudiée est donc le pourcentage de temps de supervision du partenaire sur le temps total passé sur la tâche, en fonction du niveau de confiance induit.

3. RESULTATS

Les données des 40 participants sont inclues dans l'analyse. Tout d'abord, l'étude du niveau de confiance dans le résultat du partenaire confirme, en accord avec la littérature, que les différentes paires de mots induisent bien des niveaux de confiance significativement différents. Ce résultat est cohérent avec ceux obtenus en phase de pré-test (*cf.* point 2.2.2).

Bien que la variable dépendante étudiée dans cet article soit le pourcentage de temps passé par le participant à effectuer la tâche de supervision du partenaire (en %), deux autres variables dépendantes ont été recueillies : le pourcentage de réussite à la tâche personnelle, et le pourcentage de délégation (pourcentage de fois où le participant n'a pas cliqué sur le bouton d'affichage de l'image du partenaire et n'a donc pas pu vérifier les données transmises par le partenaire). Afin d'améliorer la compréhension des résultats les moyennes et écarts types de ces différentes variables sont présentées dans le tableau 1. Aucun test statistique n'est cependant présenté sur ces différentes variables mais une analyse des moyennes présentées dans le tableau 1 donne quelques indications quant à la différence entre les populations.

Nous pouvons remarquer que pour les deux catégories de participants (PN ou CA), le pourcentage de réussite personnelle ne semble pas être modulé par le niveau de confiance. Cependant, bien que le pourcentage de réussite soit relativement élevé dans tous les cas (supérieur à 75%) il semble être, en moyenne, supérieur chez les PN. Sur le pourcentage de délégations, les données indiquent une possible influence du niveau de confiance mais également de la catégorie. En effet, les CA semblent beaucoup plus déléguer lorsque le niveau de confiance est élevé (*M* = 23.3%) que lorsque le niveau de confiance est faible (*M* = 4.3%) alors que pour les PN cet effet de la confiance sur la délégation semble beaucoup plus faible.

Tableau 1 : Moyenne et écart type sur le pourcentage de réussite personnel et le pourcentage de délégation pour la catégorie Contrôleur Aérien (CA) et Personnel Navigant (PN) en fonction des niveaux de confiance

Variables dépendantes	**Catégorie**	**Moyenne (M) et écart type (SD) pour chaque variable dépendante et chaque niveau de confiance**		
		Faible	Moyen	Elevé
Réussite à la tache personnelle (%)	CA	M = 77.5 SD = 8.7	M = 72.8 SD = 14.5	M = 76.7 SD = 11.0
	PN	M = 81.4 SD = 9.6	M = 86.4 SD = 8.9	M = 78.2 SD = 12.3
Pourcentage de supervision (%)	CA	M = 4.3 SD = 8.4	M = 7.9 SD = 15.8	M = 23.3 SD = 32.4
	PN	M = 4.3 SD = 14.5	M = 5.8 SD = 15.6	M = 7.5 SD = 14.3

La variable dépendante étudiée est le pourcentage de temps passé par le participant à effectuer la tâche de supervision du partenaire (en %). Le décompte de ce temps démarre à partir du moment où le participant affiche la photographie du partenaire et est stoppé lorsque le participant quitte la visualisation de cette photographie pour retourner sur sa propre tâche. Ce temps est ensuite rapporté au temps total passé sur la tâche (temps sur sa propre tâche + temps passé sur l'écran de contrôle + temps passé sur l'écran du partenaire). Pour chaque participant la variable dépendante est moyennée sur l'ensemble de ses essais, en fonction du niveau de confiance (*cf.* tableau 2). Une ANOVA ainsi que des pairwise-t-test sont ensuite réalisés.

Tableau 2 : Moyenne et écart type sur le pourcentage de temps de supervision pour la catégorie Contrôleur Aérien (CA) et Personnel Navigant (PN) en fonction des niveaux de confiance

Variables dépendantes	Catégorie	Moyenne (M) et écart type (SD) pour le pourcentage de temps de supervision		
		Faible	Moyen	Elevé
Pourcentage de temps de supervision (%)	CA	M = 31.2 SD = 5.7	M = 30.3 SD = 6.7	M = 24.0 SD = 11.1
	PN	M = 34.4 SD = 3.4	M = 32.9 SD = 7.9	M = 31.1 SD = 6.7

En accord avec l'hypothèse les résultats de l'ANOVA montrent un effet significatif du niveau de confiance ($F(2,76) = 10.48$, $P < .001$) ce qui indique que le niveau de confiance influe sur le temps passé à superviser. Cependant, bien que les résultats de l'ANOVA indiquent également une différence significative entre les PN et les CA (montrant qu'en moyenne les PN ont un pourcentage de supervision supérieur aux CA) ($F(1,38) = 5.41$, $P = .02$) aucun n'effet d'interaction n'est présent ($F(2,76) = 2.04$, $P = .13$). Cette absence d'interaction tend à montrer que les PN et les CA sont influencés de manière similaire par le niveau de confiance. En d'autres termes, ces résultats nous indiquent que les PN passent en moyenne plus de temps à superviser leur partenaire mais que, pour les CA comme pour les PN cette supervision est dépendante du niveau de CI (lorsque le niveau de CI diminue le pourcentage de temps de supervision augmente).

4. DISCUSSION

En premier lieu, les résultats de cette expérimentation montrent que le niveau initial de CI entre deux opérateurs est impacté par la représentation que le participant a de son partenaire, alors même qu'il n'a aucune expérience de travail avec lui. D'un point de vue applicatif, ce résultat doit être à la base d'une réflexion sur les opérationnels qui seront impliquées dans la gestion d'une crise cyber, sur les informations relatives à leur partenaires qu'il serait ou pas opportun de leur transmettre, ainsi que sur la manière de les leur communiquer.

Ensuite, nous observons que ce niveau de confiance a un impact direct sur la stratégie de supervision du partenaire ; lorsque le niveau de confiance diminue le temps de supervision augmente. Ceci confirme bien que dans ces tâches courtes de coopérations, où le temps est un facteur déterminant pour limiter les conséquences d'une attaque, il est nécessaire que les opérateurs aient un niveau de confiance adéquat entre eux pour mettre en place la stratégie la plus efficace.

Enfin, l'expérimentation montre que l'influence du niveau de confiance sur la stratégie de supervision semble être dépendante du type de population étudiée. Bien que les PN et les CA puissent être considérés comme des populations proches, avec une formation militaire, des règles et des normes similaires, les résultats indiquent que le niveau de confiance ne module pas avec la même force la stratégie de supervision mise en place. Ainsi, chez les CA la variation de confiance dans le partenaire s'accompagne d'une plus grande variation de la stratégie de supervision que chez les PN qui ont un comportement plus rigide. Au sein de l'armée de l'air, le choix de la formation des opérateurs mis en poste pourrait donc être un facteur important pour favoriser ce travail collaboratif et la performance globale de l'équipe. Les résultats obtenus dans cette étude doivent cependant être nuancés. En effet, dans cette expérimentation le participant est considéré comme chef d'équipe et a, par conséquent, la responsabilité de décision sur le résultat de l'équipe. Cette responsabilité de décision fait partie intégrante du travail des officiers (tous les PN de cette expérimentation sont officiers) mais est moins présente chez les sous-officiers (tous les CA de cette expérimentation sont sous-officiers). Ainsi, il sera nécessaire de compléter ces résultats par une étude menée entre deux

populations de sous-officiers ou entre deux populations d'officiers afin de quantifier l'impact du grade sur ce comportement et affiner les critères pour la formation des futurs opérateurs.

Les résultats présentés ici font partie d'un ensemble plus large d'expérimentations sur la CI qui soutiennent les réflexions autour de la mise en place d'un système sociotechnique pour la gestion de la cyber sécurité. L'accent est mis ici sur l'importance des relations entre les personnes qui vont être amenées à travailler sur des données potentiellement corrompues, de par l'attaque qu'ils doivent détecter et gérer. Cette première étude identifie des facteurs tels que le groupe social des individus qui pourront être utilisés pour favoriser le travail coopératif. Dans cette expérimentation l'accent est mis sur le processus collaboratif dans la gestion d'une crise cyber. Cependant, ces résultats pourraient également être employés dans les entreprises afin de prévenir et de comprendre par exemple des problèmes relationnels pouvant survenir dans les relations avec des sous-traitants ou, plus largement, entre membres d'une même équipe projet.

BIBLIOGRAPHIE

Abric, J. C. (2003). 8. L'étude expérimentale des représentations sociales. In *Les représentations sociales* (Vol. 7, pp. 203-223). Presses universitaires de France.

Amalberti, R. (2013). *Piloter la sécurité: théories et pratiques sur les compromis et les arbitrages nécessaires*. Springer Science & Business Media.

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

De Jong, B. A., Dirks, K. T., & Gillespie, N. (2016). Trust and team performance: A meta-analysis of main effects, moderators, and covariates. *Journal of Applied Psychology*, *101*(8), 1134.

De Jong, B. A., & Elfring, T. (2010). How does trust affect the performance of ongoing teams? The mediating role of reflexivity, monitoring, and effort. *Academy of Management Journal*, *53*(3), 535-549.

Dirks, K. T. (1999). The effects of interpersonal trust on work group performance. *Journal of applied psychology*, *84*(3), 445.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40.

Parasuraman, R., Molloy, R., & Singh, I. L. (1993). Performance consequences of automation-induced 'complacency'. *The International Journal of Aviation Psychology*, *3*(1), 1-23.

Vilchenon, C. (2015), Recognyzed Cyber Picture de l'armée de l'air (RCP Air) la RAP cyber des aviateurs. « Réflexions sur le cyber : quels enjeux ? », Penser les ailes françaises, n°32, juillet 2015

Remerciements : Nous tenons à remercier la Chaire Cyber-résilience aérospatiale qui a aidée au financement d'une partie de ces travaux de recherche ainsi que tous les participants de l'Armée de l'Air.