Utiliser les potentialités du cyber pour des opérations psychologiques ciblées en temps de paix?

Christine Dugoin-Clément*, GREGOR (EA2474) - IAE de Paris, Chercheuse associée au Centre de recherche des écoles de Saint-Cyr Coëtquidan

Introduction

En novembre 2014, Viktor Ianoukovitch renonçait à un accord avec l'Union Européenne à une semaine de sa signature. Ce moment était pourtant préparé de longue date 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 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[1]. 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 devient 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'autre villes connurent aussi « leur » Maïdan et la tension monta jusqu'à un paroxysme atteint en février. A cette date, 80 personnes trouvèrent la mort à Kiev, notamment suite à des tirs de snipers. Le 22 février Viktor Ianoukovitch quittait Kiev et dans la foulée, un gouvernement provisoire s'installait 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

* Christine Dugoin-Clément est doctorante à l'IAE de Paris (GREGOR). Elle est également chercheuse associée au Centre de Recherche des Ecoles de Saint-Cyr Coëtquidan, pôle « Mutation des conflits ».

[1] Les Berkuts (signifiant aigles) sont des unités spéciales servant notamment de police anti-émeute au sein de la militsia ukrainienne. Créées en 1992 les unités de Berkuts sont composées d'environ 30 000 hommes.

d'Ukraine), seront aussi accompagnées d'Odessa située au sud-ouest de l'Ukraine, et par d'autres protestations en Crimée. Ces mouvements d'opposition naquirent de 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 également. 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, refusait de reconnaitre 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, suivi par la proclamation de la « République populaire de Lougansk » le 11 mai.

Les séparatistes ne reconnaissant pas le gouvernement provisoire et étant acteurs de l'insurrection, ils furent rapidement qualifiés de « terroristes » par Kiev, qui devint aux yeux des dits terroristes un gouvernement de « fascistes » et de « nazis ». A partir du 2 mai 2014, l'armée ukrainienne intervient 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 (septembre 2014) et de Minsk 2 (février 2015) qui avaient pour objet de faire revenir la paix sur le territoire - fut accompagné d'une vaste opération de cyber attaques visant les systèmes mais aussi la population au travers de vastes opérations informationnelles.

Contexte cyber en Ukraine

Afin de comprendre comment le développement d'une vague massive d'opération 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 dix premiers pays connectés à Internet d'Europe, en affichant une pénétration du réseau de 33,9% suit quelques 15,3 millions d'utilisateurs, et ce chiffre 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[2]. Concernant les connections aux réseaux sociaux, on estime que Facebook avait trois millions d'utilisateurs en Ukraine en 2013[3].

[2] Internet Association of Ukraine

[3] Olga Minchenko « Вже 3 мільйони українців користуються Facebook », *Watcher*, 20 octobre 2013 watcher.com.ua". watcher.com.ua, 25 octobre 2013, consulté le 3 août 2014.

Concernant Twitter qui fut très actif depuis le Maïdan, Google Analytics estime qu'en 2012 le nombre de visiteurs atteignait 120 000, même si GfK Ukraine[4], 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)[5]: 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 aura une influence évidente dans les opérations à visée offensive menées par la Russie 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 qui permit l'essor 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 seront des facteurs poussant la Russie à développer ses propres compétences cyber, coupées et isolées des puissances occidentales. Par ailleurs, l'interconnexion forte des infrastructures, notamment de télécommunications, entre la Russie et les anciennes Républiques de l'URSS seront autant de facilitateurs de l'unité et du développement du RuNet. Enfin, l'explosion des marchés pétroliers fournira 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 par le biais 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 laissa une longueur d'avance aux russes, même si la création en 2005 de la dorsale Trans-Europe-Asie (TEA) ouvrira 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 nous faut nous intéresser à la directive cadre de 2000 produite en Russie intitulée « Doctrine de sécurité informationnelle de la Fédération de Russie »[6]. Dans ce texte fondateur et précurseur, les notions de « guerre informationnelle » sont abordées et décrites comme une « confrontation entre deux ou plusieurs Etats dans l'espace de l'information visant à endommager les systèmes

[4] Société d'étude de marché
[5] Alexa « Top Sites in Ukraine », https://www.alexa.com/topsites/countries/UA
[6] http ://www.scrf.gov.ru/documents/5.html

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'Etat, ainsi qu'une influence forçant l'Etat visé à prendre des mesures dans l'intérêt du parti adverse ». Cette définition donne une importance primordiale aux actions portées vers les populations, et donc aux opérations psychologiques de grande échelle. 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 »[7] 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.

Le cyber dans les conflits modernes: le cas ukrainien

Concernant le volet des attaques cyber dans le conflit ukrainien, il apparait 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 »[8] en Crimée, le 28 février 2014, et après la maîtrise des aéroports de Simféropol et Sébastopol, fut de prendre le contrôle des structures télécoms. Cette motivation prit corps au travers de coupure des câbles à fibre optique reliant la Crimée à l'Ukraine. En mars, soit à peine un mois après l'annexion, Rostelecom[9] 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.

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

[8] 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.

[9] Entreprise russe de télécoms

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. Ce dispatch des données a notamment été rendu 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 mise au service d'opérations informationnelles servant des objectifs géopolitiques.

D'un point de vue de menace 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 si le Président Porochenko accusait la Russie d'être à l'origine de ces offensives[10], 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 terme de désorganisation et de limiter le risque de contagion pour son créateur. A la différence des malwares et autres logiciels malveillants, qui, par l'interconnexion du réseau, pourrait revenir en boomerang vers leur pays d'origine de leur créateur, elles se cantonnent aux seuls sites visés. Cependant, le risque de contagion n'empêcha pas l'Ukraine d'être touchée par NotPetya qui impacta environ 20% des structures administratives de l'Etat. Les attaques menées sur les centrales électriques en 2015 et 2016 restent également mémorables, la seconde plongeant Kiev dans le noir pendant plus d'une heure[11]. Dans le cas précis de cette attaque, les soupçons se portent sur un groupe de hackers d'origine russe, Sandworm. Pour nombre d'experts en cyber sécurité, cette attaque pourrait tout à fait avoir été un test en prévision d'opérations de plus grande ampleur.

Au niveau informationnel, de nombreux « leaks » ou fuites, hacks de mails et vols d'informations stratégiques furent réalisés, comme par exemple le hack des communications 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 apparus dans le paysage du conflit ukrainien en avril 2014. Si ce groupe se dit autonome, il est fortement soupçonné d'être directement lié au Kremlin.

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

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

Concernant les opérations visant la population qu'elle soit ukrainienne ou occidentale, de nombreux « bots » et « trolls » ont été démasqués alors qu'ils agissaient sur plusieurs réseaux sociaux et plateformes. A titre d'exemple, une étude de réseaux menée par Alexander Laurence[12] sur Twitter présentait une analyse se basant sur des réseaux de comptes utilisant des phrases clés 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 étaient des bots : 93% ne montraient aucun emplacement sur leur profil, 96% n'avaient pas d'informations sur le fuseau horaire et 97% n'avaient aucun favori Twitter enregistré.

Outre les actions menées via Twitter qui visaient probablement tout autant les populations occidentales qu'ukrainiennes, de vastes opérations de trolling furent mises au jour qui s'attaquaient 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. A 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 leur poste, des opérations 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 en termes d'impact psychologique.

Point important, si certains messages étaient clairement et immédiatement décelables comme anti-gouvernementaux ou visant à saper le moral ou à désinformer leurs destinataires, d'autres étaient plus subtils. Ils commençaient par défendre des valeurs communément partagées par les soldats et les combattants avant de fournir des éléments liant des personnalités du gouvernement ou de la hiérarchie militaire à des comportements ou prises de décisions allant à l'encontre des valeurs prônées précédemment et partagées par une large majorité des militaires.

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

Pour analyser ces opérations et leurs effets sur les personnes visées, nous avons mené une série d'observations 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 termes de genre puisque principalement masculin (une seule femme). Les sujets avaient des profils socio-professionnels 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 civile paya un lourd tribut[13]. L'ensemble des trente entretiens est divisé en deux sections de quinze individus chacune, une composée de soldats actifs, l'autre de vétérans tous blessés à des degrés divers et des moments divers (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 se 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 permettant un cadrage des 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 suite à des informations prises sur Internet. Dans un second temps, la perception et la confiance accordée aux différents médias et canaux d'information étaient remises en question. Ensuite, il leur était demandé s'ils pensaient pouvoir être la cible d'attaques cyber informationnelles en tant que militaire et pas seulement en tant qu'Ukrainiens, et, finalement si leur vision et leur confiance dans les structures institutionnelles avaient changée.

Le choix était fait 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 motivation poussant à se concentrer sur cette population était basée sur le constat que ce sont ces hommes qui agissent quotidiennement sur le front lors des combats et qu'à ce titre ils sont en eux-mêmes des éléments stratégiques ne se percevant pas toujours comme tels. Selon les résultats de ces entretiens, la chute de la confiance dans les médias officiels est proportionnelle à la confiance accordée aux réseaux sociaux et aux médias alternatifs.

[13] Sébastien Gobert, « Nouvelle escalade de violence sur le front ukrainien », *Libération*, 1er 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

L'une des raisons principalement évoquée 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-séparatistes. La confiance portée aux personnes supposées partager le mode de vie des Ukrainiens ordinaires est encore renforcée si la personne délivrant l'information, ou la partageant, 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 direct 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 anti-gouvernementale. D'autres encore disent ne pas avoir changé pour leurs « frères d'armes » mais 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 tentés par un glissement vers la criminalité, tout en citant certaines de leurs connaissances ayant déjà pris ce virage répréhensible.

En terme d'interaction entre l'évolution de leur comportement et la consommation internet, il semble que les hommes les plus touchés, ceux exprimant la plus grande évolution dans leur comportements soit les consommateurs de trois à quatre heures d'Internet par jour, particulièrement la tranche des trois heures quotidiennes. Les consommations inférieures à deux heures semblent ne guère être touchées, ce qui parait logique car ces hommes déclarent utiliser internet principalement pour consulter leur mails ou communiquer avec leurs familles (notamment via Skype) et non pour « s'informer ». De même, les consommations supérieures ne semblent pas être plus affectées que le pic des trois heures. Cependant, ce constat mérite une recherche plus poussée notamment quant aux conditions de la consommation (privée, publique etc…). Concernant la tranche d'âge, les membres de la « génération Y »[14] sont le plus sensibles et il semble que les grades de sergent et caporal soit plus touchés que les lieutenants.

Enfin sur tous les soldats interrogés, aucun ne se percevait comme pouvant être une cible en tant que militaire. A cela plusieurs raisons étaient évoquées de manière récurrente : tout d'abord ils ne se perçoivent pas comme ayant un intérêt stratégique assez important pour pouvoir en faire des cibles, ensuite, ils pensent ne pas pouvoir être dupés car « ils connaissent trop bien les séparatistes et leurs mensonges ».

[14] 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

Ce point est particulièrement intéressant quand on le met en relation avec leur baisse de confiance dans les médias officiels unanimement reconnus, ce qui laisse entendre qu'ils ont bien été impactés. Enfin, interrogés pour savoir s'ils avaient changé de point de vue quant aux structures étatiques en s'informant, la réponse était unanimement positive chez les caporaux et sergents consommant trois à quatre heures d'internet, alors même qu'ils annonçaient ne pas être dupes de stratégies informationnelles et ne pas être des cibles.

Potentialités du cyber

Le cyber est aujourd'hui un acteur incontournable dans les conflits modernes pour plusieurs raisons. Tout d'abord, par l'interconnexion du réseau, il permet d'abolir les frontières physiques et géographiques connues jusqu'alors, et cette négation des distances géographique a une conséquence pragmatique immédiate en limitant le coût d'action menées loin du territoire donneur d'ordre. La plasticité du cyber, sa volatilité, permet une adaptation extrêmement rapide aux contextes et à leurs variations, ce qui autorise une modification de la perception d'un élément jusqu'alors limitant : le temps. Cette contraction temporelle reste cependant liée à la capacité de calcul mise à disposition : en effet, un grand nombre de données aura besoin de mobiliser une grande puissance de calcul pour pouvoir être analysée et traitée correctement. Ce besoin pouvant aller jusqu'à nécessiter l'utilisation de supers calculateurs, notamment s'il faut avoir 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 multi-vectorialité 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 via le cyber particulièrement difficiles à détecter : bien organisées et pensées par une même tête, elles peuvent utiliser différents axes qui ne prennent leur sens qu'une fois vues dans leur globalité. Or cette vision globale, cette « big picture » peut devenir quasi impossible une fois les canaux d'influences noyés dans le bruit du réseau, au cas particulier dans la masse de données et de sites consultés par la personne visée.

Autre point d'intérêt, Internet est une source d'informations permettant 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 un profil de la personne observée.

Dans le cas ukrainien, que les données de ses citoyens qui utilisent Yandex, VKontakte et Mail.ru partent directement sur des serveurs moscovites est un problème majeur pour le gouvernement car cela représente une source d'information très importante pour les renseignements russes sans même qu'il y ait la nécessité de mettre en place 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 délicat de pouvoir amener des éléments de preuves indiscutables permettant une mise en cause pénale de ce gouvernement.

L'utilisation de groupes de hackers aura été un des éléments participant à 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 fournir. Ces groupes se présentent eux-mêmes comme totalement indépendants et déconnectés du Kremlin, lequel fait écho à ces déclarations annonçant ne pas avoir de prise sur les hackers, alors même que la puissance et l'importance de la guerre informationnelle a été clairement formalisée 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 pas d'impliquer clairement ces individus et de faire le lien avec le gouvernement. Quand bien même ce lien avec le gouvernement serait mis 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 selon leur propre volonté pendant leurs congés et non sur ordre gouvernemental.

Une fois que l'on a pris conscience de ce nuage de fumée offert 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 de pouvoir être démasqué et condamné reste minime.

Le cyber, facteur d'influence sur la confiance?

Dans l'analyse faite suite aux entretiens menés en Ukraine en 2017, il apparait 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 de s'attacher à observer l'influence du cyber sur la confiance portée aux informations de manière générale. Ce travail doit permettre de définir si cette inflexion était uniquement contextuelle ou si elle est plus générale et, par conséquent, si elle pourrait être utilisée de façon plus vaste pour servir une stratégie globale.

Dans les observations de 2017, il ressort que les militaires interrogés accordaient majoritairement leur confiance aux informations - ou éléments d'information - donnés 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'individu la recevant. Diverses études ont été menées sur ce sujet, principalement aux Etats-Unis. Cependant, si le terrain de ces études n'était ni l'Ukraine ni la France, notons que les taux de pénétration d'Internet sont assez proches entre l'Europe et les Etats-Unis donnant un premier socle commun solide à l'analyse.

En effet, le taux de pénétration d'Internet est de 88% en Europe de l'Ouest et de 84% aux Etats-Unis[15]. Enfin, en termes de pénétration des médias sociaux, les Etats-Unis affichent un score de 66% et l'Europe de l'Ouest de 56% et la pénétration des médias sociaux est de 54% en Europe de l'Ouest en 2017 et de 66% aux Etats-Unis.

Ainsi, en se basant sur ces chiffres, nous sommes nombreux à pouvoir être influencés par Internet. L'accroissement de la consommation de données mobiles ne fait qu'augmenter la possibilité de toucher n'importe qui à toute heure du jour ou de la nuit. Or, sur les 2,8 milliards d'utilisateurs de médias sociaux, plus de 91% sont connectés via des appareils mobiles. Parler d'une connexion tout au long de la journée n'est pas excessif : dans une étude sur cette question, le cabinet Deloitte[16] montre que 16% des Français consultent leurs smartphones dans les cinq minutes après le réveil (jusqu'à 35% chez les 18-24 ans), et 42% dans les trente 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, 79% disent « répondre aux messages dès leur réception ». Ce n'est pas un phénomène local, au Royaume-Uni une enquête menée par Omnibus Institut[17] montre que les 18-34 ans regardent leurs smartphones jusqu'à 100 fois par jour, soit toutes les dix minutes. Les chiffres sont assez similaires pour les 25-34 ans interrogés avec un coup d'œil à la même fréquence.

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[18], 58% de la génération Z et 33% de la génération Y utilisent les médias sociaux pour accéder à l'information, ces chiffres deviennent 30% et 41% quand on parle

[15] We are social, « Digital, social, mobile: les chiffres de 2017 », janvier 2017 https://wearesocial.com/fr/blog/2017/01/digital-social-mobile-les-chiffres-2017

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

[17] Omnibus Institut survey for Kana Software

[18] The American Press Institute and the Associated Press-NORC Center for Public Affairs Research, « A new understanding: What makes people trust and rely on news », American Press Institut, avril 2017

d'accès à l'information à travers 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 et la « génération Z » est légèrement inférieure à 70%. Ces deux tranches d'âge sont des utilisatrices de réseaux sociaux avec respectivement 65% et 88%[19]. Avec ces chiffres en tête, il apparaît qu'une analyse de la confiance dans les informations reçues sur le web sera pertinente pour comprendre 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 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. Cinquante et un pour cent des personnes disent qu'un article publié est de qualité quand il est partagé par une personne de confiance. Seulement trente quatre pour cent 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 la nature de celui qui partage influence également la perception relative à la représentativité des divers points de vues 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% avait ce sentiment quand le même document n'était pas transmis par un « ami ». Enfin, la même information transmise par une personne de confiance et provenant d'une source connue convainc 52% des destinataires que l'article a bien restitué les faits. Le même article non transmis par une personne de confiance mais provenant de la même source ne recueille que 32% d'avis favorables. 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 qui a publié un article influence la confiance qu'elles lui accordent.

A la lumière de ces données, il apparaît clairement que celui qui partage le message semble être plus important que la source originale de l'information. Considérant que la formation particulière des militaires développe « l'esprit de corps », il est possible que si la personne partageant un contenu est supposée être un soldat cela augmentera la confiance accordée au contenu partagé.

[19] Eurostat, "Internet activities in the past three months by age group EU-28, 2016 (% of internet users)", décembre 2016

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 cette règle. Non seulement ils sont aussi connectés que leurs concitoyens mais de plus la « génération Y », qui est l'une des plus connectées, est très présente parmi les grades allant de l'homme du rang au lieutenant. Ainsi, selon les différents travaux compilés, une large part de leur population appartient à la tranche d'âge la plus susceptible d'être influencée par le cyber et de voir leur confiance influencée. Si l'on pose l'hypothèse selon laquelle la confiance peut être altérée par des opérations de « cyberwarfare », alors il parait nécessaire d'analyser l'importance et le rôle de la confiance dans le fonctionnement des équipes militaires.

A cet égard, il convient d'évoquer le contexte dans lequel ces équipes évoluent. Dans le cadre de leurs missions, les soldats interviennent dans des situations extrêmes au sens qui leur est donné par Lièvre (2005). Selon lui, une situation est considérée comme extrême quand elle présente trois caractéristiques principales : être évolutive, incertaine et risquée. Cet attendu fait consensus avec d'autres auteurs parmi lesquels Rivolier (1998), qui affine le sens « d'évolutive ». Il explique qu'évolutive se réfère à une situation en rupture avec la vie quotidienne, ainsi la situation extrême présenterait un écart entre le quotidien, la situation « A », et la situation qualifiable d'extrême, « B », qu'elle soit présente ou à venir dans un futur proche. L'incertitude est ici entendu comme étant radicale et totale (Knight, 1923) c'est-à-dire qu'il sera difficile voire impossible de mesurer la probabilité qu'un événement quelconque - mais le plus souvent à risque - apparaisse. En somme, 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 être entendu à diverses échelles en termes de dommages subis mais n'exclut ni le risque de blessure ni le risque de mort. Là encore, comme dans l'incertitude, l'échelle de risque n'est pas toujours précisément mesurable par les personnes vivant cette situation. En nous basant sur les trois caractéristiques, il apparait clairement que les missions militaires revêtent tous les caractéristiques permettant de les définir des situations de crises. Or, les soldats interviennent de façon régulière dans ces situations qui ne devraient être qu'exceptionnelles. En outre, de par ces caractéristiques propres, la situation extrême aura tendance à exacerber les comportements y intervenant en faisant par la même un sujet d'observation privilégié. Dans le cas des soldats, les commandements ont parfaitement conscience que pour pourvoir vivre et intervenir de façon récurrente dans des situations extrêmes nécessitera un conditionnement fort afin de minimiser les risques et de tenter de faire décroitre l'incertitude.

Si ce conditionnement, cet entrainement, s'avère efficace sur le terrain, il sera donc validé par l'expérience empirique du soldat, il sera donc plus que probable qu'il y adhère de manière quasi intime, transformant des éléments cognitifs en éléments affectifs faisant partie du cœur de leur personnalité, un fonctionnement indiscutable de leur système de pensée. Il apparait donc que l'incertitude est une pierre angulaire de la situation extrême ce qui nous 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 au domaine de l'action militaire, la performance pourrait être définie comme l'atteinte du but fixé par le commandement en subissant le minimum possible de dégâts matériels et de pertes humaines. Ainsi, la confiance serait en relation directe avec la cohésion et la performance. 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, la performance de l'équipe, ce qui augmentera le facteur de risque pour le succès de la mission. 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 basé sur les actions attendues d'une autre partie dans une interaction affectée par 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). A 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 rentrent chez eux blessés ou morts) ou dans les relations interalliées.

Par conséquent, 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 Etat, infléchir ses prises de décisions sans que cela soit évident ou détectable correspond en tout point aux objectifs affichés de la théorie du chaos dirigé, chère à un certains nombre de puissances.

Potentiels opérationnels - l'utilisation de la dissonance cognitive

En croisant les potentiels liés à l'altération de la confiance chez les soldats et les observations de terrain, il semble que nous soyons face à la mise en œuvre de théories psychologiques connues depuis les années cinquante et qui recourent à la dissonance cognitive pour expliquer certains comportements individuels. Selon Léon Festinger (1956), la dissonance cognitive est un état d'inconfort psychologique motivationnel ressenti par un individu dès lors que deux cognitions dites « inconsistantes » s'affrontent. Pour revenir à un état de quiétude, le sujet soumis à cet inconfort aura tendance à agir, à poser une action pour affirmer son choix premier et se dégager de la situation inconfortable engendrée par la confrontation. C'est ce que l'on appelle des stratégies de réduction de la dissonance cognitive. Plus l'amplitude est grande entre les cognitions inconsistantes, plus la pression pour mettre en place des stratégies de réduction sera forte. Ces stratégies pourront prendre des formes variées : la modification des éléments présents dans la situation d'inconsistance, l'ajout d'éléments consistants permettant d'invalider une des deux cognitions à l'origine de la dissonance et de l'inconfort, ou encore la diminution de l'importance des éléments inconsistants avec la cognition la plus résistante. Cet enchainement induira donc sur la cible un changement de comportement, faisant de l'état de dissonance cognitive un phénomène orienté vers l'action (Harmon-Jones, 2002-2003).

En revenant sur les observations de terrain, les soldats ukrainiens n'ont jamais cessé de croire en la cause qu'ils défendent (se battre pour l'Ukraine) mais leurs doutes envers le gouvernement augmentaient progressivement, pour certains d'entre eux ces doutes se cristallisaient 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 occupaient d'autres professions avant le déclenchement du conflit). Cette identité, ces valeurs sont étroitement liées à la lutte patriotique pour leur pays. De plus, lorsqu'ils se décrivent, ils utilisent des termes faisant appel à des valeurs souvent associée au monde militaire, laissant penser qu'ils adoptent ces éléments cognitifs (appris par la formation, le conditionnement dû à la nature même de leur métier) comme faisant partie d'eux-mêmes, des éléments constitutifs de leur soi.

Ainsi, ces éléments cognitifs acquis par le conditionnement deviendraient des composants de leur personnalité relevant de l'affectif. Le glissement vers l'émotionnel de ces éléments initialement cognitifs est renforcé par le test in vivo de leur bien fondé : leur formation les aidant à sauver leur vie, elle a été testée avec succès, elle est devenue indiscutable dans son intégralité. Elle fonctionnerait alors sur le modèle d'une action réflexe, émotionnelle, qui ne passe pas par le 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. L'opération d'influence pourrait intervenir de façon assez discrète avant le déploiement des militaires et ne prendre tout son sens qu'une fois les hommes au cœur de l'action de la situation extrême rencontrée, par exemple sur un théâtre d'opération.

Cette hypothèse de stratégie d'influence et le mode de fonctionnement observé chez les militaires nous pousse à nous intéresser à la variante fonctionnelle de la théorie de la dissonance cognitive présentée dans les travaux d'Elliott Aronson (1968, 1992). Cet auteur développera le concept de l'« auto-consistance ». Selon lui, 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 se trouve face à une idée ou 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 le profil parfait 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 conséquences irréversibles (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 model intégratif de Stone et Cooper (1999), le « Self Standard Model » (SSM). Dans cette proposition, les éléments cognitifs susceptibles d'être atteints par la dissonance cognitive peuvent relever de normes personnelles (on parlera d'excitation idiographique) ou de standards normatifs (l'excitation nomothétique). Dans le cas des soldats, les standards normatifs se transforment parfois en normes personnelles.

De ce fait, les militaires apparaissent à nouveau 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 une des pierres angulaires du bon fonctionnement des opérations militaires. Dans le contexte actuel, le cyber offre la possibilité, du fait de 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'auto-consistance, 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. Au final, 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. Cette mise en place 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, alors il pourra soumettre les cibles choisies à un feu roulant d'attaque cognitives.

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, alors 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 les forces armées occidentales. En se basant sur les éléments présentés dans cet article, il apparait que plus une cible sera conditionnée, plus elle sera réceptive à 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. La force de cette organisation repose notamment sur le professionnalisme, sur des compétences acquises au fil de l'entraînement et donc du conditionnement. Or, dans le cadre de la dissonance cognitive, plus une personne sera conditionnée et entrainée, plus elle sera lisible en termes de réaction possible face à des éléments cognitifs inconsistants. Autrement dit, ce qui est un des éléments même de la force des armées occidentales, pourrait devenir une faiblesse en terme d'attaques cyber psychologiques 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 blog, « Cyber Bait », discussions de groupes, plateforme de diffusion comme YouTube, « Native Advertising », médias d'information alternatifs, etc.), que la consommation de données intervient sans que le commandement ne le voit et que la cible ne se sentira pas attaquée car, dans la plupart des cas, l'attaque revêtira 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 dissonance, 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 prévision d'un potentiel conflit ultérieur, voire d'un conflit planifié. Dans ce cas, les hommes pourraient être attaqués en avance de phase, et ne pas jouir de la totalité 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 touché pourrait modifier son comportement, ne pas être en adéquation avec celui attendu par le commandement. Que cette modification soit une hyper-réaction (action hors du cadre défini par les ordres) ou une hypo-réaction (manque de réactivité, temps de latence, ou mise en retrait), elle sera également dangereuse quant au bon déroulement de la mission confiée : nous parlerons alors de « désengagement » au sens ou 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 se sont concentrées en termes de nombre, ainsi, les hommes ont tendance à intervenir en équipes plus réduites que par le passé. Or si, trois hommes sont touchés dans une équipe de six personnes, alors, c'est en réalité la moitié de la capacité opérationnelle du groupe qui sera atteinte, ce qui représente un risque fort quant à l'aboutissement satisfaisant de la mission confiée.

Enfin, si les hommes ciblés par une attaques cyber utilisant la dissonance cognitive résistent à l'inconfort psychologique engendré par l'affrontement de cognitions et ne modifient pas leur comportement, il n'est pas certain que le stratège à l'origine de l'attaque ait tout de même perdu. 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, V., Krug, M.K., Schooler, J.W., & Carter, C.S , 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 est le cas, alors outre la problématique opérationnelle l'utilisation de la dissonance cognitive pourrait devenir un problème de ressources humaines touchant à la santé des personnels. Enfin, outre les conséquences induites par la hyper stimulation de zones cérébrales, la persistance d'un inconfort psychologique pourrait mener à des conduites addictives tendant à faire décroitre l'inconfort. Dans tous les cas, sur le long terme la personne ciblée serait fragilisée et potentiellement instable alors que la mission exige une efficience optimum et une stabilité sans faille.

En conclusion, ces diverses observations ouvrent sur plus de questions que de solutions qu'il conviendra de creuser au travers d'un travail de recherche. Ces problématiques sont à ce jour le sujet d'une thèse visant à vérifier les effets de la dissonance cognitive sur les personnes conditionnées, mais également à tenter de définir quels seraient les facteurs cognitifs permettant le développement de la dissonance cognitive visant à atteindre la confiance, à développer

l'incertitude et par construction à engendrer le désengagement. D'après les observations menées sur le terrain, les contours d'un premier profil ayant réagi plus fortement semble apparaître en termes de tranche d'âge, de temps de consommation internet et de formation reçue. Il reste à affiner ces différents éléments et à mettre en lumière les variables d'intérêt permettant le déclenchement de l'inconfort psychologique dans des milieux socioprofessionnels donnés, jouissant d'un conditionnement particulier.

Bibliographie

Adams B, Webb R, « Trust development in small teams », Defense research and development Canada, 2003, Toronto contract report, CR-2003-016. Guelph, Ontario; HumanSystem Incorporated.

American Press Institute and the Associated Press-NORC Center for Public Affairs Research, « A new understanding: What makes people trust and rely on news », American press Institute, avril 2017

Battacharya Rajeev, Devinney Timothy M, Pillutla Madan M, "A formal model of trust based on outcomes", *Academy of management review*, 1998, 23(3), pp 459-472

Buckley T, *What Happens to the Brain During Cognitive Dissonance?*, Scientific American, 2017

Cabinet Deloitte, « Usages Mobiles 2015: A Game of Phones », annual report, janvier 2016

Marco Colosio, Anna Shestakova, Vadim V. Nikulin, Evgeny Blagovechtchenski and Vasily Klucharev, "Neural mechanisms of cognitive dissonance (revised): An EEG study", *Journal of Neuroscience*, publié en ligne, 24 avril 2017

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

Eurostat, "Internet activities in the past three months by age group EU-28, 2016 (% of internet users)", décembre 2016

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

Festinger Leon, *Une théorie de dissonance cognitive*, Les classiques de sciences humaines et sociales, Paris, Enrick B Editions, 1956

Girandola F (2000), « Le soi la théorie de la dissonance cognitive », *Revue Internationale Sociale*, 13, pp 115-147

Girandola F (2001), « Dissonance cognitive: le retour à Festinger », *Revue Internationale de Psychologie Sociale*, 14, 71-111

Gobert S, « Nouvelle escalade de violence sur le front ukrainien », *Libération*, 1er février 2017

Url : http://www.liberation.fr/planete/2017/02/01/nouvelle-escalade-de-violence-sur-le-front-ukrainien_1545664

Harmon-Jones E, Brehm J, Greenberger J, Simon L & Nelson D, «Evidence that the production of aversive consequence is not necessary to create cognitive dissonance », *Journal of Personality and Social Psychology*, 1996, 70, pp 5-16

Harmon-Jones Eddie, "A cognitive dissonance theory perspective on persuasion", in *The Persuasion Handbook: Developments in Theory and Practice,* eds. James Price Dillard, Michael Pfau London, Sage publication, 2002

Jonas E, Greenberg J, Frey D, « Connecting terror management and dissonance theory: evidence that mortality salience increases the preference for supporting information after decision », *Personality and social psychology Bulletin*, 2003, 29, pp 1181-1189

Knight Franck, *Risk, Uncertainty and Profit*, 1923, Lanham, National Book Network (janvier 1997)

Lièvre P, Ris G (2005), « Le management des expédiaions polaires », *Revue Française de Comptabilité*, 383, décembre, p 46-52

Le Moigne JL, *La modélisation des systèmes complexes*, Paris, Dunod, 1990

Mayer R C, Davis J H. and Schoorman F. D, "An Integrative Model of Organizational Trust", *The Academy of Management Review*, Jul.1995, Vol. 20, No. 3 pp. 709-734

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

Mullen Brian, Cooper Carolyn, "The relation between group cohesiveness and performance: An integration", *Psychological Bulletin*, 1994, 115, pp210-227

Omnibus Institute survey for Kana Software

Orléan André (1986), « Hétérodoxie et incertitude », *Epistémologie et Autonomie,* Les cahiers du CREA, n°5, Ecole Polytechnique, Paris.

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

Rousseau Denise, Sikins Sill, Burt Ronald, and Camerer Collin Farell, "Not so different after all: a cross discipline view of trust", *Academy of management review*, 1998, 23(3), pp 393-404

Stewart N K, *The South Atlantic conflict of 1982. A case study on military cohesion*, 1998, U.S Army, Alexandria

Stone J, Cooper J, « A self-standards model of cognitive dissonance », *Journal of Experimental Social Psychology*, 1999, pp228-243

Thibodeau R. et Aronson E. (1992), "Taking a closer look: Reasserting the role of the self-concept in dissonance theory", *Personality and Social Psychology Bulletin*, 18, pp. 591-602.

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

Van Veen, V., Krug, M.K., Schooler, J.W., & Carter, C.S. (2009), "Neural activity predicts attitude change in cognitive dissonance », *Nature Neuroscience*, 12(11), 1469–1474

We are social, « Digital, social, mobile: les chiffres de 2017 », janvier 2017, URL : https://wearesocial.com/fr/blog/2017/01/digital-social-mobile-les-chiffres-2017