COGNITIVE WARFARE
LA GUERRE COGNITIQUE

Première réunion scientifique Cognitive Warfare
Bordeaux (FR) - 21 juin 2021

Sous la direction scientifique de : B. CLAVERIE, B. PRÉBOT ET F. DU CLUZEL.

Journée organisée par l'Innovation Hub de NATO-ACT et l'ENSC, avec le soutien de l'État-Major des Armées (FR – Major Général), du NATO-CSO et de la Région Nouvelle Aquitaine.

Ouvrage publié par le CSO - Neuilly (France) © édition 2021

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

www.sto.nato.int

Cognitive Warfare : La guerre cognitique

Première réunion scientifique Cognitive Warfare Bordeaux (FR) – 21 juin 2021.
Journée organisée par l'Innovation Hub de NATO-ACT et l'ENSC, avec le soutien de l'État-Major des Armées (FR – Major Général), du NATO-CSO et de la Région Nouvelle Aquitaine.

Sous la direction scientifique de
B. Claverie, B. Prébot et F. Du Cluzel.

Ouvrage publié par le NATO-CSO-STO avec le soutien de l'Innovation Hub NATO-ACT, de l'ENSC Bordeaux-INP, de l'État-Major des Armées (FR) et de la Région Nouvelle Aquitaine.

Published October 2021

ISBN 978-98-837-2368-4

Sommaire

Liste des illustrations

Liste des tableaux

Avant propos – par le directeur adjoint du Collaboration Support Office (CSO) STO

Général Philippe Montocchio [1]

« Agir non seulement sur ce que pensent les individus-cibles, mais aussi sur la façon dont ils pensent, et in fine, dont ils agissent. »

Les technologies de l'information ont connu une évolution spectaculaire – en fait, une révolution – au cours des vingt dernières années. L'ordinateur familial, la tablette, le smart phone pour tous, la mondialisation du réseau Internet, l'affirmation des réseaux sociaux comme mode de communication privilégié, les débuts de la réalité virtuelle, et bien d'autres évolutions technologiques dans le domaine de l'information, sont en train de modeler la façon dont les individus et les communautés vont échanger et communiquer entre eux.

D'une manière plus globale, le monde de demain va être marqué par certaines grandes tendances qui vont régir les rapports entre états et façonner leur manière d'appréhender les conflits futurs. Les confrontations entre grandes puissances, impliquant aussi les organisations internationales pourvoyeuses de sécurité, comme l'Alliance Atlantique, vont ainsi être affectées par l'interdépendance des économies, l'hyper-connectivité des sociétés, la digitalisation de notre environnement, l'explosion des données – ou Data – et la fragmentation du monde en communautés d'intérêt.

Ces grandes tendances, associées à la dissuasion nucléaire qui va conserver une certaine pertinence, vont rendre les chocs militaires dévastateurs entre grandes puissances moins ou peu probables. Cependant, dans la mesure où les luttes d'influence persisteront, ces mêmes grandes puissances et alliances de pays devront trouver d'autres champs d'action « pour prolonger la guerre par d'autres moyens », en détournant la célèbre phrase de Clausewitz. Le recours à des modes d'action dits hybrides va devenir beaucoup plus régulier, voire permanent, effaçant totalement les frontières entre temps de paix et temps de crise.

Parmi ces moyens hybrides, la guerre de la communication et de l'information, ou *information warfare* en anglais, a souvent été perçue comme une sous-fonction secondaire dans la planification des opérations de gestion de crise qui, en général, font reposer l'essentiel de l'action sur des capacités militaires classiques. Dans le monde qui se dessine, l'*information warfare*, et le *cognitive warfare*, objet de cette réunion scientifique, vont probablement devenir des modes d'action permanents, se suffisant à eux-mêmes, pour obtenir dans la durée un état final recherché : la déstabilisation d'un leader politique, d'une force ennemie, d'un pays, … ou d'une Alliance.

Le *cognitive warfare* est la forme la plus aboutie, à ce jour, de manipulation permettant d'influer sur le comportement d'un individu ou d'un groupe d'individus, avec le but d'en tirer un avantage tactique ou stratégique. Dans ce domaine d'action, le cerveau humain devient le théâtre d'opérations. L'objectif est d'agir non seulement sur ce que pensent les individus-cibles, mais aussi sur la façon dont ils pensent, et en fin de compte, dont ils agissent. Le *cognitive warfare* est nécessairement associé à d'autres formes et domaines d'action pour atteindre le ou les cerveaux-cibles, tels le *cyber warfare* et l'*information warfare*.

[1] Philippe Montocchio est Général de division aérienne, en 2ème section. Diplômé de l'École de l'Air, ancien pilote de chasse, diplômé de l'École de Guerre, le Général Montocchio a été commandant des forces française à Djibouti (2014 – 2016) puis Directeur des Relations Internationales de l'État major des Armées, avant de rejoindre l'OTAN où il occupe la direction adjointe du Collaboration Support Office (CSO) en charge de l'animation, de la coordination et du soutien du programme « Science and Technology » de l'OTAN.

Dans sa conceptualisation, le *cognitive warfare* intègre aussi un pan essentiel qui a connu des développements récents : les neurosciences cognitives. En facilitant la compréhension des mécanismes du cerveau, la façon dont il intègre et traite les différentes catégories d'information, les neurosciences vont permettre d'optimiser l'emploi des autres *warfare(s)*, notamment l'*information warfare*.

La prise de conscience collective par l'OTAN de l'importance accrue de cette forme de conflictualité est en train de s'opérer progressivement. Le Sommet OTAN de Varsovie, en 2016, avait vu la reconnaissance du domaine opérationnel cyber, et les enjeux de la guerre hybride avaient été soulignés dans le communiqué du Sommet, mais vus essentiellement au travers du prisme des modes d'action cyber et des opérations spéciales. Le communiqué du récent Sommet OTAN, qui s'est tenu le 14 juin 2021, marque un vrai tournant. Pour la première fois, la Chine et la Russie sont mentionnées avec insistance pour leurs actions de désinformation, traduisant l'intérêt croissant que portent les Alliés à ces nouveaux défis hybrides.

Face à ces deux adversaires potentiels, l'OTAN est confrontée à la difficulté d'agir et de réagir collectivement à trente, avec des disparités significatives entre Alliés, tant au niveau de leurs aptitudes militaires et technologiques qu'au niveau de leurs intérêts propres. Elle ne dispose pas des capacités collectives pour détecter et caractériser les actions hybrides, notamment dans les domaines informationnel et cognitif. De même, identifier le ou les auteurs d'une agression hybride, et convenir d'une réponse appropriée, seront autant de défis qui affecteront la crédibilité de l'Alliance si la réaction des Alliés est inadaptée. Les questions éthiques se poseront aussi immanquablement. Si la désinformation et la déstabilisation sont des modes d'action acceptables pour des pays totalitaires, peuvent-elles être officiellement intégrées dans la panoplie des réponses possibles de l'Alliance ? Dernière difficulté de taille pour l'Alliance : les opérations hybrides peuvent certes viser les capacités collectives de l'OTAN, ses leaders ou son système décisionnel, mais elles ciblent en général davantage les intérêts stratégiques nationaux des pays membres : infrastructures et services vitaux, population, leaders politiques, etc. Les enjeux de souveraineté nationale vont donc forcément complexifier la prise en compte collective de telles agressions et l'élaboration de la riposte commune que pourraient produire les Alliés.

En concertation et complémentarité avec le Commandement allié pour la transformation (ACT), l'Organisation pour la Science et la Technologie (STO) de l'OTAN mène la réflexion amont sur les technologies susceptibles de maintenir l'avance scientifique et technologique de l'Alliance face à ses adversaires potentiels.

La STO regroupe en son sein un réseau de près de 6 000 chercheurs provenant des pays alliés et de certains pays partenaires, notamment la Suède, la Finlande, l'Australie, et le Japon. La STO couvre l'intégralité des thèmes scientifiques et technologiques de défense et de sécurité, répartis dans sept grands domaines de recherche. Ces sept domaines scientifiques sont explorés par des Panels et un Groupe, dont quatre présentent un intérêt particulier dans le cadre de l'étude sur le *cognitive warfare* : les Panels Human Factors and Medicine (HFM), Information Systems Technology (IST), System Analysis and Studies (SAS) et NATO Modelling and Simulation Group (MSG).

La journée de réflexion sur le *cognitive warfare*, organisée le 21 juin dernier par l'Innovation Hub de l'ACT et l'École nationale supérieure de cognitique de Bordeaux INP, avec le soutien de l'État-Major des Armées françaises, de la STO, et de la Région Aquitaine, a donné lieu à de riches échanges que reflètent les excellents articles regroupés dans ce document.

Préface – par le Commandant suprême allié Transformation (SACT) de l'OTAN

Général d'Armée Aérienne André Lanata [2]
Commandeur suprême transformation de l'OTAN

Exploiter les failles de la nature humaine pour mieux cibler l'esprit des individus n'est pas une idée nouvelle. La manœuvre d'influence et de déception a toujours fait partie de l'art de la guerre. Sun Tzu soulignait déjà en son temps l'importance du facteur psychologique, et si l'empire romain s'est d'abord appuyé sur la force de son armée, il doit sa longévité à sa volonté persistante d'imposer sa culture et donc sa propre vision du monde. Aujourd'hui les progrès technologiques réalisés dans le domaine informationnel et l'hyper connectivité dans laquelle nous vivons, rendus possibles par la numérisation des informations, démultiplient les possibilités de manipulation d'un individu ou de ciblage d'un groupe de personnes. L'explosion récente des procédés de manipulation psychologique à des fins d'escroquerie par le biais de l'ingénierie sociale montre bien que la connaissance du comportement humain et la capacité à l'influencer sont désormais au cœur d'un nouvel enjeu stratégique. Cette bataille des perceptions affecte tous les secteurs de la vie des sociétés et en particulier celui de la sécurité et de la défense.

Surveillant en permanence les menaces émergentes, l'OTAN s'est rapidement intéressée à ce sujet. Le commandement allié pour la Transformation, situé à Norfolk (États-Unis), responsable de la préparation et du développement des futures capacités de l'Alliance, a récemment travaillé sur une étude appelée *cognitive warfare* destinée à éclairer et anticiper la militarisation des technologies que l'on regroupe sous l'acronyme NBIC (Nanotechnology, Biotechnology, Information Technology and Cognitive Science).

C'est pourquoi je salue la tenue de cette première réunion scientifique qui s'est tenue le 21 juin dernier à Bordeaux sur le thème de la guerre cognitive. Ce thème me paraît tout à fait remarquable et je remercie bien sincèrement l'École Nationale Supérieure de Cognitique, avec laquelle mon commandement entretient depuis de nombreuses années une coopération fructueuse, d'avoir accueilli et organisé avec notre Innovation Hub ce premier opus. Je salue également la participation des éminents experts internationaux qui ont répondu à notre invitation et ont contribué au succès de cette journée.

La richesse des échanges en Français comme en Anglais, les présentations, les tables rondes mais également les démonstrations pratiques de l'ENSC témoignent de la belle vitalité de la recherche et du développement en *cognitive warfare* dont disposent les Alliés. Il revient au commandement de la Transformation de l'OTAN de continuer à fédérer les énergies pour entretenir et développer cette dynamique, au service de la stabilité, de la prévention des conflits et de sécurité du milliard de citoyens que compte l'Alliance Atlantique.

[2] André Lanata est Général d'Armée Aérienne. Ancien pilote chasse, il a dirigé l'ensemble de l'Armée de l'Air française comme chef d'État Major de 2014 à 2018, date à laquelle il été nommé Commandeur Suprême pour la Transformation de l'OTAN (NATO Supreme Allied Commander Transformation).

Cognitive Warfare « La guerre cognitique »
Première réunion scientifique OTAN[3]
21 juin 2021

« Cognitive warfare est la rencontre de la cyberpsychology, de la weaponization of neurosciences et de la cyber-influence pour l'altération provoquée de la perception du monde et de son analyse rationnelle chez les humains, militaires, politiques ou autres acteurs et décideurs, à des fins d'influence de leur décision ou de leur action, pour une supériorité stratégique à tous les niveaux d'intervention concernant l'intelligence naturelle individuelle ou collective, comme l'intelligence artificielle ou augmentée dans les systèmes hybrides. »

La première réunion scientifique *cognitive warfare* s'est tenue à Bordeaux (France) le 21 juin 2021 à l'initiative de l'Innovation Hub (NATO Allied Commander Transformation – Norfolk USA) et de l'École Nationale Supérieure de Cognitique (Bordeaux INP France), en présence des scientifiques, militaires et industriels concernés, des représentants de l'IH et de l'ENSC, du directeur adjoint du Collaboration Support Office (NATO Science and Technology Organization - Neuilly France) et du Major Général des Armées françaises (État-Major des Armées - Paris France).

Cet ouvrage reprend les principales conférences qui ont été données lors de la réunion, et celles dont les textes ont été fournis en début de la session pour enrichir et faciliter les débats.

Les articles ont été revus et adaptés à la thématique de l'ouvrage par les éditeurs de l'ouvrage.

Il est édité par le Collaboration Support Office (CSO) de la Science and Technology Organization (STO) de l'Organisation du traité de l'Atlantique Nord (NATO).

Comité scientifique

- Baptiste Prébot : Ingénieur ENSC, Docteur de l'Université de Bordeaux, assistant d'enseignement et de recherche à l'ENSC / IMS UMR 5218, réserviste DGA.
- Bernard Claverie : Professeur des universités, Directeur honoraire de l'ENSC – Réseau ADER.
- François Du Cluzel : Responsable de projets innovants – Innovation Hub - NATO-ACT.

Comité d'organisation

- Baptiste Prébot : ENSC/DGA.
- Thomak Leduc : Doctorant en ingénierie cognitive – Université de Bordeaux / Thales AVS.
- Isabelle Sesé : Responsable administrative de l'ENSC.

[3] La thématique *cognitive warfare* a été développée par l'Innovation Hub de la NATO-ACT (Norfolk) dans le cadre de la convention de collaboration associant l'Ecole Nationale Supérieure de Cognitique (ENSC – Bordeaux INP – France) et ACT, signée le 15 juin 2017 sous le titre « Letter of Accord to Collaborate Between Ecole Nationale Superieure de Cognitique and Headquarters, Supreme Allied Commander Transformation » et sous l'égide du Général d'Armée Aérienne André Lanata (SACT – 2017 – 2021). La collaboration a été initiée dès 2013 par le Général d'Armée Aérienne Denis Mercier (SACT – 2013 – 2017) et le Professeur Bernard Claverie (directeur de l'ENSC – 2009 – 2019) sur la thématique *cyberpsychology* puis *weaponization of neurosciences*.

L’organisation a été assurée par l’ENSC avec l’appui et le soutien de ACT, de l’État-major des armées et de la Région Nouvelle Aquitaine.

La publication des actes est assurée par le CSO.

Programme scientifique – 21 juin 2021

10h00	**Mot de bienvenue** (en Français et Anglais)
	Pr. Benoît LE BLANC, directeur de l'ENSC.
10h10	**Conférence d'introduction** (en Français)
	Pr. Bernard CLAVERIE, directeur honoraire fondateur de l'ENSC – Bordeaux (France).
10h40	**Keynote** (en Français) : « Le Domaine Cognitif, un sixième domaine d'opération ? »
	Hervé Le Guyader – responsable relations ENSC-STO – membre associé au panel IST STO.
11h00	**Keynote** (en Français) : « Cognitive Warfare – Perspectives Otaniennes. »
	François Du Cluzel – Innovation Hub – NATO-ACT – Norfolk (VA, USA).
11h10	**Table ronde** (en Français) : « Le futur du *cognitive warfare* – menaces globales et réponses industrielles. »
	Animateur : François Du Cluzel – Innovation Hub – NATO-ACT – Norfolk (VA, USA) ;
	Gal. Gilles Desclaux – ancien CDAOA – conseiller Défense – ENSC – Bordeaux (France) ;
	Thierry Lemoine – responsable de l'unité Thales LAS « La Ruche » – Rennes (France) ;
	Marc Rodier – ingénieur docteur – IBM distinguished engineer – Chaire Sciences et technologies Cognitiques – Toulouse et Bordeaux (France) ;
	Patrice Lefeu – EY partenaire associé – Global R&D and Innovation services – Paris (France).

PAUSE

Démonstrations et visite du laboratoire défense de l'ENSC

14h00	Introduction thématique (en Anglais) : « Narratives overwhelme the world. » (en visio.)
	Pr. Michael Wunder – Directeur du Département C2 & Intelligence FKIE – directeur scientifique honoraire (→2021) du panel IST de la STO de l'OTAN – Wachtberg (Allemagne).
14h20	Conférence débat (en Français) : « Les enjeux du « domaine cognitif »pour la France et son implication otanienne. »
	Gal. Eric Autellet – Général d'armée aérienne – Major général des armées – Paris (France).
15h00	Table ronde (en Anglais) : Le Cognitive Warfare – développements scientifiques.
	Animateur : Gal. Jean-Marc LAURENT – Chaire Défense & Aérospatial – Bordeaux (France).
	Pr. Benoît Le Blanc – Directeur ENSC, président de l'AFIA – Bordeaux (France) ;
	Gal. Philippe Montocchio – Directeur adjoint du Collaboration Support Office (CSO) Organisation pour la science et la technologie (STO) de l'OTAN ;
	Pr. Tanguy Struye De Swielande – directeur du Center d'étude des Crises et Conflits Internationaux (CECRI) de l'Université catholique de Louvain – Louvain La Neuve ;
	Célestin Sédogbo – ingénieur docteur – directeur de l'Institut Carnot « Cognition » et de l'unité propre du CNRS UAR2203 ;
	Philippe Mouttou – ingénieur docteur – directeur du développement et des études amonts – Thales Recherche et Technologies – Palaiseau (France).
16h30	Conférence de clôture (en Anglais) : « Technological Maturity of "Cognitive" Human Networked Systems. » (en visioconférence).
	Dr. Norbou Buchler – Army DEVCOM Data & Analysis Center – Aberdeen Proving Ground (MD, USA)
17h00	Préparation de la prochaine rencontre.

Liste des participants

Jean-Marc André	Professeur des universités – Directeur de la recherche – ENSC.
Eric Autellet	Général d'armée aérienne – Major général des armées – Etat Major des Armées.
Valérie Baron	Ingénieur de recherche – Unité de recherche « La Ruche » – Thales LAS.
Renaud Besselère	Médecin en chef – Information médicale – Service de Santé des Armées.
Julien Briand	Élève ingénieur – Réserviste de l'Armée de Terre – ENSC.
Norbou Buchler	Chercheur – DEVCOM Data & Analysis Center – US Army Research Lab.
Géraud Cazenave	Officier supérieur AAE – Etat Major des Armées.
Nicolas César	Journaliste Sud–Ouest – quotidien régional Nouvelle Aquitaine.
Bernard Claverie	Professeur des universités – réseau ADER/AAE-ENSC.
Gérard De Boisboissel	Ingénieur de recherche – École de Saint-Cyr – Armée de Terre.
Renaud Delbru	Chef d'entreprise – Société SIREN.
Gilles Desclaux	Général (2s) AAE (GCA) – Président de RACAM – chercheur HEAL-ENSC.
Jaime Diaz-Pineda	Expert facteur humain – Laboratoire HEAL – Thales AVS.
François Du Cluze	Chef de projets innovants – Innovation Hub – NATO-ACT.
Pascal Fouillat	Professeur des universités – Conseiller scientifique Région Nouvelle Aquitaine.
Tsiporah Fried	Administrateur civil – Etat Major des Armées.
Lola Gagnon	Analyste – CICDE – Ministère des Armées.
Marc Gatti	Directeur technique – Chef du département HAT – Thales AVS.
Daniel Hauret	ancien officier supérieur AAE – expert SCAF, conseiller militaire – Thales AVS.
Sylvain Hourlier	ancien médecin en chef, expert FH – Laboratoire HEAL – Thales AVS.
Thoiwhidine Ibrahim	Analyste – CICDE – Ministère des Armées.
Loïc Jacob	Élève ingénieur – Réserviste de l'Armée de Terre – ENSC.
Nicolas Largeault	Élève ingénieur – Réserviste de l'Armée de Terre – ENSC.
Jean-Marc Laurent	Général 2s AAE (GCA) – Directeur de la Chaire AD Sciences-Po Bordeaux.
Benoît Le Blanc	Professeur – Directeur de l'ENSC – membre du panel IST STO-ENSC.

Hervé Le Guyader	Chargé de mission – membre Panel IST STO-ENSC.
Thomak Leduc	Doctorant CIFRE – Laboratoire HEAL – ENSC – Thales AVS.
Patrice Lefeu	Associé EY.
Thierry Lemoine	Directeur technique de l'unité « La Ruche » – Thales LAS.
Ludovic Lorfanfan	Officier supérieur AAE – Commandement des Forces Aériennes.
Damien Marion	Chercheur à l'unité « La Ruche » – Thales LAS.
Jean-Paul Mochin	Général 2s AAE (GDA) – Conseiller militaire – Thales LAS.
Philippe Montocchio	Général 2s AAE (GDA) – Directeur adjoint du CSO – NATO-STO.
Philippe Mouttou	Directeur développement études amont – Thales Research and Technologies.
Jean-Christophe Noel	Chercheur à l'Institut Français des Relations Internationales.
Kimberly Orinx	Doctorante – CECRI – Univ. Catholique de Louvain.
Martial Papillon	Ingénieur de recherche – Société ThinkDeep.
David Pappalardo	Officier supérieur AAE – DEGRIS – Ministère des Armées.
Jean-François Pierron	Responsable Sud-Ouest de la France – IBM.
Baptiste Prébot	Assistant d'enseignement et de recherche – Réserviste de la DGA – ENSC.
Marc Rodier	Directeur de la Chaire Sciences et Technologies Cognitives – IBM.
Lucas Salles	Analyste – Direction zonale de sécurité intérieure Sud-Ouest.
Célestin Sédogbo	Directeur d'unité propre CNRS – Institut Carnot Cognition.
Vincent Van Steenbergen	Chef d'entreprise – Société ThinkDeep.
Michael Wunder	Directeur du Département C2 & Intelligence FKIE – membre panel IST STO.

Organismes représentés

Liste des institutions et entreprises d'appartenance des participants

Allied Command Transformation – NATO – Norfok – VA, USA.

École Nationale Supérieure de Cognitique – Bordeaux INP, FR.

Centre de Recherche des Écoles de Saint-Cyr Coëtquidan (CREC) – Saint-Cyr, FR.

Centre d'Étude des Crises et des Conflits Internationaux (CECRI) – Université Catholique de Louvain – Louvain-La-Neuve, BE.

Centre Interarmées de Concepts, Doctrines et Expérimentations – Paris, FR

Chaire « Aérospatiale et Défense » – Institut des Sciences Politiques de Bordeaux, FR.

Collaboration Support Office (CSO) NATO-STO – Neuilly, FR.

Commandement des Forces Aériennes – Armées de l'Air et de l'Espace – Mérignac, FR.

Département C2 & Intelligence – Institut Fraunhofer pour la Communication, le Traitement de l'Information et l'Ergonomie – FKIE – Wachtberg, DE.

Direction de l'Information médicale – Service de Santé des Armées – Begin – St-Mandé, FR.

Direction Générale des Relations Internationales et de la stratégie (DGRIS) – Ministère des Armées – Paris, FR.

Direction zonale de sécurité intérieure Sud-Ouest – Ministère de l'Intérieur – Bordeaux, FR.

EY – La Défense, FR.

IBM – Bois-Colombes, FR.

Innovation Hub – NATO-ACT – Norfolk – VA, USA.

Institut Carnot Cognition – UAR CNRS – Talence, FR.

Institut Français des Relations Internationales – Paris, FR.

La Ruche – centre de recherche Thales LAS – Rennes, FR.

Laboratoire commun « Human Engineering for Aerospace Lab. » – Thales-ENSC – Talence, FR.

Major Général – État Major des Armées – Ministère des Armées – Paris, FR.

Panel Information Systems Technology (IST) NATO-STO – Neuilly, FR.

RACAM (Réunion Aviation Civile – Aviation Militaire – Paris, FR.

Région Nouvelle Aquitaine – Bordeaux/limoges/Poitiers, FR.

SIREN – Galway, IO.

Thales Research and Technologies – TRT – Palaiseau, FR.

Thales Avionics – Mérignac, FR.

Thales Land-Air Systems – Massy, FR.

Thales Raytheon Systems – Massy, FR.

Think Deep – Talence, FR.

U.S. Army Combat Capabilities Development Command Data & Analysis Center (DEVCOM) – Army Research Lab – Aberdeen Proving Group (MA), USA.

Cognitive Warfare : La guerre cognitique

Cognitive warfare la guerre cognitique : ou comment exploiter les technologies de l'information pour amener les soldats, les techniciens et les ingénieurs, les décideurs et les politiques, à avoir une représentation erronée du monde… et en tirer profit ? Sachant que certains utilisent cela à des fins guerrières pour précipiter leurs victimes dans l'erreur, comment s'en prémunir ? Comment allumer les alarmes combinant triggers et informations pertinentes, et protéger les cibles humaines en leur donnant les moyens de prévenir ou de surmonter les automatismes, les distorsions et les erreurs dans lesquels ils sont amenés par un ennemi qui ne dit pas son nom ? Manipulation sémantique, illusion provoquée, distorsion perceptive, saturation de l'attention, trouble des apprentissages, de la mémoire de travail ou des souvenirs à long terme en sont des exemples qui se combinent entre eux. Mais la cognition est aussi collective, collaborative, pour une décision partagée ; le partage des représentations qui émergent dans l'acte de communication numérique est bien fragile, et son altération un moyen facile à mettre en œuvre.

Qu'elle soit individuelle ou collective, la cognition correspond à l'ensemble des processus que le ou les cerveaux mobilisent pour connaître le monde, prendre les décisions adéquates à une action espérée réussie sur lui. Deux mondes sont ici articulés, les cerveaux et les machines, exprimant ou exprimés par des pensées et des programmes. La rencontre de l'intelligence naturelle et de l'intelligence artificielle est au centre d'un débat qui oblige aujourd'hui à concevoir la guerre comme une action d'intelligence hybride. Les interfaces technologiques, la décision augmentée, le contrôle de l'erreur humaine ou du dépassement des limites des programmes, l'intégration humain- système, l'autonomie des acteurs aidée du numérique ou celle des machines enrichies par la pensée sont les grands chapitres techniques de ce qu'est déjà la guerre cognitique : le *cognitive warfare.*

Les plans d'action sont prêts. Le constat est lourd, multiforme, et porteur d'ambiguïté. La cognition est mal connue, et pourtant tout le monde s'en sert, et en revendique une forme d'expertise naïve.

Tout le monde a tendance à penser la maîtriser, et se sentir protégé. Sa propre pensée paraît à chacun inexpugnable, car l'erreur arrive aux autres, moins éduqués. Et si le spécialiste s'égare parfois, il trouve alors l'excuse de la distraction, de la fatigue ou de la faiblesse de l'autre. La prise de conscience est souvent tardive, et le *cognitive warfare* est exploité depuis longtemps, dans un double aspect : d'une part sa pratique est par essence discrète et sa mise en œuvre secrète, et d'autre part la cible nie son effet et minimise sa propre fragilité à en être la victime.

Cet ouvrage publié par le CSO de l'OTAN réunit des articles reprenant les principales interventions de la première réunion Cognitive Warfare tenue à Bordeaux en juin 2021 à l'initiative de l'Innovation Hub du Commandement pour la Transformation de l'OTAN et de l'École Nationale Supérieure de Cognitique avec la collaboration de l'État-major des armées françaises, du CSO et de l'ACT de l'OTAN, et de la Région Nouvelle Aquitaine. Cette première initiative fait un point sur la cognition humaine, sa force et ses faiblesses, son organisation collaborative pour la décision militaire, ses rapport et dépendance à la technologie numérique et ses dimensions sociales et politiques notamment dans la dure compétition internationale. Elle donne la parole au Major général des armées et au Commandeur pour la transformation de l'OTAN, et sévira de point de départ à une suite de rencontres d'approfondissement, à l'initiative du CSO et de l'ACT.

Chapitre 1 – LE *COGNITIVE WARFARE* ET L'AVENEMENT DU CONCEPT DE « GUERRE COGNITIQUE »

Bernard Claverie [1], François Du Cluzel[2]

« La guerre cognitique est parmi nous. Le problème majeur est qu'elle est invisible ; seules ses traces sont là…souvent trop tard. »

Le *cognitive warfare* est aujourd'hui conçu comme un domaine à part entière des guerres modernes. À côté des quatre domaines concrets de l'action militaire, « terre », « mer », « air » et « espace », et du domaine transverse des moyens numériques, le « cyber », on a pu voir, au cours de récents épisodes qui ont transformé les équilibres géopolitiques, l'émergence et la mise en œuvre de cette nouvelle dimension de la guerre.

Son champ d'action est global, puisqu'il s'impose à l'ensemble du monde humain cyberconnecté. Ses moyens sont les technologies de l'information, avec leurs outils, dispositifs, réseaux et systèmes numériques. Sa cible est bien définie : il s'agit de l'esprit des individus. Ceux-là sont à considérer à titre individuel comme dans leur dimension de groupe ou de collectivité.

Les attaques sont spécifiées, structurées, organisées pour la transformation ou le faussement de la pensée des décideurs comme des opérationnels, des membres d'une catégorie professionnelle ou sociale, des militaires d'une armée, ou même plus largement des citoyens d'une région, d'un pays ou d'un ensemble de pays. Les objectifs sont multiples et diffèrent selon la stratégie : conquêtes territoriales (p. ex. région frontalière, péninsule, ensembles insulaires), influence (élections, troubles de population), perturbation de services publics (administrations, hôpitaux, secours, assainissement, eau ou énergie) ou de transport (espaces aériens, déséquilibres maritimes…), effraction d'information (divulgation involontaire, publication de mots de passe…), etc.

Le *cognitive warfare* correspond à l'art d'utiliser les technologies pour altérer la cognition de cibles humaines, le plus souvent à leur insu et à l'insu de ceux qui seraient en charge d'éviter, minimiser, contrôler les effets recherchés, ou dont un contrôle possible serait dépassé ou trop tardif.

1.1 QUELQUES MOTS DE DEFINITION

La « *guerre cognitique* », ou *cognitive warfare,* est donc une guerre non conventionnelle qui s'appuie notamment sur les outils cyber et dont le but est d'altérer les processus cognitifs d'ennemis, d'exploiter des biais ou des automatismes, mentaux, de provoquer des distorsions des représentations, des altérations de décision ou des inhibitions de l'action, et entraîner des conséquences funestes, tant du point de vue des individus que du collectif. Le nom composé est utilisé préférentiellement dans sa version anglaise plutôt que sa traduction littérale qui reste ambiguë.

La notion est à rapprocher de celle de « guerre informatique » (*cyber warfare*) qui utilise les moyens numériques de l' « information », et ambitionne leur maîtrise, leur altération ou leur destruction. Néanmoins, elle ne s'attache pas au strict champ de l' « information » mais à celui de la « cognition », c'est-à-dire à ce que le cerveau fait de cette information. Elle n'est donc pasréductible au simple volet des conséquences humaines

[1] Bernard Claverie est professeur des universités, directeur honoraire et fondateur de l'Ecole Nationale Supérieure de Cognitique – Institut Polytechnique de Bordeaux (France) – et chercheur au CNRS – UMR5218 – Université de Bordeaux.

[2] François Du Cluzel de Remaurin est colonel de cavalerie (retiré) et coordinateur et chef de projets innovants de l'*Innovation Hub* NATO ACT – à Norfolk (Virginie – USA).

d'une « cyber guerre » de l'ingénierie des ordinateurs, des robots et des programmes ; l'effet cognitif n'est pas une conséquence de l'action, il en est le but.

Ce but est à considérer indépendamment des technologies. On pourrait parler de « guerre psycho-socio-technique » qui associe les aspects d'une part de « guerre cyber-psychologique » et d'autre part de « guerre d'influence » conduite grâce aux moyens cybernétiques. C'est, plus concrètement dans le domaine militaire, la mise en œuvre d'une stratégie visant à la réalisation d'une action guerrière, de surveillance ou de sécurité.

Certaines définitions découlent de cela. Ainsi, la notion de « combat cognitique » relève de la mise en œuvre concrète, locale et temporaire, d'outils tactiques concernant la cognition. Cela s'inscrit dans le cadre d'une stratégie plus globale de « lutte cognitique ». On peut évoquer, pour ce qui estde l'attaque, un état d'esprit vers le harcèlement, l'exploitation systématique de faiblesses ou, au contraire pour ce qui est de la défense, la mise en œuvre de capacités de résilience et de prévention utilisant ou ayant recours à des outils de même nature. On parlera de « conflit cognitique » dans le cadre de la généralisation des luttes et de la confrontation des processus dans un équilibre qui, pour l'heure, reste à théoriser.

1.2 LA *COGNITIVE WARFARE* EST PARMI NOUS

Le cognitive warfare est une pratique exploitée avec plus ou moins d'excellence, et peut-être sans la nommer encore ainsi, par des états ou par des acteurs non étatiques, institutions ou entreprises, organisations terroristes, mouvements religieux belliqueux ou sectaires, etc. Elle est bien sûr utilisée et mise en œuvre par des unités spécialisées, souvent fort compétentes, de grands services de renseignement numérique, mais également par des agences et des firmes industrielles dans le cadre de leur concurrence ou dans le domaine plus prosaïque du marketing et de la manipulation d'une clientèle potentielle. Dans tous les cas, il s'agit d'asservir ou d'affirmer une supériorité, voire de conquérir et parfois anéantir, et cette pratique atteint aujourd'hui une dimension remarquable pour que les décideurs politiques se saisissent de son importance critique.

Historiquement, le terme *cognitive warfare* est utilisé dans ce sens depuis 2018 par les États-Unis qui désignent plus précisément les moyens d'action qu'un état ou un groupe d'influence utilise *« pour manipuler les mécanismes spontanés de la cognition d'un ennemi ou de son peuple, pour l'affaiblir, le pénétrer, l'influencer, voire le soumettre ou même le détruire »*. Bien que partie intégrante de l'art militaire, il s'agit, dans cette acception, d'un champ disciplinaire nouveau, qu'il convient de mieux identifier. Il est issu à la fois issu des techniques cyber de l'*information warfare*, et du volet humain de « *soft power* » ou d'influence, avec les ambitions de manipulation des PsyOps. Il s'agit le plus fréquemment de présentation biaisée d'une réalité, le plus souvent numériquement manipulée, pour faciliter ou valoriser ses propres intérêts. Et les nouveaux moyens de communication offrent aujourd'hui des possibilités infinies, ouvrant la voie à de nouvelles méthodes et autorisant de nouveaux objectifs. Cette complexité doit engager les victimes potentielles à une posture de résilience permanente au risque, comme c'est souvent le cas, d'une prise de conscience trop tardive.

Cette démarche de *cognitive warfare* prend aujourd'hui une dimension militaire globale, et couvre àla fois le volet stratégique et un ensemble de dimensions opérationnelles, plus ou moins codifiées. Elle échappe pour l'heure aux règles et aux doctrines éthiques établies. Elle a connu une poussée remarquée avec l'avènement de la numérisation de l'aide à la décision stratégique, celle des champsopérationnels et l'envahissement des *big data* et des *analytics*, pour l'information, le *wargaming* et la conduite d'opérations. Elle envahit progressivement tout le champ de l'usage numérique, et permet de manière silencieuse la mise en œuvre des dimensions d'ingérence et de contre-ingérence, d'attrition cognitive et de défense des populations qui y seraient soumises. Il s'agit donc à la fois d'un ensemble raisonné de processus d'attaque mais également de contremesures et de mesure préventives.

1.3 THEORISATION

On commence à voir apparaître des théorisations qui abordent à la fois des notions comme la résilience ou la faiblesse en « neurosciences », l'utilisation des « biais cognitifs » et la propension spontanée à l' « erreur cognitive », à la manipulation des perceptions, à la saturation ou à la tunnellisation attentionnelles, et à l'induction du stress cognitif. Les conséquences sont prévisibles sur l'aptitude et le dépassement des opérations mentales, sur les relations sociales et les motivations, et sur la désorganisation institutionnelle.

Ce début de mouvement conceptuel rencontre l'intérêt de plusieurs scientifiques et militaires. Ainsi, parmi tant d'autres, le nanotechnologue et neuroéthicien Giordano[3] a-t-il décrit « le cerveau comme le champ de bataille du XXIe siècle » et formule une hypothèse de *weaponization of neuroscience*s, le général Goldfein[4] déclare que nous sommes passés des guerres d'usure aux « guerres de cognition », le Colonel Banach[5] propose la notion de « guerre virtuelle », le lieutenant-général Stewart[6] de la Defense Intelligence Agency, déclare que *« la guerre moderne est une bataille cognitive »* et le Général Desclaux[7] théorise le processus stratégique de *command and control* comme un triangle cognitif impliquant à la fois la dominance de la connaissance représentationnelle (*knowledge dominance*), la performance cybernétique massive (*cyber confidence*) et la supériorité décisionnelle hybride (*decision superiority*) pour guider la stratégie au service des ambitions du commandeur. Alors que « le rôle du cognitif dans la planification et la conduite des opérations » devient fondamental, le colonel Remanjon[8] du commandement pour la transformation de l'OTAN s'interroge pour savoir si « le cerveau humain sera-t-il l'ultime champ de bataille ? ».

Une théorisation de ce sixième domaine de la guerre a été récemment développée, selon le rapport du « technium », ensemble des technologies, à la « noosphère »[9] conçue comme dimension globale de l'intelligence humaine médiée par les technologies, dans un récent ouvrage sur la *cognitive superiority* dû à l'expert en management Hartley[10] et au psychiatre Jobson[11] (2021).

1.4 LES PRINCIPES

Le *cognitive warfare* représente la convergence de tous les éléments de l'information warfare en l'élargissant à des notions opérationnelles de psychologie et de neurosciences, basées sur lesthéories systémiques et de la complexité, au service de l'action guerrière. On se place à l'interface des deux champs opérationnels gérés jusqu'ici de manière séparée : d'une part les Opérations Psychologiques (PsyOps) et opérations d'influence (*soft power*), et d'autre part les cyber-opérations (technologies de cyberdéfense) qui tentent à l'atteinte d'intégrité des moyens physiques d'information ou à leur destruction. Cette interface permet une unification

[3] James Giordano est professeur au département de neurologie de l'université Georgetown à Washington (Washington DC, USA) et directeur du *« Neuroethics Studies Program » du « O'Neill-Pellegrino Center for Clinical Bioethics ».*

[4] David Goldfein est général et chef d'état-major de l'US Air Force. Il est membre de l'état-major interarmées américain et conseiller militaire du Conseil de sécurité nationale, du secrétaire à la Défense et du président des États Unis.

[5] Steve Banach est colonel de l'US Army. Il est l'ancien directeur de la *« School of Advanced Military Studies »* (SAMS) à Leavenworth (Kansas, USA).

[6] Vincent R. Stewart est Lieutenant Général de *l'US Marine Corp*, directeur de la *Defense Intelligence Agency (DIA)*.

[7] Gilles Desclaux est général de corps aérien en deuxième section. Il a été commandeur des opérations aériennes pendant la guerre de Libye et contribue aujourd'hui à des travaux industriels sur le C2.

[8] Jérôme Remanjon est colonel de cavalerie, directeur du groupe d'action, études, cohérence, synthèse du Commandeur au NATO *Allied Command Transformation* (ACT).

[9] Au sens de Kelly (2011) : ensemble de l'information disponible pour les cerveaux humains.

[10] Dean S. Hartley III directeur de cabinet conseil (*Hartley Consulting*) à Oak Ridge (TN, USA) et Président honoraire de plusieurs groupes de conseil pour l'entreprise.

[11] Kenneth O. Jobson est docteur en psychiatrie, créateur de l'International Psychopharmacology Algorithm, acteur du domaine de la biotechnologie.

de concepts et de points de vue de différentes communautés d'intérêts scientifique, militaire ou du renseignement, une formed'interdisciplinarité de l'action technologique sur l'homme.

Le principe majeur n'est pas uniquement d'accompagner une stratégie et de gagner sans se battre, c'est aussi une guerre contre ce que pense, aime ou croit une communauté ennemie en modifiant sesreprésentations du réel. C'est donc une guerre contre ses façons de penser, ses logiques mentales,ses représentations spontanées et ses processus conceptuels. Les conséquences recherchées sontd'en altérer la représentation du monde, mais aussi par conséquent la quiétude, les certitudes, la compétitivité ou la prospérité.

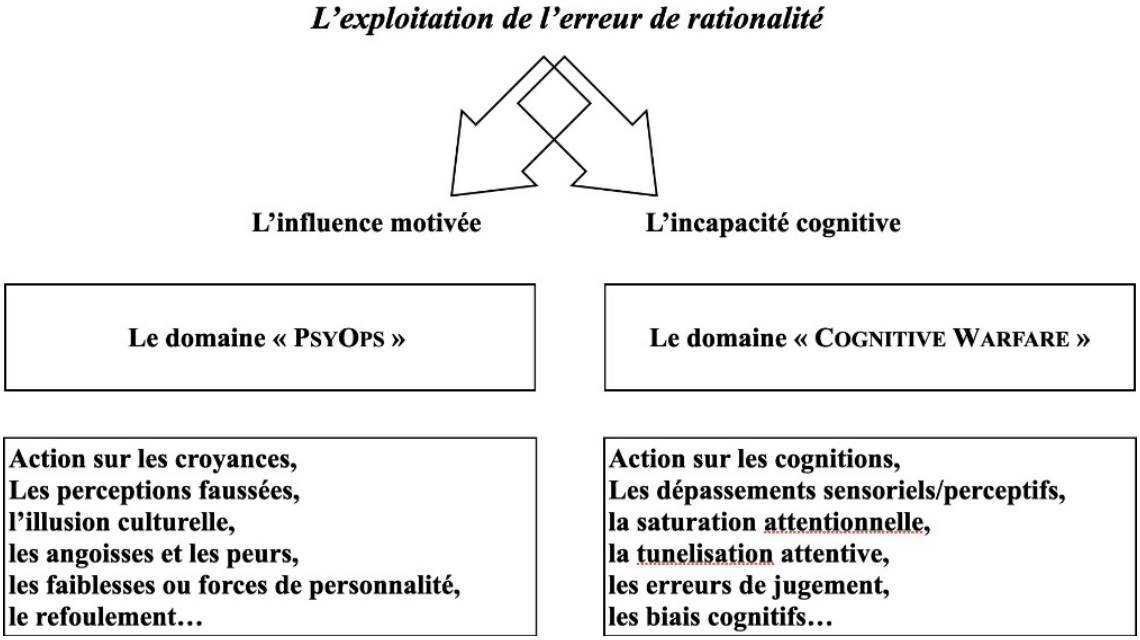


Figure 1-1 : Différentiation des domaines *cognitive warfare* et PsyOps (dans lesquelles on englobe de manière simplifiée es « opérations psychologiques » proprement dites, et d'autres actions non kinétiques telles que les actions d'influence et les coopérations Civilomilitaires (CiMiC).

L'objectif affiché est d'attaquer, exploiter, détériorer voire détruire les représentations, le tissu de la confiance mentale, celui de la croyance en des logiques établies nécessaires au fonctionnement sain d'un groupe, d'une société, voire d'une nation. Bien qu'il s'en distingue par son côté technique (cyber), le *cognitive warfare* est un compagnon des Opérations Psychologiques (PsyOps).

1.5 LES NIVEAUX DE L'ACTION

Le *cognitive warfare* peut être étudié à deux niveaux : celui de l'attitude globale, celui des outils disponibles. Le premier est caractérisé par sa contribution à une culture de la manipulation des esprits, ou au contraire à une culture de résilience et de sécurité globale. Il s'agit alors à la foisd'une information et d'une formation des personnes susceptibles d'être la cible d'intention ou d'action malveillantes, mais également d'utilisation d'outils cognitifs de contre ingérence.

Le domaine repose à la fois sur les connaissances de la psychologie des acteurs, de la psychosociologie des populations et des groupes restreints, ainsi que de l'influence culturelle sur la rationalité des acteurs. Le second niveau concerne plus précisément plusieurs domaines de l'action cognitique. On peut en citer plusieurs chapitres tels que la décision et l'indécision, l'erreur et les biais cognitifs, la perception et l'illusion,

la cybernétique et l'absence ou la rupture de contrôle, l'influence et le soft power, la psychologie et la cyber psychologie, la collaboration usager-système, la robotique et les drones, l'autonomie et l'éthique technologique, la motivation aux usages et le découragement (abandon, désespoir), les morales et les conflits de valeurs, la psychologie et la religion, l'urgence médico-psychologique, post traumatique ou du passage à l'acte, la cybersécurité et la fiabilité humaine, ainsi que les dimensions cognitives du C2 qui semblent embrasser nombre des autres, notamment dans ses dimensions multi-domaines et multiculturelles.

1.6 ATTITUDE DE DEFENSE

Ce type d'approche cognitique n'est pas à considérer selon les classifications classiques des instruments de la guerre, mais plutôt comme des outils de perturbation d'individus ciblés ou de masse, pour qu'elle puisse avoir des effets d'entraînement à plusieurs échelles, de l'homme seul au système sociotechnique dans son entier. Les capacités et effets perturbateurs sont utiles en amont, pendant et après les engagements cinétiques, tout en échappant encore aujourd'hui auxréglementations internationales pour pouvoir être définis comme des actes de guerre. Ces actions « non cinétiques » contribuent à créer des déséquilibres à l'avantage de l'auteur et des inconvénients pour la ou les cibles. Mais aujourd'hui elles sont capables d'être les éléments d'une action globale, discrète, voire invisible, ou d'actions ponctuelles, précises et indétectables, constituant les seuls éléments d'une ou d'un ensemble d'opérations agressives, appelant à une prise de conscience de leur danger et à l'usage de techniques de défense et de menace efficaces pour pouvoir les parer et paliers leurs éventuelles conséquences.

1.7 VERS UN DOMAINE HUMAIN

Quelles en sont ces conséquences ? L'ère de l'information a évolué en une ère des réseaux, le mondeétant de plus en plus défini et façonné par des techniques interconnectées. Cette évolution entraîne de nouvelles complexités à mesure que les moi physique, moi numérique et moi mental fusionnent au sein de ces réseaux « anthropotechniques ». Ils sont une marque du domaine humain – le domaine où la résolution de problèmes complexes dépend essentiellement de la représentation, de lacompréhension et de la conception de l'information. Ce domaine doit tenir compte des forces, des limites, des vulnérabilités et de la diversité des individus pris dans des opérations de décision ou d'application de consignes et procédures.

Les défis de défense sont nombreux ; qu'il s'agisse d'assurer la sécurité cognitive des individus afin de préserver le fonctionnement des états, de gagner et maintenir la supériorité cognitive pourl'action et la compétitivité, de prévoir et de certifier les performances des systèmes intelligents ou d'Intelligence artificielle développés afin de soutenir le travail humain, d'augmenter l'« intelligence collective » du rapport homme-système (HAT pour *Human Autonomy Teaming*), pour améliorer la prise de décisions complexes et partagées. Assurer la garantie d'un avantage dans le domainehumain nécessite de nouvelles approches permettant de combiner plus efficacement l'humain et la technologie, et de maîtriser les conséquences à la fois techniques et psychologiques.

1.8 LES MOYENS DE L'ACTION

Depuis une vingtaine d'années, la conception des outils numériques a su prendre en compte les différences et les caractéristiques des utilisateurs pour leur faciliter des usages spontanés. Cette compétence a aiguisé les esprits pour que ces comportements guidés soient manipulés afin d'amener l'humain à une meilleure intégration avec le système. Aujourd'hui, l'intention n'est plus simplement facilitatrice, mais incitatrice, voire impérative.

L'action la plus efficace, pour l'attaquant, mais la plus difficile pour lui, consiste donc à promouvoirdes outils numériques qui engendrent des disruptions ou atteintes des processus cognitifs desennemis, à différents niveaux. Les différentes étapes de la décision sont visées, depuis la prise d'information, qui peut être saturée, en passant par le filtrage, dont les capacités peuvent être dépassées, en altérant la construction de représentations, en influant sur les stocks mnésiques, en induisant des décisions inadéquates, ou en paralysant la prise de décision et la programmation des réponses, jusqu'à la paralysie de l'action ou le mauvais ajustement de l'objectif attendu. Chacune de ces étapes est aujourd'hui connue, codifiée, voire substituée par des outils numériques. Il est donc simple de les atteindre par cette voie.

Les relations entre les domaines d'action :

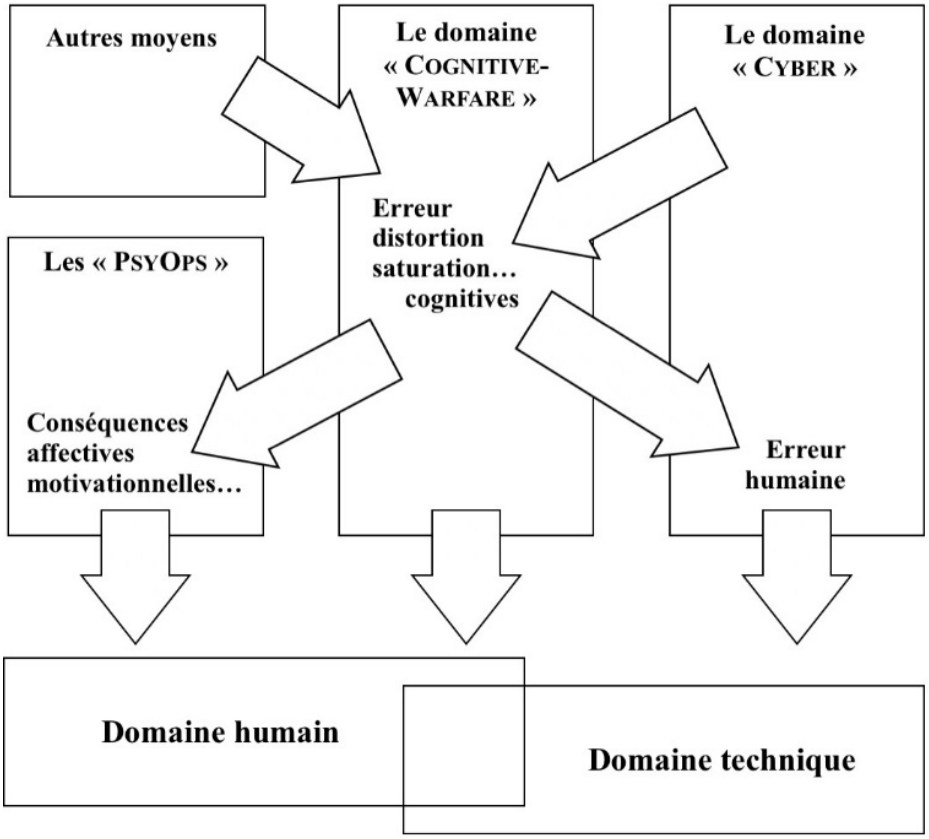


Figure 1-2 : Complémentarité du domaine humain et du domaine technique, et relations qu'ils entretiennent avec les domaines d'action de la guerre *cyber warfare*, *cognitive warfare* et PsyOps.

Les conséquences attendues le sont aujourd'hui à trois niveaux potentiels :

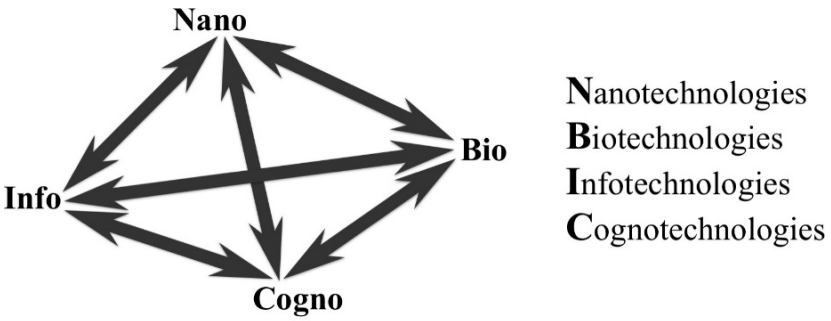
1) Une influence sur les dimensions psychologiques, affectives, motivationnelles, sur la certitude ou le doute, sur la chronicisation des conséquences ;
2) Sur le domaine cyber par factorisation ou induction directe d'erreur humaine entraînant une atteinte du réseau, des informations qu'il supporte ou des interfaces homme-système ; et
3) Directement sur les aptitudes cognitives des individus dont les moyens et capacités cognitives sont altérés de manière chronique.

Mais la guerre des esprits va prendre de nouvelles dimensions avec le développement des technologies embarquées et des objets connectés, et surtout avec l'intégration intra corporelle de ces derniers avec l'avènement du soldat augmenté.

1.9 PREPARER LE FUTUR AVEC LE CYBER-EMBARQUE

Les NBIC sont un projet scientifique qui engage à la convergence de quatre domaines jusqu'ici dissociés : les nanotechnologies (*nanorobotical technology, nanosensors, nanostructures, energy…*), les biotechnologies (*bio-genomic technology, Crisp-Cas9, neuropharmacology…*), l'informatique (*information technology, computer science, microelectronics…*) et la cognitique (*cognitive technology, cognitive science and neuropsychology).* Ce projet a été formalisé en 2002 grâce au Département de la défense américain, puis a été suivi par les grandes institutions internationales et les grandes nations, pour la convergence des technologies du futur.

Il s'agit de promouvoir le développement d'outils et l'adaptation, voire le perfectionnement d'individus grâce à un réel rapprochement anthropotechnique, une hybridité homme-système, pour des ambitions de santé, de sécurité, de défense et d'adaptation à de nouveaux biotopes (espace, mer, déserts…). Aujourd'hui, et grâce à ce projet, on assiste à des convergences partielles des domaines, principalement deux à deux : avec de l'informatique et des nanotechnologies de santé, de nouveaux produits chimiques d'amplification de la cognition, de l'électronique implantée, etc. Le projet est à terme d'avoir un opérateur humain augmenté, voire hybride, embarquant des substances ou des nanotechnologies d'amplification, de résistance et de supériorité informationnelle. On connaît déjà des projets d'un soldat augmenté.



NBIC technologies tetrahedron

Figure 1-3 : Technologies convergentes telles que définies pour le DoD des Etats-Unisdans le rapport de Roco et Bainbridge (2012).

Qui dit information, dit cyber menace et détournement ou manipulation. Et lorsqu'il s'agit du cerveau connecté, notamment celui du combattant et de l'action qu'on peut envisager sur lui, ou desprotections qu'on peut lui appliquer, il s'agit d'un volet offensif et d'un volet défensif de *cognitive warfare*. De nombreux auteurs ont anticipé ces menaces. Pour l'heure, elles sont encore pour la plupart du domaine de la *science-fiction*, mais on commence à voir apparaître des projets qui sont très sérieusement programmés, voire déjà concrètement testés, notamment sur l'implantation neurocomputionnelle ou l'hybridation technique d'amplification perceptive (vision, audition), voire sur les modifications de génomes.

Au-delà de la menace plus traditionnelle, et très actuelle, du *cognitive warfare* au service d'États alliés ou concurrents, et de ce que peuvent développer des entités non officielles de type terroristeou d'ambition de suprématie culturelle ou religieuse, il convient de s'intéresser au futur du NBIC, età son volet d'influence sur la cognition humaine, par détournement, saturation, ou même, on peut l'envisager, prise de contrôle et détournement d'objectif. Une mention doit être faite du problème de l'obsolescence des implants et de son exploitation.

1.10 CONCLUSION

Le monde cyber est caractérisé par sa pervasion, sa diffusion généralisée, et l'impossibilité quetoute action ou toute décision puisse être menée sans ses outils. Cet usage n'est pas sans conséquences sur les opérations cognitives des individus qui les utilisent ou y sont soumis. Ces conséquences sont individuelles et collectives, et les effets recherchés sont à concevoir à tous les niveaux, tant du côté psychologique, avec des conséquences humaines, que cyber par altération involontaire des systèmes par erreur humaine. Ce domaine est en plein développement, et de nouvelles pistes viennent concrètement bousculer les frontières de la connaissance et des usages actuels. La première des prudences est d'anticiper l'ensemble des menaces que les technologies du proche futur vont nous amener, et nous amènent déjà pour certaines, à connaître.

Ces menaces seront de plus en plus fréquentes, et leurs conséquences se manifesteront de manièrede plus en plus globale, amenant l'OTAN et les nations de l'alliance à anticiper les différentes dimensions de la guerre cognitive. Les anticiper revient à se donner les moyens de dépasser le risque de la seule réaction, sans avoir l'initiative technologique qui devient, chaque jour un peuplus, une notion essentielle de la stratégie militaire.

1.11 BIBLIOGRAPHIE

Claverie, B. (2021). Des Théories Pour la Cognition : Différences et Complémentarité des Paradigmes. Paris (France) : L'Harmattan.

Cole, A., Le Guyader, H., (2020). Cognitive, a 6th Domain of Operations? Norfolk VA, USA : Innovation Hub, NATO ACT Edition.

Devilliers, L. (2021). Désinformation : les Armes de l'Intelligence Artificielle. Pour La Science, 523, 26-33.

Hartley, D.S.III, Jobson, K.O. (2021). Cognitive Superiority : Information to Power. New-York (NY, USA) : Springer.

Kelly, K. (2011). What Technology Wants. New York (NY, USA) : Penguin Books. ISBN : 978-0143120179.

Roco, M.C., Bainbridge, W.S. (2003). Converging Technologies for Improving Human Performance : Nanotechnology, Biotechnology, Information Technology and Cognitive Science. NY, USA : Springer-Verlag.

Underwood, K. (2017). Cognitive Warfare Will Be Deciding Factor in Battle : Lt. Gen. Stewart's Remarks at DoDIIS17. Signal, The Cyber Edge. https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle; https://www.youtube.com/watch?v=Nm-lVjRjLD4.

Wall, T. (2010). U.S. Psychological Warfare and Civilian Targeting. Peace Review 22, 3: 288-294.

Chapitre 2 – LE DOMAINE COGNITIF – UN SIXIEME DOMAINE D'OPÉRATIONS ?

Hervé Le Guyader[1]

« Ce sixième domaine, celui de l'influence et de la manipulation, est celui qui permet à l'adversaire de faire l'économie de tout affrontement ouvert, toujours coûteux, souvent hasardeux. »

2.1 L'INVENTION DU SIXIEME DOMAINE

L'idée d'un sixième domaine a émergé au début de l'année 2020. Elle a été présentée comme la toute première recommandation énoncée dans l'essai Weaponization of Neurosciences (Le Guyader, 2000) écrit dans le cadre de l'étude Warfighting 2040 lancée par le Allied Command Transformation (ACT) fin 2019.

Les trois recommandations figurant dans le résumé de cet essai étaient les suivantes :

- "Human mind" should be NATO's next domain of operations.
- AWACS successor must address NBIC.
- Global security is what's at stake today.

À la suite de cette première publication, ACT a demandé qu'une suite soit écrite, toujours dans le style dit de Fiction intelligente (FICINT), de sorte que l'hypothèse de l'adjonction d'un nouveau domaine d'opérations aux cinq domaines existants (terre, mer, air, cyber et espace) y soit développée plus avant.

C'est ainsi que l'essai « Cognitif : Un sixième domaine d'opérations ? » fut publié, en version bilingue, Anglais et Français (Cole et Le Guyader, 2020 ; Le Guyader et Cole, 2020)[2].

S'inscrivant dans le contexte plus large de l'étude Cognitive Warfare menée par l'Innovation Hub d'ACT, l'idée de la nécessité de la création d'un sixième domaine d'opérations fait ainsi son chemin au plus haut niveau de l'OTAN. Rejoignant en cela la troisième recommandation de l'essai précédent (c'est de sécurité globale, civile comme militaire, qu'il s'agit). Le concept de sixième domaine trouve également un écho dans les médias généralistes (Orinx et Struye de Swielande, 2021 ; Le Guyader, 2021).

La définition du périmètre précis de ce sixième domaine – doit-il s'agir du « simple » domaine cognitif ou, d'une façon plus large, d'un « domaine humain » ? – reste, cela dit, en suspens.

C'est la seconde approche (domaine humain) qui est privilégiée par l'essai Cognitif : Un sixième domaine d'opérations, pour des raisons que vient résumer l'extrait suivant, issu de son premier chapitre, un échange entre le général Weaver (SACT) et le professeur Béthany :

> *« Ce 'Domaine Humain', est-ce une autre façon de baptiser ce « domaine cognitif », dont on me rebat les oreilles ces temps-ci ? » demanda le général. En voyant le regard de Weaver s'évader vers les toits, Béthany comprit qu'il était en train de perdre l'attention de son ami, le général étant déjà convaincu de l'importance du concept de « guerre cognitive ».*

[1] Hervé Le Guyader est ingénieur diplômé de l'École nationale supérieure d'électrotechnique, d'électronique, d'informatique, d'hydraulique et des télécommunications. Il a créé puis dirigé le Centre Européen de la Communication, puis a intégré l'Ecole Nationale Supérieure de Cognitique – Institut Polytechnique de Bordeaux (France) – comme chargé de l'innovation. Il est membre du Panel IST de la STO et participe aux travaux de l'innovation Hub du NATO ACT. Hervé Le Guyader est expert judiciaire près la Cours d'Appel et près la Cours Administrative d'Appel de Bordeaux.

[2] L'Anglais et le Français sont les deux langues officielles de l'OTAN.

« Non. Bon, forcément, ça en fait partie, mais se borner à créer un « simple » domaine cognitif, ce serait trop restrictif, même si le terme passerait sûrement bien. Je sais que le cerveau, ce « bout de bidoche interconnecté » – Béthany mimant à nouveau des guillemets avec ses mains – cette machine extraordinaire à fabriquer de la pensée a pu inciter certains à recommander l'ajout d'un domaine cognitif aux cinq domaines d'opérations actuels del'OTAN. On m'a même invité à me joindre à cette petite coterie, mais cela ne prendrait vraiment pas le problème au bon niveau. Bien sûr, la cognition est un élément vital du processus de prise de décision et est un facteur contributif important, capable d'induire certains types de comportements à un niveau individuel ou collectif mais, quitte à vraiment perturber vraiment les esprits, ce que l'on peut appeler « les armes cognitives » ne représentent qu'une partie de l'arsenal que développent nos adversaires aujourd'hui.

Ajouter un 'domaine cognitif' à la liste des domaines d'opérations de l'OTAN, ça ferait sûrement les titres des journaux et ça paraîtrait cool, mais ça ne tiendrait pas la route longtemps ! » …

« Mais enfin, qu'entends-tu précisément par Domaine Humain ? », demanda le général Weaver, un peu déconcerté.

« OK, H.P., je tente le drop : le Domaine Humain, c'est celui qui nous définit en tant qu'individus et qui structure nos sociétés. Pas de chance, il présente une complexité spécifique, liée à la diversité des sciences qui lui sont sous-jacentes, notamment celles qui intéressent le plus nos adversaires dans la recherche qu'ils mènent pour identifier noscentres de gravité, nos vulnérabilités. Dans le désordre, je citerai : histoire, géographie, sciences politiques, biologie, sciences cognitives, commerce, médecine et santé, psychologie, démographie, économie, sciences de l'environnement, sciences de l'information, études internationales, droit, linguistique, gestion, médias, philosophie, systèmes électoraux, administration publique, relations internationales, politique internationale, religion, sciences de l'éducation, sociologie, arts et culture… »

2.2 LES QUATRE QUESTIONS QUI SE POSENT.

2.2.1 Qu'est-ce qu'un « domaine d'opérations » pour l'OTAN ?

Alors que l'on trouve sans difficulté une telle définition au niveau national (notamment aux US), on n'en trouve paradoxalement pas dans la littérature otanienne, fût-ce dans les cinquante et quelques documents composant sa doctrine. Le concept de « domaine » est toutefois présenté dans son document fondateur Comprehensive Operations Planning Directive (Collectif, 2010), mais les domaines qui y sont identifiés, constitutifs de l'acronyme PMESII, désignent les domaines politique, militaire, économique, social, infrastructure et information.

Face à ce manque étonnant de définition au plus haut niveau, certains auteurs en ont proposé certaines, notamment celles-ci :

- *A domain is a space in which forces can manoeuvre to create effects* (Garreston, 2017).
- *The sphere of influence in which activities, functions, and operations are undertaken toaccomplish missions and exercise control over an opponent in order to achieve desired effects* (Allen et Gilbert, 2018).
- *Critical macro manoeuvre space whose access or control is vital to the freedom of action and superiority required by the mission* (Donnelly et Farley, 2019).

Paradoxalement encore, on assiste aujourd'hui à une véritable compétition entre différents candidats souhaitant être retenus comme le « 6e domaine d'opérations » de l'OTAN. En dehors du « domaine cognitif » et du « domaine humain », le « domaine électromagnétique » ou le « domaine de l'information » comptent ainsi de nombreux et très motivés avocats.

2.2.2 Le Domaine Humain répond-il aux 6 critères établis par la John Hopkins University ?

Le document d'Allen et Gilbert cité plus haut, tout en défendant la thèse de l'accession au rang de domaine d'une « sphère de l'information » a le grand mérite de proposer une grille d'analyse fondéesur les six critères que doit remplir un « candidat » pour pouvoir prétendre à la qualité de domaine :

- Des capacités spécifiques sont requises pour pouvoir opérer dans ce domaine ;
- Le domaine ne peut pas être entièrement inclus dans un autre domaine ;
- Des capacités amies et ennemies peuvent être conjointement trouvées dans ce domaine ;
- Un contrôle de ce domaine peut être exercé ;
- Le domaine offre des possibilités de synergie avec d'autres domaines ; et
- Le domaine offre des possibilités d'actions asymétriques sur d'autres domaines.

Domaine humain comme domaine cognitif répondent tous deux à l'ensemble de ces six critères, mais on peut avancer que le second critère (« Le domaine ne peut pas être entièrement inclus dans un autre domaine ») est particulièrement pertinent, s'agissant d'une « compétition » entre domaine cognitif et domaine humain. On peut en effet soutenir que le domaine cognitif est entièrement inclus dans le domaine humain.

2.2.3 Qu'est ce qui « clocherait » avec un « domaine cognitif » ?

Au-delà de la citation faite supra tirée du premier chapitre de l'essai Cognitif : Un sixième domaine d'opérations, on avancera les points suivants :

- Ajouter un domaine ne saurait être fait « à la légère » et, tant qu'à faire, la sélection entre des candidats doit être impitoyable.
- La dimension cognitive constitue bien évidemment une partie essentielle du domaine humain (pris au niveau individuel comme au niveau collectif), mais une personne, une communauté, peuvent-elles être uniquement définies pas ses capacités cognitives ?
- Quid, par exemple, des biotechnologies ou nanotechnologies ?
- Ces technologies ne représentent-elles pas un ensemble de menaces potentielles et, si oui, ces menaces sont-elles prises en compte par les cinq domaines existants ?
- Le seraient-elles par un « domaine cognitif » ?

2.2.4 Quel serait le risque si on en restait aux cinq domaines actuels ?

Qu'il s'agisse des grandes tendances technologiques, telles que résumées par le Dr. Bryan H. Wells, Directeur Scientifique de l'OTAN dans sa présentation faite à la conférence ICMCIS'21 (Wells, 2021), des synergies entre Technologies Emergentes Disruptives (EDT en anglais) et de leurs calendriers respectifs, il suffit de prendre la peine de réfléchir au poids des considérations humaines (facteur humain) associées à ces grandes tendances pour se persuader du risque existentiel qui résulterait d'une approche purement technique, c'est-à-dire d'une approche qui n'intégrerait pas, de façon pluri et interdisciplinaire, les sciences humaines et sociales.

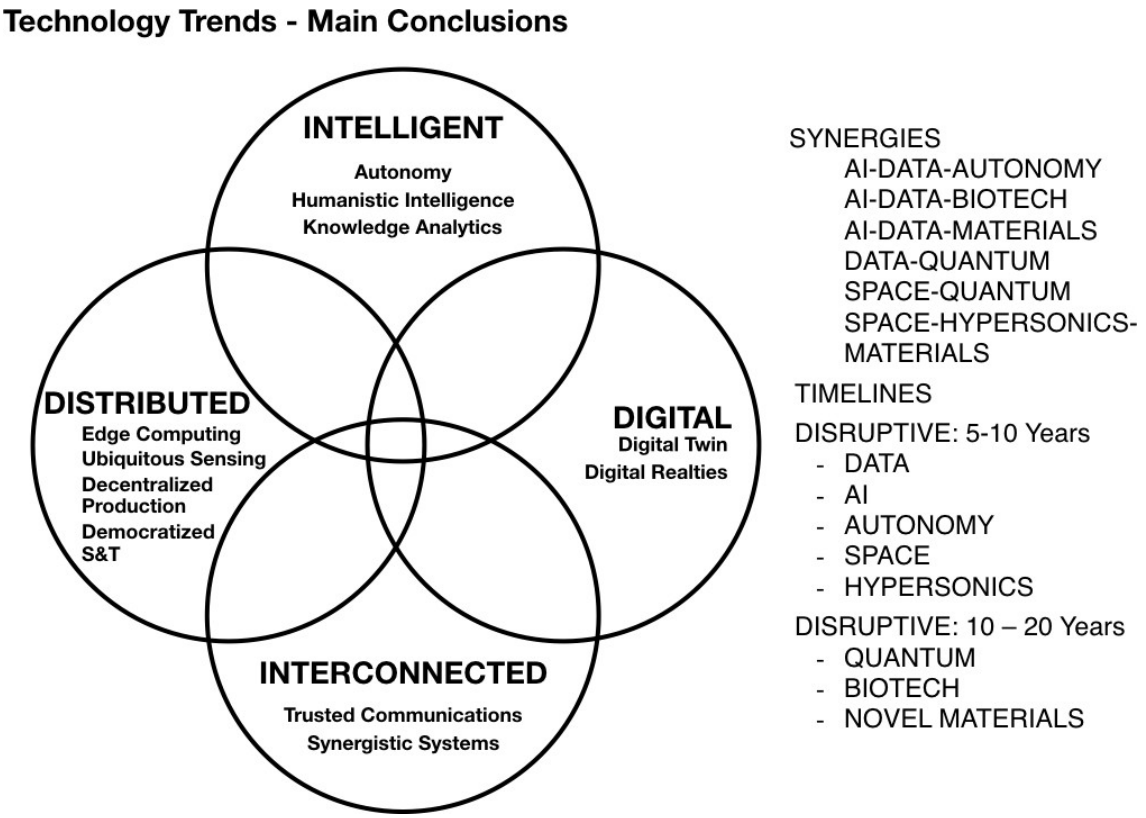


Figure 2-1 : Représentation multidisciplinaire de l'approche DOTMLPF(d'après Wells, 2021).

Et l'on citera, pour mémoire, les nouvelles formes de conflit – « hybride », « sous le radar », « ambigu », « guerre et paix simultanées », « non-guerres » … ainsi que les approches chinoises (théorie des « trois guerres » : i) Opinion, ii) Psychologique et iii) Légal) ou russes (Gerasimov, 2013).

2.2.5 La spécificité d'un Domaine Humain

On apportera tout d'abord les deux remarques suivantes :

- Les cinq domaines actuels ne sont pas, entre eux, « orthogonaux » : des avions décollent de navires et leurs pilotes recourent à des procédés cyber ; des forces spéciales agiront tout aussi efficacement dans les quatre domaines, des navires rejoindront un port terrestre, etc. ; et
- Aux cinq domaines actuels correspondent des acteurs industriels gigantesques qui, avec leurs centaines de sous-traitants, représentent des enjeux stratégiques et de compétitivité directe, ainsi qu'en matière financière et en matière d'emploi.

Le sixième domaine, le domaine humain diffère profondément des cinq autres en cela

- Qu'il est un domaine d'opérations en tant que tel (cf. paragraphe supra) ; et
- Qu'il constitue la matrice de l'ensemble des autres domaines, dont l'existence est entièrement liée au – et justifiée par – ce sixième domaine.

Il s'agit d'un domaine dont les contours sont, d'un point de vue topologique, intéressants.

2.2.6 Quelle suite ?

À cette question, on répondra en pointant certaines des difficultés devant être affrontées et en apportant une suggestion de nature opérationnelle.

On rappellera tout d'abord qu'une fois un domaine créé, il convient d'en implémenter l'approche opérationnelle, ce qui se traduit par la mise en place de lignes d'action autour des questions de *doctrine, organisation, training, matériel, leadership, personnel* et *facilities* ou DOTMLPF (cf. Fly, 2009).

À ces considérations génériques viendront se greffer des questions complexes, qui vonts'appliquer :

- Au niveau scientifique, notamment en matière d'interdisciplinarité (« sciences dures » vs. SHS). Il n'est que de penser à la question d'une représentation partagée en matière de données SHS.
- Au niveau technique : Bien sûr, on parle ici d'un « système de systèmes », mais les questions de i) Fusion multi-domaines, particulièrement ardues, ne serait-ce que par la très grandedisparité des constantes de temps applicables aux différents domaines (dans le domaine humain, les choses se passent tant sur plusieurs générations qu'en une picoseconde) ; de ii) Visualisation ; et iii) D'outils d'aide à la décision sont particulièrement ardues.
- Au niveau ressources humaines, que ce soit en matière de recrutement comme en matière de formation/entraînement.

Face à ces réelles difficultés mais aussi face à la nécessité d'agir, utiliser le projet Allied Future Surveillance and Control (AFSC), paraît constituer une approche opérationnelle particulièrement pertinente, car :

- L'AFSC doit prendre la suite de l'AWACS dès 2035 ;
- L'AFSC doit intégrer l'approche interdisciplinaire résumée supra ; et
- En concevant ainsi l'AFSC, l'approche DOTMLPF en résultera naturellement.

2.3 BIBLIOGRAPHIE

Allen, P.D., Gilbert, D.P. (2018). The Information Sphere Domain Increasing Understanding and Cooperation. Tallinn (Estonie): The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. https://www.ccdcoe.org/uploads/2018/10/09_GILBERT-InfoSphere.pdf.

Garretson, P. (2017). USAF Strategic Development of a Domain. Over The Horizon (OTH) Journal, 10 juin 2017. Montgomery (AL, USA): Air Command and Staff College. https://othjournal.com/2017/07/10/strategic-domain-development/.

Gerasimov, V. (2013). The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Military-Industrial Kurier, 27 février 2013. Traduction du Russe à l'Anglais par R. Coalson, Military Review, 1, 2016. http://www.theatlantic.com/education/archive/2015/10/ complex-academic-writing/412255/.

Lee, C. (2019). News from AUSA Global: Army Fleshing Out Updated Modernization Strategy. National Defense, NDIA's Business & Technology Magazine, 26 mars 2019. Arlington (VA, USA): National Defense Industrial Association. https://www.nationaldefensemagazine.org/articles/2019/3/26/army-looks-to-modernize-dotmlpf-in-modernization- strategy.

Le Guyader, H. (2000). Weaponization of Neuroscience. Technical Report. Norfolk (VA, USA): NATO ACT innovation Hub. https://www.innovationhub-act.org/sites/default/files/docs/WoNS.pdf.

Le Guyader, H., Cole, A. (2020). Cognitif, un Sixième Domaine d'Opérations ? FICINT document. Norfolk VA, USA : NATO ACT Innovation Hub. https://www.innovationhub-act.org/sites/default/files/2021-04/FR%20version%20v6.pdf.

Le Guyader, H. (2021). Le Domaine Cognitif de la Manipulation est Devenu un Terrain de Conflit. Paris (France) : Le Monde, 6 mai 2021. https://www.Lemonde.Fr/Idees/Article/2021/05/06/Le-Domaine-Cognitif-De-La-Manipulation-Est-Devenu-Un-Terrain-De-conflit_6079291_3232.html.

Orinx, K., Struye de Swielande, T. (2021). Carte Blanche : la Guerre Cognitive et les Vulnérabilités des Démocraties. Bruxelles (Belgique) : Le Soir, 11 mai 2021. https://plus.lesoir.be/371510/article/2021-05-11/carte-blanche-la-guerre-cognitive-et-les-vulnerabilites-des-democraties.

Wells, B.H. (2021). Emerging and Disruptive Technologies: Challenges and Opportunities. Scientists Discuss Future CIS Technologies for Defence in Global Online Conference. 21th International Conference on Military Communication and Information Systems ICMCIS'2021. Virtual Edition: 4 – 5 mai 2021. Bruxelles (Belgique): NATO Communications and Information Agency (NCIA). https://www.ncia.nato.int/about-us/newsroom/scientists-discuss-future-cis-technologies-for-defence-in-global-online-conference.html.

Collectif (2010). Allied Command Operations – Comprehensive Operations Planning Directive (COPD). Bruxelles (Belgique): Supreme Headquarters Allied Power Europe. https://info.publicintelligence.net/NATO-COPD.pdf.

Cole, A., Le Guyader, H. (2020). Cognitive, a 6th Domain of Operations? FICINT document. Norfolk (VA, USA): NATO ACT innovation Hub. https://www.innovationhub-act.org/sites/default/files/2021-04/ENG%20version%20v6.pdf.

Donnelly, J., Farley, J. (2019). Defining the 'Domain' in Multi-Domain. Shaping NATO for Multi-Domain Operations of the Future, Joint Air & Space Power Conference, Berlin (Allemagne) 8 – 10 octobre 2019. Kalkar (Allemagne) : Joint Air Power Competence Centre. https://www.japcc.org/defining-the-domain-in-multi-domain/.

Fry, S.A. (Ed.) (2009). Joint Department of Defense Dictionary of Military and Associated Terms – Joint Pub 1-02. Washington (DC, USA): Department of Defense. https://web.archive.org/web/20091012193530/; http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

Chapitre 3 – *COGNITIVE WARFARE* – MGA – CONTRIBUTION DU MAJOR GENERAL DES ARMEES (REPUBLIQUE FRANÇAISE)

Général Eric Autellet [1]

« The Human Brain is the Battlefield of the 21st Century »
(James Giordano, 2018)

Si l'on prend au pied de la lettre, la citation du neuroscientifique James Giordano (2018), alors le champ cognitif doit être une de nos priorités, en termes de recherche mais aussi pour la conduite de nos opérations.

L'intensification des rivalités entre puissances se traduit, tout au long d'un continuum « contestation – compétition – confrontation », par des actions dans les « zones grises » visant à intimider ou à contraindre. Il ne faut pas attendre la phase de confrontation pour agir notamment sur le champ des perceptions, d'autant que l'action létale et cinétique ne sera pas toujours la réponse la plus adaptée.

L'EMA doit, dans cette perspective, s'approprier ce sujet et accompagner les réflexions en cours à l'OTAN, pour nourrir le débat notamment en amont des travaux du futur concept stratégique. Il doit aussi l'intégrer dans l'agenda européen pour sensibiliser les nations européennes et les amener à investir un champ qui deviendra essentiel au travail en coalition et à notre interopérabilité.

Les travaux conduits par l'ENSC dans ce domaine, en particulier l'organisation de cette journée scientifique et stratégique qui a su identifier les enjeux et les menaces liés au domaine cognitif, contribuent dès lors activement à notre réflexion. Au-delà des développements scientifiques et biotechnologiques, les échanges ont montré que le champ cognitif couvre un vaste spectre intégrant notamment les sciences humaines, dont la psychologie et la sociologie.

Les actions d'influence, le soft et smart power, les actions de désinformation et de déstabilisation deviennent des composantes essentielles des stratégies de conquête et de domination entre pays, organisations et acteurs non étatiques des relations internationales : un brouillage intentionnel des repères et des frontières, indifférent à la réalité, tend à s'installer.

Influencer et manipuler l'opinion publique sont des modes d'action à part entière pour des puissances visant à déstabiliser nos démocraties, dans un contexte de « post-vérité », de remise en question des savoirs, des institutions et gouvernements, des connaissances et de la démarche scientifique, où le fait compte moins que l'émotion et les mensonges de ceux qui les profèrent. Ces puissances (étatiques ou pas) s'appuient sur la technologie qui leur procure des leviers de diffusion et d'intrusion puissants pouvant cibler chaque individu, tout se donnant la capacité d'influencer etde manipuler à son insu l'opinion publique à grande échelle. Les *fake news*, la rumeur, la mystification et le complotisme en sont des exemples très concrets, dont la diffusion est démultipliée par les réseaux sociaux.

La référence au triangle de Clausewitz « peuple, politique, militaire » permet d'identifier la place dumilitaire dans une thématique qui semble au premier abord ne concerner que le domaine civil. Le champ des manipulations de l'information dans une perspective militaire n'a, en effet, rien de nouveau en soi. L'arme de l'information est un vieil héritage de la guerre froide (on pourrait d'ailleurs remonter aux conflits

[1] Eric Autellet est général d'armée aérienne. Ancien pilote de chasse, il a été directeur général de l'Ecole de l'Air de Salon-de- Provence dont il a conduit la transformation pour devenir un « grand établissement » d'enseignement supérieur et de recherche, reconnu à un niveau international. Après avoir été Major général de l'Armée de l'air et de l'espace en 2020, il commande depuis mars 2021 l'ensemble des armées françaises dans les fonctions de « Major général des Armées ».

mondiaux du début du XX^{ème} siècle) et dès les années 1960 – 1970, la vision du domaine des perceptions rentre dans le champ doctrinal des principales forces armées.

Depuis le Vietnam, malgré les succès militaires, nos guerres se perdent notamment par la faiblesse de notre narratif, tant vis-à-vis des populations locales, sur les théâtres d'opération, qu'à l'égard de nos propres populations.

Nos enjeux sont doubles s'agissant de notre action vis-à-vis d'un ennemi ou d'un ami et l'on peut définir des modes d'action passif et actif pour l'un comme pour l'autre, en tenant compte des limites et des contraintes de notre modèle de liberté et de démocratie. À l'égard de notre ennemi, il faut se mettre en capacité de « lire » dans le cerveau des adversaires afin d'anticiper leurs réactions. Le cas échéant, il faut pouvoir « pénétrer » dans les cerveaux adverses pour les influencer, les faire agir selon nos souhaits. S'agissant de notre ami (comme de nous-mêmes) il faut être en mesure de protéger nos cerveaux tout autant que d'améliorer les capacités de compréhension et de décision de nos cerveaux. Ces enjeux sont indétachables de la démarche de transformation digitale qui impactera résolument nos structures de commandement.

Si le concept de c*ognitive warfare* reste encore à définir, il me semble essentiel de poursuivre la démarche d'approfondissement du sujet, de sensibilisation et d'éducation, d'identification des défis technologiques et cyber et des enjeux de préparation opérationnelle, auxquels nous seront confrontés par ce biais.

L'État-Major des Armées participe d'ores et déjà aux travaux conduits au sein d'ACT sur ce sujet. Cette journée organisée par l'École Nationale Supérieure de Cognitique a permis d'amorcer une collaboration qui ne peut que se renforcer entre l'EMA et l'ENSC et qui pourra se traduire notamment par l'organisation de modules de formation au sein de nos écoles, au profit de personnel d'active ou de réserve et l'accompagnement et l'appui à nos travaux internes, stratégiques, conceptuels et doctrinaux.

3.1 BIBLIOGRAPHIE

Giordano, J. (2018). The Brain is the Battlefield of the Future. Modern War Institute Speaker Series, WH5300, Multimedia PAO AO103 – 25th September 2019. United States Military Academy: West Point NY, USA.

Chapitre 4 – QU'EST-CE QUE LA COGNITION ET COMMENT EN FAIRE L'UN DES MOYENS DE LA GUERRE ?

Professeur Bernard Claverie[1]

« À l'examen médical, le cyber warfare porterait sur le stéthoscope et le contenu des tuyaux, le cognitive warfare s'intéresse au diagnostic du médecin. »

Le *cognitive warfare* est l'un des moyens que des spécialistes utilisent pour modifier, orienter, et altérer la pensée humaine à des fins de conquête, supériorité ou inféodation des individus, ensemble d'individus, groupes ou populations. Il s'appuie sur la connaissance que l'on peut avoir des processus cognitifs que mobilisent ces individus dans l'utilisation et la maîtrise de leur environnement, notamment technologique, en ayant justement recours aux technologies numériques. De manière générale, il s'agit de modifier la conscience qu'ont les individus de la réalité pour leur faire prendre des décisions erronées ou les empêcher de prendre des décisions nécessaires. Le *cognitive warfare* est donc une pratique d'atteinte de la cognition à des fins de supériorité militaire.

Le *cognitive warfare* s'inscrit dans la triade suivante :

1) Les sciences humaines et sociales (Sallaberry et Claverie, 2018) ;
2) La méthodologie et l'ingénierie des facteurs humains (Claverie, 2019) ; et
3) Les théories de la cognition et les modèles des processus cognitifs (Claverie, 2021) sur lesquels on entend agir.

Mais pour agir ou protéger des atteintes volontaires de la cognition les acteurs militaires ou civils, opérateurs ou décideurs, soldats ou commandeurs, citoyens ou élus, il faut comprendre ce qu'est ce phénomène de connaissance du monde, de traitement de l'information par le cerveau : la cognition.

Figure 4-1 : Le penseur et l'inhibition de l'action par indécision ou surcharge cognitive.

De la simple prise de données environnementales à l'exploitation des souvenirs sémantiques les plus sophistiqués, du contrôle du geste à la prise de décision en situation complexe, l'ensemble des « processus cognitifs » permet à l'homme de vivre de manière raisonnable dans son monde.

[1] Bernard Claverie est professeur des universités, directeur honoraire et fondateur de l'Ecole Nationale Supérieure de Cognitique – Institut Polytechnique de Bordeaux (France) – et chercheur au CNRS – UMR5218 – Université de Bordeaux. Il est rédacteur en chef de la revue en ligne « Ingénierie Cognitique » – ISTE Open Science.

L'atteinte revêt deux aspects délétères :

1) L'inadaptation contextuelle, celle de l'erreur, du geste manqué ou de l'inhibition temporaire ; et
2) Le trouble durable, celui qui atteint la personnalité, qui transforme sa victime en l'enfermant dans une forme d'étrangeté comportementale ou d'inaptitude àcomprendre le monde.

Figure 4-2 : L'animal regard-t-il à droite ou à gauche, vers le haut ou vers le bas, rit-il ou fait-il mauvaise figure ? On remarque qu'il est impossible de voir les deux formes en même temps et que le passage volontaire de l'une à l'autre demande une forme d' « énergie cognitive ». On dit que la figure est « réversible » et « bistable » (inspiré de la figure du « canard-lapin » d'auteur inconnu et reproduite par Joseph Jastrow, 1900).

Dans le premier cas, il s'agit de provoquer des conséquences transitoires, circonscrites à un environnement critique particulier (cf. Figure 4-2). Le second concerne la transformation des principes décisionnels d'individus devenant alors perturbateurs ou responsables d'actions erronées, voire de non-action (cf. Figure 4-1).

4.1 DEFINIR LA COGNITION

La cognition est l'ensemble des moyens, des équipements corporels et des processus qui les mobilisent, qui permettent d'avoir grâce à eux une connaissance et une représentation du monde dans lequel il s'insère et agît sur lui. Ces moyens sont les comportements, ou activités corporelles, et les pensées, ou activités mentales.

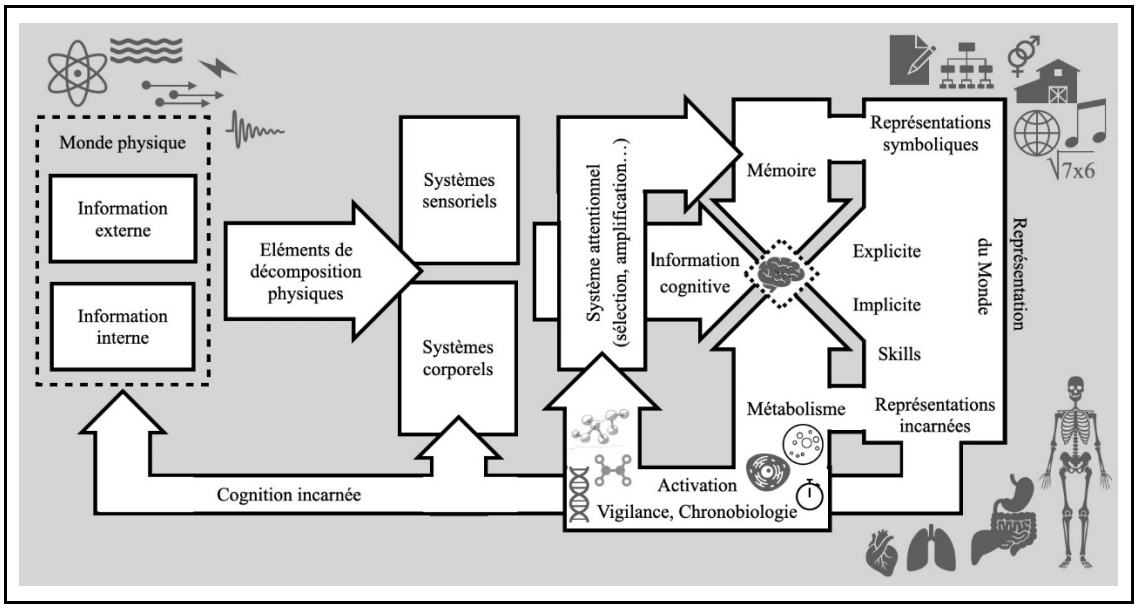


Figure 4-3 : Représentation schématique de l'appareil cognitif humain représentant quelques processus majeurs de traitement de l'information extérieure comme intérieure.

Les équipements sont ceux qui assurent l'interface avec l'information environnementale, sensation et action, ou assurent le traitement interne de cette information. Il s'agit du système nerveux, mais également de parties de systèmes qui lui sont associés, endocrinien, musculaire, en charge de régulations végétatives ou de la vie de relation, etc. Les processus correspondent aux grands chapitres du traitement de l'information, depuis la sensation/perception jusqu'à la programmation motrice et au contrôle d'ajustement du geste, en passant par le filtrage de l'attention, les différents stockages des mémoires à court, moyen ou long terme, la représentation et les capacités d'intégration ou de contractualisation, l'expression et le langage, etc. Cela implique à la fois des dimensions tournées vers l'information extérieure comme celle de l'intérieur. Une définition simplifiée pourrait correspondre à « la cognition, c'est ce que fait le cerveau de l'information du monde ».

4.2 LE CERVEAU ET NUMERIQUE

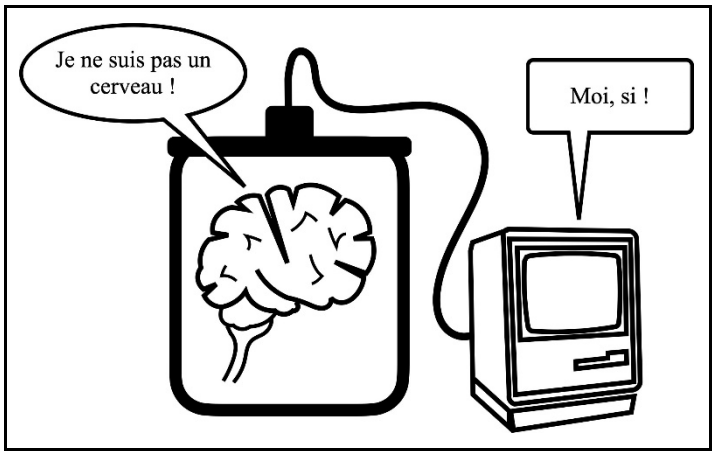


Figure 4-4 : Des relations étroites du cerveau et du numérique : causalité et codépendance (Claverie, 2021).

Le monde n'a que peu à voir avec ce que le cerveau connaît de lui. Ainsi, la gamme des ondes électromagnétiques que perçoit l'homme est extrêmement limitée, comprise entre les infrarouges et les ultraviolets, et les fréquences sonores ne sont connues que dans la stricte gamme des infrasons aux ultrasons. Le pouvoir discriminant des équipements sensoriels est faible, contraint par des capacités de transfert limitées. Leurs aptitudes sont fragiles, relatives aux heures de la journée comme dépendantes de la durée des stimulations et de la fatigue nerveuse. L'attention est une sorte de filtre protégeant le cerveau de la surcharge. Elle élimine la très grande majorité des inputs pour ne laisser passer que ceux que le cerveau juge préalablement utiles. Les capacités de mémoire, d'apprentissage comme de reconnaissance, sont médiocres. Elles se bornent à quelques bases perceptives, conceptuelles ou sémantiques qui appauvrissent d'autant plus la connaissance du monde à ce qui est connu et, le plus souvent, attendu. Et ainsi de suite.

De ces limites découle la nécessité de se faire aider, et c'est de tout temps le rôle de la technologie. On lui confie aujourd'hui volontiers les opérations cognitives les plus rébarbatives ou nécessitant le plus d'énergie. Il en est ainsi de la perception, avec des dispositifs allant des simples lunettes de correction de vue aux jumelles de vision nocturne ou aux écrans synthétique, dits « tête haute », des pilotes d'automobile ou d'aéronef. Pour la mémoire, les aides artificielles sont également nombreuses. Les notes et rappels sur téléphone portable, la consultation en ligne des encyclopédies accessibles par ordinateur, les cartes d'atterrissage ou les procédures embarquées sur tablettes en sont d'autres exemples. La décision repose sur la reconnaissance d'image, de son ou de composés chimiques atmosphériques. La programmation motrice bascule sur des dispositifs d'ajustement et de contrôle électronique de l'action, et la simulation permet de voir les conséquences potentiellesd'une action…

Le revers de la médaille est que l'aide numérique produit de la dépendance. Le premier niveau concerne l'impossibilité nouvelle de s'adapter à la complexité du monde sans le prolongement des capacités cognitives, vers un « homme augmenté » (Claverie, 2010) qui aujourd'hui n'est plus du fantasme de la réalité quotidienne. Le second en est une conséquence. C'est l'habitude et même le désir d'accès permanent et immédiat à l'information numérisés, photos, films, données de presse ou analyses savantes, etc. S'y ajoute cette motivation de nouveaux usagers soumis à la logique des réseaux internet et de l'utilisation continue des réseaux sociaux, du partage numérique et de la culture du *like*.

Cette proximité de la vie cognitive avec le monde de la connaissance numérique est définie par certains auteurs comme un « technium » (Hartley et Jobson, 2021), en rapport avec la connaissance humaine globalisée et interconnectée, dite « noosphère » (Kelly, 1995). La cognition n'est plus qu'une affaire de cerveau ; elle est, tout au moins depuis cette dernière décennie, en relation naturelle avec la technologie numérique et la connaissance partagée. Cette double relation est donc bilatérale et duale. Elle est bilatérale puisque le numérique est une production de la cognition et celle-là nécessite aujourd'hui l'aide numérique. Elle est duale car ces relations concernent à la fois l'individu et les collectivités. On différenciera donc les technologies des outils personnels et matériels embarqués, et celles de l'internet des objets, des réseaux et des collectivités. Ce sont deux champs distincts mais complémentaires du *cognitive warfare*.

4.3 DE LA CAPACITE LIMITEE ET DE L'ATTENTION

Un des premiers constats de l'étude de la cognition est qu'elle ne dispose que de capacités limitées au sein des gammes déjà restreintes de ce que le cerveau peut connaître du monde. Cela concerne à la fois la quantité d'information à traiter que l'énergie dirigée sur les contenus de ce traitement. Les quelques informations qui arrivent aux senseurs sont manipulées par des processus de filtrage internes dont le but est de protéger le cerveau d'une surcharge et d'augmenter la saillance de ce que traite le cerveau.

Ce phénomène, l'attention, possède plusieurs caractéristiques. Il est dépendant du type d'information, de son intensité physique comme de sa force sémantique, mais il peut également être volontairement orienté vers certaines dimensions de l'information. Dans le premier cas, on parle d'une « attention flottante », avec une mobilisation cognitive en fonction des caractéristiques d'intensité ou de signification du signal afférent. Dans le second, on définit une « attention dirigée » vers des caractéristiques attendues. À partir de cela, on peut concevoir que l'attention dirigée vers une cible limite toute capacité attentionnelle à d'autres destinations. On ne connaît alors du monde que ce qu'on attend de lui.

Si cette organisation de l'appareil cognitif permet la protection de la surcharge informationnelle et l'efficacité de ce qui est sélectionné, ce qui est hors du champ attentionnel échappe au traitement. C'est ce que l'on observe par exemple dans la conduite automobile avec le détournement de l'attention par l'usage du téléphone portable, ou dans le phénomène de tunnellisation dans des tâches de contrôle aérien, au cours desquelles ce qui se passe à côté du foyer d'attention échappe à la sagacité du radariste. De tels exemples pavent les traités de psychologie appliquée et la mise en œuvre de procédures de balayage visuel imposées aux opérateurs, pilotes, chirurgiens, et autres experts impliqués dans des obligations de surveillance, est systématisée dans les formations. Ces procédures sont elles-mêmes très coûteuses en ressources attentionnelles, très fatigantes, et demandent une organisation collaborative des postes de travail, avec des dispositifs numériques d'aide, de suppléance et de surveillance des acteurs humains.

Ce domaine de la distraction est un des principaux chapitres du *cognitive warfare*. Il dispose de deux volets complémentaires : la pollution attentionnelle avec détour de la focalisation, et l'exploitation des failles numériques ou des interfaces des outils numériques d'aide ou de surveillance. Ainsi, la survenue répétée et sans objet d'intérêt de multiples alarmes entraîne l'opérateur à minimiser la signification de ces alarmes, voire à négliger le dispositif lui-même ou même le débrancher. De nombreux accidents ont ainsi été provoqués par un bricolage de suppression des avertisseurs (domaine hospitalier, du contrôle de l'énergie, de la navigation aérienne, de l'accidentologie routière ou domestique, etc.).

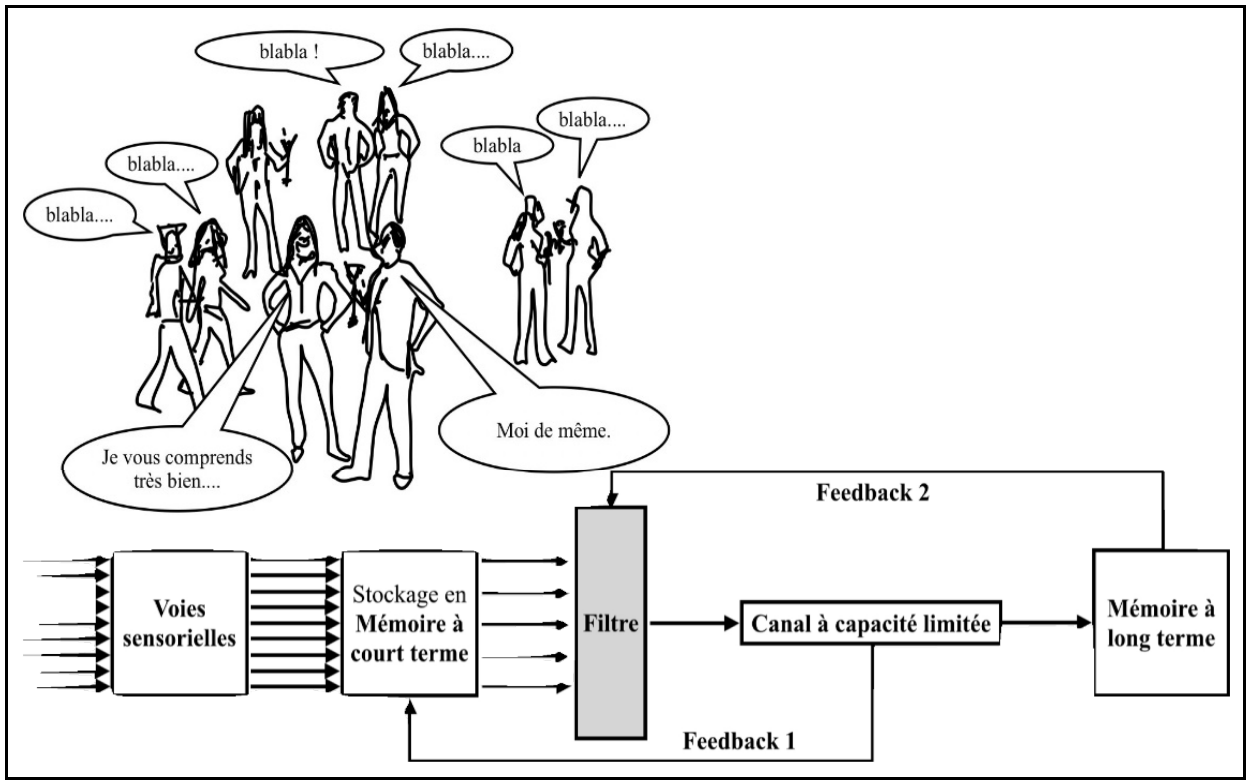


Figure 4-5 : Principe de sélection de l'information pour protéger l'appareil cognitif à capacité limitée – l'information choisie ou ayant une force signifiante passe ; l'information non utile est négligée. Expérience de la *cocktail party* : on entend ce qui dit l'interlocuteur sans entendre les autres, sauf à ce que ce qu'ils disent soit signifiant, alors on n'entend plus l'interlocuteur (on fait ou ne fait pas attention).

4.4 DU CONFLIT COGNITIF ET DE L'ILLUSION

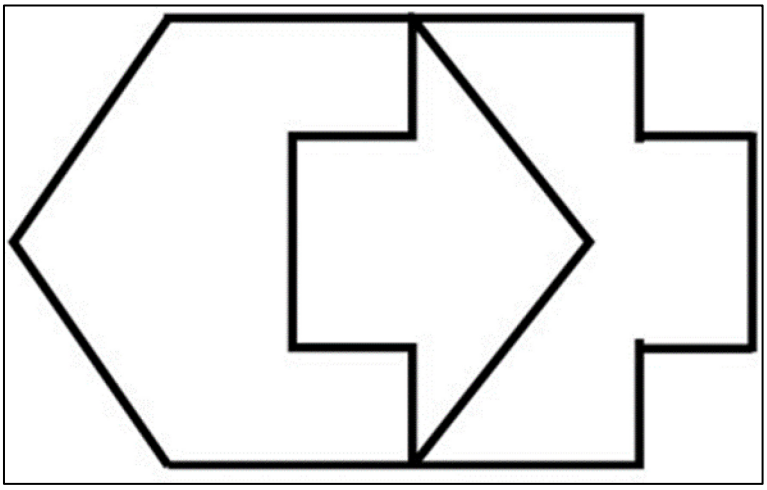


Figure 4-6 : « La flèche indique-t-elle la droite ou la gauche pour rejoindre la pharmacie ? » et « est-ce un hexagone ou une croix ? » Exemples de figures ambiguës qui nécessitent un travail cognitif couteux en énergie pour pouvoir répondre à une question simple.

Un conflit cognitif est une situation que doit gérer un individu en traitant une information dans un but attendu qui n'est pas cohérent avec ce que cette information lui permet de faire. C'est le cas, par exemple, lorsque le traitement est incompatible avec le résultat attendu ou soulève une ambiguïté cognitive que le sujet ne peut résoudre simplement. C'est le cas des figures ambiguës qui sont perçues comme des formes incompatibles entre elles ou qui entraînent le sujet dans une tâche de résolution impossible.

Ce type de figures a très tôt été documenté par la « psychologie de la forme » (Köhler, 1969) et a servi de base à de nombreuses études de psychologie et de neuro-ophtalmologie (p. ex. Meng et Tong, 2004 ; Kawabata et Mori, 1992). Le temps utilisé pour régler le conflit cognitif n'est pas disponible pour autre chose et le conflit devient souvent obsédant, engageant les raisonnements futurs (cf. Figure 4-2 et Figure 4-6. L'énergie cognitive orientée sur la résolution de problème de surface augmente le coût psychologique et permet de diminuer les ressources à allouer à d'autres taches.

4.5 DES HIERARCHIES ET DES DOMINANCES COGNITIVES

L'appareil cognitif est globalement structuré en niveaux fonctionnels dont l'activité est complémentaire et se combine à celle des autres pour donner un comportement adapté. Cette organisation correspond à l'apparition, au cours de l'évolution des vertébrés, de nouvelles structures encéphaliques. La cognition est donc un phénomène général ; elle apparaît dès que l'animal est capable de comprendre son environnement, d'en avoir une « conscience » et d'en valoriser l'expérience pour une meilleure adaptation grâce à de stratégies qu'il invente : une « intelligence ».

L'intelligence est ici à concevoir comme « aptitude à résoudre des problèmes non directement résolubles » pour une meilleure adaptation, une meilleure survie, une meilleure longévité et une meilleure quantité ou qualité de plaisir (Claverie, 2005). La cognition entretient un rapport étroit avec l'intelligence et avec la conscience du monde. Elle est déjà présente chez les ancêtres des humains, et ceux-là en ont gardé des aptitudes particulières, qu'ils ont perfectionnées pour donner les fonctions les plus sophistiquées que sont le symbolisme et le langage, et la conscience de soi.

L'appareil cérébral supporte la cognition, de formes les plus élémentaires jusqu'aux plus hautes. Il correspond à un empilement de niveaux d'apparition successive, ayant des propriétés, complémentaires, parfois antagonistes, et de plus en plus élaborées pour un comportement de plus en plus complexe et de mieux en mieux adapté. Il est environné des entrées et sorties de l'appareil sensori-moteur et d'une partie du système endocrinien (certaines hormones sont impliquées dans le stress, la vigilance et l'attention).

Le cerveau est donc un dispositif hiérarchique, organisé en niveau et exprimant des fonctions cognitives et des aptitudes de pensée de plus en plus performantes.

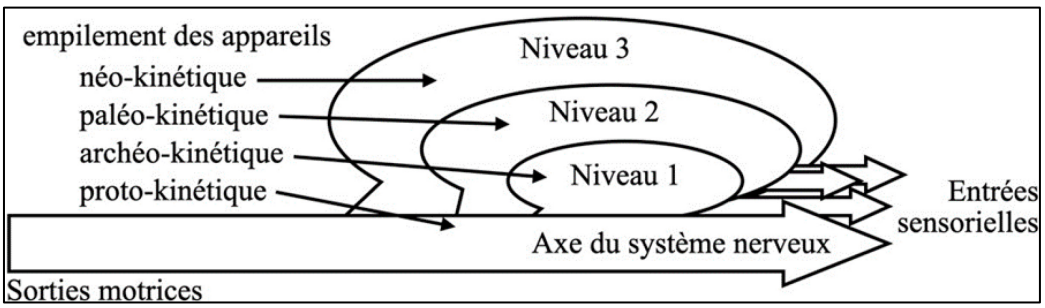


Figure 4-7 : Schéma simplifié de l'organisation des niveaux cognitifs sur les couches du cerveau, entre entrées sensorielles et sortie motrices. Cette structure cérébrale abrite les entités nerveuses responsables des différentes fonctions cognitives signalées à la Figure 4-2. Nota : kinétique, du grec κινησις (mouvement) ; littéralement qui permet le mouvement, et par extension l'adaptation au milieu par intégration sensorielle et programmation motrice.

Le niveau le plus simple exprime une cognition de premier niveau liée aux automatismes, avec des limites sensorielles, des compétences programmées (skills), des mémoires rudimentaires… C'est le niveau des apprentissages de base, de l'établissement des processus en tout ou rien, ceux qui ne demandent plus d'attention une fois établis, mais échappent à tout contrôle une fois déclenchés. Ce niveau est particulièrement facile à leurrer. On le retrouve dans les illusions, les mauvaises perceptions, les fausses certitudes, et l'induction des automatismes moteurs. Le second niveau est fortement dépendant des processus de mémoire et d'affectivité. Ces deux composantes de la vie mentale sont en intime collaboration, impliquant le fonctionnement de structures très proches (complexe amygdalo-hypocampique, circuit de Papez, cortex cingulaire…). Les manipulations de l'une de ces composantes affectent l'autre, et il est aisé de stabiliser des souvenirs parasites par implication affective et de déclencher des réflexes émotionnels par imposition de souvenirs.

D'autres dimensions du *cognitive warfare* peuvent concerner la modification de l'élaboration des règles stockées par surcharge d'information ou de décision, en accélérant des boucles d'analyse ne permettant pas l'élaboration de procédures ou au contraire en provoquant des conflits de ces règles. Un exemple peut être donné dans les difficultés de la détection fond/forme ou le recours à un processus qui en inhibe un autre.

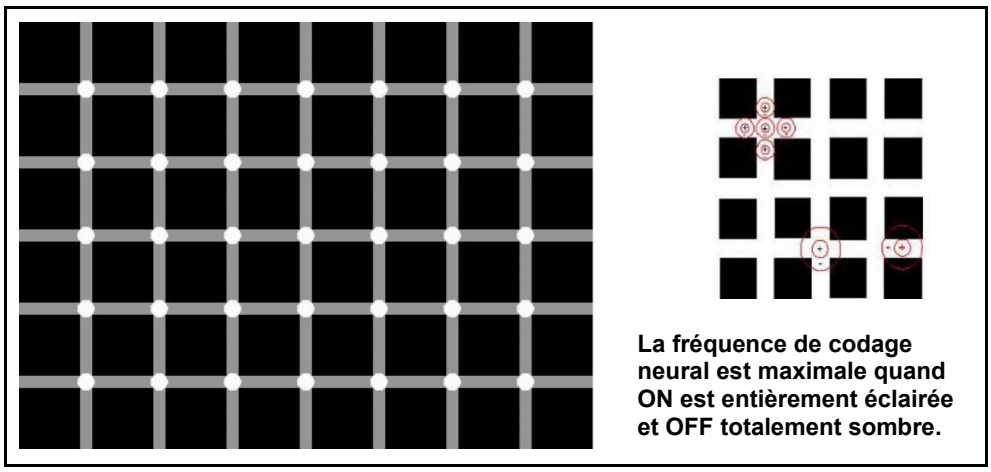


Figure 4-8 : « Combien y-a-t'il de points noirs dans la grille d'Hermann ? » Les contrastes perçus aux intersections sont attribués à la variation de la fréquence des potentiels d'action selon les surfaces relatives des régions rétiniennes appelées ON et OFF (champs récepteurs visuels primaires).

Figure 4-2 et Figure 4-6 sont ambiguës et leur analyse dépend de règles de bas niveau qui s'excluent l'une l'autre. La factorisation de l'une d'elles empêche l'autre de s'exprimer. Même en le sachant parfaitement, on ne peut en avoir une quelconque maîtrise ; on ne peut pas voir les deux formes en même temps, ce qui est pourtant élémentaire pour une machine. De même, certaines inférences peuvent faciliter certains processus, avec par exemple la surestimation des verticales par rapport aux horizontales. C'est également le domaine des *nudges*, ces « petits coups de pouce » que l'on introduit aujourd'hui un peu partout pour guider et orienter le comportement (Thaler et Sunstein, 2009) dans une forme de manipulation constructive des comportements, bien connue en management et en sécurité routière ou industrielle.

Le niveau cognitif supérieur est principalement impliqué dans les stratégies sémantiques, faisant appel au langage ou à des significations symboliques. C'est celui de la conscience explicite ou des phénomènes inconscients refoulés, de l'imagerie mentale et des représentations sophistiquées. Il entre parfois en concurrence avec les niveaux inférieurs avec des recours aux automatismes ou à des règles apprises dans un effort volontaire d'orientation cognitive.

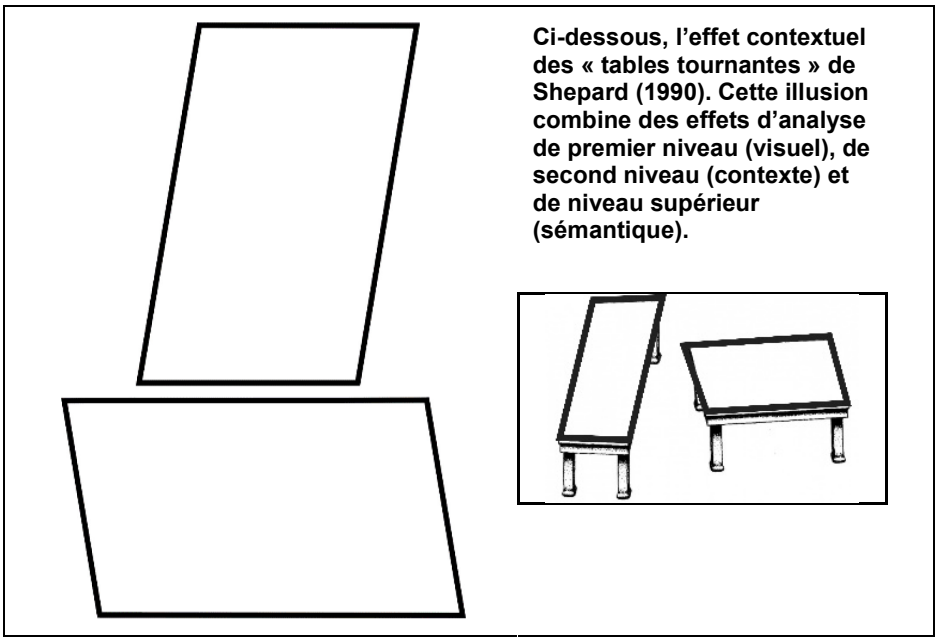


Figure 4-9 : Exemple de deux figures parfaitement identiques mais dont la différence d'orientation les fait paraitrede dimensions et surfaces différentes.

C'est aussi celui des biais de haut niveau portant sur des ambiguïtés de sens, aussi bien par manque que par en-trop de signification, par conflit sémiotique, par ambiguïtés sémantiques. Plusieurs théories exploitent ses distorsions de fonctionnement. On les trouve dès la fin des années 1960 en sociologie expérimentale (Zajonc, 1968), puis dans de nombreux travaux de psychologie sociale (Goffman, 1974), en économie expérimentale (Martinez, 2010), ainsi qu'en ergonomie du risque avec une place particulière pour les « décisions absurdes » (Morel, 2002) et la force du « contre intuitif » (Berthet, 2018). Elles ont été notamment vulgarisées par le Prix Nobel d'économieKahneman (1979) et son collègue Tversky (1992) sous le nom de « biais cognitifs ».

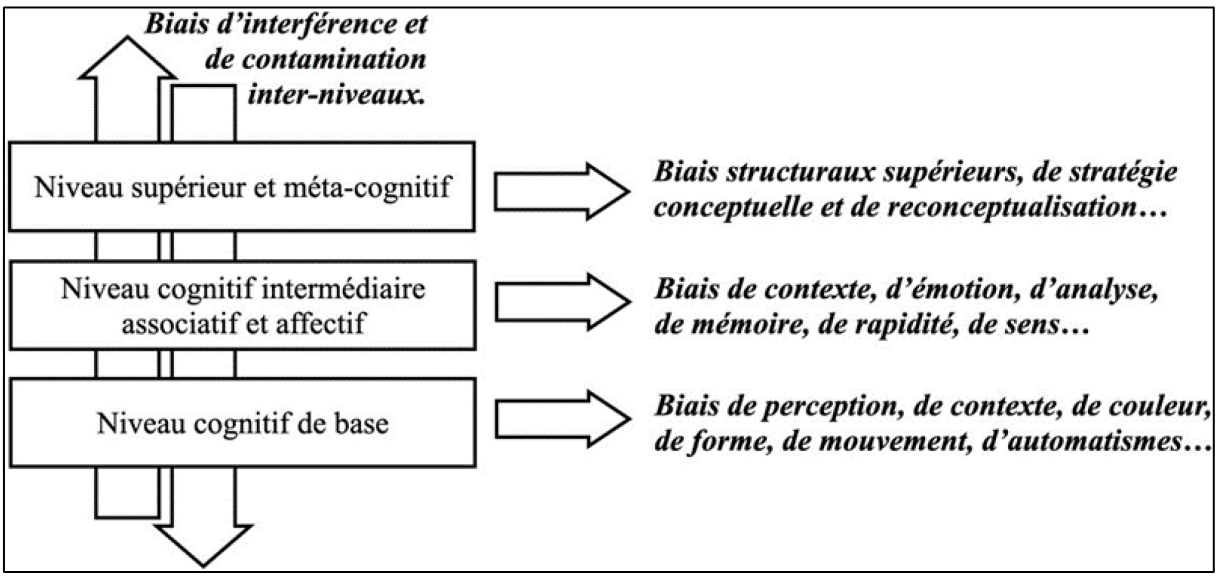


Figure 4-10 : Organisation de l'appareil cognitif en niveaux, avec hiérarchie des biais cognitifs exploités en fonction des niveaux ainsi que par l'interaction entre ces niveaux.

Autant les processus cognitifs sont hiérarchisés en niveaux fonctionnels, langage et formalisme de haut niveau, affectivité et mémoire, extraction de traits et perceptions, autant les relations entre étages sont importantes dans la contribution à une connaissance globale de l'environnement et sa prise de conscience.

Les conflits au sein de chaque étage sont alors complétés par des conflits entre les étages. Les processus s'enrichissant les uns les autres, ils peuvent interagir de manière inhibitrice en empêchant par exemple de réaliser une tâche, ou excitatrice en déformant les productions. Ces phénomènes sont à l'origine de mauvaises conceptions sémantiques liés à des traitements ascendants erronés, pouvant ou non entrer en concurrence avec des données de la mémoire. Il en est de même de processus descendants qui tendent à orienter l'attention et ne laisser connaître du monde que ce qu'on en attend, minimisant l'importance des éléments non prévus et négligeant les signaux faibles.

4.6 DES PERSONNALITES COGNITIVES ET DES STEREOTYPIES

La personnalité cognitive est la façon spontanée qu'un individu a de connaître le monde. C'est, en quelque sorte, l'ensemble de ses habitudes de pensée, de voir, entendre, mémoriser… Cet individu a plus tendance à mobiliser, prioriser ou au contraire inhiber tels processus cognitifs que tels autres. Cette personnalité est notamment relative à la répartition des priorités allouées à chaque étage cognitif, mais également à l'habitude de faciliter ou inhiber les interrelations entre niveaux. Le monde est donc conçu et connu de manière différente selon les critères de personnalité cognitivedes individus qui l'explorent, s'y insèrent ou en parlent.

Un des critères correspond à la priorisation de tel étage plutôt que tel autre. Certains individus ont tendance à valoriser les informations sensorielles concrètes au détriment de la valeur émotionnelle ou mémorielle de chacun d'eux. D'autres s'attachent à leur conceptualisation interprétative, modulée par le langage ou par des théories intellectuelles apprises. Un autre exemple réside dans la tendance à s'attacher aux détails alors que d'autres privilégient les ensembles, d'autres encore les contextes par rapport aux éléments isolés, etc. Certaines personnes ont plus tendance à intellectualiser leurs perceptions et ne retenir du monde que ce qui s'inscrit dans une démarche analytique ou constructive, par exemple la valorisation des nombres sur les mots ou vice-versa, de la géométrie sur les relations logiques, des séries et régularités sur les indices de nouveauté, etc.

Au niveau cognitif supérieur, réputé dépendre du cortex des deux hémisphères cérébraux, on connaît des différences cognitives selon la latéralité des processus : la dominance cérébrale. Certaines personnalités cognitives dépendent de processus réputés latéralisés à droite, alors que d'autres privilégient ceux de gauche. Les commissures (relations entre les deux hémisphères) peuvent être plus ou moins sollicitées avec des individus plus bilatéralités que d'autres…

Le monde n'est donc pas tel que notre cerveau permet à chacun de le concevoir ni comme un autre peut le faire. C'est le langage qui permet une négociation linguistique à son propos. Il permet de s'entendre et contribuer ainsi à sa théorisation. Cette dimension métacognitive sert à la fois de guide et de facilitation des cognitions liées aux niveaux inférieurs. De tels processus descendants, influencés par l'expérience et la culture, constituent un véritable modèle dans lequel s'inscrivent les connaissances. Ils forment des sortes de prototypes de pensée.

Il est alors aisé d'utiliser des distorsions entre individus, de faciliter les absences de cohérence entre les modèles conceptuels et les connaissances personnelles. Sont ici concernés le domaine des apprentissages manqués, mais également, de manière plus critique, celui de certains rapts ou troubles psychopathologiques aussi difficiles à maîtriser que simples à induire et exploiter.

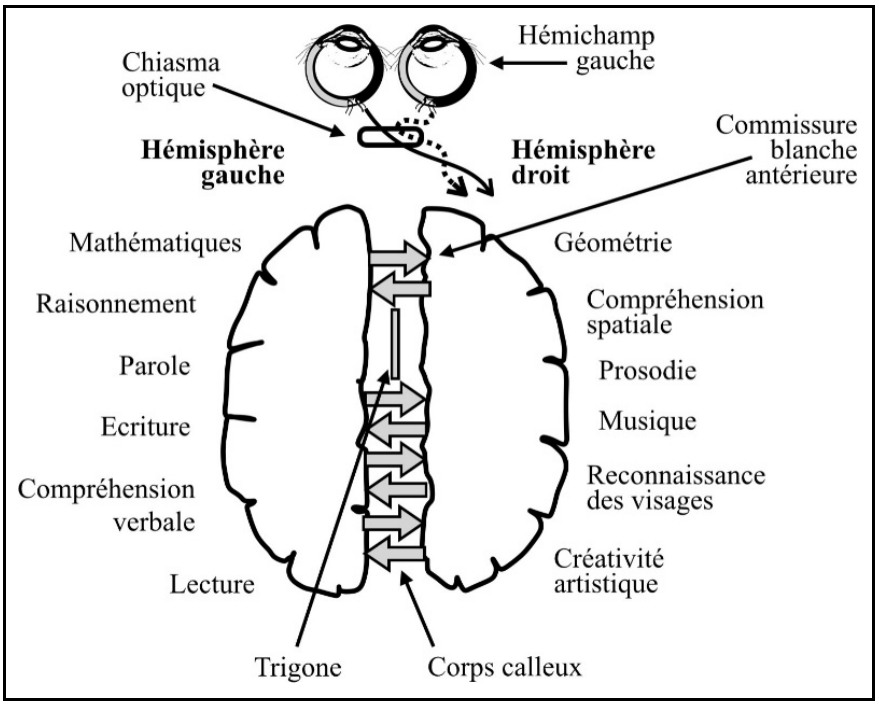


Figure 4-11 : Exemple de fonctions cognitives latéralisées recrutant des territoires neuro-fonctionnels différents, à droite ou à gauche, en avant ou en arrière (ici chez le droitier). Les processus spontanés de dominance cognitive contribuent à la personnalité cognitive.

4.7 DE L'ATTRIBUTION CAUSALE ET DE LA MANIPULATION

Le processus dit d'attribution repose sur l'inférence causale. Cela veut dire qu'au niveau le plus sophistiqué de sa pensée, un individu ne déduit pas objectivement des données ni ne recherche une solution interprétative par processus d'essais-erreurs. Il interprète le monde en fonction des mécanismes précédents et de ses prototypes et croyances spontanées. L'attribution permet de donner une signification aux événements, et cela d'autant plus qu'ils sont complexes et que l'on n'en dispose pas d'explications simples. Elle concerne à la fois les propres conduites et comportements des individus comme ceux d'autrui, et cela pour l'interprétation du passé comme dans la prédiction, l'attente spontanée et l'interprétation du futur (Heider, 1958). Deux dimensions sont à prendre en considération, celle du contexte et de l'organisation que l'on croit être celle de l'environnement, et celle des personnes et de l'importance qu'ils considèrent être de leur rôle dans ce futur (Jones et Davis, 1965 ; Nisbett et Ross, 1980). On détermine ainsi deux dimensions de l'attribution. La première consiste à penser que l'évolution de la situation est principalement relative à soi-même, à ses propres choix et comportements, voire à sa simple présence : il s'agit de l' « attribution interne ». La seconde consiste à croire que quasiment tout est dépendant de l'environnement, de l'histoire ou des autres, que le contexte est prégnant et que l'action personnelle n'a que peu d'importance : c'est l' « attribution externe ».

On a pu constater que les décideurs sont contraints par leur tendance attributive, souvent selon leur passé professionnel et leur expérience, mais également leurs préjugés. Lorsque des faits viennent contredire l'attribution, certains d'entre eux maintiennent leurs jugements par des biais de confirmation de l'explication préétablie et par la négation autoritaire d'hypothèses alternatives.

La constitution et le recours systématique aux « idées toutes faites », notamment dans les relations humaines avec le recours à des « théories psychologiques naïves », permettent aux individus de s'inscrire dans un cadre rassurant de compréhension du monde. L'importance n'est plus alors de savoir quelque chose

d'exact sur le monde, mais de conjurer l'incertitude par des « théoriesspontanées » que leurs auteurs tentent coûte que coûte de confirmer. Certains dérapages peuvent même conduire aux *fake news*, fausses controverses, révisionnisme, contestation de la science, etc.

Un des principes habituels consiste en un filtre d'analyse des seuls faits du réel confirmant les convictions. Chacun en tire des conclusions sur l'avenir à partir d'échantillons choisis du passé. Les règles permettent de considérer les événements du monde comme des cas particuliers tombant sous l'interprétation due à ces règles. Pour chacune d'elles, les écarts à la règle sont considérés comme des exceptions qui constituent les bases de l'élaboration de nouvelles règles interprétatives du réel, participant à un biais d'autoconviction. On peut donc réduire la problématique des personnalités cognitives, c'est-à-dire de la tendance de chaque individu à mobiliser spontanément certains processus cognitifs, selon les principales bases de l'attribution causale : la dimensionnalité du « moi » distribuée autour des deux pôles de l'hypertrophie et du misérabilisme personnel ; le sentiment de responsabilité, passant de l'orientation de la cause vers soi jusqu'au sentiment de persécution ; la fausseté du jugement qui repose sur des inadéquations des formes du raisonnement.

Là commence le glissement d'une science des biais cognitifs et des personnalités qui y sontsoumises vers la psychologie clinique. Ces biais d'attribution sont en effet caractéristiques de nombreux troubles psychopathologiques. Ils font l'objet d'une expression systématique dont se saisissent alors certains manipulateurs.

4.8 DES BIAIS ET DE L'ERREUR GENERALISEE

Certains auteurs ont étudié plusieurs formes de biais. Une forme particulière intéressante constitue le biais dit de « complaisance », L'interprétation de la réalité y est attachée à l'issue potentielle positive ou négative d'une situation (Nisbett et Ross, 1980). On note d'ailleurs une différence de position selon qu'on est acteur et impliqué, et observateur ou non concerné par la situation. Ainsi les acteurs impliqués attribuent-ils plus une causalité attachée au « moi », aux motivations personnelles et à la valorisation des effets potentiels de leur propre action, alors que des observateurs ou de collaborateurs extérieurs valorisent les causes dispositionnelles et contextuelles, tout en minimisant l'importance des personnes impliquées et de leur action.

Dans les deux cas, le biais de « prétentiosité » consiste à penser, pour un individu, être au centre du problème posé ou au contraire ne pas être concerné par ce problème qui ne concerne, évidemment, que les autres. L'incompréhension, voire le mépris sont des conséquences spontanées de l'un par rapport à l'autre, facteurs de d'ostentation sociale et même de difficultés relationnelles. L'expression d'une hypertrophie du moi se concrétise souvent dans une forme de convictiond'unicité, d'appartenance à une sorte d'élite, convaincue de toute imperméabilité au biais considéré. Une autre forme d'expression, habituelle, consiste à croire au pouvoir de la formation dans la transformation de la personnalité pour être ainsi protégé du biais. Ces deux positions se combinent souvent pour donner naissance ou justifier des corporations, collégialités, communautés professionnelles, voire factions et autres organisations élitistes. Elles posent le problème de la formation pratique, par l'exemple, ou dans le cadre d'un « éclairement » initiatique.

Deux autres convictions, aussi fréquentes qu'erronées, consiste à penser que ce sont les autres qui sont victimes des erreurs cognitives, et que le formalisme et la formation résoudront les problèmes de biais. Pourtant, tout le monde est concerné par l'erreur perceptive de Figure 4-9 et Figure 4-10, et ce n'est pas parce qu'on en a l'explication rationnelle ni qu'on répète l'expérience que l'erreur disparaît. Seules la connaissance que l'on a de l'erreur et celle de savoir comment en maîtriser les conséquences peuvent être utiles. L'appareil cognitif ne varie pas ; il n'évolue en la matière ni avec l'expérience ni avec l'apprentissage, et ses caractéristiques biologiques font que tout le monde, sansgrande exception, est concerné. L'expérience ou la formation ne changent rien à l'affaire. Les seules choses qui peuvent être apprises sont donc l'autocontrôle ou le contrôle partagé, et l'analysemétacognitive d'anticipation (*gaming* et simulation) et de

rattrapage (« retex » dynamique). Mais dès que les niveaux inférieurs sont impliqués, que la charge mentale, le stress ou la pression temporelle augmentent, les individus ont tendance à revenir sur leurs bases cognitives stabilisées.

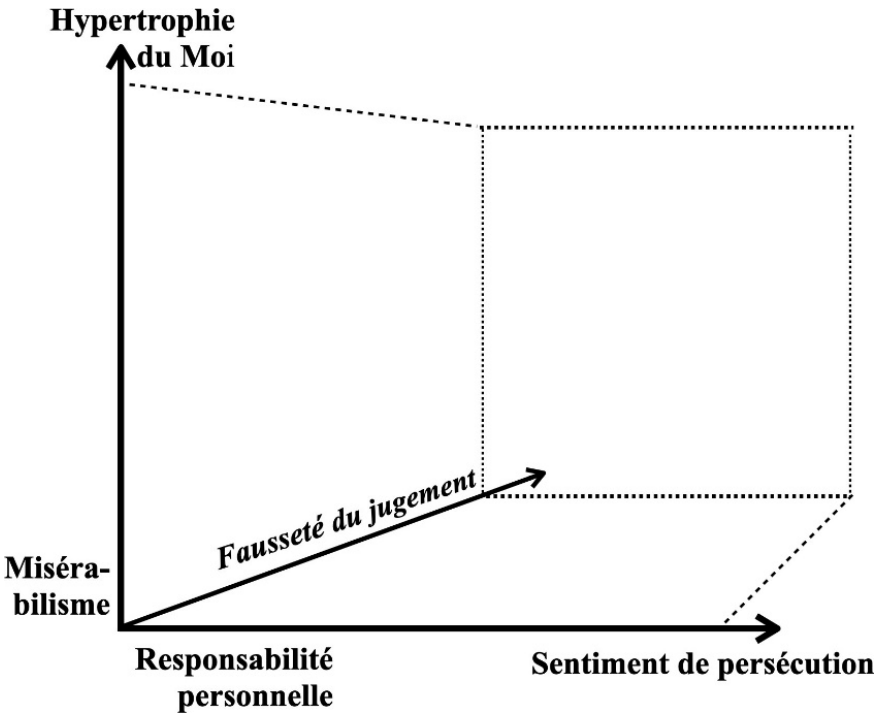


Figure 4-12 : Trois axes cliniques de distorsions cognitives dans l'attribution causale. En bas, devant et à gauche, les biais de tendance à la mélancolie et au repli sur soi ; en haut, au fond et à droite, les personnalités paranoïdes ; au fond à gauche, les biais de prétentiosité en haut, ou d'auto-complaisance en bas ; en haut, devant et à droite, les biais de maîtrise par méticulosité, etc.

Les biais cognitifs sont des erreurs générales. L'économie comportementale en a inventorié des centaines. Ils reposent tous sur la structure de l'appareil cognitif tel qu'il s'est constitué, soumis aux contraintes neurobiologiques de l'évolution. Celle-là a favorisé l'émergence et a sélectionné des processus utiles à la survie, éliminant les individus qui n'étaient pas soumis à cette logique. Deux principes biologiques majeurs ont été à l'œuvre. Le premier est la tendance à la « minimisation de l'énergie ». Ce principe biologique majeur se manifeste en optimisation du « coût cognitif » spontanément estimé. L'individu valorise inconsciemment les raisonnements courts et un des moteurs de cette régulation réside dans la conviction motivationnelle que les pensées simples sont les plus vraies. Une fois posées, les représentations spontanées, les croyances, les prototypes de pensée stabilisés contribuent à des certitudes parasitant l'objectivité ou engageant l'individu dans les contraintes d'un autre principe : devoir faire des choix. Un choix cognitif est un abandon de pensée, et on abandonne difficilement ce à quoi on tient. Les apprentissages de règles explicites permettent ici d'éviter l'ambiguïté. Leur concaténation pour résoudre des problèmes complexes mobilise à la fois la mémoire et l'attention, ainsi que la réflexion pour savoir les choisir et les ordonner.

Ce sont trois cibles de l'action cognitive. Au premier niveau, il s'agit de saturer l'attention et exploiter les automatismes, au second, de perturber la mémoire et exploitant notamment les influences émotionnelles et les interférences, et au troisième d'empêcher la réalisation des raisonnements par pression temporelle, parasitage ou facilitation des erreurs de raisonnement.

4.9 EXPLOITER LES ERREURS COGNITIVES

Pour ce qui est du raisonnement, il est souvent faux. Pour faire simple, on peut considérer que la pensée humaine repose sur la mise en œuvre de trois types de raisonnement dont deux sont utiles, voire indispensables, mais erronés. Il s'agit alors simplement de les faciliter.

Le plus simple est le plus fréquent, le moins coûteux, dont on suppose qu'il correspond aux formes de base de l'appareil cognitif, est l'abduction. C'est le mode de pensée constitutif d'une physique naïve et de la psychologie spontanée. Ces deux dimensions du savoir permettent à chacun d'avoir une forme de compréhension simplifiée du monde et d'établir des relations naturelles aux autres. Elle est probablement liée à la survie immédiate des individus, avec une connaissance rapide, basée sur la catégorisation des contextes de vie et celle des dangers ou des ressources. En psychologie, l'abduction est la forme principale du raisonnement intuitif ; elle consiste à minimiser les hypothèses gênantes par économie du coût cognitif, et supprimer les solutions considérées comme improbables. Or l'abduction, aussi efficace soit elle, est une erreur logique.

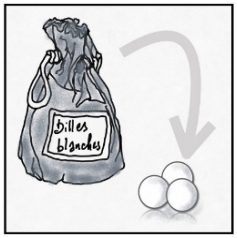
Ce raisonnement s'appuie principalement sur l'observation et l'expérience. C'est une généralisation abusive des causes. Ce raisonnement est très utile s'il est contrôlé, employé en science, pour poser un diagnostic médical, ou pour enquêter et motiver l' « intime conviction » des magistrats. Or l'abduction n'aboutit pas à une réalité, mais apporte une « vérité probable » qu'il y a lieu d'explorer et de vérifier a posteriori grâce à des protocoles stricts. Or cette vérification prend du temps et peut apparaître comme superfétatoire. L'abduction produit de l'erreur par naïveté ou par risque accepté puisque jugé improbable.

Un second niveau de la pensée, plus sophistiqué, correspond à l'induction, qui est également une erreur logique. Elle tombe sous les mêmes caractéristiques d'utilité et critiques de non-vérification conséquente. Elle contribue également à une représentation du monde par l'élaboration de catégories spontanées qui permettent aux sujets une représentation plus sophistiquée qu'avec l'abduction, bien qu'aussi naïve.

L'induction se constitue principalement autour de l'estimation temporelle. C'est elle qui permet de croire que l'avenir ressemblera au passé et que l'on peut attendre des stabilités dans des estimations temporelles raisonnables. « Demain, il fera jour », « la nuit porte conseil » et « le ciel est à l'orage »en sont des exemples utiles pour une vie normale. Il s'agit d'une tendance à faire une généralisation, ayant un rôle explicatif du futur, basée sur des évènements passés ou établis, en négligeant les exceptions. Cette forme de raisonnement remonte du singulier au général, du cas particulier aux loisqui le régiraient, d'une conséquence au principe dont elle découlerait et à une cause postulée. Ce type raisonnement a également montré son intérêt et sa puissance en sciences, en médecine et en économie, pour peu que le processus de pensée soit borné par la qualification de la probabilité de sa propre erreur (la validité interne) et la recherche permanente d'un contre-exemple qui réfuterait la généralité admise pourtant sans certitude (la validité externe). Là encore résident deux faiblesses du raisonnement, l'introduction de fausses croyances à partir d'éléments erronés ou la négligence des exceptions et contre exemples souvent présents dans les signaux faibles.

L'abduction et l'induction s'opposent à la déduction qui, lorsqu'elle est formulée de manière correcte et établie sur des éléments vérifiés (vérité des prémisses) mène à une conclusion toujours vraie (vérité de la conclusion).

De manière générale, les erreurs cognitives peuvent être rapportées à ces trois catégories, ou dans une suite combinée d'éléments de ces trois catégories de pensée. Il suffit alors de repérer les éléments constitutifs de la stratégie cognitive de l'adversaire pour agir au moins sur l'un d'eux, en exploitant les contraintes de rapidité de pensée et de non-vérification, la tendance à négliger ces vérifications, la facilitation des généralisations abusives, et la confirmation des convictions établies de manière erronée. Le défenseur veille, quant à lui, à valoriser les étapes de la vérificationdéductive en chassant le recours aux raccourcis de pensée, notamment en détectant les failles potentielles des raisonnements ou des procédures et règles doctrinales ou établies.

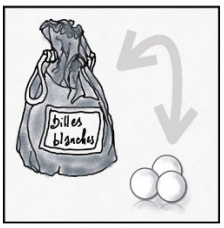


Déduction

Ce sac est rempli de billes blanches.
Ces billes viennent de ce sac.
Ces billes sont donc blanches.

Induction

Ces billes viennent de ce sac.
Toutes ces billes sont blanches.
Ce sac est donc rempli de billes blanches.



Abduction

Ces billes sont toutes blanches.
Ce sac est rempli de billes blanches.
Ces billes viennent donc de ce sac.

Figure 4-13 : Trois formes de la pensée. La première nécessite du temps et n'a qu'un faible pouvoir de généralisation. C'est pourtant la seule exacte. Les deux autres formes des pensées correspondent à des réflexes cognitifset sont des erreurs logiques. Leur utilité ne peut être considérée qu'accompagnée de procédures méthodologiques de vérification, qui sont coûteuses en temps et en énergie (in Claverie, 2019).

Demain, et face à l'attaque par force brute et la difficulté de la repérer, émergera la double nécessité d'une stricte méthodologie de pensée et du recours aux outils d'intelligence artificielle et aux programmes analytiques sur big data, d'une part dans la surveillance des erreurs cognitives et d'autre part pour le repérage des actions malveillantes d'incitation à l'erreur.

4.10 DE LA METHODE ET DES CRISES DE CONCEPTION DU MONDE

Si penser est un acte spontané, penser de manière professionnelle ne se fait pas n'importe comment. Le diagnostic médical n'est pas une simple impression, issue d'une attention flottante et de l'émergence d'informations mémorisées par le patient ou le praticien. L'anamnèse est soumise à de strictes règles d'incitation, de conduite dirigée et d'analyse structurée. Le diagnostic procède par allers-retours entre abductions, inductions et déductions, se focalisant sur des éléments à éliminerou, au contraire, à valoriser. L'examen complémentaire prend ici tout son sens dans la complétion de l'avis. Il en est de même aujourd'hui des techniques de profilage criminel qui abandonnent les impressions au bénéfice de méthodes scientifiques, strictes et logiques, pouvant être reçues par les tribunaux.

Cette procédure est bien connue en science. Elle s'attache à chercher les éléments de réfutation à une théorie afin d'en affiner les bords. Les éléments de falsification théorique sont alors examinés et font l'objet d'une recherche spécifique, soit pour dénoncer la théorie générale, soit pour la préciser. Cette méthode fonctionne par conjectures et réfutations (Claverie, 2019).

On peut schématiser le raisonnement par une ou plusieurs hypothèses posées par induction ou abduction, qui permettent des prédictions qu'il reste à confronter à l'expérience réelle. Elles en sortent réfutées ou acceptées comme potentiellement valides jusqu'à une nouvelle contradiction. La vérité n'est donc que

temporaire, elle est admise dans le cadre d'une vigilance permanente à être invalidée ou reconsidérée. En dehors de cette stricte pratique, c'est le domaine de l'erreur et le terrain de jeu potentiel du *cognitive warfare*.

La connaissance objective du monde porte d'abord sur des généralités. Elles sont construites à partir de données statistiquement établies, d'informations vérifiées décrivant notamment des valeurs de tendance centrale. Elles sont explicatives de la totalité de ces valeurs, et de la meilleure partie des données marginales dont certaines peuvent pourtant entrer en conflit avec elles. Là réside le problème, puisqu'une théorie explicative du réel, c'est-à-dire sa représentation, est par essence transitoire. Elle est précisée et enrichie en permanence, et lorsqu'elle ne peut plus l'être, doit être abandonnée malgré les investissements qui y ont été consacrés et les convictions personnelles aussi établies soient-elles.

Un exemple devenu célèbre est dû à l'épistémologue Karl Popper (1959) développant à son propos le paradigme du rationaliste critique. Une théorie dispose que tous les corbeaux (oiseaux du genre *Corvus*) sont noirs. Or un signal faible produit une expérience cruciale : on a repéré un corbeau blanc. Dans un premier cas, soit il s'agit d'une erreur ou d'un trouble cognitif (e.g. : erreur d'observation ou illusion perceptive), soit il y a corbeau qui temporairement a été ou est devenu blanc (e.g. : devenu blanc par vieillesse), soit quelqu'un a fait croire qu'existe un corbeau blanc (e.g. : en peignant un corbeau en blanc, en construisant un faux corbeau en carton blanc, en altérant l'instrument d'observation…). Dans le premier cas, il convient d'abord de réexaminer la véracité et la robustesse informationnelle des observations, des observables et des observés ainsi que la fiabilité des observateurs. Dans un second temps, il faut vérifier les sources et capteurs, ainsi que les procédures de filtrage et d'amplification des signaux, pour une cyber confiance. On peut également mettre en évidence un aspect transitoire de l'observable, ou une intention nocive et l'existence d'un acteur malfaisant. Bien que la théorie soit devenue inexacte, on l'adapte. Elle doit alors évoluer par affinement ou précisions conceptuelles : tous les corbeaux sont noirs, sauf les albinos, qui devront alors faire l'objet d'une théorie propre, ou sauf les peints en blancs, ou sauf les vieux oiseaux, etc. S'il s'avérait que les affinements successifs faisaient perdre tout sens à la théorie, celle-là serait alors abandonnée pour être devenue incapable de décrire et expliquer la réalité : il existe vraiment des corbeaux blancs.

L'abandon des théories établies est coûteux, et surtout anxiogène si l'on ne dispose pas de théorie alternative. Il soulève des résistances notables chez les adeptes de la théorie comme chez ses utilisateurs qui devront modifier leur conception d'une partie du monde et leurs procédures expérimentales qui s'y attachent. Cette crise ouvre, en science une révolution épistémologique, en sociologie une révolution conceptuelle, et partout à une crise de la représentation et des modèles interprétatifs de la réalité. Il est donc prudent de flanquer toute certitude d'interprétations secondaires qui peuvent alors servir de base à une nouvelle conception du réel.

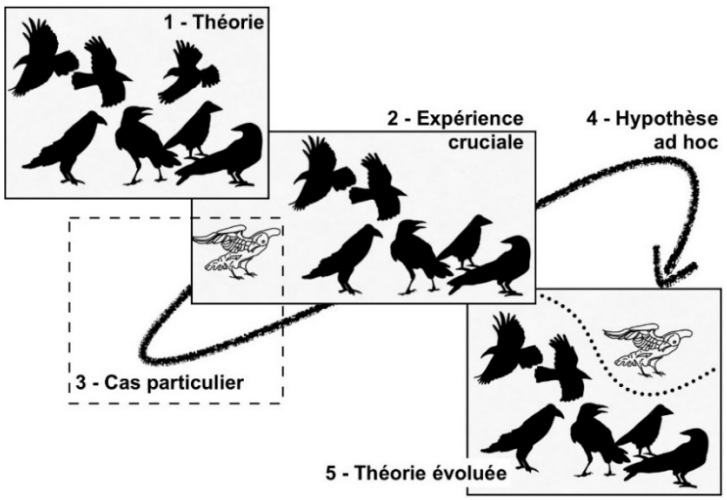


Figure 4-14 : Processus d'évolution des théories par affinement, pour ne pas devenir de simples croyances (Claverie, 2019).

Là encore, plusieurs dangers du *cognitive warfare* dans lesquels il est facile de tomber peuvent être théorisés. Le premier consiste en l'accumulation de fausses certitudes, par induction ou abduction répétées, sans vérification possible, et élaboration conséquente d'une forme de croyance en un modèle erroné. Le second consiste à utiliser l'accumulation de contre-exemples pour déguiser l'un d'eux qui passera inaperçu, en déguisant en noir un corbeau blanc. Enfin, la saturation des temps d'analyse réside dans la culture de l'ambiguïté, avec toutes les gammes de corbeaux gris. Les mesures de prévention sont d'autant plus critiques qu'elles sont difficiles à anticiper.

4.11 DES LIMITES DE LA PAUVRETE COGNITIVE

Le *cognitive warfare* est donc l'art de tromper le cerveau ou de le faire douter sur ce qu'il croit savoir. Son domaine de jeu est celui des limites, contraintes et stéréotypies de la pensée humaine, des fausses théories et de la culture de l'erreur dans laquelle il mène l'adversaire. L'altération des processus cognitifs sert de base à une réelle action d'autant plus facile qu'elle exploite la puissance du numérique. Concevoir même cette action n'est pas chose facile. Et cela rencontre plusieurs résistances : celle des opérateurs comme celle des décideurs. Dans cette nouvelle guerre desthéories, les pratiques et les doctrines n'évoluent pas aussi rapidement que les technologies et l'inventivité de ceux qui s'en servent, en usent où en abusent. Pour l'heure, plusieurs problèmessont évidents.

Le premier est celui de la discrétion et de l'insensibilité ; la stratégie cognitive n'est pas publique et elle reste « locale ». On n'en constate que les effets, et sa validité n'est alors établie qu'à postériori, souvent lorsque c'est trop tard. Le second réside dans l'incapacité spontanée du cerveau humain à concevoir qu'il est lui-même soumis à des contraintes, préférences et limitations, pouvant être l'objet d'action extérieure. L'incapacité est celle qui fait que ce n'est pas parce qu'on sait qu'on pense mal qu'on va penser mieux. Savoir que les deux formes de la Figure 4-11 sont les mêmes ne nous aide pas à les voir égales. Et l'apprentissage ne peut rien à cela. On peut néanmoins y porter attention et essayer de contrôler sa pensée ou celle des collaborateurs, en éliminant les fausses certitudes et en valorisant celle qui sont attestées.

Un autre problème concerne la confusion facile entre monde réel et monde numérique. Ce n'est pas parce que le numérique nous dit quelque chose de la réalité que c'est autre chose qu'une vérité numérique. Il convient de l'interpréter au mieux pour une action la plus concrète possible. Cemonde numérique peut être lui-même objet de distorsions, omissions de tout ou parties, ou au contraire d'ajouts ou d'illusions spontanées ou induites.

La confusion entre corrélation et causalité, ou la confusion dans le sens de la causalité sont dus à la confusion temporelle caractéristique de la pensée humaine. Elle est spontanément abductive, voire inductive, alors que la seule vérité émerge de la déduction. Le raisonnement ou la vérification déductive prennent des délais dont ne disposent souvent pas les acteurs. Dans beaucoup de cas, le temps imparti à la réflexion est limité, trop bref pour mobiliser des processus rationnels, valorisant d'autant plus des formes de pensée partiellement erronées qui pourtant s'avèrent souvent efficaces. Là réside un autre danger. Les observations répétées et les habitudes de pensée mènent à une sorte d'activité cognitive conjuratoire, automatisée, dont on ne peut pas sortir sans malaise, angoisse ou refus de l'incertitude. Les biais cognitifs sont des formes de raisonnement intuitif qui consistent à minimiser les solutions improbables et chercher des lois générales spontanées à partir de faits particuliers. Cette notion s'oppose à une logique d'exploration systématique énergivore autant que chronophage, et à laquelle refusent de se soumettre la majorité des personnes.

Enfin, la négligence des signaux faibles semble être une constante cognitive. De manière générale, il s'agit d'une nécessité, et eux qui sont soumis à la prégnance des signaux faibles sont incapables d'une pensée normale. La clinique psychopathologique est éclairante. Pourtant, les détails sont souvent importants et le « corbeau blanc » peut s'avérer un indice majeur de la conduite d'une sainepensée. Pourtant, il est délaissé, voire nié. La négligence des signaux faible est probablement due à une culture occidentale de la simplification par « ébarbement », dont la conviction a fait les choux gras d'une certaine

« idée de l'essentiel ». Le « rasoir d'Occam » est d'ailleurs devenu le pourvoyeur d'une pensée squelettique bien partagée. Les signaux faibles sont pourtant les lieux de l'évolution des certitudes ; c'est dans les marges qu'émergent les innovations, et le diable est aussi souvent dans les détails. À l'opposé, l'obsession du détail devient un handicap, canalisant sur lui l'attention laissée vacante pour d'autres éléments, partiels ou globaux.

4.12 LA CIBLE COGNITIVE DU C2

Le processus de la conduite des opérations militaires est désigné sous le terme de C2. Cet acronyme de *command and control*. Il s'agit d'un ensemble organisé de processus réglés, adaptés à la gestion d'une situation de crise. Il permet de mettre en œuvre et mener, grâce à l'exécution de lignes de force adaptées, une stratégie consistant à transformer des objectifs en réalisations concrètes concourant à la réalisation d'un état final recherché.

On considère le C2 comme un dispositif mobilisant plusieurs bases de l'intelligence humaine (Alberts et Haye, 2006) et son centre comme un ensemble de processus cognitifs supportés par trois piliers : la dominance informationnelle, la sécurité du traitement de l'information, la supériorité décisionnelle (Desclaux et Claverie, 2015).

Le C2 est le cœur de la machine militaire, de l'information à la décision pour la minimisation et la maximisation respectives des forces et puissances concrètes comme immatérielles, celles des ennemis et des alliés. Il est théorisé comme une véritable machine cognitive (Claverie et Desclaux, 2016). C'est donc le lieu de toutes les fragilités, et il nécessite toutes les attentions et préventions. Ceux qui le négligeraient seraient demain, le cas échéant, ceux qui le regretteraient.

En effet, autant le C2 peut être appliqué au traitement de situations complexes orientées, accident industriel ou écologique, gestion de foules, conflictualité unilatérale, autant il prend à nouveau une dimension particulière en quittant l'asymétrie. Le retour à des conflits de haute intensité deviendrait alors un combat des C2, et la supériorité porte à la fois sur la meilleure stratégie mais aussi sur la meilleure conduite de la stratégie. L'erreur cognitive devient une altération stratégique. C'est l'une des lignes de force.

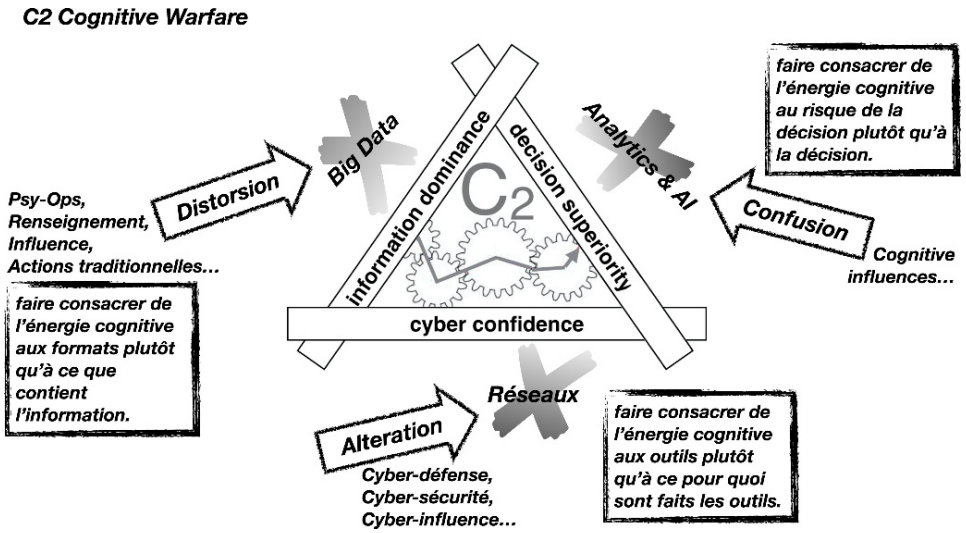


Figure 4-15 : Le triangle cognitif du *Command and Control* (C2) avec les trois bases des processus de dominance informationnelle, de cyber confiance et de supériorité décisionnelle, et les modes de l'action *cognitive warfare* utilisant les complémentarités des PsyOps, de la Cyber-influence et de la Cognitive supériorité, avec les modes d'attaque. (d'après Claverie et Desclaux, 2016).

Le *cognitive warfare* devient un outil d'atteinte, d'altération ou d'influence de la pensée stratégique comme des éléments cognitifs de sa mise en œuvre et de sa vie future. C'est l'aspect de supériorité décisionnelle qui en devient la cible privilégiée, en s'appuyant sur les deux autres volets de l'action psychologique et cyber.

4.13 CONCLUSION

La cognition fait l'objet d'une attention particulière des stratèges. On peut la définir comme l'ensemble des processus, mécanismes et actions, qui permettent de connaître le monde réel pour y agir ou agir sur lui. Chacune de ses dimensions fait l'objet d'un intérêt particulier du point de vue de l'action militaire et de la défense. La connaissance est nécessaire pour l'action et l'action pour la survie, la conquête ou la dominance. Elle impose le filtrage, la mémoire, la catégorisation et la compréhension sémantique, ainsi que la communication pour leurs échanges dans l'action collective. Ce sont autant de dimensions de la vie cognitive. L'action nécessite, quant à elle, la stratégie, l'anticipation et la programmation ; le comportement s'inscrit dans la nécessaire boucle du contrôle et de sa représentation pour l'ajustement. Les motivations sont similaires ; l'appétence dynamique et l'appétence cognitive ; bouger pour croître et survivre, bouger pour vivre et savoir.

Pourquoi en faire un contenu de la guerre ; la cognition est à la base de l'action du combattant comme du commandeur. Elle s'inscrit dans les dimensions de la tactique comme de la stratégie. Le *cognitive warfare* est un outil d'atteinte de la cognition de ceux qui conduisent, font ou évitent la guerre, En quelque sorte, le *cognitive warfare* constitue un ensemble tridimensionnel (information, numérique et décision) d'atteinte des éléments cognitifs de la pensée de l'opérateur militaire comme du stratège, dans une complémentarité psychologique, cybernétique et cognitique.

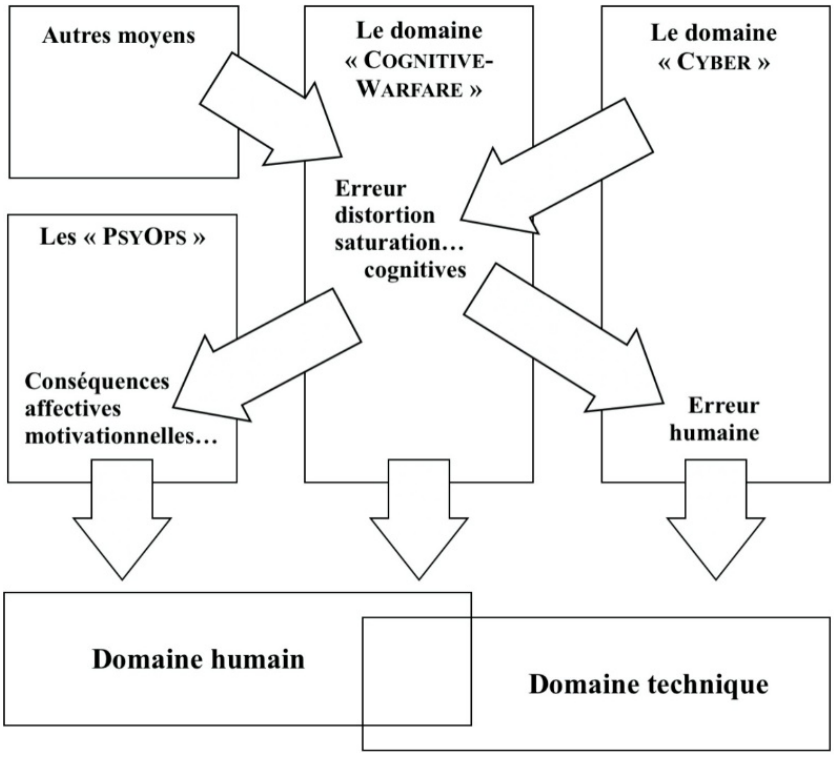


Figure 4-16 : Complémentarité du domaine humain et du domaine technique, et relations qu'ils entretiennent avec les domaines d'action de la guerre *cyber warfare*, *cognitive warfare* et PsyOps. Le *cognitive warfare* s'appuie sur ces deux bases afin de promouvoir l'action sur la cognition : action offensivedéfensive, comme préventive.

Les résistances cognitives, naturelles et spontanées, à admettre que l'on puisse soi-même être concerné ou que l'éducation, la formation ou l'habitude sont inadéquates à un traitement des distorsions cognitives, ainsi que les coûts d'énergie et d'investissement des processus de prévention parallèle, jugés superfétatoires, sont les deux meilleurs complices de l'acteur du *cognitive warfare*.

4.14 BIBLIOGRAPHIE

Alberts, D.S., Haye, R.E. (2006). Understanding Command and Control. Washington (DC, USA): CERP Publication Series. https://www.researchgate.net/publication/235144493_Understanding_Command_And_Control.

Berthet, V. (2018). L'erreur Est Humaine. Aux Frontières de la Rationalité. Paris (France) : CNRS éditions. https://www.cnrseditions.fr/catalogue/biologie-et-sante/lerreur-est-humaine/.

Claverie, B. (2005). Cognitique: Science et Pratique des Relations à la Machine à Penser. Paris(France) : L'Harmattan. https://www.editions-harmattan.fr/livre-9782747591355-20242.html.

Claverie, B. (2010). L'Homme Augmenté. Paris (France) : L'Harmattan. https://www.editions-harmattan.fr/livre-9782296133617-32941.html.

Claverie, B., Desclaux, G. (2016). C2 – Command and Control : un Système de Systèmes pour Accompagner la Complexité. Communication et Organisation, 50, 255-278. http://communicationorganisation.revues.org/5449.

Claverie, B. (2019). Introduction à l'Épistémologie et à la Méthode de Recherche à l'Usage des Ingénieurs et Autres Scientifiques de l'Industrie. Paris (France): L'Harmattan. https://www.editions-harmattan.fr/livre-9782343175676-63619.html.

Claverie, B. (2021). Des Théories pour la Cognition: Différences et Complémentarité des Paradigmes. Paris (France) : L'Harmattan. https://www.editions-harmattan.fr/livre-9782343234526-70130.html.

Desclaux, G., Claverie, B. (2015). "C2 et Cyber". Penser les Ailes Françaises, Paris (France) : Centre d'Études Stratégiques Aérospatiales, 32, 61-68. https://www.irsem.fr/data/files/irsem/documents/document/file/1859/PLAF_32.pdf.

Goffman, E. (1986). Frame Analysis: An Essay on the Organization of Experience (New edition). Boston (MA-USA): Northeastern University Press. https://www.academia.edu/9520207.

Hartley, D.S., Jobson, K.O. (2021). Cognitive Superiority: Information to Power, the Road to Winning in the Sixth Domain. New-York (NY-USA): Elsevier. https://www.springer.com/gp/book/9783030601836.

Heider, F. (1958). The Psychology of Interpersonal Relations. New-York (NY, USA): John Wiley and Sons. https://psycnet.apa.org/record/2004-21806-000.

Jastrow, J. (1900). Fact and Fable in Psychology. Boston (MA, USA), Houghton-Mifflin and Co. https://www.jstor.org/stable/2176513.

Jones, E.E., Davis, K.E. (1965). From Acts to Dispositions: The Attribution Process in Social Psychology. In L. Berkowitz (Ed.) Advances in Experimental Social Psychology, 2, 220-226. Miami (FL, USA): Academic Press. https://www.radford.edu/~jaspelme/443/spring-2007/Articles/Jones_n_Harris_1967.pdf.

Kahneman, D., Tversky, A. (1979). Prospect Theory: An Analysis of Decisions Under Risk. Econometrica, 47, 2, 313-327. https://www.uzh.ch/cmsssl/suz/dam/jcr:00000000-64a0-5b1c-0000-00003b7ec704/10.05-kahneman-tversky-79.pdf.

Kawabata, N., Mori, T. (1992). Disambiguating Ambiguous Figures by a Model of Selective Attention. Biological Cybernetics, 67, 5, 417-425. https://pubmed.ncbi.nlm.nih.gov/1391114/.

Kelly, K. (1995). Singular Visionary. Wired (Science) Singular Visionary: Sci-fi Master/Math Nerd Vernor Vinge Believes that Machines are About to Rule the Human Race as Humans Have Ruled the Animal Kingdom, 06-01-1995, 161. https://www.wired.com/tag/magazine-306.

Köhler, W. (1969). The Task of Gestalt Psychology. Princeton University Press : Princeton NJ, USA. https://press.princeton.edu/books/hardcover/9780691646794/the-task-of-gestalt-psychology.

Martinez, F. (2010). L'Individu Face au Risque : l'Apport de Kahneman et Tversky. Idées Economiques et Sociales, 3, 161, 15-23. https://www.cairn.info/revue-idees-economiques-et-sociales-2010-3-page-15.html.

Meng, M., Tong, F. (2004). Can Attention Selectively Bias Bistable Perception? Differences Between Binocular Rivalry and Ambiguous Figures. Journal of Vision, 4, 7, 539-551. https://pubmed.ncbi.nlm.nih.gov/15330700/.

Morel, C. (2002). Les Décisions Absurdes, Sociologie des Erreurs Radicales et Persistantes. Paris (France) : Gallimard. https://www.furet.com/media/pdf/feuilletage/9/7/8/2/0/7/0/4/9782070457663.pdf.

Nisbett, R.E. Ross, L. (1980). Human Inference: Strategies and Shortcomings of Social Judgment. Englewood Cliffs (NJ, USA): Prentice-Hall. https://www.jstor.org/stable/2392481.

Popper, K. (1959). The Logic of Scientific Discovery. Abingdon-on-Thames (UK): Routledge. https://books.google.fr/books?id=0a5bLBbe_dMC&printsec=frontcover.

Shepard, R.N. (1990). Mind Sights: Original Visual Illusions, Ambiguities, and Other Anomalies. with a Commentary on the Play of Mind in Perception and Art. W. H. Freeman and Company, Macmillan Higher Education, Henry Holt & Co, London. https://psycnet.apa.org/record/1990-98210-000.

Thaler, R., Sunstein, C. (2009). Nudge: Improving Decisions About Health, Wealth and Happiness. Yale University Press, New Haven CT, USA. https://www.consilium.europa.eu/fr/documents-publications/library/library-blog/posts/nudge-improving-decisions-about-health-wealth-and-happiness/.

Tversky, A., Kahneman, D. (1992). Advances in Prospect Theory: Cumulative Representation of Uncertainty. Journal of Risk and Uncertainty, 5, 4, 297-323. https://link.springer.com/article/10.1007%2FBF00122574.

Zajonc, R.B. (1968). Attitudinal Effects of Mere Exposure, Journal of Personality and Social Psychology. 9, II, 2, 1-27. https://www.psy.lmu.de/allg2/download/audriemmo/ws1011/mere_exposure_effect.pdf.

Chapitre 5 – CONFIANCE ENTRE LES HUMAINS ET LES MACHINES INTELLIGENTES ET BIAIS COGNITIFS INDUITS

Général Gilles Desclaux[1]

« L'homme a beaucoup appris des machines qu'il a lui-même construites, sauf peut-être savoir mieux vivre avec elles. »

Le domaine stratégique de la gestion de crise repose à la fois sur la connaissance de l'information la plus complète possible, la confiance dans les meilleures technologies qui les délivrent, et l'aptitude décisionnelle du commandeur qui s'appuie sur une organisation forte et efficace.

Dans le contexte de l'information massive, ces trois dimensions nécessitent le développement d'agents logiciels dits « intelligents », capables de sélectionner, fusionner et représenter les informations pertinentes et de proposer à haute vitesse des solutions décisionnelles. Ces agents sont développés par de grands industriels ; ils progressent de façon constante vers une plus grande autonomie. Malgré ces progrès, et face à une complexité croissante de la criticité des situations, le projet de systèmes purement autonomes s'éloigne des perspectives réalistes à court et moyentermes. Les experts de la gestion de crises et ces systèmes artificiels doivent de plus en plus travailler de manière collaborative, chacun apportant au duo humain-système le meilleur de ses compétences. La notion de confiance est alors centrale pour l'Interaction/Intégration Humain-Système (I_2HM), et la collaboration entre humains et machines. La robustesse ou la faiblesse de cette relation de collaboration est un enjeu clé pour la sécurité, et donc l'une des cibles de la guerre cognitive (*cyber warfare*).

5.1 LA COLLABORATION HUMAINS-MACHINES POUR LA GESTION DE CRISE

Le management des systèmes de défense ou d'opérations militaires est un domaine aussi complexe que codifié. La gestion rapide des crises en est un des domaines stratégiques. La doctrine, le droit de la guerre, la responsabilité quant à l'attrition humaine minimale pour une efficacité tactique matérielle adéquate bornent l'action du décideur qui doit pourtant agir vite et bien. Gérer une crise, c'est mobiliser de manière la plus efficace possible des moyens mis à disposition pour imaginer, évaluer et mettre en œuvre les solutions mesurées et mesurables les plus pertinentes menant à une solution favorable la plus rapide possible. Les crises peuvent être ponctuelles, en lieu comme en temps, ou plus globales et durables, nécessitant des ajustements ou des solutions dont la complexité évolue avec de multiples dimensions évolutives à prendre en compte.

Pour cela, la connaissance est le véritable « carburant » de la mesure, de l'anticipation et de la conduite de l'action. Elle est un critère majeur de différenciation pour maîtriser la criticité des situations. Elle s'élabore à partir de masses de données qui dépassent aujourd'hui les capacités humaines de représentation ou de compréhension globales, et nécessite le recours à des techniques utilisant les *Big Data*, l'intelligence artificielle » et la « visualisation » de solutions potentielles et changeantes sur lesquelles repose la décision.

Depuis quelques années, le développement d'agents logiciels « intelligents » progresse vers une plus grande autonomie. De nombreux obstacles restent à surmonter pour atteindre la perspective de véritables systèmes capables de se substituer efficacement aux experts humains. Dans un avenir proche, ces experts

[1] Gilles Desclaux est Général de Corps Aérien (2s), président de RACAM (Réunion Aviation Civile - Aviation Militaire). Il est chercheur du Laboratoire Human Engineering for Aerospace Laboratory (HEAL) – ENSC Bordeaux-INP / THALES. Il y coordonne la recherche sur les processus d'aide IA à la décision humaine « Anticipe » dans le « C2 Air. »

et les systèmes artificiels vont devoir continuer à « travailler en équipe », de manière encore plus collaborative. Le concept de *Human-Autonomy Teaming* (*HAT*) a été proposé pour cela par des équipes de la NASA en 2018 (O'Neill et al., 2020) pour rendre compte de cette « collaboration étrange », qui mêle Intelligence artificielle (IA) et Intelligence naturelle (IN). Elle contribue à l'émergence de systèmes hybrides, anthropotechnique, une forme d'intelligence duale et partagée, qui n'est pas sans poser de problèmes concrets de fragilité et de fiabilité dans le domaine cognitif.

5.2 UNE COOPERATION BASEE SUR DES PROCESSUS COGNITIFS DIFFERENTS

Le processus de décision mis en œuvre par les humains est radicalement différent de celui des machines intelligentes. Des architectures cognitives identiques pourraient faciliter la communication, mais contrairement aux humains, les machines sont restreintes à des objectifs et des priorités bien définis, sans capacité d'improvisation ou d'adaptation interprétatives, et sans réelle inventivité au-delà de la proposition algorithmique de solutions inattendues. Les humains, cependant, peuvent développer ces qualités mais restent médiocres dans la description précise de leurs intentions, de leurs objectifs et de leurs priorités comme les machines intelligentes l'exigent. De même, leurs capacités en attention, en mémoire ou en fiabilité de raisonnement sont fragiles et fréquemment mises en défaut alors que les systèmes artificiels sont particulièrement fiables en la matière.

Au sein d'un « réseau décisionnel » de type HAT, humains et machines modifient continuellement leurs propres rôles, tâches et relations avec les autres acteurs, naturels comme artificiels, partenaires comme extérieurs. Cette activité est dite « réseaux centrée ». Lorsque les processus habituels semblent ne pas correspondre à leurs attentes, des stratégies nouvelles sont mises en œuvre : les machines ouvrent des procédures de consultation de bases de données extérieures, alors que les humains constituent ou restructurent des groupes de travail informels ou ad hoc, et recherchent de nouveaux experts.

Les machines intelligentes restent et resteront, tout au moins dans un proche avenir, partiellement incompréhensibles pour les humains. Il en est évidemment de même des humains pour les machines. Établir une confiance entre les deux types d'entités est donc difficile. Les machines intelligentes sont sensibles aux cyber-intrusions qui peuvent compromettre leurs « perceptions », la pertinence de leur « prise de décision » et leurs capacités de gestion de données et de communication. Les humains présentent d'autres fragilités, telles que fatigue, mémoire limites, et capacités cognitives fragiles et influençables. Dans un tel contexte, une solution consiste à favoriser l'établissement de relations constructives de surveillance de la performance, entre experts humains, entre machines et, dans les deux sens, entre experts et machines.

5.3 LE PROBLEME DE L'INTERPRETABILITE

L'interprétabilité présente deux dimensions. Dans un premier aspect, elle correspond, pour l'utilisateur d'un système automatisé ou autonome, à son degré de compréhension de ce que le système fait, comment il le fait et pourquoi il le fait. L'interprétabilité du système peut conduire au développement d'un modèle cognitif aussi complet que possible afin de fournir une compréhension de son fonctionnement, et la capacité de prédire ce qu'il ferait dans certaines circonstances. Deux approches permettent de faciliter l'interprétabilité :

- La rétroaction (*feed-back*) du système améliore l'expérience des interactions avec les utilisateurs et facilite leur sentiment de contrôle. Ceux-là souhaitent habituellement que le système fournisse lui-même des informations compréhensibles sur son propre niveau de fiabilité afin de pouvoir ou non lui faire confiance.
- L'explication post-hoc, connue dans le monde anglo-saxon sous le nom d'IA explicable (Adadi et Berrada, 2018) ou XAI, fournit à l'utilisateur une explication qui justifie la prise de décision, rendant ainsi le système plus interprétable et facilitant le Retour d'expérience (Retex).

Dans un second aspect, l'interprétabilité concerne la limitation, pour l'utilisateur ou le partenaire humain, à des comportements ou des prises de décisions compréhensibles pour la machine, ou cohérentes avec ses propres registres de connaissances. Cette limite est nécessaire au maintien du lien de collaboration efficace. Cette dimension n'est pas sans poser de problèmes d'acceptabilité pour des utilisateurs humains naïfs, qui doivent apprendre à collaborer avec les machines pour faciliter la compétence et le maintien de l'efficacité du système HAT. Là encore, les systèmes apprenants sont soumis à la fréquentation des experts et doivent pouvoir les identifier afin de s'adapter à leurs particularités et les spécificités de leurs caractéristiques cognitives : personnalité, âge, performances mnémoniques plus ou moins grandes, visuelles ou formelles, sensibilité aux sons ou aux images, dépendance ou indépendance au champ, saturations attentionnelles, résistance à la fatigue, maîtrise du stress, etc. Le recours aux technologies portables (*wearable tech*.), aux capteurs et aux auto-quiz sur tablettes est aujourd'hui étudié pour cela par les laboratoires de l'U.S. Army (Buchler et al., 2016) et dans le cadre de collaborations entre certains industriels et des écoles d'ingénieurs universitaires ou de la Défense des pays de l'OTAN.

Bien que cette piste soit encore exploratoire, on prévoit des technologies capables de faciliter la collaboration et l'efficacité du couple humain-système et la performance de la mission en fonction du partenaire humain reconnu et identifié par la machine, et qui informe en continue la machine de l'évolution de son état cognitif et de ses connaissances.

5.4 L'EVALUATION DE L'INCERTITUDE

À ce jour, la plupart des automatisations décisionnelles fonctionnent de manière satisfaisante pour des situations spécifiques, et pour lesquelles elles sont conçues, mais nécessitent le recours à une expertise humaine dès qu'il s'agit de gérer des situations en dehors de certains environnements définis ou limités. Notamment, lorsque les algorithmes informatiques sont confrontés à l'incertitude et à l'ambiguïté des données, ils sont souvent dépassés dans le registre de la prise de décision.

Les humains surpassent les machines pour la compréhension du contexte. Les machines restent incapables d'exercer un jugement nuancé sur les environnements complexes ou ambigus et évolutifs. De plus, étant donné que des machines sont programmées ou entraînées à l'aide d'ensembles d'informations pertinentes pour une tâche ou un problème spécifique, rencontrer un nouveau problème à tendance à entraîner des ambiguïtés, voire provoquer un échec. La capacité humaine à s'adapter à de nouvelles situations est bien supérieure et même des réponses incomplètes ou imparfaites sont susceptibles d'être performantes. Les humains utilisent des capacités de substitution mentale et des estimations à partir de compétences ou de tâches familières, et peuvent ainsi fournir des réponses approximatives, ce que les technologies d'IA ne sont pour l'instant pas capables de faire.

Ils surpassent également les machines dans ce qui est leur capacité à évaluer la qualité de leur cognition. La métacognition est une des caractéristiques de l'esprit humain. Elle échappe pour l'instant à la machine. Des travaux sont entrepris afin de comprendre ce phénomène d'expertise sur sa propre expertise cognitive, en donner un formalisme qui puisse être compris par la machine, et doter celle-là de capacités de « méta-programmatique » pour s'évaluer elle-même, être capable d'évoluer, et surtout d'évaluer la cognition humaine pour s'adapter à son évolution ou sa performance dans une relation HAT dynamique.

5.5 LE MANQUE DE TRANSPARENCE

Lorsque les systèmes autonomes manquent de compréhensibilité et de prévisibilité, on évoque un problème de manque de « transparence ». Cette notion désigne l'incapacité qu'a l'humain de comprendre pourquoi le système prend telle mesure ou, au contraire, ne prend pas la décision d'une action attendue. Le manque de transparence produit un manque de conscience, notamment il ne permet pas aux opérateurs de savoir quelles sont les informations utilisées pour effectuer une tâche.

Ce manque de transparence est alors parfois à l'origine d'un manque de confiance qui conduit à la fois à une sous-utilisation du système par méfiance ou au contraire à une surutilisation en raison d'une confiance aveugle (Clark et al., 2014). Ce problème de confiance doit pouvoir être évalué sur des bases objectives, avec des indicateurs clairs.

Ces domaines de difficultés ne sont pas des problèmes indépendants et peuvent se combiner de manière souvent dangereuse (Endsley, 2016). Les systèmes intelligents sont fragiles, et peuvent rapidement passer d'un bon fonctionnement à une dégradation rapide et globale. Il incombe donc à l'opérateur humain de surveiller la survenue de telles défaillances, et d'en anticiper les conséquences. Or surveiller un système qui semble fonctionner correctement est un travail pour lequel les humains sont mal préparés. On évoque ici des phénomènes de « mise hors de la boucle », ou *Out-Of-The-Loop* (*OOTL*), en anglais (cf. Suhir, 2021), qui induisent une conscience restreinte, voire très réduite de la situation (Endsley, 2015).

5.6 LA CONFIANCE AU CŒUR DE LA RELATION HUMAIN/MACHINE INTELLIGENTE

Dans le contexte HAT, la confiance doit être examinée à deux niveaux.

Pour la machine, la qualité de la relation se base sur des algorithmes statistiques de surveillance psychophysiologique ou de qualité et quantité d'information échangée. Le monitoring des partenaires humains peut permettre la mise en œuvre de processus automatisés ou de rappel à l'opérateur. Ce type de processus est particulièrement étudié dans l'aide à la conduite automobile et la détection d'états d'endormissement ou de baisse d'attention du conducteur, mais également la non-détection de dangers imminents (piéton, obstacles, verglas, etc.). Le formalisme computationnel requis nécessite un modèle cognitif du conducteur (Bellet et al., 2011). La cyber défense de ces programmes reste une des préoccupations majeures face à la nécessité d'évolution et de mise à jour permanente des logiciels.

Pour le partenaire humain, la confiance est généralement définie comme « le degré auquel un utilisateur pense qu'un système se comportera comme prévu ». Sans ce niveau de confiance approprié, les opérateurs peuvent refuser l'utilisation des systèmes autonomes ou au contraire se décharger complètement sur eux. Ces phénomènes de sur-dépendance pouvant aller jusqu'à l'échec, suivis d'une sous-dépendance à l'automatisation, sont bien documentés. Les principaux facteurs qui favorisent le développement de la confiance, sont l'acceptabilité, la tolérance, la transparence et la bidirectionnalité de la communication Humain/Système.

La confiance dépend du contexte spécifique d'une interaction humain/système intelligent, et est influencée par l'environnement et l'état mental de l'opérateur. L'utilité perçue d'un système autonome, en matière de capacité à effectuer une tâche difficile ou exigeante, influence la décision de l'individu de lui faire confiance. Mais les opérateurs ayant une charge de travail élevée ont aussi tendance à s'appuyer davantage sur la machine, quel que soit leur niveau de confiance réel dans le système. L'automate, en dehors des tâches simples, ne remplace généralement pas complètement l'humain. Au contraire, il change la nature de son travail en le délestant de certaines tâches pour lesquelles il est plus performant. Cela pose clairement le problème de l'acceptabilité réciproque. La compréhension, la capacité d'utilisation et l'attente des utilisateurs d'un système intelligent sont corrélées à la probabilité de faire confiance.

La confiance se construit au fil du temps et, en conséquence, pour le partenaire humain, la formation et l'entrainement favorisent la familiarité nécessaire à l'utilisation du système. Pour cequi est du système artificiel, elle doit aujourd'hui être programmée faute de pouvoir disposer d'algorithmes évolutifs, voire de machines adaptatives.

5.7 LES BIAIS COGNITIFS DANS LE DUO HUMAIN-SYSTEME

La transparence est ce qui permet à l'opérateur de déterminer si la machine autonome est susceptible de fournir la bonne réponse dans une situation complexe donnée, et ce qui permet à la machine de savoir si les informations données par l'humain sont dignes de confiance ou présentent des incongruités qu'il convient d'éclaircir.

Mais, cette transparence va au-delà de la simple mise à disposition des informations à l'opérateur humain ou au partenaire artificiel autonome. Pour être transparent, l'automate doit présenter les informations de manière adaptée au modèle mental de l'opérateur, en tenant compte de ses préférences et contraintes cognitives, alors que, à l'inverse, le partenaire humain doit s'adapter au modèle mental du concepteur du programme. Là réside un premier biais cognitif : la machine n'est pas un partenaire comme un autre, elle a été programmée par quelqu'un. Elle peut d'ailleurs être déprogrammée, reprogrammer, subir l'influence de patchs ou de programmes complémentaires, et donc de virus, chevaux de Troie et autres malwares. Ce biais de dissonance cognitive est d'autant plus grâce qu'il s'impose sans réelle solution, face à des informaticiens ou industriels persuadés queleur mode de pensée est le meilleur pour les autres.

Les biais cognitifs sont des distorsions spontanées de la pensée rationnelle qu'adoptent les humains et qui sont à là sources de nombreuses erreurs (Kahneman et Tversky, 1974). Ils sont étudiés par leséconomistes et les psychologues, notamment pour ce qui est de la prise de décision, mais ils font l'objet d'une attention nouvelle de ces experts et de ceux du traitement de l'information, avec l'étude des biais des machines (Bertail et al., 2019) et la création algorithmique d'inéquité, voire de discrimination posant des problèmes éthiques incontournables.

Dans un contexte d'informations massives, et pour ce qui est des usagers des systèmes, les humains se concentrent le plus souvent sur des sources et des méthodes de sélection qu'ils connaissent bien et auxquelles ils font confiance, introduisant de ce fait un autre type redoutable de biais. C'est un domaine où les machines sont pourtant très performantes, apportent une vitesse élevée d'acquisition et de traitement de gros volumes d'informations, ainsi qu'une gestion cohérente, rigoureuse et impartiale des données. Mais sans un niveau de transparence qui permet de reconnaître les sources d'information et d'en analyser la qualité, l'efficacité de tels systèmes restera insuffisante, et le doute reste sous-jacent à la relation de l'humain face à la machine.

Un exemple permet d'illustrer cette notion. Un système semi-autonome présente plusieurs options qu'il a générées, accompagnées d'évaluations d'efficacité potentielle quant à l'adéquation de chacune d'elles. Un tel dispositif de facilitation de la transparence doit être accompagné de la possibilité, pour l'opérateur, d'ajouter des informations que le dispositif autonome ne connaît pas. L'opérateur doit pouvoir proposer des solutions et les faire évaluer par l'automate. La résolution collaborative de problèmes est alors un processus de va-et-vient, de type *wargaming*. Ce type de communication bidirectionnelle favorise le partenariat et permet d'évaluer les solutions favorables de résolution potentielle de problème.

Un troisième type de biais concerne le sentiment spontané de supériorité de l'humain sur la machine. Un niveau d'engagement cognitif faible rend intrinsèquement difficile, pour un opérateur, de comprendre ce qui se passe quand il n'exerce qu'une surveillance passive d'un système autonome. La passivité dans l'exécution d'une tâche est alors un obstacle à l'efficacité de l'interaction humain-machine intelligente. Ce défi dépend de ce que certains auteurs (Endsley, 2016) désignent comme « énigme de l'automatisation ». Ainsi, « plus on ajoute d'automatisation à un système, et plus cette automatisation est fiable et robuste, moins il est probable que les opérateurs humains la supervisent. Ils seront alors incapables de comprendre la situation, et auront tendance à reprendre le contrôle du système. Le système devient alors dégradé, restreint aux simples capacités limitées des opérateurs, ce qui est évidemment un avantage significateur pour l'ennemi potentiel. L'énigme de l'automatisation crée un obstacle majeur à l'autonomie dans les domaines où la sécurité est critique.

5.8 CONCLUSION

La complexité de la gestion de crises demande aujourd'hui de traiter une quantité de données, et de prendre des décisions souvent critiques dans des temps de plus en plus courts et dans des contextes de plus en plus contraints. Les décideurs à la tête d'organisations de gestion de crise doivent donc deplus en plus se reposer sur des systèmes hybrides. L'aide de systèmes intelligents est devenue indispensable. Malgré les performances incontestables de tels systèmes, ils sont encore incertains dans plusieurs domaines, et les humains, qui continueront de jouer un rôle important dans cette collaboration avec les machines, ont une tendance à ne pas maîtriser un ensemble de biais générés par l'échange HAT. Des voies de progrès résident d'une part dans la capacité de ces machines à mieux expliquer, à établir une confiance étayée, à communiquer plus aisément, voire à comprendre les intentions dissimulées et les émotions des acteurs humains, et d'autre part dans une nouvelle culture d'acceptation des machines par les humains.

Dans un article fondateur (2017), Kott et Alberts, écrivaient : « Bienvenue à bord des choses intelligentes. Quelles que soient nos lacunes respectives, nous serons plus forts et plus agiles en travaillant ensemble dans les organisations décisionnelles. »

5.9 BIBLIOGRAPHIE

Adadi, A., Berrada, M. (2018). Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). IEEE Access, 6, 52138-52160.

Alberts, D.S., Haye, R.E (2006). Understanding Command and Control. Washington (DC-USA) : DoD CCRP Publication Series.

Bellet, T. Mayenobe, P. Gruyer, D. Bornard, J.C. Claverie, B. (2011). The Living Cognition Paradigm: An Application to Computational Modeling of Drivers' Mental Activities. US-China Education Review, 1, 4, 568-578.

Bertail, P., Bounie, D., Clémençon, S., Waelbroeck. P. (2019). Algorithmes : Biais, Discrimination et Equité. Rapport de la Fondation Abeona et de Télécom ParisTech. Paris (France) : Telecom ParisTech.

Buchler, N., Fitzhugh, S.M., Marusich, L.R., Ungvarsky, D.M., Lebiere, C., Gonzalez, C. (2016). Mission Command in the Age of Network-Enabled Operations: Social Network Analysis of Information Sharing and Situation Awareness. Frontiers in Psychology, 7, 937, 1-15.

Clark, B.B., Robert, C., Hampton, S.A. (2014). The Technology Effect: How Perceptions of Technology Drive Excessive Optimism. Journal of Business and Psychology, 15, 4-18.

Claverie, B. (2005). Cognitique, Science et Pratique des Rapports à la Machine à Penser. Paris (France): L'Harmattan.

Claverie, B., Desclaux, G. (2015). La Cybernétique : Commande, Contrôle et Comportement dans la Gestion des Systèmes D'information et de Communication. Hermès, 71, 72-79.

Endsley, M. (2015). Situation Awareness Misconceptions and Misunderstanding. Journal of Cognitive Engineering and Decision Making, 9, 1, 4-32

Endsley, M. (2017). From Here to Autonomy : Lessons Learned from Human-Automation Research. Human Factors, 59, 1, 5-27.

Gutzwiller, S.R., Espinosa, S.H., Kenny, C., Lange, D. (2018). A Design Pattern for Working Agreements in Human-Autonomy Teaming. In D.N. Cassenti (Ed.) Advances in Human Factors in Simulation and Modeling : Proceedings of the AHFE 2017 International Conference on Human Factors in Simulation and Modeling. New-York (NY, USA) : Springer, 12-24.

Kahneman D., Tversky, A. (1974). Judgment Under Uncertainty: Heuristics and Biases. Science, New Series, 185, 4157, 1124-1131.

Kott, A., David S.A. (2017). How Do You Command an Army of Intelligent Things? Computer, 12, 96-100.

Le Guyader, H., Eshelman-Hayne, C., Irandousr, H., Lange, D., Genchev A., Cakir M., Verstraete, E., Brill, J.C., Desclaux, G. (2021 – à paraître – H. Leguyader Ed.). Human Considerations for Artificial Intelligence in Command and Control. Technical Report of the NATO Science and Technology Organization Research Group IST-157, NATO. Paris (France) : NATO-STO Collaboration Support Office.

O'Neill, T., McNeese, N., Barron, A., Schelble, B. (2020). Human-Autonomy Teaming: A Review and Analysis of the Empirical Literature. Human Factors. 2020 octobre 22, 18720820960865.

Shively, R., Lachter, J., Brandt, S.L., Matessa, M., Battiste, V., Johnson, W. (2018). Why Human-Autonomy Teaming? Proceedings of the AHFE 2017 International Conference on Neuroergonomics and Cognitive Engineering, July 17–21, 2017, Los Angeles (CA, USA). Advances in Neuroergonomics and Cognitive Engineering, 586, 3-11.

Suhir, E. (2021). Human-In-The-Loop: Probabilistic Modeling Approach in Aerospace Engineering. Boca Raton (FL, USA) : CRC Press.

Chapitre 6 – MATURITE TECHNIQUE DES SYSTEMES COGNITIFS DES RESEAUX HUMAINS[1]

Docteur Norbou Buchler[2]

6.1 TENDANCES DU DEVELOPPEMENT DES RESEAUX

La première tendance est le développement de l'organisation en réseau. Les progrès des technologies de l'information et des réseaux transforment de manière significative la façon dont les organisations humaines fonctionnent et communiquent entre elles. Ces organisations en réseau sont au cœur des tissus sociaux, politiques, militaires ou économiques du XXI^{e} siècle. La gestion et la protection de la convergence systématique entre personnes, informations et technologie est un des principaux défis de notre époque.

Cette transformation est assez récente et a été très rapide. Pour les organisations militaires, elle s'est opérée au tournant du siècle, vers 2003 pour les pays nord-américains et leurs alliés de l'OTAN, et aimpacté nombre d'entre nous, modifiant profondément les spécialités et même les carrières des spécialistes.

Socialement, les environnements opérationnels en réseau sont massivement collaboratifs : le nombre de collaborations potentielles est pratiquement illimité. Toutefois, ils présentent des désavantages potentiels tels que la complexité de plus en plus importante, et le déluge d'informations dans ces environnements en réseau peut rapidement submerger les capacités cognitives humaines. Le défi continu consiste à obtenir l'adéquation de la bonne information pourla bonne personne au bon moment.

La seconde tendance est celle d'une autonomie croissante : la nature du travail évolue constamment en raison de la vitesse foudroyante des changements technologiques. Cela inclut les outils etsystèmes d'intelligence artificielle et les technologies d'assistance automatique (AI/AA) dotées de plus en plus d'autonomie.

Dans les organisations militaires, un obstacle majeur reste celui de l'interaction des opérateurs humains et de leurs outils. Certains aspects clés sous-jacents à cette transformation de l'équipe d'Humain-agent autonome (HAT) sont les suivants : l'étalonnage des niveaux de confiance de la relation et sa transparence, notamment en ce qui concerne les hypothèses sous-jacentes, l'incertitudeet les processus de raisonnement.

Les humains et les machines ont chacun leurs forces et leurs faiblesses. Et en fin de compte, une preuve concrète du succès de cette association est que l'on obtient des niveaux de performance, grâce à la collaboration humains/machines, qui ne pouvaient antérieurement être obtenus sans une liaison complète et complémentaire entre humain et machine. Une de nos préoccupations reste que le développement rapide et la complexité de l'intelligence artificielle moderne limitent notre capacité à intuiter et imaginer les impacts futurs de l'utilisation de nouvelles technologies. Nous avons encore besoin de beaucoup d'expérience pour réussir en cela.

La troisième tendance concerne le *cognitive warfare* ou « guerre cognitive » qui exploite, à visées de déstabilisation, les cyberattaques, le Big Data et les médias sociaux. Les menaces de cybersécurité reposent sur des programmes malveillants, chevaux de Troie et autres botnets. La convergence des environnements cyber, physiques et sociaux est également un lieu de faiblesse, avec des attaques massives à grande échelle.

[1] Cette conférence a été donnée en Anglais et sa traduction en Français réalisée a posteriori par les organisateurs de la conférence.

[2] Norbou Buchler est docteur en psychologie expérimentale (PhD), spécialisé en neurosciences cognitives (IRM fonctionnelle) et modélisation computationnelle. Il est chef de la branche « Systèmes en réseaux » de la division « Intégration Humains-Systèmes » du DEVCOM Data & Analysis Center (DAC) de l'US Army – Aberdeen Proving Ground, Maryland, USA.

L'impact de l'intelligence artificielle sur les grandes bases de données et sur les réseaux sociaux constitue une menace majeure. Elle permet de tirer parti de la guerre de l'Information Cognitive (Cogiw)[3], dans une échelle sans précédent, pour déstabiliser les démocraties et miner les alliances. La furtivité des attaques, le manque d'attribution de causes ou d'auteurs, la tromperie et la méfianceconséquente sapent le tissu social.

Le document de l'OTAN-ACT de Cole et Le Guyader (2020) attire notre attention sur le « domaine humain » appuyé par l'AI (futur contrôle et surveillance des alliés), résonnant comme une alerte anticipée contre la déstabilisation des campagnes Cogiw. À mon avis, la thématique est plus vaste etconcerne la sauvegarde de la démocratie numérique, et apportant des garanties cyber-sociales tels que l'authentification en ligne des citoyens pour leur participation démocratique.

6.2 LE PROCESSUS DE DECISION INSTITUTIONNELLE

Par sa nature même, le *cognitive warfare* concerne la difficile question de la prise de décision organisationnelle. Pour relever ce défi, nous pouvons nous poser deux questions :

La première est de savoir comment altérer le processus de prise de décision dans les unitésennemies.

Le Dr Alex Kott, directeur scientifique du laboratoire de recherche de l'armée américaine, est un collègue de l'OTAN pour beaucoup d'entre vous. Je fais ici référence à certains de ses travaux intitulés *Breakdown of Control* ou « rupture du contrôle ». Sa thèse s'appuie sur la théorie des systèmes de contrôle et prend pour référence des exemples historiques pour affirmer que la tromperie et la méfiance au sein d'une organisation force à prendre des mesures de compartimentation et de vérification qui ralentissent et entravent considérablement l'action et la décision, provoquant une « rupture » dans la prise de décision organisationnelle (Kott, 2007). On note notamment des décisions tardives (retards), des modifications des seuils de décision dans la guerre de l'information, des excès d'inhibition (timidité) ou d'agressivité – gain faible ou élevé –, des erreurs d'autorenforcement, comme dans les boucles de rétroaction (voir aussi Kott, 2008 ; Kott et Alberts, 2017 ; Kott et Linkov, 2021 ; Théron, Kott et al., 2019, etc.).

La seconde question concerne le soutien à la prise de décision de notre propre coalition pouratténuer la menace précédente. Comment une organisation bien conçue, équipée et formée peut éviter d'être touchée par une telle attaque ? Avec ses propres équipements, cette organisation peut anticiper et répondre de manière décisive. On définit ici deux dimensions complémentaires qui sont d'une part les apports de l'entraînement et de la technologie, et d'autre part les modèles prédictifs, modèles mentaux humains ou modèles numériques programmés.

Une conceptualisation du cycle de prise de décision militaire est connue sous le terme de « boucle OODA » pour Observer – Orienter – Décider – Agir. Également connue sous le nom de « cycle de Boyd » (1976), elle définit un processus compétitif dans le temps par lequel un individu ou une organisation observe et s'oriente dans un environnement opérationnel et prend à plusieurs reprises etde manière itérée des décisions à la lumière d'événements dynamiques, tout en agissant de manière efficace. Il s'agit d'un cadre utile pour réfléchir aux fonctions organisationnelles, aux flux de travail et aux technologies de support.

On peut commenter quatre domaines techniques différents qui soutiennent la question de la prise de décision humaine et de l'efficacité organisationnelle (Figure 6-1). En fin de compte, ces domaines soutiennent l'efficacité de la mission.

[3] Cogiw : cognitive information warfare, guerre de l'information cognitive.

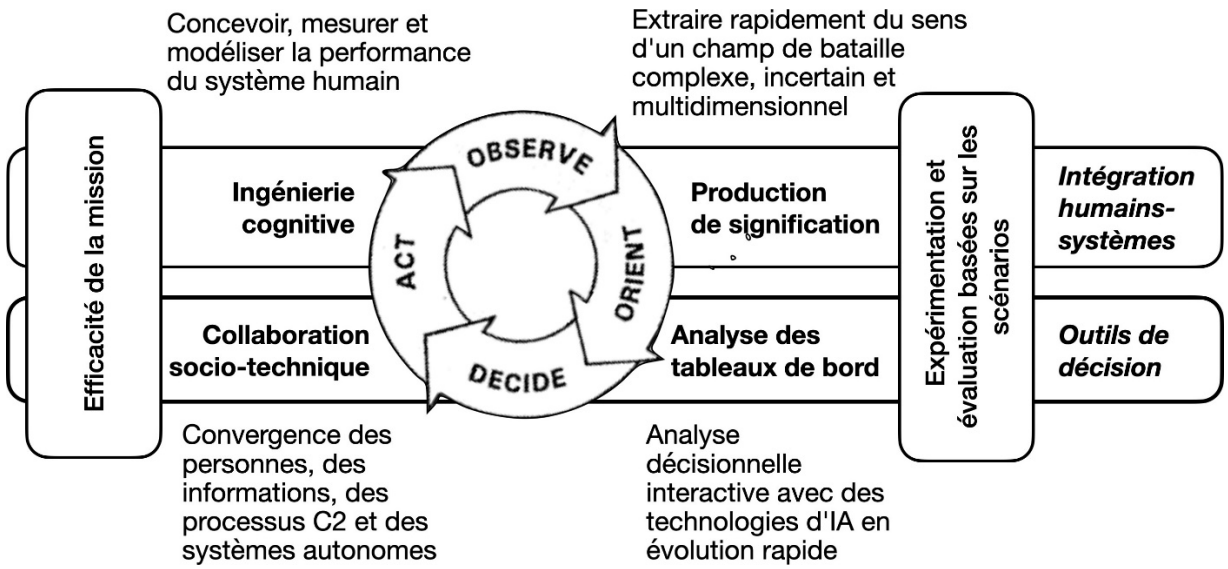


Figure 6-1 : Boucle OODA, ou cycle de Boyd, avec les 4 étapes : observation, orientation de l'action, décision, et action. Ce cycle conduit à une nouvelle observation qui réentendre le cycle de manière continue (selon Boyd, 1976).

On peut signaler l'importance de l'ingénierie cognitive et de l'intégration humains-systèmes. Néanmoins, la majorité de mon exposé va se concentrer sur la collaboration et plus précisément, la dimension cognitive des systèmes humains en réseau.

6.3 DES TRL AUX HRL OU *HUMAN READINESS LEVELS*

L'organisation dans laquelle j'effectue ma recherche, le U.S. Army Developmental Command (DEVCOM), et en son sein le Data & Analysis Center (DAC), s'intéressent à ce que le développement des technologies soit bien aligné sur les besoins du soldat. Il s'agit donc de s'assurer de la maturité de l'adaptation des technologies aux utilisateurs humains.

La notion *Technology Readiness Level* (*TRL*) existe depuis les années 1970, et désigne le niveau de maturité technologique d'un équipement ou d'un logiciel donné, allant du premier niveau du développement du concept à celui du prototypage en passant par les tests de développement et opérationnels (ISO, 2013). L'un des principaux défis du développement de la technologie est de s'assurer qu'elle prend en compte les dimensions humaines et organisationnelles de leur utilisation ; et c'est particulièrement le cas pour l'intelligence artificielle et les systèmes complexes pour soutenirle *cognitive warfare*.

Je me permets d'attirer votre attention sur les travaux récents d'une de mes collègues, le Dr. Pamela Savage-Knepshield (Savage et al., 2015) qui développe l'usage de la notion de Niveaux de préparation humaine (HRL) qui reflètent la logique des TRL pour une compréhension facile de la maturité de l'intégration humain-système (Handley et Savage-Knepshield, 2021). Cet indice fournit un numéro unique d'évaluation de la préparation à la communication pour une utilisation humaine. Pour chaque niveau, il y a à la fois des critères d'entrée et de sortie.

Les HRL s'appliquent universellement, des programmes scientifiques en technologie à l'acquisition de systèmes. Cela va de l'identification précoce des exigences basées sur les performances humaines à la conception et au perfectionnement de l'interface utilisateur, en passant par les évaluations successives des utilisateurs et par les tests opérationnels complets par les humains (Savage-Knepshield et al., 2021).

Actuellement, l'American National Standards Institute (ANSI) et la Human Factors and Ergonomics Society (HFES) envisagent de porter les Niveaux de préparation humaine (HRL) comme future norme.

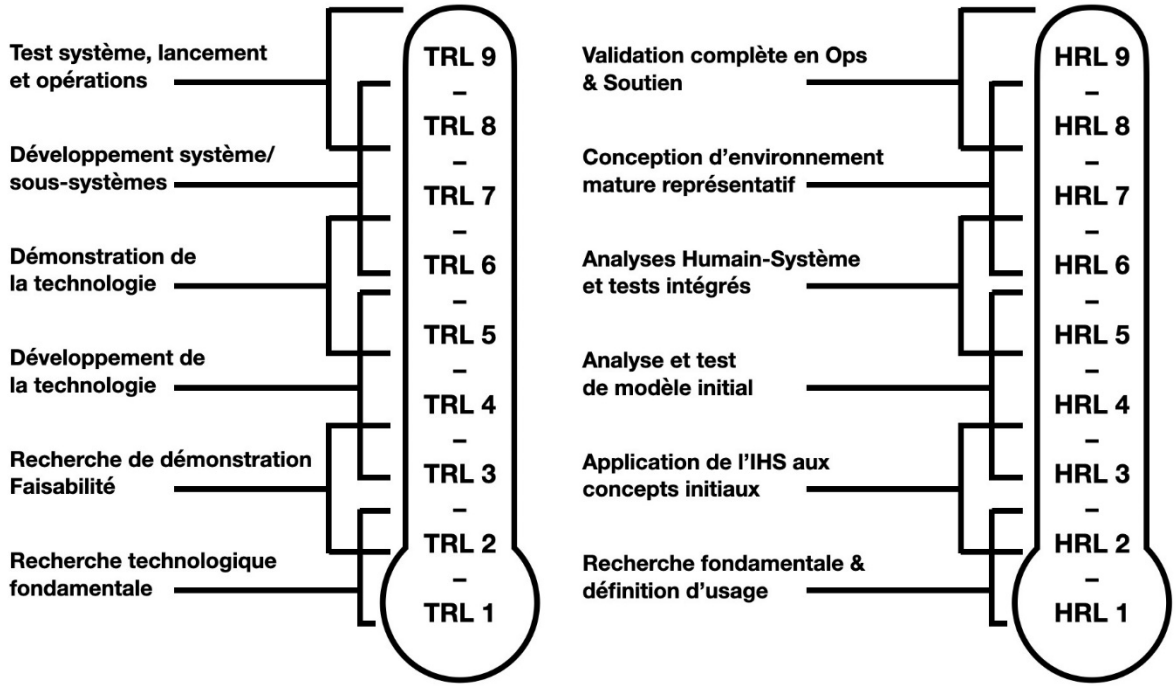


Figure 6-2 : Equivalence entre les deux échelles de maturité technologique (TRL) et de maturité des solutions technologiques pour les usages humains (HR).

6.4 BOITE A OUTILS D'OBSERVATION COMPORTEMENTALE

Pour ce qui est de l'Ingénierie Cognitive, le centre de recherche s'oriente également vers la numérisation des relevés et de l'ensemble des données d'observations comportementales.

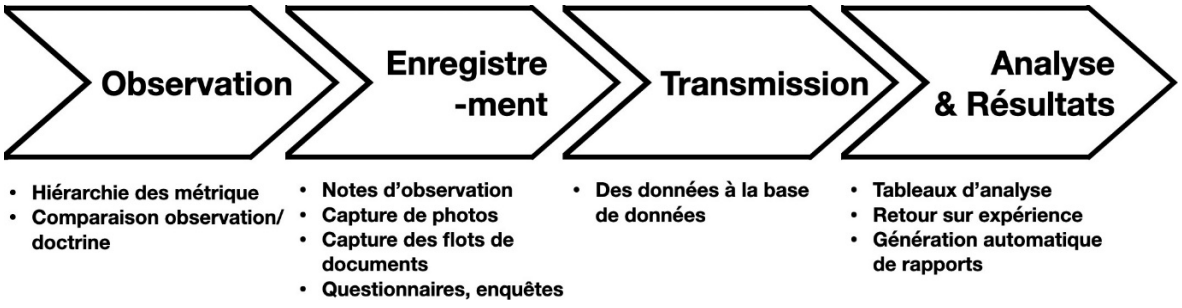


Figure 6-3 : Principe de la boite à outil d'étude IHS « BOLT ».

Une boîte à outils numérique a été constituée pour l'étude de l'ensemble des données d'observation comportementale. Il s'agit du « Behavioral Observations Logging Toolkit » ou BOLT.

Le système BOLT est basé sur une logique à quatre temps (cf. Figure 6-3). Il permet un saut technologique dans l'analyse IHS par rapport aux technologies courantes actuelles qui, même en utilisant des appareils portables tels que des smartphones ou tablettes, demande une retranscription, ne sont pas en temps réel,

n'agrègent pas les données de plusieurs observateurs et ne donnent pas une visibilité globale aux leaders des opérations en cours. La logique du système BOLT est de donner une représentation en ligne permettant l'évaluation de la formation, de la technologie et des opérations en prenant en charge tous les observateurs experts humains, en rationalisant la collecte des données, le suivi et l'analyse des informations sans délai (Garneau et al., 2020).

6.5 LES RESEAUX COGNITIFS ET LE *COGNITIVE WARFARE* COMME SCIENCE DES RESEAUX

En référence au film Matrix des Wachowski, nous pouvons choisir la pilule bleue, et ne rien voir, ou la rouge pour ouvrir les yeux et explorer le monde comme une série de réseaux interconnectés.

La Figure 6-4 est issue de l'U.S. Army Field Manual FM 3 – 13, Inform and Influence Activities (2016). Nous y voyons six types de réseaux qui traversent les domaines Politique, Militaire, Économique, Social, Infrastructurel et Informationnel (PMESSI) Les noeuds individuels peuvent représenter des personnes, des lieux ou bien des équipements.

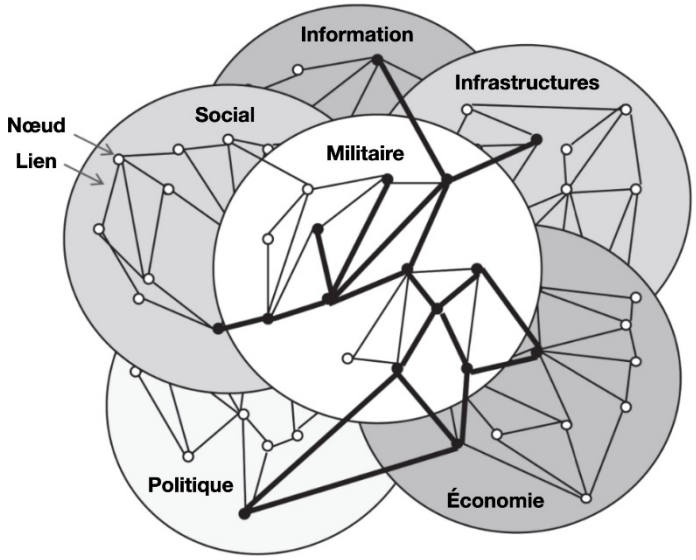


Figure 6-4 : Le réseaux PMESII influençant l'environnement opérationnel militaire, de plus en plus complexe et interconnecté (d'après l'U.S. Army Field Manual).

La Guerre Cognitive implique de cartographier tous ces différents types de réseaux et d'exploiter les interdépendances critiques qui existent entre eux. Par exemple, en 2015, un Russe a cherché à déstabiliser la capitale ukrainienne de Kiev par une attaque à plusieurs niveaux. Une cyberattaque a mis hors service des infrastructures électriques essentielles, privant 200 000 Ukrainiens d'électricité dans des quartiers majoritairement russes, et a été rapidement suivie d'une campagne de désinformation imputant la panne au gouvernement ukrainien. Cette attaque hybride a été menée sur 3 réseaux : Infrastructure, Social, Informationnel.

Je vais présenter plus en détail le travail scientifique appliqué que nous avons réalisé. Je vais me concentrer sur les travaux scientifiques appliqués que nous avons réalisés et qui visent à déterminer comment cartographier et comprendre trois de ces réseaux – les réseaux militaires, cognitif/social, et informationnel.

La transformation militaire des États-Unis et des pays de l'OTAN s'est déroulée dans un cadre conceptuel dit des « opérations en réseau » ou « réseaux-centrées » (*Network-Enabled Operations* (*NEO*)) développé par Alberts et al. (2004). Ses principes fournissent un cadre conceptuel pertinent pour comprendre la cognition humaine, la collaboration et l'efficacité organisationnelle dans le domaine militaire. Il comprend quatre principes principaux :

- Une solide mise en réseau d'une force améliore le partage de l'information et la collaboration ;
- Un tel partage et cette collaboration améliorent à la fois la qualité de l'information et la conscience de situation partagée ;
- Cette amélioration permet à son tour une auto-synchronisation supplémentaire et améliore la durabilité et la vitesse du commandement ; et
- La combinaison de ces facteurs augmente considérablement l'efficacité de la mission.

Ce cadre est cumulatif, de sorte que la communication et le partage de l'information agissent comme une boucle de rétroaction positive. Un partage accru de l'information entraîne une meilleure connaissance partagée de la situation. Ce qui, à son tour, favorise les adaptations organisationnelles telles que l'auto-synchronisation qui, en fin de compte, augmente l'efficacité globale de la mission. (Alberts et Garstka, 2004).

6.6 LA RECHERCHE DE FORT LEAVENWORTH

Notre recherche (Buchler et al., 2016) s'inscrit dans le contexte NEO. Elle a porté sur les deux premiers principes en examinant le partage de l'information et la connaissance de la situation lors d'un exercice militaire à grande échelle au Mission Command Battle Laboratory à Fort Leavenworth (KS-USA).

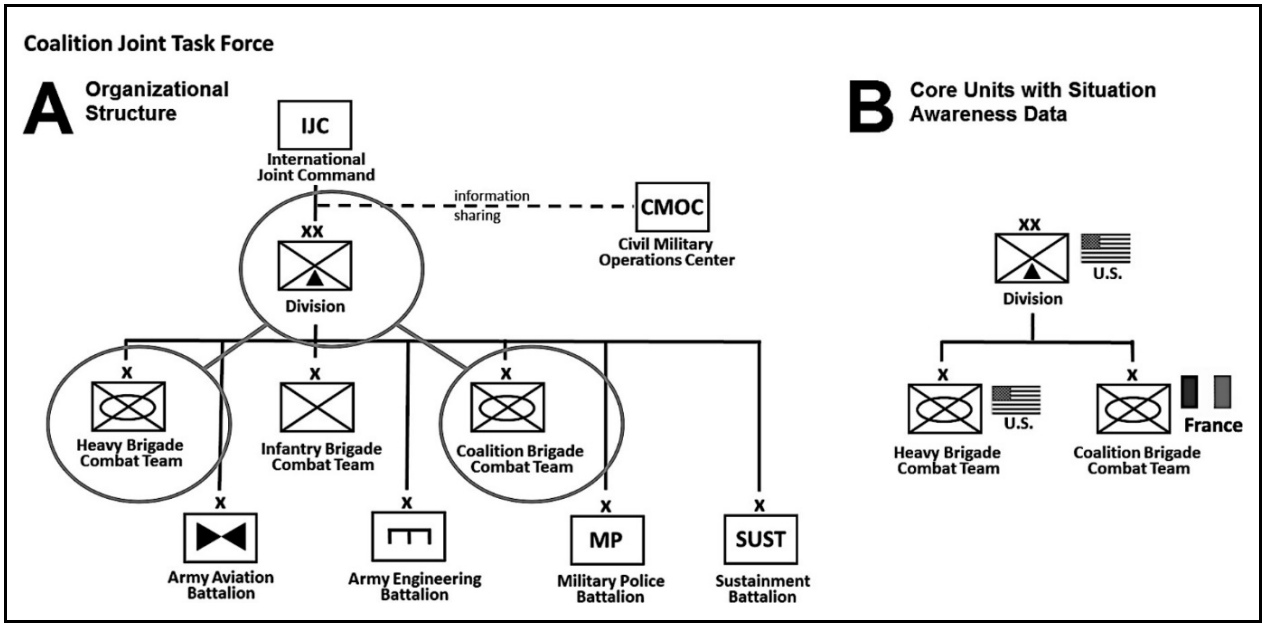


Figure 6-5 : (A) Structure organisationnelle de la Force opérationnelle interarmées de la coalition au cours de l'expérimentation. L'organisation en réseau s'étend sur plusieurs échelons, du commandement conjoint à la division en passant par la brigade et les bataillons de soutien. (B) Unités exercées : commandement de mission de la division, et deux brigades subordonnées.

On a appliqué une approche de la science des réseaux basée sur la théorie des graphes des communications recueillies pour l'ensemble de l'organisation de la force opérationnelle interarmées de la coalition.

L'hypothèse portait sur le fait que « le partage accru d'informations conduit à une meilleureconnaissance de la situation ». L'expérimentation se déroulait pendant un exercice de formation au commandement de mission (MCBL : Fort Leavenworth, KS) de deux semaines.

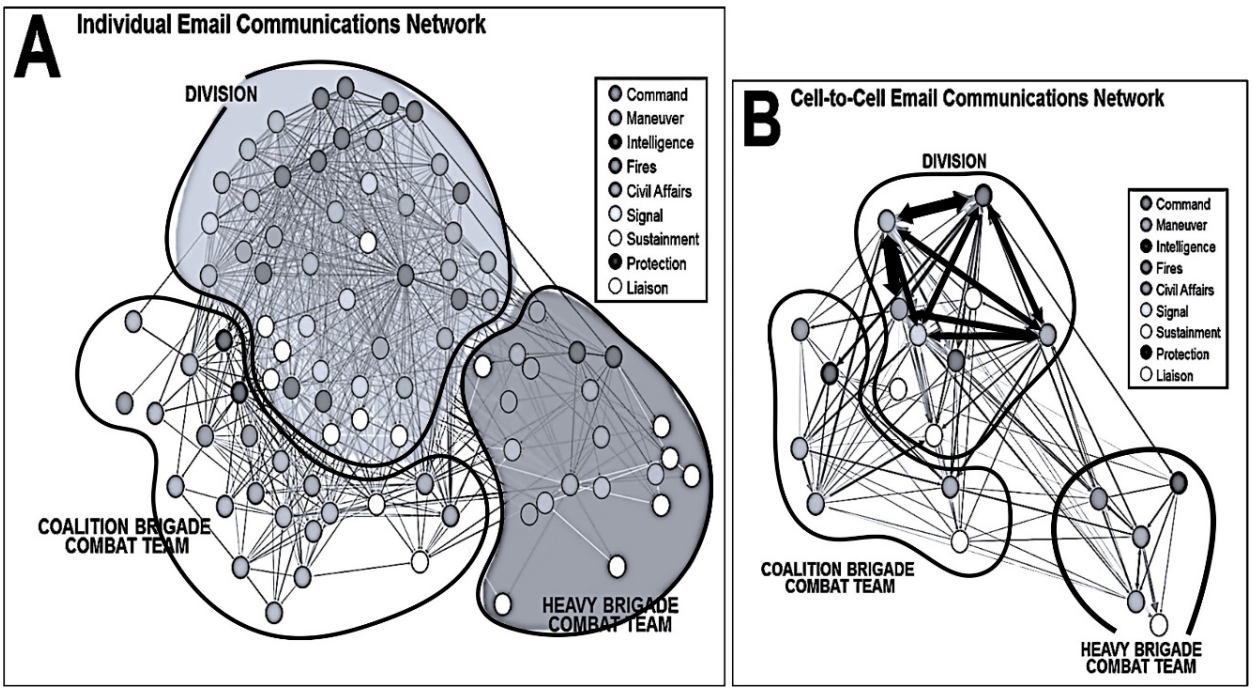


Figure 6-6 : Réseau des communications intra et inter unités (trois structures de la Figure 6-5). La teinte des cellules indique les rôles fonctionnels et l'épaisseur des lignes indiquent lacellule fonctionnelle de l'expéditeur et le volume du message.

Les trois unités de base exercées à une communication accrue et équipée étaient composées du personnel du commandement de mission d'une division américaine et de deux brigades subordonnées participantes, d'une équipe de combat de brigade lourde américaine et d'une équipe de combat de brigade de coalition française.

Les données de connaissance de la situation individuelle ont été collectées à l'aide de la méthodologie SAGAT auprès du personnel participant de ces trois unités de base, et le traitement des données utilisait l'Analyse de la « théorie des graphes » sur l'ensemble des communications par courriel et les données de conscience de la situation (recueillies par quiz).

Les communications par courrier électronique sont agrégées au niveau de la cellule pour révéler les correspondances fonctionnelles de cellule à cellule (A) et recombinées au niveau de nœud individuel en fonction de la quantité d'information échangée (B).

Nous avons observé des déséquilibres de type « Pareto » dans le partage des informations au sein des réseaux de communication du Commandement de la Mission. Sur les 250 personnes quecompte le réseau, nous constatons que des individus clés, situés à la queue de la distribution de Pareto, dominent les collaborations. La plupart des individus, qui constitue ce que nous appelons le *trivial many* n'ont que quelques interactions, alors que quelques individus, que nous appellerons les *vital few* ont de très nombreuses interactions et occupent une place dominante dans le réseau des interactions.

L'étude de la conscience de situation a été menée à partir d'un *pop-quiz* électronique basé sur le modèle de Endsley (2000) portant sur les événements importants de la mission et développées à partir d'une méthodologie d'analyse des tâches axée sur les objectifs. Il permet la mesure objective de la conscience de la situation de chaque individu, et ces résultats sont analysés en fonction de l'étude des communications précédente.

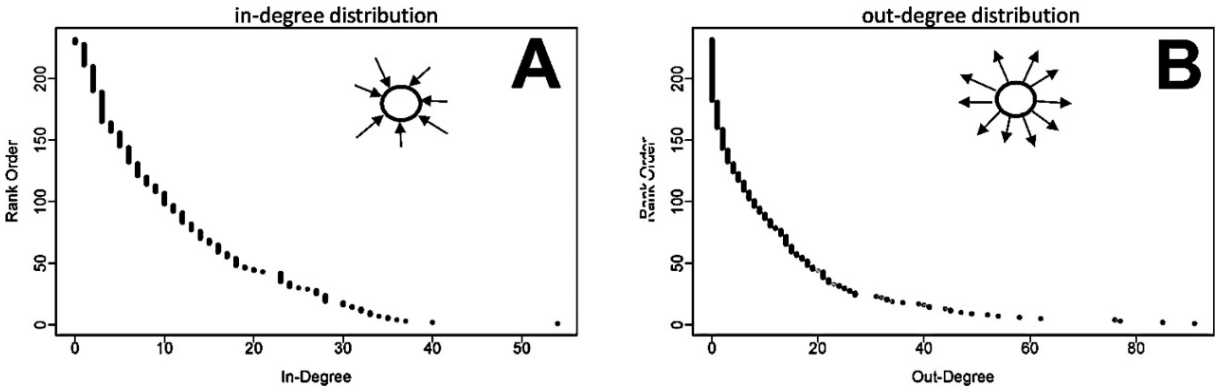


Figure 6-7 : Fonctions de distribution cumulative des communications des entrées par courrierélectronique (a) et des sorties (b) pour l'ensemble du réseau de communications. La prédominance de certains membres du personnel du commandement est évidente lorsqu'elleest exprimée en pourcentage de tous les liens.

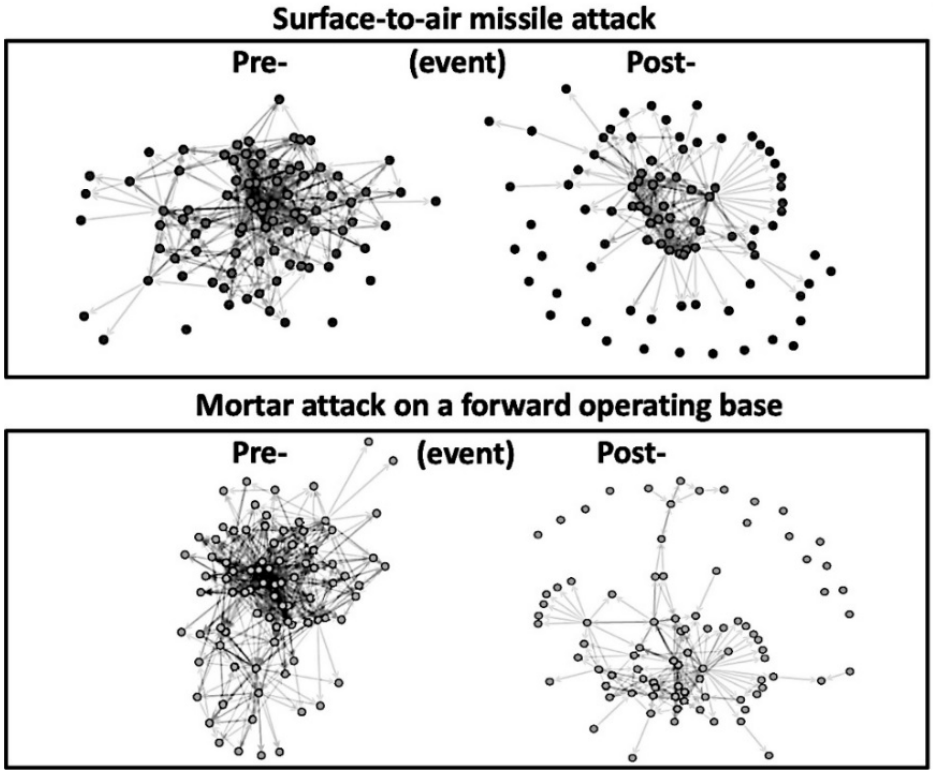


Figure 6-8 : Exemples de réorganisation des réseaux de communication du commandement des unités en fonction de chocs (pré- et post-évènement critique : missile ou attaque de mortier).

Les résultats sont détaillés dans Buchler et al. (2016) et mettent en évidence des défis auxquels sont confrontées les organisations militaires en réseau : le partage d'informations robuste mais inégal, des sources et des « puits d'information », une conscience de la situation clairement stratifiée, et le fait que le partage d'informations n'augmente pas toujours la conscience de situation.

Restent des questions qu'il nous faut éclaircir. Comment le réseau réagit-il aux chocs ou événements indésirables ? Quelles sortes d'adaptations organisationnelles se produisent (p. ex. auto-synchronisation) ? (Fitzhugh et al., 2020). Par exemple quelle est l'évolution de la conscience de situation en fonction de la réorganisation du réseau à la suite d'un choc ?

Une des caractéristiques d'observation concerne l'existence de « coordonnateurs émergents » et leur rôle dans la réorganisation du réseau. Ces rôles sont non formalisés, et chaque événement a produit le dégagement de 2 à 5 coordinateurs émergents (Buchler et al., 2018).

6.7 LES CYBERSIMULATIONS CCDC

La transformation militaire des pays des États-Unis et de l'OTAN dans une philosophie « réseau centrée » (NEO) a été effectuée selon un cadre conceptuel comprenant quatre principes principaux :

- Une force en réseau robuste améliore le partage de l'information et la collaboration ;
- Ce partage et cette collaboration améliorent la qualité de l'information et la connaissance partagée de la situation ;
- Cette amélioration, à son tour, permet une plus grande auto-synchronisation et améliore la durabilité et la rapidité de la commande ; et
- La combinaison augmente considérablement l'efficacité des missions.

Nous avons pu étudier les comportements des équipes d'acteurs lors de trois épisodes d'une compétition cyber, la U.S. Collegiate Cyber Defense Competition (CCDC 2016, 2017 et 2018 – www.nationalccdc.org). Notre objectif était de comprendre quelle combinaison de compétences ou d'outils, de dynamique d'équipe et de style de leadership rend une équipe plus ou moins efficace, par la mesure objective de l'efficacité de la mission.

La question stratégique était de savoir comment étudier ce qui fait qu'une équipe est meilleure que les autres. Le scénario opposait des équipes d'attaquants (les rouges) à des équipes de défenseurs (les bleus), et était conçu pour favoriser le cyber travail en équipe. L'environnement de simulation offrait un degré de réalisme suffisant, avec contrôle expérimental par des mesures des résultats des performances.

La tâche était globalement conforme aux prestations assurées par des professionnels de la sécurité de l'information. Elle consistait à maintenir efficaces les services qui doivent rester gérés efficacement, disponibles et opérationnels. Les équipes devaient terminer des tâches assignées dans un laps de temps donné, tels que créer des documents de politique, apporter des modifications techniques, assister à des réunions, répondre aux incidents, c'est-à-dire analyser les incidents de cybersécurité et soumettre des rapports, et contrecarrer les cyberattaques adverses.

Les mesures de la qualité et de la performance d'équipe étaient des données sociométriques, avec des capteurs portables qui mesurent les interactions entre les membres de l'équipe, une enquête remise aux observateurs de l'équipe (en 2016 et 2017) pour évaluer le degré de collaboration et le style de leadership de l'équipe, et des mesures de compétences à partir d'enquête remise à l'équipe des défenseurs afin d'évaluer l'expérience, le style de communication, les tâches/rôles et la structure de l'équipe.

Les analyses factorielles sur les données des questionnaires ont été menées en fonction des trois catégories de groupes : échec par prise d'assaut (classé faible), normal (classé moyen), performant (classé haut).

On constate que la dynamique de groupe évolue avec le temps dans une perspective cohérente avec une forme de « maturation de l'équipe » selon la théorie de Tuckman (1965) : modèle « Forming, Storming, Norming, and Performing ». Ce modèle décrit les étapes que traverse une équipe, à partir du moment où un groupe se réunit pour la première fois jusqu'à la fin d'un projet. De plus les membres de l'équipe évoluent eux-mêmes en parallèle en accédant progressivement au statut de collègue. La performance de l'équipe dépend de la réussite de cette maturation.

Les résultats sont résumés (Buchler et al., 2018), pour deux compétitions, dans la Figure 6-7 et confirment la nécessité d'une structuration d'équipe avec une probable maturation de la conscience de situation partagée en fonction de l'avancée de l'expérience avec un modèle d'étape séquentiel (modèle de Tuckman). Ils indiquent que la dimension du leadership et les interactions en face-à-facesont des facteurs importants qui déterminent le degré de succès d'une équipe. On observe notamment que les facteurs de bonne performance varient selon le type de tâche demandée à l'équipe, traduisant l'agilité et la capacité d'adaptation acquise par une équipe mature. Ainsi, il semble que la spécialisation fonctionnelle au sein d'une équipe et un leadership bien guidé sont des prédicteurs significatifs de la détection et de la rapidité de réponse efficace aux chocs, ici les cyberattaques.

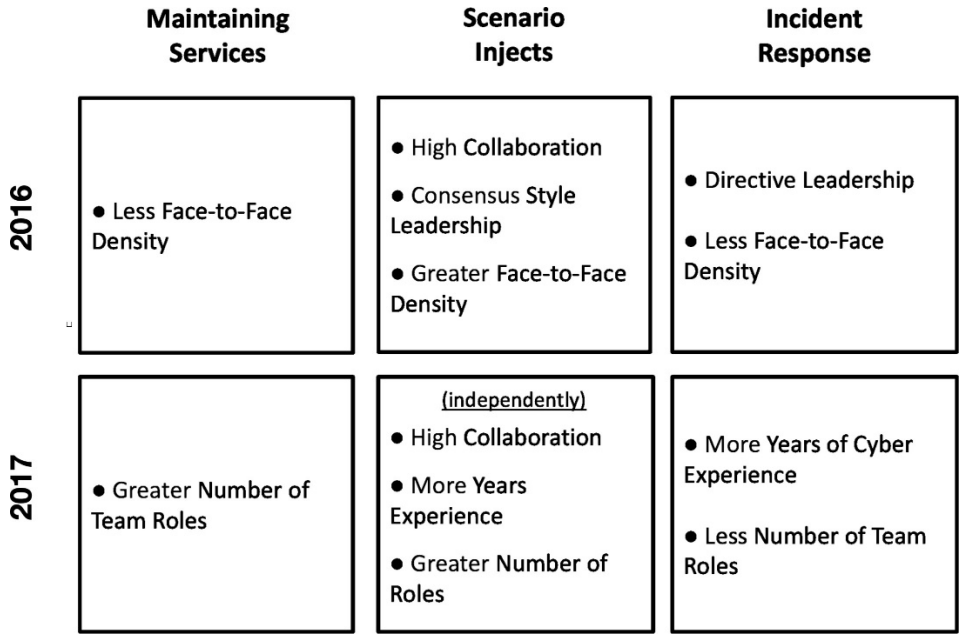


Figure 6-9 : Résultats de l'expérience CCDC.

Au vu de la quantité et de la profondeur des compétences nécessaires pour être performant dans le domaine cyber, ces mesures prédictives nous donnent quelques perspectives pour supporter le développement de bonnes équipes cyber.

6.8 CONCLUSION

Ces deux études convergent vers notre conviction que la résistance aux attaques, et notamment pourla guerre cognitive, nécessite la formation des équipes et l'établissement de routines normatives de travail pour la performance en accompagnant les équipes vers un haut niveau de maturité.

La collaboration humaine et la structure du leadership des équipes sont essentielles à la gestion de systèmes techniques complexes et à la coordination de réponses efficaces aux menaces.

Ces recherches ont également montré l'utilité des mesures obtenues par les technologies portables, collectées pendant la période de travail : capture automatique des interactions humaines en face-à-face par détecteur infrarouge, temps des conversations et caractéristiques vocales des échanges, proximité physique des collaborateurs et niveaux d'activité physique spontanée captée par accéléromètres. Les rapides avancées technologiques dans le domaine des technologies portables et de l'enregistrement physiologique sont une aubaine pour les études, mais également pour la gestion des équipes œuvrant dans des environnements dont les caractéristiques peuvent également être détectées en ligne, comme les communications. L'analyse performante des « données volumineuses » est également un facteur favorable.

Parallèlement, on peut rapprocher ces études de la théorie sur la prise de décision avec la boucle OODA pour favoriser la résistance et la performance cognitive (cf. Figure 6-1), avec la proposition, en complément des échelles TRL et HRL, d'une échelle de « Cognitive Technological Maturity » construite à partir des données d'une part de l' « Intégration humain-système » (IHS) et de lacapacité de structuration des équipes dans lesquelles sont impliqués les opérateurs utilisant les systèmes.

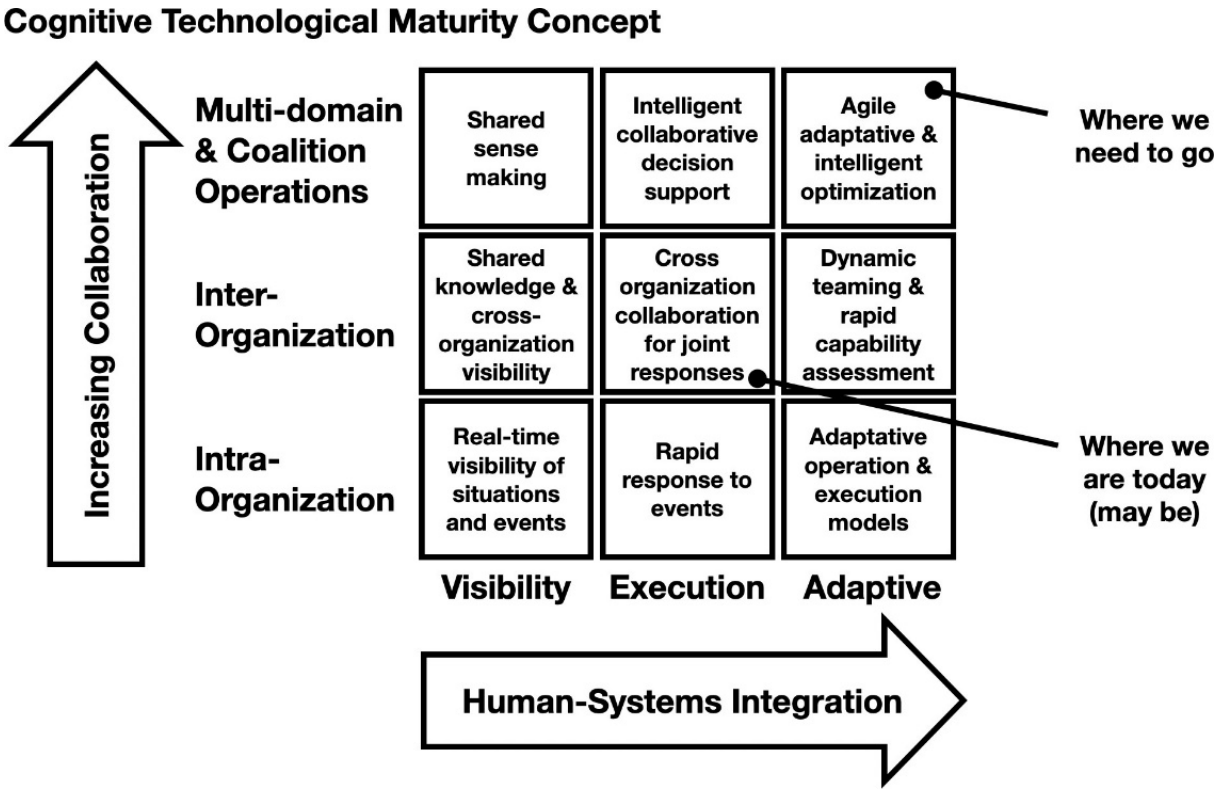


Figure 6-10 : Concept de Maturité Cognitive Technologique (adapté de Lin et al, 2004).

La Figure 6-8 représente, dans cette échelle, l'état de la situation des équipes des forces actuelles et le point d'adaptation agile et d'organisation intelligente vers lequel doivent tendre les forces des USA et de ses alliés de l'OTAN. Cet objectif doit se traduire, d'une part par un effort coordonné de collaboration accrue au sein des équipes mais également entre les équipes, les domaines et les nations, et d'autre part, par le développement de métriques humaines pertinentes pour garantir une intégration humain-système efficace.

6.9 BIBLIOGRAPHIE

Alberts, S.D., Garstka J. (2004). Network Centric Operations Conceptual Framework Version 2.0. Technical Report, US Office of Force Transformation and Office of the Assistant Secretary of Defense for Networks and Information Integration, US Department of Defense : Washington DC, USA. https://www.hsdl.org/?view&did=446190.

Alberts, S.D., Garstka J., Stein, F.P. (2004). Network Centric Warfare: Developing and Leveraging Information Superiority. Department of Defense CCRP Publication Series, Washington DC, USA. http://www.dodccrp.org/files/Alberts_NCW.pdf.

Boyd, J.R. (1976). Destruction and Creation. Command and General Staff College : Fort Leavenworth KS, USA. http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf.

Buchler, N., Fitzhugh, S.M., Marusich, L.R., Ungvarsky, D.M., Lebiere, C., Gonzalez, C. (2016). Mission Command in the Age of Network-Enabled Operations: Social Network Analysis of Information Sharing and Situation Awareness. Frontiers in Psychology, 7, 937, 1-15. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4916213/pdf/fpsyg-07-00937.pdf.

Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., Gonzalez, C. (2018). Sociometrics and Observational Assessment of Teaming and Leadership in a Cyber Security Defense Competition. Computers & Security, 73, 114-136. https://www.researchgate.net/publication/321057288_Sociometrics_and_observational_assessment_of_teaming_and_leadership_in_a_cyber_security_defense_competition.

Cole, A., Le Guyader, H. (2020). Cognitive: 6th Domain of Operation. NATO-ACT Innovation Hub : Norfolk VA, USA. https://www.innovationhub-act.org/sites/default/files/2021-01/NATO%27s%206th%20domain%20of%20operations.pdf.

Endsley, M. R. (2000). Theoretical Underpinnings of Situation Awareness: A Critical Review. In M.R. Endsley, D.J. Garland (Eds.) Situation Awareness Analysis and Measurement. Lawrence Erlbaum Associates : Mahwah NJ, USA , 3-32. https://www.researchgate.net/publication/230745477_Theoretical_underpinnings_of_situation_awareness_A_critical_review.

Fitzhugh, S.M., Decostanza, A.H., Buchler, N., Ungvarsky, D.M. (2020). Cognition and Communication: Situational Awareness and Tie Preservation in Disrupted Task Environments. Network Science, 8, 4, 508-542. https://www.cambridge.org/core/journals/network-science/article/abs/cognition-and-communication-situational-awareness-and-tie-preservation-in-disrupted-task-environments/47D44CB0AF1F48B39F029E53F25C6655.

Garneau, C.J., Hoffman, B.E., Buchler, N.E. (2020). Behavioral Observations Logging Toolkit (BOLT): Initial Deployed Prototypes and Usability Evaluations. CCDC Data & Analysis Center – DEVCOM Reports. Aberdeen Proving Ground MD, USA. https://apps.dtic.mil/sti/pdfs/AD1099977.pdf.

Handley, H.A.H., Savage-Knepshield, P. (2021). Evaluating the Utility of Human Readiness Levels (HRLs) with Human System Integration Assessments (HSIAs). Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 64, 1, 1537-1540. https://journals.sagepub.com/doi/abs/10.1177/1071181320641368?cookieSet=1.

International Organization for Standardization (2013). Space Systems: Definition of the Technology Readiness Levels (TRLs) and their Criteria of Assessment. ISO 16290:2013. American Society for Testing and Materials – ASTM International Editions : West Conshohocken PN, USA. http://www.iso.org/iso/catalogue_detail.htm?csnumber=56064.

Kott, A. (2007). Information Warfare and Organizational Decision-Making. Artech House Publishers. Norwood MA, USA. https://us.artechhouse.com/Information-Warfare-and-Organizational-Decision-Making-P1031.aspx.

Kott, A. (2008). Battle of Cognition: The Future Information-Rich Warfare and the Mind of the Commander. Greenwood Publishing Group: Westport CT, USA. https://products.abc-clio.com/abc-cliocorporate/product.aspx?pc=C2605C.

Kott, A., Alberts, D.S. (2017). How Do You Command an Army of Intelligent Things? IEEE Computer, 50, 96-100. https://arxiv.org/pdf/1712.08976;How.

Kott, A., Linkov, I. (2021). To Improve Cyber Resilience, Measure It. IEEE Computer, 54, 2, 80-85. https://arxiv.org/pdf/2102.09455.pdf.

La Fleur, C., Hoffman, B., Gibson, C. B., Buchler, N. (2021). Team Performance in a Series of Regional and National US Cybersecurity Defense Competitions: Generalizable Effects of Training and Functional Role Specialization. Computers & Security, 104.

Lin, G., Wang, K.-Y., Luby, R. (2004). A New Model for Military Operations. OR/MS Today, 6 décembre 2004. https://doi.org/10.1287/orms.2004.06.15.

Savage-Knepshield, P., Martin, J., Lockett III, J., Allender, L. (2015). Designing Soldier Systems: Current Issues in Human Factors (Human Factors in Defence). Ashgate : Burlington VT, USA. https://1lib.fr/book/2836338/3d230e.

Savage-Knepshield, P.A., Hernandez, C.L., Sines, S.O. (2021). Exploring the Synergy Between Human Systems Integration and Human Readiness Levels: A Retrospective Analysis. Ergonomics in Design: The Quarterly of Human Factors Applications, 22 avril 2021 (sous presse). https://journals.sagepub.com/doi/full/10.1177/10648046211009718.

Théron, P., Kott, A., Drašar, M., Rzadca, K., Le Blanc, B., Pihelgas, M., Mancini, L., De Gaspari, F. (2019). Reference Architecture of an Autonomous Agent for Cyber Defense of Complex Military Systems. In Jajodia, S., Cybenko, G., Subrahmanian, V., Swarup, V., Wang, C., Wellman M. (Eds) Adaptive Autonomous Secure Cyber Systems. Springer, Cham. New-York, NY, USA. https://link.springer.com/chapter/10.1007/978-3-030-33432-1_1.

Tuckman, B.W. (1965). Developmental Sequence in Small Groups. Psychological Bulletin, 63, 384-399. http://dennislearningcenter.osu.edu/references/GROUP%20DEV%20ARTICLE.doc.

U.S. Army Headquarters (2016). U.S. Army Field Manual FM 3-13, Information Operations. Army Publishing Directorate : Washington DC, USA. https://www.globalsecurity.org/military/library/policy/army/fm/3-13/fm3-13_2016.pdf.

Chapitre 7 – LES NARRATIONS SUBMERGENT LE MONDE

Docteur Michael Wunder[1]

« Nous sommes en fait en guerre – la guerre de l'information – une sorte de guerre perfide. »

7.1 SITUATION

Les récits narratifs (*narratives*) peuvent être utilisés pour étayer des déclarations plus courtes. Il s'agit d'instruments caractéristiques des spots publicitaires ou des campagnes politiques. La théorie qui sous-tend l'utilisation de la narration et celle des messages publicitaires, est assez ancienne. Elle était déjà utilisée pour le commerce des marchandises et d'autres biens économiques il y a plusieurs décennies – nous nous souvenons de l'homme *Marlboro* et de son image bien construite d'homme libre et de fumeur *cool*. Dans la genèse typique d'un récit, des faits universels sont mélangés à des significations tendancielles, suivis d'une diffusion continue via divers canaux médiatiques et de nombreuses répétitions. Une fois qu'un récit est diffusé, il peut être référencé par quelques mots-clés, une mélodie ou une image. Il est très utile de se référer à un récit existant lorsque le temps est trop limité pour entrer dans des explications détaillées, comme dans les interviews télévisées, les articles courts, les publicités, les gros titres, etc.

Une notion importante réside dans le fait que les gens ont tendance à accorder leur attention aux narrations qui correspondent à leur compréhension de base, à leurs croyances fermes, à ce qu'ils souhaitent ou simplement à ce qui leur semble familier. Les convictions existantes peuvent être renforcées mais pas inversées.

Il est cependant possible d'attirer certains esprits influençables et de les persuader. C'est l'une des conditions de réussite de la formation de communautés sociales solitaires et de chambres d'écho. Les gens sélectionnent et se concentrent sur les informations qui sont conformes à leurs narrations préférées et ignorent les autres. Dans cette situation, la validité de l'information n'est plus pertinente. Il est difficile ou presque impossible d'ouvrir à d'autres arguments les esprits déjà piégés.

Avant l'ère d'Internet, il était coûteux de concevoir, lancer et maintenir une campagne d'information efficace. Aujourd'hui, diffuser largement des informations via les médias sociaux est bon marché et ne nécessite qu'un équipement technique relativement faible et quelques compétences. La portée étendue des médias sociaux et la vitesse de partage des récits narratifs sont étonnantes.

Les principaux moteurs sont les innovations techniques que les entreprises de l'internet appliquent et améliorent afin d'établir et de promouvoir leurs modèles d'entreprise – ce sont les « algorithmes ». Aujourd'hui, les narrations et leur dispersion par les algorithmes sont étroitement liées. C'est ainsi que l'on peut décrire le modèle commercial des sociétés Internet qui fournissent des boîtes à outils sophistiquées aux clients désireux de vendre quelque chose. Les produits proposés ne sont pas du tout limités aux biens physiques. Il peut s'agir d'une vision, d'une éthique d'entreprise, d'une idéologie, d'un mythe, d'une diffamation, d'une théorie construite, etc.

Les algorithmes peuvent être conçus pour s'adapter au mieux aux domaines d'activité de chacun, ils peuvent être affinés pour répondre aux besoins et aux souhaits des consommateurs. Grâce à la collecte des *Big Data* et à l'exploitation de toutes les empreintes laissées par les consommateurs sur Internet, le profil d'un client est très complet et permet de prédire son comportement ainsi que ses centres d'intérêt, ce qui permet aux publicités de ne plus être gênantes, mais plutôt souhaitées ou du moins inaperçues, et donc très efficaces.

[1] Michael Wunder est directeur du Département C2 and Intelligence de l'Institut Fraunhofer pour la Communication, le Traitement de l'Information et l'Ergonomie – FKIE – à Wachtberg (Allemagne). Michael Wunder a assuré la présidence scientifique du Panel IST de la STO - OTAN jusqu'en mai 2021.

Pour cela, les sociétés Internet s'appliquent à mettre en œuvre tous les outils *high-techs* modernes, comme des analyses et des projections des contenus des médias sociaux basées sur l'intelligence artificielle.

7.2 MENACES

Les sociétés Internet maintiennent un modèle commercial très fort, robuste et extrêmement rentable et n'ont donc aucun intérêt à changer la situation. Il est très probablement illusoire de penser qu'elles peuvent être motivées pour filtrer et exclure les clients douteux. Le bannissement de certains utilisateurs importants est une mesure orientée vers le public, mais il ne peut pas empêcher une utilisation générale abusive de leurs services.

Et c'est une situation bienvenue pour une grande variété de contemporains malveillants qui peuvent facilement profiter de ces outils et garder leur identité cachée. Il est étonnant de constater à quel point les algorithmes sont parfaitement alimentés par de nombreux seigneurs de la guerre, terroristes, antisémites, extrémistes, etc. afin de promouvoir leurs narrations et leurs campagnes – quasiment pour améliorer leur référencement dans les moteurs de recherche.

Dans notre monde frénétique, le temps de réflexion consacré à un sujet diminue et de nombreuses informations se disputent l'attention. D'une part, les médias réputés sont mis au défi de fournir des faits vérifiés à grands frais et, d'autre part, les faits sont moins pertinents puisque le message le plus excitant et palpitant promet le plus grand nombre de clics. Les consommateurs des médias sociaux (qui ont tendance à n'accorder que 7 secondes d'attention) ne vérifient pas la validité et la véracité des informations ou, pire encore, ils aspirent à trouver et à accepter en particulier les informations qui sont compatibles avec leurs convictions existantes.

Les sociétés sont sensibles aux informations biaisées et fausses. L'examen de l'impact des campagnes d'information est compliqué. Il se peut également qu'une reconnaissance publique ne soit pas souhaitée par certaines parties de la société si une narration leur est bénéfique et va dans leur sens. Certains politiciens sont favorables à l'utilisation de narrations douteuses lorsque cela permet de discréditer leurs rivaux.

Souvent, les récits ne comportent pas le nom de leur véritable initiateur et il est difficile de découvrir leurs impératifs et celui qui en est à l'origine. Étant donné que les récits peuvent être combinés avec divers éléments d'information et diverses sources dans le cadre d'une campagne systématique et globale, il semble facilement possible de lancer des émeutes, des manifestations pour influencer la position de la société dans son ensemble, de manipuler la position d'une communauté et enfin de provoquer de graves distorsions dans une nation. Cet instrument est attrayant non seulement pour les États agressifs qui ne disposent que d'une capacité technique et militaire limitée, mais aussi pour ceux qui profitent des inconvénients économiques résultant de la manipulation de l'opinion publique et de la déstabilisation du système social. Un exemple decampagne de guerre de l'information réellement efficace en tant que « sous-produit » d'un conflit militaire s'est produit lors de la dernière guerre de Crimée. Un autre exemple a été la discréditation de l'efficacité des vaccins anti-coronavirus.

7.3 CONTRE-MESURES

Les tentatives visant à réfuter une fausse déclaration et à fournir des contre-déclarations sont moins efficaces que la fausse déclaration elle-même. De plus, le message d'une fake news peut être fortifié et se manifester par la référence à celle-ci, quel que soit le contexte. On se souvient des rumeurs selon lesquelles Barack Obama n'était pas né aux États-Unis et de leur impact stupéfiant sur une partie de la population américaine – même la divulgation de son certificat de naissance ne les a pas suffisamment convaincus. Les tentatives pour convaincre les gens du contraire sont inefficaces ou généralement vaines – les partisans de Donald Trump en sont un autre exemple frappant. Beaucoup de gens savent qu'il est un menteur, ses partisans le savent aussi, mais ils s'en moquent tant qu'il soutient simultanément et bruyamment leurs croyances actuelles. Il n'existe pas de moyen simple de combattre le mensonge.

Certes, l'éducation à l'école peut être un moyen. Mais sa portée est limitée, elle prend du temps et nécessite des enseignants compétents. Il existe des chaînes internet (p. ex. www.twitch.tv) qui s'adressent à la jeune population, informent de manière ludique sur les menaces des médias sociaux et montrent comment regarder derrière la façade. Les vérificateurs de faits constituent un autre moyen important dont la portée se développe également. Leur influence s'accroît actuellement dans le secteur des médias. Les journalistes sérieux utilisent divers sites web où les fausses informations sont identifiées en référençant la provenance et la source (www.politifact.com ; www.factcheck.org ; www.newsguard.com). Au sein des réseaux de vérificateurs de faits (comme www.poynter.org), plusieurs de ces spécialistes s'engagent à respecter un code de conduite afin de se distinguer des opérateurs de médias sociaux douteux. Les vérificateurs de faits peuvent vérifier si une histoire ou une image a déjà été utilisée dans un autre contexte et aider ainsi les journalistes ou les lecteurs à prouver l'exactitude d'une information – vraie ou fausse.

L'*Organisation pour la science et la technologie* (STO) de l'OTAN avait diagnostiqué que la manipulation de l'information par le biais des médias sociaux relevait incontestablement de la défense militaire. Les agresseurs extérieurs peuvent se concentrer sur la déstabilisation d'une sociétésociale et sur sa prospérité économique. La guerre de l'information et les cyber-opérations combinées dans un scénario hybride ont le potentiel de déclencher des conflits évolutifs, allant de dommages ponctuels à une destruction complète. Ce qui les rend extrêmement dangereuses, c'est le fait qu'elles peuvent être préparées de manière totalement dissimulée, qu'elles peuvent être appliquées sans aucun avertissement, qu'elles peuvent être lancées de n'importe où dans le monde et qu'il n'y a pas d'équilibre des forces puisque les pays de l'OTAN ne considèrent actuellement pas la manipulation de l'information comme un élément communément accepté dans leur arsenal.

Il y a quelques années, la STO de l'OTAN a lancé deux *Groupes recherche et technologie* qui travaillent sur les contre-mesures dans le contexte de l'utilisation abusive des médias sociaux. Ils se concentrent sur les techniques et les outils d'analyse de fond pour aider les analystes du renseignement à obtenir des indications sur la source, l'origine, la plausibilité, les faits techniques concernant les procédures de diffusion, les tendances du contenu, etc. Par exemple, une simple observation des temps de diffusion peut révéler qu'un robot est à l'origine des messages, s'il n'y a pas de délais d'attente réguliers. Une personne réelle aurait besoin de ces temps d'arrêt périodiques pour dormir. Un autre exemple pour trouver des indications de supercherie peut être l'utilisation des particularités linguistiques des messages propres à un groupe particulier (phrases spéciales ou syntaxe irrégulière). De même, le trafic numérique entre les nœuds Twitter et leurs liens existants peut fournir des indications sur les nœuds (concentration, transfert, réplique, traduction, etc.). La combinaison de techniques et d'outils adéquats permet de sensibiliser efficacement les analystes des médias sociaux et de fournir des preuves suffisantes pour mettre en place des contre-mesures.

Un groupe de recherche et de technologie sur « l'exploitation des médias sociaux à des fins de renseignement » a présenté un rapport (STO-TR-SAS-IST-102, 2018). Un autre groupe de la STO de l'OTAN-STO (IST-177) sur « l'exploitation des médias sociaux pour les opérations dans l'environnement informationnel » achèvera une recherche de trois ans à l'été 2022.

7.4 SYNTHESE

Les récits narratifs submergent et menacent le monde.

La manipulation de l'information est efficace, elle doit être considérée comme une arme puissante, elle peut déclencher des conflits graves et illimités. Des événements limités (« sondes ») se produisent déjà. L'OTAN et les pays alliés ont besoin de concepts exhaustifs pour concevoir des contre-mesures.

7.5 BIBLIOGRAPHIE

Forrester, B. and the High Level Group exp. (2018). Intelligence Exploitation of Social Media – Final Report of Task Group SAS-IST-102. NATO Science and Technology Organization – Collaborative Support Office: Neuilly (France). https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-SAS-IST-102/$$TR-SAS-IST-102-ALL.pdf.

Chapitre 8 – LA GUERRE COGNITIVE – POURQUOI L'OCCIDENT POURRAIT PERDRE FACE A LA CHINE ?

Kimberly Orinx[1], Tanguy Struye de Swielande[2]

« Les Chinois dépasseront l'Occident en matière de guerre cognitive. »

Depuis quelques années, nous assistons au retour des rivalités entre les grandes puissances. Afin de faire obstacle aux États-Unis en particulier et à l'Occident en général, la Chine applique une guerre hybride. Bien qu'aucune confrontation militaire directe avec l'Ouest n'ait eu lieu au XXI[e] siècle, la Chine et d'autres nations contestataires, ont développé et utilisent des moyens hybrides pour l'affaiblir, tels que la guérilla, le terrorisme, la pression économique, la guerre cognitive, les cyber attaques, la paramilitarisation ou encore la *lawfare* (réinterprétation des normes et standards).

Agir ainsi permet à ces nations de rester sous le seuil de la « véritable guerre » et de produire les effets escomptés de leur stratégie tout en prévenant le déclenchement du *jus ad bellum* (le droit de la guerre). Cette stratégie brouille le seuil entre paix et guerre qui structure notre compréhension fondamentale des relations interétatiques. L'Occident doit donc s'attendre à ce que les adversaires potentiels recourent de plus en plus à cette forme de guerre, accessible et peu coûteuse, soit en soutien d'opérations militaires plus conventionnelles, soit de manière autonome pour défendre leurs intérêts.

La guerre cognitive, peu étudiée, est l'une des composantes de la guerre hybride. Celle-ci est définie par Bernal et al., comme « l'armement » de l'opinion publique, par une entité externe, dans le but :

1) D'influencer la politique publique et gouvernementale ; et
2) De déstabiliser les institutions publiques.

La déstabilisation et l'influence sont les objectifs fondamentaux de la guerre cognitive (Bernal et al., 2020). La guerre cognitive est, en outre, continue : les Israéliens parlent même de campagnes cognitives entre les guerres (Kuperwasser et Siman-Tov, 2019).

8.1 LA CULTURE STRATEGIQUE CHINOISE

La culture stratégique est définie comme « un ensemble distinctif et durable de croyances, devaleurs et d'habitudes concernant la menace et l'usage de la force qui sont ancrées dans lesinfluences fondamentales de l'environnement géopolitique sur l'histoire et la culture politique » (Booth et Trood, 1999). La culture stratégique chinoise, influencée entre autres par le Confucianisme, le Taoïsme, l'interprétation du temps, Sun Tzu et les 36 Stratagèmes, est flexible, subversive, se concentre sur le potentiel de la situation (Julien, 2015) et est mieux adaptée à la guerre cognitive que la culture stratégique occidentale. De nos jours, cela s'illustre, entre autres, parle concept de « *sānzhàn* 三戰 » (« Trois Guerres »), à savoir la guerre psychologique, la guerre del'opinion publique et la guerre juridique. L'objectif de ce concept est « d'essayer d'influencer la perception publique du conflit en conservant le soutien de sa propre population, en le dégradant dans la population de l'adversaire et en influençant les tiers ». Afin de dominer la mise en œuvre à long terme de la guerre psychologique et juridique, la guerre de l'opinion publique est appliquée

[1] Kimberly Orinx est assistante de recherche à l'Université Catholique de Louvain-La-Neuve (Belgique), chercheure au CECRI et doctorante en relations internationales, spécialiste de l'Information Warfare et du Cognitive Warfare.

[2] Tanguy Struye de Swielande est professeur à l'Université Catholique de Louvain-La-Neuve (Belgique). Il est spécialisé dans la géopolitique et politique étrangère des grandes puissances (Etats-Unis, Russie et Chine), la puissance, la grande stratégie, l'analyse de la prise de décision et la guerre cognitive. Il dirige la collection Scène internationale aux Presses universitaires de Louvain et est fondateur du réseau GENESYS.

parle biais de divers canaux tels que les médias et réseaux sociaux, permettant de cibler les adversaires et les ennemis (potentiels) (Cheng, 2012). La guerre psychologique, quant à elle, vise à influencer lecomportement ou la façon de penser de l'adversaire (saper la volonté de l'adversaire, éroder le soutien populaire) et à consolider la psychologie amie, c'est-à-dire à renforcer le soutien des partenaires et des alliés et à garantir la neutralité des indécis ou des neutres. La guerre juridique, enfin, à son niveau le plus élémentaire, consiste à s'assurer que son propre camp respecte la loi, à présenter des arguments en sa faveur dans les cas où il y a néanmoins des violations de la loi, et à critiquer son adversaire pour le non-respect de la loi (Yanrong, 2006).

Ces trois guerres se renforcent mutuellement : la propagation du discours comprend le récit stratégique visant à convaincre les populations nationales et étrangères par les vecteurs de transmission (« guerre d'opinion ») en créant un environnement mental favorable (guerre psychologique) qui rend le message conforme aux idées reçues, tout en se protégeant derrière la logique de la souveraineté cybernétique, que la Chine tente d'imposer juridiquement au niveau international (« guerre juridique »).

En outre, la guerre cognitive menée par la Chine ne fait pas de différence entre la guerre et la paix, entre les combattants et les non-combattants (tout le monde est une cible potentielle), et est donc permanente. C'est une différence majeure avec l'Occident, où il existe une différenciation entre la guerre et la paix. À la fin du XXe siècle, la publication de la monographie Unrestricted Warfare par deux colonels de l'armée chinoise, Qiao et Wang (2006), a marqué une étape importante dans la compréhension de la pensée stratégique contemporaine à Pékin. Selon ces auteurs, les développements technologiques, la mondialisation et la montée en puissance au-delà de l'État-nation, combinés aux nouvelles capacités des armes modernes, offriraient un nouveau contexte aux conflits. Les champs de bataille passeraient ainsi d'une dimension physique à une arène plus abstraite, comme le cyberespace, le moral de la population ou son cerveau. En d'autres termes, Qiao et Wang démontrent que la guerre n'est plus « l'utilisation de la force armée pour forcer l'ennemi à se plier à nos désirs » mais plutôt « tous les moyens, qu'ils soient armés ou non armés, militaires ou non militaires [...] [sont utilisés] pour forcer l'ennemi à se soumettre à ses propres intérêts ». Par conséquent, le champ de bataille est partout. La guerre n'est plus un concept purement militaire mais devient également civile. Cela a deux conséquences : premièrement, les victimes de ces nouvelles guerres ne seront pas seulement les combattants réguliers qui meurent sur le champ de bataille, mais aussi les civils qui sont indirectement touchés. Deuxièmement, la guerre est permanente et holistique, toutes les forces et tous les moyens sont réunis.

Enfin, les auteurs affirment que la seule règle est qu'il n'y a pas de règles. Ainsi, les menaces militaires ne sont plus nécessairement le principal facteur affectant la sécurité nationale d'un pays. L'intention n'est pas nécessairement de vaincre l'Occident sur le champ de bataille, mais d'affaiblir les démocraties à un point tel, « qu'elles sont incapables, ou non désireuses, de répondre à une agression » (Zeman, 2021).

La guerre cognitive menée par Pékin (et d'autres) attaque qui nous sommes, notre histoire, notre passé, notre identité. James Rogers résume cette logique à la perfection :

> *Pour être efficace, une opération de positionnement hostile devrait comporter un processus en trois étapes : Désactiver l'identité existante du pays cible par des tactiques telles que : la désynchronisation de son récit historique ; La remise en question ou la démolition de la perception qu'il a de sa pertinence internationale ; et la délégitimation de son statut et de son rôle international ; Construire – si possible en travaillant en tandem avec des forces politiques nationales mécontentes ou séparatistes – une nouvelle identité pour la cible, en la reliant à des mythes historiques nouveaux ou préexistants (mais souvent marginalisés) ; Encourager l'adoption et la diffusion de la nouvelle position, à la fois : au niveau national (à l'intérieur du pays cible), en particulier parmi les éléments mécontents et séparatistes ; et au niveau international, parmi les élitesd'autres pays* (Roger, 2021).

L'objectif est de monter les gens les uns contre les autres de l'intérieur. Le centre de gravité est désormais la population et les processus politiques dans les sociétés ouvertes.

De plus, comme l'explique Vadim Shtepa (2021) : « si les effectifs et les infrastructures peuvent être restaurés, l'évolution de la conscience ne peut être inversée, d'autant plus que les conséquences de cette guerre « mentale » n'apparaissent pas immédiatement mais seulement après au moins une génération, lorsqu'il sera impossible de réparer quelque chose ». Et le facteur temps, est du côté de la Chine : La Chine a le temps. Son approche du temps est très différente de celle de l'Occident. « Pour un Occidental, dit José Frèches, le temps est linéaire : le temps perdu n'est jamais récupéré et nous percevons notre vie comme un compte à rebours qui se terminera définitivement le jour de notre mort […] ; pour un Chinois, le temps est cyclique : le temps repasse […] en d'autres termes, le temps ne se perd pas » (Allègre et Jeambar, 2006). Parallèlement, « ceux qui n'hésitent pas à mentir auront toujours l'avantage du temps » (Ya'alon, 2019).

Les adversaires occidentaux ont, comme le dit Victor Davis Hanson, « maîtrisé la connaissance de l'esprit occidental » (Hanson, 2004). Nos adversaires potentiels connaissent nos vulnérabilités bien mieux que nous ne les connaissons nous-mêmes. Ils savent que la lutte ne peut être gagnée sur le champ de bataille, mais qu'elle peut l'être sur le terrain des images, de la rhétorique et de l'évolution des opinions publiques, comme David a terrassé Goliath. Pour faire simple, la perception est le nouveau champ de bataille et l'esprit est l'arme.

8.2 LES FAIBLESSES DE L'OUEST

Bien que la culture stratégique chinoise soit plus adaptée à la guerre cognitive, l'Occident a facilité la politique chinoise de deux façons : la fragilité des démocraties et la culture stratégique occidentale dépassée.

La polarisation au sein des démocraties est une bénédiction pour Pékin. Les gens sont plus susceptibles de regarder les informations qui confirment leur idéologie, plutôt que des informations contradictoires. Les développements technologiques ont amplifié l'importance des informations et des données dans notre environnement sécurisé. L'information est une ressource qui est et sera de plus en plus utilisée pour déstabiliser les pays, en particulier les démocraties. Bien qu'elles ne soient pas nouvelles, les campagnes de désinformation à travers les *fake news* ou les théories du complot sont utilisées pour fragmenter les États occidentaux et polariser l'opinion publique, affaiblissant ainsi les valeurs et systèmes démocratiques, augmentant la méfiance et le mécontentement à l'égard des systèmes politiques et favorisant les mouvements populistes et nationalistes. Les gens recherchent sur les réseaux sociaux des informations et des personnes qui confirment leur logique (chambres d'écho). Cela exacerbe les antagonismes existants, sème la division sociale et sape la foi dans les institutions. Cette démarche est facilitée par le microciblage et les données comportementales (p. ex. Cambridge Analytica) fondés sur le renseignement de sources ouvertes (p. ex. *Open Source Intelligence* (*OSINT*)).

La montée des leaders populistes et le soutien croissant à l'autoritarisme numérique dans le monde entier illustrent la pénétration et le succès de la guerre cognitive par les États autoritaires. Notre société de l'information démocratique et ouverte sera de plus en plus la cible de telles opérations de manipulation de l'information. Les technologies de rupture vont accentuer cette tendance, car la surface et la vitesse opérationnelles sont décuplées par l'IA et l'informatique quantique. Le cerveau humain est ainsi le champ de bataille du XXIe siècle[3]. En s'appuyant sur les failles cognitives humaines telles que le biais de confirmation ou notre paresse intellectuelle naturelle (conduisant à une absence d'esprit critique), la manipulation de l'information à travers l'environnement informationnel restera un moyen privilégié pour affaiblir les démocraties.

Les affrontements de récits, de narration et de communication feront partie intégrante de la stratégie opérationnelle dans les conflits futurs. Les adversaires des démocraties ont compris, comme le note Nick Reynolds, que « dans la guerre politique, le dégoût est un outil plus puissant que la colère. La colère pousse les gens aux urnes ; le dégoût fait éclater les pays ». De plus, les citoyens des pays démocratiques participent à ce déclin, renforçant ces logiques de silos et de tribalisme, puisque ces fausses informations

[3] MWI Video: « The Brain Is the Battlefield of the Future » par le Dr. James Giordano », Modern War Institute, 29 Octobre 2018.

sont « likées » et/ou repartagées. Alicia Wanless parle de « propagande participative » (Wanless et Berk, 2017). Tout cela est encore facilité par les *bots* et les usines à *trolls*, ainsi que par une exposition répétitive et caractérisée, par des histoires qui se renforcent mutuellement. Par conséquent, le développement de moyens de plus en plus sophistiqués tels que l'intelligence artificielle, les stratégies de communication, le marketing, le *branding* et les neurosciences facilitent la manipulation et constituent un défi majeur en raison des caractéristiques inhérentes au fonctionnement du cerveau humain, telles que les biais cognitifs et l'heuristique.

Dans un monde où la domination des « valeurs occidentales » est de plus en plus contestée par d'autres cultures et modèles, il serait naïf de croire que la manière de combattre, impliquant des règles d'engagement et des codes d'honneur, sera maintenue dans les guerres à venir. Au contraire, les cultures et les visions stratégiques opposées vont se multiplier dans les années à venir. L'un des deux colonels auteurs d' « *Unrestricted Warfare* » amplifiera encore sa pensée en août 1999 : « La guerre a des règles, mais elles sont fixées par l'Occident… Si vous utilisez ces règles, alors les États faibles n'ont aucune chance… Nous sommes un État faible, alors devons-nous nous battre selon vos règles ? Non ». Il y a une tendance en Occident à supposer que l'ennemi adoptera un comportement similaire au nôtre. La vision contemporaine des conflits est ainsi encore trop imprégnée du « paradigme occidental de la guerre » : la confrontation entre des États ayant les mêmes concepts politiques, culturels et idéologiques. Par conséquent, la culture stratégique occidentale n'est pas adaptée à la guerre hybride et cognitive. L'Occident semble oublier trop souvent que la guerre est une dialectique des volontés et, plus encore aujourd'hui qu'hier, une bataille de perceptions et de visions du monde. On peut retenir différentes raisons à cela.

Premièrement, la culture stratégique occidentale est liée à une approche binaire des choses : bon ou mauvais, blanc ou noir. L'Occident se trouve dans une relation théorie-pratique prédéterminée, laissant peu de place à la réflexion hors des sentiers battus. Pour Womack, la pensée occidentale est déterminée par une « logique de transaction ». Celle-ci se caractérise par une relation contractuelle et un désir d'être dans une relation gagnant-perdant, coût-bénéfice (Pan, 2016). Les Chinois mettront davantage l'accent sur la relation elle-même et ses avantages mutuels en jouant sur le respect pour finalement obtenir un avantage. De même, contrairement à l'Occident, par exemple, la Chine évitera de qualifier les États d'ennemis. C'est un grand avantage dans la guerre cognitive. En d'autres termes, la stratégie occidentale sera souvent préétablie dans un canevas bien défini, dont il est difficile de sortir – les faits devant s'adapter à la conceptualisation ou à la modélisation, voire forcer les faits à entrer dans le modèle. D'où également, le fait que la Chine défend les principes de non-ingérence, et qu'elle évite souvent de prendre une position définitive et tranchée dans les dossiers internationaux (p. ex. la Syrie, la Libye…). En refusant de voir les choses à travers une lecture binaire (bien-mal et démocratie-dictature), elle se laisse une marge de manœuvre continue, évitant de forcer ou d'imposer la situation, ce qui lui permet de surfer sur la vague du potentiel de la situation, ce qui n'est pas le cas de l'Occident.

Deuxièmement, le mode de guerre occidental est basé sur la technologie et la cinétique dans une logique de jeu à somme nulle. La *Revolution in Military Affairs* ou *Offset Strategy* des États-Unis sont par exemple basées sur la supériorité technologique dans les différents domaines (air, terre, mer, espace et cyberespace), le domaine cognitif ou humain est absent. L'approche chinoise est plus centrée sur les personnes, moins techno-centrée, basée sur des victoires relatives, la subversion et la tromperie. La Chine joue au Go, l'Occident aux échecs. Or, la supériorité technologique n'est pas synonyme de victoire comme l'ont montré la Libye, l'Afghanistan et l'Irak. L'Occident souffre aujourd'hui d'atrophie et d'incompétence stratégiques, toujours en train de mener la dernière guerre, et ne comprenant pas la suivante. La guerre cognitive est un excellent exemple de cette paralysie stratégique occidentale.

Troisièmement, l'Occident distingue encore la paix de la guerre, ce qui n'est pas le cas de la Chine comme dit précédemment. Les règles de la guerre ne sont plus déterminées par l'Occident mais par nos adversaires et nous ne l'avons pas encore compris : « Les adversaires rusés exploitent l'espace entre la guerre et la paix pour obtenir un effet dévastateur. Washington a une expression à la mode pour cela : la « zone grise ».

D'autres ont une stratégie » (McFate, 2019). La distinction paix-guerre est dépassée et l'Occident ne s'est pas conformé et adapté à cette nouvelle réalité.

Quatrièmement, les armées occidentales sont encore trop hiérarchisées, bureaucratiques, lentes, travaillant dans une logique de silos ou de vision en tunnel, alors que la société est plus horizontale, adaptative, flexible et fonctionnant en réseau. Comme l'explique le Général McChrystal : « Notre culture n'oblige pas les dirigeants à tenir compte de l'intersection entre la stratégie et l'adaptabilité […] nous devons combiner la pensée hors des sentiers battus et la pensée ordonnée. Ce type de leadership hybride sera nécessaire non seulement pour réussir dans la guerre, mais aussi dans d'autres mondes »[4].

Enfin, ces différences de culture stratégique entre la Chine et l'Occident se reflètent également dans les différences cognitives entre les Asiatiques et les Occidentaux. Dans différentes études, Nisbett affirme que les Orientaux, par rapport aux Occidentaux, « ont une vision contextuelle du monde » et que les événements sont perçus comme « hautement complexes et déterminés par de nombreux facteurs », alors que les Occidentaux suivront une logique d' « objets isolés de leur contexte » et donc de « contrôle du comportement des objets » (Nisbett, 2003). Pour Nisbett, la pensée chinoise est plus dialectique que logique : les choses se produisent dans un contexte approprié. Elle est également plus fondée sur les relations et, enfin, là où les Occidentaux croient en la stabilité, les Orientaux voient davantage le changement. Toujours selon Nisbett, les Chinois ont une approche holistique du monde, mettant l'accent sur les relations, les interrelations, les cycles, alors que l'Occident sépare les objets de l'environnement, voit un mouvement linéaire des événements et a l'impression de contrôler personnellement les événements : « Les Asiatiques ont une vision globale et ils voient les objets en relation avec leur environnement – à tel point qu'il peut être difficile pour eux de séparer visuellement les objets de leur environnement. Les Occidentaux se concentrent sur les objets tout en minimisant le champ et ils voient littéralement moins d'objets et de relations dans l'environnement que les Asiatiques » (ibid.).

8.3 CONCLUSION

La guerre reste imprévisible car elle est menée par l'homme, un être émotionnel et faillible. La guerre n'est pas une science mais un art, ouvert à l'évolution et à l'adaptation. La complexité de la guerre reste le maître mot. Chaque adversaire forme un système, un organisme qu'il faut pénétrer. Comme l'a dit Mao : « si l'on ne comprend pas les conditions de la guerre, son caractère, les liens qui l'unissent à d'autres phénomènes, on s'expose à ignorer les lois de la guerre, la manière de la faire, on est impuissant à vaincre ». L'Occident a été dépassé par ses adversaires sur deux niveaux asymétriques – l'asymétrie ontologique – culturelle et l'asymétrie cognitive – ayant un impact direct sur le rapport de force entre l'Occident et la Chine.

Au cours des deux derniers siècles, la plupart des guerres, en particulier en Europe, ont pris une forme symétrique. Il n'y avait pas seulement une symétrie instrumentale, mais aussi une symétrie des normes et des rationalités. Les guerres étaient pensées et menées selon un même schéma, un même code d'honneur. La symétrie tend de plus en plus à céder la place à l'asymétrie. D'une certaine manière, les peuples et les États se combattent, mais sans comprendre leurs stratégies réciproques, car ils agissent selon des schémas culturels, ontologiques, cognitifs différents, rendant impossible l'adoption de règles communes.

Dans ce contexte, les sciences sociales, bien que n'étant pas des sciences de la linéarité, ont l'avantage d'ouvrir nos esprits à la complexité, et in fine à un monde néo-clausewitzien[5]. Alors peut-être avons-nous besoin de plus de philosophie, de sociologie, d'histoire, de disciplines dont les principes et les applications ne sont pas, par essence, linéaires et peuvent supposer une meilleure préparation mentale pour affronter les réalités du combat.

[4] General Stanley A. McChrystal, cité par McFate, 2019.

[5] La notion « Neo-clausewitzianisme » a été initialement inventée dans un sens péjoratif, pour tenter d'expliquer la logique destenants de la guerre nucléaire (Henrotin et al., 2004).

Nos adversaires ne perçoivent pas seulement leurs avantages comparatifs en termes technologiques, mais en termes d'identité, de cognition, de culture, de psychologie collective et de volonté populaire. La rationalité stratégique occidentale exigera, en plus de son ancienne composanteinstrumentale, de prendre en compte la rationalité culturelle et cognitive des adversaires, ce que nos adversaires maîtrisent.

Ce point est important car il a un impact direct sur la puissance d'un État. Comme l'expliquent Dekel et Moran-Gilad (2019), que nous citons longuement :

> *La structuration de la cognition lors d'un conflit entre acteurs adverses comprend plusieurs étapes : la formulation du récit du conflit en décrivant la réalité qui prévalait auparavant ; la nécessité et la légitimité de changer la situation ou de la maintenir, en raison d'une évaluation selon laquelle les états finaux possibles sont inférieurs à la situation actuelle ; les raisons de définir les objectifs politico-militaires ; et les principes de conduite de la campagne de manière à influencer la conscience des différents publics cibles d'une manière qui serve l'objectif stratégique.*

Les différentes mesures et pouvoirs exercés doivent correspondre au « récit » que l'acteur souhaite transmettre aux publics cibles désignés. Ceci afin que la construction de la cognition soit efficace et renforce la légitimité de l'exercice du hard power, en particulier du pouvoir militaire ; afin que les résultats de l'exercice du *hard power* ou du *soft power* se traduisent en résultats politiques et internationaux ; afin qu'il soit possible de façonner une image de la victoire qui illustre la réalisation des objectifs politico-militaires ou qui contrebalance les résultats de l'adversaire ».

8.4 BIBLIOGRAPHIE

Allègre, C., Jeambar, D. (2006). Le Défi du Monde. Fayard: Paris, France.

Bernal, A., Carter, C., Singh, I., Cao, K., Madreperla, O. (2020). Cognitive Warfare: An Attack on Truth and Thought. NATO & John Hopkins University: Baltimore MD, USA.

Booth, K., Trood, R. (1999). Strategic Cultures in the Asia-Pacific Region. St. Martin's Press: New York NY, USA.

Cheng, D. (2012). Winning Without Fighting: Chinese Legal Warfare. Backgrounder, 2692, 12 mai 2012. The Heritage Foundation: Washington DC, USA.

Dekel, U., Moran-Gilad, L. (2019). Cognition: Combining Soft Power and Hard Power. In Y. Kuperwasser, D. Siman-Tov (Eds.), The Cognitive Campaign: Strategic and Intelligence Perspectives, Intelligence in Theory and in Practice. 4, 10, 2019, 151-164. The Institute for the Research of the Methodology of Intelligence & The Institute for National Security Studies: Tel Aviv, Israel.

Hanson, V.D. (2004). Our Weird Way of War. National Review Online, 7 mai 2004.

Henrotin, J., De Neve, A., Struye de Swielande, T. (2004). Vers un monde néo-clausewitzien ? In J. Henrotin (Ed.) Au risque du chaos. Premières leçons de la guerre d'Irak. Armand Colin: Paris, France.

Jullien, F. (2015). De l'Être au Vivre. Éditions Gallimard: Paris, France.

Kuperwasser, Y., Siman-Tov, D. (Eds.) (2019). The Cognitive Campaign: Strategic and Intelligence Perspectives. Intelligence in Theory and in Practice. 4, 10, 2019. The Institute for the Research of the Methodology of Intelligence & The Institute for National Security Studies: Tel Aviv, Israel.

McFate, S. (2019). The New Rules of War: Victory in the Age of Durable Disorder. William Morrow & Cie: New-York NY, USA.

Nisbett, R. (2003). The Geography of Thought: How Asians and Westerners Think Differently… and Why. The Free Press: New York NY, USA.

Pan, Z. (2016). Guanxi, Weiqi and Chinese Strategic Thinking. Chinese Political Science Review, 2016, 1, 306.

Qiao, L., Wang, X. (1999). Unrestricted Warfare. Beijing (Chine): People's Liberation Army Literature and Arts Publishing House. La Guerre Hors Limites, traduction de H. Denès (2006). Rivages: Paris (France); Réédition (2015) Unrestricted Warfare. Echo Point Books & Media: Brattleboro VT, USA.

Rogers, J. (2021). Discursive Statecraft: Preparing for National Positioning Operations. Council on Geostrategy, 7 avril 2021. Geostrategy Ltd: London, UK.

Shtepa, V. (2021). Advisor to Russian Defense Minister Warns of 'Mental War': Who Is Waging It and Against Whom? Eurasia Daily Monitor, 18, 61, 15 avril 2021.

Ya'alon, M. (2019). The Cognitive War as an Element of National Security: Based on Personal Experience, In Y. Kuperwasser, D. Siman-Tov (Eds.) The Cognitive Campaign: Strategic and Intelligence Perspectives, Intelligence in Theory and in Practice. 4, 10, 2019, 13-23. The Institute for the Research of the Methodology of Intelligence & The Institute for National Security Studies: Tel Aviv (Israel).

Yanrong, H. (2006). Legal Warfare: Military Legal Work's High Ground: An Interview with Chinese Politics and Law University Military Legal Research Center Special Researcher Xun Dandong, Legal Daily (Journal de la République Populaire de Chine), 12 février 2006.

Wanlass, A., Berk, M. (2017). Participatory Propaganda: The Engagement of Audiences in the Spread of Persuasive Communications. Proceedings of the Social Media and Social Order, Culture Conflict 2.0 International Conference. Oslo (Norvège): 30 novembre 2017.

Zeman, P. (2021). Social Antiaccess/Area-Denial (Social A2/AD). Journal of Advanced Military Studies, 12, 1, 149-164.

Chapitre 9 – CYBERPSYCHOLOGIE[1]

Professeur Bernard Claverie[2], Professeur Barbara Kowalczuk[3]

La « cyberpsychologie » peut être définie comme étant l'étude des phénomènes mentaux enrelations avec les cyber-systèmes et les contextes cybernétiques. Le terme[4] est un néologisme qui se réfère à deux concepts interdépendants : la « psychologie » comme étude scientifique ducomportement et de la pensée, et la « cybernétique » comme science des lois du contrôle et de la communication des mécanismes et des machines.

9.1 LES MACHINES ET LES HUMAINS

S'il est courant de parler de confrontation entre Intelligence artificielle (IA) et Intelligence naturelle (IN), alors qu'augmenter l'IN avec des systèmes d'IA peut être compris de manière erronée, comme revêtant un aspect effrayant car l'IA pourrait attenter, voire menacer nos libertés individuelles et collectives, de nombreux scientifiques ont développé un champ de réflexions sur la cyberpsychologie. L'avènement des machines intelligentes est pour certains de ces scientifiques unesolution pour faire face aux problèmes humains ; pour d'autres, il représente une menace pour l'avenir de l'humanité. Bien entendu, il est évident que le monde cybernétique a transformé et transforme encore aujourd'hui les humains, et il les transformera probablement encore plus dans le futur.

Les robots intelligents sont utilisés dans les usines, les hôpitaux, les gares et les aéroports. Ils apparaîtront bientôt sur les champs de bataille. Des partenaires numériques et des cyber- collaborateurs envahissent nos maisons, nos bureaux et nos lieux de vie. Cela n'est pas sans conséquence sur la société, sur les groupes sociaux, mais aussi sur les individus qui les composent, en transformant progressivement leurs corps et leur pensée. Comme les humaines s'adaptent-ils à cechangement global, et comment le monde cybernétique s'adapte-t-il aux humains qui eux-mêmes changent ? Ces questions amènent le scientifique à s'interroger sur cette évolution conjointe, leurs effets mutuels sur la pensée, sur l'intelligence, les émotions, les personnalités, et sur les façons de concevoir des nouvelles machines, sur leurs usages et leur transformation. Ainsi est-il nécessaire d'étudier la relation entre les humains et les systèmes cybernétiques, l'intelligence artificielle, les robots, etc.

L'évolution de l'IA fait apparaître de nouveaux mots, de nouveaux concepts, mais aussi de nouvelles théories qui englobent une étude du fonctionnement naturel des humains et des machines, celles qu'ils ont construites et qui, aujourd'hui, sont pleinement intégrées à leur environnement naturel (anthropotechnique). Les humains de demain devront donc développer une psychologie de leur relation aux machines, mais le défi du futur sera probablement de développer une psychologie des machines entre elles, celle des logiciels intelligents artificiels ou des robots hybrides.

Dans ce contexte, la cyberpsychologie est au croisement des deux champs psychologique et cybernétique. Elle est entendue comme étant la science des mécanismes du comportement et de la pensée chez l'homme

[1] Ce texte a été initialement publié en langue anglaise sur le site de l'Innovation Hub de NATO-ACT (Norfolk, Virginie, USA), le 1er juin 2018.

[2] Bernard Claverie est professeur des universités, directeur honoraire et fondateur de l'Ecole Nationale Supérieure de Cognitique – Institut Polytechnique de Bordeaux (France) – et chercheur au CNRS – UMR5218 – Université de Bordeaux.

[3] Barbara Kowalczuk est professeur agrégée de lettres, docteur en littérature anglaise à l'Université de Bordeaux.

[4] Cyberpsychology et cyber-psychology sont synonymes. Idem pour cybercognitique et cyber-cognitique, psychocybernetique et psycho-cybernetique, cybersystèmes et cyber-systèmes, cyberdépendance et cyber-Dépendance, cybertechnologie et cyber-technologie, etc.

en relation avec les machines, et des lois psychologiques qui s'appliquent à l'espace cybernétique et aux systèmes cybernétiques eux-mêmes. En tant que discipline autonome, en relation avec ses disciplines maternelles, elle s'est développée depuis la fin du XX^{e} siècle et partage avec ces disciplines leurs caractéristiques, leurs limites et leurs méthodes tout en en développant d'autres qui résultent de leurs relations réciproques. Centrée sur la clarification des mécanismes de la pensée et sur les conceptions, les usages et les limites des systèmes cybernétiques, la cyberpsychologie est une discipline s'inscrivant dans le vaste domaine des sciences cognitives.

9.2 LA CYBERPSYCHOLOGIE ET LE PROBLEME DE LA CAUSALITE

La relation entre l'esprit (*psycho*) et le cyber (technologie de l'information) peut être étudiée sous différents points de vue. Alors que le domaine de la cyberpsychologie est parfois réduit de façon rapide à une définition à sens unique, il est crucial de ne pas restreindre le champ de la recherche aux seules applications de réalité virtuelle ou de psychothérapie. La cyberpsychologie soulève de nombreuses autres questions, notamment celles concernant les motivations, les besoins, les réticences et les difficultés liées à l'utilisation des cyber-outils et à leurs environnements. D'autres questions concernent la conception, la mise en œuvre ou le contrôle des systèmes informatiques en ce qui concerne les caractéristiques et les processus psychologiques des concepteurs ou utilisateurs.

Ainsi, la cyberpsychologie peut être reliée à différents sujets concrets, en ce qui concerne les questions de santé, dans l'aérospatiale et le transport, pour la sécurité globale, les organisations militaires, la prise de décision, l'éducation, etc. En fait, la cyberpsychologie comprend trois catégories distinctes. Leurs différences sont basées sur le lien de causalité entre les éléments respectifs de chacun des mondes psychologiques et cybertechniques, et leur variation. Ces éléments sont appelés des « variables causales ».

Selon le célèbre épistémologue anglais Karl Popper, le sens commun tend à affirmer que « tout événement est causé par un événement qui le précède ». Cette conviction spontanée est à la base de la « perspective déterministe » selon laquelle chaque chose ou chaque évènement a une cause. Certains scientifiques vont même plus loin et sont convaincus que chaque événement provoque un autre événement. Ainsi, tout peut être considéré comme ayant une cause et une conséquence.

Cette position intellectuelle est appelée « déterminisme universel ». En science, au moins deux conséquences découlent de cette théorie : on peut ainsi « expliquer » n'importe quelle chose ou n'importe quel événement ; on peut également « prédire » les choses ou les événements quidécouleront du présent ou du passé.

Dans ce contexte déterministe, une « variable dépendante » est traditionnellement définie comme unélément dont la variation dépend de celle d'un autre élément qui reste indépendant de la forme de la causalité. Nous disons alors que les variations d'une cause produisent les variations d'une autre. On parle alors respectivement de variable Indépendante (I) et de variable Dépendante (D). Le lien causal est orienté de I vers D ($d\mathrm{I} \Rightarrow d\mathrm{D}$). Inversement, les variations de D ne sont pas causales de celles de I ($d\mathrm{D} \not\Rightarrow d\mathrm{I}$), sauf pour définir des variables covariantes ou corrélatives, dans une relation non- causale ($d\mathrm{D} \Leftrightarrow d\mathrm{I}$) ou plus exactement, pour certains scientifiques, une relation causale potentielle qui n'est pas encore connue car pas encore découverte.

Ces trois sous-thèmes de la cyberpsychologie peuvent être définis comme « cyber-cognitique », « psycho-cybernetique » et « cyberpsychologie globale ».

Table 9-1 : Représentation factorielle des différents domaines de la cyberpsychologie relativement au statut de lacausalité technique (cyber) ou psychologique (cognitique).

	Psycho-cybernetique	Cyber-cognitique
Données Psychologiques	Variables dépendantes (D) non causales	Variables indépendantes (I) causales
Données Techniques	Variables indépendantes (I) causales	Variables dépendantes (D) non causales
Co-relativité	Covariation/corrélation/causalité cachée/indétermination	

9.3 L'INFLUENCE CYBERTECHNIQUE

L'effet du cybernétique sur la dimension psychologique (humaine) constitue donc une première partie de la cyberpsychologie. Pour tous les aspects de la recherche, les conditions expérimentales déterminent un statut de variable indépendante aux données techniques, et un statut de variable dépendante aux données psychologiques. Ce champ peut être littéralement désigné comme « psycho-cybernétique ».

Les effets de ces dimensions cyber-techniques sur l'esprit concernent (liste non exhaustive) :

- Le comportement et la pensée (facilitation cognitive, ergonomie, déficience cognitive, erreur humaine, etc.) ;
- Les traits psychologiques et la personnalité (structuration, altérations, utilisation du « soft power » ou techniques d'ingénierie sociale) ;
- La formation professionnelle et l'apprentissage ;
- L'éducation (des enfants et adolescents, des adultes, des apprentis par rapport aux experts, la gestion des connaissances, etc.) ;
- La psycho-réhabilitation, les psychothérapies (psychiatrie, santé mentale, trouble de stress post-traumatique, lésion cérébrale, lésion morale) ; et
- La prévention (la cyberdépendance est désormais officiellement reconnue comme une maladie psychologique par l'Organisation mondiale de la santé).

9.4 LA CAUSALITE PSYCHOTECHNIQUE

Les conséquences des variables psychologiques sur le monde cyber définissent un domaine « cyber-cognitique ». Il est possible de décrire certains des effets de la psychologie sur la cybertechnologie ou sur le cyberdomaine (liste non exhaustive) avec :

- Les styles de programmation informatique, la structure des programmes, etc. ;
- Les imitations et l'analogie (réseaux neuronaux versus programmation symbolique, modes hybrides, IA différentes, etc.) ;
- Les modes de mise en œuvre (réseaux, computeurs, calcul intensif, parallélisme, logique floue et informatique quantique, etc.) ;
- La confiance numérique (autonomie complète ou partielle, suivi et contrôle, de la délégation aux machines, etc.) ;
- La résistance au numérique (stratégies d'évitement, procrastination, etc.) ;

- Le domaine de cyberdéfense psychologique (cybersécurité, notamment invasive ou défensive, techniques d'attrition, etc.) « l'homme est la première faille des systèmes numériques », *MIMA*[5], etc. ; et
- La cyber-radicalisation (processus cognitifs, environnements sociaux, milieu carcéral, libertés, droits, etc.).

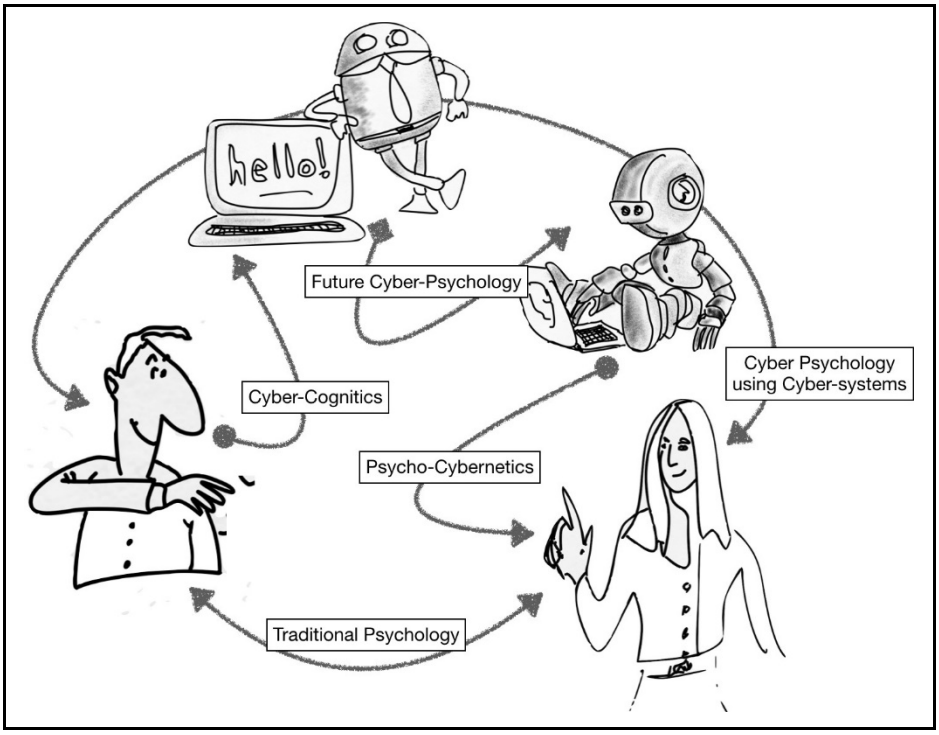


Figure 9-1 : Différent domaines de la cyberpsychologie.

9.5 LES SYSTEMES INTEGRES

Le troisième type d'effet peut être caractérisé par des relations non causales, ou des relations causales inconnues, principalement dans des systèmes complexes. Il concerne le domaine de l'intégration homme système (*HSI*)[6] (Booher, 2003 ; Pew et Mavor, 2007) ou de l'Association humain-automates (*HAT*)[7] (Shively et al., 2007 ; Demir et al., 2017), dans un monde anthropotechnique (liste non exhaustive) :

- Certains éléments de l'interface homme-machine ;
- L'association de machines humaines ;
- Symbiose de machine humaine, hybridité de machine humaine ;
- NBIC ou technologies convergentes pour la valorisation humaine associant les 4 domaines des nanotechnologes, biotechnologies, infotechnologie (informatique) et cognitique (sciences cognitives appliquées) ; et
- etc.

[5] *MIMA* : *Man-In-the-Middle Attack*.

[6] *HSI* : *Human-System Integration*.

[7] *HAT* : *Human-Autonomy Teaming*.

9.6 CONCLUSION

On peut affirmer que la cyberpsychologie est un champ scientifique complexe et en rapide développement qui englobe des phénomènes divers et des sous-thèmes différents. Avec l'avènement des machines intelligentes et autonomes, il est devenu primordial de développer une nouvelle forme de psychologie, qui examinera la façon dont les humains et les machines se touchent les uns les autres. En outre, il explorera comment la relation entre les humains et l'IA va changer les interactions humaines et l'intercommunication des machines.

Il nécessite des définitions et des différenciations précises afin de ne laisser aucune ambiguïté. La recherche et les applications doivent donc prendre en considération le type et la spécificité de la relation causale qui sous-tend le lien entre la psychologie et la cybernétique. En termes de recherche et de mise en œuvre, elle concerne une variété de questions liées à la défense et la sécurité, et à tous les domaines prioritaires de l'OTAN pour préparer l'avenir.

9.7 BIBLIOGRAPHIE

Booher, H.R. (Ed.) (2003). Handbook of Human Systems Integration. Wiley : Hoboken NJ, USA.

Demir, M., McNeese, N.J., Cooke N.J. (2017). Team Synchrony in Human-Autonomy Teaming, Advances in Human Factors in Robots and Unmanned Systems – Proceedings of the AHFE 2017, New-York (NY, USA): Springer Verlag, 303-312.

Pew, R.W., Mavor, A.S., (2007). Human-System Integration in the System Development Process: A New Look. National Academies Press : Washington DC, USA.

Popper K. (2002). The Logic of Scientific Discovery, London (UK): Routledge.

Roco M.C., Bainbridge W.S. (Eds.) (2002). Converging Technologies for Improving Human Performance. National Science Foundation: Arlington VA, USA.

Shively R.J., Brandt S.L., Lachter J., Matessa M., Sadler G., Batiste H. (2007). Application of Human-Autonomy Teaming (HAT) Patterns to Reduced Crew Operations (RCO). White paper, NASA Ames Research Center, NASA WP: Moffett Field CA, USA.

Chapitre 10 – LE PARTAGE DE CONSCIENCE DE SITUATION EST UN LIEN DE FRAGILITE COGNITIVE[1]

Baptiste Prébot[2]

« Savoir ce que pense l'autre de la situation afin d'en partager la même conscience est au fondement de la collaboration. »

Construire et maintenir une conscience de situation commune est l'une des activités cognitives les plus difficiles auxquelles sont confrontés les partenaires d'une équipe. C'est aussi l'un des lieux de fragilité du travail d'équipe ou en réseau. À l'échelle individuelle comme collective, la représentation est au cœur du processus cognitif de prise de décision. Le partage d'une compréhension commune de la situation, c'est-à-dire similaire entre coéquipiers, est nécessaire à la cohérence de la décision.

La conscience de situation et son partage, sont particulièrement sensibles aux influences contextuelles, et il convient d'apporter toute l'aide technologique nécessaire, tant en ce qui concerne sa facilitation que sa sécurisation dans l'encadrement de l'erreur potentielle.

Ce partenariat peut être cible du *cognitive warfare*. Il s'agit, pour des attaquants, d'influencer la représentation individuelle en agissant sur tous les moyens de partage de celles-ci, qu'ils soient technologiques ou sociaux. Face à une menace d'influence ou de manipulation, le défenseur doit traiter ce risque et faciliter les conditions de la robustesse du partage de conscience de situation.

10.1 LA CONSCIENCE DE LA SITUATION

On entend par « conscience de situation » (*Situation Awareness* (*SA*)) la résultante de l'ensemble des processus cognitifs qui concourent à la « représentation qu'un individu se fait de la situation dans laquelle il est impliqué » (Nofi, 2000). Ces 30 dernières années, son évaluation s'est imposée comme incontournable dans l'étude des environnements opérationnels complexes, notamment en matière militaire. Issue des études d'accidentologie de la fin des années 1980 (Foushee et Helmreich, 1988), la notion de conscience de situation est devenue un sujet de préoccupation dans des contextes de formation, de conception et d'opération (Buchler et al., 2016 ; Chen et al., 2016 ; Endsley, 2004 ; Endsley et al., 2003 ; Salas et al., 1997). Sa place centrale dans le processus de prise de décision, des opérateurs, que ce soit au niveau individuel ou à celui d'une équipe, fait de son évaluation un élément clé dans la prédiction de la performance.

Alors que la technologie devient de plus en plus personnalisable, l'attention s'est orientée vers des moyens d'évaluation en temps réel de l'état cognitif des utilisateurs ou des équipes. Le but est notamment d'offrir des systèmes d'information aux commandeurs d'opérations comme aux opérateurs eux-mêmes. À terme, on envisage des systèmes d'aide technique dotés de capacités de réaction automatique pour pallier les états de défaut de conscience de situation de l'utilisateur qui présenteraient des risques pour la performance. Par exemple, on a pu montrer que dans des systèmes d'enseignement adaptatifs, certaines mesures en temps réel permettent de surveiller et de garantir un état optimal pour l'apprentissage, en mesurant et en ajustant par

[1] Texte additionnel fourni aux participants.

[2] Baptiste Prébot est ingénieur diplômé de l'Ecole Nationale Supérieure de Cognitique de Institut Polytechnique de Bordeaux (France), et docteur de l'Université de Bordeaux en ingénierie cognitique. Il est professeur assistant (ATER) à l'ENSC et chercheur dans l'UMR5218, unité mixte de recherche du CNRS, de l'Université de Bordeaux, de Bordeaux INP. Il a soutenu sa thèse en 2019 au sein de l'Ecole doctorale des Sciences Physiques et de l'Ingénieur (ED-209). Sur la conscience de situation partagée dans les activités de C2.

exemple en continu le niveau de sollicitation attentionnelle (Carneiro et al., 2016 ; Szafir et Mutlu, 2012). Dans des contextes opérationnels militaires ou lorsque certains experts gèrent des systèmes de décision complexes, ce type de mesures en continu permet de soulager les utilisateurs en adaptant le niveau d'automatisation et le mode d'interaction ou de communication (Scerbo, 1996).

Les méthodes sont conçues pour détecter ce qui est erroné dans la représentation que les individusse font d'une situation donnée. Elles se sont jusqu'ici plus centrées sur l'exactitude de la conscience de situation que sur la rapidité avec laquelle elle est acquise. Les méthodes ont donc été plus qualitatives que quantitatives. En effet, selon les auteurs du domaine (Endsley et al., 2003), la conscience de situation est avant tout une construction cognitive dont l'évaluation demande unaccès déclaratif à son contenu. De ce fait, la mesure a recours à la verbalisation, la rendant inévitablement tardive (*ex post facto*) et nécessairement subjective et partielle. À mesure que l'environnement évolue, la conscience de situation est reconstruite, soumise à un processus continu de mise à jour pour intégrer de nouveaux événements et aux aléas de la mémoire. Des nouvelles informations et de nouveaux objectifs émergent avec le temps. La conscience de situation est donc dynamique (Hjelmfelt et Pokrant, 1998 ; Nofi, 2000) et constitue une structure en constante évolution. Les techniques d'évaluation classiques de la psychologie ou de l'ergonomie restent incapables de traduire cette nature dynamique hors de la verbalisation, et donc de la décontextualisation des sujets interrogés (Stanton et al., 2017). Par ailleurs, en cas de problème,cette évaluation arrive trop tard.

Les évaluations temporelles en temps réel sont donc souhaitables, notamment pour savoir quand adapter les comportements ou les interfaces, réagir et intervenir lorsque la situation devient critique,ou déclencher immédiatement les aides artificielles par des moyens d'augmentation cognitive, voirede substitution en cas de dépassement. Dans le cas d'une équipe d'opérateurs, cette évaluation continue de la conscience de situation est indispensable pour déterminer quand la performance de l'équipe risque souffrir de différences de compréhension ou de représentation. Plusieurs auteurs s'accordent à penser que l'élaboration de mesures objectives de la conscience de situation, non intrusives et en temps réel, est une étape logique et nécessaire des systèmes opérationnels de demain (De Winter et al., 2019 ; Nofi, 2000).

Néanmoins, mettre en relation des indices objectifs, mesurables sans délai, avec des contenus subjectifs dont on n'a connaissance qu'à posteriori n'est pas chose simple. Pour répondre à cette nécessité de mesure objective de la conscience de situation pour des systèmes de surveillance et de prise de décision, les chercheurs se sont intéressés à un phénomène qui caractérise plusieurs opérateurs travaillant sur une même tache : le processus de synchronie des consciences de situation *(SA Synchrony*).

10.2 SYNCHRONIE COGNITIVE

La représentation de la situation dépend de la perception et de l'interprétation continue des éléments de l'environnement (Salas et al., 1995). Dans le contexte *Human-Autonomy Teaming* (HAT) des systèmes collaboratifs adaptatifs, aussi bien utilisés en formation qu'en situation opérationnelle, un des besoins est celui de la connaissance en temps réel de l'état de l'opérateur. L'évaluation des modifications temporelles de la conscience de situation (dynamique de la SA) (Adams et al., 1995 ; Ziemke et al., 2017), dans le cas de la collaboration, permet de savoir quand et pendant combien de temps les SA sont (ou ne sont pas) synchronisées. Évaluer ce partage permet de prévenir l'erreur humaine et sa documentation à des fins de Retex et de formation des équipes et équipages.

La mesure de la conscience de situation repose sur le concept de similarité. Celui-là est à examiner vis-à-vis de la réalité, il s'agit alors de l' « exactitude », soit vis-à-vis d'un autre individu, et on parle alors de « similarité ». La synchronie des consciences de situation correspond à l'apparition temporelle de cette similarité, et sa mesure est un indicateur de sa dynamique et du degré de partagede conscience de situation. La mesure de la synchronie s'appuie sur l'estimation de la connaissance ou non d'éléments d'information par les individus de l'équipe. Selon le modèle d'Endsley (1995), laconstruction d'une conscience de situation

partagée découle de la perception et de l'intégration similaire des « bons » éléments situationnels par les coéquipiers ; les « éléments de connaissance nécessaires » (*Necessary Knowledge Elements* (*NKE*)) (Cain et Schuster, 2016). On peut donc considérer les « éléments de connaissance partagée nécessaires » (*Necessary Shared Knowledge Eléments* (*NSKE*)), qui définissent les éléments d'information dont la connaissance est nécessaire à plusieurs membres d'une équipe pour accomplir une partie collaborative de leurs tâches, ou « *Shared SA Requirements* » (Endsley et Jones, 2001).

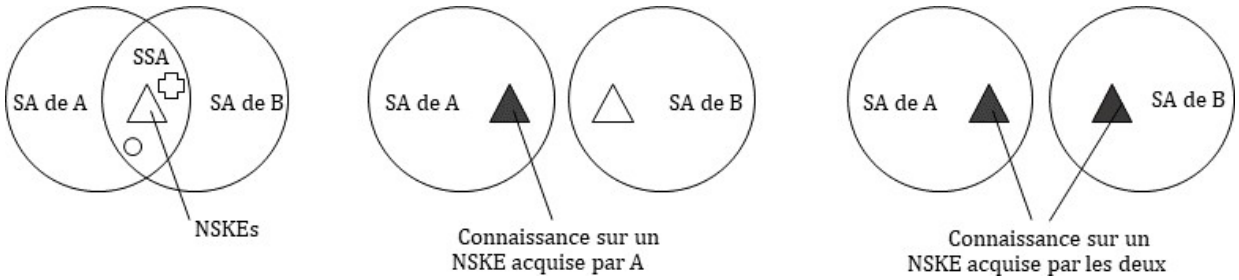


Figure 10-1 : Illustration des trois états de connaissance possible sur un élément de connaissance partagée nécessaire (*Necessary Shared Knowledge Elements* (*NSKE*)). Soit aucun des deux coéquipiers ne possède une connaissance à jour sur l'élément (schéma de gauche), soit l'un la possède et pas l'autre (schéma central), ou soit les deux sont à jour et partagent la connaissance de ce NSKE (schéma de droite).

Tous ces éléments de connaissance dépendent de l'interconnexion des tâches des individus, ils sont donc préalablement identifiés. La formation des équipages permet notamment de construire les modèles mentaux partagés requis, comprenant entre autres cette connaissance des besoins mutuels en termes d'information. D'où la nécessite de constitution d'équipe ayant appris à travailler ensemble et connaissant les systèmes à disposition.

Cependant, les NSKE sont rarement perçus simultanément par chacun des équipiers (Cain et al., 2016 ; Endsley et Jones, 2001), avec des « latences » qu'il convient de définir et prendre en considération. Ainsi, lorsque toutes les informations utiles sont à la disposition de deux coéquipiers (A et B) ayant tous deux réussi à en former la même représentation, ils partagent un même niveaude conscience de situation initial. Chaque fois qu'un nouvel NSKE apparaît, il invalide l'état de la conscience de situation en cours, jusqu'à ce qu'il soit intégré à un nouvel état de conscience de situation des coéquipiers, ou « conscience de situation modifiée », pour obtenir une nouvelle conscience de situation partagée ainsi mise à jour. Dans ce modèle, on distingue 4 phases, créant trois latences remarquables à prendre en compte.

La première latence est dite « latence d'intégration initiale » (*Intial Integration Latency* (*IIL*)). C'est le temps initial requis par un premier coéquipier pour percevoir et intégrer le nouveau NSKE à sa propre conscience de situation. L'intervalle entre l'apparition du NSKE et son intégration dans la conscience de situation de A (Phase 2 de la Figure 10-2) représente une période de conscience de situation partagée mais inexacte qui s'accompagne d'une possibilité de prise de décision erronée. Pendant cette période, les coéquipiers disposent toujours d'une représentation commune de lasituation. Les décisions individuelles sont cohérentes entre-elles et les décisions collectives sont cohérentes avec la stratégie en cours. Cependant, la représentation de la situation n'est plus à jour. Cette différence d'avec la réalité augmente évidemment le risque de prise de décision inappropriée. La durée de cette latence est influencée par les mêmes facteurs concernant l'attention et le système sensori-perceptif qui ont un impact sur la conscience de situation de premier niveau (*level 1 SA*) (Endsley et Garland, 2000) : stress, fatigue, charge de travail ou complexité de l'interface.

La seconde latence, ou « latence de synchronisation de l'équipe » (*Team Synchronization Latency* (*TSL*)), représente le temps mis par un second coéquipier pour percevoir et intégrer le nouveau NSKE à sa conscience de situation après que le premier coéquipier l'a fait (phase 3 de la Figure 10-2). Cela crée

un délai entre les deux mises à jour des *SA* durant lequel, en tenant compte de la première latence (IIL), les représentations de la situation divergent. Pendant cet intervalle de temps, en plus d'être inexacte pour au moins l'un des coéquipiers, la conscience de situation n'est pas non plus partagée ; cela augmente la probabilité d'une prise de décision incohérente. Dans ce cas, deux coéquipiers, dont l'un est à jour avec la situation et l'autre non, peuvent envoyer des instructions incohérentes, voire contradictoires à un troisième.

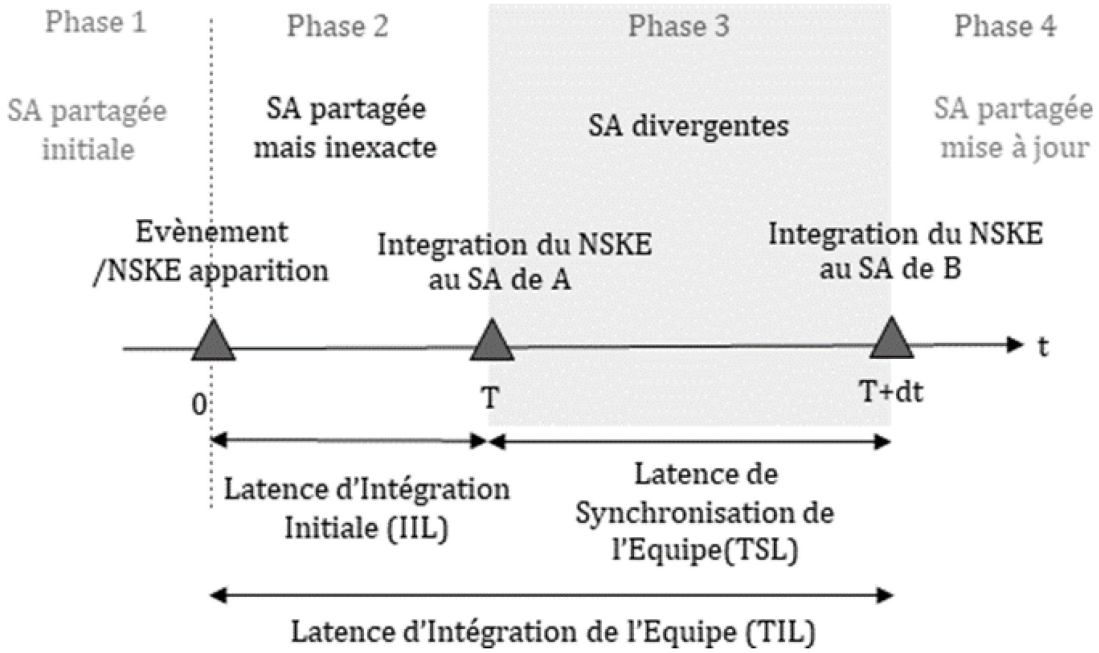


Figure 10-2 : Illustration de l'évolution temporelle des SSA et les latences associées : Latence d'Intégration Initiale (*Initial Integration Latency* (*IIL*)), Latence de Synchronisation de l'Équipe (*Team Synchronization Latency* (*TSL*)) et Latence d'Intégration de l'Équipe (*Team Integration Latency* (*TIL*)).

La « latence d'intégration de l'équipe » (*Team Integration Latency* (*TIL*)), est la composée des deux premières latences. Elle représente le temps écoulé entre l'apparition du NSKE et son intégration par le dernier membre de l'équipe concerné (Phase 2 + Phase 3 ; cf. Figure 10-2). Elle représente la durée pendant laquelle les membres de l'équipe ne maîtrisent pas tous une conscience de situation exacte.

En étant inhérentes au processus de mise à jour et de partage de la conscience de situation, ces latences illustrent l'importance de leurs propriétés dynamiques. Ce modèle s'adapte aussi bien à la modélisation de la dynamique de partage d'une équipe colocalisée qu'à celle d'une équipe distribuée, travaillant en réseau.

10.3 MESURES ET APPLICATIONS POUR UN CONTROLE EN LIGNE

Ces latences de synchronie cognitive étant définies, se pose la question de leur mesure concrète, en ligne, à des fins de contrôle, de détection d'erreur et d'aide par des systèmes artificiels.

Initialement, la mesure concrète de la conscience de situation des individus et des équipes a reposé sur l'analyse du comportement et des processus de raisonnement à voix haute par des observateurs (Cooke et al., 1977). Elle nécessitait la présence des observateurs au sein des équipes. Plus récemment, de nouvelles méthodes sont utilisées avec des quiz sur tablettes permettant de raccourcir les délais d'analyse (Buchler et al. 2018), mais restent relativement invasives.

Les mesures comportementales et physiologiques (Delaherche et al., 2012) ont l'avantage d'être continues et sont faciles à utiliser pour la quantification de l'état et de l'activité de l'utilisateur (Fuchs et Schwarz, 2017 ; Jorna, 1993 ; Tomarken, 1995). La synchronisation des consciences de situation est alors établie par la comparaison temporelle des mesures entre individus. Mais les mesures sont coûteuses en calculs et les équipements lourds et encombrants, pouvant handicaper les opérateurs. C'est récemment qu'on a pu établir la pertinence de l'évaluation continue de la conscience de situation en utilisant une mesure dérivée des mouvements oculaires (De Winter et al., 2019) par des moyens non intrusifs, externes aux sujets (caméra ou capteurs intégrés aux écrans ou situés à proximité).

Le suivi de la position du regard a d'abord permis l'étude de la conscience de situation dans l'aviation (Kilingaru et al., 2013 ; Moore et Gugerty, 2010 ; van de Merwe et al., 2012) et la conduite automobile (Hauland, 2019). La méthode peut être facilement enrichie et croisée avec des mesures des temps de réaction à partir du suivi de la souris ou d'autres comportements résultant de l'interaction (IHM) avec toutes les interfaces (Freeman et Ambady, 2010 ; Frisch et al., 2015 ; Kieslich et al., 2018). Les approche multi-mesures semble d'ailleurs être utiles pour saisir une construction aussi complexe que la conscience de situation (Salmon et al., 2006) et l'approche multidimensionnelle du monitoring « autour de l'opérateur » fournit la base d'une nouvelle évaluation continue et objective en temps réel. Les techniques sont très sensibles mais complexes à mettre en œuvre. Les mesures peuvent en effet être influencées par de nombreux phénomènes parasites qu'il convient d'identifier pour les maîtriser (Cooke et al., 1997).

Comme les communications ajoutent une latence inhérente, une synchronisation idéale des consciences de situation entre les membres d'une équipe n'est pas réaliste (Cooke et al., 2018 ; Sonnenwald et al., 2004 ; Walker et al., 2012). Il faut comprendre que lors d'une collaboration, la pertinence du *NSKE*, son interprétation et la hiérarchisation des tâches sont fonction des stratégies personnelles et des objectifs individuels des opérateurs mesurés. L'identification des problèmes passe par l'évaluation de l'écart par rapport à une latence attendue, requérant une compréhension approfondie de l'ensemble de la tâche, au niveau individuel comme collectif. Les processus et les communications, ainsi que la qualification des marqueurs comportementaux doivent être contextualisés par rapport à l'environnement dans lequel ils sont appliqués (Salas et al., 2017). De même que l'exactitude optimale théorique (Hooey et al., 2011), une meilleure synchronisation des consciences de situation pourrait ainsi être définie sur la base de l'analyse des tâches d'équipe, comme descripteur de la collaboration et de la performance. Elle fournit en temps réel un feedbackà l'équipe, au chef d'équipe ou à un système artificiel d'aide et surveillance.

Grâce à de telles mesures, des entraînements, des interventions adaptatives, des facilitations d'expériences peuvent alors être conçues. Des programmes numériques de facilitation peuvent être développés pour la détection des erreurs de partage de représentation et de synchronisation de la conscience de situation peut être envisagée. Concrètement, l'information et l'aide artificielle peuvent être établies à partir des états optimisés de synchronisation entre les coéquipiers, en identifiant les périodes problématiques au cours des processus de collaboration. Dans un contexte de formation, on peut entraîner les collaborateurs à valoriser des temps d'interaction optimaux.

La complexité et la rapidité des tâches nécessitent de plus en plus la collaboration avec des machines qui peuvent alors aider à éviter les erreurs. La nature dynamique de la conscience de situation et son évolution temporelle nécessitent des moyens légers et non intrusifs (Buchler et al., 2016) qui restent encore aujourd'hui de l'ordre de l'expertise et difficiles à généraliser.

En se concentrant sur le contenu de la conscience de situation, les méthodes de mesure classiques sont de fait limitées par la nature subjective de l'évaluation, la représentation de la situation portant sur une évaluation déclarative. Cela rend difficile une évaluation en temps réel, notamment en situation de stress ou de gestion de situation complexe ne permettant pas de temps de Retex en ligne. Par contre, on peut considérer la synchronie des consciences de situation, et en fournir des indicateurs. On peut repérer leur survenue et leur dynamique dans l'équipe. Par exemple, la mesure des activités pupillométriques (diamètre pupillaire) peut

être réalisée en direct sans équipement porté, par la simple caméra, en croisant ces données avec des mesures comportementales non invasives (activité sur la souris, le clavier, le nombre de communications, les déplacements de la chaise, etc. C'est dans le développement de ces mesures indirectes que réside le repérage d'une activité nécessitant le partage de conscience de situation, et donc, à partir de là, l'utilisation de méthodes a posteriori.

C'est ainsi que, n'évaluant pas nécessairement la qualité du contenu de la représentation mentale, la mesure de la synchronie permet de s'affranchir du besoin de verbalisation et donc d'interruption ou d'intrusion dans la tâche, entrainant la perturbation de cette conscience, ou pouvant altérer l'efficacité de la tâche. Celle-là peut alors être menée à son terme en toute efficacité, alors que les équipiers sont informés en ligne et que les aides numériques peuvent être mobilisées avant que les opérateurs eux-mêmes en expriment le besoin.

10.4 LE PARTAGE DES SA, FAIBLESSE DE L'EQUIPE DANS LE COGNITIVE WARFARE

L'un des objets de la guerre cognitive est d'influencer la prise de décision de l'adversaire, de la manière la plus subtile et indétectable possible, en manipulant la représentation. Si certaines techniques, visant par exemple la stabilité sociale et politique d'une nation ou d'un groupe, jouentsur des temporalités longues, les stratégies développées peuvent également s'appliquer sur la prisede décision en temps réel, notamment par le biais d'opérations cyber.

Il ne s'agit alors plus seulement d'empêcher l'ennemi d'accéder à certaines informations (p. ex. brouillage), mais également de manipuler ces informations, par exemple en lui en fournissant de fausses, par le biais de ses canaux habituels, avec la capacité de cibler quand et à qui fournir quelle information, pour optimiser la déstabilisation de la décision.

De telles techniques permettent d'une part de bénéficier de la confiance que l'individu à envers ses sources d'information, puis dans un second temps, en cas de détection de l'intrusion, de mettre à malcette confiance, que ce soit envers les sources elles-mêmes (systèmes) ou leurs vecteurs (canaux de communication ou coéquipiers).

Par exemple, en fournissant sciemment des informations contradictoires à des coéquipiers, ou à différents niveaux hiérarchiques, on peut conduire à la construction de représentations non cohérentes ou à des conflits de perception au sein d'une équipe. L'impact à long terme peut être une dégradation des confiances interpersonnelles, de la confiance en son propre jugement et de la cohésion de l'équipe.

Les leviers et facteurs influant le partage de la représentation et les processus d'équipe sont connuset font l'objet de nombreux travaux, tant sur la conception adéquate des systèmes, que sur la composition et la formation des équipes (Endsley et al., 2003 ; Nofi, 2000). Contrer ces potentielles influences doit donc passer par la conception de systèmes et outils transparents (eXplainable AI) et fiables, facilitant l'acquisition et le partage de SA. Cela souligne également l'importance de références communes (modèles mentaux) et de méta-connaissances sur l'équipe (tâches, rôles, besoins de chacun), acquises sur le long terme par l'entrainement, l'éducation et la formation.

10.5 CONCLUSION

Le partage réussi de la conscience de situation par les opérateurs d'une même équipe ou de personnes travaillant en réseau est un processus cognitif fondamental au succès des tâches degestion de crise. Il est particulièrement nécessaire au sein des équipages et des systèmes de surveillance ou de conduite d'opérations militaires.

La conscience de situation est l'exemple d'un processus cognitif mobilisant à la fois attention, mémoire, décision, et qui est facilité par les processus d'apprentissage. Le partage de la conscience de situation entre plusieurs acteurs contribuant à une même tâche est un phénomène émergent, repérable et reste malgré tout difficilement altérable. Si les méthodes actuelles pour mesurer son contenu ne sont pas réellement compatibles avec les situations opérationnelles, la mesure de cette émergence, de son actualisation et de leur synchronie, par le biais de méthodes indirectes, est une piste de recherche sérieuse. Une fois mesurée, elle peut alors faire l'objet de procédures d'aide artificielle, par exemple par une visualisation enrichie pour soutenir ou orienter l'attention, ou d'un support au commandement des équipes. Cette détection reste un moyen immédiat et robuste aux influences extérieures ; elle permet à la fois la facilitation de la tâche de collaboration comme le repérage des phases stratégiques pour le Retex.

Ainsi, dans des environnements où construire et maintenir une compréhension commune de la situation est en temps normal un tâche difficile, source des principales erreurs et accidents, la conscience de situation représente un point fragilité de l'équipe, soumis aux effets de la guerre cognitive. Dès lors, l'enjeu de défense porte sur les méthodes et les outils permettant de renforcer la cohésion collective ainsi que sur la fiabilité et la sécurité des systèmes d'information.

10.6 BIBLIOGRAPHIE

Adams, M. J., Tenney, Y. J., Pew, R. W. (1995). Situation Awareness and the Cognitive Management of Complex Systems. Human Factors, 37, 1, 85-104.

Buchler, N., Fitzhugh, S.M., Marusich, L.R., Ungvarsky, D.M., Lebiere, C., Gonzalez, C. (2016). Mission Command in the Age of Network-Enabled Operations: Social Network Analysis of Information Sharing and Situation Awareness. Frontiers in Psychology, 7, 937, 1-15.

Buchler, N., Rajivan, P., Marusich, L.R., Lightner, L., Gonzalez, C. (2018). Sociometrics and Observational Assessment of Teaming and Leadership in a Cyber Security Defense Competition. Computers & Security, 73, 114-136.

Cain, A.A., Schuster, D., Edwards, T., Schuster, D. (2016). A Quantitative Measure for Shared and Complementary Situation Awareness. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 60, 1, 1816-1820.

Carneiro, D., Pimenta, A., Gonçalves, S., Neves, J., Novais, P. (2016). Monitoring and Improving Performance in Human-Computer Interaction. Concurrency Computation, 28(4), 1291-1309. https://doi.org/10.1002/cpe.3635.

Chen, Y., Qian, Z., Lei, W. (2016). Designing a Situational Awareness Information Display: Adopting an Affordance-Based Framework to Amplify User Experience in Environmental Interaction Design. Informatics, 3, 2, 6. https://doi.org/10.3390/informatics3020006.

Cooke, N.J., Stout, R.J., Salas, E. (1997). Broadening the Measurement of Situation Awareness Through Cognitive Engineering Methods. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 41, 4, 215-219. https://doi.org/10.1177/107118139704100149.

Cooke, N. J., Stout, R.J. Salas, E. (2018). A Knowledge Elicitation Approach to the Measurement of the Team Situation Awareness. In E. Salas (Ed.), Situational Awareness, 157-182. Routledge: London UK. https://doi.org/10.4324/9781315087924-10.

De Winter, J.C.F., Eisma, Y.B., Cabrall, C.D.D., Hancock, P.A., Stanton, N.A. (2019). Situation Awareness Based on Eye Movements in Relation to the Task Environment. Cognition, Technology andWork, 21, 1, 99-111. https://doi.org/10.1007/s10111-018-0527-6.

Delaherche, E., Chetouani, M., Mahdhaoui, A., Saint-Georges, C., Viaux, S., Cohen, D. (2012). Interpersonal Synchrony: A Survey of Evaluation Methods Across Disciplines. IEEE Transactionson Affective Computing, 3, 3, 349-365. https://doi.org/10.1109/T-AFFC.2012.12.

Endsley, M.R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. HumanFactors, 37, 1, 32-64. https://doi.org/10.1518/001872095779049543.

Endsley, M.R. (2004). Designing for Situation Awareness: An Approach to User-Centered Design.CRC Press : Boca-Raton FL, USA. https://doi.org/10.1201/b11371.

Endsley, M.R., Bolstad, C.A., Jones, D.G., Riley, J.M. (2003). Situation Awareness Oriented Design: From User's Cognitive Requirements to Creating Effective Supporting Technologies. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 47, 3, 268-272. https://doi.org/10.1177/154193120304700304.

Endsley, M.R., Garland, D.J. (Eds.) (2000). Situation Awareness Analysis and Measurement. Lawrence Erlbaum Associates : Mahwah NJ, USA.

Endsley, M.R., Jones, W.M. (2001). A Model of inter and intra Team Situation Awareness: Implications for Design, Training and Measurement. In M. McNeese, E. Salsa, M. Endsley (Eds) New Trends in Cooperative Activities: Understanding System Dyanmics in Complex Environments, 46–67. Human Factors and Ergonomics Society: Santa Monica CA, USA. https://www.researchgate.net/publication/285745823_A_model_of_inter_and_intra_team_situation_awareness_Implications_for_design_training_and_measurement_New_trends_in_cooperative_activities_Understanding_system_dynamics_in_complex_environments.

Foushee, H.C., Helmreich, R.L. (1988). Group Interaction and Flight Crew Performance. In E.L. Wiener, D.C. Nagel (Eds.) Human Factors in Aviation. Academic Press : Cambridge MA, USA, 89-227.

Freeman, J.B., Ambady, N. (2010). MouseTracker: Software for Studying Real-Time Mental Processing Using a Computer Mouse-Tracking Method. Behavior Research Methods, 42, 1, 226-241. https://doi.org/10.3758/BRM.42.1.226.

Frisch, S., Dshemuchadse, M., Görner, M., Goschke, T., Scherbaum, S. (2015). Unraveling the Sub-Processes of Selective Attention: Insights from Dynamic Modeling and Continuous Behavior. Cognitive Processing, 16,4, 377-388.

Fuchs, S., Schwarz, J. (2017). Towards a Dynamic Selection and Configuration of Adaptation Strategies in Augmented Cognition. Lecture Notes in Computer Science (Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10285, 101-115. https://doi.org/10.1007/978-3-319-58625-0_7.

Hauland, G. (2019). Measuring Team Situation Awareness by Means of Eye Movement Data. Proceedings of HCI International 2003, 3, 230-234.

Hjelmfelt, A. T., Pokrant, M. A. (1998). Coherent Tactical Picture. In A.A. Nofi (Ed.) Defining and Measuring Shared Situational Awareness, 97-129. Center for Naval Analyses CRM : Alexandria VA, USA,. https://www.cna.org/cna_files/pdf/D0002895.A1.pdf.

Hooey, B.L., Gore, B.F., Wickens, C.D., Scott-Nash, S., Socash, C., Salud, E., David, C., Foyle, D.C. (2011). Modeling Pilot Situation Awareness. In P.C. Cacciabue (Ed.) Human Modelling in Assisted Transportation, 207-213. Springer Publishing : New York NY, USA.

Jorna, P. (1993). Heart Rate and Workload Variations in Actual and Simulated Flight. Ergonomics, 36, 9, 1043-1054.

Kieslich, P., Henninger, F., Wulff, D., Haslbeck, J., Schulte-Mecklenbeck, M. (2018). Mouse-Tracking: A Practical Guide to Implementation and Analysis. In M. Schulte-Mecklenbeck, A. Kühberger, J.G. Johnson (Eds.) A Handbook of Process Tracing Methods, 131-145. Routledge : New York NY, USA. https://doi.org/10.31234/osf.io/zuvqa.

Kilingaru, K., Tweedale, J.W., Thatcher, S., Jain, L.C. (2013). Monitoring Pilot "Situation Awareness". Journal of Intelligent & Fuzzy Systems, 24, 3, 457-466.

Moore, K., and Gugerty, L. (2010). Development of a Novel Measure of Situation Awareness: The Case for Eye Movement Analysis. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 54, 19, 1650-1654. https://doi.org/10.1518/107118110X12829370089768.

Nofi, A. (2000). Defining and Measuring Shared Situational Awareness. Final Report, 5, 11. Alexandria (VA, USA) : Center for Naval Analyse CRM. https://doi.org/10.1371/journal.pone.0013350.

Salas, E., Cannon-Bowers, J., Johnston, J. H. (1997). How Can You Turn a Team of Experts into an Expert Team? Emerging Training Strategies. In C.E. Zsambok, G. Klein (Eds.) Naturalistic Decision Making, 359-370. Routledge : New York NY, USA.

Salas, E., Prince, C., Baker, D.P., Shrestha, L. (1995). Situation Awareness in Team Performance: Implications for Measurement and Training. Human Factors, 37, 1, 123-136.

Salas, E., Reyes, D.L., Woods, A.L. (2017). The Assessment of Team Performance: Observations and Needs. In A.A. Von Davier, M. Zhu, P.C., Kyllonen (Eds.) Innovative Assessment of Collaboration, 21-36. Springer International Publishing: New York NY, USA. https://doi.org/10.1007/978-3-319-33261-1.

Salmon, P.M., Stanton, N.A., Walker, G.H., Green, D. (2006). Situation Awareness Measurement: A Review of Applicability for C4i Environments. Applied Ergonomics, 37, 2, 225-238. https://doi.org/10.1016/j.apergo.2005.02.001.

Scerbo, M.W. (1996). Theoretical Perspectives on Adaptive Automation. In R. Parasuraman, M., Mouloua (Eds.) Automation and Human Performance: Theory and Applications, 37-63. Lawrence Erlbaum Associates : Abingdon-on- Thames, UK.

Sonnenwald, D.H., Maglaughlin, K.L., Whitton, M.C. (2004). Designing to Support Situation Awareness Across Distances: An Example from a Scientific Collaboratory. Information Processing & Management, 40, 6, 989-1011.

Stanton, N.A., Salmon, P.M., Walker, G.H., Salas, E., Hancock, P.A. (2017). State-of-Science; Situation Awareness in Individuals, Teams and Systems. Ergonomics, 60, 4, 449-466. https://doi.org/10.1080/00140139.2017.1278796.

Szafir, D., Mutlu, B. (2012). Pay Attention! Designing Adaptive Agents That Monitor and Improve User Engagement. In J.A. Konstan, H. Chi, K. Höök (Eds.) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, May 5 – 10, 2012, 11-20. Association for Computing Machinery : New York NY, USA.. https://doi.org/10.1145/2207676.2207679.

Tomarken, A.J. (1995). A Sychometric Perspective on Psychophysiological Measures. Psychological Assessment, 7, 3, 387-395.

Van de Merwe, K., Van Dijk, H., Zon, R. (2012). Eye Movements as an Indicator of Situation Awareness in a Flight Simulator Experiment. The International Journal of Aviation Psychology, 22, 1, 78-95.

Walker, G.H., Stanton, N.A., Salmon, P.M., Jenkins, D.P., Monnan, S., Handy, S. (2012). Communications and Cohesion: A Comparison Between Two Command and Control Paradigms. Theoretical Issues in Ergonomics Science, 13, 5, 508-527. https://doi.org/10.1080/1463922X.2010.544340.

Ziemke, T., Schaefer, K.E., Endsley, M. (2017). Situation Awareness in Human-Machine Interactive Systems. Cognitive Systems Research, 46, 1-2. https://doi.org/10.1016/j.cogsys.2017.06.004.

Chapitre 11 – ARTICLES DE PRESSE GENERALISTE[1]

Hervé Le Guyader[2]

Tribune – Opinion - parue dans le quotidien « Le Monde » du 6 mai 2021.

Le domaine cognitif de la manipulation est devenu un terrain de conflit

Si elle ne veut pas perdre des batailles, l'OTAN doit prendre en compte un nouveau domaine d'opérations, celui de l'influence par les outils numériques, estime l'ingénieur Hervé Le Guyader, dans une tribune au « Monde », pour qui jouer sur les leviers de la pensée, « c'est contrôler l'individu ».

https://www.lemonde.fr/idees/article/2021/05/06/le-domaine-cognitif-de-la-manipulation-est-devenu-un-terrain-de-conflit_6079291_3232.html

Kimberly Orinx et Tanguy Struye de Swielande[3]

Opinion – Carte blanche – parue dans lequotidien « Le Soir » du 11 mai 2021.

Carte blanche : la guerre cognitive et les vulnérabilités des démocraties

La désinformation est l'une des grandes menaces qui pèsent sur nos démocraties. Les Etats doivent s'emparer de cette problématique en développant des programmes et des outils qui pourront garantir la cohésion sociale.

https://plus.lesoir.be/371510/article/2021-05-11/carte-blanche-la-guerre-cognitive-et-les-vulnerabilites-des-democraties.

[1] Textes additionnels fournis aux participants.

[2] Ecole Nationale Supérieure de Cognitique – Bordeaux INP (France).

[3] Centre d'étude des crises et des conflits internationaux – Université Catholique de Louvain - Louvain-La-Neuve (Belgique).

Chapitre 12 – CONCLUSION GÉNÉRALE ET PERSPECTIVES – LA GUERRE COGNITIQUE ET SES IMPLICATIONS POUR LE PANEL IST DE LA STO

Colonel Docteur Nikolai Stoianov[1]

« Notre responsabilité est de protéger nos soldats afin de les rendre prêts pour la guerre cognitique. »

Les technologies ont toujours modifié la façon dont les différents acteurs sont entrés en conflit, ainsi que les aspects stratégiques, opérationnels et tactiques de la guerre, mais l'explosion des technologies d'information et de communication ainsi que les façons dont il est désormais possible d'influencer l'ensemble des parties prenantes ont totalement changé la philosophie du combat.

Il est clair que le nombre de conflits purement « cinétiques » va diminuer et que l'esprit humain va devenir la cible prioritaire. Il sera par exemple plus difficile d'expliquer à quelqu'un pourquoi il devrait combattre, de façon cinétique, quelqu'un d'autre, mais il sera en même temps plus facile de faire passer son processus de réflexion d'une direction à une autre.

Internet, les réseaux sociaux, l'internet des objets, l'apprentissage machine, l'intelligence artificielle, toutes ces technologies accroissent les possibilités d'analyser finement les processus cognitifs qui définissent les points de vue de nos adversaires potentiels ; inversement, nos ennemis disposent désormais d'options leur permettant de mieux nous connaître et nous comprendre.

De nombreuses communautés de recherche travaillent sur ces sujets, notamment au sein de la STO au travers des travaux menés par ses panels IST, HFM et SET. Il y a aujourd'hui beaucoup plus de questions ouvertes que de problèmes résolus, et de nombreuses décisions en matière de recherche restent à prendre, qui devront tenir compte des aspects légaux, humains et technologiques des problématiques à résoudre.

En tant que chercheurs, membres de la communauté IST, notre responsabilité est de développer des technologies capables de détecter, d'identifier, de suivre et d'éviter ces types de menaces et d'en protéger nos soldats afin de les rendre prêts pour la guerre cognitique.

Sofia, le 25 août 2021.

Le président du panel Information Systems Technology (IST) de la Science & Technology Organization (STO) de l'OTAN.

[1] Nikolai Stoianov est colonel de l'armée bulgare, et professeur associé à l'Université Nationale Militaire « Vasil Levski » (Veliko Tarnovo). Il est directeur adjoint de l'Institut Bulgare de Défense (Bulgarian Defence Institute - BDI - Iskar-Sofia). Il représente la Bulgarie comme membre du « Science & Technology Board » (STB) de l'OTAN, et préside le panel « Information Systems Technology » (IST) de la « Science & Technology Organization » (STO) de l'OTAN.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
		ISBN 978-98-837-2368-4	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Cognitive Warfare : La guerre cognitique

7. Presented at/Sponsored by

Première réunion scientifique Cognitive Warfare Bordeaux (FR) – 21 juin 2021. Journée organisée par l'Innovation Hub de NATO-ACT et l'ENSC, avec le soutien de l'État-Major des Armées (FR – Major Général), du NATO-CSO et de la Région Nouvelle Aquitaine.

8. Author(s)/Editor(s)	9. Date
B. Claverie, B. Prébot, F. Du Cluzel.	October 2021
10. Author's/Editor's Address	**11. Pages**
Multiple	116

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Biais cognitifs; Cognition; Cognitive warfare; Cyberpsychologie; Domaine cognitive; Guerre cognitique; Humain

14. Abstract

Cet ouvrage publié par le CSO de l'OTAN réunit des articles reprenant les principales interventions de la première réunion Cognitive Warfare tenue à Bordeaux en juin 2021 à l'initiative de l'Innovation Hub du Commandement pour la Transformation de l'OTAN et de l'École Nationale Supérieure de Cognitique avec la collaboration de l'État-major des armées françaises, du CSO et de l'ACT de l'OTAN, et de la Région Nouvelle Aquitaine. Cette première initiative fait un point sur la cognition humaine, sa force et ses faiblesses, son organisation collaborative pour la décision militaire, ses rapport et dépendance à la technologie numérique et ses dimensions sociales et politiques notamment dans la dure compétition internationale. Elle donne la parole au Major général des armées et au Commandeur pour la transformation de l'OTAN, et sévira de point de départ à une suite de rencontres d'approfondissement, à l'initiative du CSO et de l'ACT.

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document
Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and
Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-98-837-2368-4