COGNITIVE WARFARE

First NATO scientific meeting on Cognitive Warfare
Bordeaux (France) – 21 June 2021

Scientific Editors: B. CLAVERIE, B. PRÉBOT, N. BUCHLER & F. DU CLUZEL.

First NATO scientific meeting on Cognitive Warfare (France) – 21 June 2021. Symposium organized by the Innovation Hub of NATO-ACT and ENSC, with the support of the French Armed Forces Deputy Chief of Defence, the NATO Science and Technology Organization / Collaboration Support Office, and the Region Nouvelle Aquitaine.

Published by the Collaboration Support Office - Neuilly (France) © 2022

NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

www.sto.nato.int

Cognitive Warfare:
The Future of Cognitive Dominance

First NATO scientific meeting on Cognitive Warfare (France) – 21 June 2021.
Symposium organized by the Innovation Hub of NATO-ACT and ENSC,
with the support of the French Armed Forces Deputy Chief of Defence,
the NATO Science and Technology Organization / Collaboration
Support Office, and the Region Nouvelle Aquitaine.

Scientific Editors
B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel.

Published by the NATO-STO Collaboration Support Office, with the support of the NATO-ACT Innovation Hub, Bordeaux ENSC, the French Armed Forces Joint Staff and the Region Nouvelle Aquitaine.

Published March 2022

ISBN 978-92-837-2392-9

Table of Contents

List of Figures

List of Tables

Foreword – By the Deputy Director of the NATO Collaboration Support Office (CSO)

Major General Philippe Montocchio[1]

"Influence not only what targeted individuals think, but also the way they think, and ultimately, the way they act."

There has been a spectacular evolution – in fact, a revolution – in the field of Information Technologies over the past twenty years. The home family computer, tablet, a smart phone for everyone, the globalization of the Internet network, social media becoming more and more the mode of communication and information of first choice, the first use of virtual reality and many other technological evolutions in the realm of information are shaping the way individuals and communities are exchanging information and communicating.

More globally, tomorrow's world will be characterized by some major trends that are going to define how states will interact with each other and the ways they are going to manage future conflicts. Confrontations between major powers, involving defence and security international organizations, such as NATO, will be impacted by economies' interdependence, societies' hyper-connectivity, the digitalization of our environment, the exponential increase of data, and the fragmentation of the world in communities of interest (social, religious, ethnical, political, etc.).

These major trends, associated with nuclear deterrence, will remain relevant, will reduce the occurrence probability of devastating direct military confrontations between major powers. However, as wars of influence will persist, the major powers and alliances of nations will have to find different battlefields to "continue War with the admixture of other means," to adapt Clausewitz's famous quote about War and Politics. Using so-called "hybrid" courses of action will become much more regular, if not permanent, totally blurring the limits between peacetime and crisis periods.

Among these hybrid means, Communication and Information Warfare has often been perceived and treated as a secondary sub-function in the planning of crisis management operations, which, in general, relies on the use of traditional military capabilities. In this emerging world, Information Warfare, and Cognitive Warfare, the subjects of this scientific meeting, are likely to become permanent action modes, self-sufficient to reach, in the long-term, the desired end state: destabilization of a political leader, a military commander, an entire staff, a population, or an Alliance…

Cognitive Warfare is the most advanced form of human mental manipulation, to date, permitting influence over individual or collective behavior, with the goal of obtaining a tactical or strategic advantage. In this domain of action, the human brain becomes the battlefield. The pursued objective is to influence not only what the targets think, but also the way they think and, ultimately, the way they act. Cognitive Warfare is necessarily associated with other modes and domains of action for reaching targeted brains, such as Cyber Warfare and Information Warfare. As a concept, Cognitive Warfare also includes another crucial domain that is fast evolving: the cognitive neurosciences. By facilitating the understanding of the brain cognitive mechanisms,

[1] Gen. Philippe Montocchio is a French Air Force Major General (ret). He graduated from the French Air Force Academy and was a fighter pilot in the first part of his military career. General Montocchio then took over positions of command, in particular being the General Officer commanding the French Forces stationed in Djibouti (2014 – 2016), before becoming the Director for International Relations in the French Armed Forces Joint Staff. He is currently the Deputy Director of the NATO Collaboration Support Office in charge of supporting the S&T cooperation between NATO Nations.

i.e., the way the brain processes the different categories of information, the neurosciences will allow optimization of the use of other forms of Warfare, notably Information Warfare.

NATO's collective awareness of the increasing importance of this form of conflict is happening progressively. In 2016, on the occasion of the Warsaw NATO Summit, the cyber domain was recognized as an operational domain, and hybrid warfare stakes were underlined in the Summit communiqué, but only through the limiting prism of cyber courses of action and special operations. The recent NATO Summit, which took place in Brussels on 14 June 2021, represented a true turning point. For the first time, China and Russia were mentioned, with emphasis, in the Summit communiqué for their disinformation activities, demonstrating the growing concern Allied Nations had for these new hybrid challenges.

Against these two potential adversaries, NATO is already facing difficulties, the first being to have to collectively act, react, and coordinate as an Alliance of thirty Nations with significant military and technological differences amongst themselves. A second challenge is the lack of collective capabilities to detect and characterize hostile hybrid activities, in particular in the information and cognitive domains. In the same vein, identifying the perpetrators of a hybrid aggression, and agreeing on the appropriate answer might prove to be very difficult, threatening the Alliance's credibility if the Allies fail to deliver the adequate response to the malicious action. Ethical questions will also be raised. If disinformation and destabilization are acceptable courses of action for dictatorial countries, could they officially and openly be part of the Alliance's inventory of possible responses to aggressions? One last important difficulty for NATO: how to collectively address attacks on NATO Nations' particular interests? Hostile hybrid operations can target Alliance capabilities, leadership, or decision-making systems, but they usually target allied Nations' strategic interests, such as critical infrastructures and services, populations, political leaders, etc. Collectively dealing with aggressions aiming at some national interests might prove to be complex.

In close coordination and complementarity with the NATO Allied Command Transformation (ACT), the NATO Science and Technology Organization (STO) conducts studies on technologies that should allow NATO to keep the technological edge against its potential adversaries. The STO is a strong network of 6,000 scientists from Allied and some Partner Nations, in particular Australia, Finland, Japan, and Sweden. The STO covers the full spectrum of sciences and technologies related to security and defence which are broken down into seven main research domains. These seven scientific domains are explored by different Panels and one Group, of which four are, or might become, involved in the study on Cognitive Warfare: the Human Factors and Medicine (HFM) Panel, the Information Systems Technology (IST) Panel, the System Analysis and Studies (SAS) Panel and the NATO Modelling and Simulation Group (NMSG).

The symposium on Cognitive Warfare, organized on 21 June 2021 by the NATO-ACT Innovation Hub and the *Ecole Nationale Supérieure de Cognitique* (ENSC) in Bordeaux, France, with the support of the French Armed Forces Joint Staff, the STO and *Région Nouvelle Aquitaine*, was the scene of many fruitful discussions and presentations, reflected in the excellent articles assembled in this report.

Preface – By the Supreme Allied Commander Transformation

General André Lanata[2]

Exploiting the flaws of human nature to better target the minds of individuals is not a new idea. The maneuver of influence and deception has always been part of the art of war. Sun Tzu already underlined the importance of the psychological factor in his time, and if the Roman Empire first relied on the strength of its army, it owed its longevity to its persistent will to impose its culture and thus its own vision of the world. Today, the technological progress made in the informational field and the hyper-connectivity in which we live, made possible by the digitization of information, multiply the possibilities of manipulating an individual or targeting a group of people. The recent explosion of psychological manipulation processes for the purpose of swindling through social engineering clearly shows that knowledge of human behavior and the ability to influence it are now at the heart of a new strategic issue. This battle of perceptions affects all sectors of society and in particular the security and defence sectors.

NATO is constantly monitoring emerging threats and has quickly become interested in this subject. The Allied Command for Transformation, located in Norfolk (USA), responsible for the preparation and development of future Alliance capabilities, has recently worked on a study called "Cognitive Warfare," which aims to shed light on and anticipate the militarization of technologies that are grouped under the acronym NBIC (Nanotechnology, Biotechnology, Information Technology and Cognitive Science).

This is why I welcome the holding of this first scientific meeting, which took place on June 21 in Bordeaux on the theme of Cognitive Warfare. This theme seems to me to be quite remarkable and I sincerely thank the École Nationale Supérieure de Cognitique, with which my command has had a fruitful cooperation for many years, for having hosted and organized this first meeting with our Innovation Hub. I also salute the participation of the eminent international experts who responded to our invitation and contributed to the success of this day. The richness of the exchanges in French and English, the presentations, the round tables, and the practical demonstrations at the ENSC testify to the great vitality of the research and development in Cognitive Warfare available to the Allies. It is up to NATO's Allied Command Transformation to continue to federate energies to maintain and develop this dynamic, in the service of stability, conflict prevention and security of the one billion citizens of the Atlantic Alliance.

[2] Gen. André Lanata is an Air-Force General (ret.). He was a French fighter pilot and served as Chief of the French Air Force (CEMAA 2015 – 2018), then as NATO Supreme Allied Commander Transformation – Norfolk (ACT 2018 – 2021).

Acknowledgements

This book owes a great deal to the authors whose articles appear between the covers, without forgetting all the other participants in the “Cognitive Warfare” scientific meeting held on June 21, 2021. The diversity of the contributions, from cognitive psychology to international strategy, makes the book provocative and useful for the future of NATO’s ACT and STO thinking.

We owe a thank-you to all the academic or military institutions, laboratories and companies that took part in this meeting, and that contributed to the richness of these intellectual exchanges on Cognitive Warfare.

Production of the book was made possible by the team of four scientific editors and the staff of NATO’s CSO. The meeting itself was made possible thanks to the support of the Innovation Hub NATO-ACT, of the French Armed Forces Deputy Chief of Defence, of ENSC Bordeaux INP, and of Nouvelle Aquitaine Regional Council. Special thanks are extended to Philippe Montocchio, deputy director of CSO, for his patience and dedication to the cause of scientific thinking within STO, and to André Lanata, Supreme Allied Commander Transformation for his commitment to promoting reflection on Cognitive Warfare as a field of major importance for future conflicts and for the security of nations.

Cognitive Warfare
First NATO Science Meeting[3]
Bordeaux – June 21, 2021

"Cognitive Warfare" is the convergence of "Cyber-Psychology," "Weaponization of Neurosciences," and "Cyber-Influence" for a provoked alteration of the perception of the world and its rational analysis in the military, politicians, and other actors and decision makers, for the purpose of altering their decision or action, for a strategic superiority at all levels of tactical intervention concerning individual or collective natural intelligence, as well as artificial or augmented intelligence in hybrid systems.

The first NATO scientific meeting on "Cognitive Warfare" was held in Bordeaux (France) on 21 June 2021 at the initiative of the ACT's Innovation Hub (NATO Allied Command Transformation – Norfolk, USA) and the ENSC (French national institute on Cognitics – École Nationale Supérieure de Cognitique – Bordeaux INP France), in the presence of academic scientists, military and industrial stakeholders, representatives of the Innovation Hub, the Deputy Director of the Collaboration Support Office (NATO Science and Technology Organization – Neuilly France) and the French Armed Forces Deputy Chief of Defence (General Staff – Paris France).

This book contains the main papers that were given during the meeting, and those whose texts were provided at the beginning of the session to enrich and facilitate the debates.

It is published by the Collaboration Support Office (CSO) of the Science and Technology Organization (STO) of the North Atlantic Treaty Organization (NATO).

Organization Committee

- Baptiste Prébot PhD, Research Associate – DDM Lab – Carnegie Mellon Univ.
- Bernard Claverie PhD, University professor, honorary director of ENSC – ADER French Air Force.
- Norbou Buchler PhD, U.S. Army Combat Capabilities Development Command Analysis Center.
- François Du Cluzel, Innovative projects manager – Innovation Hub – ACT-NATO.

[3] The "Cognitive Warfare" theme was developed by the Innovation Hub of NATO-ACT (Norfolk) in the framework of the collaboration agreement associating ENSC (Ecole Nationale Supérieure de Cognitique – Bordeaux INP – FR) and ACT, signed on 15 June 2017 under the title "Letter of Agreement to collaborate between Ecole Nationale Superieure de Cognitique and Headquarters, Allied Command Transformation" and under the aegis of General (French Air Force) André Lanata (SACT 2017 – 2021). The collaboration was initiated in 2013 by General (French Air Force) Denis Mercier (SACT 2013 – 2017) and Professor Bernard Claverie (Director of the ENSC 2009 – 2019) on the theme "Cyberpsychology" and then "Weaponization of Neurosciences."

Scientific Program
Bordeaux, France, 21 June 2021

09.30	Welcome
10h00	**Greetings from the Director of ENSC**
	Pr. Benoît LE BLANC
10h10	**Opening Conference**
	Pr. Bernard CLAVERIE, Director Emeritus at ENSC
10h40	**Keynote** (in French): "Cognitive," a Sixth Domain of Operation?
	Hervé Le Guyader – Deputy for ENSC-STO relationship – member of the IST Panel – NATO-STO
11h00	**Keynote** (in French): "Cognitive Warfare" NATO Perspectives
	François Du Cluzel – Innovation Hub – NATO-ACT
11h10	**Round Table Discussion** Future of "Cognitive Warfare" – Global Threats, Industrial Responses
	Moderator: François Du Cluzel – Innovation Hub – NATO-ACT – Norfolk (VA, USA)
	Lt Gen (ret.) Gilles Desclaux – Former French Air Operations com. – ENSC Defence Advisor
	Thierry Lemoine – "La Ruche" Research Unit Director – THALES
	Marc Rodier PhD – IBM distinguished engineer – Cognitive Sciences and Technologies chair
	Patrice Lefeu – EY associated partner – Global R&D and Innovation service
	Show room at the ENSC Defence Lab
14h00	Thematic introduction: Narratives Overwhelm the World
	Pr. Michael Wunder – Fraunhofer Institute for Communication, Information Processing and Ergonomics – Germany – Member of the NATO-STO IST Panel (by VTC)
14h20	**Conference/Discussion**: Challenges of the Cognitive Domain for France and its Role in NATO
	Gen Eric Autellet – Deputy Chief of Defence – France
15h00	**Round table discussion**: "Cognitive Warfare" – Scientific Perspectives
	Moderator: Lt Gen (ret.) Jean-Marc Laurent – Chairman "Defence & Aerospace" – Bordeaux
	Pr. Benoît Le Blanc – ENSC Director, President of the AFIA (French AI Scientific Association)
	Maj Gen (ret.) Philippe Montocchio – Deputy Director of the Collaboration Support Office (CSO) – NATO Science and Technology Organization (STO)
	Pr. Tanguy Struye De Swielande PhD – Director Center for the Study of Crises and International Conflicts (CECRI) – Catholic University of Louvain – Louvain-la-Neuve
	Célestin Sédogbo PhD – Director of the "Carnot Cognition" Institute – Director of CNRS UAR2203
	Philippe Mouttou PhD – Deputy head of advanced studies – Thales Research and Technology
16h30	**Final Conference**: Technological Maturity of "Cognitive" Human Networked Systems
	Dr. Norbou Buchler – Army DEVCOM Data & Analysis Center (Aberdeen Proving Ground – MD-USA) (by VTC)
17h00	Preparation for next meeting

Participants: Agencies, Companies, and Organizations Represented[4]

Aerospatial and Defence Chair – Institute of Political Science of Bordeaux – FR
Air Force Command (CFA) – French Air Force – Mérignac – FR
C2 & Intelligence Department – Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE – Wachtberg – DE
Carnot Cognition Institute – CNRS UAR 2203 – Talence – FR
Centre for International Crisis and Conflict Studies (CECRI) – UC Louvain – Université Catholique de Louvain – Louvain-La-Neuve – BE
Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE) – Paris – FR
Collaboration Support Office (CSO) NATO Science and Technology Organization – Neuilly – FR
Combat Capabilities Development Command Data & Analysis Center (DEVCOM) – Aberdeen Proving Ground (MD) – USA
Direction of the Medical Information – Military Health Service – HIA Begin – Saint-Mandé – FR
École Nationale Supérieure de Cognitique – ENSC Bordeaux INP – FR
EY – Paris La Défense – FR
French General Staff of the Armed Forces – Ministry of Defence – Paris – FR
French Institute of International Relations – Paris – FR
General Directorate for International Relations and Strategy (DGRIS) – French Ministry of Defence – Paris – FR
Human Engineering for Aerospace Lab. (HEAL) – Thales-ENSC – Talence – FR
IBM – Bois-Colombes – FR
Integration from Composent unit to System – Cognitics dept. – MS UMR CNRS 5218 – Talence – FR
Innovation Hub – NATO-ACT – Norfolk (VA) – USA

[4] List of institutions and companies to which the participants belong.

Nouvelle Aquitaine Council – Bordeaux/Limoges/Poitiers – FR
Panel Information Systemes Technology (IST) NATO-STO – Neuilly – FR
RACAM (Rencontre Aviation Civile – Aviation Militaire) – Paris – FR
Research Center of Saint-Cyr Coëtquidan Army Academy (CREC) – Saint-Cyr – FR
SIREN – Galway – IO
SW Directorate of Internal Security – French Ministry of Internal Security – Bordeaux – FR
Thales “La Ruche” Research Center – Thales LAS – Rennes – FR
Thales Avionics – Mérignac – FR
Thales Land-Air Systemes – Massy – FR
Thales Raytheon Systems – Massy – FR
Thales Research and Technologies – TRT – Palaiseau – FR
Think Deep – Talence – FR

Cognitive Warfare

Summary

Cognitive warfare is waged on the battlefield of the human mind. Tactical or strategic objectives are achieved by pursuing warfare by other means. This method of warfare directly exploits advances in digital technology, applied both at individual and networked levels, to manipulate the psychological, social and information environment. This shapes not only what people think individually and group-think as social networks, but also influences how they collectively act and interact. Launched by a sophisticated adversary, cognitive warfare manipulates individual and group representations or beliefs with the desired effect of amplifying targeted behaviors and actions that favor the adversary. Pursued to the fullest, cognitive warfare has the potential to destabilize societies, military organizations, and fracture alliances.

Cognitive warfare is achieved by integrating cyber, information, psychological, and social engineering capabilities. Exploiting information technology, it seeks to create confusion, false representations, and uncertainty with a deluge of information over-abundance or misinformation. This is achieved by focusing attention on false targets, by causing distraction, by introducing false narratives, radicalizing individuals, and amplifying social polarization to muster the cognitive effects needed to achieve short-term and long-term objectives.

The susceptibility to Cognitive Warfare raises many questions and concerns for the Alliance. How to guard against such attacks? This requires understanding what makes certain individuals or groups more or less susceptible to targeted cognitive manipulation. New capabilities are needed to combat the rise of networked automations (i.e., botnets) that distort and manipulate the information sphere. How to detect it? Such a broad attack surface requires new alert signals to be correlated across the social-information-cyber network to detect such attacks. How to attribute such attacks to a particular adversary is challenging. Ultimately, cognitive warfare forces us to understand human cognition and collective social action. How do we arrive at our conclusions and, for example, process semantic uncertainty, provoked illusion, perceptual distortion, attention saturation, learning disorders, cognitive bias, working memory or long-term memories? But cognition is also collaborative and purposive in our social systems with shared decision making, and especially democracies. How is shared understanding achieved, especially in social networks, and why is it particularly fragile and susceptible to manipulation? Whether individual or collective, cognition corresponds to all of the processes that are mobilized to fashion our understanding of the world, make decisions, and act upon it.

We articulate our modern world as replete with human thought and machines, expressing or expressed circulation of thoughts and programs. The cohabitation of natural intelligence and artificial intelligence is at the center of this debate that forces us to conceive of war as hybrid, with our thoughts and societies increasingly shaped by machines. Cognitive warfare is already here and the main chapters are already being written by the increasing convergence of people, information, and technology across our social networks. The trend lines include technological interfaces that facilitate human-system integration, novel capabilities to augment human decision making, increasing automation with system controls of human error (i.e., driving), and artificial intelligence outstripping programs' limitations, autonomy of the assisted digital actors or of machines enriched by human thought.

Ultimately, we must face ourselves and the ambiguity of human cognition and social action. Cognition is poorly known, and yet it claims a form of naive expertise. Everyone tends to think of controlling it and feeling protected. Awareness comes often too late; it is highly necessary to try to anticipate cognitive attacks in order to guard against them.

This book published by CSO brings together articles on the main interventions of the first “Cognitive Warfare” meeting held in Bordeaux in June 2021. This first initiative focuses on human cognition, its strength and weaknesses, its collaborative organization for the military decision, its reporting and dependence on digital technology and its social and political dimensions. The initiative serves as a starting point for subsequent in-depth meetings, at the initiative of CSO and ACT while inviting Scientists of the different Nations of the Alliance to contribute to the advance of science of Cognitive Warfare.

This initiative is supported by STO – Information Systems Technology Panel and ACT – Innovation Hub.

Texts collected and edited by Bernard Claverie, ENSC Bordeaux INP, Baptiste Prébot, DDM Carnegie Mellon University, Norbou Buchler, US Army DEVCOM Analysis Center, Aberdeen Proving Ground, François du Cluzel, Innovation Hub NATO-ACT Norfolk.

Chapter 1 – COGNITIVE WARFARE – CONTRIBUTION OF THE FRENCH ARMED FORCES DEPUTY CHIEF OF DEFENCE

General Eric Autellet[1]

"The Human Brain is the Battlefield of the 21st Century."
James Giordano (2018).

If we take the neuroscientist James Giordano's quote literally, then the cognitive field must be one of our priorities, in terms of research but also for the conduct of our operations.

The intensification of rivalries between powers translates, along a continuum of "contestation – competition – confrontation," into actions in the "grey zones" aimed at intimidating or coercing. We must not wait for the confrontation phase to act, particularly in the field of perceptions, especially since lethal and kinetic action is not always the most appropriate response.

In this perspective, EMA must take ownership of this subject and accompany the reflections underway at NATO, in order to feed the debate, notably upstream of the work on the future strategic concept. It must also integrate it into the European agenda in order to raise awareness among European nations and encourage them to invest in a field that will become essential for coalition work and our interoperability.

The work carried out by ENSC in this field and the organization of this scientific and strategic workshop identified the stakes and the threats linked to the cognitive domain and galvanized our thinking, and today contributes actively to our reflection. Beyond scientific and biotechnological developments, the exchanges have shown that the cognitive field covers a vast spectrum, including human sciences such as psychology and sociology.

Actions of influence, soft and smart power, actions of disinformation and destabilization are becoming essential components of the strategies of conquest and domination between countries, organizations and non-state actors in international relations: an intentional blurring of reference points and borders, indifferent to reality, tends to take hold.

Influencing and manipulating public opinion are full-fledged modes of action for powers aiming to destabilize our democracies. The current destabilization context is one of "post truth," of questioning knowledge, institutions and governments, of knowledge and of the scientific approach, where the fact counts for less than the emotion and the lies of those who utter them. These powers (state or not) rely on technology that provides them with powerful levers of dissemination and intrusion that can target each individual, while giving them the ability to influence and manipulate public opinion on a large scale without their knowledge. "Fake news," rumors, mystification, and conspiracy are very concrete examples, whose diffusion is multiplied by social networks.

The reference to Clausewitz's triangle of "people, politics, military" allows us to identify the place of the military in a theme that at first glance seems to concern only the civilian domain. The field of information manipulation from a military perspective is in fact nothing new in itself. The weapon of information is an old legacy of the Cold War (one could go back to the world conflicts of the beginning of the 20th century) and since the 1960s – 70s, the vision of the field of perceptions has been part of the doctrinal field of the main armed forces.

[1] Gen. Eric Autellet is an Air-Force General. He is currently the French Armed Forces Deputy Chief of Defence. He was a fighter pilot and was the Director of the French Air Force Academy (Ecole de l' Air) in Salon-de-Provence from 2016 to 2018. Promoted to the rank of Major General, he was appointed Deputy Chief of the Air Force in April 2020 before taking the rank of General and the responsibility of Deputy Chief of Defence in March 2021 in Paris, France.

Since Vietnam, despite military successes, our wars have been lost, in particular because of the weakness of our narrative (i.e., 'win hearts and minds'), both with regard to local populations in theaters of operation, and with regard to our own populations.

Our stakes are twofold when it comes to our action vis-à-vis an enemy or a friend, and we can define passive and active modes of action for both, taking into account the limits and constraints of our model of freedom and democracy. With regard to our enemy, we must be able to "read" the brain of our adversaries in order to anticipate their reactions. If necessary, we must be able to "penetrate" the brains of our adversaries in order to influence them and make them act according to our wishes. As far as our friend is concerned (as well as ourselves), we must be able to protect our brains as well as to improve our cognitive capabilities of comprehension and decision-making capacities. These issues are inseparable from the digital transformation process that will have a decisive impact on our command structures.

Although the concept of Cognitive Warfare has yet to be defined, I believe it is essential to pursue the process of deepening the subject, raising awareness and education, identifying the technological and cyber challenges and the issues of operational readiness, which we will be confronted with as a result.

The Joint Chiefs of Staff are already participating in the work carried out within ACT on this subject. This day, organized by the Ecole Nationale Supérieure de Cognitique, was the beginning of a collaboration that can only be strengthened between the EMA and the ENSC, and which could result in the organization of training modules within our schools, for the benefit of active and reserve personnel, and in the accompaniment and support of our internal strategic, conceptual and doctrinal work.

Chapter 2 – "COGNITIVE WARFARE": THE ADVENT OF THE CONCEPT OF "COGNITICS" IN THE FIELD OF WARFARE

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

"Cognitive warfare is now with us. The main challenge is that it is essentially invisible; all you see is its impact, and by then … it is often too late."

Cognitive warfare is now seen as its own domain in modern warfare. Alongside the four military domains defined by their environment (land, maritime, air and space) and the cyber domain that connects them all, recent events upsetting the geopolitical balance of power have shown how this new warfare domain has emerged and been put to use.

It operates on a global stage since humankind as a whole is now digitally connected. It uses information technology and the tools, machines, networks, and systems that come with it. Its target is clear: our individual intelligences, to be considered both individually and as a group.

Attacks are defined, structured, and organized to alter or mislead the thoughts of leaders and operators, of members of entire social or professional classes, of the men and women in an army, or on a larger scale, of an entire population in a given region, country or group of countries. It can have a variety of objectives and will adapt itself to the strategy being used: territorial conquest (a bordering region, peninsula, or group of islands for instance), influence (elections, stirring up popular unrest), service interruptions (national or local administrations, hospitals, emergency services, and sanitation, water, or energy supplies) or transportation (airspaces, maritime chokepoints…), information theft (through involuntary disclosure or the sharing of passwords…) etc.

Cognitive warfare is the art of using technology to alter the cognition of human targets, who are often unaware of any such attempt, as are those entrusted with countering, minimizing, or managing its results, whose reaction is too slow or inadequate.

2.1 A FEW DEFINITIONS

Cognitive warfare is thus an unconventional form of warfare that uses cyber tools to alter enemy cognitive processes, exploit mental biases or reflexive thinking, and provoke thought distortions, influence decision making and hinder action, with negative effects, both at the individual and collective levels.

This is obviously related to the concept of cyber warfare that uses digital information tools to gain control, alter or destroy said tools. However, cognitive warfare goes beyond information to target what individual brains will do with this information. It therefore extends beyond the human consequences of cyber warfare involving computer engineering, robotics, and programs; a cognitive effect is not a by-product of action, but its very objective.

This objective is independent of the technologies used to achieve it. One way of thinking about it is as a "psychological-social-technical warfare" on the one hand and of a form of "influence warfare" on the other,

[1] Pr. Bernard Claverie is University Professor, Honorary Director and Founder of ENSC (Ecole Nationale Supérieure de Cognitique – Bordeaux National Polytechnical Institute) and a researcher affiliated with the CNRS (Centre National de Recherche Scientifique – UMR5218 – Bordeaux University FR).

[2] François du Cluzel is Lieutenant Colonel (ret.) of the French Army and is currently Head of Innovative Projects within Allied Command Transformation Innovation Hub in Norfolk (Virginia, USA).

using cyber means. In the military context specifically, it involves the use of a strategy intended to carry out a combat, surveillance, or security action.

Other definitions exist for related concepts. “Cognitive Combat” is related to the actual, local, and temporary use of tactical tools to affect cognition. This action occurs within a larger strategy designed to engage cognitive targets. For offensive actions, it is characterized by an approach centered on harassment, the systematic exploitation of weaknesses, whereas in a defensive posture it involves the development of resilient and preventative capabilities using similar tools. The notion of “Cognitive Conflict” could be used when the contact is generalized and the confrontation of cognitive processes is the rule. But that notion is still to be theorized.

2.2 COGNITIVE WARFARE IS ALL AROUND US

Cognitive Warfare is already being used, with more or less success and not necessarily under that name, by a number of state and non-state players, institutions or companies, including terrorist organizations, aggressive religious movements, etc. They include specialized and highly-competent units working for digital intelligence services, as well as industry agencies and companies engaged in competition with others or in the more routine area of marketing and manipulation of potential clients. In all these cases, the object is to dominate, establish one’s superiority, or even conquer and destroy. Today these practices have reached such a level that political leaders can no longer ignore their importance.

The term Cognitive Warfare has been used with that meaning in the United States since 2017 (Underwood, 2017) to describe in particular the modes of action available to a state or influence group seeking to “manipulate an enemy or its citizenry’s cognition mechanisms in order to weaken, penetrate, influence or even subjugate or destroy it.” While that broad mission has always formed a part of the art of war, here we have a new discipline that requires further elucidation. It is the combination of the newer cyber techniques associated with information warfare and the human components of soft power, along with the manipulation aspects of PSYOPS. They usually involve a biased presentation of a reality, usually digitally altered, intended to favor one’s own interests. New communication tools now offer infinite possibilities, opening the way to new methods and new objectives. This increased complexity should encourage potential victims to develop a constant posture of resilience, even if in most cases, victims usually realize they were attacked too late.

This approach to Cognitive Warfare has caught the eye of armed forces across the world and includes both strategic and operational aspects, some of which are more developed than others. It currently is not covered by established ethical considerations and doctrines. It expanded considerably with the arrival of digital strategic decision-making assistants, new operational domains and the invasion of big data and analytics, in the realm of information, wargaming and the conduct of operations. It is now spreading to all areas where digital information is used, including the quiet implementation of offensive and defensive uses, cognitive attrition, and defence measures intended to protect likely target populations. It is a mix of well-thought out attack processes as well as counter and preventative measures.

2.3 THEORIZATION

New theories are being developed, including those dealing with resilience or the weaknesses of neurosciences, the exploitation of cognitive biases and the likelihood of cognitive errors, the manipulation of perceptions, how our attention spans can be overwhelmed or steered, and cognitive stress induced. All of these have predictable consequences on our mental acuity, social relations, and motivations and on the efficiency of organizations.

These early conceptual efforts caught the attention of many researchers and military thinkers. Including, among many others, neuro-ethicist James Giordano[3] who has described the brain as the site for the battlefields of the 21st century and studied the weaponization of neurosciences, General Goldfein[4] has stated that we have moved on to wars of attrition to wars of cognition, Colonel Banach[5] has talked about the idea of virtual warfare, while Lieutenant General Stewart[6] of the Defense Intelligence Agency, saw modern warfare as a cognitive battleground and General Desclaux[7] described the command and control strategic process as a cognitive triangle involving knowledge dominance, cyber confidence and decision superiority, all of which serving to guide strategy to achieve the commander's objectives. As the cognitive aspects of the planning and conduct of is operations is becoming increasingly vital, Colonel Remanjon of NATO's Allied Command Transformation has studied whether the human brain is now the ultimate battlefield?

And the theoretical underpinnings of the sixth domain of warfare have recently been developed, linking the technium to the noosphere[8] seen as the global representation of human intelligence as mediated through technologies, in a recent book on Cognitive Superiority by Dean S. Hartley[9] and Kenneth Jobson[10] (2021).

2.4 BASIC PRINCIPLES

Cognitive Warfare is where all the elements of information warfare – including the operational aspects of psychology and neurosciences, based on systemics and complexity – combine for military action. It sits at the intersection of two operational fields that hitherto were managed separately: PSYOPS and influence operations (soft power) on the one hand, and cyber operations (cyber defence) intended to degrade or destroy physical information assets on the other. This intersection makes it possible to unite concepts and points of views from different scientific, military or intelligence communities of interest, bringing about an interdisciplinary approach to how technologies impact humankind.

The main goal is not to serve as an adjunct to strategy or to defeat without a fight, but to wage a war on what an enemy community thinks, loves or believes in, by altering its representation of reality. It is a war on how the enemy thinks, how its minds work, how it sees the world and develops its conceptual thinking. The effects sought are an alteration of world views, and thereby affect their peace of mind, certainties, competitiveness, and prosperity.

The stated objective is to attack, exploit, degrade or even destroy how someone builds their own reality, their mental self-confidence, their trust in processes and the approaches required for the efficient functioning of groups, societies or even nations. Although its technical aspects (cyber) are somewhat different, it is a companion to Psychological Operations (PSYOPS).

3 Pr. James Giordano is a professor in the Georgetown Department of Neurology in Washington D.C. and the Director of the Neuroethics Studies Program at the O'Neill-Pellegrino Center for Clinical Bioethics.

4 David Goldfein was a former general and Chief of Staff of the US Air Force, member of the Joint Staff and a military advisor in the Council of National Security and to the Secretary of Defense and President of the United States.

5 Steve Banach is a colonel in the US Army and former director of the School of Advanced Military Studies (SAMS) at Leavenworth (Kansas, USA).

6 Vincent R. Stewart is a former Lieutenant General of the Marine Corps and Director of the Defense Intelligence Agency (DIA).

7 Gilles Desclaux is a retired French Air Force Lieutenant General. He commanded air operations during the war in Libya and is now a frequent contributor to C2 work being conducted in industry.

8 As defined by Kelly (2011): all the information available to human brains.

9 Dean S. Hartley III Director of Hartley Consulting at Oak Ridge (TN, USA) and honorary president of a number of other consulting firms.

10 Kenneth O. Jobson is a psychiatrist and the creator of the International Psychopharmacology Algorithm and is particularly active in biotechnologies.

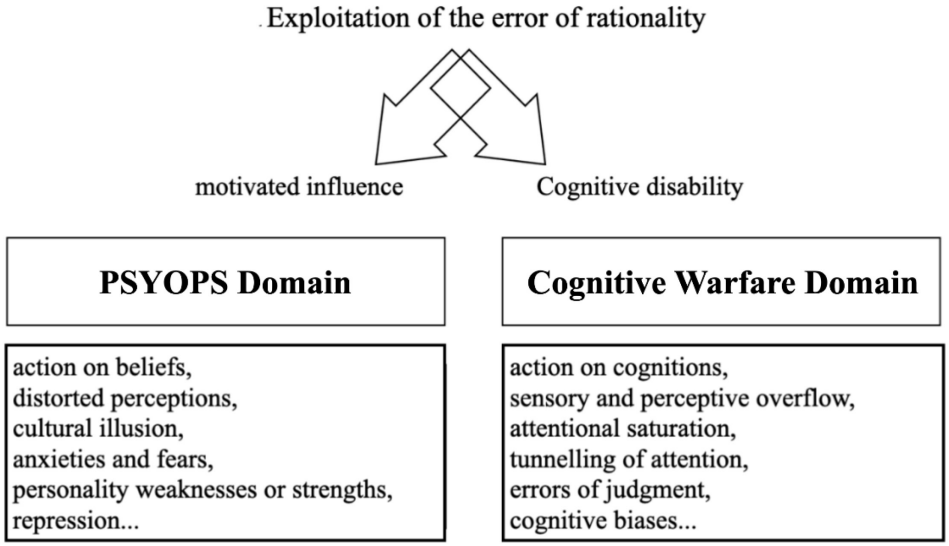


Figure 2-1: Differences Between Cognitive Warfare and PSYOPS (Including, in Broad Terms Actual Psychological Operations and Other Non-Kinetic Actions such as Influence Operations and Civil-Military Cooperation (CiMiC)).

2.5 LEVELS OF ACTION

Cognitive Warfare can be studied from two points of view: a global one and one based on the available tools. The first is intended to contribute to a culture which seeks to manipulate minds or, at the other end of the spectrum, to build up resilience and global security. It is both intended to inform and train those most likely to be targeted by ill-intentioned actions or intentions and uses cognitive tools to counter such actions.

The domain is based both on a knowledge of the psychology of players involved, of the sociology of specific populations or groups, and the influence of culture on the decision making and rationality of various players. The second level is related more specifically to various fields of cognition, including for instance the decision/indecision dichotomy, cognitive errors and biases, perceptions and illusions, cybernetics and the absence or loss of control, influence and soft power, psychology and cyber psychology, interactions between users and systems, robotics and drones, autonomy and the ethics associated with new technologies, motivation and loss thereof (giving up and despair), morality and the clash of values, psychology and religion, the urgency of psychiatric support in cases of post traumatic care or after someone has snapped, cybersecurity and human reliability, and the cognitive aspects of C2, which involve a considerable number of other considerations, including multi-domain and multi-cultural aspects.

2.6 A DEFENSIVE POSTURE

This kind of cognitive approach cannot be defined along the traditional categories of instruments of war, but rather as a tool for interfering with individual or massed targets, seeking to achieve effects at various scales, from the single person all the way to an entire social/technical system. These capabilities and effects can be used before, during and after kinetic actions, while remaining outside current international definitions of what constitutes an act of war. These non-kinetic actions will allow imbalances that will benefit their creators and hinder those targeted. But now they may become part and parcel of a global, discreet, or even invisible action, or specific, precise, and undetectable actions, or as only components of one or several aggressive operations, all of which requires we learn the dangers posed and how to develop defensive techniques and effective deterrent options or ways of dealing with the consequences.

2.7 MOVING TOWARDS A HUMAN DOMAIN

What are the consequences? The information era has morphed into a network era since the world is increasingly defined by its interconnections. This evolution has grown more complex as our physical, digital, and mental personas have merged within these human enhancement networks. They are typical of the human domain, where the ability to solve complex problems is dependent on how information is represented, understood, and developed. This domain must take into account the strengths, limitations, vulnerabilities, and diversity of those involved in decision making or when applying rules and procedures.

From a defensive point of view, the challenges are many: they involve ensuring the cognitive security of individuals, facilitating the efficient running of state structures, and establishing and maintaining cognitive superiority for decisive action. Further challenges relate to improving competitiveness, developing and certifying the performance of intelligent systems or artificial intelligence systems intended to augment human labor, improving the collective intelligence of Human-Autonomy Teaming (HAT), and improving complex and shared decision making. Guaranteeing an advantage in the human domain will require new approaches which are better able to combine humans and technology, while managing both technical and psychological consequences.

2.8 MEANS OF ACTION

Over the last twenty years or so, the design of digital tools has taken into account the differences and characteristics of users in order to encourage their spontaneous use. This has led some to think about how these guided approaches can be manipulated to allow for greater integration of human users within the system. The intention has gone from facilitating the user experience to instigating or even dictating how they behave.

From the attacker's point of view, the most efficient action – albeit the hardest to execute – is to encourage the use of digital tools that can disrupt or affect all levels of an enemy's cognitive processes. The various decision-making stages are targeted, starting with how information is taken in, which can be overwhelmed, how it is then filtered, which can be side-stepped, by altering how representations are constructed, by influencing memory storage, leading to inadequate decisions or by paralyzing the taking of action and making it difficult to alter objectives. Each of these phases is now understood, codified, or even replaced by digital tools. They can therefore be targeted.

Consequences may be found at three potential levels:

1) The influence over psychological, relationship, motivational dimensions, or by sowing doubt or consolidating certainties, or causing chronic consequences;
2) In the cyber domain by factorizing or inducing human errors directly, to affect the network, the information it carries or human-system interfaces;
3) Or by targeting individual cognitive abilities directly, in particular those whose cognitive capabilities are chronically altered.

This kind of warfare between intelligences will assume new dimensions as we develop wearable technologies and connected objects, and in particular the internalization of these new tools with the appearance of the augmented soldier.

Relations between domains of action

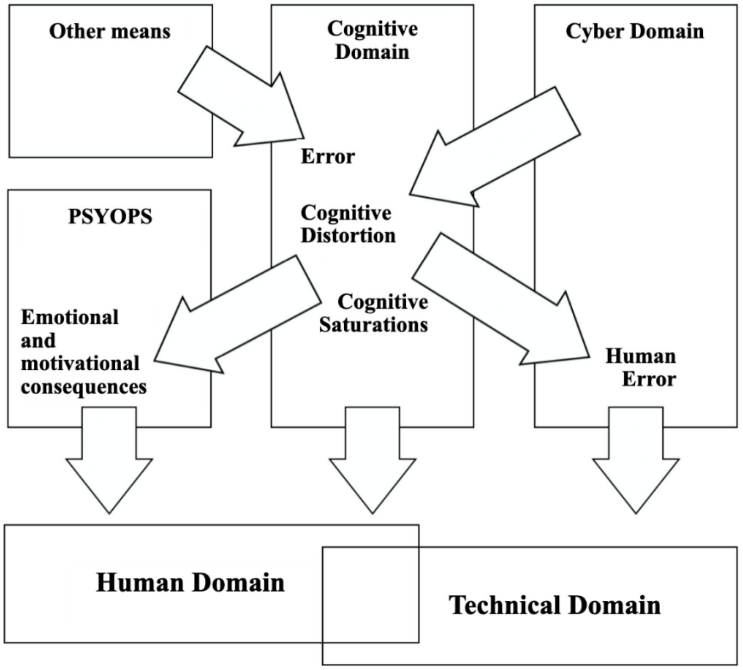


Figure 2-2: Complementarity of Human and Technical Domains and How They Interact with Other Domains.

2.9 PREPARING THE FUTURE WITH MOBILE CYBER CAPABILITIES

NBIC is a scientific project bringing together four previously distinct domains: nanotechnology (nanorobot technology, nano-sensors, nanostructures, energy, etc.), biotechnology (bio-genomic technology, bio-engineering, neuropharmacology, etc.), information technology (computer science, microelectronics, etc.) and cognitive technology (cognitive science and neuropsychology). The project was formalized with the encouragement of the US Department of Defense (DoD) in 2002 and subsequently taken up by major international institutions and a number of nations, to bring together future technologies.

The object is to encourage the development of tools and adapt or improve humans through an anthropotechnical approach to develop a hybridized human-system to meet health, security, defence objectives and prepare them for specific bio-environments (space, sea, deserts, etc.). Today, this project has led to the partial convergence of domains, mostly through pairing information technology and health nanotechnologies, new chemical cognition enhancers, embedded electronics, etc. Ultimately, it will lead to an augmented human operator (or even a hybrid one), injected with amplifying substances or nanotechnologies, providing informational resilience and superiority. A number of enhanced soldier projects are already underway.

Information, of course, implies cyberthreats and information distortion or manipulation. And a connected brain, in particular a soldier's connected brain, will lead to offensive and defence forms of "cognitive warfare." Many writers have already imagined what threats might emerge. Most of them remain science-fiction, but some projects are benefiting from real resources, programmed and in some cases tested, using, for instance, neurocomputing implants and perception-augmenting technical hybrids (vision and hearing), or even genomic modifications.

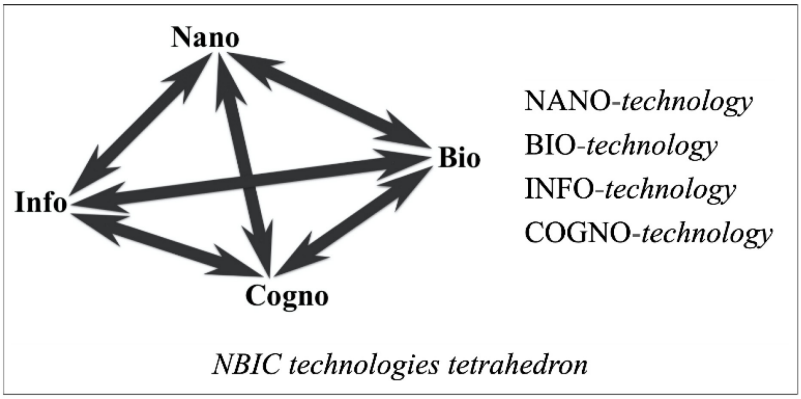


Figure 2-3: Convergent Technologies as Defined by the US DOD in the Roco and Bainbridge Report (2012).

Beyond traditional and existing threats associated with cognitive warfare as used by allied or competing nations, or those that might be developed by unofficial entities (such as terrorists or entities seeking cultural or religious domination), we need to think about the future of NBIC, and how it might influence human cognition, by distracting, saturating or even taking over and modifying objectives. We should also mention the issue of these implants' obsolescence and their exploitation.

2.10 CONCLUSION

The cyber world is now all-encompassing and ever-present. No decision or action can be executed without the tools it provides. This obviously affects the cognition of those who use these tools and will impact individuals and groups, at all levels, both psychologically, with human consequences, and technically when human errors impact systems. This is a fast-growing domain and new paths are constantly pushing back the limits of our knowledge and what potential uses might be developed. It is imperative we try to anticipate threats born of future technologies and learn more about those being developed today.

These threats are increasingly common and their consequences, more often than not, will have global repercussions, requiring NATO and its member Nations to think about cognitive warfare's varied dimensions. To anticipate these dimensions will mean acquiring the means to go beyond a reactive posture that will lead to our losing the technological initiative that is so vital to military strategy today.

2.11 REFERENCES

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.

Chapter 3 – COGNITIVE DOMAIN: A SIXTH DOMAIN OF OPERATIONS?

Hervé Le Guyader[1]

"The sixth domain, a domain where influence and mind control make it possible for the adversary to avoid frontal confrontation, always costly, often risky."

3.1 INCEPTION OF A SIXTH DOMAIN

The concept for a sixth domain of operations emerged at the beginning of 2020. It was introduced as the first recommendation in the essay "Weaponization of neurosciences" (Le Guyader, 2000) written for the "Warfighting 2040" study ran by Allied Command Transformation (ACT).

Its executive summary offered the three following recommendations:

- "Human mind" should be NATO's next domain of operations;
- AWACS successor must address Nanotechnology, Biotechnology, Information technologies, Cognitive technologies (NBIC); and
- Global security is what's at stake today.

After this first publication, ACT asked for a follow up essay to be written in the same so-called "FICINT" (intelligent fiction) style, to further develop the idea for a sixth domain of operations to be added to the five existing ones (land, sea, air, cyber, space).

A second essay, "Cognitive: A Sixth Domain of Operations" was then published in a bilingual (English/French) version (Cole and Le Guyader, 2020; Le Guyader and Cole, 2020).[2]

With this essay, part of the larger "Cognitive Warfare" study led by ACT's Innovation Hub, the concept of this sixth domain of operations reached NATO's highest echelons, together with the third recommendation presented by the previous essay ("Global Security Is What's at Stake Today"). Of note, general media followed suit and started addressing the sixth domain issue (Le Guyader, 2021; Orinx and Struye de Swielande, 2021).

Having said that, precisely defining the scope of this sixth domain is still debated – should it be restricted to a mere "Cognitive domain," or should it rather address a more ambitious "Human Domain"?

The essay "Cognitive, A Sixth Domain of Operations?" clearly favors that second option (Human Domain), as illustrated by the following excerpt from its first chapter (Tallinn chat and walk), an exchange between General Weaver (SACT) and Professor Béthany:

> *Is this 'Human Domain' just another label for the 'Cognitive Domain' that I keep hearing about?"* asked General Weaver.

[1] Hervé Le Guyader is a graduate engineer from ENSEEIHT (École nationale supérieure d'électrotechnique, d'électronique, d'informatique, d'hydraulique et des télécommunications – Toulouse FR). Founder and former director of the European Center for Communication (Centre Européen de la Communication), he then joined ENSC (Ecole Nationale Supérieure de Cognitique Institut Polytechnique de Bordeaux FR) as Head of Innovation. As a distinguish member of the STO IST panel, he partakes in activities led by the NATO ACT Innovation Hub. He is currently a sworn judiciary cyber expert for the Court of Appeal and the Administrative Court of Appeal of Bordeaux FR.

[2] English and French are the two official languages of NATO.

Béthany saw Weaver's gaze wander to the rooftop architecture, a sign that his interest was waning because, his friend knew, he was already convinced of the relevance of the "Cognitive Warfare" concept.

"No, it's not. Well, actually, cognition is naturally included in the Human Domain but a Cognitive Domain would be far too restrictive, as tempting as it may be. I know the human brain, this extraordinary piece of 'connected flesh'," Béthany made another finger quote gesture, *"this unbeatable 'thinking machine' has been luring some into advocating the Cognitive Domain should become NATO's sixth domain of operations. I know this from experience; they tried to corral me into their little club but, believe me, this would be a half-baked decision. Cognition is of course crucial to any decision-making process and key to any individual or organization's behavior but, as discomforting as it may sound, 'cog-weapons' only fill one drawer of the arsenal our adversaries are designing right now.*

Adding a Cognitive Domain to NATO's list of domains of operations would certainly look cool and make headlines, but relief would be very short-lived."

"But, what do you really mean by Human Domain?" General Weaver asked, a bit unsettled.

"Well, the Human Domain is the one defining us as individuals and structuring our societies. It has its own specific complexity compared to other domains, because of the large number of sciences it's based upon. I'll list just a few and, trust me, these are the ones our adversaries are focusing on to identify our centers of gravity, our vulnerabilities. We're talking political science, history, geography, biology, cognitive science, business studies, medicine and health, psychology, demography, economics, environmental studies, information sciences, international studies, law, linguistics, management, media studies, philosophy, voting systems, public administration, international politics, international relations, religious studies, education, sociology, arts and culture …"

3.2 FOUR KEY QUESTIONS

3.2.1 What Exactly Does NATO Mean by "Domain of Operations"?

Paradoxically, while it's relatively easy to find such a definition at the national level (US, in particular), one is hard pressed to find the one used by NATO in its literature, even in the 50 odd documents part of its doctrine. Of note, the word "domain" is introduced in its "Comprehensive Operations Planning Directive" (Collective, 2010) document, but the domains identified there correspond to the acronym PMESII, i.e., the Political, Military, Economic, Social, Infrastructure and Information domains.

Some authors have attempted to address this surprising shortcoming, offering in particular:

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

Interestingly, several candidates are today jockeying for position to become "NATO's sixth domain of operations." Next to "Cognitive Domain" and "Human Domain," "Electromagnetic Spectrum (EMS) Domain" or "Information Domain" have quite a few motivated advocates.

3.2.2 Would Human Domain Address All 6 Criteria Selected by the Johns Hopkins University?

The paper "The Information Sphere Domain Increasing Understanding and Cooperation," by Dr. Patrick Allen and Dennis Gilbert, of Johns Hopkins University, has introduced an elaborate and robust methodology for assessing whether "a field" can be considered as a war fighting domain.

While their point was to advocate the merits of what they call the "information sphere," the authors "offer for discussion what they consider to be the six key features of a domain," adding "The authors posit that if a domain has these six features, it qualifies as a domain, and if it does not have all six features, it should not qualify as a domain. This checklist of features can then be used as criteria to determine whether a new realm, such as the Information Sphere, qualifies as a domain:

- Unique capabilities are required to operate in that domain;
- A domain is not fully encompassed by any other domain;
- A shared presence of friendly and opposing capabilities is possible in the domain;
- Control can be exerted over the domain;
- A domain provides the opportunity for synergy with other domains;
- A domain provides the opportunity for asymmetric actions across domains.

The Human Domain clearly addresses these six features, but the second criterium "A domain is not fully encompassed by any other domain" probably would disqualify a Cognitive Domain, in particular if a competition between both candidates were to happen, as one can certainly argue that Cognitive Domain is, by construction, a (significant, of course) part of the Human Domain.

3.2.3 What Would Be Wrong With a "Cognitive Domain"?

Besides the arguments presented by Professor Béthany in the excerpt quoted above, several points need to be made:

- Adding a domain of operation is a highly complex task and its selection among several candidates has to be fierce and rigorous: there can only be one sixth domain!
- The cognitive dimension is, of course, a key component of the Human Domain both at individual and collective level, but is a person, is a community solely defined by its cognitive capacities?
- What about, for instance, biotechnologies, nanotechnologies?
- Don't these two technologies represent some potential threat and, should the answer be yes, are these threats addressed by the five existing domains?
- Would they be addressed by a "Cognitive Domain"?

3.2.4 What Risk Would One Take if Sticking to the Five Existing Domains?

Dr. Bryan H. Wells, NATO chief scientist, in his presentation at the ICMCIS'21 conference (Wells, 2021) eloquently presented what he sees as being the most relevant major technology trends and their accelerating synergies with Emerging and Disruptive Technologies (EDT), together with their respective timelines (see Figure 3-1). There are some fundamental human considerations attached to each of these technologies, to each of these synergies, and sticking to a purely technological approach to them would cause an existential issue. As happens with any existential issue, its nature is multidisciplinary and addressing it requires an interdisciplinary approach in order to be correctly tackled. That approach needs to put Social Sciences and Humanities (SSH) on an equal footing with the so-called "hard sciences."

Further illustrating the dual "hard sciences / social sciences and humanities" approach are these various ways of naming modern forms of warfare, such as: "hybrid," "under the radar," "ambiguous," "war and peace," "no-war."

As a reminder, China, with its "Three Warfares" strategy 1) Public opinion warfare, 2) Psychological warfare, 3) Legal warfare; and Russia (Gerasimov, 2013) have long made it clear – and public – that they fully intended to use the Human Domain to their advantage and to add it to their own multidomain strategies.

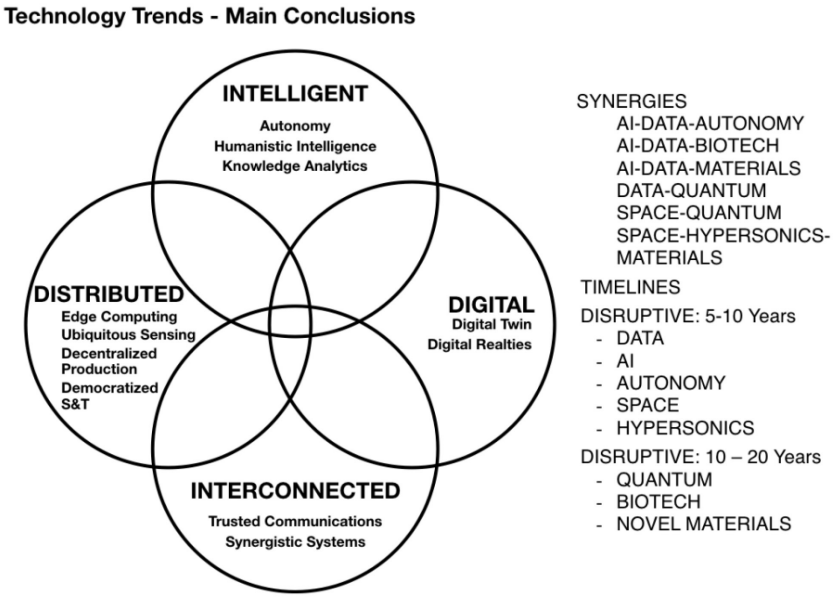


Figure 3-1: Technology Trends, Synergies and Timelines (Wells, 2021).

3.2.5 The Uniqueness of a Human Domain

Two points need first to be made:

- No existing domain is orthogonal to the others: planes take off from land or vessels, ships dock in harbors, satellites are filled with Cyber hardware and software, special operation forces use whatever tool, technique, device they will see fit to their mission.
- The industrial sectors relative to the defence dimension of the five current domains have created over the years, decades and sometimes centuries, some industry juggernauts. Together with thousands of SMEs, they employ hundreds of thousands of highly qualified workers and represent significant chunks of national economies and some crucial exports.

Human Domain is of a different nature. It is based on SSH sciences which do not fall "naturally" into one of the five existing domains and do not typically offer "off the shelf" devices. These sciences rather are to be found, simultaneously, in all five current domains. Their applications constitute a basic tenet of modern warfare as they provide key ingredients to modern threats.

SSH precede, explain, and lead to all domains. They're both inside and outside each of them and, taken as a whole, they embrace, encompass all of the five existing domains.

Human Domain IS a domain as such, but it is also the "womb" for all other domains whose existence is solely based on and justified by this 6th domain.

3.2.6 And Now, What?

As a reminder, an operational approach always needs to be designed to turn a "domain" into a "domain of operation" proper. This translates into the design of main Lines of Action corresponding to the each of the letters of the DOTMLPF-I acronym (cf: Fly, 2009), that is "doctrine," "organization," "training," "materiel," "leadership," "personnel," "facilities," and "interoperability."

Three different challenges have to be met so that the operational suggestion we wish to make here can be followed.

- A scientific challenge, because of the necessary interdisciplinarity of the approach (in particular, the combination of "hard" and "SSH" sciences);
- A technical challenge: the solution will of course be based on a "system of systems," but the issues associated with i) Multi-domain fusion, with the drastic timescale differences within each and between all domains (Human Domain attacks can go from one picosecond to several generations); ii) Computer aided (AI, ML, BD …) visualization; iii) Decision-making assistance, are bound to be quite arduous;
- A human resource challenge, both in terms of hiring (the right persons), of career progression and of (lifelong) education and training.

The Allied Future Surveillance and Control (AFSC) project would provide a unique and concrete opportunity to address these three challenges and, to put it bluntly, to prevent it from missing a significant share of the threats the Alliance faces today and will be facing onwards, part of the continuum of threats its core mission demands to "surveil and control."

AFSC will replace the retiring AWACS in 2035. Given its ambition, the competence level of its contractors, the budgets allocated and the far-reaching vision behind the project, AFSC must be designed with the requirement of building a system of systems up to today's and tomorrow's NBIC induced warfare challenges. Its multidomain coverage must address all six domains.

3.3 REFERENCES

Allen, P.D., Gilbert, D.P. (2018). The Information Sphere Domain Increasing Understanding and Cooperation. Tallinn (Estonia): 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.

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.

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

Donnelly, J., Farley, J. (2019). Defining the 'Domain' in Multi-Domain. Shaping NATO for Multi-Domain Operations of the Future, Joint Air and Space Power Conference, Berlin (Germany) 8 – 10 October 2019. Kalkar (Germany): 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.

Garretson, P. (2017). USAF Strategic Development of a Domain. Over The Horizon (OTH) Journal, 10 June 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 February 2013. Translation from Russian to English by R. Coalson, Military Review, 1, 2016. http://www.theatlantic.com/education/archive/2015/10/complex-academic-writing/412255/.

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. (2021). Le Domaine Cognitif de la Manipulation est Devenu un Terrain de Conflit. Paris (France): Le Monde, 6 May 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.

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.

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

Orinx, K., Struye de Swielande, T. (2021). Carte Blanche: la Guerre Cognitive et les Vulnérabilités des Démocraties. Brussels (Belgium): Le Soir, 11 May 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. 21st International Conference on Military Communication and Information Systems ICMCIS'2021. Virtual Edition: 4 – 5 May 2021. Brussels (Belgium): 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.

Chapter 4 – WHAT IS COGNITION? AND HOW TO MAKE IT ONE OF THE WAYS OF THE WAR

Pr. Bernard Claverie[1]

"Metaphorically, during the medical examination, cyber warfare uses the stethoscope and PSYOPS the contents of the pipe; cognitive warfare is concerned with the doctor's diagnosis."

"Cognitive warfare" is one of the ways used by specialists to modify, orient and alter human reasoning for the purpose of conquest, superiority or inferiority of individuals, a group of individuals, groups, or populations. It is based on the knowledge of the cognitive processes mobilized by these individuals in the use and the control of their environment, notably technological, by means of digital technologies. Generally speaking, the aim is to modify the awareness that individuals have of reality in order to make them take erroneous decisions or prevent them from taking necessary decisions. "Cognitive warfare" is therefore a practice of using cognition for the purpose of military superiority.

Cognitive warfare is part of the following triad: i) Human and social sciences; ii) Human factors methodology and engineering; iii) Theories of cognition and models of the cognitive processes on which we intend to act. But in order to act or to protect military or civilian actors, operators or decision makers, soldiers or commanders, citizens or elected officials, from deliberate attacks on cognition, it is necessary to understand the phenomenon of world knowledge, of information processing by the brain: cognition.

From the simple acquisition of data from the environment, to the use of the most sophisticated semantic memories, from the control of gestures to decision making in complex situations, all of the "cognitive processes" allow humans to live reasonably in the world. The impairment of cognitive processes has two harmful consequences: i) Contextual maladaptation, resulting in errors, missed gestures or temporary inhibition; and ii) Lasting disorder, which affects the personality and transforms its victim by locking him or her into a form of behavioral strangeness or inability to understand the world.

In the first case, it is a question of causing transitory consequences, circumscribed by a particular critical environment (cf. Figure 4-1). The second concerns the transformation of the decision-making principles of individuals who then become disruptors or responsible for erroneous actions, or even non-action (cf. Figure 4-2).

Figure 4-1: Does the Animal Look to the Right or to the Left, Up or Down, Does it Laugh or Does it Look Bad? Note that it is impossible to see both forms at the same time and that the voluntary passage from one to the other requires a form of "cognitive energy." The figure is said to be "reversible" and "bistable" (inspired by the figure of the "duck-rabbit" by unknown author and reproduced by Joseph Jastrow, 1900).

[1] Pr. Bernard Claverie (PhD) is a University Professor, Honorary Director, and founder of ENSC (Ecole Nationale Supérieure de Cognitique – Institut Polytechnique de Bordeaux FR) – and a cognitive science researcher affiliated with the CNRS (UMR5218 – Bordeaux University FR). He is Editor-in-Chief of the online journal "Cognitive Engineering" – ISTE Open Science.

Figure 4-2: A Thinker: What About the Inhibition of Action Due to Indecision or Cognitive Overload?

4.1 DEFINING COGNITION

Cognition is the whole of the means, of the bodily equipment and of the processes that mobilize them, which make it possible to have a knowledge and a representation of the world in which they are inserted and to act on it.

These means are the behaviors or physical activities, and the thoughts or mental activities.

The equipment is what ensures the interface with the environmental information (sensations and actions) or ensures the internal processing of this information. This refers to the nervous system, but also to parts of systems that are associated with it, such as the endocrine system, the muscular system, the system in charge of vegetative regulation or the system of relationships, etc.

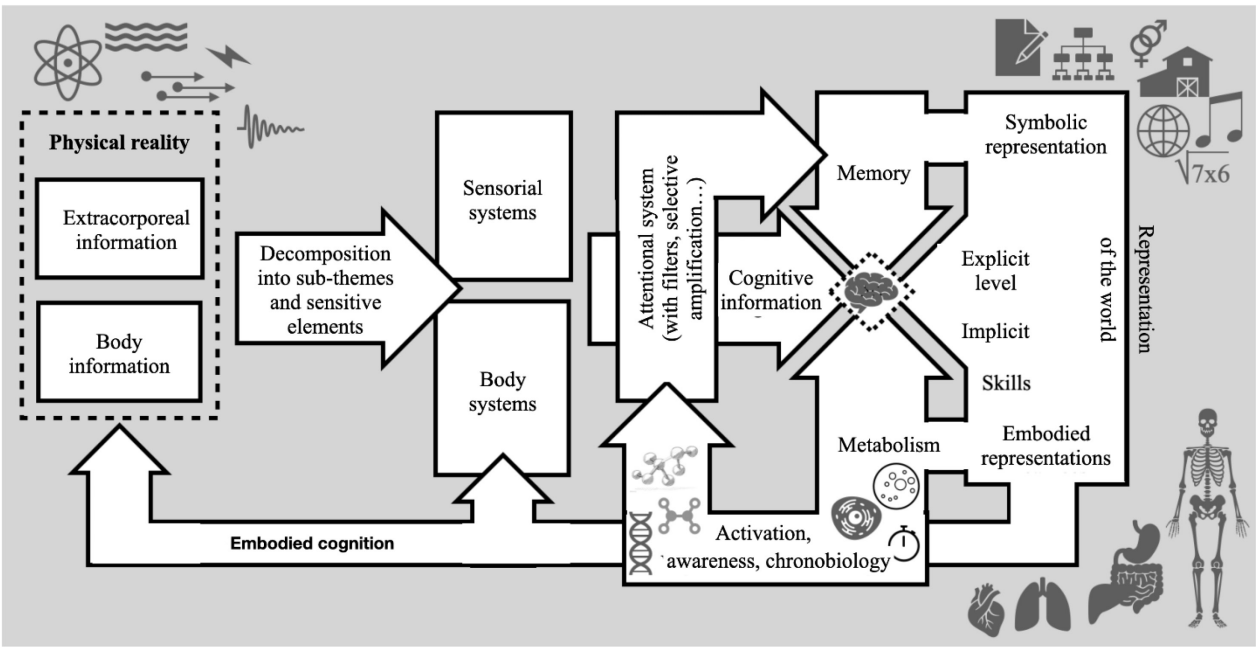


Figure 4-3: Schematic Illustration of the Human Cognitive System Representing Some Major Processes of External and Internal Information Processing.

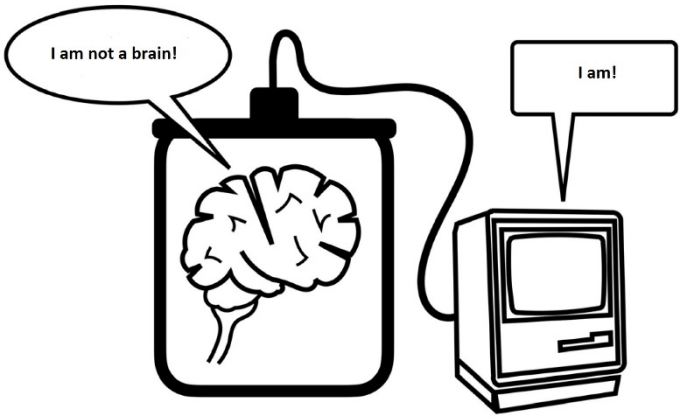


Figure 4-4: Close Relationships Between Brain and Digital World: Causality and Co-Dependence (Claverie, 2021).

The processes refer to the major stages of information processing, from sensation/perception to motor programming and gesture adjustment control, including attention filtering, the various short-term, medium-term, and long-term memory storages, representation, and integration or contractualization capacities, expression, and language, etc. This involves dimensions that are both oriented towards external information and internal information. To simplify, we could say that "cognition is what the brain does with the information in the world."

4.2 BRAIN AND DIGITAL TECHNOLOGY

The world has little to do with what the brain knows about it. For example, the range of electromagnetic waves that man perceives is extremely limited, between infrared and ultraviolet, and sound frequencies are only known in the strict range of infrasound to ultrasound. The discriminating power of sensory equipment is poor, constrained by limited transfer capacities. Human abilities are fragile, depending on the time of day, on the duration of the stimuli and on nervous fatigue. Attention is a sort of filter protecting the brain from overload. It eliminates the vast majority of inputs, only allowing to pass those that the brain considers useful. Memory, learning, and recognition capacities are mediocre. They are limited to a few perceptual, conceptual, or semantic bases, which reduce the knowledge of the world to what is known and, most often, expected.

From these limits comes the need to get help. This has always been the role of technology. Today, we willingly entrust it with the most boring cognitive operations or those requiring the most energy. This is the case for perception, with devices ranging from simple glasses for vision correction to night vision binoculars or synthetic screens, called "head-up displays," for car or aircraft pilots. For memory, artificial aids are also numerous. Notes and reminders on cell phones, online consultation of encyclopedias accessible by computer, landing maps or onboard procedures on tablets are other examples.

The downside is that digital assistance produces dependency. The first level concerns the new impossibility of adapting to the complexity of the world without the extension of cognitive capacities, towards an "augmented man" (Claverie, 2010), which today is no longer an everyday fantasy. The second is a consequence. It is the habit and even the desire for permanent and instant access to digitized information, photos, films, press data or scientific analyses, etc. On top of that, there is also the motivation of new users driven by the logic of internet networks and the continuous use of social networks, digital sharing and the "like" culture.

This proximity between cognitive life and the world of digital knowledge has been defined by some authors as a "technium" (Hartley and Jobson, 2021), in relation to globalized and interconnected human knowledge, the so-called "noosphere" (Kelly, 1995). Cognition is no longer just a matter of the brain. It is, at least since the last decade, in a natural relationship with digital technology and shared knowledge. This double relationship is therefore bilateral and dual. It is bilateral because digital technology is a production of cognition, and today this requires digital assistance. It is dual because these relations concern both the individual and the communities. We will therefore differentiate between the technologies of personal tools and embedded hardware, and those of the Internet of Things, networks, and communities. These are two distinct but complementary fields of cognitive warfare.

4.3 LIMITED CAPACITY AND ATTENTION

One of the first things to be noticed about cognition is that it has only limited capacities within the already restricted range of what the brain can know about the world. It concerns both the quantity of information to be processed and the energy directed on the contents of this processing. The little information that reaches the sensors is manipulated by internal filtering processes whose purpose is to protect the brain from overload and to increase the salience of what the brain is processing.

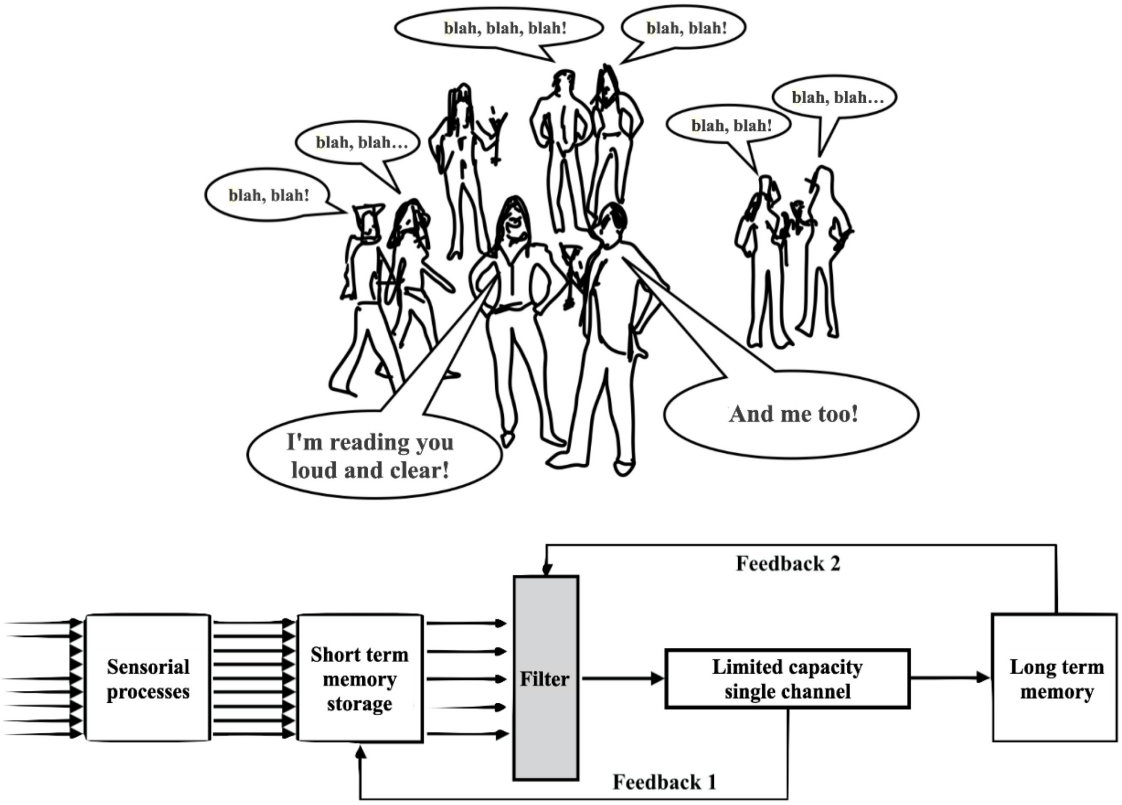


Figure 4-5: Illustration of the Principle of Information Selection to Protect the Cognitive System with Limited Capacity – the Selected Information or the Information Having a Significant Force Passes; the Non-Useful Information is Neglected. Experience of the "cocktail party": one hears what the interlocutor says without hearing the others unless what they say is significant, then one does not hear the interlocutor (one does or does not pay attention).

The attention phenomenon has several characteristics. It is a function of the type of information, its physical intensity, and its semantic strength, but it can also be voluntarily oriented towards certain dimensions of the information. In the first case, we speak of a "floating attention," with cognitive mobilization depending on the characteristics of intensity or meaning of the afferent signal. In the second case, we define a "directed attention" towards expected characteristics. From this, we can conceive that attention directed towards a target limits any attentional capacity to other destinations. One then knows of the world only what one expects of it.

If this organization of the cognitive system protects against information overload and ensures the efficiency of what is selected, what is outside the attentional field escapes processing. This is what we observe, for example, in distracted driving while using cell phones, or in the tunnelization effect in air traffic control, during which what happens outside the focus of attention escapes the sagacity of the radar operator. Such examples are to be found in applied psychology textbooks, and the implementation of visual scanning procedures imposed on operators, pilots, surgeons, and other experts involved in surveillance duties, is systematized in training courses. These procedures are themselves very costly in terms of attentional resources, very tiring, and require a collaborative organization of the workstations, with digital devices to assist, substitute and monitor the human actors.

The distraction domain is one of the main aspects of cognitive warfare. It has two complementary components: attentional pollution with the distraction of focus, and the exploitation of digital flaws or interfaces of digital assistance or monitoring tools. Thus, the repeated occurrence of multiple alarms with no object of interest leads the operator to minimize the significance of these alarms, or even to neglect the device itself or even disconnect it. Numerous accidents have been caused by a do-it-yourself approach to the suppression of alarms (in hospitals, energy control, air navigation, road, or domestic accidents, etc.).

4.4 COGNITIVE CONFLICT AND ILLUSION

A cognitive conflict is a situation that an individual must manage by processing information for an expected purpose that is not consistent with what that information allows him to do. This is the case when the processing is incompatible with the expected result or raises a cognitive ambiguity that the subject cannot simply resolve. For example, this is the case for ambiguous figures that are perceived as mutually incompatible shapes or that lead the subject into a task that is impossible to resolve.

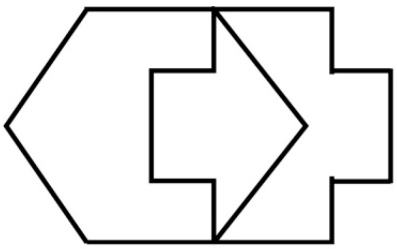


Figure 4-6: Does the Arrow Point to the Right or the Left to Reach the Pharmacy? And is it a hexagon or a cross? Examples of ambiguous figures that require a lot of cognitive work in order to answer a simple question.

This type of figure was documented early on by Gestalt Psychology (Köhler, 1969) and has been the basis for many studies in psychology and neuro-ophthalmology (e.g., Meng and Tong, 2004; Kawabata and Mori, 1992). The time used to resolve the cognitive conflict is not available for anything else and the conflict often becomes obsessive, engaging future reasoning (see Figure 4-1 and Figure 4-5). Cognitive energy directed towards surface problem solving increases the psychological cost and reduces the resources to be allocated to other tasks.

4.5 HIERARCHIES AND COGNITIVE DOMINANCE

The cognitive system is globally structured into functional levels whose activity is complementary and combined with that of the others to produce an adapted behavior. This organization corresponds to the emergence of new encephalic structures during the evolution of vertebrates. Thus, cognition appears as soon as the animal becomes capable of understanding its environment, of being "aware" of it and of using its experience to better adapt to it, thanks to strategies that it invents: an "intelligence."

Intelligence is to be understood here as "the ability to solve problems that cannot be solved by themselves," for a better adaptation, a better survival, a better longevity and a better quantity or quality of pleasure (Claverie, 2005). Cognition is closely related to intelligence and awareness of the world. It is already present in humans' ancestors. They have kept particular aptitudes, which they have perfected to give the most sophisticated functions, such as symbolism and language, and self-awareness.

The cerebral system supports the cognition, from the most elementary forms to the highest. It represents a stack of successive levels of development, with properties that are complementary, sometimes antagonistic, and more and more elaborate for a more and more complex and better adapted behavior. It is surrounded by the inputs and outputs of the sensory-motor system and part of the endocrine system (some hormones are involved in stress, vigilance, and attention).

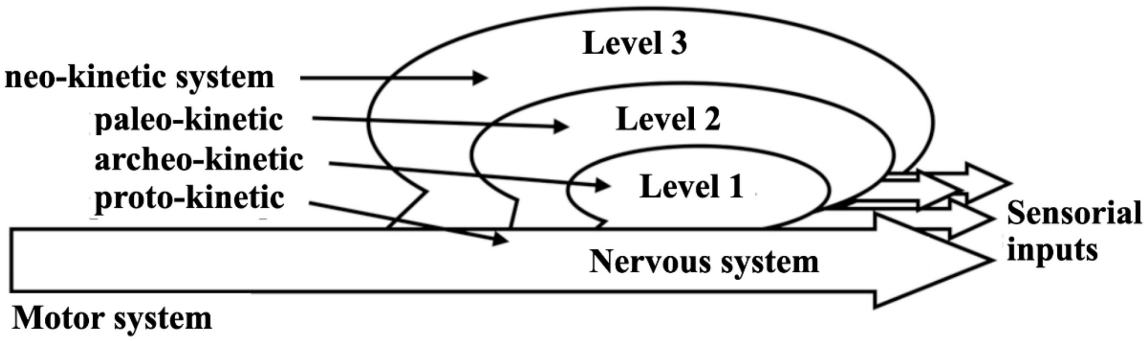
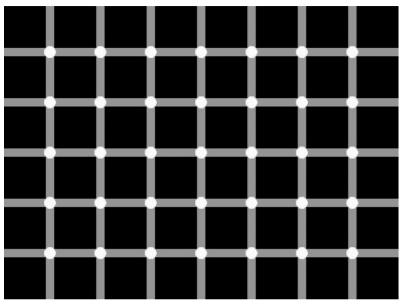


Figure 4-7: Simplified Diagram of the Cognitive Levels Organization on the Brain Layers, Between Sensory Inputs and Motor Outputs. This cerebral structure contains the nervous entities responsible for the different cognitive functions indicated in Figure 4-1 Note: kinetic, from movement (Greek); literally which allows movement and by extension adaptation to the environment by sensory integration and motor programming.

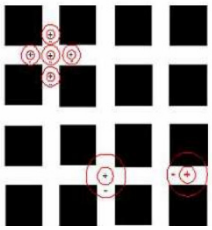
The brain is therefore a hierarchical device, organized in levels and expressing cognitive functions and thinking skills that are increasingly powerful.

The simplest level represents a first level cognition linked to automatisms, with sensory limits, programmed skills, rudimentary memories, etc. It is the level of basic learning, of the establishment of all-or-nothing processes, those that no longer require attention once established, but escape all control once triggered. This level is particularly easy to deceive. It is involved in illusions, bad perceptions, false certainties, and the induction of motor automatisms. The second level is strongly dependent on the processes of memory and affectivity. These two components of mental life are in close collaboration, involving the functioning of very close structures (amygdalo-hypocampal complex, Papez circuit, cingulate cortex, etc.). The manipulation of one of these components affects the other, and it is easy to stabilize parasitic memories by affective involvement and to trigger emotional reflexes by imposing memories. Three different challenges have to be met so that the operational suggestion we wish to make here can be followed.

Other dimensions of cognitive warfare can concern the modification of the elaboration of stored rules by information or decision overload, by accelerating analysis loops that do not allow the elaboration of procedures or, on the contrary, by provoking conflicts of these rules. An example can be given in the difficulties of background/form detection or the use of a process that inhibits another one.



The contrasts perceived at the intersections are attributed to the variation in the frequency of the action potentials according to the relative areas of the retinal regions called ON and OFF (primary visual receptive fields).



The neural coding frequency is maximal when the ON region is fully lit and the OFF is completely dark.

Figure 4-8: How Many Black Dots Are There in the "Hermann Grid"?

Figure 4-1 and Figure 4-5 are ambiguous. Their analysis depends on low-level rules that exclude each other. The factorization of one of them prevents the other from being expressed. Even if we know it perfectly, we cannot have any control over it; we cannot see both forms at the same time, which is elementary for a machine. In the same way, certain inferences can facilitate certain processes with, for example, the overestimation of the verticals compared to the horizontals. This is also the domain of "nudges," those "little nudges" that are nowadays introduced almost everywhere to guide and orient behavior (Thaler and Sunstein, 2009) in a form of constructive manipulation of behavior, well known in management and in road or industrial safety.

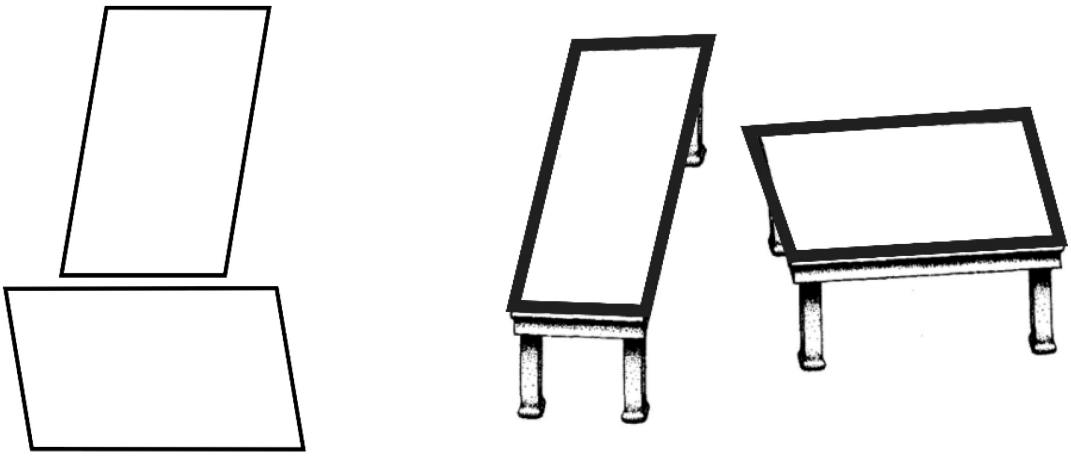


Figure 4-9: Example of Two Perfectly Identical Figures Whose Difference in Orientation Makes Them Appear to Have Different Dimensions and Surfaces. (Right) The contextual effect of "Shepard's tables" (1990). This illusion combines the analysis effects of first level (visual), second level (context) and higher level (semantic).

The higher cognitive level is mainly involved in semantic strategies, using language or symbolic meanings. This is the level of explicit consciousness or repressed unconscious phenomena, of mental images and sophisticated representations. It sometimes competes with the lower levels with the use of automatisms or rules learned in a voluntary effort of cognitive orientation.

It is also the level of high-level biases concerning ambiguities of meaning, either due to a lack or an excess of meaning, a semiotic conflict, or semantic ambiguities. Several theories exploit these operating distortions. They can be found as early as the end of the 1960s in experimental sociology (Zajonc, 1968), then in numerous works of social psychology (Goffman, 1974), in experimental economics (Martinez, 2010), as well as in risk ergonomics with a particular focus on "absurd decisions" (Morel, 2002) and the strength of the "counterintuitive" (Berthet, 2018). They were notably popularized by the Nobel Prize-winning economist Kahneman (1979) and his colleague Tversky under the name of "cognitive biases."

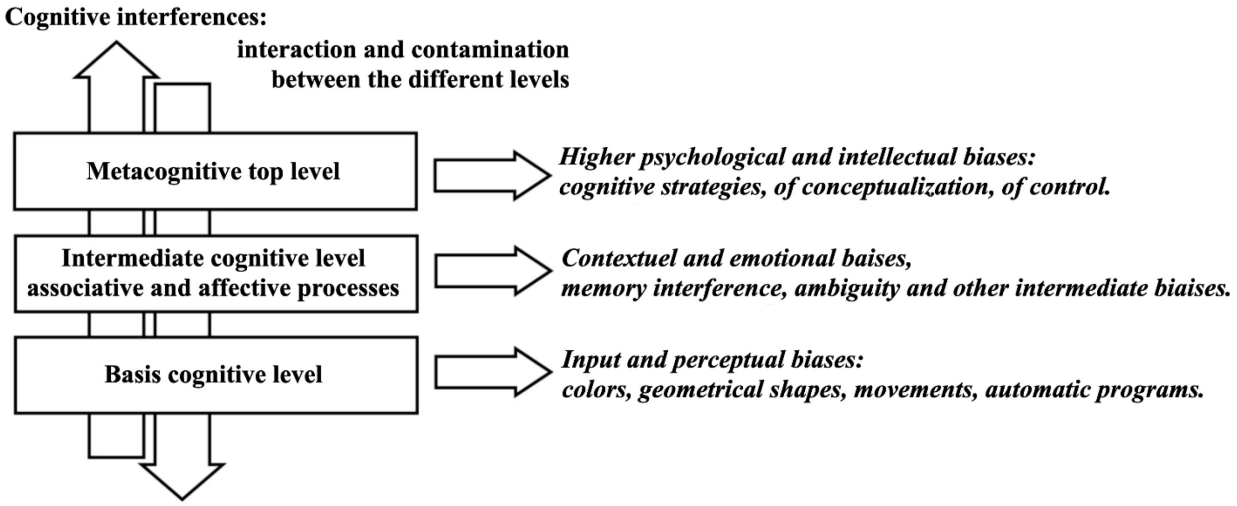


Figure 4-10: Organization of the Cognitive System in Levels, with a Hierarchy of Cognitive Biases Based on the Levels as Well as on the Interaction Between These Levels.

Just as cognitive processes are hierarchically organized into functional levels, such as language and high-level formalism, affectivity and memory, feature extraction and perception, the relationships between these levels are equally important in contributing to a global knowledge of the environment and its awareness.

The conflicts within each level are then completed by conflicts between levels. As the processes enrich each other, they can interact in an inhibiting way by preventing a task from being carried out, for example, or in an exciting way by distorting the productions. These phenomena are at the origin of semantic misconceptions linked to erroneous bottom-up processing, which may or may not compete with data in the memory. The same applies to top-down processes that tend to direct attention and let us know about the world only what we expect from it, minimizing the importance of unexpected elements and neglecting weak signals.

4.6 COGNITIVE PERSONALITIES AND STEREOTYPES

The cognitive personality is the spontaneous way an individual has of knowing the world. In a way, it is the set of habits of thinking, seeing, hearing, memorizing, etc. Each individual has a tendency to mobilize, prioritize or, on the contrary, inhibit certain cognitive processes more than others. This personality is particularly related to the distribution of priorities allocated to each cognitive level, but also to the habit of

facilitating or inhibiting the interrelations between levels. The world is thus conceived and known in a different way according to the criteria of the cognitive personality of the individuals who explore it, insert themselves into it or speak about it.

One of the criteria is the priority given to one level over another. Some individuals tend to value concrete sensory information to the detriment of the emotional or memory value of each of them. Others focus on their interpretative conceptualization, modulated by language or by intellectual theories learned. Another example is the tendency to focus on details while others focus on wholes, or contexts versus isolated elements, etc. Some people have a greater tendency to intellectualize their perceptions and to retain only what is analytical or constructive, for example the preference for numbers over words or vice versa, for geometry over logical relationships, for series and regularities over novelty, etc.

At the higher cognitive level, which is considered to be dependent on the cortex of both cerebral hemispheres, cognitive differences are known according to the laterality of the processes: the cerebral dominance. Some cognitive personalities depend on processes considered to be lateralized on the right, while others favor those on the left. The commissures (relations between the two hemispheres) can be more or less solicited with some individuals being more bilateral than others.

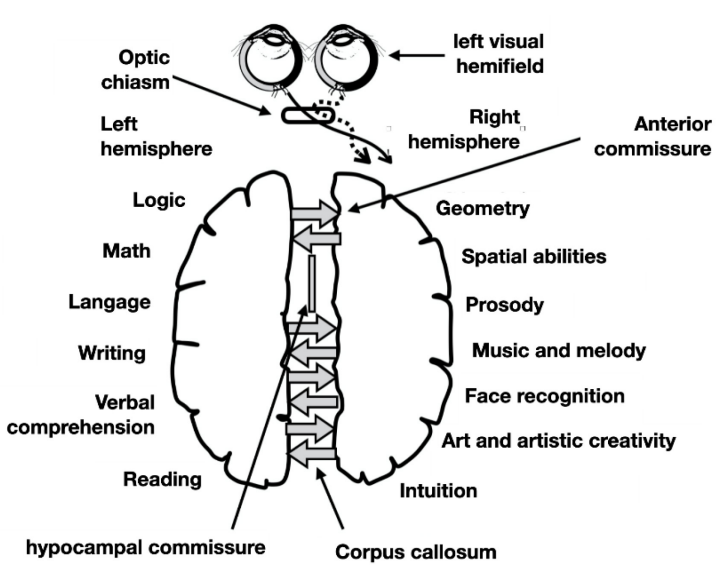


Figure 4-11: Example of Lateralized Cognitive Functions Recruiting Different Neurofunctional Territories, on the Right or on the Left, Forwards or Backwards (here in the Right-Handed Person). Spontaneous cognitive dominance processes contribute to cognitive personality.

Therefore, the world is not as our brain allows each of us to conceive it, nor as another can conceive it. It is through language that a linguistic negotiation about it is possible. It allows us to understand each other and thus contribute to its theorization. This metacognitive dimension serves both as a guide and as a facilitator of the cognitions linked to the lower levels. Such top-down processes, influenced by experience and culture, constitute a real model in which knowledge is embedded. They form a kind of prototype of thought.

Thus, it is easy to use distortions between individuals, to facilitate the lack of coherence between conceptual models and personal knowledge. The field of failed learning is concerned here, but also, in a more critical way, that of certain abductions or psychopathological disorders that are as difficult to control as they are simple to induce and exploit.

4.7 CAUSAL ATTRIBUTION AND MANIPULATION

The attribution process is based on causal inference. This means that at the most sophisticated level of thinking, an individual does not objectively infer data or seek an interpretive solution through a trial-and-error process. The individual interprets the world according to previous mechanisms, prototypes, and spontaneous beliefs. Attribution makes it possible to give meaning to events, especially when they are complex and when there are no simple explanations. It concerns both the individual's own conduct and behavior and that of others, and this applies to the interpretation of the past as well as to predictions, spontaneous expectations, and the interpretation of the future (Heider, 1958). Two dimensions are to be taken into consideration, that of the context and the organization that is believed to be the environment, and that of the individuals and the importance that they consider to be their role in this future (Jones and Davis, 1965; Nisbett and Ross, 1980). Two dimensions of attribution are thus identified. The first consists of believing that the evolution of the situation is mainly relative to oneself, to one's own choices and behaviors, or even to one's mere presence: this is "internal attribution." The second is to believe that almost everything depends on the environment, history, or others, that the context is predominant and that personal action is of little importance: this is the "external attribution."

We have seen that decision makers are constrained by their attributional tendencies, often based on their work history and experience, but also by their biases. When facts contradict the attribution, some of them maintain their judgments by confirming the pre-established explanation and by authoritatively denying alternative hypotheses.

The constitution and the systematic recourse to "ready-made ideas," in particular in human relations with the recourse to "naive psychological theories," allows the individuals to inscribe themselves into a reassuring framework of understanding of the world. The importance is no longer to know something exact about the world, but to ward off uncertainty with "spontaneous theories" that their authors try to confirm at all costs. Some slippages can even lead to "fake news," false controversies, revisionism, and contestation of science, etc.

One of the usual principles consists in a filter of analysis that permits only the facts of reality that confirm the convictions. Everyone draws conclusions about the future from selected samples of the past. The rules make it possible to consider the events of the world as particular cases falling under the interpretation due to these rules. For each of them, the deviations from the rule are considered as exceptions which constitute the basis for the elaboration of new interpretative rules of reality, participating in a bias of self-conviction. We can therefore reduce the problem of cognitive personalities, i.e., the tendency of each individual to spontaneously mobilize certain cognitive processes, according to the main bases of causal attribution: the dimensionality of the "self" distributed around the two poles of hypertrophy and personal miserabilism; the feeling of responsibility, passing from the orientation of the cause towards oneself to the feeling of persecution; the falsity of the judgment which rests on inadequacies of the forms of reasoning.

This is where the shift from a science of cognitive biases and the personalities that are subject to them to clinical psychology begins. These attribution biases are indeed characteristic of many psychopathological disorders. They are the object of a systematic expression exploited by certain manipulators.

4.8 BIASES AND GENERALIZED ERROR

Some authors have studied several forms of bias. One particularly interesting form is the so-called "complacency" bias, in which the interpretation of reality is linked to the potential positive or negative outcome of a situation (Nisbett and Ross, 1980). Moreover, there is a difference in position depending on whether one is an actor and involved, and an observer or not concerned by the situation. Thus, the actors involved attribute more causality to the "me," to personal motivations and to the valuation of the potential

effects of their own action, whereas observers or external collaborators value dispositional and contextual causes, while minimizing the importance of the people involved and their action.

In both cases, the bias of "pretentiousness" consists in thinking, for an individual, to be at the center of the problem or on the contrary not to be concerned by this problem. Misunderstanding, or even contempt, are spontaneous consequences of the one in relation to the other and are factors of social ostentation and even of interrelational problems. The expression of a hypertrophy of the self is often concretized in a form of conviction of uniqueness, of belonging to a kind of elite, while being convinced of impermeability to the considered bias. Another usual form of expression consists in believing that training can transform one's personality and thus protect one from the bias. These two positions often combine to give rise to or justify corporations, collegialities, professional communities, even factions and other elitist organizations. They pose the problem of practical training, by example, or within the framework of an initiatory "enlightenment."

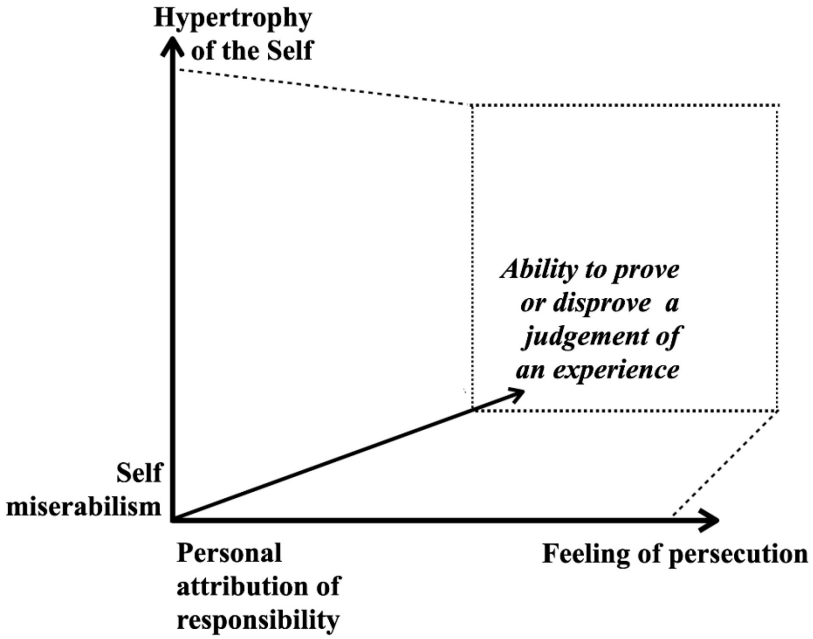


Figure 4-12: Three Clinical Axes of Cognitive Distortions in Causal Attribution. At the bottom, front and left, biases tend toward melancholy and withdrawal. At the top, back and right, paranoid personalities. At the bottom left, biases of pretentiousness at the top, or self-indulgence at the bottom. At the top, in front and on the right, the meticulousness biases, etc.

Two other beliefs, as common as they are erroneous, are that only others are victims of cognitive errors, and that formalism and training will solve the problems of bias. However, everyone is concerned by the perceptual error in Figure 4-8 and Figure 4-9, and it is not because we have a rational explanation for it or because we repeat the experiment that the error disappears. Only the knowledge that one has of the error and the knowledge of how to control its consequences can be useful. The cognitive system does not vary; it does not evolve with experience or with learning, and its biological characteristics mean that everyone, without exception, is affected. Experience or training do not change anything. The only things that can be learned are therefore self-control or shared control, and metacognitive analysis of anticipation ("gaming" and simulation) and catch-up ("dynamic retex"). But as soon as the lower levels are involved, as soon as the mental load, stress or time pressure increase, individuals tend to revert to their stabilized cognitive bases.

Cognitive biases are general errors. Behavioral economics has inventoried hundreds of them. They are all based on the structure of the cognitive system as it has been constituted, subject to the neurobiological

constraints of evolution. This has facilitated the emergence and selection of processes useful for survival, eliminating individuals who were not subject to this logic. Two major biological principles are at work. The first is the tendency to "minimize energy." This major biological principle manifests itself in optimization of the spontaneously estimated "cognitive cost." The individual unconsciously values short reasonings and one of the motors of this regulation resides in the motivational conviction that simple thoughts are the most truthful. Once established, spontaneous representations, beliefs, and stabilized thought prototypes contribute to certainties that interfere with objectivity or commit the individual to the constraints of another principle: having to make choices. A cognitive choice is an abandonment of thought, and it is difficult to abandon what one holds dear. The learning of explicit rules makes it possible to avoid ambiguity. Their concatenation to solve complex problems mobilizes both memory and attention, as well as the reflection to know how to choose and order them.

These are three targets of cognitive action. At the first level, it is a question of saturating attention and exploiting automatisms, at the second level, of disturbing memory and exploiting emotional influences and interferences, and at the third level, of preventing the realization of reasoning by temporal pressure, interference, or facilitation of reasoning errors.

4.9 EXPLOITING COGNITIVE ERRORS

As far as reasoning is concerned, it is often false. To put it simply, we can consider that human thought is based on the implementation of three types of reasoning, two of which are useful, or even indispensable, but erroneous. It is then simply a matter of facilitating them.

The simplest and most frequent type is called abduction. It is also the less expensive one, which we suppose corresponds to the basic forms of the cognitive system. It is the constitutive mode of thinking of a naive physics and of spontaneous psychology. These two dimensions of knowledge allow each person to have a simplified form of understanding of the world and to establish natural relationships with others. It is probably linked to the immediate survival of individuals, with rapid knowledge based on the categorization of life contexts and that of dangers or resources. In psychology, abduction is the main form of intuitive reasoning; it consists in minimizing troublesome hypotheses by saving cognitive costs, and eliminating solutions considered improbable. But abduction, however efficient, is a logical error.

This reasoning is based mainly on observation and experience. It is an abusive generalization of causes. This reasoning is very useful if it is controlled, used in science, to make a medical diagnosis, or to investigate and motivate the "intimate conviction" of magistrates. However, abduction does not lead to a reality, but brings a "probable truth" that needs to be explored and verified a posteriori thanks to strict protocols. But this verification takes time and can appear superfluous. Abduction produces error through naivety or through accepted risk since it is considered improbable.

A second, more sophisticated level of reasoning is called induction, which is also a logical error. It falls under the same characteristics of usefulness and criticality of consequent non-verification. It also contributes to a representation of the world by the elaboration of spontaneous categories which allow the subjects a more sophisticated representation than with abduction, although also naive.

Induction is mainly built around time assessment. It is the belief that the future will look like the past and that we can expect stability in reasonable time frames. "Tomorrow there will be daylight," "the night is young" and "the sky is stormy" are useful examples for a normal life. It is a tendency to make a generalization, with an explanatory role for the future, based on past or established events, ignoring exceptions. This form of reasoning goes from the singular to the general, from the particular case to the laws that would govern it, from a consequence to the principle from which it would follow and to a postulated cause. This type of reasoning has also shown its interest and power in science, medicine, and

economics, as long as the thought process is limited by the qualification of the probability of one's own error (internal validity) and the permanent search for a counter-example that would refute the generality admitted, however without certainty (external validity). Here again, there are two weaknesses of reasoning, the introduction of false beliefs from erroneous elements or the neglect of exceptions and counter-examples often present in weak signals.

Abduction and induction are opposed to deduction which, when correctly formulated and established on verified elements (truth of the premises), leads to a conclusion that is always true (truth of the conclusion).

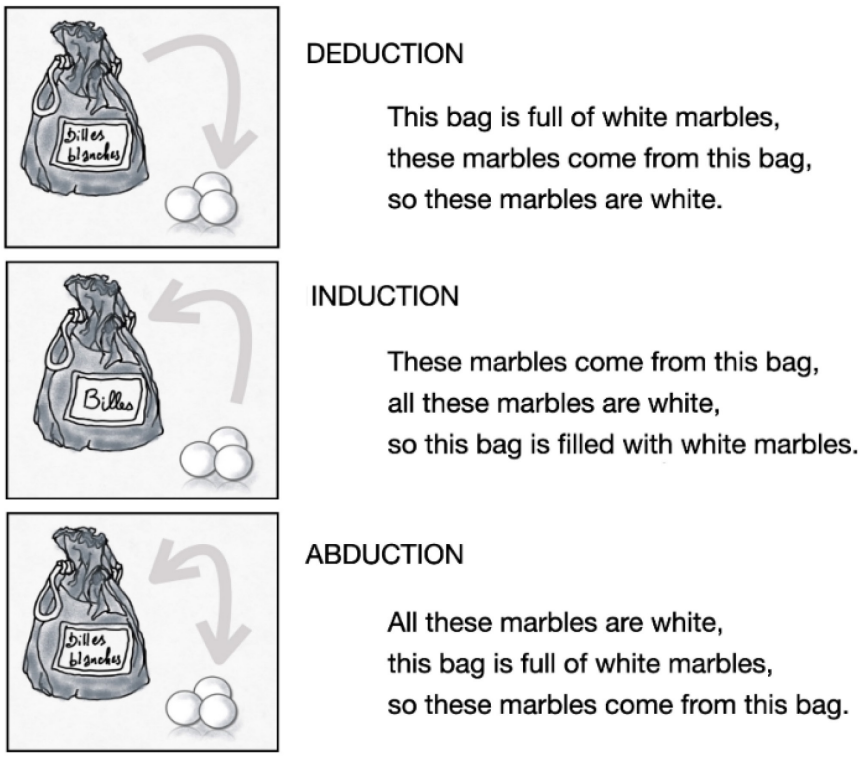


Figure 4-13: Three Forms of Thinking. The first one needs time and has only a weak power of generalization. It is however the only exact one. The other two forms of thinking correspond to cognitive reflexes and are logical errors inducing psychological biases and spontaneous psychology rules (folk psychology). Their usefulness can only be considered if accompanied by methodological procedures of verification, which are costly in time and energy (in Claverie, 2019).

Generally speaking, cognitive errors can be related to these three categories, or to a combined sequence of elements of these three types of reasoning. It is then sufficient to identify the constituent elements of the opponent's cognitive strategy to act on at least one of them, by exploiting the constraints of speed of thought and non-verification, the tendency to neglect these verifications, the facilitation of abusive generalizations, and the confirmation of erroneously established convictions. The defender, on the other hand, takes care to value the steps of deductive verification by chasing away the recourse to shortcuts of thought, notably by detecting the potential flaws of reasoning or doctrinal or established procedures and rules.

In the future and faced with the brute force attack and the difficulty of spotting it, the double necessity of a strict methodology of reflection and the use of artificial intelligence tools and analytical programs on big data will emerge, on the one hand in the surveillance of cognitive errors and on the other hand for the detection of malicious actions of incitement to error.

4.10 METHODOLOGY AND CRISES OF UNDERSTANDING OF THE WORLD

While thinking is a spontaneous act, thinking professionally is not something done without careful consideration. For example, medical diagnosis is not a simple impression, resulting from floating attention and the emergence of information memorized by the patient or the practitioner. The diagnosis is subject to strict rules of prompting, directed questioning and structured analysis. It proceeds by going back and forth between abductions, inductions, and deductions, focusing on elements to be eliminated or, on the contrary, to be valued. Complementary examination takes on its full meaning here in the completion of the opinion. The same is true today of criminal profiling techniques that abandon impressions in favor of scientific, strict, and logical methods that can be accepted by the courts.

This procedure is well known in science. It focuses on looking for elements of refutation to a theory in order to refine its edges. The elements of theoretical falsification are then examined and are the object of a specific research, either to refute the general theory or to clarify it. This method works by conjectures and refutations (Claverie, 2019).

We can schematically describe the reasoning process by one or several hypotheses posed by induction or abduction, which allow predictions that must be confronted with real experience. They are then refuted or accepted as potentially valid until a new contradiction is found. The truth is thus only temporary. It is admitted within the framework of a permanent vigilance to be invalidated or reconsidered. Outside this strict practice, it is the domain of error and the potential playground of cognitive warfare.

Objective knowledge of the world is first of all based on generalities. They are constructed from statistically established data, verified information describing notably central tendency values. They explain the totality of these values, and the best part of the marginal data, some of which may however conflict with them. This is where the problem lies, since an explanatory theory of reality, i.e., its representation, is by essence transitory. It is constantly being refined and enriched. When it can no longer be refined and enriched, it must be abandoned, despite the investments that have been made and the personal convictions, however established.

A famous example is offered by the epistemologist Karl Popper (1959), who developed the paradigm of the critical rationalist. A theory states that all crows (birds of the Corvus family) are black. However, a weak signal produces a crucial experience: a white crow has been spotted. In the first case, it is either an error or a cognitive disorder (e.g., observation error or perceptive illusion), or there is a crow, which temporarily was or became white (e.g., became white by old age), or somebody made believe that a white crow exists (e.g., by painting a crow white, by building a false crow out of white cardboard, by altering the observation instrument, etc.) In the first case, the veracity and informational robustness of the observations, the observables and the observed, as well as the reliability of the observers, must be re-examined. Second, the sources and sensors, as well as the signal filtering and amplification procedures, must be checked for cyber confidence. One can also highlight a transient aspect of the observable, or a harmful intent and the existence of a malicious actor. Although the theory has become inaccurate, it is being adapted. It must then evolve by conceptual refinement or clarification: all crows are black, except for albinos, which will then have to be the subject of a theory of their own, or except for those painted white, or except for old birds, etc. If it turns out that the successive refinements cause the theory to lose all meaning, it will be abandoned because it has become incapable of describing and explaining reality: white crows do exist.

Abandoning established theories is costly, and especially anxiety-provoking if no alternative theory is available. It raises notable resistance among the followers of the theory as well as among its users, who will have to modify their conception of a part of the world and their experimental procedures attached to it. In science, this crisis opens up an epistemological revolution, in sociology it opens up a conceptual revolution, and everywhere it opens up a crisis of representation and of interpretative models of reality. It is therefore wise to flank any certainty with secondary interpretations which can then serve as a basis for a new conception of reality.

There too, it is possible to theorize several dangers of cognitive warfare into which it is easy to fall. The first is the accumulation of false certainties, by repeated induction or abduction, without possible verification. This leads to the development of a form of belief in an erroneous model. The second consists in using the accumulation of counter-examples to disguise one of them that will go unnoticed, for example by disguising a white crow as black. Finally, the saturation of analysis time lies in the culture of ambiguity, with all the ranges of grey crows. Preventive measures are all the more critical as they are difficult to anticipate.

4.11 THE LIMITS OF COGNITIVE POVERTY

Cognitive warfare is therefore the art of deceiving the brain or making it doubt what it thinks it knows. Its playground is the domain of the limits, constraints, and stereotypes of human thought, of false theories and of the culture of error in which it leads the opponent. The alteration of cognitive processes serves as a basis for a real action that is facilitated by the power of the digital. To conceive even this action is not easy. And it meets resistance from operators as well as decision makers. In this new war of theories, practices and doctrines are not evolving as quickly as technologies and the creativity of those who use or abuse them. For the time being, several problems are obvious.

The first of them is the problem of discretion and lack of sensitivity. The cognitive strategy is not public and it remains "local." We only notice its effects, and its validity is only established after the fact, often when it is too late. The second problem lies in the spontaneous incapacity of the human brain to conceive that it is itself subject to constraints, preferences, and limitations, which can be the object of external action. This incapacity implies that it is not because we know that we think badly that we will think better. Knowing that the two forms of Figure 4-9 are the same does not help us to see them as equal. And learning can do nothing about that. Nevertheless, we can pay attention to it and try to control our thinking or that of our collaborators, eliminating false certainties and valuing those that are proven.

Another problem is the easy confusion between the real world and the digital world. It is not because the digital world tells us about reality that it is anything other than a digital truth. It should be interpreted as well as possible for the most concrete action possible. This digital world can itself be the object of distortions, omissions of all or parts, or on the contrary of additions or spontaneous or induced illusions.

There is also a confusion between correlation and causality, or a confusion in the meaning of causality, due to the temporal confusion characteristic of human thought. It is spontaneously abductive, even inductive, whereas the only truth emerges from deduction. Reasoning or deductive verification takes time that is often not available to the actors. In many cases, the time allotted to reflection is limited, too short to mobilize rational processes, thus valorizing even more partially erroneous forms of thought, which nevertheless often prove to be effective. Here lies another danger. Repeated observations and habits of thought lead to a kind of conjurative, automated cognitive activity from which one cannot escape without discomfort, anxiety, or refusal of uncertainty. Cognitive biases are forms of intuitive reasoning that consist in minimizing improbable solutions and looking for spontaneous general laws from particular facts. This notion is opposed to a logic of systematic exploration that is both time-consuming and energy-consuming, and to which the majority of people refuse to submit.

Finally, the negligence of weak signals seems to be a cognitive constant. Generally speaking, it is a necessity, and those who are subjected to the prevalence of weak signals are incapable of normal thought. Yet, the details are often important and the "white crow" can be a major clue to the conduct of healthy thinking. Yet it is neglected, even denied. The negligence of weak signals is probably due to a Western culture of simplification by "trimming," the conviction of which has made the headlines of a certain "idea of the essential": "Occam's razor" has become the purveyor of a well-shared skeletal thinking. Weak signals are, however, the places where certainties evolve. It is in the edges that innovations emerge, and the devil is also often in the details. On the contrary, the obsession with detail becomes a handicap, channeling on it the attention left vacant for other elements, partial or global.

4.12 THE C2 COGNITIVE TARGET

The process of conducting military operations is referred to as C2. This acronym stands for "command and control." It is an organized set of regulated processes, adapted to the management of a crisis situation. It allows for the implementation and execution of a strategy that consists of transforming objectives into concrete achievements that contribute to the realization of a desired end state, thanks to the execution of adapted lines of force.

C2 is considered as a device mobilizing several bases of human intelligence (Alberts and Haye, 2006). Its core is a set of cognitive processes supported by three pillars: informational dominance, information processing security, and decisional superiority (Desclaux and Claverie, 2015).

C2 is the heart of the military machine, from information to decision for the respective minimization and maximization of concrete as well as immaterial forces and powers, those of enemies and allies. It is theorized as a true cognitive machine (Claverie and Desclaux, 2016). It is therefore the place of all fragilities, and it requires all attention and precautions. Those who neglect it will be the ones who regret it tomorrow.

Indeed, C2 can be applied to the handling of complex situations, such as industrial or ecological accidents, crowd management, or unilateral conflict, but it takes on a new dimension when it leaves asymmetry. The return to high-intensity conflicts would then become a C2 battle, and superiority concerns both the best strategy and the best conduct of the strategy. The cognitive error becomes a strategic alteration. This is one of the lines of force.

Cognitive warfare becomes a tool to reach, alter or influence strategic thinking as well as the cognitive elements of its implementation and future life. The aspect of decisional superiority becomes the privileged target, relying on the two other components of psychological and cyber action.

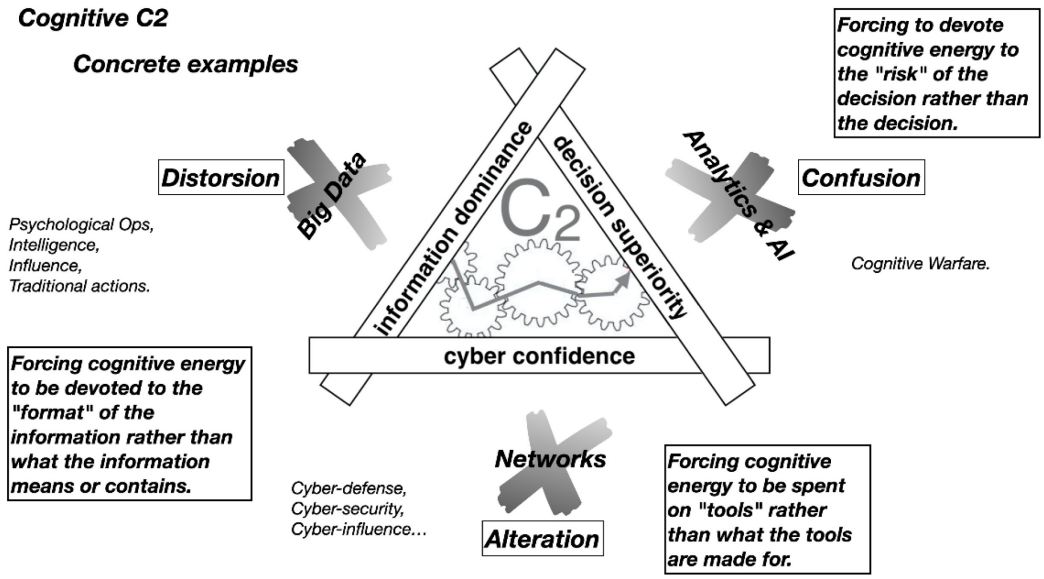


Figure 4-14: The Cognitive Triangle of "Command and Control" (C2) with the Three Bases of Informational Dominance, Cyber Confidence and Decisional Superiority Processes, Along with the Modes of "Cognitive Warfare" Action Using the Complementarities of PsyOps, Cyber-Influence and Cognitive Superiority, and Possible Modes of Attack. (From Claverie and Desclaux, 2016).

4.13 CONCLUSION

Cognition is the object of particular attention from strategists. It can be defined as the set of processes, mechanisms and actions that allow us to know the real world in order to act on it. Each of its dimensions is the object of particular interest in terms of military action and defence. Knowledge is necessary for action and action is necessary for survival, conquest, or dominance. It imposes filtering, memory, categorization, and semantic comprehension, as well as communication for their exchanges in the collective action. These are all dimensions of cognitive life. Meanwhile, action requires strategy, anticipation, and programming. Behavior is part of the necessary loop of control and of its representation for adjustment. The motivations are similar; dynamic appetite and cognitive appetite; move to grow and survive; move to live and know.

Why make it a content of war? Cognition is at the base of the action of the combatant as well as the commander. It is part of the dimensions of tactics and strategy. Cognitive warfare is a tool to reach the cognition of those who lead, make, or avoid war. In a way, cognitive warfare constitutes a three-dimensional set (information, numerical and decision) to reach the cognitive elements of the military operator's thought as well as the strategist's, in a psychological, cybernetic, and cognitive complementarity.

The natural and spontaneous cognitive resistance to admit that one might be affected or that education, training, or habit are inadequate to deal with cognitive distortions, as well as the energy and investment costs of parallel prevention processes, which are considered superfluous, are the two best allies of the cognitive warfare actor.

4.14 REFERENCES

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.

Chapter 5 – TRUST BETWEEN HUMANS AND INTELLIGENT MACHINES AND INDUCED COGNITIVE BIASES

Lieutenant General Gilles Desclaux[1]

"Humanity has learned a lot from the machines built by itself,
except perhaps how to live better with them."

The strategic field of crisis management is based both on knowledge of the most complete information possible, confidence in the best technologies that deliver them, and the decision-making ability of the commander who relies on a strong organization and effective.

In the context of massive information, these three dimensions require the development of so-called "intelligent" software agents capable of selecting, merging, and representing relevant information and of delivering decision-making solutions at high speed. These agents are developed by large industrialists; they are progressing steadily towards greater autonomy. Despite this progress and faced with an increasing complexity of the criticality of the situations, the project of purely autonomous systems is moving away from realistic prospects in the short and medium term. Experts in crisis management and these artificial systems must increasingly work in a collaborative manner, each bringing the best of their skills to the human-system duo. The notion of trust is therefore central for the I2HM (Human-System Interaction/Integration), and the collaboration between humans and machines. The strength or weakness of this collaborative relationship is a key security issue, and therefore one of the targets of cognitive warfare (Cyber Warfare).

5.1 HUMAN-MACHINE COLLABORATION FOR CRISIS MANAGEMENT

The management of defence systems or military operations is a field as complex as it is codified. One of the strategic areas is rapid crisis management. Doctrine, the law of war, the responsibility for minimal human attrition for adequate tactical material effectiveness limit the action of the decision maker who must nevertheless act quickly and well. Managing a crisis means mobilizing in the most effective way possible the means made available to imagine, evaluate and implement the most relevant measured and measurable solutions leading to a favorable solution as quickly as possible. Crises can be ad hoc, in place or in time, or more global and lasting, requiring adjustments or solutions whose complexity evolves with multiple evolutionary dimensions to be taken into account.

For this, knowledge is the real "fuel" for measuring, anticipating, and driving action. It is a major criterion of differentiation to control the criticality of situations. It is developed from masses of data which today exceed human capacities for global representation or comprehension and requires recourse to techniques using "Big Data," "Artificial Intelligence" and "Visualization" of potential and changing solutions upon which the decision is based.

In recent years, the development of "intelligent" software agents has progressed towards greater autonomy. Many obstacles remain to be overcome in order to achieve the prospect of real systems capable of effectively replacing human experts. In the near future, these experts and artificial systems will have to continue to "work as a team," in an even more collaborative way. The concept of "Human-Autonomy Teaming" (HAT) was proposed for this by NASA teams in 2018 (O'Neill et al., 2020) to account for this "strange collaboration," which mixes Artificial Intelligence (AI) and Natural Intelligence (IN). It contributes to the emergence of

[1] Gen. Gilles Desclaux is Air Force Lieutenant General (ret), president of RACAM (Civil Aviation – Military Aviation Interface). He is researcher at the Human Engineering for Aerospace Laboratory (HEAL – ENSC Bordeaux-INP / THALES, FR). There, he coordinates the "Anticipe" program: AI-human decision support processes for "Air C2".

hybrid, anthropotechnical systems, a form of dual and shared intelligence, which is not without posing concrete problems of fragility and reliability in the cognitive domain.

5.2 COOPERATION BASED ON DIFFERENT COGNITIVE PROCESSES

The decision-making process implemented by humans is radically different from that of intelligent machines. Identical cognitive architectures could facilitate communication, but unlike humans, machines are restricted to well-defined objectives and priorities, without the capacity for improvisation or interpretive adaptation, and without real inventiveness beyond the algorithmic proposition of unexpected solutions. Humans, on the other hand, can develop these qualities but remain mediocre in accurately describing their intentions, goals, and priorities as intelligent machines demand. Likewise, their capacities for attention, memory or reliability of reasoning are fragile and frequently compromised, whereas artificial systems are particularly reliable in this area.

Within a HAT-type "decision-making network," humans and machines continually modify their own roles, tasks, and relationships with other actors, natural and artificial, partners and external alike. This activity is called "centered networks." When the usual processes do not seem to correspond to their expectations, new strategies are implemented: machines open procedures for consulting external databases, while humans form or restructure informal or ad hoc working groups and are looking for new experts.

Intelligent machines remain and will remain, at least for the foreseeable future, partially incomprehensible to humans. It is obviously the same with humans for machines. Establishing trust between the two types of entities is therefore difficult. Intelligent machines are susceptible to cyber intrusions that can compromise their "perceptions," the relevance of their "decision making," and their data management and communication capabilities. Humans have other weaknesses, such as fatigue, limited memory, and fragile and easily influenced cognitive abilities. In such a context, one solution is to foster the establishment of constructive performance monitoring relationships between human experts, between machines and, in both directions, between experts and machines.

5.3 THE PROBLEM OF INTERPRETABILITY

Interpretability has two dimensions. The first aspect corresponds, for the user of an automated or autonomous system, to the user's degree of understanding of what the system does, how it does it and why it does it. The interpretability of the system can lead to the development of a cognitive model that is as complete as possible in order to provide an understanding of how it works, and the ability to predict what it would do under certain circumstances. Two approaches make it possible to facilitate interpretability:

- System feedback improves the experience of interacting with users and facilitates their sense of control. Users usually want the system itself to provide understandable information about its own level of trustworthiness, in order to know whether to trust it or not.
- The post hoc explanation, known in the English-speaking world as eXplainable AI (Adadi and Berrada, 2018) or XAI, provides the user with an explanation that justifies the decision making, thus making the system more interpretable and facilitating feedback (Retex).

The second aspect, interpretability, concerns the limitation, for the user or the human partner, to behaviors or decisions that are understandable for the machine, or consistent with its own knowledge registers. This limit is necessary to maintain the effective collaboration link. This dimension is not without problems of acceptability for naive human users, who must learn to collaborate with machines to facilitate the competence and maintenance of the efficiency of the HAT system. Here again, the learning systems are frequented by experts and must be able to identify them in order to adapt to their peculiarities and the specifics of their cognitive characteristics: personality, age, greater or lesser mnemonic performance, visual

or formal, sensitivity to sounds or images, field dependence or independence, attentional saturation, resistance to fatigue, stress control, etc. To address this issue, the use of portable technologies (wearable tech.), sensors and auto-quizzes on tablets is now being studied by the laboratories of the US Army (Buchler et al., 2016) and within the framework of collaborations between certain industrialists and university or defence engineering schools in NATO countries.

Although this avenue is still exploratory, we can expect to see technologies capable of facilitating the collaboration and efficiency of the human-system pair and the performance of the mission in terms of making the human partner recognized and identified by the machine, and continuously informing the machine of the evolution of the human partner's cognitive state and his knowledge.

5.4 THE ASSESSMENT OF UNCERTAINTY

To date, most decision-making automations work well for specific situations, and for which they are designed, but require the use of human expertise when it comes to managing situations outside certain defined or limited environments. In particular, when computer algorithms are confronted with uncertainty and ambiguity in data, they are often overwhelmed by decision making.

Humans surpass machines in understanding context. Machines remain incapable of exercising nuanced judgment in complex or ambiguous and evolving environments. Additionally, as machines are programmed or trained using sets of information relevant to a specific task or problem, encountering a new problem tends to lead to ambiguities or even to failure. The human capacity to adapt to new situations is much greater and even incomplete or imperfect responses are likely to perform well. Humans use mental surrogate abilities and estimations from familiar skills or tasks, and can thus provide approximate answers, which AI technologies are not yet able to do.

Humans also surpass machines in their ability to assess the quality of their cognition. Metacognition is a hallmark of the human mind. It escapes the machine for now. Work is being undertaken in order to understand the cognitive expertise of this human phenomenon, to give it a structure that can be understood by the machine, and to endow the machine with "metaprogrammatic" capacities to evaluate itself, to be able to evolve, and especially to evaluate human cognition in order to adapt to its evolution or its performance in a dynamic HAT relationship.

5.5 LACK OF TRANSPARENCY

When stand-alone systems lack understandability and predictability, there is a problem of lack of "transparency." This notion refers to the inability of humans to understand why the system takes such action or, on the contrary, does not take the decision of an expected action. Lack of transparency produces a lack of awareness, in particular it does not allow operators to know what information is used to perform a task.

This lack of transparency is sometimes the origin of a lack of trust which leads both to underuse of the system through mistrust or on the contrary to overuse due to blind trust (Clark et al., 2014). This confidence problem must be able to be assessed on an objective basis, with clear indicators.

These areas of difficulty are not independent problems and can combine in often dangerous ways (Endsley, 2016). Intelligent systems are fragile, and can quickly go from good operation to rapid, global degradation. It is therefore the responsibility of the human operator to monitor the occurrence of such failures, and to anticipate their consequences. But monitoring a system that appears to be working properly is a job that humans are ill-prepared for. We are talking here about phenomena of "taking out of the loop," or "OOTL" (Out-Of-The-Loop, in English – cf. Suhir, 2021), which induce a restricted awareness, even very reduced of the situation (Endsley, 2015).

5.6 TRUST AT THE HEART OF THE HUMAN/INTELLIGENT MACHINE RELATIONSHIP

In the HAT context, trust must be examined at two levels.

For the machine, the quality of the relationship is based on statistical algorithms for psychophysiological monitoring or on the quality and quantity of information exchanged. Monitoring human partners can allow the implementation of automated processes or operator reminders. This type of process is particularly studied in driving assistance and the detection of sleepiness or loss of driver attention, but also the non-detection of imminent dangers (pedestrian, obstacles, ice, etc. .). The required computational formalism requires a cognitive model of the driver (Bellet et al., 2011). The cyber defence of these programs remains one of the major concerns in view of the need for continuous evolution and updating of software.

For the human partner, trust is generally defined as "the degree to which a user believes that a system will behave as expected." Without this appropriate level of trust, operators may refuse the use of stand-alone systems or, on the contrary, completely offload onto them. These phenomena of overdependence that can lead to failure, followed by underdependence on automation, are well documented. The main factors that promote the development of trust are acceptability, tolerance, transparency, and the bidirectional nature of Human-System communication.

Confidence depends on the specific context of a human/intelligent system interaction and is influenced by the environment and the mental state of the operator. The perceived usefulness of an autonomous system in terms of the ability to perform a difficult or demanding task influences an individual's decision to trust it. But operators with a high workload also tend to rely more on the machine, regardless of their actual level of confidence in the system. The automaton, apart from simple tasks, generally does not completely replace humans. On the contrary, he changes the nature of his work by relieving it of certain tasks for which he is more efficient. This clearly poses the problem of reciprocal acceptability. The understanding, usability, and expectation of users of an intelligent system are correlated with the likelihood of trusting.

Confidence is built over time, and as a result, for the human partner, education and training foster the familiarity necessary to use the system. As for the artificial system, it must now be programmed due to the lack of scalable algorithms, or even adaptive machines.

5.7 COGNITIVE BIASES IN THE HUMAN-AUTONOMY DUO

Transparency is what allows the operator to determine if the autonomous machine is likely to provide the right response in a given complex situation. Transparency allows the machine to know if the information given by the human is trustworthy, or contain incongruities that need to be clarified.

But this transparency goes beyond the simple provision of information to the human operator or to the autonomous artificial partner. To be transparent, the automaton must present the information in a way adapted to the mental model of the operator, taking into account the operator's preferences and cognitive constraints, while, conversely, the human partner must adapt to the mental model of the program designer. Therein lies a first cognitive bias: the machine is not a partner like any other, it has been programmed by someone. It can also be deprogrammed, reprogrammed, be influenced by patches or additional programs, and therefore viruses, Trojans, and other malware. This cognitive dissonance bias is all the more, thanks to the fact that it imposes itself without any real solution, in the face of computer scientists or industrialists convinced that their way of thinking is the best for others.

Cognitive biases are spontaneous distortions of the rational thinking that humans adopt and which are the source of many errors (Kahneman and Tversky, 1974). They are studied by economists and psychologists,

especially with regard to decision making, but they are the subject of new attention from these experts and those of information processing, with the study of machine bias (Bertail et al., 2019) and the algorithmic creation of inequity, or even discrimination, posing unavoidable ethical problems.

In the context of big information, and for the users of the systems, humans most often focus on sources and methods of selection that they know well and trust, thereby introducing a different dreadful type of bias. This is an area where machines are nevertheless very efficient, providing a high speed of acquisition and processing of large volumes of information, as well as consistent, rigorous, and impartial data management. But without a level of transparency that makes it possible to recognize the sources of information and analyze their quality, the effectiveness of such systems will remain insufficient, and doubt remains underlying the relationship between humans and machines.

An example illustrates this notion. A semi-autonomous system presents several options that it has generated, along with evaluations of potential effectiveness as to the adequacy of each. Such a transparency facilitation device must be accompanied by a capacity for the operator to add information that the autonomous device does not know. The operator must be able to suggest solutions and have them evaluated by the controller. Collaborative problem solving is therefore a back-and-forth, "Wargaming"-type process. This type of two-way communication promotes partnership and helps assess favorable solutions to potential problem solving.

A third type of bias concerns the spontaneous feeling of human superiority over the machine. A low level of cognitive engagement makes it inherently difficult for an operator to understand what is going on when he is only performing passive surveillance of an autonomous system. Passivity in performing a task is then an obstacle to the effectiveness of intelligent human-machine interaction. This challenge depends on what some authors (Endsley, 2016) refer to as the "automation conundrum." Thus, the more automation you add to a system, and the more reliable and robust this automation is, the less likely it is that human operators will oversee it. They will then be unable to understand the situation and will tend to regain control of the system. The system then becomes degraded, restricted to the simple limited capabilities of the operators, which is obviously a significant advantage for the potential enemy. The automation conundrum creates a major obstacle to autonomy in areas where security is critical.

5.8 CONCLUSION

Today, the complexity of crisis management requires processing a large amount of data and making critical decisions in ever shorter times and increasingly constrained contexts. Decision makers at the head of crisis management organizations must therefore increasingly rely on hybrid systems. The help of intelligent systems has become indispensable. Despite the indisputable performance of such systems, they are still uncertain in several areas, and humans, who will continue to play an important role in this collaboration with machines, have a tendency not to master a set of biases generated by the exchange HAT. Ways forward lie on the one hand in the capacity of these machines to better explain, to establish a supported confidence, to communicate more easily, even to understand the hidden intentions and the emotions of the human actors, and on the other hand in a new culture of acceptance of machines by humans.

In a seminal article (2017), Kott and Alberts wrote, "Welcome aboard smart things. Whatever our respective shortcomings, we will be stronger and more agile by working together in decision-making organizations."

5.9 REFERENCES

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., Irandoust, H., Lange, D., Genchev, A., Cakir, M., Verstraete, E., Brill, J.C., Desclaux, G. (2022 in press), Human Considerations for Artificial Intelligence in Command and Control. H. Le Guyader (Ed.). 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 Oct 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.

Chapter 6 – TECHNICAL MATURITY OF HUMAN NETWORK COGNITIVE SYSTEMS

Dr. Norbou Buchler[1]

"Human collaboration and team leadership structure are critical to managing complex technical systems and coordinating effective responses to threats. The notion of maturity of technological solutions for human use (Human Readiness Levels: HRLs) is essential in this context."

6.1 TRENDS IN NETWORK DEVELOPMENT

A first trend is the development of the networked organization. Advances in information and network technologies are significantly transforming the way human organizations operate and communicate. These networked organizations are at the heart of the social, political, military, or economic fabric of the 21st century. Managing and safeguarding the systematic convergence of people, information, and technology is one of the key challenges of our time.

This transformation to distributed network operations is quite recent and has occurred rather rapidly. For military organizations, it took place at the turn of the century, around 2003 for North American countries and their NATO allies, and has impacted many of us, profoundly changing the specialties and even the careers of specialists.

Socially, networked operational environments are massively collaborative: the number of potential collaborations is virtually unlimited. However, they have potential disadvantages such as increasing complexity, and the deluge of information in these networked environments can quickly overwhelm human cognitive abilities. The ongoing challenge is to get the right information to the right person at the right time.

The second trend is one of increasing autonomy: the nature of work is constantly changing due to the blistering pace of technological change. This includes tools and systems of Artificial Intelligence and Automatic Assistance technologies (AI/AA) that are increasingly capable of operating on their own and in concert with human operators.

In military organizations, a major focus remains the interaction of human operators and their tools. Some key aspects underlying this transformation of the Human-Autonomous Agent (HAT) team are calibrating trust levels of the relationship and its transparency, especially with respect to underlying assumptions, uncertainty, and reasoning processes.

Both humans and machines have their strengths and weaknesses. Ultimately, a key marker of the success of this combination is that levels of performance are being achieved through human/machine collaboration that could not previously be achieved without a full and complementary human/machine partnership. One of our concerns remains that the rapid development and complexity of modern artificial intelligence limits our ability to intuit and imagine the future impacts of using new technologies. We still need a lot of experience and experimentation to succeed in this.

The third trend is "Cognitive Warfare" which leverages cyber-attacks, Big Data, and social media for destabilization purposes. Cyber security threats are based on malware, Trojans, and botnets. The convergence

[1] Norbou Buchler holds a PhD in experimental psychology researcher, specialized in cognitive neuroscience (functional MRI) and computational modeling. He works at the Human Systems Integration Division of the U.S. Army Combat Capabilities Development Command (DEVCOM) Analysis Center – Aberdeen Proving Ground, Maryland USA.

of cyber, physical, and social environments is also a place of weakness, with massive attacks on a large scale that specifically target the seams and boundaries of these cyber, physical, and social networks.

The impact of artificial intelligence that leverages large databases and social networks is a major threat. It enables Cognitive Information Warfare (CogIW) on an unprecedented scale to destabilize democracies and undermine alliances. The stealth of attacks, lack of attribution of cause or perpetrator, deception and consequent distrust undermine the social fabric.

The NATO-ACT paper by Cole and Le Guyader (2020) draws our attention to the AI-supported "human domain" (future monitoring and surveillance of allies), sounding an early warning against the destabilization of CogIW campaigns. A broader theme might be about safeguarding digital democracy and bringing cyber-social safeguards such as online authentication of citizens for participation in digital democracy.

6.2 THE INSTITUTIONAL DECISION-MAKING PROCESS

This question echoes some of the work of Dr. Alex Kott, Director of Science at the U.S. Army Research Laboratory, entitled "Breakdown of Control." His thesis draws on Control Systems theory and uses historical examples to argue that deception and mistrust within an organization forces compartmentalization and verification measures that significantly slow and impede action and decision making, causing a "breakdown" in organizational decision making (Kott, 2007). These include late decisions (delays), changes in decision thresholds in information warfare, excessive inhibition (timidity) or aggression – low or high gain, self-reinforcing errors, as in feedback loops. See also Kott (2008), Kott and Alberts (2017), Kott and Linkov (2021), Theron, Kott et al., (2019).

The second question concerns our own coalition's decision-making imperative to mitigate the previous threat. How can a well-designed, equipped, and trained organization avoid being hit by such an attack? With its own equipment, this organization can anticipate and respond decisively. Two complementary dimensions are defined here, which are on the one hand the contributions of training and technology, and on the other hand predictive models, human mental models or programmed digital models.

One conceptualization of the military decision-making cycle is known as the "OODA loop" for Observe – Orient – Decide – Act. Also known as Boyd's cycle (1976), it defines a time-competitive process by which an individual or organization observes and orients itself in an operational environment and repeatedly and iteratively makes decisions in light of dynamic events, while acting effectively. It is a useful framework for thinking about organizational functions, workflows and supporting technologies.

We can comment on four different technical areas that support the issue of human decision making and organizational effectiveness (Figure 6-1). These areas ultimately support mission effectiveness.

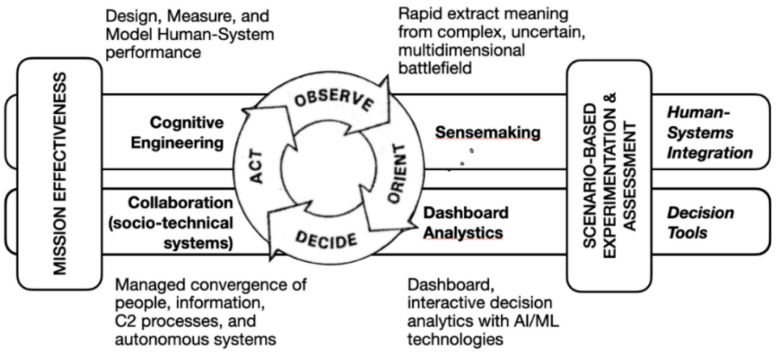


Figure 6-1: Human Decision Making and Organizational Effectiveness Aligned to the Military Decision-Making Cycle (OODA Loop).

One can point to the importance of cognitive engineering and human-systems integration. Nevertheless, the majority of this chapter will focus on collaboration and more specifically, the cognitive dimension of networked human systems.

6.3 FROM TRL TO HRL OR "HUMAN READINESS LEVELS"

The U.S. Army Combat Capabilities Developmental Command (DEVCOM), and within it the Analysis Center, are interested in ensuring that technology development is well aligned with the needs of the soldier. This means ensuring the maturity of the adaptation of technologies to human users (see Figure 6-2).

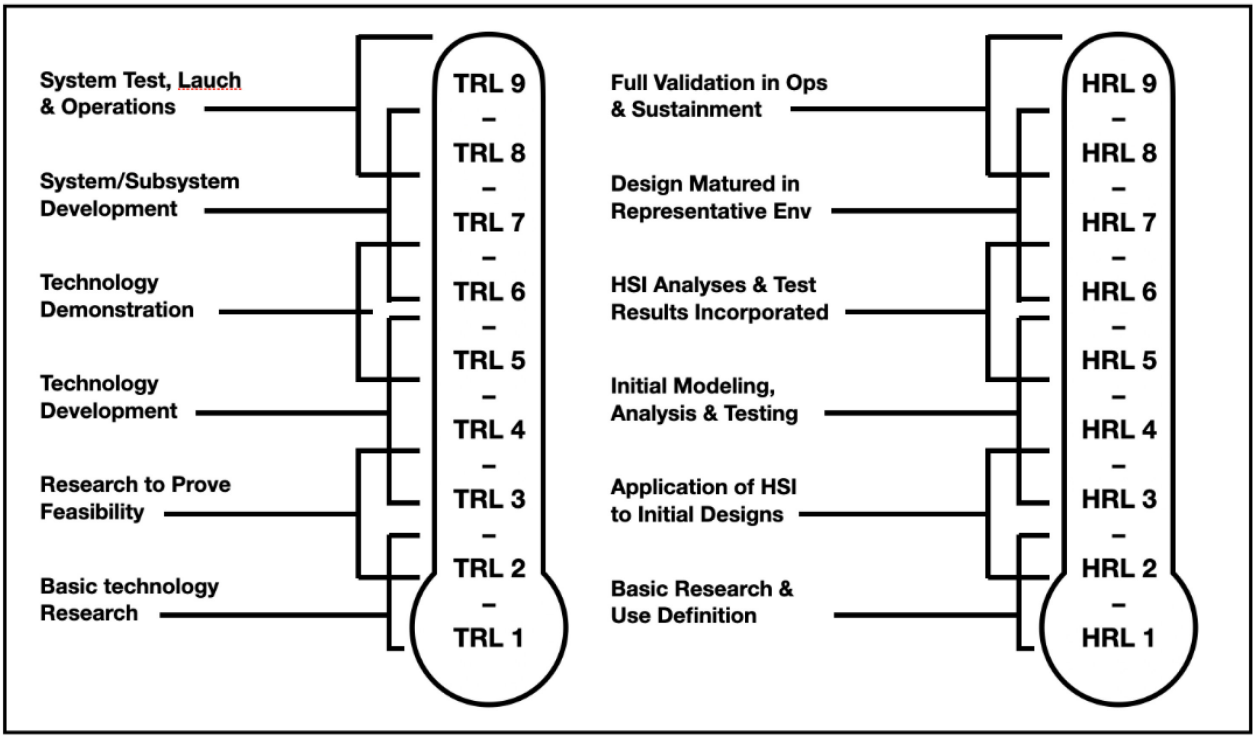


Figure 6-2: Equivalence Between the Two Scales of Technological Maturity (TRL) and Maturity of Technological Solutions for Human Uses (HR).

The term TRL, or Technology Readiness Level, has been around since the 1970s, and refers to the level of technological maturity of a given piece of equipment or software, ranging from the first level of concept development through development and operational testing to prototyping (ISO, 2013). One of the key challenges in developing technology is to ensure that it takes into account the human and organizational dimensions of their use; and this is particularly the case for artificial intelligence and complex systems to support Cognitive Warfare.

Dr. Pamela Savage-Knepshield (Savage et al., 2015) is developing the use of the notion of Human Readiness Levels (HRLs) that mirror the logic of TRLs for an easy understanding of human-system integration maturity (Handley and Savage-Knepshield, 2021). This index provides a single number for assessing communication readiness for human use. For each level, there are both input and output criteria.

HRL applies universally, from technology science programs to systems acquisition. This ranges from early identification of human performance-based requirements to user interface design and refinement, through successive user evaluations and full operational testing by humans (Savage-Knepshield et al., 2021). In 2021,

the American National Standards Institute (ANSI) and the Human Factors and Ergonomics Society (HFES) accepted Human Readiness Levels (HRL) as a current standard, made available at (https://www.hfes.org/Publications/Technical-Standards).

The HRL scale provides questions that serve as triggers to consider applicability of multiple human-system integration topics throughout design and development. Ultimately, the HRL scale supports iterative evaluation of human-centered domain principles and provides a single 'human readiness' number to support program decision-makers.

6.4 BEHAVIORAL OBSERVATIONS LOGGING TOOLKIT

In terms of Cognitive Engineering, the analysis center is also moving towards the digitization of surveys and behavioral observation data.

A digital toolkit has been developed for the study of all behavioral observation data. It is called the Behavioral Observations Logging Toolkit or BOLT.

The BOLT system is based on a four-step logic (see Figure 6-3). It provides a technological leap in Human-System Integration (HSI) analysis over current mainstream technologies that, even when using handheld devices such as smartphones or tablets, require transcription, are not real-time, do not aggregate data from multiple observers, and do not provide global visibility to leaders of current operations. The logic of the BOLT system is to provide an online representation that allows for the evaluation of training, technology, and operations by supporting all human expert observers, streamlining data collection, tracking, and analysis of information without delay (Garneau et al., 2020).

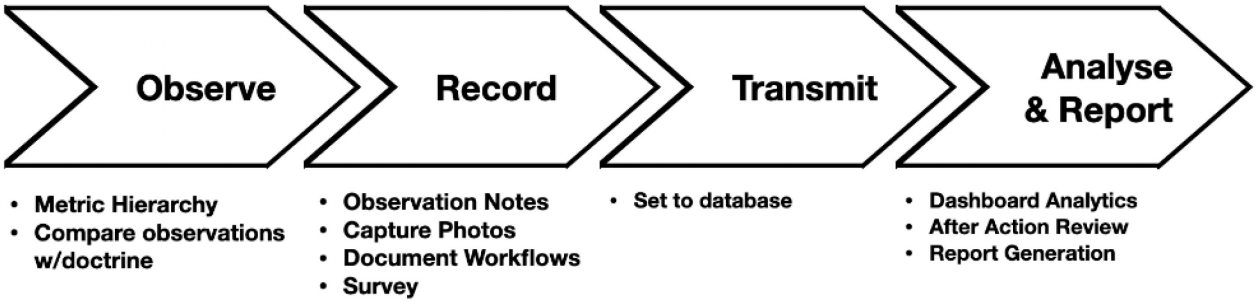


Figure 6-3: Principles of the BOLT Digital Tablets (Behavioral Observations Logging Toolkit).

6.5 COGNITIVE NETWORKS AND THE COGNITIVE WARFARE AS NETWORK SCIENCE

As in the Wachowskis' movie "Matrix," we can choose the blue pill, and see nothing, or the red one to open our eyes and explore the world as a series of interconnected networks.

Figure 6-4 is from the U.S. Army Field Manual FM 3-13 "Inform and Influence Activities" (2016). It shows six types of networks that span the Political, Military, Economic, Social, Infrastructural, and Informational (PMESSI) domains Individual nodes can represent people, places, or equipment.

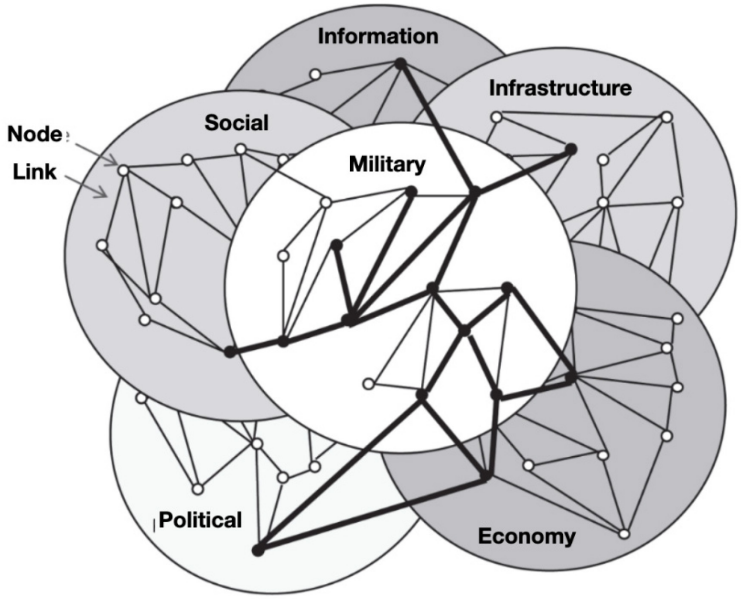


Figure 6-4: Enhance Capabilities of Soldiers and Commanders to Leverage and Safeguard the PMESII Dimensions to Inform and Influence an Increasingly Complex and Interconnected Operational Environment (from U.S. Army Field Manual, FM 3-13 – Inform and Influence Activities).

Cognitive Warfare involves mapping all of these different types of networks and exploiting the critical interdependencies that exist between them. For example, in 2015, a Russian sought to destabilize the Ukrainian capital of Kiev with a multi-layered attack. A cyber-attack knocked out critical electricity infrastructure, leaving 200,000 Ukrainians without power in predominantly Russian neighborhoods, and was quickly followed by a disinformation campaign blaming the outage on the Ukrainian government. This hybrid attack was carried out on 3 networks: Infrastructure, Social, Information.

More specifically, our applied work focuses on how to map and understand three of these networks – the military, cognitive/social, and informational networks.

The military transformation of the United States and NATO countries has taken place within a conceptual framework known as "Network-Enabled Operations" (NEO) developed by Alberts et al. (2004). It provides a relevant conceptual framework for understanding human cognition, collaboration, and organizational effectiveness in the military domain. It includes four main principles:

- A strong networking force improves information sharing and collaboration.
- Such sharing and collaboration improves both the quality of information and shared situation awareness.
- In turn, this improvement allows for additional self-synchronization and improves the sustainability and speed of command.
- The combination of these factors significantly increases mission effectiveness.

This framework is cumulative, so communication and information sharing act as a positive feedback loop. Increased information sharing leads to greater shared situation awareness. This, in turn, promotes organizational adaptations such as self-synchronization that ultimately increases overall mission effectiveness. (Alberts and Garstka, 2004).

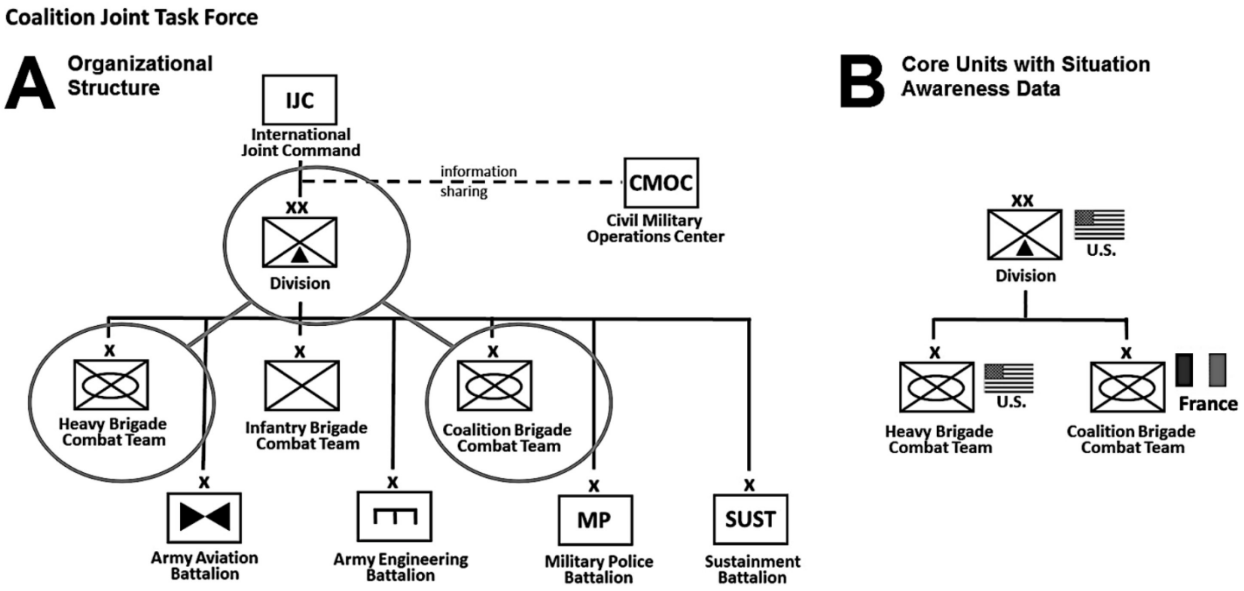


Figure 6-5: (A) Organizational Structure of the Coalition Joint Task Force During the Experiment. The network organization spans several levels, from the Joint Command to the Division, including the brigade and support battalions. (B) Units practiced: division Mission Command, and two subordinate brigades.

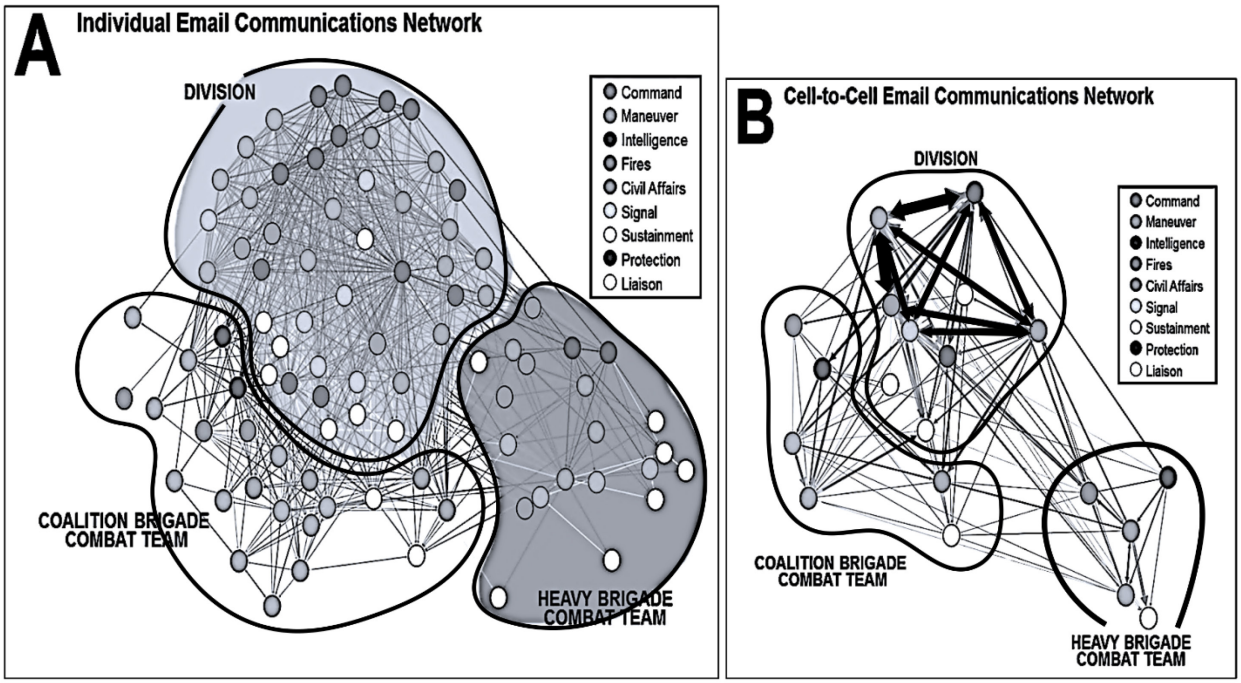


Figure 6-6: Intra and Inter-Unit Communication Network (Three Structures in Figure 6-5). The color of the cells indicates the functional roles and the thickness of the lines indicate the functional cell of the sender and the volume of the message.

6.5 FORT LEAVENWORTH

In 2016, we focused specifically on the first two principles (Buchler et al., 2016). We examined information sharing and situation awareness during a large-scale military exercise at the Mission Command Battle Laboratory at Fort Leavenworth, KS-USA. A network science approach based on graph theory of collected communications was applied to the entire coalition joint task force organization.

The hypothesis was that "increased information sharing leads to increased situation awareness." The experiment was conducted during a two-week Mission Command Training Exercise (MCBL: Fort Leavenworth, KS).

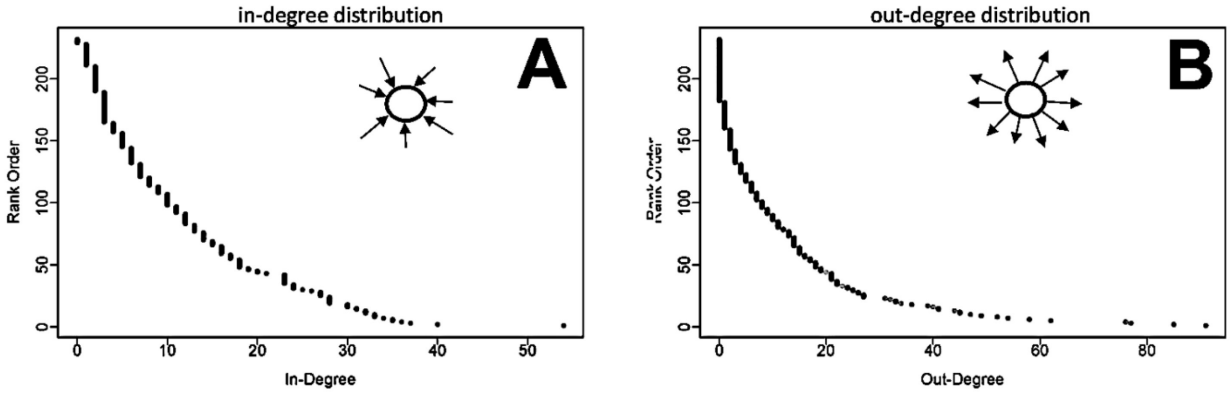


Figure 6-7: Cumulative Communication Distribution Functions of Email Inputs (A) and Outputs (B) for the Entire Communications Network. The predominance of some command personnel is evident when expressed as a percentage of all ties.

The three basic units trained in enhanced and equipped communication consisted of Mission Command personnel from one U.S. division and two participating subordinate brigades, one U.S. heavy brigade combat team, and one French coalition brigade combat team.

Individual Situation Awareness data were collected using the SAGAT methodology from participating staff at these three base units, and data processing used "Graph Theory" Analysis on all email communications and Situation Awareness data (collected by quiz).

Email communications are aggregated at the cell level to reveal cell-to-cell functional matches (A) and recombined at the individual node level based on the amount of information exchanged (B).

We observed Pareto imbalances in information sharing within Mission Command's communication networks. Of the 250 people in the network, we find that key individuals at the tail end of the Pareto distribution dominate collaborations. Most individuals, who constitute what we call the "trivial many," have only a few interactions, while a few individuals, who we will call the "vital few," have a very large number of interactions and occupy a dominant place in the interaction network. From a systems perspective, these individuals are most likely to experience cognitive overload and should be the primary beneficiaries of assistive automation.

The study of Situation Awareness was conducted using an electronic "Pop Quiz" based on Endsley's (2000) model of important mission events and developed using a goal-oriented task analysis methodology. It allows for the objective measurement of each individual's SA. These results are analyzed in relation to the previous communication study.

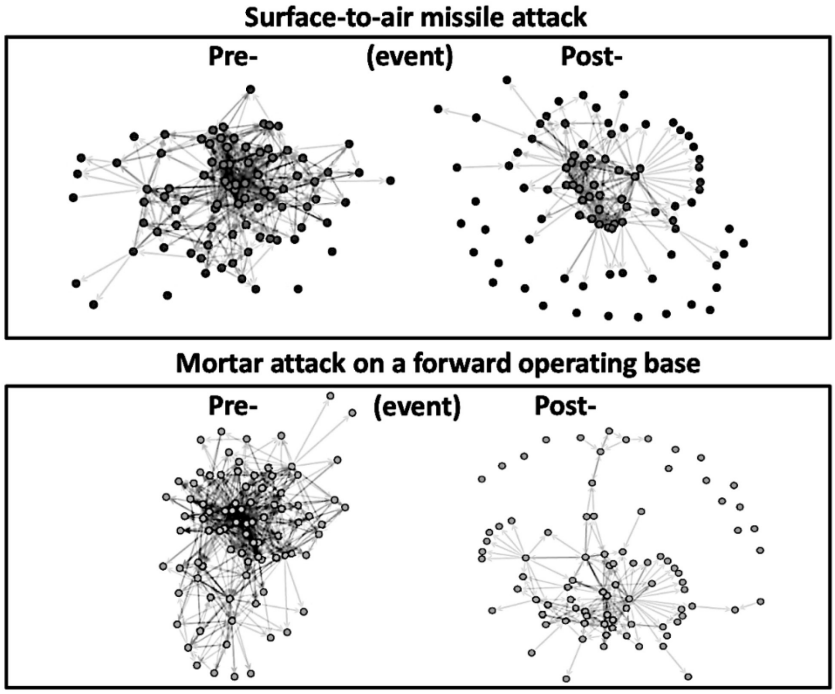


Figure 6-8: Examples of Reorganization of Unit Command Communication Networks According to Shocks (Pre- and Post-Critical Event: Missile or Mortar Attack).

The results are detailed in Buchler et al. (2016) and highlight challenges faced by networked military organizations: robust but uneven information sharing, sources and "information sinks," clearly stratified situation awareness, and that information sharing does not always increase situation awareness.

There are still questions that need to be answered. How does the network react to shocks or adverse events? What kinds of organizational adaptations occur (e.g., self-synchronization)? (Fitzhugh et al., 2020). For example, what is the evolution of situation awareness as a function of network reorganization following a shock?

One observational feature concerns the existence of "emergent coordinators" and their role in network reorganization. These roles are unformalized, and each event produced the release of 2 – 5 emergent coordinators (Buchler et al., 2018).

6.6 CYBERSIMULATIONS DEVCOM

We were able to study the behaviors of teams of actors during three episodes of a cyber competition, the "U.S. Collegiate Cyber Defense Competition" (CCDC 2016, 2017, and 2018 – www.nationalccdc.org). Our goal was to understand what combination of skills or tools, team dynamics, and leadership style makes a team more or less effective, through the objective measurement of mission effectiveness.

The strategic question was how to study what makes one team better than others. The scenario pitted teams of attackers (the reds) against teams of defenders (the blues) and was designed to foster team-based cyberwork. The simulation environment provided a sufficient degree of realism, with experimental control through performance outcome measures.

The task was broadly consistent with the performance of information security professionals. It consisted of keeping the services that must remain efficiently managed, available, and operational. Teams were required

to complete assigned tasks within a given time frame, such as creating policy documents, making technical changes, attending meetings, responding to incidents, i.e., analyzing cybersecurity incidents and submitting reports, and thwarting adversarial cyber-attacks.

Measures of team quality and performance were sociometric data, with wearable sensors measuring interactions between team members, a survey given to team observers (in 2016 and 2017) to assess the degree of collaboration and leadership style of the team, and skill measures from survey given to the team of defenders to assess experience, communication style, tasks/roles, and team structure.

Factorial analyses on the survey data were conducted based on the three group categories: failure by storming (ranked low), normal (ranked medium), successful (ranked high).

It can be seen that group dynamics evolve over time in a manner consistent with a form of "team maturation" according to Tuckman's (1965) "Forming, Storming, Norming, and Performing" model. This model describes the stages that a team goes through, from the moment a group meets for the first time until the end of a project. In addition, team members evolve in parallel as they progressively reach the status of colleague. The performance of the team depends on the success of this maturation.

The results (Buchler et al., 2018) are summarized and presented, for two competitions, in Figure 6-9. They confirm the need for team structuring with a probable maturation of shared situational awareness as a function of the progress of the experiment with a sequential stage model (Tuckman model). They indicate that the leadership dimension and face-to-face interactions are important factors that determine the degree of success of a team. On expert teams, everyone knows what to do. These high-performing teams exhibit less face-to-face interaction. In addition, it is observed that the factors of good performance vary according to the type of task asked of the team, reflecting the agility and adaptability acquired by a mature team. Thus, it appears that functional specialization within a team and well-guided leadership are significant predictors of detection and speed of effective response to shocks, in this case cyber-attacks.

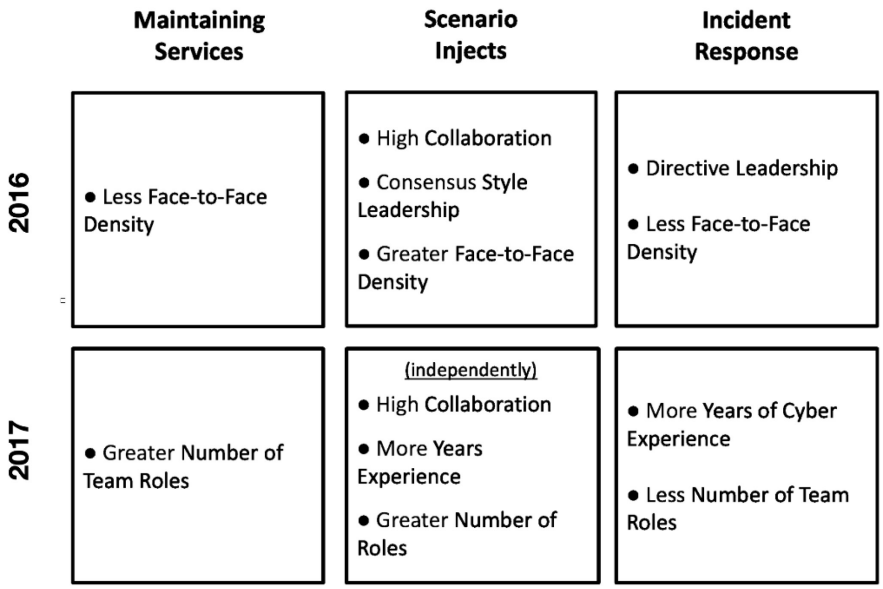


Figure 6-9: Results of the DEVCOM Experience.

Given the quantity and depth of skills needed to perform well in the cyber domain, these predictive measures give us some insights to support the development of good cyber teams.

6.7 CONCLUSION

These two studies converge in our belief that resilience to attacks, and especially to cognitive warfare, requires training teams and establishing normative work routines for performance by coaching teams to a high level of maturity.

Human collaboration and team leadership structure are critical to managing complex technical systems and coordinating effective responses to threats.

This research has also shown the utility of wearable technology metrics collected during the workday: automatic capture of face-to-face human interactions via infrared sensors, conversation times and voice characteristics of exchanges, physical proximity of employees, and spontaneous physical activity levels captured by accelerometers. Rapid advances in wearable technology and physiological recording are a boost to research, but also to the management of teams working in environments whose characteristics can also be detected online, such as communications. The efficient analysis of "big data" is also a favorable factor.

At the same time, we can bring these studies closer to the theory of decision making with the OODA loop to promote resistance and cognitive performance (see Figure 6-1), with the proposal, in addition to the TRL and HRL scales (see Figure 6-2), of a "Cognitive Technological Maturity" scale built from data on "Human-System Integration" (HSI) and the structuring capacity of the teams in which the operators using the systems are involved.

Figure 6-10 represents, in this scale, the state of the situation of the teams of the current forces and the point of agile adaptation and intelligent organization towards which the forces of the USA and its NATO allies must tend. This goal must be achieved through a coordinated effort of increased collaboration within teams, but also across teams, domains, and nations, and through the development of relevant human metrics to ensure effective human-system integration.

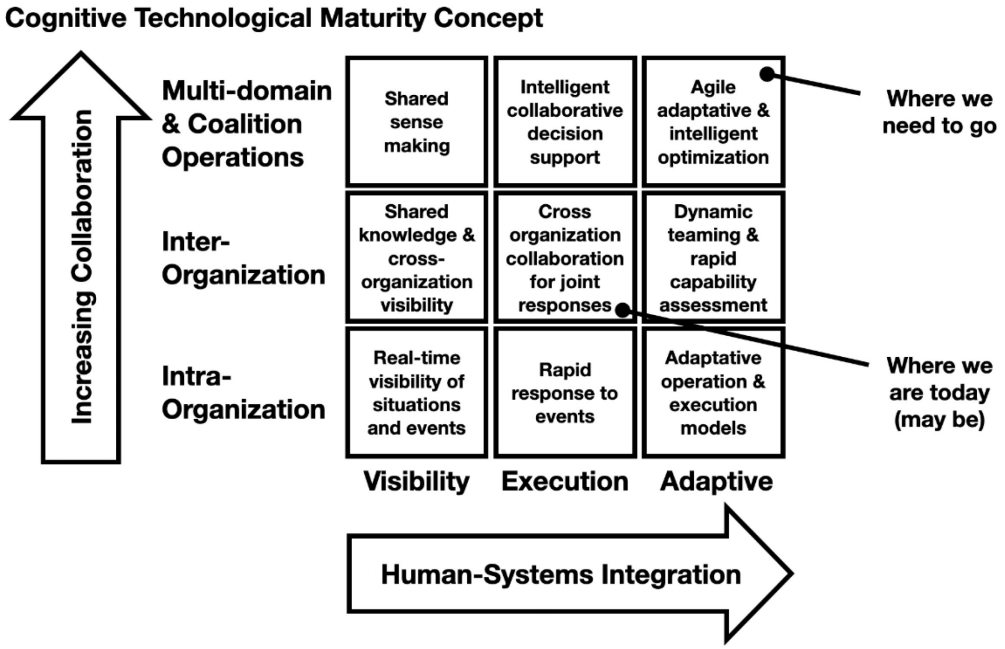


Figure 6-10: Concept of Cognitive/Technological Maturity Concept (inspired by Lin et al, 2004).

6.8 REFERENCES

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 December 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 April 2021 (in press). 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.

Chapter 7 – NARRATIVES OVERWHELM THE WORLD: A "BRIEF HELLO TALK"

Dr. Michael Wunder[1]

"We are in fact at war – the war of information – a kind of perfidious war."

7.1 SITUATION

Narratives are helpful to underpin shorter statements. Narratives are not malicious in general and are a typical instrument for commercials or politic campaigns. It is very helpful to refer to an existing narrative when there is limited time for detailed explanations, like in television interviews, short articles, advertisements, headlines, etc. The theory behind narratives and commercials is old and was already used for trading of commodities and other economic goods many decades ago – remember the Marlboro Man and his well-constructed image of a free man and cool smoker.

An important notion is that people tend to concentrate their attention on narratives that comply with their basic understanding, their firm beliefs, and their heart's desires. They can be fortified but not inverted. At best, the changeable minds can be convinced and attracted. This is one of the conditions of a successful formation of solitary social communities and echo chambers.

Relatively new is the extended reach by use of social media and the speed of sharing narratives. The most important drivers are the technical innovations that internet companies have created to establish their business models – the so-called algorithms.

Nowadays, narratives and their dispersion by algorithms are closely linked. Before the internet age it was expensive to design, launch and maintain an effective information campaign, now it is cheap and requires relatively low technical equipment and just a few skills to widely disperse information via social media.

This describes exactly the business model of the internet companies who provide sophisticated toolboxes for all customers who want to sell something – and offered products are not at all limited to physical goods. The algorithms can be adopted to best fit one's fields of operation and they can be fine-tuned to meet the needs and wishes of consumers. By collecting Big Data and exploiting all footprints that consumers leave on the internet, the picture about a customer becomes very complete and allows predictions to be made about the customer's behavior and developing interests, thus making advertising no longer annoying, but rather desired or at least unnoticed and thus very effective. And of course, the internet companies apply all the modern high-tech tools like AI-based social media exploitations and forecasts.

7.2 THREAT

Internet companies maintain a very strong, robust, and extremely profitable business model and thus have no real interest in changing the situation. It is most likely an illusion that they can be motivated to filter and dismiss dubious customers. Single bans for prominent users of services are public-oriented but cannot prevent general misuse.

[1] Dr. Michael Wunder is a mechanical engineer with the main focus on process engineering. His thesis was about the economic growth of the steel industry. He served as system analyst at the automotive industry and followed by a position as Director for IT at an automotive supplier concern. Currently he is Director of the Department "C2 & Intelligence" at the Fraunhofer Institute for Communication, Information Processing and Ergonomics – FKIE – in Wachtberg (Germany). In parallel Michael Wunder served as IST-Chair for 4 years until May 2021.

This is a very welcome situation for ill-intentioned contemporaries who can easily use these tools and can keep their identity concealed as long as they pay for the services.

In our frantic world, the amount of time dedicated to considering a subject is decreasing and a wealth of information competes for our attention. This brings along that on one hand, reputable media are challenged to provide cost-intensively checked and proofed facts and on the other hand, that facts are less relevant since the most excited and thrilling message promises the highest number of clicks. The consumers of social media (with tendency to just a 7 second attention-span) do not check the validity and truth of "facts," or worse, aspire to find and accept only information compatible with their existing beliefs.

Societies are susceptible to slanted and false information. Examining the impact of information campaigns is complicated. It could equally be the case that public recognition of false information can be unwanted by parts of the society if the narrative benefits them or supports their way of thinking.

Narratives are often not labeled by the real originator and it is often hard to discover their underlying aims and origins. Since narratives can be combined with various information elements and various sources in a systematic and comprehensive campaign, it seems easily possible to launch riots, demonstrations to influence the disposition in a greater society, to manipulate the position of a society and finally to cause severe distortions in a nation. This makes information operations attractive not only to aggressive states that have only limited technical and military means but also to those who benefit from economic drawbacks as consequence of a manipulated common opinion and a destabilized social system.

7.3 COUNTERMEASURES

Countermeasures try to disprove a false statement and to provide counter statements that are more effective than the false statement itself. Moreover, the message of fake news can be fortified and manifested by referencing. Countermeasures that attempt to convince people away from the opposite side are hard or generally impossible. Supporters of a particular narrative don't care about its validity as long as it supports their existing beliefs. There is no simple way to combat lies.

Education can be a strong countermeasure. But its reach is limited, takes time, and requires skillful teachers who can teach truth, and both sides of the story, uninfluenced by their own bias or others' biases, presenting just facts that can be backed by evidence. Fortunately, there is another approach to address false narratives: fact checkers. Their range of influence is currently growing in the media branch. Serious journalists use various websites where false facts are identified by referencing provenance and source (www.politifact.com; www.factcheck.org; www.newsguard.com). For instance, in checker networks (for example, www.poynter.org) the various fact checker members obligate themselves to commit to a code of conduct in order to distinguish from dubious social media providers.

NATO's Science and Technology Organization has identified that information manipulation falls, unquestionably, within the realm of military defence. External aggressors can focus on the destabilization of a social society and its economic prosperity. Information warfare and cyber operations combined in a hybrid scenario have the potential to trigger conflicts that are scalable from occasional damage to comprehensive destruction. What makes acts of hybrid warfare so extremely dangerous is the fact that they can be prepared totally concealed, they can be applied without any advance warning, they can be launched from everywhere and there is no balance of forces, since the NATO countries don't have information manipulation as an accepted item in their weapon arsenal.

A few years ago, NATO STO launched a couple of Research and Technology Groups to work on countermeasures in the context of social media. They focus on background analyses and support intelligence analysts with information about source, origin, plausibility, technical facts about the dissemination

procedures, tendencies in the content, etc. For example, a simple observation of broadcast times can reveal that a bot is behind the messages if there are no regular time outs, whereas a person needs some periodic timeouts for sleeping. Another clue to identifying a hoax might be features in the diction of messages that are typical to a special group. Also, the traffic between Twitter nodes can provide evidence about concentrations, references, etc.

A research and technology group on “Intelligence Exploitation of Social Media” has provided a report (STO-TR-SAS-IST-102, 2018). Another NATO STO group (IST-177) on “Social Media Exploitation for Operations in the Information Environment” will conclude with a report on 3 years of research in summer 2022.

7.4 ROUNDUP

Narratives overwhelm the world.

Information manipulation is effective, it must be seen as a potent weapon, it can trigger severe and unlimited conflicts. Limited events (tests?) happen already. NATO and nations need exhaustive concepts for countermeasures. NATO STO can provide expertise.

7.5 REFERENCES

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.

Chapter 8 – CHINA AND COGNITIVE WARFARE: WHY IS THE WEST LOSING?

Kimberly Orinx[1] Pr. Tanguy Struye de Swielande[2]

"The Chinese will overtake the West in cognitive warfare."

In recent years, we have seen the return of competition between the great powers. To counter the United States in particular and the West in general, the Chinese are applying hybrid warfare. Even though no direct military confrontation with the West has occurred in the 21st century, China and other contesters use hybrid means such as guerrilla, terrorism, economic pressure, cognitive warfare, cyber-attacks, paramilitarization, lawfare (reinterpretation of norms and standards), to weaken the West.

In doing so, they remain below the threshold of actual war in order to produce their strategic effect while preventing the activation of jus ad bellum. This strategy blurs the threshold between peace and war that we have come to adopt as basic understanding of interstate relations. The West must thus expect that potential adversaries will increasingly resort to this form of warfare, which is accessible and not expensive, either in support of more conventional military operations or autonomously to defend their interests.

One of the components of the hybrid warfare is the understudied cognitive warfare. The latter is defined by Bernal et al. as "the weaponization of public opinion, by an external entity, for the purpose of 1) influencing public and governmental policy and 2) destabilizing public institutions. Destabilization and influence are the fundamental goals of cognitive warfare" (Bernal et al., 2020). Cognitive warfare is moreover continuous: the Israelis are even talking about cognitive campaigns between wars (Kuperwasser and Siman-Tov, 2019).

8.1 CHINESE STRATEGIC CULTURE

Strategic culture is defined as "a distinctive and enduring set of beliefs, values, and habits about the threat and use of force that are rooted in the fundamental influences of the geopolitical environment on history and political culture" (Booth and Trood, 1999). Chinese strategic culture, influenced amongst others by Confucianism, Taoism, the interpretation of time, Sun Tzu and the 36 Stratagems is flexible, subversive, concentrates on the potential of the situation (Julien, 2015) and is better adapted to cognitive warfare than the Western strategic culture. Among other strategies, this is illustrated nowadays through the famous concept of "sānzhàn 三戰" – Three Warfare: psychological warfare, the war of public opinion and legal warfare. The objective of this concept is to "try to influence the public perception of the conflict by maintaining the support of its own population, by degrading it in the opponent's population and by influencing third parties." The war of public opinion is applied through various channels such as the media and social networks to disseminate information to a target audience, namely the (potential) adversaries and enemies to dominate the long-term implementation of psychological and legal warfare (Cheng, 2012). Psychological warfare, on the other hand, aims to influence the opponent's way of thinking or behavior (undermining the opponent's will, eroding popular support) and to consolidate the friendly psychology, i.e., reinforcing the support of partners and allies and guaranteeing the neutrality of the undecided or neutral. Legal warfare, finally, at its most basic

[1] Kimberly Orinx is research assistant at UC Louvain (Université Catholique de Louvain, BE), researcher at CECRI and PhD student in international relations, specializing in strategic culture and cognitive warfare. The subject of her thesis is China's cognitive warfare in Belgium.

[2] Pr. Tanguy Struye de Swielande, PhD, is professor in international relations at UC Louvain (Belgium). His research focuses on great power relations, the Indo-Pacific, power, grand strategy and information warfare. As co-coordinator of the Belgian Ministry of Defence's Strategic committee updating the 2016 Strategic Vision, he supervised and led the work of a group of experts in writing the 2030 security environment and the Ministry's strategic vision in 2021.

level, consists of ensuring that one's own side complies with the law, presents arguments in one's favor in cases where there are nevertheless violations of the law, and criticizes one's opponent for non-compliance with the law.

These three wars are mutually reinforcing: the propagation of discourse includes the strategic narrative to convince domestic and foreign populations through the vectors of transmission (war of opinion) by creating a favorable mental environment (psychological warfare) that makes the message conform to preconceptions, while protecting itself behind the logic of cyber sovereignty, which China is trying to impose legally at the international level (legal warfare).

Furthermore, cognitive warfare does not differentiate between war and peace, between combatant and non-combatant, (everyone is a potential target), and it is permanent. This is a major difference with the West, where there is a differentiation between war and peace. At the end of the 20th century, the publication of the monograph Unrestricted Warfare by two Chinese army colonels, Qiao and Wang (2006), marked an important step in understanding contemporary strategic thinking in Beijing. According to the authors, technological developments, globalization and the rise of power beyond the nation-state, combined with the new capabilities of modern weapons, would provide a new context for conflict. Battlefields would thus shift from a physical dimension to a more abstract arena such as cyberspace, the morale of the population or their brains. In other words, Qiao and Wang demonstrate that war is no longer "the use of armed force to force the enemy to bend to our wishes," but rather "all means, whether armed or unarmed, military or non-military force... [uses] to force the enemy to submit to its own interests." As a result, the battlefield is everywhere, war is no longer a purely military concept but also becomes civil. This has two consequences: firstly, the victims of these new wars will not only be regular combatants who die on the battlefield, but also civilians who are indirectly affected. Secondly, war is permanent and holistic, all forces and means are combined.

Finally, the authors argue that the only rule is that there are no rules. Thus, military threats are no longer necessarily the main factor affecting the national security of a country. The intent is not necessarily to defeat the West on the battlefield, but to weaken the democracies to such a point, "they are unable, or unwilling, to respond to aggression" (Zeman, 2021).

Cognitive warfare conducted by Beijing (and others) attacks who we are, our history, our past, our identity. James Rogers summarizes this logic extremely well:

> *To be effective, a hostile positioning operation would need to involve a three-step process: Deactivate the target country's existing identity through tactics such as: The desynchronization of its historical narrative; The questioning or demolition of its self-perception of its international relevance; and The delegitimation of its international status and role; Construct – if possible working in tandem with disgruntled or separatist domestic political forces – a new identity for the target, connecting it to new or pre-existing (but often marginalized) historical myths; Encourage the adoption and spread of the new position, both: Domestically (inside the target country), particularly among disgruntled and separatist elements; and Internationally, among the elites of other countries* (Rogers, 2021).

The objective is to turn people against each other from within. The center of gravity is now the population and the political processes in open societies.

Furthermore, as Vadim Shtepa explains: (2021): "while manpower and infrastructure can be restored, the evolution of consciousness cannot be reversed, especially since the consequences of this 'mental' war do not appear immediately but only after at least a generation, when it will be impossible to fix something." And the time factor, is on the side of China: China has time. Its approach to time is very different from the West. "For a Westerner," says José Frèches, "time is linear: lost time is never recovered and we perceive our life as a countdown that will end definitively on the day of our death (...); for a Chinese, time is cyclical: time passes again (...) in other words, time is not lost" (Allègre and Jeambar, 2006). In parallel, "those who do not

hesitate to lie will always have the advantage of time" (Ya'alon, 2019). Time is thus a social construct and is therefore interpreted differently in different cultures and will therefore have an impact on the way war is understood and conducted, whether at the strategic, tactical or operational level.

The Western adversaries have, like Victor Davis Hanson puts it, "mastered the knowledge of the Western mind" (Hanson, 2004). Our potential adversaries know our vulnerabilities far better than we do ourselves. They realize that the struggle can't be won on the battlefield, but can be on the field of images, rhetoric and changing public opinions, like David took down Goliath. Simply presented, perception is the new battlefield and the mind is the weapon.

8.2 WEAKNESSES OF THE WEST

Although the Chinese strategic culture is more adapted to cognitive warfare, the West has facilitated the Chinese policy at two levels: the state of our democracies and the outdated Western strategic culture.

Polarization within democracies is a blessing for Beijing. People are more likely to look at information that confirms their ideology, rather than contradictory information. Technological developments have amplified the importance of information and data in our security environment. Information is a resource that is and will increasingly be used to destabilize countries, in particular democracies. While they are not new, disinformation campaigns, fake news, or conspiracy theories, are used to fragment Western states and polarize the public opinion, thereby weakening our democratic values and systems, increasing distrust and discontent towards political systems, and promoting populist and nationalist movements. People look for information and people on social networks that confirm their logic (echo chambers). This exacerbates existing antagonisms, sows social division, and undermines faith in institutions. This is facilitated through microtargeting and behavioral data (e.g., Cambridge Analytica) based on Open Sources Intelligence (OSINT).

The rise of populist leaders and increasing support for digital authoritarianism worldwide illustrates the penetration and success of cognitive warfare by authoritarian states. Our democratic and open information society will increasingly be targeted by such operations of information manipulation. Disruptive technologies will increase this trend, as the operational surface and speed increase tenfold with AI and quantum computing. The human brain is the battlefield of the 21st century (MWI, 2018). By relying on human cognitive flaws such as confirmation bias or our natural intellectual laziness (leading to an absence of critical thinking), manipulating information through the information environment will continue to be a preferred means to weaken our democracies. These clashes of narratives, storytelling and communication will be an integral part of the operational strategy in future conflicts.

The opponents of democracies have understood, as Nick Reynolds (2020) notes, that "in political warfare, disgust is a more powerful tool than anger. Anger drives people to the polls; disgust breaks up countries." Moreover, citizens of democratic countries participate in this decline, reinforcing these logics of silos and tribalism, as this false information is "liked" and/or re-shared. Alicia Wanless talks about "participative propaganda." All this is further facilitated by bots and troll factories as well as by repetitive and characterized exposure, by mutually reinforcing stories. Therefore, the development of more and more sophisticated means such as artificial intelligence, communication strategies, marketing, branding and neurosciences facilitate manipulation and form a major challenge because of the inherent characteristics of human brain functioning, such as cognitive bias and heuristics.

In a world in which the dominance of "Western values" is increasingly challenged by other cultures and models, it would be naïve to believe that the way of fighting, implying rules of engagement and codes of honor, will be maintained in the wars to come. On the contrary, opposing cultures and strategic visions will multiply in the coming years. One of the two colonels who wrote Unrestricted Warfare amplified his thoughts in August 1999: "War has rules, but they are set by the West.... If you use these rules, then the weak

states don't stand a chance... We are a weak state, so should we fight according to your rules? No." There is a tendency in the West towards "mirror imaging" the enemy, presupposing that he will follow the same rationality. The contemporary vision of conflicts is in this way still too much impregnated with "the Western paradigm of war": the confrontation between States with the same political, cultural and ideological concepts. Consequently, Western strategic culture is not adapted to hybrid and cognitive warfare. The West appears to forget too often that war is a contest of wills, and even more today than in the past, a battle for perceptions and worldviews. We can retain different reasons for this.

First, Western strategic culture is linked to a binary approach to things: good or bad, white or black. The West finds itself in a predetermined theory-practice relationship, leaving little room for out-of-the-box thinking. For Womack, Western thought is determined by a "transaction logic." This is characterized by a contractual relationship and a desire to be in a win-lose, cost-benefit relationship (Pan, 2016). The Chinese will place more emphasis on the relationship itself and its mutual benefits by playing on respect in order to ultimately gain an advantage. Also, unlike the West, for example, China will avoid calling states enemies. This is a big advantage in cognitive warfare. In other words, Western strategy is often going to be pre-established in a well-defined canvas, from which it is difficult to break out – the facts having to fit the conceptualization or modeling, even forcing the facts into the model. Hence also, that China defends the principles of non-interference, and that it often avoids taking a definitive and clear-cut position in international issues (e.g., Syria, Libya, etc.). By refusing to see things through a binary reading (good-evil, democracy-dictatorship), it leaves itself a continuous margin of maneuver, avoiding forcing or imposing the situation, allowing it to ride the wave of the situation's potential, which is not the case for the West.

Second, the Western way of war is based on technology and is kinetic in a logic of a zero sum game. The Revolution in Military Affairs or Offset strategies of the US for example are based on technologic superiority in the different domains (air, land, sea, space and cyberspace), the cognitive or human domain is absent. Chinese approach is more people-centric, less techno-centric, based on relative wins and subversion and deception. China plays Go, the West chess. Technological superiority is not synonymous with winning wars as Libya, Afghanistan and Iraq have shown. The West suffers from strategic atrophy and incompetence, always fighting the last war, and not understanding the next one. Cognitive warfare is an excellent example of this Western strategic paralysis.

Third, the West additionally differentiates peace from war: this is not the case for China. The rules of war are not determined anymore by the West but by our adversaries and we have not yet grasped it: "Cunning adversaries leverage the space between war and peace for devastating effect. Washington has a buzz phrase for this: the "Gray Zone." Others have a strategy" (McFate, 2019). The peace-war distinction is outdated and the West has not conformed and adapted to this new reality.

Fourth, Western military is still too hierarchical, bureaucratic, slow, working in a logic of silos or tunnel vision, whereas society is more horizontal, networked, adaptive and flexible. As explained by General McChrystal: "Our culture does not force leaders to reckon with the intersection of strategy and adaptability (…) we must combine outside-the-box and ordered thinking. This kind of hybrid leadership will be necessary not only for success in warfare, but in other worlds as well" .

Finally, these differences of strategic culture between China and the West are also reflected in cognitive differences between Asians and Westerners. R. Nisbett in different studies argues that Easterners, compared to Westerners "have a contextual view of the world" and events are seen as "highly complex and determined by many factors," whereas Westerners will follow a logic of "objects in isolation from their context" and thus "control the objects' behavior" (Nisbett, 2003). For Nisbett, Chinese thought is more dialectical for Nisbett then logical: things happen in an appropriate context. It is also more relationship based and finally where Westerners believe in stability, Easterners see more change. Still according to Nisbett, the Chinese have a holistic approach of the world, emphasizing relationships, interrelations, cycles, whereas the West separates the objects of the environment, sees a linear movement of events and has the impression to be

personally in control of events: "Asians see the big picture and they see objects in relation to their environments – so much so that it can be difficult for them to visually separate objects from their environments. Westerners focus on objects while slighting the field and they literally see fewer objects and relationships in the environment than do Asians" (Nisbett, 2003).

8.3 CONCLUSION

War remains unpredictable because it is led by humans, who are emotional and fallible beings. War is not a science but an art, open to evolution and adaptation. Complexity in war remains the key word. Each adversary forms a system, an organism that must be penetrated. As Mao once said: "if one does not understand the conditions of war, its character, the links that unite it to other phenomena, one exposes oneself to ignoring the laws of war, the way to make it, one is powerless to win."

In the last two centuries, most of the wars, particularly in Europe, have taken a symmetric form or shape. There was not only an instrumental symmetry, but also a symmetry of norms and rationalities. The wars were thought and conducted following the same pattern, with the same code of honor. Symmetry tends more and more to give way to asymmetry. In a certain way, people and States are fighting each other, but without understanding each other's reciprocal strategies, because they are acting according to different cultural, ontological, cognitive patterns, making it impossible to adopt common rules. The West has been outplayed thus by its adversaries on two levels – ontological-cultural and cognitive – having a direct impact on the power relation between the West and China.

In this context, social sciences although not sciences of linearity, have the advantage to open our minds to complexity, and, in fine, to a neo-clausewitzian world[3] . So maybe we do need more philosophy, more sociology, more history, some disciplines whose principles and applications are not, by essence, linear and can assume a better mental preparation to confront combat realities.

Our adversaries do not only perceive their comparative advantages in technological terms, but in terms of identity, cognition, culture, collective psychology and popular will. The Western strategic rationality will require, in addition to its former instrumental component, taking into account the cultural and cognitive rationality of the adversaries, something our adversaries do master.

This is important because it has a direct impact on the power of a state. As Dekel and Moran-Gilad (2019) explain, and we quote them in length:

> *The shaping of cognition during a conflict between adversarial actors includes several stages: formulating the narrative of the conflict by describing the reality that prevailed before; the need and the legitimacy to change the situation or to maintain it, due to an assessment that the possible end states are inferior to the current situation; the reasons for defining the political-military objectives; and the principles for conducting the campaign such that it will influence the consciousness of the various target audiences in a way that serves the strategic objective.*
>
> *The various measures and powers exerted need to match the "story" that the actor wishes to convey to the designated target audiences. This is so that the construction of cognition is effective and strengthens the legitimacy of exerting hard power, especially military power; so that the achievements of exerting hard or soft power are translated into political and international achievements; so that is possible to shape an image of victory that illustrates the achievement of the political-military objectives, or offsets the achievements of the adversary.*

[3] "Neo-clausewitzianism" was initially coined in a pejorative sense, trying to explain the thinking of the tenants of nuclear warfighting. Joseph Henrotin, Alain De Neve et Tanguy Struye de Swielande "Vers un monde néo-clausewitzien?" (in Henrotin et al., 2004).

8.4 REFERENCES

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 and Johns 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 May 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 and The Institute for National Security Studies: Tel Aviv, Israel.

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

Modern War Institute (MWI) (29 October 2018). Video: The Brain Is The Battlefield of the Future – Dr. James Giordano. Modern War Institute.

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 April 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 April 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 and 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 People's Republic of China), 12 February2006.

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 (Norway), 30 November 2017.

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

Chapter 9 – CYBERPSYCHOLOGY[1]

Pr. Bernard Claverie[2], Dr. Barbara Kowalczuk[3]

Cyberpsychology can be defined as the study of mental phenomena related to cyber-systems and their context. The term "cyberpsychology"[4] is a neologism which refers to two interwoven concepts: "psychology," the study of behavior and thought, and "cybernetics," the science of the laws of control and communication for mechanisms and machines operations.

9.1 MACHINES AND HUMANS

While it is common to speak of the confrontation between AI and Natural Intelligence (NI), or of transcending NI with an AI that can be misunderstood as something frightening, which might cause disturbances or even threaten our individual and collective liberties, many scientists have been developing a reflection under the term "cyberpsychology." The advent of intelligent machines is for some a solution to cope with human problems; for others, it stands as a threat to the future of humanity. Undoubtedly, the cybernetic world keeps transforming humans and it will probably transform them even more in the future.

Intelligent robots are used in factories, hospitals, railway stations and airports. They will soon appear on battlefields. Cyber collaborators invade our homes, offices and living spaces. This is not without consequences for society, for social groups, but also for individuals, as they transform their bodies and their minds. How do humans adapt to this global change, and how does the cybernetic world adapt to humans who change? These questions lead scientists to take an interest in these joint evolutions, in their mutual effects on thought, intelligence, emotions, personalities, and on the modes of machines design, their use and their transformation. Thus, it is necessary to investigate the relation between humans and cybernetic systems, artificial intelligence, robots, etc.

The evolution of AI involves new words, new concepts, but also new theories that encompass a study of the natural functioning of humans and of the machines they have built and which, today, are fully integrated in their natural environment (anthropotechnical). Tomorrow's human beings will have to invent a psychology of their relation to machines, but the challenge is to develop also a psychology of machines, artificial intelligent software or hybrid robots.

In this context, cyberpsychology is at the crossroads of two main fields: psychology and cybernetics. It is understood as the science of the mechanisms of behavior and thought in humans, and of the psychological laws that apply to the cybernetic space and to cybernetic systems. As an autonomous discipline correlated to its mother disciplines, it has been developing since the end of the 20th century, and it shares their characteristics, their limits and their methods while encompassing other traits which result from their reciprocal relations. Centered on the clarification of the mechanisms of thought and on the conceptions, uses and limits of cybernetic systems, cyberpsychology is a key issue in the vast field of Cognitive Sciences.

---

[1] This text was originally published on the NATO-ACT Innovation Hub website (Norfolk, Virginia, USA) on 1 June 2018. It was provided to the participants of the first "Cognitive Warfare" day as a basis for discussion.

[2] Pr. Bernard Claverie, PhD in Neuroscience, is university full Professor (Psychology), honorary director and founder of the ENSC (Ecole Nationale Supérieure de Cognitique – Institut Polytechnique de Bordeaux FR) and researcher in Cognitive Sciences at CNRS & Bordeaux University – UMR5218 Lab. – FR.

[3] Barbara Kowalczuk, PhD in American Literature, teaches at University of Bordeaux – FR.

[4] Cyberpsychology and Cyber-Psychology are synonyms. The same goes for Cybercognitics and Cyber-Cognitics, Psychocybernetics and Psycho-Cybernetics, Cybersystems and Cyber-Systems, Cyberdependance and Cyber-Dependance, Cybertechnology and Cyber-Technology, etc.

9.2 CYBERPSYCHOLOGY AND THE "CAUSALITY PROBLEM"

The relationship between mind (psycho) and cyber (Information technology) should be investigated from different angles. While the scientific field is sometimes inappropriately reduced to a one-sided definition of cyberpsychology, it is crucial not to restrict the field of research to virtual reality or psychotherapy applications. Cyberpsychology raises numerous questions, in particular those regarding the motivations, the needs, the reluctances and the difficulties linked to the use of cyber tools and to their environments. Other issues include the design, the implementation, or the control of cyber-systems with respect to psychological characteristics and processes.

Therefore, cyberpsychology can be connected to different concrete topics, among them health issues, aerospace and transport, global security, military organizations, decision making, education, etc. In fact, in terms of research and application, cyberpsychology includes three distinct categories, and their differences are based on the causality link between the respective elements of each of the psychological and of the cybertechnical worlds, and their variation. These elements are called "variables."

According to the famous English epistemologist Karl Popper (2002), common sense tends to assert that "every event is caused by an event that precedes it." This spontaneous conviction is central to the "deterministic perspective," according to which everything or every fact has a cause. Some scientists go even further and are convinced that each event provokes another event. Thus, everything can be said to have a cause and a consequence. This intellectual position is called "universal determinism." In science, at least two consequences follow from the above-mentioned theories: one can thus "explain" anything or any event; and one can also "predict" things or events that will flow from the present or the past.

In this deterministic context, a dependent variable is traditionally defined as an element whose variation depends on the variation of another element which remains independent of the form of the causality. We then say that the variations of one cause or produce the variations of another one. We speak then of independent variable (I) and dependent variable (D). The causal link is oriented from I to D ($d\mathrm{I} \Rightarrow d\mathrm{D}$). Conversely, the variations of D are not causal of those of I ($d\mathrm{D} \Rightarrow d\mathrm{I}$), except to define co-variant or correlational variables, in a non-causal relation ($d\mathrm{D} \Leftrightarrow d\mathrm{I}$) or more exactly, for some scientists, a causal relation that is not yet known or discovered.

These three sub-themes could be respectively defined for cyberpsychology as "cyber-cognitics," "psycho-cybernetics" and "global cyberpsychology."

9.3 THE CYBERTECHNICAL INFLUENCE

The cyber effect on the psychological dimension of humans constitutes the first part of cyberpsychology. In all the areas of research, the experimental conditions determine a statute of independent variable for the technical data, and a statute of dependent variable for the psychological data. This field is literally "psycho-cybernetics."

The effects of these cyber technical dimensions on the mind concern the following points (non-exhaustive list):

- Behavior and thought (cognitive facilitations, cognitive impairments, cognitive errors, ergonomics, etc., cognitive impairment, human error, etc.);
- Psychological traits and personality (structuring, alterations, use in soft power or social engineering);
- Professional training and apprenticeship;
- Education (children, adolescents, adults, young experts, knowledge management, etc.);

- Psycho-rehabilitation, psychotherapy (psychiatry, mental health, post-traumatic stress disorder, brain injury, moral injury);
- Prevention (cyberdependence is now officially recognized as a psychological disease by the World Health Organization).

Table 9-1: Factorial Representation of Different Domains of Cyberpsychology Depending on the Status of Technical (Cyber) or Psychological Causality.

	Psycho-Cybernetics	Cyber-Cognitics
Psychological Data	dependent variables (D) non-causal	independent variable (I) causal
Technical Data	independent variable (I) causal	dependent variable (D) non-causal
Correlativity	covariation/correlation/unknown causality/indeterminacy	

9.4 THE PSYCHOTECHNICAL CAUSALITY

The psychological effect on the cyber field defines a cyber-cognitics domain, and it is possible to describe some of the effects of psychology on cybertechnology or on the cyberdomain (non-exhaustive list):

- Computer programming styles, program structure, etc.;
- Imitations (neural networks versus symbolic programming, hybrid modes, different AI, etc.); – modes of implementation (networks, main frames, intensive computing, parallelism, fuzzy logic and cyberquantum, etc.);
- Digital trust (complete or partial autonomy, monitoring, control, delegation, etc.);
- Digital resistance modes (avoidance coping, procrastination, etc.);
- Psychological cyber defence (cybersecurity, especially invasive, defensive, techniques, attritive, etc.) "man is the first flaw in digital systems," Man-In-the-Middle Attack (MIMA), etc.;
- Cyber-radicalization (cognitive processes, social environments, prison environment, liberties, rights, etc.).
- etc.

9.5 THE INTEGRATED SYSTEMS

The third type of effect can be characterized by non-causal relations, or unknown causal relations, mainly in complex systems. It concerns the domain of Human-System Integration (HSI) (Booher, 2003; Pew and Mavor, 2007) or Human-Automation Teaming (HAT) (Shively et al., 2007; Demira et al., 2017), in an anthropotechnical world (non-exhaustive list):

- Some elements in human machine interface;
- Human machine teaming;
- Human machine symbiosis, human machine hybridity;
- NBIC[5] (converging technologies for human enhancement);
- etc.

[5] NBIC: Nanotechnology, Biotechnology, Information technology and Cognitive sciences (Cognitics) (Roco and Bainbridge, 2002).

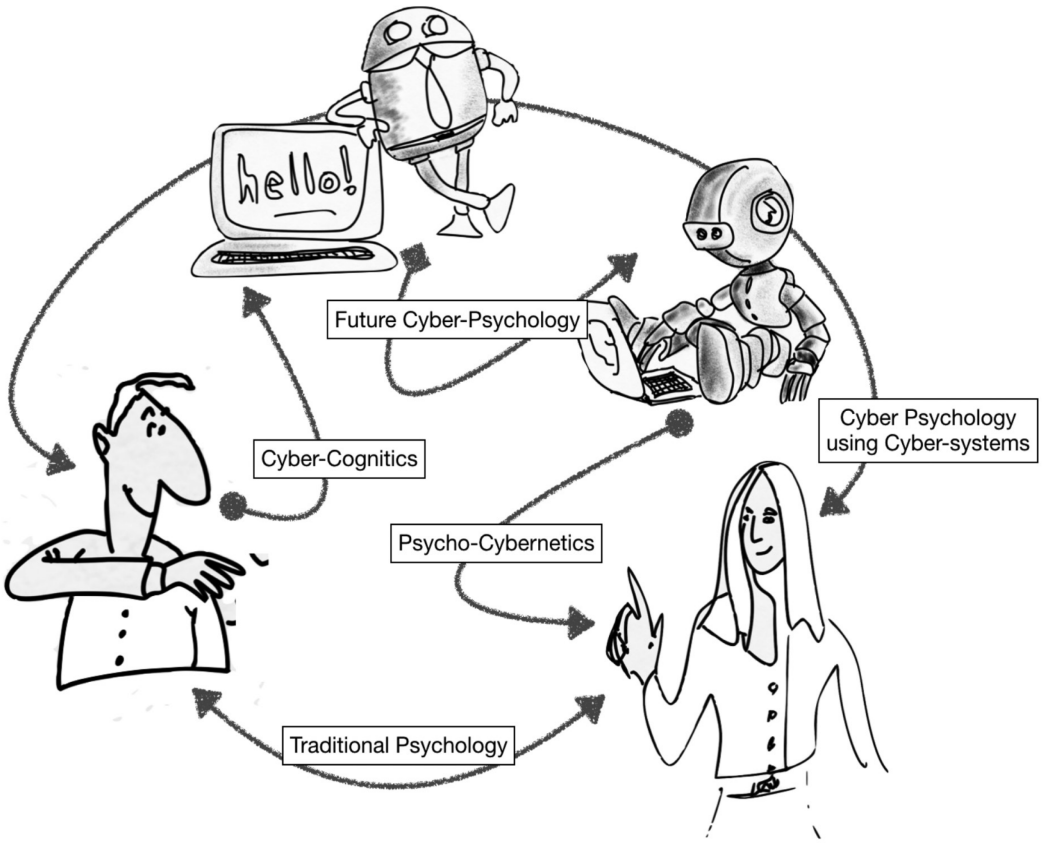


Figure 9-1: The Different Fields of Cyberpsychology in the Psychology Domain.

9.6 CONCLUSION

To conclude, cyberpsychology is a domain of the general psychology, and a developing, complex scientific field which embraces diverse phenomena and different sub-themes involving machines as humans. With the advent of smart and autonomous machines, it has become primordial to develop a new form of psychology, one that will examine the way humans and machines impact on each other. In addition, it will explore how the relation between humans and AI will change human interactions and machines intercommunication.

It calls for accurate definitions and differentiations so as to leave no ambiguity. Research and applications should therefore take into consideration the type and the specificity of the causal relation that underlies the link between psychology and cybernetics. In terms of research and implementations, it concerns a variety of issues related to Defence and Security and to all the areas which NATO prioritizes to prepare its transformation.

9.7 REFERENCES

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.

Chapter 10 – SITUATION AWARENESS SHARING: A LINK OF COGNITIVE VULNERABILITY

Dr. Baptiste Prébot[1]

"Knowing what the other person thinks about the situation in order to share the same awareness is the basis of collaboration."

Building and maintaining a common situational awareness is one of the most difficult cognitive activities faced by team partners. It is also one of the most fragile areas of team and collaborative work. At the individual and collective levels, representation is at the heart of the cognitive decision-making process. The sharing of a common understanding of the situation, i.e., similar between team members, is necessary for the coherence of the decision.

Situation Awareness (SA) and its sharing are particularly sensitive to contextual influences, and it is necessary to provide all the required technological support, both in terms of its facilitation and its security in the management of potential errors.

This partnership can be the target of cognitive warfare. It is a question, for the attackers, of influencing the individual representation by acting on all the tools for sharing them, whether they are technological or social. Faced with a threat of influence or manipulation, the defender must deal with this risk and facilitate the conditions of a robust situation awareness sharing.

10.1 SITUATION AWARENESS

Situation Awareness (SA) is the result of all the cognitive processes that contribute to the "representation that an individual makes of the situation in which he is involved" (Nofi, 2000). Over the last 30 years, its evaluation has become essential in the study of complex operational environments, particularly in the military field. Originating from accidentology studies in the late 1980s (Foushee and Helmreich, 1988), the notion of situation awareness has become a topic of concern in training, design, and operational contexts (Buchler et al., 2016; Chen et al., 2016; Endsley, 2004; Endsley et al., 2003; Salas et al., 1997). Its central role in the decision-making process, of operators, whether at the individual or team level, makes its evaluation a key element in predicting performance.

As technology becomes more and more customizable, attention has turned to ways of assessing the cognitive state of users or teams in real time. The goal is to provide information systems for both operations commanders and operators. In the long term, technical assistance systems with automatic reaction capabilities are envisaged to overcome states of lack of situational awareness of the operator, which would present risks for the performance. For example, it has been shown that in adaptive teaching systems, certain real-time metrics can monitor and ensure an optimal state for learning, by continuously measuring and adjusting the level of attentional demand (Carneiro et al., 2016; Szafir and Mutlu, 2012). In military operational contexts or when some experts are managing complex decision systems, this type of continuous measurement can relieve users by adapting the level of automation and the mode of interaction or of communication (Scerbo, 1996).

[1] Baptiste Prébot, PhD, is a graduate engineer from ENSC (Ecole Nationale Supérieure de Cognitique – Institut Polytechnique de Bordeaux FR) and holds a PhD in cognitive engineering from the University of Bordeaux. He was an assistant professor at ENSC and a researcher in UMR5218, a joint research unit of CNRS, University of Bordeaux, Bordeaux INP. He defended his thesis in 2020 on "Shared Situation Awareness in C2 Activities." Since November 2021, Baptiste Prébot has been a research fellow at the Dynamic Decision Making Laboratory of Carnegie Mellon University.

SA assessment methods are designed to detect what is wrong with individuals' representations of a given situation. They have so far focused more on the accuracy of the situation awareness than on the speed with which it is acquired. The methods have therefore been more qualitative than quantitative. Indeed, according to authors in the field (Endsley et al., 2003), situation awareness is above all a cognitive construct whose evaluation requires declarative access to its content. As a result, measurement relies on verbalization, making it inevitably delayed and necessarily subjective and incomplete. As the environment evolves, situation awareness is rebuilt, undergoing a continuous process of update to integrate new events. New information and new goals emerge over time. Thus, Situation Awareness is dynamic (Hjelmfelt and Pokrant, 1998; Nofi, 2000) and is a constantly changing construct. Traditional assessment techniques from psychology or ergonomics remain unable to reflect this dynamic nature outside of verbalization, and thus decontextualization of the probed subjects (Stanton et al., 2017). Furthermore, when problems arise, this assessment comes too late.

Real-time temporal assessments are therefore desirable, in particular to know when to adapt behaviors or interfaces, to react and intervene when the situation becomes critical, or to immediately trigger artificial aids by means of cognitive augmentation, or even substitution in case of overshoot. In the case of a team of operators, this continuous evaluation of situational awareness is essential to determine when the team's performance is likely to suffer from differences in understanding or representation. Several authors agree that developing objective, non-intrusive, real-time measures of situation awareness is a logical and necessary step for future operational systems (De Winter et al., 2019; Nofi, 2000).

Nevertheless, linking objective cues that can be measured without delay with subjective content that is only known after the fact is not a simple task. To address this need for objective measurement of situation awareness in monitoring and decision-making systems, researchers have focused on a phenomenon that characterizes several operators working on the same task: the process of Situation Awareness Synchrony (SA Synchrony).

10.2 COGNITIVE SYNCHRONY

The representation of the situation depends on the perception and continuous interpretation of the elements of the environment (Salas et al., 1995). One of the needs in the HAT (Human-Autonomy Teaming) context of adaptive collaborative systems, adaptive collaborative systems is real-time knowledge of the operator's state, whether used in training or in operational settings. In the case of collaboration, assessing temporal changes in Situation Awareness (SA dynamics) (Adams et al., 1995; Ziemke et al., 2017) provides insight into when and for how long SAs are (or are not) synchronized. Evaluating this sharing helps prevent human error, and document it for Retex and team/crew training purposes.

The measurement of situation awareness is based on the concept of similarity. This concept is to be examined with respect to reality, it is then a question of "accuracy", or with respect to another individual, and one speaks then about "similarity". The synchrony of situation awareness corresponds to the temporal emergence of this similarity, and its measurement is an indicator of its dynamics and the degree of sharing of situation awareness. The measurement of synchrony is based on the estimation of the knowledge or lack of knowledge of pieces of information by the individuals of the team. According to Endsley's (1995) model, the construction of shared situational awareness stems from teammates' similar perception and integration of the "right" situational elements; the "Necessary Knowledge Elements" (NKE) (Cain and Schuster, 2016). Therefore, one can consider the "Necessary Shared Knowledge Elements" (NSKE), which define the pieces of information whose knowledge is needed by multiple team members to accomplish a collaborative part of their tasks (Figure 10-1).

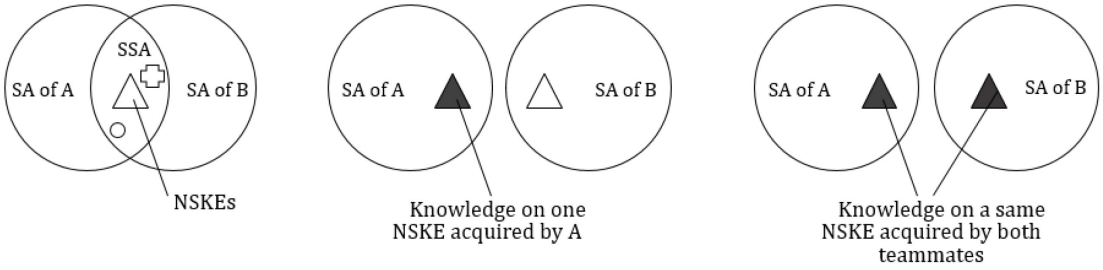


Figure 10-1: Illustration of the Three Possible States of Knowledge on a Necessary Shared Knowledge Element (NKSE). Either none of the teammates has an up-to-date knowledge of the NSKE (left), only one of them possesses it (center), or both are up to date and share the same knowledge of the NSKE (right).

All these elements of knowledge depend on the articulation of the individuals' tasks and are therefore identified beforehand. The training of crews allows the construction of the required shared mental models, including this knowledge of mutual needs in terms of information. Therefore, it is essential to build a team that has learned to work together and knows the relevant systems.

However, NSKEs are rarely perceived simultaneously by each team member (Cain et al., 2016; Endsley and Jones, 2001). Therefore, "latencies" must be defined and considered. Thus, when all useful information is available to two teammates (A and B) who have both successfully formed the same representation, they share the same initial level of situation awareness. Each time a new NSKE appears, it invalidates the current state of situation awareness, until it is integrated into a new state of situation awareness of the teammates, or "modified situation awareness", to obtain a new shared situation awareness thus updated. In this model, 4 phases are distinguished, creating three remarkable latencies to be taken into account, as shown in Figure 10-2.

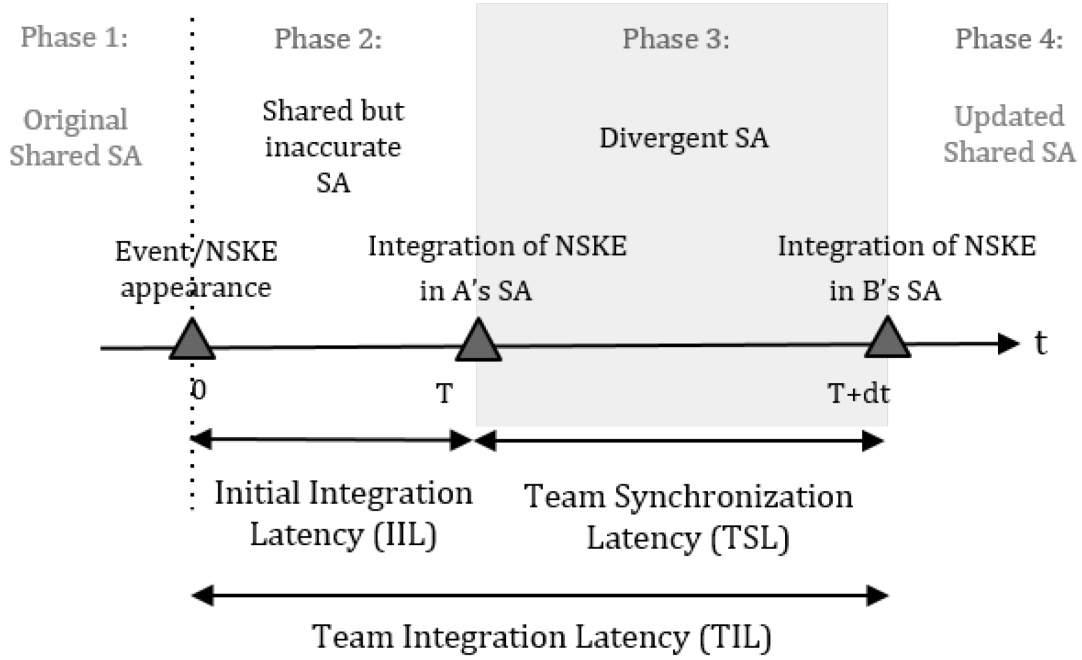


Figure 10-2: Shared Situation Awareness Dynamics and the Related Latencies: Initial Integration Latency (IIL), Team Synchronization Latency (TSL) and Team Integration Latency (TIL).

The first latency is called the Initial Integration Latency (IIL). It is the initial time required by a first teammate to perceive and integrate the new NSKE into his own situation awareness. The interval between the occurrence of the NSKE and its integration into A's situation awareness (phase 2 in Figure 10-2) represents a period of shared but inaccurate SA that is accompanied by the possibility of erroneous decision making. During this period, teammates still have a shared representation of the situation. Individual decisions are consistent with each other and collective decisions are consistent with the current strategy. However, the representation of the situation is no longer up to date. This difference from reality obviously increases the risk of inappropriate decision making. The duration of this latency is influenced by the same factors concerning attention and the sensory-perceptual system that have an impact on first-level situation awareness (level 1 SA) (Endsley and Garland, 2000): stress, fatigue, workload, or complexity of the interface.

The second latency, or "Team Synchronization Latency" (TSL), represents the time it takes for a second teammate to perceive and integrate the new NSKE into his or her SA after the first teammate has done so (phase 3 in Figure 10-2). This creates a delay between the two SA updates during which, taking into account the first latency (IIL), representations of the situation diverge. During this time span, in addition to being inaccurate for at least one of the teammates, situation awareness is also not shared. This increases the probability of inconsistent decision making. In this case, two teammates, one of whom is up to date with the situation and the other who is not, may send inconsistent or even contradictory instructions to a third teammate.

The "Team Integration Latency" (TIL) is the composite of the first two latencies. It represents the time elapsed between the modification of the environment and its integration by the last team member concerned (Phase 2 + Phase 3, cf. Figure 10-2). It represents the time during which the team members do not all have an exact SA.

By being inherent to the process of updating and sharing of situation awareness, these latencies illustrate the importance of its dynamic properties. This model is suitable for modeling the sharing dynamics of a co-located team as well as a distributed team, working in a network.

10.3 APPLICATION PERSPECTIVES FOR A REAL-TIME EVALUATION

Now that these latencies of cognitive synchrony have been defined, the question of their practical real-time measurement arises, to be used for control, error detection and assistance by artificial systems.

Initially, the measurement of situation awareness of individuals and teams was based on the analysis of behavior and reasoning processes (Cooke et al., 1977). It required the presence of observers in the teams. More recently, new methods are being used with tablet quizzes that allow for shorter analysis times (Buchler et al. 2018) but remain relatively invasive.

Behavioral and physiological measures (Delaherche et al., 2012) have the advantage of being continuous and easy to use for quantification of user state and activity (Fuchs and Schwarz, 2017; Jorna, 1993; Tomarken, 1995). Synchronization of Situation Awareness is then established by temporal comparison of measurements across individuals. But measurements are computationally expensive and the equipment heavy and cumbersome, potentially handicapping operators. Only recently has the relevance of continuous assessment of Situation Awareness been established using a measure derived from eye movements (De Winter et al., 2019) by non-intrusive means, external to the subjects (camera or sensors embedded in or near the displays).

Gaze position tracking first enabled the study of situation awareness in aviation (Kilingaru et al., 2013; Moore and Gugerty, 2010; van de Merwe et al., 2012) and driving (Hauland, 2019). The method can be easily augmented and crossed with reaction time measurements from mouse tracking or other behaviors

resulting from interaction (human computer interactions: HCI) with all interfaces (Freeman and Ambady, 2010; Frisch et al., 2015; Kieslich et al., 2018). Multi-measurement approaches appear to be useful for capturing such a complex construct as Situation Awareness (Salmon et al., 2006), and the "around the operator" multidimensional monitoring approach provides the basis for a new continuous and objective real-time assessment. The techniques are very sensitive but complex to implement. The measurements can be influenced by many parasitic phenomena that need to be identified in order to control them (Cooke et al., 1997).

Because communications add an inherent latency, ideal synchronization of situation awareness among team members is not realistic (Cooke et al., 2018; Sonnenwald et al., 2004; Walker et al., 2012). It must be understood that during collaboration, NSKE relevance, interpretation, and task prioritization are a function of the personal strategies and individual goals of the operators. Problem identification involves assessing the deviation from an expected latency, requiring a thorough understanding of the entire task, both at the individual and collective level. Processes and communications, as well as the qualification of behavioral markers, must be contextualized with respect to the environment in which they are applied (Salas et al., 2017). Similar to theoretical optimal accuracy (Hooey et al., 2011), improved synchronization of situation awareness could thus be defined on the basis of team task analysis as a descriptor of collaboration and performance. It provides real-time feedback to the team, the team leader or an artificial monitoring and support system.

With such metrics, training, adaptive interventions, and experience facilitation can then be designed. Digital facilitation programs can be developed for the detection of errors in representation sharing and synchronization of situation awareness. Specifically, information and artificial assistance can be established from the optimized states of synchronization between teammates, identifying problematic periods during collaborative processes. In a training context, collaborators can be trained to value optimal interaction times.

The complexity and speed of tasks increasingly require collaboration with machines that can then help avoid errors. The dynamic nature of situation awareness and its temporal evolution requires lightweight, non-intrusive means (Buchler et al., 2016) that are still expertise-based and difficult to generalize today.

By focusing on the content of situation awareness, traditional measurement methods are limited by the subjective nature of the evaluation, as the situation representation is based on a declarative evaluation. This makes it difficult to evaluate in real time, especially in stressful or complex situations that do not allow for online Retex time. On the other hand, we can consider the synchrony of situation awareness and provide indicators of it. We can identify their occurrence and their dynamics in the team. For example, the measurement of pupillometric activity (pupillary diameter) can be done live without wearing any equipment, by simply using a camera, crossing this data with non-invasive behavioral measures (activity on the mouse, keyboard, number of communications, chair movements, etc.). It is in the development of these indirect measures that the identification of an activity requiring the sharing of situational awareness lies, and thus, from there, the use of a posteriori methods.

Thus, since it does not necessarily evaluate the quality of the content of the mental representation, the measurement of synchrony makes it possible to free oneself from the need for verbalization and thus from the need to interrupt or intrude into the task, causing the disturbance of this awareness or possibly of the task. The task can then be completed efficiently, while the team members are informed online and the digital aids can be mobilized before the operators themselves express the need.

10.4 THE SHARING OF SA, A WEAKNESS OF THE TEAM IN COGNITIVE WARFARE

One of the objectives of cognitive warfare is to influence the decision making of the adversary, in the most subtle and undetectable way possible, by manipulating representations. If certain techniques, aiming for

example at the social and political stability of a nation or a group, operate on long time frames, the strategies developed can also be applied to real time decision making, notably through cyber operations.

It is not only a question of preventing the enemy from accessing certain information (e.g., jamming), but also of manipulating this information. This can be done, for example by providing false information through usual channels, with the ability to target when and to whom to provide what information, in order to optimize the disruption of the decision.

Such techniques allow, on the one hand, to benefit from the trust that the individual has towards his sources of information, and on the other hand, in case of detection of the intrusion, to undermine this trust, either towards the sources themselves (systems) or their vectors (communication channels or teammates).

For example, deliberately providing contradictory information to teammates or to different hierarchical levels can lead to the construction of inconsistent representations or conflicts of perception within a team. The long-term impact can be a degradation of interpersonal trust, of confidence in one's own judgment and of team cohesion.

The factors influencing the sharing of representation and team processes are well known and are the subject of much work, both on the design of appropriate systems and on the composition and training of teams (Endsley et al., 2003; Nofi, 2000). To counter these potential influences, it is necessary to design transparent (eXplainable AI) and reliable systems that facilitate the acquisition and sharing of SA. This also underlines the importance of common references (mental models) and meta-knowledge about the team (tasks, roles, individual needs), acquired over the long term through training and education.

10.5 CONCLUSION

The successful sharing of situation awareness by operators in the same team or by people working in a network is a cognitive process fundamental to the success of crisis management tasks. It is particularly necessary in crews and systems for monitoring or conducting military operations.

The acquisition of situation awareness is an example of a cognitive process that mobilizes attention, memory, and decision making, and that is facilitated by learning processes. The sharing of SA between several actors contributing to the same task is an emergent phenomenon, which can be identified and yet remains difficult to alter. If the current methods for measuring its content are not really compatible with operational situations, the measurement of this emergence, of its actualization and of their synchrony, by means of indirect methods, is a serious research opportunity. Once measured, it can then be the object of artificial assistance procedures, for example by an enhanced visualization to support or direct attention, or a support to the commander. This detection remains a tool that is immediate and robust to external influences. It allows both the facilitation of the collaborative task and the identification of strategic phases for the Retex.

Thus, in environments where building and maintaining a common understanding of the situation is under normal circumstances a difficult task, situation awareness represents a fragility of the team, subject to the effects of cognitive warfare. Therefore, the challenge of defence is to find methods and tools to reinforce collective cohesion as well as to ensure the reliability and security of information systems.

10.6 REFERENCES

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 andMeasuring 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 Analyses 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.

Chapter 11 – COGNITIVE WARFARE: COMPLEXITY AND SIMPLICITY

John Whiteaker[1], Cadet Sam Konen[2]

"For the Psychological Operations practitioner, a "new" third operational dimension is adding complexity to an already over complicated field."

For the Psychological Operations practitioner, a "new" third operational dimension is adding complexity to an already over complicated field. "Behind NATO's 'Cognitive Warfare': 'Battle for Your Brain' Waged by Western Militaries" (Norton, 2021) sums up the issue nicely in its title "waged by Western militaries." The current idea of Western and Eastern military diverges and divulges the true reason some are better than others in the understanding and operationalization of Cognitive Warfare. For many, Cognitive Warfare is not its own complex dimension, it is the only dimension that is then played out in the original five physical domains and is manifested in cyber and physical actions or products. Historically, the United States has multiple examples of successful cognitive-focused teams and operations. This paper suggests that learning from the lessons of our past and developing a constructive way forward will allow for the full utilization of units already established to conduct Cognitive Warfare.

11.1 INTRODUCTION

The United States' history of Psychological, Cognitive and Information operations, or warfare, began in the earliest days of our history. Military leaders of the past accepted and came to use the concept of "All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near" (Tzu, 1910). All warfare or competition, whichever term is appropriate for the time, revolves around the created perception of one's forces. Time has moved past the feints, cavalry charging an enemy's flank and progressed to identifying forces by collection of publicly available information or attempting to work through the ever-growing information environment to influence a target audience. The U.S. historically has cultivated personnel trained to conduct cognitive-focused operations. This was a task originally performed by the Office of Strategic Services (OSS), which was divided into the Central Intelligence Agency (CIA), United States Information Agency (USIA), and Psychological Warfare. Psychological Warfare has now been diluted down to the smallest regiment in the U.S. Army, Psychological Operations.

11.2 BACKGROUND

On 12 November 1943, the Psychological Warfare Branch (PWB) conducted operations through three functional teams during the Sicilian Campaign. Combat Teams (Reconnaissance), Occupational (Dissemination) teams, and Base (Permanent) teams made up one of the formations used during World War II. An underlying key to these teams was the personnel within them.

> *Combat teams were made up of three to five men, mixed military and civilian. One was attached to the 7th (American) Army under John Whittaker of Morale Operations, civilian, with one British and one American officer; and one attached to the 8th (British) Army under Lt. Col. McFarlane of PWB with a British and American Officer* (Oechsner, 1943, para. 2).

[1] John Whiteaker – Special Operations Command – USSOCOM. Tampa (FL, USA).

[2] Sam Konen – Cadet – United States Military Academy, West Point (NY, USA).

The true joint nature of this multi-nation, mixed military and civilian teams allowed for a more actionable force with the ability to create a long-term plan. The varied experiences of these teams allowed for different perspectives to be applied to a problem. The memorandum outlines lessons learned by these teams and very much like today revolved around the need for improved coordination with G2 (intelligence units) and "Civilian Administration Authorities." The Civilian Administration Authorities can be compared to local government authorities and Civil Affairs teams of today. Also emphasized was the importance of understanding cultural and information related nuances to positively influence populations, and reliable communication.

Morale Operations (MO), another forgotten term for cognitive, psychological, and information operations, is outlined as such within the OSS Morale Operations Field Manual (1943).

> *Definitions: The term MORALE OPERATIONS as considered in this Manual includes all measures of subversion other than physical used to create confusion and division, and to undermine the morale and the political unity of the enemy through any means operation within or purporting to operate within enemy countries and enemy occupied or controlled countries, and from bases within other areas, including neutral areas, where action or counteraction may be effective against the enemy.*

Section IV of the field manual addresses the largest hindrance to the effecting of human decision-making operations: coordination. The calculation and coordination of the cognitive effects at all levels of planning is integral to success.

> *a. Morale operations will be most effective when they are planned as part of common campaigns conducted by various underground services and integrated closely with actual or planned military operations and Allied strategy. (OSS, 1943)*

The decentralization of forces has been a continuing process since the end of World War II. This further partitioning complicates the complex nature of creating cognitive impacts in a planned manner. As suggested in historical reviews of operations, the need is for improved communication and coordination not the creation of continuing doctrinal changes that only affect the practitioner negatively. An improved feedback loop could provide further insight into what future doctrine is required. The loop would require recently forward personnel integrated in the policy and doctrine process. Currently, there is little to no interaction with Special Operations Forces from the officer level and below with policy and strategic decision makers above.

11.3 CURRENT

America's ability to wage psychological warfare and dominate the information space mostly relies on a small regiment of active-duty Army personnel. The joint nature involves technological assistance from both the Navy and the Air Force, as well as a small Marine Corps contingent focused on information operations. Every branch is trying to institute some form of information and influence focused unit. However, since the end of OSS, PSYOPs is primarily focused on this mission. PSYOP currently has as a ten-day selection process that each candidate must pass, as well as a "43-week official qualification course (PSYOP Operations Specialist Course), where one learns the core skills of being PSYOPS Soldiers, including basic speaking and listening proficiency in a foreign language, military intelligence, advanced interpersonal communication, adaptive leadership, cultural analysis, and advanced social media and marketing." (U.S. Army, 2020). This quote highlights the issues that surround the world of PSYOP, as even the Army's website outlining the process a candidate must attend contains an alternate name than what is used to define the course that must be completed to become a PSYOP soldier. Upon completion of the Psychological Operations Qualification Course (POQC) the soldier will be assigned to either a regionally aligned battalion, tactical company or a production and dissemination battalion.

Psychological Operations has passed through multiple names but for this piece, Psychological Operations (PSYOP) is the noun and Military Information Support Operations (MISO) is the verb usage of today's force. Currently, there are around two thousand active-duty PSYOP personnel. The purpose of MISO is to

"establish and reinforce foreign perceptions of U.S. military, political, economic power, and resolve. In conflict, MISO as a force multiplier that can degrade the enemy's relative combat power, reduce civilian interference, minimize collateral damage, and maximize the local populace's support for operations." (Joint Chiefs of Staff, 2010). The levels of war PSYOP is meant to act upon are defined as; "Joint MISO support policy and commanders' objectives from strategic to tactical levels." Military leadership and local key communicators are examples of TA engaged at the operational and tactical levels that can affect the accomplishment of a strategic objective (Joint Chiefs of Staff, 2010). These definitions are pulled from Joint Publications written by the Joint Chiefs of Staff and also CJCSI 3110.05F and DODI 3607.02, which also outline MISO as to be conducted by PSYOP forces.

PSYOP is one of the Information Related Capabilities (IRC) that the U.S. military must conduct for Information Operations (IO).

> *(2) IRC specialists can include, but are not limited to, personnel from the EW (electronic warfare), cyberspace operations (CO), military information support operations (MISO), civil-military operations (CMO), military deception (MILDEC), intelligence, and public affairs (PA) communities. They provide valuable linkage between the planners within an IO staff and those communities that provide IRCs to facilitate seamless integration with the Joint Force Commander's objectives.* (Joint Chiefs of Staff, 2012).

Today, as counter terrorism operations wind down and forces transition to Great Power Competition, the use of irregular warfare comes to the forefront of U.S. military operations. U.S. Special Operations Forces, which includes Air Force Special Operations Command (AFSOC), Marine Special Operations Command (MARSOC), Naval Special Warfare Command (WARCOM), United States Army Special Operations Command (USASOC), and Joint Special Operations Command (JSOC)), has fundamentally been on the edge of both these operational use cases. However, the information environment has always been amongst the core competencies of the PSYOP force. Despite the disparity in manpower and funding between the rest of USASOC and the PSYOP regiment, they hold the task to persuade, change, and influence through all mediums in which target audiences receive information.

> *Irregular warfare (IW) is defined as a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. When MISO occurs in IW, their role usually is much greater than during major operations and campaigns. MISO are key supporting operations to each contextual application of indirect approaches to executing IW. The ideological and political factors associated with IW create a fertile field for MISO.* (Joint Chiefs of Staff, 2010).

To truly assess the disconnect between the actions of the PSYOP regiment, doctrinal guidance, and the understanding by senior leaders of how psychological focused operations past, current, and future are to be used, simply ask a military member to describe PSYOP, MISO, Cognitive Warfare, or Information Operations.

An added restraint is the traditional way the military views seniority, expertise, and rank. In the past, experience matched rank as a service member progressed. Now, when dealing with IRCs often junior soldiers have more knowledge and expertise on the subject. This will continue to be a true fundamental issue among Cyber, IRCs, and other tech related fields.

11.4 FUTURE

The need for a collective understanding among senior leaders across the U.S. and International partners is necessary to begin the coordination and synchronization of the IRCs, not just MISO. If the addition of "Cognitive Warfare" as a discipline develops the sort of coordination across the force, then that is where it must start. A constant among IO practitioners is the need to educate their own command on the ability and need for proper funding, manning, and training. The addition of a fresh look at the human dimension could provide the basis for shifting the mindset of senior leaders.

The need for an organization solely focused on the information realm and a centralized approach is required not just in the U.S. but throughout international partners as well. However, the synchronization will never be successful if the information realm is not taken seriously, and we continue prioritizing other areas.

Technology's role in the cognitive and information space is one of the largest gaps we currently have between adversaries and our partners. Without a true reassessment and reorganization of priorities, the gap will continue to grow. We now live in a world where a digital model can mimic not just physical attributes but also cognitive/human attributes. Digital twins could be developed to assist in the planning and understanding of our forces. Publicly Available Information (PAI), and Open-Source Intelligence (OSINT) provides more usable information than ever before. Our forces regularly provide information to private industry, foreign actors, and the public that when properly aggregated, and visualized allows for the largest operational security issues imaginable.

11.5 CONCLUSION

With the growing Information Environment, target audiences are living in an over-saturated world. This requires a truly cognitive, psychological centered approach to persuade, change, and influence. As the inability to trust information resources continues to grow, the need to understand the mental drivers that lead to the how of providing the information that has the trust of a target audience becomes more important. The history of global competition and conflict are not far off base from the struggles we currently face. The continued coordination of information from past, present, and future require addressing true gaps rather than perceived doctrinal needs. Also, there are current forces at the forefront of this working environment that should be addressed rather than recreation of efforts. As time will continue, units looking to maintain relevancy or establish their own IO-focused effort will continuously re-create a wheel that began over 70 years ago. Doctrine written in 2012 provides a framework for Joint Task Forces focused on IO, personnel are doing so now, yet we continuously look to re-define operations focused on human behavior. First, we must educate our own leaders on the current capabilities and then allow subject matter experts to guide their field.

11.6 REFERENCES

Joint Chiefs of Staff (2010). Military Information Support Operations. Washington (DC – USA): Department of Defence. Joint Doctrine Publications: 3-0 Operations Series, Joint Publications Operations Series. JP 3-13.2.

Joint Chiefs of Staff (2012). Information Operations. Washington (DC – USA): Department of Defence. Joint Doctrine Publications: 3-0 Operations Series, Joint Publications Operations Series. JP 3-13.

Norton, B. (2021, October 9). Behind NATO's "Cognitive Warfare": "Battle for Your Brain" Waged by Western Militaries. The Grayzone. https://thegrayzone.com/2021/10/08/nato-cognitive-warfare-brain/.

Oechsner, F.O. (1943). NND843099, Memorandum, PWB Field Teams – Combat Teams. (Declassified January 2009).

Office of Strategic Services. (1943). Morale Operations Field Manual – Strategic Services (Manual No. 2 ed.). Fort Bragg (NC – USA): OSS Reproduction Branch.

Tzu, S. (1910). Sun Tzu on the Art of War, translated by Lionel Giles. Classics Etexts Series, Allandale Online Publishing (2000).

US Army. (2020). Psychological Operations. Goarmy.Com. https://www.goarmy.com/careers-and-jobs/specialty-careers/special-ops/psychological-operations.html.

Chapter 12 – CONCLUSION – COGNITIVE WARFARE AND ITS IMPLICATIONS FOR THE NATO STO IST PANEL

Colonel Dr. Nikolai Stoianov[1]

"Our responsibility is to protect our soldiers to make them ready for cognitive warfare."

Technologies always change the ways in which different players enter into conflict and the strategies, operations and tactics of war, but the recent explosion of information and communication technologies and options for influencing different groups has totally changed the philosophy of combat. What appears obvious is that as cyber warfare and social warfare continue to increase, the number of kinetic conflicts may reduce and that the main target will become the human mind.

It will be harder to explain why someone needs to fight against somebody else (kinetically) but, at the same time, it will be easier to "switch" human thinking from one direction to another. Internet, Social Media, IoT, Big data, Machine learning, Artificial Intelligence, etc., all foster the possibilities for building advanced analyses based on the cognitive aspects defining our potential enemies' point of view and, conversely, our enemies will have options to know and understand us better.

Several research communities deal with this matter, in particular within STO in studies carried out by the IST, HFM, and SET panels. Currently, open issues far surpass solved ones. A lot of research topics will be explored in the future, based in the legal, human, and technological aspects of this subject.

As researchers and members of the IST community, we are responsible for developing technologies that can detect, identify, track, prevent and defend our soldiers against cognitive attacks and campaigns, making them ready for cognitive warfare.

Sofia, August 25, 2021.

The Chairman of the Information Systems Technology (IST) Panel of the NATO Science & Technology Organization (STO).

[1] Nikolai Stoianov is a colonel in the Bulgarian Army, and an associate professor at the National Military University "Vasil Levski" (Veliko Tarnovo). He is the deputy director of the Bulgarian Defence Institute (BDI) Iskar-Sofia. He represents Bulgaria as a member of the NATO Science & Technology Board (STB) and has been Chair of the Information Systems Technology (IST) panel of the NATO Science & Technology Organization (STO) since 2021.

Chapter 13 – BIOGRAPHIES

Air-Force General Eric AUTELLET

Eric Autellet is the French Armed Forces Deputy Chief of Defence. He was a fighter pilot and was General Director of the French Air Force Academy (Ecole de l'Air) in Salon-de-Provence – France from 2016 to 2018. Promoted to the rank of Major General, he was appointed Deputy Chief of the Air Force in April 2020 before taking the rank of General and the responsibility of French Armed Forces Deputy Chief of Defence in March 2021 in Paris, France.

Dr. Norbou BUCHLER

Norbou Buchler holds a PhD in Experimental Psychology, specializing in cognitive neuroscience (functional MRI) and computational modeling. His work has focused on applying network science approaches to Mission Command and human cybersecurity. He works as Chief of the Networked Systems Branch of the Human Systems Integration Division at the U.S. Army Combat Capabilities Development Command (DEVCOM) Analysis Center – Aberdeen Proving Ground, Maryland USA.

Pr. Bernard CLAVERIE

Bernard Claverie is a university professor, Honorary Director and Founder of ENSC, and a Cognitive Science researcher affiliated with the CNRS (UMR5218 – Bordeaux University FR). He is Editor-in-Chief of the online journal "Cognitive Engineering" – ISTE Open Science. He is a member and contributes to the work of the French Air Force ADER network.

Pr. Tanguy Struye DE SWIELANDE

Tanguy Struye de Swielande is a professor in International Relations at UC Louvain (Belgium). His research focuses on great power relations, the Indo-Pacific, power, grand strategy, and information warfare. As co-coordinator of the Belgian Ministry of Defence's Strategic committee updating the 2016 Strategic Vision, he supervised and led the work of a group of experts in writing the 2030 security environment and the Ministry's strategic vision in 2021.

Air-Force Lieutenant General Gilles DESCLAUX

Gilles Desclaux is president of RACAM (French Civil Aviation – Military Aviation Interface). He is researcher at the Human Engineering for Aerospace Laboratory (HEAL – ENSC Bordeaux- INP / THALES RAYTHEON SYSTEMS Massy FR) where he is coordinator of the "Anticipe" program focused on AI-human decision support processes for Air Command and Control (C2).

LCol. François DU CLUZEL DE REMAURIN

François du Cluzel is a retired Lieutenant Colonel of the French Army (cavalry). He is currently Head of Innovative Projects at the Innovation Hub of NATO's Allied Command Transformation (ACT) in Norfolk, Virginia USA. He is particularly in charge of new dimensions of military action and of cognitive warfare.

Cadet Sam KONEN

Sam Konen is a cadet in his third year at the United States Military Academy. He is studying international affairs with a focus on security studies and great power competition.

Dr. Barbara KOWALCZUK

Barbara Kowalczuk teaches literature at the University of Bordeaux. She holds a PhD from Bordeaux Montaigne University (Tim O'Brien. L'Écriture de la hantise/Writing on What Haunts). Her research focuses on American literature and visual arts (19th – 21st centuries). She explores moral injury, war trauma, war ethics and the anthropology of war violence, as well as the accountability of perpetrators.

Air-Force General André LANATA

André Lanata is NATO Supreme Allied Commandeur Transformation. He was a fighter pilot in the first part of his military career and served as Chief of Staff of the French Air Force (CEMAA) from 2015 to 2018, and as Commander of NATO's ACT from 2018 to 2021.

Hervé LE GUYADER

Hervé Le Guyader is a graduate engineer in Electronics. Founder and former director of the European Center for Communication. He joined ENSC as Head of Innovation from 2016 to 2020. As a distinguished member of the STO IST panel, he partakes in activities led by NATO ACT's Innovation Hub. Today he serves as an associated member of ENSC where he facilitates the collaboration agreement with ACT for ENSC. He is a sworn judiciary cyber expert for the Court of Appeal and the Administrative Court of Appeal of Bordeaux FR.

Air-Force Major General Philippe MONTOCCHIO

Philippe Montocchio is a retired French Air Force Major General. He graduated from the French Air Force Academy and was a fighter pilot in the first part of his military career. General Montocchio then took over commanding positions, notably as the General Officer commanding French Forces stationed in Djibouti (2014 – 2016), before becoming the Director for International Relations in the French Armed Forces Joint Staff. He currently is the Deputy Director of the NATO Collaboration Support Office in charge of supporting the S&T cooperation between NATO Nations.

Kimberly ORINX

Kimberly Orinx is research assistant at UC Louvain (Université Catholique de Louvain, BE), researcher at CECRI and PhD student in International Relations, specializing in strategic culture and cognitive warfare. The subject of her thesis is China's cognitive warfare in Belgium.

Dr. Baptiste PRÉBOT

Baptiste Prébot is a graduate engineer in Cognitive Technology. He was recently awarded his Cognitive Engineering PhD from the University of Bordeaux with a thesis on "Shared Situation Awareness in Command and Control (C2) Activities." He served as assistant professor at ENSC and a researcher in UMR5218 (CNRS, University of Bordeaux, Bordeaux INP) from 2016 to 2021. Baptiste Prébot is currently a Research Fellow at the Dynamic Decision Making Laboratory of Carnegie Mellon University.

Col. Dr. Nikolai STOIANOV

Nikolai Stoianov is a colonel in the Bulgarian Army, and an associate professor at the National Military University "Vasil Levski" (Veliko Tarnovo). He is Deputy Director of the Bulgarian Defence Institute (BDI) Iskar-Sofia. He represents Bulgaria as a member of NATO Science & Technology Board (STB) and has been Chair of the Information Systems Technology (IST) Panel of the NATO Science & Technology Organization (STO) since June 2021.

John WHITEAKER

John Whiteaker has spent the last 5 years working as an active-duty Psychological Operations Specialist within the United States Army Special Operations community. His primary focus has been within the Indo-Pacific Command with additional work being done on academic and industry integration, supply chain risk management, and trans-regional problem sets.

Dr. Michael WUNDER

Dr. Michael Wunder is a mechanical engineer with a main focus on process engineering. His thesis concerned the economic growth of the steel industry. He served as system analyst at the automotive industry, followed by a position as Director for IT at an automotive supplier concern. Currently he is Director of the Department “C2 & Intelligence” at the Fraunhofer Institute for Communication, Information Processing and Ergonomics – FKIE – in Wachtberg (Germany). In parallel, Michael Wunder served as IST-Chair for 4 years, until May 2021.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
		ISBN 978-92-837-2392-9	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: The Future of Cognitive Dominance

7. Presented at/Sponsored by

First NATO scientific meeting on Cognitive Warfare (France) – 21 June 2021. Symposium organized by the Innovation Hub of NATO-ACT and ENSC, with the support of the French Armed Forces Deputy Chief of Defence, the NATO Science and Technology Organization / Collaboration Support Office, and the Region Nouvelle Aquitaine.

8. Author(s)/Editor(s)	9. Date
B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel	March 2022
10. Author's/Editor's Address	**11. Pages**
Multiple	118

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

Cognition; Cognitive bias; Cognitive domain; Cognitive war; Cognitive warfare; Cyber-psychology; Human

14. Abstract

This document, published by the NATO-CSO, brings together articles related to the presentations given during the first Symposium on Cognitive Warfare, held in Bordeaux, France, in June 2021, on the initiative of the NATO-ACT Innovation Hub and the Bordeaux-based ENSC, with the support of the French Armed Forces Joint Staff, the NATO-STO-CSO, and the Region Nouvelle Aquitaine. This first Symposium reflected on human cognition, its strengths and weaknesses, its collaborative organization for military decision-making, its relation with and dependence on digital technology, and its social and political dimensions within the context of fierce international competition. The Supreme Allied Commander for Transformation (SACT) and the French Armed Forces Vice-Chief of Defence expressed their views on the topic. This first Symposium was the starting point of a series of meetings and workshops further exploring the subject, on the initiative of NATO CSO and 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 978-92-837-2392-9