



AC/323(HFM-356)TP/1120



www.sto.nato.int

STO TECHNICAL REPORT

TR-HFM-ET-356

Mitigating and Responding to Cognitive Warfare

(Atténuer et répondre à la guerre cognitive)

This technical report documents the findings of HFM Exploratory Team 356.



Published March 2023





STO TECHNICAL REPORT

TR-HFM-ET-356

Mitigating and Responding to Cognitive Warfare

(Atténuer et répondre à la guerre cognitive)

This technical report documents the findings
of HFM Exploratory Team 356.

Edited by:

Dr. Yvonne R. Masakowski (USA) and Dr. Janet M. Blatny (NOR)

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published March 2023

Copyright © STO/NATO 2023
All Rights Reserved

ISBN 978-92-837-2433-9

Single copies of this publication or of a part of it may be made for individual use only by those organisations or individuals in NATO Nations defined by the limitation notice printed on the front cover. The approval of the STO Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

Table of Contents

	Page
List of Figures	vii
List of Tables	ix
List of Acronyms	x
Technical Activity Proposal	xi
Acknowledgements	xii
Disclaimer	xiii
HFM-356 Membership List	xiv
 Executive Summary and Synthèse	ES-1
 Chapter 1 – Towards a Framework of Science and Technological Competencies for Future NATO Operations	1-1
1.1 Introduction – A New Strategic Environment	1-1
1.2 The Challenges and Impact of Cognitive Warfare	1-3
1.3 To Defend and Mitigate	1-5
1.4 HFM-ET-356 Scope, Aims, and Proposed Outcomes	1-5
1.5 Organization of the Report	1-6
1.6 References	1-9
 Chapter 2 – Towards a Science and Technological Framework “The House Model”	2-1
2.1 Introduction	2-1
2.2 The House Model	2-1
2.2.1 The Pillars	2-3
2.2.2 The Horizontal Bars	2-3
2.3 Summary	2-4
 Chapter 3 – Cases and Scenarios of Cognitive Warfare	3-1
3.1 Introduction	3-1
3.2 Cognitive Warfare Case Study #1: Chrystia Freeland Smear Campaign	3-1
3.3 Cognitive Warfare Case Study #2: Novi Sanzhary COVID-19 Riots	3-4
3.4 Cognitive Warfare Case Study #3: Russo-Georgian War (2008)	3-5
3.5 References	3-7
 Chapter 4 – The Influence and Impact of Social and Cultural Sciences in Cognitive Warfare	4-1
4.1 Introduction	4-1
4.2 Method and Theory	4-1

4.3	Areas of Investigation Within Social and Cultural Science Impacting CogWar	4-3
4.4	Modus Operandi – A Cross-Cutting Enabler	4-4
4.5	References	4-5

Chapter 5 – Cognitive and Behavioral Science (Psychological Interventions) **5-1**

5.1	Introduction – Cognitive and Behavioral Science (Psychological Interventions)	5-1
5.2	Influence of Cognitive Warfare	5-1
5.3	Cognitive Warfare and Selective Attention	5-2
5.4	Recommendations	5-3
5.5	References	5-4

Chapter 6 – Developing Cognitive Neuroscience Technologies for Defence Against Cognitive Warfare **6-1**

6.1	Introduction – Cognitive Neuroscience: Defence Against Cognitive Warfare	6-1
6.2	Neuroscience and Neuromodulation Techniques	6-2
6.2.1	Neural and Brain-Machine Interfaces	6-3
6.2.2	Automation, Autonomy, and Artificial Intelligence (AI): Improved Human-Machine Teaming and Decision Making	6-4
6.2.3	Technical Areas Requiring De-Risking for Effective Counter-Cognitive Warfare	6-4
6.3	Recommendations and Concluding Remarks	6-5
6.3.1	Technical Gaps Limiting the Adoption of BMI Systems into Military	6-6
6.4	Science and Technology Directions: The Way Ahead	6-6
6.5	References	6-6

Chapter 7 – Defence Against 21st Century Cognitive Warfare: Considerations and Implications of Emerging Advanced Technologies **7-1**

7.1	Introduction	7-1
7.2	Social Media and Cyber Networks	7-3
7.3	Cognitive Security and Securing the Future	7-5
7.4	Defending Against Cognitive Warfare	7-6
7.5	Countering Cognitive Warfare	7-6
7.6	Ethical Implications of Technological Advances	7-7
7.7	The Role of Technological Competency	7-8
7.8	Conclusion and the Future Security Environment	7-8
7.9	References	7-9

Chapter 8 – Situational Awareness, Sensemaking and Future NATO Multinational Operations **8-1**

8.1	Introduction	8-1
8.2	Situational Awareness: A Human Endeavor	8-2

8.3	Cognitive Effects: Science and Technology Pillars	8-3
8.4	Decision Making and the OODA Loop in Cognitive Warfare	8-4
8.5	The OODA Loop Decision Making Cycle	8-4
8.6	Implications for the Future Security Environment	8-5
8.7	References	8-7

Chapter 9 – Human-Machine Teaming Towards a Holistic Understanding of Cognitive Warfare **9-1**

9.1	Introduction	9-1
9.2	Cognitive War and Human Cognition	9-3
9.3	The Holistic BowTie Model	9-6
9.4	Conclusion and Recommendations: How to Proceed with Cognitive Warfare and Beyond	9-8
9.5	References	9-10

Chapter 10 – Education and Training for Cognitive Warfare **10-1**

10.1	Introduction	10-1
10.2	Training and Education	10-2
10.3	Knowledge Development	10-4
10.4	Conclusion and Recommendations	10-5
10.5	S&T Recommendations	10-5
10.6	References	10-7

Chapter 11 – Simulator: Developing CogWar Resilience Through Social Media Training **11-1**

11.1	Introduction	11-1
11.2	Issues Related to Social Media Training	11-1
11.3	Proposed Solutions	11-2
11.4	Design Methods	11-3
11.4.1	Input from Potential Users and Core Goals that Emerged	11-3
11.4.2	Low Threshold for Use	11-4
11.4.2.1	Ease of Organizing Training	11-4
11.4.2.2	Content Control	11-4
11.5	Lessons Learned and Future Directions	11-6
11.6	References	11-7

Chapter 12 – Legal and Ethical Implications Related to Defence Against Cognitive Warfare **12-1**

12.1	Introduction	12-1
12.2	Defending against Cognitive Warfare: Issues related to <i>jus ad bellum</i>	12-1
12.3	The Conduct of War: Thoughts on Issues Related to <i>jus in bello</i>	12-3
12.4	Conclusion and Recommendations for Future Research	12-3
12.5	References	12-4

**Chapter 13 – Cognitive Warfare and the Human Domain:
Appreciating the Perspective that the Trajectories of
Neuroscience and Human Evolution Place Cognitive Warfare
at Odds with Ideas of a Human Domain****13-1**

13.1	Introduction	13-1
13.2	The Human Domain as Defined in the Literature	13-1
13.3	Cognitive Warfare and the Human Domain: Is a Human Domain at Odds with the Trajectory of Neuroscience and Human Evolution?	13-3
13.4	Conclusion and Future Perspectives	13-3
13.5	References	13-4

Chapter 14 – Science and Technology Roadmap Based on the House Model**14-1**

14.1	Introduction	14-1
14.2	Overview of Overall Future S&T Areas	14-3
14.3	Cognitive Neuroscience, Behavioral, and Social and Cultural Pillars	14-4
14.3.1	Pillar One: Cognitive Neuroscience	14-4
14.3.2	Pillar Two: Cognitive and Behavioral Science	14-5
14.3.3	Pillar Three: Social and Cultural Science	14-5
14.4	Sensemaking and Situational Awareness: Precursors to Achieving Decision Superiority	14-6
14.5	Cognitive Effects and <i>Modus Operandi</i>	14-7
14.6	Technology Enablers and Force Multipliers	14-7
14.6.1	Adaptive Command and Control, Brain-Machine Interfaces and SA	14-8
14.6.2	Human-Machine Teaming and Training	14-9
14.7	Ethical and Legal Implications	14-9
14.8	Conclusion and Recommendations	14-10
14.9	References	14-11

Chapter 15 – Conclusion and Recommendations**15-1**

15.1	Introduction	15-1
15.2	Emerging Technologies and Cognitive Warfare	15-2
15.3	Future Human Systems, Factors, and Performance and Cognitive Warfare	15-2
15.4	Concluding Remarks	15-4

List of Figures

Figure		Page
Figure 2-1	The House Model Developed by HFM-ET-356	2-2
Figure 2-2	The Scientific Pillars of Knowledge – House Model of CogWar ET 356	2-3
Figure 6-1	Differences Between CogWar and PSYOPS (Claverie and Cluzel, 2022)	6-2
Figure 8-1	The House Model: Sensemaking and Situational Awareness	8-2
Figure 8-2	The OODA Loop Decision Cycle (John Boyd, 1986)	8-5
Figure 9-1	One of the Spears of Schoeningen as an Early Example of Human Factors, Human Systems Integration and of Cognitive Warfare (Thieme, 1997)	9-1
Figure 9-2	Cognitive Loop and Perception-Action Cycle of Humans or Machines	9-3
Figure 9-3	Top: Signal Detection Theory; Bottom: Cognitive Loop and OODA Loop of Humans or Machines, with Decision to Action or Non-Action Under Uncertainty (“In the Fog of War”)	9-4
Figure 9-4	A Look into the Details of Cognitive Processes in Individuals or Organizations: Example OODA Loop of Observation, Orientation, Decision, and Action (Boyd, 1996)	9-5
Figure 9-5	Human-Machine System and Cooperation with Other Agents, Forming Joint Cognitive Systems of Interlinked OODA-Loops	9-6
Figure 9-6	Holistic Bowtie Model of Human-Machine Cognition (Adapted from Flemisch et al. 2022)	9-7
Figure 9-7	Holistic Bowtie Model of Cognitive Warfare, with Examples for Defence and Attack Vectors, and One Feedback Loop from Accountability to Ability, Authority, Transparency, and Trust	9-8
Figure 9-8	Outlook, Holistic Bowtie Model, Including an Ethical Layer into Physical and Cognitive Warfare	9-10
Figure 10-1	Hierarchy of Competence	10-3
Figure 11-1	Screenshot of Mastodon, the Twitter Clone	11-3
Figure 11-2	Second of the Five Steps When Deploying Somulator	11-4
Figure 11-3	Prepared Content Ready for Deployment in Somulator	11-5
Figure 14-1	The House Model Proposed by HFM-ET-356	14-2
Figure 14-2	The Link Between the House Model and the Observe, Orient, Decide and Act (OODA) Loop	14-2

Figure 14-3 OODA-Loop of Observation-Orientation-Decision-Action
(Boyd's)

14-6

List of Tables

Table		Page
Table 6-1	Technical Areas of Neurotechnology Requiring De-Risking	6-4

List of Acronyms

AI	Artificial Intelligence
AUV	Autonomous Undersea Vehicle
BDA	Battle Damage Assessment
BMI	Brain Machine Interface
C ²	Command-and-Control
COGSEC	Cognitive Security
CogWar	Cognitive Warfare
DRL	Deep Reinforcement Learning
ELSEI	Legal and ethical frameworks
FFAO	Framework for Future Alliance Operations
ICT	Intelligence Communication Technology
IE	Information Environment
INFOSEC	Information Security
IPB	Intelligence Preparation of the Battlespace
ISR	Intelligence, Surveillance, Reconnaissance
ML	Machine Learning
NBIC	Nano, Biotech, Information tech, Cognitive
NGO	Non-Governmental Agency
OODA	Observe-Orient-Decide-Act
OPSEC	Operational Security
OSINT	Operation Security Intelligence
PfP	Partners for Peace
PSYOPS	Psychological Operations
PTSD	Post Traumatic Stress Syndrome
QKD	Quantum Key Distribution
R&D	Research and Development
S&T	Science and Technology
SA	Situational Awareness
TAP	Technical Activity Proposal

Technical Activity Proposal

Panel/Group	HFM	Activity Title	
Reference Number	HFM-ET-356	Mitigating and responding to Cognitive Warfare	
Activity Type	Exploratory Team		
Panel Approval Date	Board Approval Date	Activity Start Date	Activity End Date
Related Activity	D3TX, NATO ACT		
Projected Meeting Location(s)			
Lead Nation(s)	Norway		
Team Leader(s)	Dr Janet M. BLATNY (NOR) & Dr. Yvonne R. MASAKOWSKI (USA)		
Panel/Group Mentor			
NATO Nations/Orgs Invited to Participate	NATO Bodies		
Non-NATO Nations/Orgs Invited to Participate	STOEOP		
Nations/Orgs Committed to Participate			
Security Classification Level or Marking of the Activity	Releasable to the Public		
Keywords	Cognitive, Artificial Intelligence, Cyber, Human, Information, Neuroscience, Trust, Cognitive Warfare		
NATO and National Resources Required	<p>Support from CSO to facilitate physical meetings and/or coordinate digital meetings (Webex). Assistance from CSO creating the video to enable communication and exploitation of the results. Request for funding:</p> <ul style="list-style-type: none"> • Support of notetaking and engaging a rapporteur • Keynote speakers 		

Acknowledgements

The Human Factors and Medicine (HFM) Exploratory Team (ST) 356 on **Mitigating and Responding to Cognitive Warfare** (HFM-ET-356) operated in the context of the NATO Science and Technology Organization (STO) Human Factors and Medicine (HFM) Panel. The ET-356 team consists of representatives from Canada, Germany, Italy, the Netherlands, Norway, United Kingdom, and the United States. Representatives from the NATO STO Information Systems Technology Panel (IST) Panel also took part.

We would especially like to acknowledge the support of the NATO STO HFM Executive and NATO CSO staff.

The Chair (Norway) and Co-Chair (United States) of HFM-ET-356 are grateful for all the efforts by the HFM-ET-356 Team. Over the course of its 1-year mandate, the Team held numerous virtual meetings, virtual due to the impact of COVID-19. Still, the HFM-ET-356 Team has successfully enabled the establishment of new networks and relationships through its work.

Members of HFM-ET-356 participated in the **NATO Tide Sprint Spring Cognitive Warfare (CogWar) Workshop** hosted in Poland, April 4 – 8, 2022. The hosts of this conference provided support for the Tide Sprint CogWar workshop and facilitated virtual participation for members and participants. We would like to acknowledge the Directors, Organizers, Staff, and Facilitators of the NATO ACT Tide Sprint Spring Conference for their support of the CogWar workshop and share our team's appreciation for their generous hospitality and the logistical support they provided.

Disclaimer

This publication contains the opinions of the respective authors only. They do not necessarily reflect the policy or the opinion of their institution, NATO, or any agency or any government.

STO may not be held responsible for any loss or harm arising from the use of information contained in this report and is not responsible for the content of the external sources, including external websites referenced.

HFM-356 Membership List

CHAIR

Dr. Janet M. BLATNY*
Norwegian Defence Research Establishment
NORWAY
Email: janet-martha.blatny@ffi.no

CO-CHAIR

Dr. Yvonne R. MASAKOWSKI*
US Naval War College
UNITED STATES
Email: Yvonne.masakowski@innovationhub-act.org

MEMBERS

Ms. Lea BJORGUL*
Norwegian Defence Research Establishment
NORWAY
Email: Lea-Kristina-Petronella.bjorgul@ffi.no

Dr. Jennifer CARPENA
Air Force Research Laboratory
UNITED STATES
Email: jennifer.carpena.ctr@us.af.mil

Mr. Francois-Pierre DU CLUZEL DE REMAURIN
NATO Allied Command Transformation
NATO ACT
Email: francois-pierre.ducluzelderemaurin@act.nato.int

Dr. Johan EGBERT KORTELING*
TNO
NETHERLANDS
Email: hans.korteling@tno.nl

Prof. Dr. Frank FLEMISCH*
Fraunhofer
GERMANY
Email: f.flemisch@iaw.rwth-aachen.de

Mr. Eskil GRENDALH SIVERTSEN*
Norwegian Defence Research Establishment
NORWAY
Email: eskil-grendahl.sivertsen@ffi.no

Dr. Claude GRIGSBY II*
Air Force Research Laboratory
UNITED STATES
Email: claude.grigsby@us.af.mil

Prof. Dr. Jose KERSTHOLT
TNO Human Factors
NETHERLANDS
Email: Jose.Kerstholt@tno.nl

Dr. Benjamin James KNOX*
Norwegian Armed Forces Cyber Defence Warfare Center
NORWAY
Email: bknox@mil.no

Mr. Mike LAFIANDRA
Office of Naval Research
UNITED STATES
Email: michael.e.lafiandra.civ@us.navy.mil

Mt. Matthew LAUDER*
Defense Research and Development Canada
CANADA
Email: Matthew.Lauder2@ecn.forces.gc.ca

Mr. Herve LE GUYADER
Ecole Nationale Supérieure de Cognitique
FRANCE
Email: herve.le-guyader@ensc.fr

* Contributing Author

Dr. Patrick MASON
Department of Defense
UNITED STATES
Email: Patrick.a.mason2.civ@us.navy.mil

Dr. Richard MCKINLEY*
Air Force Research Laboratory
UNITED STATES
Email: richard.mckinley.2@us.af.mil

Mr. Paolo PROIETTI
Leonardo SpA
ITALY
Email: paolo.proietti@leonardo.com

Mr. Antoine SMALLEGANGE
TNO
NETHERLANDS
Email: antoine.smallegange@tno.nl

ADDITIONAL CONTRIBUTORS

Mr. Torvald ASK*
Norwegian University of Science and Technology
NORWAY
Email: torvalda@stud.ntnu.no

Dr. Arild BERGH*
Norwegian University of Science and Technology
NORWAY
Email: arild.bergh@ffi.no

Colonel Sohrab DALAL
NATO Allied Command Transformation
NATO ACT
Email: Sohrab.dalal@act.nato.int

CDR Paul GROESTAD
NATO Allied Command Transformation
NATO ACT
Email: Paul.groestad@act.nato.int

Dr. Nathaniel BRIDGES*
Air Force Research Laboratory
UNITED STATES
Email: Nathaniel.Bridges@us.af.mil

* Contributing Author



Mitigating and Responding to Cognitive Warfare

(STO-TR-HFM-ET-356)

Executive Summary

The NATO Science and Technological Organization (STO) Human Factors and Medicine (HFM) Exploratory Team (ET) 356 performed an assessment of the Science and Technologies required to mitigate and defend against Cognitive Warfare (CogWar). The ET-356 proposed a Science and Technology (S&T) roadmap to guide NATO and Allied Partners in future research activities and investments.

For NATO to have the capability to acquire and preserve Decision and Cognitive Superiority over their adversaries and across the conflict spectrum, scientific based knowledge is needed to support and increase NATO's operational readiness to respond to CogWar. CogWar is not necessarily new but has emerged as a product of the integration and confluence of many technological advances and as availability and access to information and technology has increased. CogWar takes well-known methods within warfare to a new level by attempting to alter and shape the way humans think, react, and make decisions. CogWar has emerged replete with security challenges due to its invasive, intrusive, and invisible nature and *where the goal is to exploit facets of cognition to disrupt, undermine, influence, or modify human decisions* (proposed by ET-356).

CogWar represents the convergence of a wide range of advanced technologies along with human factors and systems, such as Artificial Intelligence (AI), Machine Learning (ML), Information Communication Technologies (ICT), neuroscience, biotechnology and human enhancement that are being deliberately used by NATO's adversaries in the 21st century battlespace. CogWar presents a significant risk to global defence and security at every level including economic, geopolitical, social, cultural, as well as threatening human decision making.

The task of ET-356 was focused solely on identifying and suggesting defensive S&T to strengthen the Alliance's deterrence against CogWar and improve NATO's and national resilience critical to NATO's core tasks to safeguard Allied nations, societies, and shared values.

CogWar gives rise to the adversaries' ability to shape human cognition, perception, sensemaking, situational awareness, and decision making at all levels. The ability to intentionally (mis)use information within digital networks and disseminate it globally on various platforms such as social media has given rise to new tools and methods for the adversary. CogWar also aims at disrupting relationships and targets human vulnerabilities, such as trust and cognitive bias, at both individual and national levels, and its impact is across all operational domains. This report presents a summary of the key areas of S&T that are required to mitigate and defend against CogWar.

The proposed S&T Road map is based on a "House Model," developed by ET-356, and is linked to the operational Observe, Orient, Decide, and Act (OODA) decision cycle. The House Model represents seven main *S&T knowledge areas and enablers* that are cross-cutting and intersectional related: Pillars: Cognitive Neuroscience, Cognitive and Behavioral Science, Social and Cultural Science; and Bars: Situational Awareness and Sensemaking, Cognitive Effects, Modus Operandi and Technology and Force Multipliers. The seven areas provide the basis for research discussions within NATO STO and its Panels and Groups.

This report provides guidance for future research within NATO STO, Allies, and national S&T investments for defence against current and future CogWar and to strengthen NATO's technological edge and strategic

advantage against CogWar. The work by the HFM ET-356 underpins the NATO Warfighting Capstone Concept and its Warfare Development Initiative Cognitive Superiority, and the new NATO Strategic Concept declared at the NATO Madrid Summit 2022.

Atténuer et répondre à la guerre cognitive

(STO-TR-HFM-ET-356)

Synthèse

L'équipe exploratoire (ET) 356 de la Commission sur les facteurs humains et la médecine (HFM) de l'Organisation pour la science et la technologie (STO) de l'OTAN a réalisé une évaluation de la science et des technologies requises pour atténuer la guerre cognitive (GC) et s'en protéger. L'ET-356 a proposé une feuille de route de science et technologie (S&T) afin de guider l'OTAN et les partenaires alliés dans leurs futures activités de recherche et leurs futurs investissements.

Si l'on veut que l'OTAN ait la capacité d'acquérir et conserver une supériorité décisionnelle et cognitive par rapport à ses adversaires et dans l'ensemble du spectre des conflits, des connaissances scientifiques doivent étayer et renforcer la préparation opérationnelle de l'OTAN à la guerre cognitive. La guerre cognitive n'est pas nécessairement nouvelle ; elle découle de l'intégration et de la convergence de nombreuses avancées technologiques à une époque où la disponibilité et l'accès à l'information et à la technologie ont augmenté. La guerre cognitive exploite les méthodes bien connues de la guerre, mais à un niveau inédit, en essayant de modifier et de façonner la manière dont les humains pensent, réagissent et prennent des décisions. La guerre cognitive entraîne des problèmes de sûreté, en raison de sa nature invasive, intrusive et invisible, *puisque son objectif est d'exploiter les différentes facettes de la cognition pour perturber, saper, influencer ou modifier les décisions humaines* (définition proposée par l'ET-356).

La guerre cognitive représente la convergence d'un large éventail de technologies perfectionnées avec les facteurs et systèmes humains tels que l'intelligence artificielle (IA), l'apprentissage automatique (ML), les technologies de l'information et de la communication (TIC), les neurosciences, la biotechnologie et l'amélioration de l'être humain, qui sont délibérément utilisés par les adversaires de l'OTAN dans l'espace de bataille du 21e siècle. La guerre cognitive constitue un risque important pour la défense et la sûreté mondiales sur tous les plans, notamment économique, géopolitique, social et culturel, ainsi qu'une menace pour la prise de décision humaine.

La tâche de l'ET-356 était uniquement d'identifier et de suggérer une S&T *défensive* pour renforcer la dissuasion de l'Alliance vis-à-vis de la guerre cognitive et améliorer la résilience des pays et de l'OTAN, qui est essentielle aux tâches fondamentales de l'OTAN, à savoir protéger les pays alliés, les sociétés et les valeurs partagées.

La guerre cognitive donne aux adversaires la capacité de façonner la cognition humaine, la perception, la création de sens, la connaissance de la situation et la prise de décision à tous les niveaux. La capacité à utiliser intentionnellement (de manière abusive) les informations sur les réseaux numériques et à les diffuser à l'échelle mondiale sur différentes plateformes, telles que les réseaux sociaux, a fait émerger de nouveaux outils et méthodes pour l'adversaire. La guerre cognitive, qui vise également à perturber les relations, cible les vulnérabilités humaines, telles que la confiance et le biais cognitif, tant au niveau individuel que national. Son impact s'étend à tous les domaines opérationnels. Ce rapport présente un résumé des domaines clés des Sciences et Technologies (S&T) nécessaires pour atténuer les conséquences de la guerre cognitive et se défendre contre cette dernière.

La feuille de route S&T proposée se fonde sur un modèle développé par l'ET-356. Elle est liée à la boucle décisionnelle OODA (observation, orientation, décision, action). Le modèle représente sept principaux

domaines de connaissances et outils S&T qui sont transversaux et intersectionnels : Piliers : Neurosciences cognitives, sciences cognitives et comportementales, sciences sociales et culturelles ; et barres : Conscience de la situation et sensibilisation, effets cognitifs, Modus operandi (manière de procéder), et technologie et multiplicateurs de force. Les sept domaines constituent la base des discussions de recherche au sein de la STO de l'OTAN et de ses commissions et groupes.

Le présent rapport fournit des conseils sur les futures recherches au sein de la STO de l'OTAN et sur les investissements en S&T des Alliés et des pays pour la défense contre la guerre cognitive actuelle et future, en vue de renforcer l'avantage technologique et stratégique de l'OTAN dans ce domaine. Les travaux du HFM ET-356 sous-tendent le concept fondamental de guerre de l'OTAN et sa supériorité cognitive dans l'initiative de développement de la guerre, ainsi que le nouveau concept stratégique de l'OTAN déclaré lors du sommet de Madrid de l'OTAN en 2022.

Chapter 1 – TOWARDS A FRAMEWORK OF SCIENCE AND TECHNOLOGICAL COMPETENCIES FOR FUTURE NATO OPERATIONS

Janet M. Blatny

Norwegian Defence Research Establishment
NORWAY

Yvonne R. Masakowski

US Naval War College
UNITED STATES

Strategic competition, pervasive instability and recurrent shocks define our broader security environment. The threats we face are global and interconnected... We will invest in our ability to prepare for, deter, and defend against the coercive use of political, economic, energy, information and other hybrid tactics by states and non-state actors.

NATO Strategic Concept 2022

1.1 INTRODUCTION – A NEW STRATEGIC ENVIRONMENT

The complexity of the 21st century operational environment has increased significantly since the turn of the 20th century. The North Atlantic Treaty Organization (NATO) has expanded its membership and increased the level of multinational military coalition operations, as well as the range of missions, including humanitarian, disaster relief, counterterrorism, regional conflicts, and traditional warfare. The complexity, diversity and tempo of these multinational military operations has increased, driven by factors such as the influence of technological advances, increase in regional conflicts and asymmetric warfare, as well as the emergence of conflicts such as the Russia-Ukraine war where Russia invaded Ukraine 24 Feb 2022 (Zinets and Vasovic, 2022).

During the NATO Summit in Brussels 2021, the following was stated (NATO 2021, Brussels Summit):

- *We remain concerned with China's frequent lack of transparency and use of disinformation.*
- *We are increasingly confronted by cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies.*

The NATO 2030 Reflection Group stated (NATO 2030 Reflection Group, 2020):

NATO and Allies must develop more capabilities for operating in the cognitive and virtual dimensions, including at the tactical level. These capabilities are needed to detect disinformation and provide support in preventing or limiting its impact, including by better understanding people, networks, online information, and related narratives. Simultaneously, NATO and Allies need to establish the legal and ethical framework to be able to operate in these dimensions effectively and legitimately.

These statements clearly highlight the need to have defence and security measures against hybrid tactics including CogWar approaches that our adversaries might and can use against NATO.

The 2010 Strategic Concept in NATO specified NATO's core missions: collective defence, crisis management, and cooperative security (NATO, 2010). These three-core mission concepts were discussed in the NATO Strategic Concept 2022, declared at the NATO Madrid Summit 2022 (NATO, 2022). The Madrid Summit 2022 highlighted the concern of the radically changed security environment and stated, “Today we endorse a new

Strategic Concept to ensure our Alliance remains fit and resourced for the future". Furthermore, the concern stated in 2021 at the Brussel Summit was again stressed during the Madrid Summit 2022: "We are confronted by cyber, space, and hybrid and other asymmetric threats, and by the malicious use of emerging and disruptive technologies". The new 2022 Concept emphasizes NATO's responsibility of ensuring the collective defence using a 360-degree approach to strengthen deterrence and defence across all domains and threats and enhances the need for military and civilian collaboration especially within cyber defence.

NATO faces an environment that is dynamic, global, complex, and uncertain. The boundaries between peace and conflict, political and military, strategic and tactical, kinetic, and non-kinetic are blurring. Potential strategic competitors continuously seek to undermine NATO's political and military-strategic objectives by deploying increasingly sophisticated strategies, often through coordinated political, military, economic, and information efforts. This has required new ways of thinking and approaches resulting in the important strategic NATO Warfighting Capstone Concept (NWCC) document (2021) that addresses temporal, spatial, functional, and structural aspects of the Alliance's approach to long term warfare development and warfighting (Tammen, 2021).

This concept describes NATO's focus on the new Alliance thinking and approach towards a simultaneous, non-linear paradigm to balance the efforts across the operational contexts of shaping, contesting, and fighting. This is critical, especially as the traditional peace, crisis, and conflict paradigm increasingly constrains NATO's ability to out-think and out-perform an adversary. *This report highlights the Science and Technology Roadmap to defend against the influence and impact of Cognitive Warfare.*

The NWCC focuses on five Warfare Development Imperatives (WDI) to accomplish NATO's core missions: cognitive superiority, layered resilience, influence and power projection, collaboration and coalition of cross-domain command, and integrated multi-domain defence (see call-out box, below). CogWar is centered in Cognitive Superiority (NWCC, WDI) and has ramifications for *layered resilience, influence and power projection and cross-domain command*.

NATO Warfighting Capstone Concept (NWCC) Warfare Development Initiatives (WDI)

Cognitive superiority: Truly understanding the operating environment, the adversary and the Alliance's goals entails cohesive and shared political-military understanding of the threats, adversaries and environment NATO operates in, from tech and doctrine, to JISR and big data. Equally, it will focus on providing the right tools for the political-military level to operate effectively (rapidly and dynamically) and safeguard decision making in the modern information age.

Layered resilience: Underpinning deterrence, the Alliance needs to be able to withstand immediate shocks to supply lines and communications, as well as effects in the cognitive dimension. It must be prepared to persevere in challenging situations over long periods and be ready from day zero.

Influence and power projection: To shape the environment to its strengths, including generating options and imposing dilemmas on adversaries, the Alliance must be proactive in taking initiative through various means to reach its objectives.

Integrated multi-domain defence: The threats that the Alliance faces are no longer in any one domain, so a joint and flexible approach to a fluid environment is essential to protect the Alliance's integrity against all threats, regardless of their origin or nature.

Cross-domain command: Command insight at the blink of an eye, the hallmark of great generals, may be out of reach in a multi-domain and integrated battlespace. Investing in our people, the art of command, critical thinking and audacious action will underpin success.

The impact of Emerging Disruptive Technologies (EDTs) relates to the five WDIs, as technology is one of the main drivers for WDI. Technology and Cognitive Superiority are critical elements to counter CogWar. Technological advances, as well as advances in cognitive neurosciences will influence our ability to achieve situational awareness and maintain the decision advantage in military operations (NATO STO, 2021). The strategic defence against CogWar requires that NATO maintain technological and cognitive superiority to strengthen NATO's resilience and military operational readiness.

In addition to the five operational domains (land, air, sea, cyber and space), discussions within various communities are ongoing to consider a new domain: "the cognitive (or the human) domain" (Cole and Le Guyader, 2020). The cognitive dimension represents a space where intra and inter domain cognitive operations can be conducted. This discussion is addressed in Chapters 11 and 12.

The NATO HQ ACT Concept Development Branch is currently developing a NATO concept on CogWar (2022). The work is part of the implementation of the NWCC, and the CogWar Concept is a delivery under the WDI Cognitive Superiority Initiative. The concept work started in 2021 and the proposed end state of the concept work is for NATO to regain the initiative by establishing a better, shared understanding of the cognitive dimension, the creation and countering of cognitive effects, and the protection of NATO's decision-making processes. Also, the NATO Industrial Advisory Group (NIAG) is conducting a study on Standards for Cognitive Augmentation for Military Applications (NIAG, 2022). There are several definitions of CogWar put forth, however, there is not yet a commonly accepted definition of CogWar. For example, CogWar is a multidisciplinary approach combining social sciences and innovative technologies to directly alter the mechanisms of understanding and decision-making to destabilize or paralyze an adversary (Pappalardo, 2022). Du Cluzel (2022) describes CogWar as the manipulation of the enemy's cognition aimed at weakening, influencing, delaying, and even destroying the enemy (Claverie et al., 2022). This type of warfare aims at influencing the heuristic of the human brain to win the "war before the war" (Takagi, 2022). Attacks of this type now no longer target policymakers or military decision-makers alone, but a broad mass that can potentially influence national decision-making (Takagi, 2022). In general, CogWar addresses the human's ability to process information and use it conflicting purposes, such as influencing military and civilian populations, organizations, and nations.

The HFM Exploratory Team 356 has therefore proposed the goal of CogWar as to exploit facets of cognition to disrupt, undermine, influence, or modify human decision making. This covers decisions also made by technological advances, as humans will always be a part of all operations.

The first NATO symposium on CogWar was held in Bordeaux, June 2021, arranged by the NATO ACT innovation Hub and the Ecole Nationale Supérieure de Cognitique (ENCS), France (Claverie et al., 2022).

1.2 THE CHALLENGES AND IMPACT OF COGNITIVE WARFARE

CogWar has been described as a multidisciplinary approach that provides a means for altering human thought, understanding, and decision making (Pappalardo, 2022). Adversaries infiltrate global digital networks at all levels to achieve their strategic objectives. CogWar attacks aim to create chaos, confusion, disrupt societies and government, and shape the geopolitical and social environments in accordance with an adversary's strategic objectives. CogWar has been viewed as an extension of Information Warfare and Psychological Operations (PsyOps). However, CogWar differs as it is the convergence of PsyOps, Information Operations (Ops) and Cyber Operations, integrated with Artificial Intelligence (AI) / Machine Learning (ML) networks and capabilities that extend its reach globally to military and civilian populations. CogWar attacks impact the broad mass population to

influence and impact civilian and military decision making. Advances in AI/ML technologies have made this technology a force enabler for the dissemination of misinformation and disinformation. Adversaries exploit these advances to set the conditions in the physical and digital battlespace in accordance with their military and national agendas.

Traditional warfare is being and will continue to be transformed by advances in AI/ML and BMI technologies. Advanced AI/ML technologies have given rise to the design of cognitive-inspired systems, which have facilitated the dissemination of misinformation and disinformation campaigns aimed at shaping human thinking, behavior, and actions. EDTs such as AI, ML, big data, cloud computing, IoT, GANs, multi-reality tools, modern ICTs, biotechnology, neuro-technologies, and other human augmenting technologies have contributed to the “power of CogWar” (NATO S&T Technology Trend Report, 2020). Increased access to information has augmented the velocity and accuracy of attacks and threats to civilian and military populations.

CogWar presents a danger to national and global stability and security at every level, including economic, geopolitical, social, and cultural. The technologies that facilitate the rapid dissemination of information to a global audience do it at a lower cost and present less risk to the aggressor. The recent COVID-19 pandemic provides evidence of the impact of disinformation campaigns on social media platforms. Lessons learned because of the spread of COVID-19 disinformation were recently published by Gill and Goolsby (2022)¹.

The use, misuse, and even the weaponization of information and advanced cognitive-inspired systems, serve as a critical threat to human thinking and decision making, not only between humans but between humans and machines, as well as autonomous machine decision making.

CogWar targets human vulnerabilities as a means of creating chaos and confusion in the mass consciousness, across nations, and the within militaries. Adversaries will target vulnerabilities in the OODA decision-making framework (Chapter 9) as a means exploit cognitive vulnerabilities, or to deliver cognitive effects. Thus, NATO nations must invest in S&T tools, techniques, and technologies that will defend against CogWar.

To address these threats, there is a need to understand the future impact of convergence between human and machine as technology develops and advances. “It becomes increasingly clear that the teaming of human and computers will become essential for any form of CogWar, whether offensive or defensive” (Chapter 9). Future human-machine teams will work collaboratively to transform the future battlespace, influencing military and civilian communities, and impacting society, including economic and political domains.

CogWar capability to impact decision making (positively or negatively) across all domains within the OODA decision framework highlights the need to develop tools for information validation and measures to ensure that data is dependable, accurate and from a trusted source. As technologies and tools evolve, there is a need to prepare to counter the effects of such tools when used by the adversary and ensure that the NATO Alliance can defend against potential attacks.

CogWar transforms the battlespace and presents challenges and threats/danger. There is therefore a strategic and operational imperative to develop Science and Technology (S&T) initiatives to mitigate and defend against CogWar if we are to ensure the defence and security of NATO and Allied Partners’ nations.

¹ The NATO STO Research Task Group 273 “Digital and Social Media Assessment for Effective Communication and Cyber Diplomacy” promoted a shared understanding of the information environment, addressed the hazards of disinformation and propaganda, and outlined the attempts to undermine the Alliance during the COVID-19 pandemic. This work founded the basis for the book “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective (Gill and Goolsby, 2022).

Misinformation and disinformation campaigns, as well as “poisoned” training datasets embedded in algorithms may be introduced into trusted networks or social media, and/or databases to influence human thought and behavior towards supporting an adversary’s strategic agendas. Thus, human cognitive processes can unwittingly be manipulated to shape human decisions and behaviors that align with those of an adversary. *“Trust” is the adversaries’ target and an essential component of CogWar in which the human is the vulnerable target.*

1.3 TO DEFEND AND MITIGATE

The operational environment consists of physical, virtual/cyber, and human/cognitive dimensions – in other words – a socio-technological environment. Therefore, increasing defensive CogWar capabilities within NATO requires multidisciplinary responses across these dimensions and where they interface.

NATO nations must address CogWar from a defensive position by building resilience and defence into AI/ML data networks that will defend against intrusions, attacks, and manipulation by adversaries.

Investments in multidisciplinary research such as cognitive and neuroscience, cognitive and behavioral science, and social and cultural studies in addition to technology is essential to defend against CogWar.

NATO nations need to develop cognitive security measures to defend information pathways and protect it from manipulation, modification, and the influence of an adversary’s intrusions. Cognitive Security sits at the intersection of multidisciplinary fields including neuroscience, brain research, human cognition, perception, and decision making. Thus, there is a need to conduct research on CogWar and cognitive security to ensure the development of a defensive toolbox for countering the influence and impact of all aspects of CogWar.

1.4 HFM-ET-356 SCOPE, AIMS, AND PROPOSED OUTCOMES

The NATO STO HFM Exploratory Team (ET) 356 **“Mitigating and Responding to Cognitive Warfare”** aimed to increase understanding of how defensive CogWar will provide effective prevention and mitigation strategies and countermeasures to increase defence and security within the NATO Alliance. As humans are part of all military operations and understanding the human and the brain is a central element in CogWar, the NATO HFM Panel included and highlighted “Cognitive Warfare” to its Program of Work (PoW) in 2021. Other STO Panels do have ongoing S&T activities that are associated with CogWar defence measures, from a technological or a systems analysis perspective.

The HFM-ET-356 team developed the “House Model” as the foundation for the development of a S&T strategic roadmap. This model was linked with the operational Observe, Orient, Decide, and Act (OODA) decision framework to highlight and facilitate understanding and the important synergy between research and operational communities.

The House Model represents seven main S&T knowledge areas and enablers that are cross-cutting and intersectionally related: *Pillars*: Cognitive Neuroscience, Cognitive & Behavioral Science, Social and Cultural Science and *Bars*: Situational Awareness and Sensemaking, Cognitive Effects, *modus operandi* and Technology and Force Multipliers.

The House Model was presented at the Cognitive Warfare Workshop during the Scientific Track of the NATO ACT Tide Sprint conference (4 – 8 April 2022, Sopot, Poland).

The current report presents the House Model framework to guide the NATO Alliance towards their S&T priorities. The Authors provide summaries of selected S&T areas (not exclusive), their relevance to defensive CogWar and propose various areas of research to eliminate capability gaps. Narratives are also provided to expand the description of the research areas and their relevance to defensive CogWar.

Given the complexity of CogWar and dynamic military operations, it has been necessary to consider strategies for developing education and training methods to prepare leaders for future CogWar challenges.

CogWar is an essential component of future military defence and warfare. It is therefore incumbent upon the S&T community to address the technology gaps that will ensure future cognitive security and the ability to defend against CogWar.

The aim of this report is to enhance each nation's awareness of CogWar, provide a S&T roadmap for the development of tools, technologies, education, and training that will support NATO's and partner nation's defence against CogWar. The investment in S&T research will strengthen NATO and its Allied partner nation's ability to counter the influence and potential impact of future CogWar.

1.5 ORGANIZATION OF THE REPORT

This report examines the S&T efforts for defending against CogWar and mitigating its influence and impact on human perceptions, thinking, and decision making. This report can be read in full, or individual chapters can be selected and read independent of the whole report.

Chapter 1 – Towards a Framework of Science and Technological Competencies for Future NATO Operations

Introduces the concept of CogWar as a multidisciplinary approach combining social sciences and innovative technologies to directly alter the mechanisms of understanding and decision making to destabilize or paralyze an adversary. CogWar is discussed within the context of NATO's strategic concept.

Chapter 2 – Towards a Science and Technological Framework “The House Model”

Introduces the need to develop a framework of human and technological competencies for future NATO operations. The chapter presents the key S&T topics related to the evolution of the CogWar. The HFM-ET-356 House Model serves as a guide for investment in S&T research in the defence against CogWar. The House Model represents the intersection of multidisciplinary S&T topics and the intersection with the characteristics of the OODA decision framework that can be seen as underpinning military operations (i.e., sensemaking, SA, social, cultural, and political contexts that influence operations). The House Model reflects a multifaceted and multidimensional approach to CogWar and lays the foundation for the development of the S&T Roadmap. The HFM-ET-356 House Model aims to capture an array of independent academic fields that become interdependent when operationalized and viewed through the lens of NATOs defence against CogWar.

Chapter 3 – Cases and Scenarios of Cognitive Warfare

This chapter introduces scenarios of CogWar to illustrate the range of activities, challenges and techniques associated with CogWar. The range of CogWar attacks at all levels from civilian, societal, and military operations, requires an ability to defend against adversaries in all environments. The purpose of this section is two-fold. The first purpose is to illustrate the breadth of activities, as well as supporting techniques, which

constitute CogWar, as well as diversity and range of potential target audiences. The second purpose is to link the varies incidents (case studies) to specific components of the House Model. This chapter is essential for understanding how best to defend against CogWar and which S&T topics must we invest in to ensure adequate defence against future CogWar.

Chapter 4 – The Influence and Impact of Social and Cultural Sciences in Cognitive Warfare

This chapter aims to discuss the role of the social and cultural sciences in CogWar. It offers unique insight into the issue of CogWar. Specifically (but not limited to) the socio-technical mechanics of audience engagement and psycho-social effects generation, as well as potential interventions or responses to neutralize, mitigate or counter cognitive attacks on audiences. In other words, the social and cultural sciences offer insight into and can help inform the development of both offensive and defensive facets of CogWar, particularly at the meso- and macro- levels of analysis (i.e., characteristics of social interaction between groups and organizations through large-scale societal interactions).

Chapter 5 – Cognitive and Behavioral Science (Psychological Interventions)

This chapter focuses on the Cognitive and Behavioral Science (CBS) pillar of the House Model. It focuses on the ways that adversaries target human vulnerabilities in the cognitive and behavioral domain. Furthermore, this chapter discusses ways that adversaries may exploit human psychological vulnerabilities to their advantage in CogWar. This chapter highlights the need to defend cognitive vulnerabilities and develop tools and technologies that will mitigate and defend against future CogWar targeting human cognitive and psychological vulnerabilities.

Chapter 6 – Developing Cognitive Neuroscience Technologies for Defence Against Cognitive Warfare

This chapter focuses on advances in our understanding of brain function and the development of sophisticated neuroimaging tools and analysis methods from biomedical/neuro-engineering fields. These advances have influenced the development of novel neural network models of human cognitive processes embedded in AI/ML network designs. This area of research plays a critical role in future CogWar. The evolution of Brain-Machine-Interfaces (BMI) presents opportunities for adversaries to seek new ways of hacking the human brain. This further suggests that adversaries may also find ways to hack the BMI network integrated with future command and control systems. This chapter addresses advances in neuroscience, brain research and the development of BMIs. These are critical areas of research that may prove to be the most significant areas of defending against CogWar in the future.

Chapter 7 – Defence Against 21st Century Cognitive Warfare: Considerations and Implications for Emerging Advanced Technologies

This chapter focuses on the emergence of disruptive technologies on future CogWar. For example, how the evolution of AI/ML algorithms, BMI, genetics, quantum computing will continue to advance and afford adversaries the opportunities to weaponize technologies and transform the battlespace. This chapter discusses the ethical challenges associated with the development of advanced super-intelligent machines, and the ethical deployment of such technologies. This chapter focuses on addressing the challenges and evolution of CogWar and seeks ways to forecast the best defence against CogWar.

Chapter 8 – Situational Awareness, Sensemaking and Future NATO Multinational Operations

This chapter focuses on Sensemaking and Situational Awareness as critical for effective decision making in military operations. CogWar focuses on the weaponization of information, including how adversaries distribute information, how it is understood, and how information influences human thought, behavior, and decision

making. This chapter examines the relationship between human understanding and the OODA decision framework. Further, it highlights the impact of the evolution of AI/ML networks and the development of independent, sentient robots with independent decision-making capabilities that will present vulnerabilities in the future CogWar battlespace.

Chapter 9 – Human-Machine Teaming: Towards a Holistic Understanding of Cognitive Warfare

This chapter presents the evolution of CogWar and its technologies from each era. This chapter takes an historic perspective of warfare wherein Sun Tzu sets the foundation for the discussion that takes us from the spear to the Human-Machine teaming age. Sun Tzu's philosophy of "Know thy enemy" is the theme to monitor throughout the ages as it provides a means of understanding intent and motivation of potential adversaries. This discussion includes the expansion of the OODA framework transformed into a "bow tie" model that reflects the complexities of human-machine decision making. The latter model highlights the need to consider the nested nature of the holistic model of CogWar if we are to defend effectively against CogWar.

Chapter 10 – Education and Training for Cognitive Warfare

This chapter highlights the need to develop more in-depth knowledge and advanced tools for supporting training in the defence about CogWar. For example, as CogWar focuses on the weaponization of information, the military should develop more awareness of the multiple CogWar practices and be able to detect and counter disinformation campaigns at an early stage. Virtual environments and wargaming provide a means of developing the skills required to operate in CogWar. The complexities of future CogWar mandate the need for more sophisticated training content, methods, and tools to meet the demands of the future CogWar environment. This requires the development of an overall framework for detecting, mitigating, countering, and developing CogWar operations on both the strategic and tactical levels.

Chapter 11 – SOMULATOR: Developing CogWar Resilience Through Social Media Training

Given the current state of propaganda and disinformation on social media, training needs to be provided for a broad range of users. This chapter summarizes the issues that were considered when a tool called "Somulator" was developed for social media training purposes. A range of open-source tools were chosen to emulate different social media platforms and presented to stakeholders. Feedback received laid the foundations for additional, custom development that were used to integrate core elements into a complete training solution. In addition, the core lessons learned from early use of the tools is discussed. The results of this pilot study have implications for defence against CogWar. Thus, the **Somulator** tool that emerged from this research holds great promise in contributing to research and training to defend against CogWar in the future.

Chapter 12 – Legal and Ethical Implications Related to Defence against Cognitive Warfare

The legal and ethical implications discussed in this chapter serve as a lens for evaluating how we might address the defence of CogWar. Today, there is no legal framework directly applicable to CogWar. This chapter discusses the implications for addressing the challenges of CogWar from a moral and legal perspective. This chapter presents challenges related to military actions within the cognitive domain and the unlawful use of force. It presents an argument for the need to develop legal policies and doctrine like those developed for cyber warfare, which define the legal parameters of CogWar itself.

Chapter 13 – Cognitive Warfare and the Human Domain: Appreciating the Perspective that the Trajectories of Neuroscience and Human Evolution place on Cognitive Warfare are at Odds with Ideas of a Human Domain

This chapter focuses on the discussion surrounding whether CogWar is unique or merely part of the “Human Domain.” The general argument is that a Cognitive Domain is too restrictive as it does not sufficiently encompass the action space in which human thinking and behavior is being weaponized. This chapter takes perspective of a ‘human domain’ as it does not a priori align with the trajectory of neuroscience and of human evolution in the context of CogWar. Instead, it argues for S&T approaches that focus on a cognitive domain, where CogWar attacks are directed and hence what needs to be protected.

Chapter 14 – Science and Technology Roadmap Based on the House Model

This chapter focuses on the development of a S&T roadmap as guide to invest S&T to ensure NATO and partner nation’s military readiness to meet the demands of future CogWar. The S&T roadmap is based upon the House Model and aims to guide the development of an effective S&T defence strategy. There are seven main S&T *knowledge areas and enablers that are cross-cutting and intersectional related*: Cognitive Neuroscience, Cognitive & Behavioral Science, Social and Cultural Science, Situational Awareness and Sensemaking, Cognitive Effects, *modus operandi* and Technology and Force Multipliers. The Chapter assess technological gaps and potential vulnerabilities associated within the scientific areas of the House Model, which is linked to the overarching military OODA decision-making objective.

Chapter 15 – Conclusion and Recommendations

This chapter highlights the main results of examining critical S&T topics within selected technologies and human factors. Examples are ICT, AI/ML, BMI advances, command and control, human-machine teaming, as well as social and cultural and cognitive & behavioral factors and their impact and/or function in CogWar. The complexity of CogWar increases with each technological advance and innovation and must be addressed within a socio-technical system perspective. There is a need to address future challenges by anticipating the intersection of multidisciplinary scientific topics and how these advances may be dual purposed by adversaries to their strategic advantage. Nations must anticipate and prepare to defend against such threats to global security. This chapter concludes with a series of recommendations for future S&T investment and technological development to ensure an effective defence against CogWar.

1.6 REFERENCES

Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. (2022). Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 20201. NATO STO, Neuilly-sur-Seine, France.

Cole, A. and Le Guyader, H. (2020). NATO Sixth’s Domain of Operations. FICINT document. Norfolk (VA, USA), NATO ACT Innovation Hub. Retrieved from: <https://www.innovationhub-act.org/sites/default/files/2021-01/NATO%27s%206th%20domain%20of%20operations.pdf>

Gill, R. and Goolsby, R. (2022). COVID-19 Disinformation: A Multi-National, Whole of Society Perspective. Springer Cham.

NATO (2010). Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Adopted by Heads of State and Government at the NATO Summit in Lisbon 19 – 20 November 2010. NATO Public Diplomacy Division, Belgium.

NATO (2021). Brussels Summit Communiqué. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021.

NATO (2022). NATO Strategic Concept 2022. Adopted at the Madrid Summit, 29 – 30 June 2022.
<https://www.nato.int/strategic-concept/index.html>

NATO 2030 Reflection Group (2020). United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General 25 Nov 2020.

NATO Industrial Advisory Group (NIAG) (2022). NIAG-N (2022)0005, NIAG Study on Standards for Cognitive Augmentation for Military Applications.

NATO STO (2020). NATO Science &Technology Trend Report, 2020. Science & Technology Trends 2020 – 2040. Exploring the S&T Edge. NATO Science & Technology Organization, Neuilly-sur-Seine, France.

NATO STO (2021). AC/323-N (2021)0023. NATO Science & Technology Board Read Ahead for the Fall 2021 Executive Session. Agenda Items 7 and 8 – STO Plans & Programmes Workshops 2021 and 2022.

Pappalardo, D. (2022). Win the War Before the War? The French Perspective on Cognitive Warfare. War on the Rocks, 1 August 2022. Retrieved August 2022 from: <https://warontherocks.com/2022/08/win-the-war-before-the-war-a-french-perspective-on-cognitive-warfare/>

Takagi, K. (2022) The Future of China's Cognitive Warfare: Lessons from the War in Ukraine. War on the Rocks. 22 July 2022. Retrieved from: <https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/>

Tammen, J.W. (09 July 2021). NATO's Warfighting Capstone Concept: Anticipating the Changing Character of War. NATO Review.

Zinets, N. and Vasovic, A. (2022). Missiles Rain Down Around Ukraine. Retrieved from Reuters <https://www.reuters.com/world/europe/putin-orders-military-operations-ukraine-demands-kyiv-forces-surrender-2022-02-24/>.

Chapter 2 – TOWARDS A SCIENCE AND TECHNOLOGICAL FRAMEWORK “THE HOUSE MODEL”

Benjamin J. Knox

Norwegian Armed Forces Cyber Defence
NORWAY

2.1 INTRODUCTION

CogWar is transformative and affords the adversary the opportunity to gain the strategic advantage by exploiting advances in technologies such as, AI, ML, BMI, as well as exploiting existing technologies in new ways. The weaponization of advanced technologies drives the need to develop tools, techniques, procedures, education, and training methods to counter the CogWar threat. The adversary uses CogWar to shape and affect the tactical, operational, strategic, and geopolitical environment in an insidious and often invisible manner to support achieving their strategic objectives. Therefore, developing an S&T roadmap that lays the foundation for how NATO can mitigate and respond to CogWar is a critical first step.

To this end, the House Model (Figure 2-1) was developed to guide S&T research concerning how NATO can ‘*get ahead*’ in the realm of CogWar. Getting ahead implies a journey involving a catching-up process to identify where the vulnerabilities are that need defending and what, therefore, are the knowledge needs to counter CogWar.

The House Model reflects the multifaceted and multidimensional nature of CogWar. Planned and applied with old and new methods, CogWar achieves overt and covert objectives below and above the threshold of war, affecting how we think, act, and make decisions. It does this by *exploiting facets of cognition to disrupt, undermine, influence, or modify human decision making*. With *modern technological enablers that act as force multipliers*, these goals become more realizable with less effort, resources, and risk. Novel *methods and ways of operating (modus operandi)* inspired by, or grounded in fields of contemporary or existing knowledge, allow adversaries to *deliver cognitive effects* that target our *situational awareness and ability to sense-make* by penetrating and permeating the conscious and subconscious of individuals and the collective. As such, the HFM 356 roadmap model aims to capture an array of independent academic fields that become interdependent when operationalized and viewed through the lens of NATO’s defence against CogWar. The following is an introduction to the House Model. Further details can be found in Chapter 14.

2.2 THE HOUSE MODEL

The CogWar House Model aims to guide the delivery of scientific outcomes that go beyond conventional thinking by challenging what we think we already know and exploring what we know we don’t know. Through well-defined research goals that reflect the cross-cutting model architecture, we can learn how to support the NATO warfighter in perceiving CogWar and comprehending it when it has occurred, and/or when it is already delivering its effect(s). Finding ways to ‘catch-up’ and ‘get ahead’ in terms of prediction and developing counter measures, or counter effects, can only occur when the right tools (cognitive and technological) operate within, or at that the edge of, *NATO Security and Defence, NWCC, Legal and Ethical Frameworks (ELSEI)*, without adversarial interference. This then ensures our sensemaking is precise and timely enough that our Situational Awareness (SA) is formed from trustworthy input data.

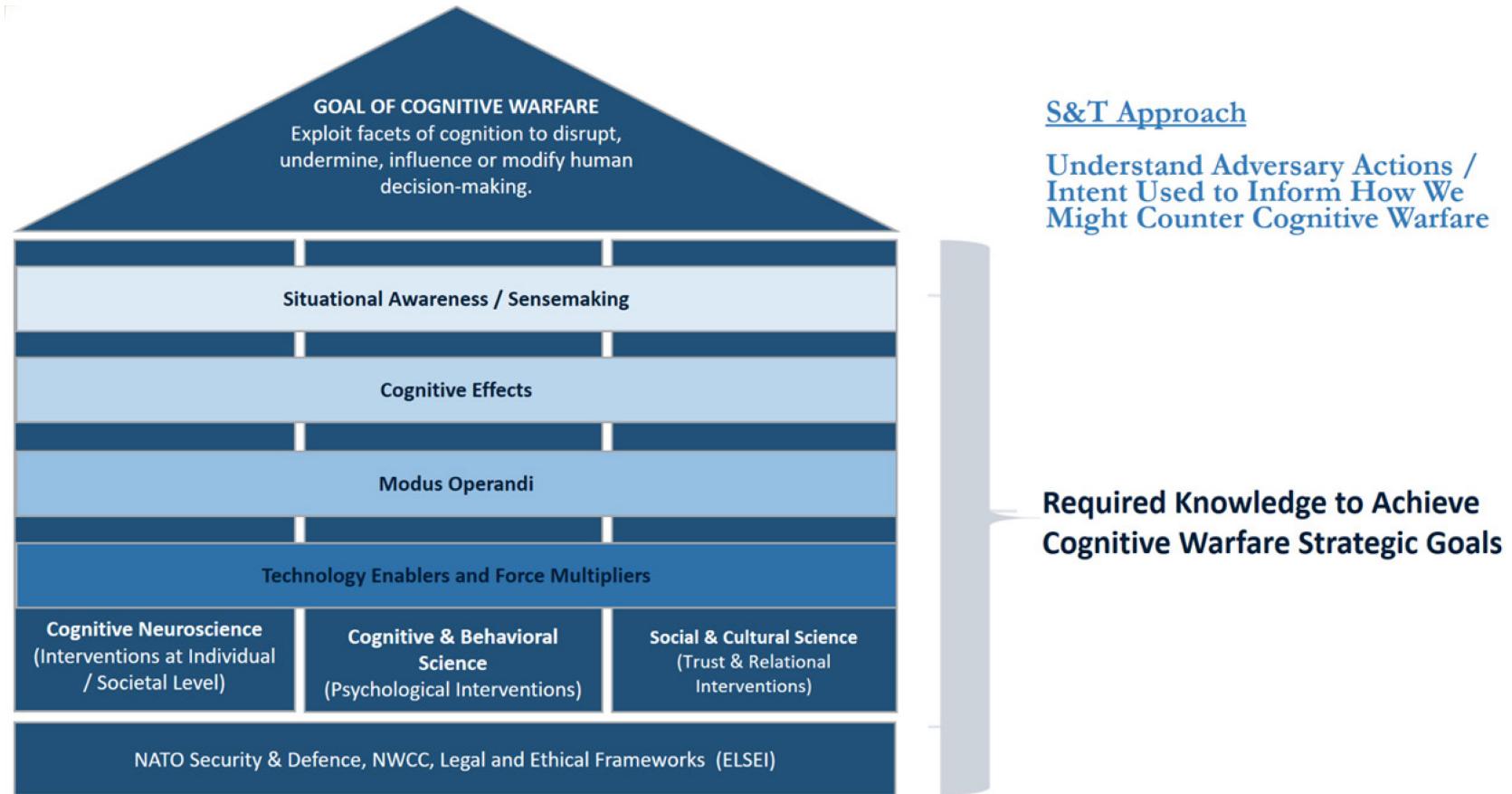


Figure 2-1: The House Model Developed by HFM-ET-356.

2.2.1 The Pillars

The three pillars in the model identify primary fields where knowledge is required to influence or modify a Target Audience (TA) (Figure 2-2). The pillar titles (Cognitive Neuroscience, Cognitive and Behavioral science, and Social and Cultural science) identify priority areas (or fields) that require research effort, including applied interventions. CogWar is a multi and inter-disciplinary concept. As such, each pillar intends to be inclusive, opening space for broad and niche research involvement. The pillars acknowledge and encourage research that exposes, investigates, and aims to understand discipline, organizational, and institutional overlaps. It is here where the adversary may be operating unchecked.

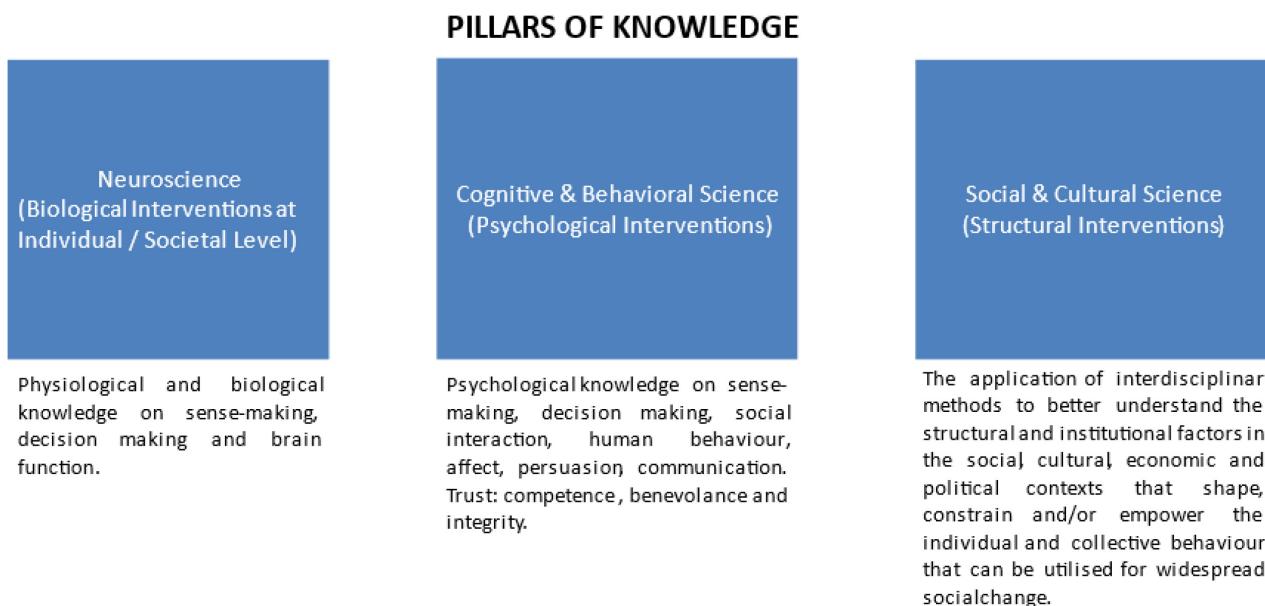


Figure 2-2: The Scientific Pillars of Knowledge – House Model of CogWar ET 356.

2.2.2 The Horizontal Bars

The horizontal bars identify enablers and force multipliers to the knowledge pillars (see call out box, below). The aspects of SA & Sensemaking, Cognitive Effects, *modus operandi*, and Technology Enables are independent areas of research that have inter-dependencies across and between the pillars of knowledge. They present opportunities to consider the ‘HOW & WHEN’ of S&T knowledge needs.

Enablers and Force Multipliers
<p>Situational Awareness (SA) / Sensemaking: Examination of the factors that enable or block attempts to make sense of an ambiguous situation. Sensemaking informs and is a prerequisite to decision making. It requires trusted data input, evaluation of meaningful information, integration with knowledge and experience to achieve an understanding of evolving non-linear events.</p>

Cognitive Effects: Describes the effects an actor may try to create on a target audience IOT achieve desired goal. Could be doctrinal effect verbs, e.g., distort, distract, etc., or more elaborate descriptions, e.g., degrade TA's trust in democratic institutions or politicians, persuade TA to believe A instead of B, etc. Related to neurobiology the effects could be to, for example, injure or impair cognitive functions, stimulate emulative functions, or trigger social contagion.

modus operandi: Examination of adversary methods and stratagems to generate the desired effect on the target/target audience, including when methods/stratagems are employed to exploit ‘cognitive openings’ and other opportunities for intervention (i.e., how and when). This effort is also concerned about the synchronization of activities by adversaries to psychologically prime and target. A better understanding of when and how adversaries conduct CW provides insights on the development and validation of countermeasures and defensive strategies.

Technology Enablers and Force Multipliers: Use technology to enable the actor to utilize one, two or all of the three knowledge pillars simultaneously, in pursuit of the goal. This aspect enables the above aspects. e.g., EDTs ICT CIS / Big Data / AI & ML / Social Media / Directed Energy / Biotech / Nanotech, etc.

2.3 SUMMARY

Future NATO military leaders will face a wide range of dilemmas as CogWar has the potential to pervade and influence all aspects of NATOs role to safeguard the Allies' freedom and security by political and military means. The intrinsic, invasive, and invisible nature of CogWar with its global network of technological enablers, will provide a continuous challenge regarding identifying the truth and making sense of what to trust in data, and data sources. Advancements in areas such as Deep Learning, Synthetic media, Neuroscience and Human-machine teaming means the Information Environment will become more contested, significant, and defining. Understanding, acknowledging, and managing the long and short-term effects from CogWar activities and operations requires we educate and train our leaders and warfighters with new approaches and adaptive ways of viewing competition, conflict, and warfare. This is essential if we are to address the challenges CogWar brings to SA and decision making. Only then can we ensure effective and accurate mitigation and response tactics – the Cognitive Superiority needed – to possess and apply faster, deeper, broader and / or more effective military thinking and understanding than adversaries. The resulting effect enables NATO and Allies to hold the information initiative and not be influenced by the potential impact of CogWar.

Future military operations will encompass the range of topics presented within the House Model. Most significantly it is likely they will be revealed at the points of creation and discovery where the pillars and the horizontal bars overlap in novel ways. We anticipate that this framework can be used to inform those who will lead competency and capability development for future NATO operations. We contend that nations would benefit from using the House Model as a reference and guide to the development of their respective national S&T research portfolio. The model encourages intra, inter and multi-disciplinary activities that can fill gaps in understanding and allow us to gain some advantage as we look to defend the entire socio-technical system against the effects of CogWar.

The following chapters will begin the discussion of each of these pillars and provide insight as to the role that each topic will play in future CogWar as a means of evaluating and assessing ways to mitigate and defend against CogWar.

Chapter 3 – CASES AND SCENARIOS OF COGNITIVE WARFARE

Matthew A. Lauder

Defence Research & Development
CANADA

Eskil Grendahl Sivertsen

Norwegian Defence Research Establishment
NORWAY

3.1 INTRODUCTION

There are a myriad of forms or types of Cognitive Warfare (CogWar) occurring at all levels of operation and across the spectrum of conflict, from peacetime through limited intervention, irregular warfare, and major combat operations. For example, at the tactical level, CogWar may take the form of SMS text messages disseminated to specific geographic areas (i.e., narrowcasting) and designed to undermine the morale of enemy soldiers by spreading disinformation about defections, non-payment of the soldier's salary, promoting contempt of senior officers, or simply threatening retaliation. In some cases, the messages are combined with a kinetic attack, such as an artillery or missile strike, to further antagonize the intended recipient. In other cases, CogWar can occur at the operational and strategic levels by targeting entire populations, policy makers, or political and military leaders. For example, large populations may be manipulated by through advanced psycho-behavioral modeling, artificial intelligence, and machine learning to target individual psychological pressure points and societal fault lines, ultimately amplifying political dissent, and encouraging internecine violence. In other cases, mass media can be manipulated to create a false understanding of a political decision, which could lead to false assumptions about the enemy and undermine the decision-making process of senior political and military leaders.

The purpose of this section is two-fold. The first purpose is to illustrate the breadth of activities, as well as supporting techniques, which constitute CogWar, as well as diversity and range of potential target audiences. The second purpose is to link the varies incidents (case studies) to specific components of the house model.

3.2 COGNITIVE WARFARE CASE STUDY #1: CHRYSTIA FREELAND SMEAR CAMPAIGN

Although largely occurring in Canada – or at least much of the effort appears to have been executed in Canada – the smear campaign conducted against Chrystia Freeland was arguably designed to undermine the credibility of the Canadian government as well as the Canadian Armed Forces (CAF) presence in Eastern Europe, primarily Ukraine, but also Latvia. Literally launched the same day that Freeland was appointed as the Minister of Foreign Affairs (Kassam, 2017), the smear campaign started with a series of posts on a pro-Russian social media account, seemingly located in Canada, on 10 January 2017 that cited documents from the archives of the Alberta government about Freeland's grandfather, Michael Chomiak, and accused her of being sympathetic to Nazism.

The following day, an editor from *VICE* magazine, who was conducting an interview on an unrelated matter at the Russian embassy in Ottawa, was handed a dossier from an unidentified embassy staff member detailing Freeland's grandfather's interaction with the German military in occupied Ukraine during World War II (Ling, 2017; Glavin, 2017b). Like the previous day's social media posts, the dossier was based on publicly available information held in the archives of the government of Alberta.

CASES AND SCENARIOS OF COGNITIVE WARFARE

A week later, on 19 January 2017, a lengthy and detailed article written by John Helmer appeared on his blog, *Dances with Bears*, and also in the *Russia Insider*, a pro-Russian newspaper believed to be funded by Konstantin Malofeev (a Russian oligarch close to Putin and accused of having funded pro-Russian separatists in Ukraine and the attempted coup in Montenegro), as well as other pro-Russian social media sites (Shekhovstov, 2015; Helmer, 2017a). Seemingly based on archival documents, the article claimed Freeland lied about her grandfather's interaction with the German army during WWII and stated that she was actively "preaching race hatred of Russians" (Helmer, 2017a). Helmer, a former White House aide, who moved to Moscow in 1989, is reputed to have been an agent for the KGB (Glavin, 2017a).¹

Between 19 and 26 January 2017, more than 30 different pro-Russian Twitter accounts posted or re-tweeted the claims regarding Freeland's grandfather or linked to and promoted the Helmer article.² Many of the social media accounts, some of which had thousands of followers, were known Russian social media trolls belonging to or affiliated with the Internet Research Agency (IRA) On 27 January 2017, a computer-generated audio recording reciting the text of Helmer's article was posted to YouTube as well as several other social media platforms. The Helmer article was published by the *Strategic Culture Foundation*, a Russian thinktank and online journal operated by the Russian foreign intelligence (SVR) and the Ministry of Foreign Affairs and a known outlet of Russian propaganda and disinformation (Ponce de Leon and Andriukaitis, 2020). Within a week, the story of Freeland's grandfather, and accusations that Freeland was sympathetic to Nazism, went viral across several social media platforms.

Just over a week later, Stanislav Balcerac, a Polish journalist known to support rightwing political movements, published an article on the same topic in the *Warszawska Gazeta* (Warsaw Gazette), a weekly publication known to publish hate-based and anti-Semitic articles (Balcerac, 2017; Glavin, 2017a). The same article was also published in *Polska Bez Cenzury* (Poland Without Censorship). Later in February, Arina Tsukanova, a pro-Russian journalist allegedly based in Crimea (Global Engagement Center, 2020), published an article in *Consortium News*, a US-based independent, online news service repeating many of the claims from the Balcerac article (Tsukanova, 2017).³ Although *Consortium News* sued a Canadian news network for claiming it was part of an elaborate Russian cyber-influence campaign (Lauria, 2020), Tsukanova was subsequently reported to be a sock puppet (i.e., a fictitious persona) operating for the Russian foreign intelligence service through the *Strategic Culture Foundation* (Global Engagement Center, 2020; Ponce de Leon and Andriukaitis, 2020).

During a press conference on 6 March 2017 about the extension to Operation UNIFIER, the Canadian military training mission to Ukraine, a reporter asked Freeland about Russian media outlets and websites and claims her grandfather was a Nazi collaborator. In response, Freeland stated that Russian disinformation and other smear campaigns, like those that recently occurred in the US and Europe, should be expected. However, the question of her grandfather's role during WWII at the press conference, which was covered by several Canadian national news media agencies, served not only to push the story into the mainstream but also provided an opportunity for the Russian government – through Kirill Kalinin, the press secretary of the Russian embassy in Ottawa – to

¹ As noted by Ledeneva (2006), this source is not in the reference list, smear campaigns are based on political (e.g., abuse of power, disloyalty, or incompetence, etc.), economic (e.g., embezzlement, nepotism, etc.), criminal (e.g., links to organized crime or bribery, etc.) and/or private information that compromising the target's reputation, including but not limited to the misdeeds, illegal or unethical behavior of family members, or unpopular personal beliefs or behaviors. Ledeneva also points out that a sustained and serious campaign against a target will draw from information from across all four categories and that some of the most effective smear campaigns are not based on perceived or real illegal behavior but related to private life and behavior associated with or contravening strong social norms or values.

² The initiation and propagation of the smear campaign against Freeland was identified and reported on by the EU East StratCom Task Force on 26 January 2017 (Staff Writer, 2017).

³ *Consortium News* was edited by Robert Parry and is regarded by Media Bias/Fact Check website to be a left leaning but with mixed reliability/mostly factual (Media Bias/Fact Check, n.d.).

publicly criticize Freeland and question her credibility. The story of Freeland's grandfather's role in WWII, and Freeland's warning of Russian disinformation, effectively dominated news media reporting and overshadowed the announcement of Canada's renewed commitment to Operation UNIFIER in Ukraine, which was likely the objective of the Russian disinformation campaign (Glavin, 2017a; Glavin 2017b).

However, that was not the end of the smear campaign. On 21 March 2017, leveraging the story of Freeland's grandfather and accusing her of lacking integrity and engaging in anti-Russian bias, the Russian Congress of Canada lodged a formal complaint with the Prime Minister. In addition to making spurious claims that Freeland lacked the proper qualifications for the job (as Minister of Foreign Affairs), the letter implied a connection between her grandfather's role in WWII and her support for Ukrainian exiles and related political issues, suggesting she acquired pro-fascist sympathies from her grandfather (Russian Congress of Canada, 2017).

While initially generating significant news media attention and public interest in Canada and abroad, as well as generating some negative coverage, some of which called into question the veracity of claims the incident was an act of Russian disinformation, the smear campaign was and is still used in Russian information confrontation, especially those designed to shape the opinions of Russian linguistic audiences in Eastern Europe (Glavin, 2017b). In addition, the smear campaign is often referenced in other disinformation activities designed to undermine Ukrainian political support abroad, particularly in Canada (Brown, 2019).

In response to the smear campaign and the attempted assassination of Sergei Skripal in the United Kingdom by GRU agents, the Canadian government announced the expulsion of four Russian diplomats in March 2018. The diplomats, who were based in Ottawa and Montreal and included Kalinin (who was alleged to have orchestrated the smear campaign by sending information about Freeland's grandfather to various news agencies), were identified as intelligence officers and alleged to have interfered in the operation of democratic institutions, including to have engaged in a campaign to shape Canadian public opinion (Guly, 2018). Three of the four were also identified as having conducted cyber-influence activities while based at the Russian consulate in Montreal, specifically an effort designed to discredit the World Anti-Doping Agency (WADA) and spread other disinformation related to Canadian institutions (Fife and Carbert, 2018).

Model Components to the House Model:

- **Required Knowledge:** Cognitive and behavior science, social and cultural science.
- **Technology Enablers:** Social media platforms and accounts, sock puppets, and online advocacy/populist news media.
- **Modus Operandi:** Smear campaign, combined with disinformation, highly emotive topics.
- **Cognitive Effects:** Attempted to create uncertainty and serve as a distraction.
- **Situational Awareness/Sensemaking:** Use of highly emotive language was an attempt to confuse and undermine the government's ability to respond to the smear campaign.
- **Goal:** To undermine credibility of the target and the Canadian government, more generally, but also to disrupt decision-making about Canadian military contributions to NATO.

3.3 COGNITIVE WARFARE CASE STUDY #2: NOVI SANZHARY COVID-19 RIOTS

With a population of less than 10,000 people, Novi Sanzhary is a small town approximately 335 kms east of Kiev in central Ukraine. On 18 February 2020, a plane carrying evacuees from China (45 Ukrainians and 27 foreign nationals, including flight personnel) arrived in Kharkiv, Ukraine. However, as soon as the plane landed, rumors started to circulate on various social media platforms that the passengers were infected and in the process of being transferred to an unidentified medical facility. In response to the rumors, the Ukrainian government confirmed the arrival of the plane, but indicated that the passengers had been tested prior to departure and that no infections or positive COVID-19 tests were reported. Ukrainian government representatives confirmed that all the passengers would be transferred to a national guard medical Center located in Novi Sanzhary and placed in a 14-day quarantine as a precautionary measure.

Following the government announcement, however, additional disinformation about the evacuees was posted and shared across multiple social media platforms, including Viber, Facebook, and Instagram. Moreover, local politicians and residents asserted they were not informed of the evacuees prior to the arrival of the plane and complained of a lack of information from the central government officials in Kyiv. Angered by the situation, residents of Novi Sanzhary started to mobilize on 19 February using social media and constructed barricades to block the arrival of the evacuees at the medical clinic. Residents also gathered and protested at the city center. Later that day, dedicated channels on various social media platforms were created which disseminated dire warnings of “countless deaths” and spread disinformation about the evacuees, as well as to encourage residents to ‘take action,’ including confronting soldiers and setting fire to the hospital (Miller, 2020). Some of the social media channels also suggested residents watch online broadcasts about the situation from NASH TV, a station own by a pro-Russian politician, as well as other online pro-Russian broadcasters (Velichko, 2020). In some cases, the administrators of social media channels did not conceal their Russian identities and overtly promoted a pro-Russian narrative and provided links to Russian news media outlets.

Dozens of police officers and security personnel, including members of the National Guard, arrived in Novi Sanzhary by the morning of 20 February 2020. However, rather than alleviating concerns, the arrival of the security services heightened tensions and, at least to residents, served as confirmation of the rumors the evacuees were infected. Increasing the level of collective anxiety, a spoofed health advisory (which was sent to the entire contact list of the Ministry of Health) confirming that at least five of the evacuees were positive with COVID-19 was released from what appeared to have been the Ukrainian Health Ministry email address. While government officials declared the email to have been spoofed, rumors of the infections still took hold and, along with paid agents provocateurs on the ground inciting violence, the situation in Novi Sanzhary reached a tipping point (Velichko, 2020). As the buses carrying the evacuees arrived in Novi Sanzhary, several hundred residents manned barricades and set fires to block their progress. In response, police in riot gear attempted to push the protesters back and clear a path for the buses, using armored personnel carriers to move vehicles blocking the road. The situation quickly degenerated into violent clashes, with residents throwing stones and other projectiles at the passing buses (Melkozerova and Parafeniuk, 2020). Aggravating the situation and adding to the uncertainty, additional disinformation was released by at least one news media outlet suggesting the staff at the medical center resigned in protest over concerns about a lack of proper equipment and training.

Later that day, and to defuse the situations, Oleksiy Honcharuk, the Ukrainian prime minister, arrived in town, along with Arsen Avakov and Zoryana Skaletska, the interior and health ministers, respectively. However, the appearance of national political officials as well as public statements, including a Facebook

post by Ukrainian President Zelensky pleading for calm, did nothing to reassure the residents. By the time the riots subsided, at least nine police officers and one civilian were injured, and 24 people arrested. Both Honcharuk and Skaletska were subsequently dismissed from their government positions.

Model Components to the House Model:

- **Required Knowledge:** Cognitive and behavior science, social and cultural science.
- **Technology Enablers:** Social media platforms and accounts, sock puppets, television broadcasts, online news media, email spoofing.
- **Modus Operandi:** Disinformation combined with highly emotive topics and exploitation of uncertainty to generate rumors, cyber-attacks.
- **Cognitive Effects:** Exploiting pervasive fear, created an elevated level of uncertainty and anxiety and undermined public confidence in Ukrainian government institutions.
- **Situational Awareness/Sensemaking:** Campaign took advantage of a lack of information released from the Ukrainian government and a general distrust of political institutions.
- **Goal:** To undermine the credibility of and trust in the Ukrainian government.

3.4 COGNITIVE WARFARE CASE STUDY #3: RUSSO-GEORGIAN WAR (2008)

The exact event that triggered the five-day war between Georgia and Russia in August 2008 is difficult to pinpoint. At the time, Mikheil Saakashvili, the President of Georgia, was blamed by many analysts for being reckless and for antagonizing Russia, which was also how the Russian government wanted the conflict to be portrayed (Lauder, 2019). However, those claims have been revisited by scholars, and many now assert the Russian government carefully planned and escalated the incidents to provoke the Georgian government into a disproportionate response which was then used by the Russia government to justify military intervention (Lauder, 2019). The provocative activities by the Russia government included an assassination attempt on the head of the Georgian-backed administration in South Ossetia, attacks on Georgian police officers, indiscriminate shelling of Georgian towns by South Ossetian militias, threats that Cossack militias and other volunteers were mobilizing, and a series of computer network attacks that disrupted the ability of the Georgian government to communicate with the public.

After a week of increasingly violent skirmishes between South Ossetia militias and Georgian defence forces, which included the arbitrary shelling of residential areas, and based on intelligence that Russian troops were about to invade through the Roki Tunnel, Saakashvili ordered the Georgian military to mobilize and advance into South Ossetia on the early afternoon on 7 August. At the same time, Georgian personnel vacated the Joint Peacekeeping Force (JPKF) headquarters, which included a joint monitoring force of Russian, South Ossetian and Georgian military representatives.

Although the situation was tense and unpredictable, Saakashvili hoped that pushing Georgian defence forces into South Ossetia would force an end to the artillery strikes and prevent the Russian military from entering the region. Shortly after the mobilization, Saakashvili declared a unilateral ceasefire and ordered a halt to the advance. This decision was based on input from the Russian military representative at the JPKF who indicated that the Russian military did not have control of South Ossetian militias, implying that Russia was not responsible for the current situation. The Russian military representative also suggested Georgian authorities order an immediate stop to the mobilization and declare a unilateral ceasefire, which Saakashvili did. Later in the day, both Russian and South Ossetian diplomatic representatives failed to appear at a prearranged meeting with

Georgian authorities to negotiate a settlement. Saakashvili provided an update on live television and publicly called for negotiations with South Ossetian and Russian officials. Saakashvili also reconfirmed a promise of unrestricted autonomy for South Ossetia and pleaded for the international community to intervene. Taking advantage of the ceasefire, South Ossetia militias renewed their shelling of Georgian towns, which forced civilians to flee. Sensing there was no other remedy or way to curtail the violence, Saakashvili rescinded the ceasefire and, at approximately 23:30 hours on 7 August, re-ordered the Georgian military to move into South Ossetia. Within hours of that-order, two Russian motorized rifle brigades passed through the Roki Tunnel and entered South Ossetia. The brigades, which were a part of the Russian 58th Army, recently participated in Kavkaz-2008, a joint counterterrorism and peacekeeping exercise. While some of the participants of the exercise returned to their bases, the two brigades were sent to the Russian side of the tunnel and told to wait for the order to enter South Ossetia. Putin, then Prime Minister of Russia, denounced the Georgian mobilization as an act of aggression against South Ossetia and threatened a Russian response. Russian news media, many of whom were prepositioned in South Ossetia by the Russian government days prior to the conflict, also accused Georgian authorities of atrocities against the civilian population.

While Georgian defence forces made some early gains, the next five days (8 – 12 August) saw Russian forces, as well as the various militias operating in South Ossetia and Abkhazia, make significant advances into Georgian territory, with the main Russian armored column halting less than 60km from Tbilisi, the capital of Georgia. During this period, Putin, who was attending the 2008 Summer Olympics in China, arrived in North Ossetia and took charge of the military operation. Putin also claimed the Georgian government's actions were criminal, and that more than 30,000 refugees fled the country and dozens of civilians were killed by Georgian forces. Despite a willingness on part of Georgian authorities to negotiate, the Russian military, along with supporting militias, conducted offensive operations along numerous fronts. Russia also conducted a well-organized cyber operation that employed both professional hackers and hacktivists which effectively crippled Georgian government, law enforcement, financial sector, and news media websites and attempted to smear Saakashvili by defacing government websites with Nazi symbols.

By 13 August, the conflict was largely over, as both sides agreed to a peace plan hastily brokered by France. On 26 August, Dmitry Medvedev, the President of Russia, signed a Presidential decree recognizing the Republics of South Ossetia and Abkhazia as independent states. The decree also authorized cooperation and mutual assistance agreements, including on defence and military support. Several features of this operation suggest that maskirovka was employed by the Russian military and a significant degree of reflexive control of the Georgian leadership may have been achieved. First, the timing of the intervention, which followed closely on Kavkaz-2008, was designed to allow the Russian military to mass troops along the border without causing undue suspicion. Second, the Russian military did not make a concerted effort to conceal their position or intention to invade, including permitting South Ossetian border guards to use Georgian telephone lines to report the initial movement of a Russian armored unit through the Roki Tunnel in the early hours of 7 August. These phone calls, which were intercepted by Georgian intelligence services, helped frame Saakashvili's understanding of the situation, and seemingly substantiated his concerns that Russia was invading, which ultimately led him to mobilize the Georgian military and push into South Ossetia (the false-optimal solution). Third, and likely sensing a degree of trepidation on part of Saakashvili, as well as his reputation for impulsivity, the Russian military exploited his eagerness to negotiate a settlement by suggesting he should halt the advance, announce a unilateral ceasefire, and have emissaries meet to discuss a peaceful solution, a meeting that both Russian and South Ossetian representatives failed to attend. There is also evidence suggesting the Russian government generated and published an extensive psychological profile of Saakashvili, which may have been used to design the manipulation (Blandy, 2009). This manipulation of Saakashvili by the Russian military served to critically delay the arrival of Georgian troops in South Ossetia which provided enough time for the remaining Russian forces to transit through the tunnel. Lastly, and while he thought he was acting in self-defence, Saakashvili's

mobilization of Georgian defence forces provided the Russian government with the moral and legal justification to invade. Moreover, this pretext was further reinforced by Russian government accusations of human rights violations by the Georgian military, including claims of ethnic genocide, which may have served to prevent Western military intervention in the conflict. In this example it seems as though the Georgian government, specifically Saakashvili, never recognized the extent to which the Russian government was manipulating the situation.

Model Components to the House Model:

- **Required Knowledge:** Cognitive and behavior science, social and cultural science.
- **Technology Enablers:** State-controlled and aligned news media, DDoS attacks, digital graffiti, and defacements.
- **Modus Operandi:** Disinformation and cyber-attacks.
- **Cognitive Effects:** Elevated level of uncertainty about adversary intentions.
- **Situational Awareness/Sensemaking:** Sent mixed signals to confuse the target, disrupted the ability of the Georgian government to function.
- **Goal:** To disrupt the ability of Saakashvili to make timely decisions and to choose a false-optimal solution.

3.5 REFERENCES

Balcerac, S. (08 February 2017). The New Foreign Minister of Canada Chrystia Freeland – Proud Granddaughter Collaborator! Warszawska Gazeta. <http://warszawskagazeta.pl/polityka/item/4562-nowa-minister-spraw-zagranicznych-kanady-chrstia-freeland-dumna-wnuczka-kolaboranta>

Blandy, C.W. (2009). Provocation, Deception, Entrapment: The Russo-Georgian Five-Day War. Advanced Research and Assessment Group, Defence Academy of the United Kingdom. https://www.files.ethz.ch/isn/97421/09_january_georgia_russia.pdf

Brown, C. (17 January 2019). Top Russian News Host Takes Aim at Ukrainian Canadians. CBC News. <https://www.cbc.ca/news/world/top-russian-news-host-takes-aim-at-ukrainian-canadians-1.4980859>

Fife, R. and Carbert, M. (29 March 2018). Russian Spies Aimed to Discredit WADA, Spread Disinformation about Canada with Cyber Campaigns. The Globe and Mail. <https://www.theglobeandmail.com/politics/article-russian-spies-aimed-to-discredit-wada-spread-disinformation-about/>

Glavin, T. (8 March 2017a). Terry Glavin: Enter the Freeland-Nazi Conspiracy – and Amping-Up of Russia's Mischief in Canada. The National Post. <http://news.nationalpost.com/full-comment/terry-glavin-enter-the-freeland-nazi-conspiracy-and-the-ampling-up-of-russias-mischief-in-canada>

Glavin, T. (14 March 2017b). How Russia's Attack on Freeland Got Traction in Canada. MacLeans. <https://www.macleans.ca/politics/how-russias-attack-on-freeland-got-traction-in-canada/>

Global Engagement Center. (August 2020). Pillars of Russia's Disinformation and Propaganda Ecosystem. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

CASES AND SCENARIOS OF COGNITIVE WARFARE

Guly, C. (13 April 2018). Smear Campaign Against Freeland Linked to Russian Diplomats' Expulsion, says Trudeau. The Ukrainian Weekly. <http://www.ukrweekly.com/uwwp/180711-2/>

Helmer, J. (19 January 2017a). SCOOP: Canada's New Foreign Minister Lying about Family's Ukrainian Nazi Past. Russia Insider. <https://russia-insider.com/en/victim-or-aggressor-christia-freelands-family-record-nazi-war-profiteering-and-murder-crakow-jews>

Kassam, A. (10 January 2017). Canada Names Chrystia Freeland, Leading Russia Critic, as Foreign Minister. The Guardian. <https://www.theguardian.com/world/2017/jan/10/canada-christia-freeland-foreign-minister-russia-critic>

Lauder, M.A. (2019). Limits of Control: Examining the Employment of Proxies by the Russian Federation in Political Warfare. Journal of Future Conflict, Issue 1. https://www.queensu.ca/psychology/sites/psycwww/files/uploaded_files/Graduate/OnlineJournal/Matthew_Lauder-Limits_of_Control-Examining_the_Employment_of_Proxies_by_the_Russian_Federation_in_Political_Warfare.pdf

Lauria, J. (13 October 2020). Consortium News Sues Canadian TV Network for Defamation Over Report CN was Part of 'Attack' 'Directed' by Russia. Consortium News. <https://consortiumnews.com/2020/10/13/consortium-news-sues-canadian-tv-network-for-defamation-over-report-cn-was-part-of-attack-directed-by-russia/>

Ledeneva, A.V. (2016). How Russia Really Works: The Informal Practices that Shaped post-Soviet Politics and Business. Cornell University Press.

Ling, J. (3 March 2017). Canada's Foreign Minister Warns of Russian Destabilization Efforts – and She Might be a Target. VICE. <https://www.vice.com/en/article/8xmyna/canadas-foreign-minister-warns-of-russian-destabilization-efforts-and-she-might-be-a-target>

Media Bias/Fact Check. (n.d.). Consortium News. Media Bias Fact Check. Retrieved 15 March 2021, from <https://mediabiasfactcheck.com/consortium-news/>

Melkozerova, V., and Parafeniuk, O. (3 March 2020). How Coronavirus Disinformation Caused Chaos in a Small Ukrainian Town. NBC News. <https://www.nbcnews.com/news/world/how-coronavirus-disinformation-caused-chaos-small-ukrainian-town-n1146936>

Miller, C. (20 February 2020). A Viral Email about Coronavirus Had People Smashing Buses and Blocking Hospitals. BuzzFeed. <https://www.buzzfeednews.com/article/christopherm51/coronavirus-ukraine-china>

Ponce de Leon, E., and Andriukaitis, L. (24 September 2020). Facebook Takes Down Assets Linked to Russian Disinformation Outlet. Medium. <https://medium.com/dfrlab/facebook-takes-down-assets-linked-to-russian-disinformation-outlet-acab0164e3d4>

Russian Congress of Canada. (21 March 2017). Appeal to Prime Minister Trudeau to Question Minister Freeland's Integrity. Russian Congress of Canada.

Shekhovtsov, A. (23 November 2015). Is Russia's Insider Sponsored by a Russian Oligarch with Ties to the European Far Right? The Interpreter. <https://www.interpretermag.com/is-russia-insider-sponsored-by-a-russian-oligarch-with-ties-to-the-european-far-right/>

Staff Writer. (26 January 2017). And You Are a Nazi, Too! EU East StratCom Task Force. <https://us11.campaign-archive.com/?u=cd23226ada1699a77000eb60b&id=d50f54d197>

Tsukanova, A. (27 February 2017). A Nazi Skeleton in the Family Closet. Consortium News. <https://consortiumnews.com/2017/02/27/a-nazi-skeleton-in-the-family-closet/>

Velichko, L. (28 February 2020). Masters of Panic: A Pro-Russian Network in Ukraine Organized a Riot in Novi Sanzhary. Texty. <https://texty.org.ua/articles/100356/specoperaciya-imeni-portnova-ta-shariya-yak-rozhanyaly-paniku-v-novyh-sanzharah-i-ho-za-cym-stoyit/>



Chapter 4 – THE INFLUENCE AND IMPACT OF SOCIAL AND CULTURAL SCIENCES IN COGNITIVE WARFARE

Matthew A. Lauder
Defence Research & Development
CANADA

4.1 INTRODUCTION

Informed by a variety of academic disciplines (e.g., anthropology, sociology, psychology, cultural studies, political sciences, communication sciences, and development studies, amongst others) and generally defined as *scientific activities focused on better understanding social behaviors, patterns, processes, and structures*, the social and cultural sciences offer unique insight into the issue of cognitive warfare (CogWar), specifically (but not limited to) the socio-technical mechanics of audience engagement and psycho-social effects generation, as well as potential interventions or responses to neutralize, mitigate or counter cognitive attacks on audiences. In other words, the social and cultural sciences offer insight into and can help inform the development of both offensive and defensive facets of CogWar, particularly at the meso and macro levels of analysis (i.e., characteristics of social interaction between groups and organizations through large-scale societal interactions).

4.2 METHOD AND THEORY

A distinctive feature of the social and cultural sciences is the breadth of methodological approaches, research techniques, and theories and analytical frameworks that can be employed to examine or underpin CogWar. For example, the social and cultural sciences includes both qualitative (e.g., case studies, participant observation, unstructured surveys, focus groups, etc.) and quantitative research methods (e.g., data surveys, correlational research, longitudinal surveys, etc.), which can also be integrated to support a mixed methods approach. Moreover, the social and cultural sciences are inherently flexible, allowing for the use of grounded theory (i.e., building theory from evidence) or more traditional approaches, such as hypothesis testing and theory validation through experimental research. Although a comprehensive list is beyond the remit of this report, some of the more prominent theories employed in the social and cultural sciences to enhance understanding of the socio-technical mechanics of, and the psycho-social effects generated by, CogWar, include:

- 1) **Social identity theory:** Originally developed by Henri Tajfel and John Turner (2004), social identity theory asserts that an individual's affiliation to a group, and the perceived status, legitimacy, and distinctions of that group, play a significant role in determining social behavior, including both social-constructive and anti-social behaviors. Two fundamental aspects of social identity theory include ingroup favoritism (showing preferential treatment to those affiliated with the ingroup) and out-group (or social) comparison (evaluating the in- to out-groups to establish a favorable perception of status), both of which play a role in developing a positive social identity and have an impact on group processes, norms, and structures as well as intergroup relations.
- 2) **Symbolic interaction theory (symbolic interactionism):** Less of a theory and more of a framework for understanding, symbolic interactionism asserts that actors respond to the subjective meanings attached to social phenomena and states that meaning may be modified through social interaction. In other words, meaning is adaptable, negotiated and reciprocal, and that reality is primarily a social product (i.e., socially constructed).

- 3) **Structural functionalism (or functionalism):** Structural functionalism is not a single, unifying, or grand theory; but a family or constellation of sometimes competing theoretical approaches and conceptual frameworks that comprehend society as a complex, open system in which the component parts strive for and maintain a degree of dynamic, interactive stability (i.e., homeostasis). Structural functionalism examines the system structures, relationships, interdependencies, functions, and conditions of a given society, the aggregation of which gives meaning to and regulates (i.e., bounds) human action.
- 4) **Conflict theory:** Commonly associated with Karl Marx, conflict theory refers to a set or constellation of theories that posits society is in a perpetual state of conflict because of competition for and access to limited resources, and that social order is maintained through power, primarily through political suppression and economic exploitation (Lauder, 2022). However, this theory posits that rather than an entirely destructive force, conflict is regarded as the engine of social change and transformation, such as through revolution.
- 5) **Framing theory:** Popularized by Irving Goffman, framing theory (also known as *frame analysis* or *simply framing*) is a multidisciplinary research method used to examine the process of selecting and creating as well as the transference, assessment, and the effects of message content on individuals and collectives (Lauder, 2022). Framing theory is often applied to news media reporting, political campaigns, and social movements, particularly to examine the construction and maintenance of meaning and account for behavioral effects. As a central component of framing theory, frames (what may also be called interpretative schemas) provide a way for people to interpret and understand social phenomena (i.e., events, issues, behaviors, etc.) by describing and giving them meaning in ways that appeal to and leverage shared knowledge structures.
- 6) **Structural strain theory:** More of a class of theories or frameworks than a single theoretical construct, structural strain theory asserts that society puts pressure on individuals to achieve a range of abstract normative goals, such as being successful. Perceiving a gap between one's status and societal goals, and lacking the means to attain these goals, people often resort to criminal activity to gain financial security. As a result, unconventional, deviant, and other anti-social behaviors become normalized. In other cases, people join sub-cultures, which allows them to reject mainstream society and substitute societal goals with more achievable goals (i.e., achieve an alternate definition of success).
- 7) **Rational choice theory:** A widely employed theory, rational choice theory proposes that an individual, motivated by self-interest, will conduct a cost-benefit analysis to determine the most profitable or beneficial option (i.e., to maximize utility or achieve the highest payoff).
- 8) **Chaos theory:** Applied across a range of disciplines, from anthropology to mathematics, chaos theory posits that, while appearing random, complex systems (such as social systems) can be distilled to underlying patterns, which can be used to predict system behavior. A central concept of chaos theory is that of the butterfly effect, which posits that, due to sensitive dependence on initial conditions, slight changes in a system can result in massive, downstream effects.
- 9) **Complexity theory:** Also referred to as *complex adaptive systems* and borrowing from chaos and systems theory, complexity theory posits that complex systems, while dynamic and adaptive, may be viewed as interdependent and constrained by order-generating rules that may predict system behavior.

4.3 AREAS OF INVESTIGATION WITHIN SOCIAL AND CULTURAL SCIENCE IMPACTING COGWAR

There are several areas of investigation to which the above-listed theories and analytical frameworks may be used to examine, or underpin the development of, CogWar. The following summary provides a list of broad topics for further consideration:

- 1) **Amplifying and exploiting social and political divides:** One facet of CogWar is for the adversary to stoke internal rifts in a target country, such as political, ethnic, economic, or class divides. The idea is that, by manipulating national discourse, often through disguised social media accounts (i.e., pretending to be a member of the targeted audience, also called *sock puppets*) and the employment of highly emotive, symbolic, and sometimes offensive language, an adversary can amplify divisions and lead to violent confrontation between groups and the state. A better understanding of the socio-technical mechanics and effects of this approach may be understood by several theories, particularly social identity theory, conflict theory, framing theory, and structural strain theory. For example, social identity theory, conflict theory and structural strain theory may offer insights into social, economic, and political divisions that may help us understand how audiences may be encouraged or incited towards rejecting normative structures, processes and engage in extreme violence, typically targeting other groups or the state. Moreover, framing theory may offer insights into how grievances are formalized, presented, and rationalized to inspire collective action.
- 2) **Disseminating rumors, gossip, and disinformation to generate collective anxiety and uncertainty:** Another key approach of CogWar employed by adversaries is that of rumors, gossip, and other forms of disguised or unattributed (e.g., black) disinformation (e.g., smear campaigns) that are specifically designed to be disseminated by and through social networks, whether virtual Peer-to-Peer (P2P) or Face-to-Face (F2F). The purpose of these attacks is to capitalize on and amplify uncertainty and create debilitating levels of fear and anxiety in a population so that they are not able to properly function. Another goal is to create conditions of social and political instability by generating distrust between the public and the state, particularly by creating a crisis of credibility on part of the state and normative structures. A range of theories can enhance an understanding of this area of investigation, including symbolic interactionism, structural functionalism, and complexity theory. For example, symbolic interactionism may offer insights into how meaning is generated and disseminated within specific audiences, particularly to ensure a high degree of message resonance. Likewise, structural functionalism and complexity theory may support better understanding of the role of social structures, including institutions and norms, in mitigating effects of negative or hostile messaging, as well as how messages spread throughout social networks.
- 3) **Exploiting cognitive errors in the decision-making process:** Often referred to as reflexive control and employed as a part of *maskirovka* (operational masking), and closely associated with perception management, the Russian government intentionally seeks to gain indirect and external control of a target's decision-making process, specifically to create conditions that lead the target to unwittingly make a false-optimal decision (i.e., a decision that favors the instigator). This may be achieved through the careful creation, selection, management, and release of information to the target, particularly to leverage and amplify any faulty perceptions, erroneous assumptions, or other cognitive errors, such as cognitive distortions, cognitive biases, and logical fallacies, et al., on part of the target. Critical in this approach is that the false-optimal decision may be selected voluntarily rather than coerced or forced upon the target by the instigator of reflexive control. In other words, the target must always cling to the idea of the *illusion of control* created by the instigator (Lauder, 2022). Other theories may help us to develop countermeasures to reflexive control and maskirovka, including framing theory, rational choice theory, and chaos theory.

- 4) **Building societal resilience to disinformation:** A range of factors have been identified as limiting societal resilience to disinformation, such as increased polarization of society, political populism, economic incentives to produce fake news, pervasive distrust of expert knowledge, mainstream news media and governance structures and traditional institutions. The question remains: How can societies build resilience to mediated forms of disinformation (i.e., disinformation that is technologically enabled)? Most solutions revolve around regulating social media platforms or identifying and removing disinformation from the information environment. However, other solutions, such as developing tools to help people evaluate information quality, address deeply embedded structural deficiencies or creating a culture of media literacy. There has been a limited amount of research conducted regarding these solutions, however, the issue of mediated disinformation continues to evolve rapidly due to changing tactics and technology. Thus, there is an array of theories presented to offer insights into how to build societal resilience, including complexity theory, structural functionalism, and symbolic interactionism.

4.4 MODUS OPERANDI – A CROSS-CUTTING ENABLER

Modus operandi is the deliberate, rigorous, and scientifically informed examination of methods, stratagems, and other patterns of behavior designed and operationalized by adversaries to generate the desired psycho-social effect on an audience, including activities employed to psychologically prime and create cognitive openings and other opportunities for adversarial intervention (i.e., pre-propaganda). Modus operandi is not limited in scope to the examination of specific tactics or tools, such as using a loudspeaker or a fraudulent social media account (although that is a part of the investigation) but is concerned with the holistic application and synchronization of a range of methods and resources across the dimensions of the information environment (i.e., cognitive, informational, and physical) to generate psycho-social effects.

The purpose of examining modus operandi is twofold. First, achieving a deep understanding of *what, when, and how* adversaries conduct CogWar can provide insights to support the development and validation of countermeasures and defensive strategies, such as programs to help build and/or maintain societal resilience or developing technological responses that significantly increase the cost of CogWar to adversaries while reducing or minimizing their effectiveness (i.e., deterrence by denial). Second, a deep understanding may offer insights into an adversary's own weaknesses and vulnerabilities, which can then inform the development and execution of offensive capabilities. For example, a close examination of Russian military reflexive control practices, and the underpinning theories and conceptual models, indicates that several vulnerabilities exist when these practices are executed, including the inadvertent release of intelligence by the instigator and the ability of the target (of the deception) to take control of the process by covertly manipulating the instigator's sense function (e.g., release of false data, technical manipulation of sensors, etc.) or the employment of perception management techniques (Lauder, 2022). Another risk of reflexive control is that the instigator of the effort can fall victim to a range of cognitive errors, particularly if the time-to-decision is artificially compressed (i.e., a hasty decision is provoked) by the target or if the instigator's analytical function is overwhelmed by a deluge of (false and positive) information or if the instigator's plans are revealed. The quick declassification and public release of classified information by the US intelligence community about the Russian government's intention to invade Ukraine during a specific time-period in February 2022 is an excellent example of undermining an instigator's attempt at reflexive control through pre-emption.

4.5 REFERENCES

Lauder, M.A., (2022). The Illusion of Control: A Pragmatic Retelling of Russian Military Maskirovka and Reflexive Control (DRDC-RDDC-2022-D024). Defence Research and Development Canada.

Tajfel, H., and Turner, J.C. (2004). The Social Identity Theory of Intergroup Behavior. In J.T. Jost and J. Sidanius (Eds.), Political Psychology: Key Readings, pp. 276-293. Psychology Press. Doi: 10.4324/9780203505984-16.



Chapter 5 – COGNITIVE AND BEHAVIORAL SCIENCE (PSYCHOLOGICAL INTERVENTIONS)

Benjamin J. Knox

Norwegian Armed Forces Cyber Defence
NORWAY

5.1 INTRODUCTION – COGNITIVE AND BEHAVIORAL SCIENCE (PSYCHOLOGICAL INTERVENTIONS)

The Cognitive and Behavioral Science (CBS) pillar intends to allow for research that can establish ways to be proactive, rather than reactive when approaching CogWar from a tactical, operational, and strategic perspective. Our adversaries study and target our psychological assets and vulnerabilities. Therefore, we must seek to know ourselves better, from an objective meta-perspective, and understand our adversaries' way of thinking and behaving from an equally critical perspective. Finding new approaches, applying known methods, and combining human and data-driven techniques in novel ways, can help learning processes that answer the question 'why' things are happening. Thus, leading to research concerned with informing decisions about 'what' should be done in response. Hence, the Cognitive and Behavioral Science pillar describes a field that is multi-disciplinary and emphasizes the criticality of psychological interventions in CogWar research.

Research on psychological processes and mechanisms in the last century have given psychologists a better understanding of human behavior, emotion, and cognition. Research in cognitive and behavioral science has identified, for example, factors of persuasion, manipulation, behavior change, and social processes (Cialdini, 1993; Hadnagy, 2010) that can be targeted in CogWar. For example, by understanding how dual processes of cognition function (emotional and rational cognitions), one can use this information not only to understand how CogWar techniques attack vulnerabilities but also how to increase resilience and mitigate such attacks. Seemingly then, research from the cognitive and behavioral sciences has identified factors to understand the goals of CogWar. Arising from a fundamental knowledge of human behavior, science has and must continue to focus on analyzing the requisite knowledge for identifying, securing, defending, and countering adversarial CogWar goals. This involves the complex process of creating causal understanding, establishing cause and effect between events, and the meaning of short and long-term attack methodologies and patterns. This knowledge is critical for military decision-making at the individual level, and necessary for the development of collective sustainable modes of resilience and countermeasures.

5.2 INFLUENCE OF COGNITIVE WARFARE

Today, targeted, arbitrary, and experimental cognitive operations occur within the information space of humans primarily through the virtual domains (Montañez et al., 2020). Advancements in CogWar are interwoven with the application and integration of narrow AI into our daily lives, and these target basic cognitive functions that were evolved for survival. For example, social media giants evoke the same mechanisms by altering their algorithm to increase user engagement by dosing their feed with stories that can trigger emotional responses which leads to more heuristic processing and automatic behavior (Stieglitz and Dan-Xuan, 2013). Our emotions are driven by the autonomic nervous system and can be difficult to regulate since they can steer both attention and behavior. As an example of how CogWar can target emotional processes, research has shown that inciting

outrage causes intense emotional responses in individuals (Berger, 2016; Fan et al., 2014) that in turn can create a social emotional contagion that can cause groupthink which can lead to more risky decision-making at higher strategic levels (Kramer et al., 2014).

CogWar can also target other cognitive aspects. The mind operates through a process of pattern recognition since working memory has limited capacity, and any information that does not fit known patterns will cause increases in working memory usage to make sense of what is happening, including emotional processes. Increase in working memory can quickly be stressful as we are processing information and coping with any outcomes that can happen. The increase of working memory use decreases attention to other factors that may be relevant. In other words, CogWar can target increasing an individual's workload so that they can be distracted or unable to identify other pertinent information. For example, when one considers that humans have such a strong tendency to impose context onto ambiguous stimuli, how one manages to redirect or override one's own projections and perceive information as it truly exists, demands a high level of deliberate effort. Should an attacker layer his/her effort with a culturally consistent narrative, present a motivation for hypervigilance, and use social media as an amplifier, this can reinforce and further direct (or mis-direct attention depending upon attacker intent) attention (Canham et al., 2022). Today, this idea is made possible through technologies such as AI, or Generative Neural Networks (the architecture responsible for creating Deepfakes), that can be applied with a policy of, "let's see what's possible." These are experiments at scale without any clear principles, rules of law, rules of engagement, ethical or moral engagement as to what the outcome may be. Whether it is used to boost or manipulate information around you, or to anchor you, or to change your opinion, one needs to be cognizant of what drives our attention, and meta enough to see something when it is interfering with our predictions, judgements, and biases (Sütterlin et al., 2022).

5.3 COGNITIVE WARFARE AND SELECTIVE ATTENTION

This point highlights the overlap with all the horizontal factors in the model. Just as we grapple with explainability issues and bias in AI, this pillar investigates what it is like to be human and the continuous effort and motivation needed to understand the cognitive barriers and strategies that explain a state i.e., control of cognitive and behavioral factors that may be affecting current SA, such as explainability issues and bias. To use the social engineering example, while social engineering tactics have been understood in marketing and persuasion, only recently has research begun to emerge that places effort into mapping individual and cognitive-emotional factors affecting susceptibility to- and resilience against social engineering attacks in cyber domains (Brangetto et al., 2016). When CogWar operations act to influence a person, or persons, to take an action that may or may not be in their best interest; then, it will be achieved by applying well-established tactics of persuasion, such as social proof or reciprocity, depending on the target. What is new is the available technologies that can affect the *input* data into our brains to grab or manipulate our attention to induce an emotional reaction. By redirecting attention towards internal processes such as the significance of emotional reactions or gut-feelings, this leads to impulsive decision-making: *output*. This occurs due to a manipulation to increase attentional processes to more emotional and subjective aspects instead of more reflective and more objective evaluations thus decreasing the possibility to critically examine the current situation and take more critical and reflective decisions.

CogWar operations tend not to be transparent. This mirrors certain technologies such as AI in our daily lives. Operations happen in a black box and outcomes often cannot be explained. The current unstoppable state in terms of super-human technological development for the good of society is that explanation and transparency is unnecessary so long as the outcomes improve human intelligence, efficiency, and economic productivity (mostly in the eyes of technologists and industry). In the pattern detection of new properties that were once

inconceivable to humans that lead to the production and advancement of antibiotics, education, and entertainment, we see narrow AI finding combinations that a human could never have seen or predicted. This is unquestionably positive. However, the inevitable industrialization of this technology and its dual-use potential should be addressed as a threat and not tolerated by NATO. As such, from a NATO S&T perspective, explanations of outcomes and transparency is essential as this knowledge can reduce the effects of CogWar. Whether the effects are unintended, self-inflicted, or induced, cognitive harm may occur. Such cognitive impairment (temporary or permanent) may accrue from naive over-exposure to certain technologies that may impact cognitive processes and/or development. It may also be the case that cognitive attacks remain obfuscated by the technological state of our lives and may target basic cognitive process such as cognitive bias. These technologies may have been designed by well-intentioned developers, or by consciously malicious technology companies linked with an adversary. Whatever the motivations, the goal is cognitive control, and by targeting the less regulated or vulnerable parts of the brain to encourage maladaptive behaviors, or to trigger an emotional response and shift our attention, adversaries exert control over cognitive processes and initiate disruption, social contagion, undermining our innate cognitive processes and shape decision-making in support of their objectives.

5.4 RECOMMENDATIONS

When technology companies use researchers and ML, or deep learning techniques to study user data to understand behavior, they make rediscoveries, and identify ways to anticipate, but not understand user behavior. In the **short-term** the Cognitive and Behavioral Science pillar should engage with behavior science experts to perform and inform studies that anticipate and test for the potential dual use of technologies. Together they can explore where technologies have been designed and operationalized already and see if users have been harmed in unintended ways. This knowledge driven approach to building understanding concerns how certain technologies are being designed and how they can be used to do harm, intentionally or unintentionally. It will allow NATO to respond not just in redirecting user behavior, but predicting CogWar operations and gain the foresight, grounded in sensemaking, to defend known human cognitive vulnerabilities before they are exposed to technologies that are intentionally designed, or misappropriated to exploit them.

In the **medium-term** S&T needs to investigate social engineering when it occurs at scale, across multiple perceptual levels, and through different modes of delivery, enabled by modern technology. The complexity lies in developing ways to build self-regulatory skills (such as metacognition) that lead to greater collective vigilance. Research needs to find the balance where being reserved can equate to vigilance, rather than revealing victim behaviors. This multi-disciplinary and multi-method approach is novel and combines cognitive science, social psychology, social and cultural science, and the neuroscience pillar. When this is discussed relating to national security, military intelligence, and NATO collective defence, research needs to address the multiple perceptual levels involved in CogWar. As shown above, CogWar can be a combination of things targeting perceptions. Therefore, people can't be vigilant all the time. Methods need to be found that augment and help people learn to be vigilant intuitively. Like battle inoculation training in simulated conditions to prepare soldiers for deployments in combat, the same basic concept can be developed to level up performance in CogWar. Preparing soldiers for the effects by exposing them to the attack, helps to prepare them and enables them to learn methods for coping in a CogWar context. This will also help them regulate their own behaviors, so they become learned System 1 intuitive behaviors.¹ When training and education for CogWar pivots to vigilance and meta-cognitive skills development, cognitive security is likely to increase as CogWar operations and attacks become more salient as the mechanisms are no longer hidden in the complexity of plain sight. Just as previous operational and combat experience helps to prepare soldiers for future situations, experiencing CogWar, teaching soldiers how it happens, letting them imagine and develop

¹ For further reading on System 1 and 2 thinking see Daniel, Kahneman (2011), Thinking, Fast and Slow.

scenarios, and then perform the attack on each other. This pedagogic approach gives the learner the tools, but the process will involve such things as group consensus and individual differences, both of which CogWar targets to achieve its goals.

Doing this can mark the beginning of the **long-term** process of recognizing CogWar intuitively in real world situations before their working memory is blocked or overloaded by the attack. The process of making intuition a positive resource rather than a bias involves individuals understanding the mechanisms of CogWar, so they have a greater chance of intervening. This does not involve every service member becoming a cognitive scientist, but it does require awareness of the factors in NATO and the alliance (or a society) that can be targeted, knowledge of individual-level cognitive vulnerabilities that make them susceptible to attack and which skills can mitigate those vulnerabilities, and implementation of individualized and collective training efforts.

This pillar will direct research in Cognitive and Behavioral Science through psychological interventions. Research will shed light on how today's technological context is enabling such things as narrow AI to guide and lead our decision-making without us being aware of it too often. When an adversary is piggybacking, hijacking or part of the development process of this technology; then, it is critical that we have the knowledge and tools to minimize and defend against instances to prevent this from happening.

5.5 REFERENCES

- Berger, J. (2016). *Contagious: Why Things Catch On*. Simon and Schuster.
- Brangetto, P., and Veenendaal, M.A. (May 2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. In 2016 8th International Conference on Cyber Conflict (CyCon), pp. 113-126, IEEE.
- Canham, M., Sütterlin, S., Ask, T.F., Knox, B.J., Glenister, L., and Lugo, R. (2022). Ambiguous Self-Induced Disinformation (ASID) Attacks: Weaponizing a Cognitive Deficiency. *Journal of Information Warfare*, 21(3), pp. 43-58.
- Cialdini, R. (1993). *Influence: Science and Practice*, 3rd Edition, New York. Harper Collins College Publishers.
- Fan, R., Zhao, J., Chen, Y., and Xu, K. (2014). Anger is More Influential than Joy: Sentiment Correlation in Weibo. *PloS one*, 9(10), p.e110184.
- Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. John Wiley & Sons.
- Kahneman, D. (2011). *Thinking Fast and Slow*. Farrar, Straus and Giroux.
- Kramer, A.D., Guillory, J.E., and Hancock, J.T. (2014). Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks. *Proceedings of the National Academy of Sciences*, 111(24), pp.8788-8790.
- Montañez, R., Golob, E., and Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, 11, p. 1755.
- Stieglitz, S., and Dang-Xuan, L. (2013). Emotions and Information Diffusion in Social Media – Sentiment of Microblogs and Sharing Behavior. *Journal of Management Information Systems*, 29(4), pp.217-248.

Sütterlin, S., Lugo, R.G., Ask, T.F., Veng, K., Eck, J., Fritschi, J., Özmen, M.T., Bärreiter, B., and Knox, B.J. (2022). The Role of IT Background for Metacognitive Accuracy, Confidence and Overestimation of Deep Fake Recognition Skills. In International Conference on Human-Computer Interaction, pp. 103-119, Springer Cham.



Chapter 6 – DEVELOPING COGNITIVE NEUROSCIENCE TECHNOLOGIES FOR DEFENCE AGAINST COGNITIVE WARFARE

Claude C. Grigsby

US Air Force Research Laboratory
UNITED STATES

Nathaniel R. Bridges

US Air Force Research Laboratory
UNITED STATES

Richard A. McKinley

US Air Force Research Laboratory
UNITED STATES

Jennifer Carpena-Núñez

US Air Force Research Laboratory
UNITED STATES

6.1 INTRODUCTION – COGNITIVE NEUROSCIENCE: DEFENCE AGAINST COGNITIVE WARFARE

Future battles will involve far less permissive environments, agile logistics, and adaptive command-and-control. With the increased role of automation, artificial intelligence-enabled virtual teammates, and remote control/supervision of technology, there is a new focus on Cognitive Warfare (CogWar). CogWar targets the human brain/mind by using disinformation, propaganda, and information overload to confuse the enemy and exploit cognitive vulnerabilities. There is a pressing need for the DoD to invest in the emerging area of CogWar, a capability that does not yet exist for allied nation's military, but near-peer adversaries are aggressively developing such capabilities. Adversarial advances in offensive CogWar must be proactively matched and exceeded by leveraging expertise in cognitive and brain sciences, brain-machine interfaces, applied psychology and AI/ML to enhance the warfighter's ability to counter such attacks and prevail in the modern battlefield.

In a military context, a warfighter's cognitive abilities are extremely important in the modern battlespace. There is a need to process vast amounts of data/information rapidly and accurately and ensure that information garnered from such processing is trustworthy, accurate, and dependable. Errors in processing may have dire cascading consequences for effective decision making in the operational environment. These abilities are often suboptimal under conditions of stress and fatigue and may further degrade information management in the command and control chain in modern joint all-domain operations. The impact of such shortfalls is detrimental to human performance and may well increase cognitive and information workload, as well as challenges related to adversaries who will exploit such errors to their advantage. These ever-increasing demands of war have led to the new concept of Cognitive Warfare. A recent NATO-sponsored study described CogWar as the “*weaponization of the brain sciences*” and contended that advances in CogWar will offer our adversaries “*a means of bypassing the traditional battlefield with significant strategic advantage, which may be utilized to radically transform Western societies.*” According to Claverie and Cluzel (2022), CogWar is “*the art of using technological tools to alter the cognition of human targets, who are often unaware of any such attempt,*” or alternatively to “*manipulate an enemy or its citizenry’s cognition mechanisms to weaken, penetrate, influence or even subjugate or destroy it.*” The ambit of CogWar can extend beyond military to target the entire nation’s human capital.

As du Cluzel stated (Du Cluzel, 2021), CogWar “*does not focus strictly on the field of “information” but on that of “cognition”, i.e., what the brain does with information. [...] the cognitive effect is not a consequence of the action; it is its goal.*” As such, it threatens cognition across all levels, and from the complex psychological aspect

may negatively influence and/or impact human interaction and socio-political factors to the most basic physiological (neurological) pathways associated with cognition. While CogWar remains intangible for the time being, this may not be the case for future CogWar. Simply put, neuroscience knowledge products along with emerging neurotechnologies will soon facilitate tangible avenues for CogWar.

Below we highlight three key areas within cognitive neuroscience (and associated fields) that will heavily influence the future of CogWar:

6.2 NEUROSCIENCE AND NEUROMODULATION TECHNIQUES

In contrast to PSYOPS, CogWar focuses on the exploitation of cognitive vulnerabilities including attention overload, perceptual narrowing (“tunnel vision”), and cognitive biases and errors of judgment that detrimentally influence decision making (Figure 6-1). This aspect of CogWar is particularly relevant to Command and Control (C2) operations. Claverie and Cluzel (2022) noted that Gen. Desclaux defined the C2 strategic processes as “a cognitive triangle involving knowledge dominance, cyber confidence, and decision superiority.” Given that attention serves the decision maker by selectively acquiring the information needed to decide, attention and decision-making are highly interconnected. Hence, these two aspects of cognition serve as a central focus and distinguisher of the CogWar domain.

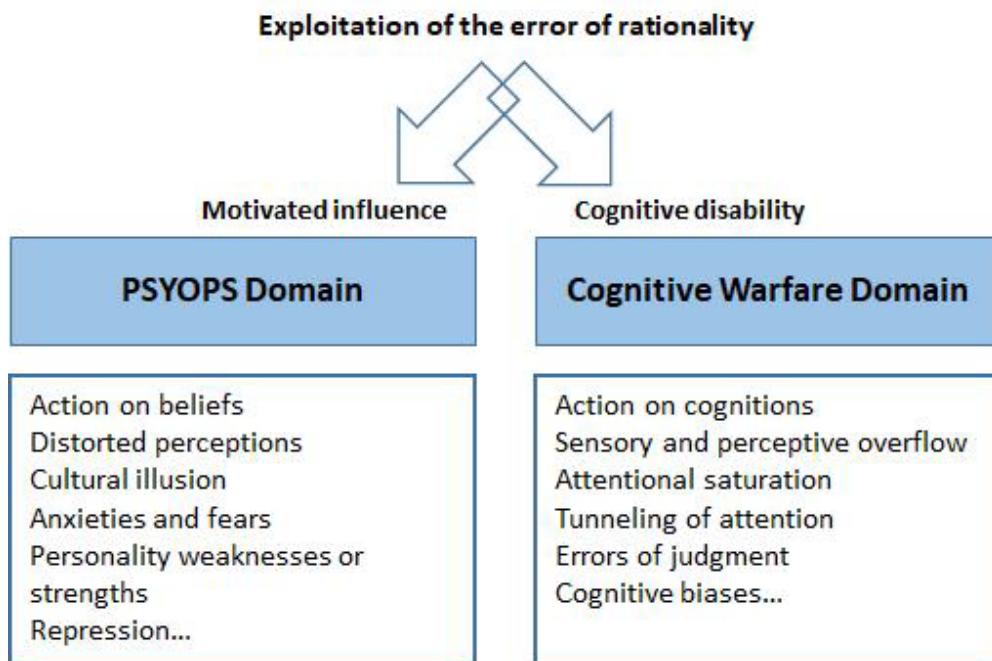


Figure 6-1: Differences Between CogWar and PSYOPS (Claverie and Cluzel, 2022).

Over the last decade, nations have made tremendous advancements in our understanding of brain function due to the accelerating pace of research in neuroscience and psychology coupled with the development of sophisticated neuroimaging tools and analysis methods from biomedical/neuro-engineering. We now have a better understanding of the neural processes that are associated with learning, memory, stress, arousal, attention, emotions, and motor control – attributes that are highly relevant to cognitive performance and decision making.

We have also witnessed the development of novel neural network models that describe and predict cognitive biases and their neural substrates and that, in doing so, now allow the systematic targeting of deviations from rationality that lead to suboptimal decision outcomes. In addition, emerging technologies such as non-invasive neuromodulation have shown great promise in modulating many aspects of performance enhancement.

Notably, both neuroscience and neurotechnology are critical elements to future Counter-CogWar. Advances to neuroscience and neurotechnology including neuroimaging, multi-modal sensors, and signal decoding, etc., will provide the means to assess human cognitive states (workload, stress, emotion, and fatigue) real-time; Active monitoring of attention during future ops will enable enhanced (faster, more accurate and dependable) human-machine teaming via AI-enabled decision aids (see AI segment below). Other advances to neuropsychopharmacology and neuromodulation paradigms will provide the means to reduce fatigue, increase learning, and overall improve cognitive performance, increasing resilience against CogWar. For example, non-invasive neuromodulation (e.g., targeted transcranial electric and magnetic stimulation, peripheral nerve stimulation) and interface and interaction design (e.g., human-centered design, adaptive information portrayal) will deliver performance augmentation by selectively targeting attention and decision making.

While allied nations and defence services have promising research efforts in cognitive neuroscience, nations have not focused their research efforts on the development of defensive CogWar capabilities. In contrast, adversarial national strategies for military-civil fusion with a focus on NBIC and CogWar has left our nation at an immense risk of being over-shadowed by adversaries in a domain that will be increasingly critical in future warfare. Indeed, CogWar is a bleeding-edge challenge space that does not exist across allied forces. Thus, an allied Counter-CogWar strategy is essential if we are to enhance our military readiness and requires that we develop programs to expand our knowledge, establish training paradigms, propel technology innovation, and deploy tactical and strategic interventions that effectively target CogWar.

6.2.1 Neural and Brain-Machine Interfaces

One controversial emerging neuro-technology is the concept of Brain-Machine Interfaces (BMI). This game-changing technology holds the promise to reduce cognitive burden during future wars via enhanced human-machine symbiosis and faster communication in contested environments. BMI also contextualizes the means to perform direct ‘read’ and ‘write’ from the brain, and to enable brain-to-brain communication. The most technologically mature aspect of BMIs (the ‘low hanging fruit’) is the ‘read’ element. BMIs with ‘read’ capabilities enable defensive CogWar by identifying physio-cognitive states that predict high vulnerability to adversarial CogWar, such as lapses of attention, fatigue, stress and uncertainty, and high workload. By classifying these emergent states in warfighters, the BMI system can seamlessly select and administer interventions in an autonomous manner. With ongoing efforts within the military and industry to increase the spatial resolution of “read” BMIs through new sensors/devices, it will become possible to issue commands to technology (e.g., bring up a surveillance camera feed, select a menu, etc.) through simple thought. BMIs with ‘read’ and ‘write’ capabilities, on the other hand, open a realm of possibilities for operators. For instance, closed loop monitoring of human operator attention combined with Artificial Intelligence- (AI-) driven decision aids, secure visual displays content, and Augmented Reality (AR) displays may provide the means to delivering information directly to the brain – like BMI concepts presented in the movie ‘The Matrix.’ Such technology poses clear threats to human autonomy and societal democracies, not just in terms of ELSEI and other privacy concerns but also in the context of cyber security and cyber supremacy. As stated by Orinx and Swielande, “*the development of more and more sophisticated means such as artificial intelligence, (...) and neurosciences facilitate manipulation*” (Orinx and Swielande, 2022) [of cognitive and decision-making processes]. Thus, future wars will rely heavily on secure means of information delivery, i.e., networks and cognitive processes that can warrant cognitive security and superiority.

6.2.2 Automation, Autonomy, and Artificial Intelligence (AI): Improved Human-Machine Teaming and Decision Making

As mentioned, attention and decision making are key players in CogWar. Thus, capabilities that leverage automation, autonomy, and AI assistants that assist cognition will be increasingly critical. Such capabilities will facilitate communication between man and machine, reduce burden on cognitive load, and accelerate the speed and volume of information processing. Mission spaces including C2, cyber defence, remotely operated vehicle control, and ISR (Intelligence, Surveillance, and Reconnaissance) all utilize massive quantities of data and information that are prone to information overload, cognitive bias, and/or attention tunneling. Operators often make decisions quickly under a variety of stressors (fatigue, workload, uncertainty, etc.), and their decision making is more likely to be influenced negatively by biases and misinformation. As the battle space becomes increasingly complex, adversaries will seek to gain military advantage by exploiting misinformation and injection of unprecedented levels of uncertainty, making it more challenging for decision makers to confidently detect and exploit reliable information amid the noise. CogWar capabilities that leverage or improve human-machine teaming and decision making via automation, autonomy, and Artificial Intelligence (AI) will provide cognitive security by ensuring the means to discretely and objectively informing decision makers. Such capabilities will safely modulate key brain areas associated with wakefulness and attention, helping each analyst/C2 decision maker accelerate information processing speed, sustain attention, and reduce fatigue.

Counter-CogWar capabilities assisted by AI will help monitor the types of tasks, the number of tasks, and the specific tasks that an operator is attending. Critically, this will allow autonomy/AI to provide customized support to operators such as target recognition technologies, neuromodulation, or alterations in display content, to help them maintain performance in times of distress and augment performance when necessary. Such tools can also provide the means to identify and deter threats associated with future capabilities, e.g., direct ‘read’/‘write’ from the brain. These may help ‘orient’ decision makers at times of cognitive overload or CogWar attacks.

6.2.3 Technical Areas Requiring De-Risking for Effective Counter-Cognitive Warfare

Table 6-1: Technical Areas of Neurotechnology Requiring De-Risking.

		Risk	Mitigation
1)	Monitoring Cognitive State	Extracting functional brain information with high spatial and temporal resolution non-invasively. This is not currently possible with existing mobile technology.	Leveraging ongoing public and private investment in the development of novel, non-invasive biosensing technology.
2)	Assessing Cognitive State	Achieving real-time classification and ‘decodification’ of brain signals at the speed of thought. This remains a challenge for existing technology and data analytics.	Exploiting advancements in computational power and the speed of edge computing coupled with a growing expertise in the latest AI/ML techniques dedicated to neurophysiological data analysis optimization.
3)	Enhancing Cognitive State	Neuromodulation of central or peripheral nervous systems to enable performance enhancement or information transfer with high spatial and temporal resolution non-invasively. This is not currently possible with existing technology.	Leveraging industry and academic investments in state-of-the-art technologies and analysis methods to ensure optimal performance enhancement and information transfer.

		Risk	Mitigation
4)	Integrating Cognitive Paradigms	Developing robust hardware/software subsystems that operate seamlessly within deployable multi-modal systems. This has only been accomplished for simple (e.g., single modality) sensor systems and rudimentary (e.g., workload tuning) augmentation systems in constrained laboratory contexts.	Establishing system-of-systems integration methodologies and dedicated interdisciplinary workforces that expedite the design and development of integrative systems.

6.3 RECOMMENDATIONS AND CONCLUDING REMARKS

It is evident that future CogWar will benefit from capabilities that adaptively select and administer neuro-enhancing techniques to boost attention and enhance decision making. Such capabilities must protect against key cognitive stressors (fatigue, uncertainty, and information overload) during critical warfighter tasks, insulating warfighters against adversarial CogWar and empowering them to administer offensive CogWar. To accomplish this, nations must shift focus from offensive to defensive mechanisms that mitigate adversarial CogWar and interrupt their offensive campaigns. Said strategies include developing tools and technologies to increase awareness of CogWar, penetrating and disrupting misinformation campaigns, securing information sharing platforms and preventing breach, developing counter Neurotechnologies, and establishing frameworks that unify CogWar efforts. Future CogWar concepts will thus require coordinated operational imperatives, robust platforms, infrastructures and data pipelines or architectures that secure our cognitive domain and penetrate and dissolve adversarial practices. Furthermore, Nations must orchestrate efforts to:

- Improve understanding of the psychological, sociological, and emotional variables influencing cognition.
- Identify and address factors that increase vulnerability in individuals or groups of individuals.
- Identify vulnerabilities and turning points (e.g., via modeling and War Games) within decision-making OODA-loops (Observe, Orient, Decide, Act).
- Identify communication/information pathways (e.g., within social or cyber networks/platforms) and points of intervention.
- Identify and deter cognitive attacks by ‘passive’ (i.e., via ‘ground truth’ campaigns) and ‘active’ (i.e., via neuro-interference and secure BMIs) means.
- Identify critical warfighter tasks that must be secured/insulated against adversarial CogWar.
- Identify militarily relevant BMI and other neurotechnologies.
- Identify and address gaps between commercial/clinical technologies and military use cases (i.e., populations, needs, and operational environments).
- Develop hardware/software optimization, protocols, and data processing pipelines that accelerate the development of Counter-CogWar technologies.
- Identify and address barriers-to-adoption of Counter-CogWar technologies (including neurotechnology, neural or brain-machine interfaces, AI, etc.) created by the lack of evaluation criteria and baseline metrics.
- Establish common practices, requirements, capabilities, and evaluation/validation criteria.
- Develop a suite of “neuro-weapons” in the form of a highly trained workforce and BMI-enabled warfighters.

6.3.1 Technical Gaps Limiting the Adoption of BMI Systems into Military

Additional hurdles impact the development, deployment, and integration of BMIs. Whilst some arise from ELSEI concerns, a significant number are technical in nature. Below is a list of key technical gaps limiting the adoption of BMIs into military CogWar concepts:

- 1) Testing and evaluation of current and emerging Brain-Machine Interface (BMI) technologies.
- 2) Quantification and assessment of signal quality, usability and comfort, and hardware and software limitations on relevant populations.
- 3) Evaluation of system/operational requirements (i.e., form factor/power restrictions, signal/noise processing, network security, etc.).
- 4) Non-human subjects engineering tests, sensor positioning accuracy and repeatability testing using 3D scanning, and BMI device property characterization procedures.
- 5) Delivery of data-driven decision matrices for codification of strengths and weaknesses of BMI technologies and their relevance to career domains and use cases.
- 6) Development of virtual reality maintenance environments and relevant tasks with the ability to quantify research subject motion dynamics.
- 7) Strategic partnerships with leaders and organizations developing BMI technologies.
- 8) Provide strategies for engagements/links between the BMI and operational communities.

6.4 SCIENCE AND TECHNOLOGY DIRECTIONS: THE WAY AHEAD

Below we delineate the near-term and long-term state of neurotechnology:

- **Now (1 – 2 years):** Mature cognitive state assessment technologies, predictive algorithms, and cognitive augmentation approaches to defend against CogWar. Leverage new sensors and stimulation techniques to increase spatial resolution for future read and write to the brain applications.
- **Next (3 – 5 years):** Develop closed loop monitor and augment systems for personalized sustainment, augmentation of Operator performance. Develop brain activity “libraries” to read user commands directly from the brain using high-resolution BMI technology.
- **Future: (5+ years):** Mission specific modular systems for cognitive/physical state assessment with real-time sustainment and augmentation feedback tech; BMI with full read and write capabilities.

6.5 REFERENCES

Claverie, B., and du Cluzel, F. (2022). Cognitive Warfare: The Advent of the Concept of “Cognitics” in the Field of Warfare. In Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. Cognitive Warfare: The Future of Cognitive Dominance. NATO STO, Neuilly-sur-Seine, France. <https://hal.archives-ouvertes.fr/hal-03635889/document> (Retrieved 10 August, 2022).

Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. (2022) Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 20201. NATO STO, Neuilly-sur-Seine, France, pp.8, 1-6. <https://www.innovationhub-act.org/sites/default/files/2022-03/Cognitive%20Warfare%20Symposium%20-%20ENSC%20-%20March%202022%20Publication.pdf> (Retrieved 10 August 2022).

Du Cluzel, F. (2021). Cognitive Warfare, a Battle for the Brain. STO-MP-AVT-211 (KN3-1 – KN3-12). <https://www.innovationhub-act.org/sites/default/files/2022-03/Cognitive%20Warfare%20Symposium%20-%20ENSC%20-%20March%202022%20Publication.pdf> (Retrieved 10 August 2022).

Orinx, K., and Struye de Swielande, T. (2022). China and Cognitive Warfare: Why Is the West Losing? In Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 20201. NATO STO, Neuilly-sur-Seine, France. <https://hal.archives-ouvertes.fr/hal-03635889/document> (Retrieved 10 August 2022).



Chapter 7 – DEFENCE AGAINST 21ST CENTURY COGNITIVE WARFARE: CONSIDERATIONS AND IMPLICATIONS OF EMERGING ADVANCED TECHNOLOGIES

Yvonne R. Masakowski

US Naval War College
UNITED STATES

Eskil Grendahl Sivertsen

Norwegian Defence Research Establishment
NORWAY

The same wide span of Fourth Industrial Revolution technology (data, processing, connectivity, AI, robotics, biosciences, autonomy and so forth) that is changing how we live, work and play will now transform the way war is waged – in a process spanning at least a generation ... Military transformation will largely be about the rapid adoption and adaptation of civil-sector-derived technology and methods in disruptive military applications ... The future of military success will now be owned by those who conceive, design, build and operate combinations of information-based technologies to deliver new combat power.

General Sir Richard Barrons (Uppal, 2022)

7.1 INTRODUCTION

Twenty-first century advances in technologies such as Artificial Intelligence (AI), Machine Learning (ML), Autonomous systems, Robotics, drones, and the emergence of a vast array of Social Media platforms have transformed the 21st century battlespace. Cheap, commercially available drones have proven to be effective Intelligence, Surveillance, and Reconnaissance (ISR) assets that may also deliver effects in the cognitive dimension. Small drones are silent and difficult to detect. Equipped with sensors as well as explosives, such as hand grenades, and off-the-shelf drones may have a significant psychological impact on troops on the ground. Combined with other technologies, such as facial recognition software, drones become a major force multiplier for cognitive warfare. Indeed, these technologies have reconfigured the battlespace and altered the character of warfare. The evolution of advanced technologies has given rise to Cognitive Warfare (CogWar). Du Cluzel describes CogWar as the “manipulation of the enemy’s cognition” aimed at weakening, influencing, delaying, and even destroying the enemy (Du Cluzel, 2021; Claverie and Du Cluzel; 2022, Claverie et al., 2022). This type of warfare influences human heuristics and decision making and extends its reach to the public, society and to the military. CogWar represents the convergence of Psychological Operations (PsyOps), Information Operations (INFO OPS), and cyber operations with the advance of AI/ML networks that serve as an enabler for the distribution of the adversary’s strategic agenda in exploiting human vulnerabilities and shaping human understanding of events (Guyader, 2021).

Information and Communications Technologies (ICTs) have changed warfare. Today, these technologies enable actors to infiltrate the cognitive dimension of the Information Environment (IE) more effectively. Overt and covert influence and interference methods are being employed systematically by malign actors to shape and manipulate the situational awareness and decision-making process on all levels – from the international political level to the military strategic, operational, tactical, and sub-tactical level.

Even in the most remote and less developed regions of the world, most people have Internet access, smart phones, and social media accounts. This enables them to document and share observations and information

about their surroundings including military equipment, troop movements and tactics. Also, most troops are connected and have social media accounts, even if they may not use their devices on the battlefield. Commercially available drones, facial recognition software, artificial intelligence, geo-tagging, and satellite imagery have added another layer of both risks and opportunities to be understood, mitigated, and exploited by all parties, civilian and military, in areas of conflict.

The permeation of Information Communication Technologies (ICTs) in operation (AO) poses obvious risks to Operation Security (OPSEC), Information Security (INFOSEC) and freedom of maneuver for any part in any conflict. For example, in the aftermath of the downing of Malaysian Airlines MH17 over Ukraine in 2014, Bellingcat was able to identify and document Russian personnel, equipment, tactics and locations using Open-Source Intelligence (OSINT) techniques including mapping of videos, images and social media accounts belonging to both civilians and Russian troops (Bellingcat, 2019). For all parts of an armed conflict today, ICTs offer vast opportunities for intelligence gathering, improved Situational Awareness (SA), Battle Damage Assessment (BDA), shaping of the battlefield and deception. However, as with all technology, the flipside of increased opportunity is increased risk. CogWar represents a new, insidious, and invisible threat to human decision making across all domains. CogWar influences human perception and decision making across the military, political, economic, and societal environments. Information has been weaponized across a wide array of platforms and used to target individuals, governments, and the mass consciousness as a means of justifying an adversaries' strategic objectives. Thus, the Tide Sprint Cognitive Warfare workshop was focused on addressing how best to defend against CogWar as we anticipate that this trend will continue to accompany future emerging technological advances in the coming years.

Namely, advances in brain research, brain-machine interfaces, neuroscience, quantum computing power, and genomic research, etc., will continue to be integrated in the design of future technologies. The integration of advances in AI and ML algorithms has provided adversaries with a new type of weapon.

The automated production of content is now possible with minimal effort as enormous amounts of information may be generated and used to target individuals, governments, and the mass consciousness at a rapid rate. This capability empowers individuals such that one person may influence a wide audience across thousands of social media accounts to influence and create confusion. Adversaries may spread their influence by setting up proxy sites, such as fake news sites or blogs, which has become quick and easy (Hao, 2020). Deep fake technology is becoming readily accessible, enabling anyone with decent computer skills to create images, voice, and video recordings that seem authentic but are not. While fake, extremely convincing content may be effective in manipulating target audiences, it may also have a chilling effect, as the increased presence of deep fake material on the Internet may lead to decreased trust in digital evidence. Thus, the Internet and social media serve as vehicles of information for transmitting their message and agenda. We anticipate that this trend will continue and shape future CogWar.

Likewise, it is easy to develop facial recognition technology that may be readily configured to identify adversaries in the battlefield. One single soldier with a cheap camera or camera drone, facial recognition software and internet access may be able to identify opposing soldiers in the battlefield. In Ukraine, drones equipped with facial recognition and social media have been used to identify Russian soldiers (Clayton, 2022). In several hundred cases, Ukrainian forces have sent photos of dead Russian soldiers to their families to stir up dissent in Russia (Lonas, 2022). So too, drones equipped with facial recognition technology has been used to conduct BDA and identify family members who were killed during the Russian invasion of Ukraine.

Adversaries may now corrupt AI/ML networks by integrating poisoned training datasets into ML algorithms (Dickson, 2021). Adversaries can now integrate poisoned datasets into social media sites and training datasets used to develop new ML algorithms (Steinhardt, Koh, and Liang, 2017; Gregory, 2021; Koh, Steinhardt and

Liang, 2022). Thus, this practice may be used to poison an entire database as it spreads like a virus throughout the social media network. At the center of this debate, AI/ML technologies are increasingly weaponized in support of adversaries' agendas and national interests.

CogWar is a reality in the 21st Century NATO operational environment. Information, as part of CogWar, is disseminated via an insidious and invisible digital network whose fingerprints are difficult to detect within the deeply embedded AI digital network. Advances in natural language, AI/ML algorithms, and the intersection of emerging scientific advances in neuroscience, genomics, quantum computing, social media platforms, and gaming will make this even more challenging in the future. The trend to enhance independent thinking via embedding advanced AI/ML algorithms in Robotics, drones, Brain-machine interfaces, etc., and developing systems with human-like logic and reasoning capabilities presents challenges for future decision makers (Aberman, 2017; Arkin, 1992; 2007; Chandra, 2017; Cole and Singer, 2020; Cummings 2007, 2010; Masakowski, 2020). These advanced Robotics, drones, and human Brain-modeled machines, etc., will evolve as colleagues, collaborators and partners designed with independent decision-making capabilities (Aberman, 2017; Arkin, 2007; Cummings, 2007; 2017; Ishiguro, 2021; Wallach and Allen, 2009; Masakowski, 2020, 2022). Thus, there is a need to imagine a future replete with advanced technologies that will outstrip current computing limitations and envision a future where autonomous AI/ML agents and machines will complement, augment, and at times, eliminate the human-in-or-on-the loop in the OODA-like decision environment.

7.2 SOCIAL MEDIA AND CYBER NETWORKS

Social media is a powerful technological enabler of CogWar on all levels, from enabling the shaping of strategic narratives and influencing mass consciousness, to tactical deception on the ground. Examples of common tactics include the use of fake and stolen accounts to infiltrate and influence domestic conversations, micro-targeting of individuals and exclusive audiences, and the distribution of false and misleading content and coordinated inauthentic behavior to amplify or suppress selected narratives or material.

As societies become increasingly reliant on computer networks and digital services, vulnerabilities for CogWar attacks increase. With the advent of 5G networks and the Internet of Things (IoT), the physical and the digital worlds merge, and the possibilities for data exploitation and manipulation grow. Attacks in the cyber domain may provide adversaries with valuable information that can be (mis)used to create cognitive affects ranging from discrediting countries, organizations, or key personnel to reducing trust in democratic institutions or computer systems (Pappalardo, 2022).

The NATO Tech Trends report (NATO, 2022) highlights the potential impact of emerging, disruptive technologies that will transform the future battlespace. AI/ML, drones, robots, and BMIs will become the military defence arsenal of the future (Giordano, Kulkarni, and Farwell, 2014; Masakowski, 2020). Advances in super-intelligent AI/ML technologies will provide a new means of collaboration and decision making among human-machine teams (Dobbyn and Stuart, 2003; Dutt and TaheriNejad, 2016; Ishiguro, 2021, Wallach and Allen, 2009; Forrest, 2015; Lin, Bekey and Abney, 2017; Masakowski, Smythe and Creely, 2014; Masakowski, 2020; 2022). Autonomous AI systems will relate to BMI as part of the new command and control network (Cole and Singer, 2020; Masakowski, 2020, 2022).

These technologies will include intelligent, integrated, and resilient artificial intelligence, analytics and decision capabilities across the technological spectrum as follows:

- **Autonomous Systems:** Artificial intelligence-enabled autonomous systems capable of some level of autonomous decision making. Such autonomous systems may be robotic, platform-based or (digital) agent-based.

- **Humanistic Intelligence:** The seamless integration of psycho-social-techno-systems supporting enhanced human-machine teaming and synergistic behaviors.
- **Knowledge Analytics:** Advanced analytical methods (including AI) exploring large data sets and advanced mathematics to provide insights, knowledge, and advice hitherto impractical.

Interconnected: Exploitation of the network (or mesh) of overlapping real and virtual domains, including sensors, organizations, institutions, individuals, autonomous agents, and processes.

- **Trusted Communications:** The use of technologies such as distributed ledger technologies (e.g., blockchain), Quantum Key Distribution (QKD), post-quantum cryptography and AI cyber-agents to ensure trusted interactions and information exchange.
- **Synergistic Systems:** The development of mixed (physical or virtual) complex systems-of systems allowing for the creation of novel ecosystems (e.g., smart cities).

Distributed: Decentralized and ubiquitous large-scale sensing, storage, computation, decision making, research and development.

- **Edge Computing:** Embedding of storage, computation and analytics/AI into agents and objects close to information sources.
- **Ubiquitous Sensing:** Embedding of low (or lower cost) sensors to create large sensor networks across the human-physical-information domains.
- **Decentralized Production:** Exploitation of AI-assisted design, novel materials, and (mixed material) 3D/4D printing technologies, to support just-in-time local digital manufacturing and production.
- **Democratized S&T:** Reducing costs of design and production, increasing computational capabilities and the broad availability of S&T information will increase innovation and the generation of novel science.

Digital: Blending of the human, physical and information domains to create new physiological, psychological, social, and cultural realities.

- **Digital Twin:** A digital simulacrum of physical, biological or information entities digitally linked (often in near real-time) to the original, supporting predictive analytics, experimentation, and assessment.
- **Synthetic Realities:** The creation of new perceived cognitive or physical realities based on the integration of psycho-socio-technical systems. Such realities may be augmented, virtual, social, or cultural in nature.

The NATO S&T Trend Report (2020) considers the intersection of multidisciplinary scientific areas of research associated with security challenges in the future CogWar operational environment as illustrated in the House Model (Chapter 2, Figure 2-1). Thus, the HFM-ET-356 team contends that S&T investment meet the demands of the future battlespace environment and include research on the following topics.

Intelligent and Distributed Autonomous AI/ML Systems, networks and Agents aimed at enhancing human capabilities also serve as a force multiplier. The development of AI-enabled Autonomous systems and Intelligent Agent networks will facilitate more sophisticated and effective decision making, support complex human-machine teaming, and expand capabilities in the cyber defence networks (Porat, Gilad, et al. 2012; Lin, Bekey and Abney, 2017; Shim and Arkin, 2012). Brain-Machine Interfaces (BMI) that may be used by warfighters as part of direct communication with command and control centers may provide enhanced Situational Awareness (SA) but may also present a vulnerability that must be defended (Giordano, Kulkarni and Farwell, 2014).

AI-enabled Autonomous systems and intelligent agents will facilitate rapid data analysis and provide strategic advisory support for operational and tactical mission planning, as well as support the OODA-Loop (Observe-Orient-Decide-Act). This enhanced intelligent agent network will accelerate the speed of the decision-making cycle and require new methods of symbiotic human-machine teaming and interactions. The evolution of ML algorithms will continue to enhance SA, with faster and more accurate sensemaking strategies and facilitate the operational effectiveness across a wide spectrum of operational domains (i.e., land, air, sea, cyber, and space.)

The interconnectedness of AI/ML digital networks will afford the development of agile and adaptive de-centralized Command and Control networks that will empower and enable operators to maintain greater SA in the battlespace. However, these AI/ML networks and human brain-machine interfaces will be targeted and subject to disinformation campaigns, cyber intrusion, and/or physical attacks. The invasive nature of cognitive attacks could be initiated prior to conflict and aim to disrupt information flow, and/or strike indirectly at personnel, logistics, information, financial, economic, medical, or other critical elements of military operational and strategic networks. Thus, CogWar presents challenges as adversaries exploit advances in AI/ML technologies and use AI/ML digital networks as a vehicle for disseminating mis-and disinformation campaigns to spread their influence aligned with their agenda (Orinx, Struye de Swielande, 2021). Consequently, CogWar mandates the need to develop defence systems that will ensure the cognitive security of the AI/ML network, as well as defend against social engineering attempts and the intrusion of systems on human perceptions, cognitive processes, and decision making.

7.3 COGNITIVE SECURITY AND SECURING THE FUTURE

Cognitive Security (COGSEC) will be required to defend the security and reliability of information that is essential for maintaining trust with our Allied Partners. Malicious attacks across social media platforms and the intrusion of poisoned data sets being used to train ML algorithms highlights the need to develop security measures and policies regarding the source of data being used to develop AI/ML digital networks. The issue of trust in data and the resilience of the digital networks are critical for ensuring that we are sharing information that is valid, reliable, and trustworthy as that is the foundation for mission planning and decision making.

This is especially critical for the development of trustworthy AI/ML algorithms and trustworthy AI networks. According to the literature, trustworthy Artificial Intelligence networks, must have the following set of characteristics:

- **Validity:** To guarantee that an AI-based system will do only and all of what it is intended to do.
- **Security:** To ensure robustness and resilience within adversarial conditions.
- **Explainability:** Provide understandable and context relevant justifications and explanations.
- **Responsibility:** Compliant with ethical, legal, and regulatory frameworks.

For the warfighter, such advances will help to shape SA and influence decision making. For the adversary, these advances will serve as a force multiplier that may be weaponized to their strategic advantage. China and Russia view emerging technologies as opportunities to exploit dual-use technologies to their strategic advantage and develop military defence capabilities that will ensure technological superiority and global supremacy across all domains, including space and satellite defence (Orinx, Struye de Swielande, 2021).

Recently, China expressed their intent to destroy Elon Musk's *Starlink* satellites as they perceived it as a threat to their national security (Turner, 2022). This type of attack in space represents a new element of warfare! Satellites provide surveillance capabilities for managing networks of military defence systems on a global scale. "Hard kill" weapons refer to the ability to physically strike and attack a target; "Soft Kill" weapons refer to the

ability to jam systems and satellites and laser weapons (Turner, 2022). The point is that this is just the beginning as satellite capabilities evolve and defence systems are required to prevent intrusion whether on the Internet and/or in Deep Space. Such attacks on satellites in space would have grave cascading consequences across the military, nations, and the global economy. We can no longer focus just on the traditional domains, land, air, sea, cyber but must include space defence. Indeed, we must also consider the impact of CogWar on the human domain; namely, think of ways to defend cognitive processes and decision making at all levels, including mass consciousness. We anticipate that this trend will become a pattern of defence in the future.

Therefore, as the need for increased security forces continues to emerge, the focus on advances in AI, computing power and cyber technologies is viewed as a means of enhancing our military readiness and force capabilities. Intelligence Preparation of the Battlespace (IPB) is the primary step for framing and preparing an effective mission plan. Autonomous, unmanned systems provide military leaders with SA across the battlespace and are an essential component for mission planning and operational success. CogWar requires the development of defensive technologies if we are to successfully defend NATO and Allied Partners' freedoms.

7.4 DEFENDING AGAINST COGNITIVE WARFARE

Nations must develop countermeasures to ensure operational readiness and defend their military strategic and operational plans from adversaries who would undermine their military operations on a global scale. The question is, how do we defend against CogWar? We must anticipate the impact of emerging technologies and that of the intersection of scientific areas to be effective in our defence strategy against CogWar. This CogWar report highlights various topics in the S&T roadmap chapter that reflect a strategy for the development of a defensive arsenal of advanced technologies such as AI/ML, BMIs, et al. technologies to defend against CogWar. Nations must consider the defence against CogWar as a national and global security imperative.

A cognitive attack may be launched to target an individual or to shape mass consciousness and justify a nation's military strategic objectives. Today, we are witnessing the influence and impact of CogWar in the Russia/Ukraine invasion. Russia is reshaping the geopolitical environment by its attack on Ukraine and provoking responses via its information network used to justify their military agenda. They are indoctrinating their youth with their version of the true enemy (New York Times, 2022). The influence of CogWar is evidenced by the level of civil unrest, political upheaval, and societal division based on perceptions and beliefs associated with manipulated information in the social media environment. This is a powerful tool for weaponizing information and inciting individuals to act based on misinformation that aligns with the adversary's agenda. This trend is dangerous and makes us all potential victims as adversaries continue to manipulate human perceptions and decisions. The threat of CogWar is not to be taken lightly as technological superiority is the enabler for adversaries to achieve military superiority and global supremacy. CogWar is a weapon in the adversary's toolbox used to achieve their objectives, shift our attention, reshape human understanding of events, trigger civil unrest, undermine democracies, and reshape the geopolitical and economic environment to their nation's advantage. Russia and China have made great strides in moving toward their strategic objectives by controlling their nation's messaging to their people, weaponizing information to global competitors, and leveraging strategic capabilities by controlling information dissemination on a global scale.

7.5 COUNTERING COGNITIVE WARFARE

NATO and its Allied Partners, Partners for Peace (PfP) nations, et al. must develop a defence strategy against CogWar. Nations need to develop Cognitive Security programs to defend AI/ML digital networks from adversarial intrusion, manipulation, misinformation/disinformation campaigns across all domains. The time is

now to develop defensive networks and systems to protect individual data and national data across all AI/ML digital networks. The manipulation of information and data associated across the AI/ML network may be weaponized to destroy a nation's economy, undermine governments and threaten national, global security, as well as fracture democratic societies across the globe.

NATO and its Allied partners must develop guidelines, rules-of-the-road, and recommendations for ensuring the security of data bases used in military operations. Nations must ensure that AI/ML networks are reliable, resilient, trustworthy, and secure by embedding forensic threat detection capabilities and trust analytics in their system designs to ensure the security of future networks. Adversarial data poisoning of AI/ML algorithms is emerging as a major threat to military defence (Dickson, 2021; Waltzman, 2017). Indeed, Ullrich, Dean of the SANS Technology Institute has stated in his RSA Keynote address: "One of the most basic threats when it comes to Machine Learning is one of the attackers being able to influence the samples that we are using to train our models..." (Gregory, 2021; Ullrich, 2021). Nations need to develop guidelines, policies, source certification processes and forensic tools to defend against these intrusions and defend against future attacks (Stokes, England, and Kane, 2021; Steinhardt, Koh, and Liang, 2017, 2022; Koh, Steinhardt and Liang, 2021).

Education must also play a pivotal role in the development of future critical thinkers. Children should be taught early in school how to recognize *fake* information on social media platforms. Children must also be taught critical thinking skills, including how to challenge assumptions, apply logic and reasoning to their thinking and develop the skills to defend against manipulation of their perceptions and reasoning. Nations must address the vulnerabilities of AI/ML networks and systems as well as defend against data breaches, poisoning of training datasets and the unrestricted exploitation of social media platforms, news networks that are used to shape public perceptions aligned with information that threatens to undermine NATO's democratic commitment.

NATO must develop the guidance to help nations develop their strategic plans for defence against CogWar. The NATO HFM-ET-356 Science and Technology roadmap is a first step toward establishing the policies and practices, as well as the technologies, which will need to be developed in the defence against CogWar.

7.6 ETHICAL IMPLICATIONS OF TECHNOLOGICAL ADVANCES

NATO needs to develop leaders who will understand how to ethically deploy advanced technologies in CogWar. It is important for military personnel and leaders to understand the ethical and legal implications of employing advanced technologies in CogWar. Given the way that adversaries are using AI/ML networks and social media platforms to engage with the population (civilian and military); there is a need to educate military personnel on the ethical issues related to CogWar attacks. NATO leaders may see these new technologies used against them on the battlefield or must make decisions on how to use new technologies within the law of armed conflict. Some of the legal and ethical questions raised by these new technologies can be addressed by the NATO Alliance in advance, but there will be unanticipated applications in contested environments that cause ethical challenges for the leaders in the immediate moment. NATO leaders must be prepared to make right decisions that are ethical, effective, and efficient in the chaos of combat.

Future technological advances could fundamentally change NATO Command and Control military operations. Even if NATO determines it will not employ a new technology, potential adversaries may choose to develop and employ the capability. Consequently, we must recognize and be prepared to address new, asymmetric threats. NATO has a duty to preserve peace and security as well as ensure the safety of its personnel.

For example, AI/ML systems, Robots, etc., will be the *digital partner* of future leaders by providing a range of options and decisions based on its ability to manage vast amounts of data from distributed networks. Today, the human maintains the principal authority for decision making. However, the level of responsibility for military operations will be shared with AI-enabled systems, Robots, and networks. Robots will be partners, collaborators, and decision makers in future military operations. Regardless of the technology, i.e., Robot, drone, weaponized AUV, or an AI-enabled weapon system, the decision to implement these technologies raises grave ethical consequences for the military leader and for society itself (Department of Defense, 2012; Masakowski, 2022). Advances in our understanding of the brain and biological modeling will contribute to future advances in AI designs and autonomous unmanned systems. However, NATO must prepare its leaders to operate in the future CogWar environment that will be replete with advanced technologies that are vulnerable to adversarial manipulation. Technology will continue to develop in both complexity and capability, however, decisions to employ such technologies ethically must be retained by the human decision-maker. We must defend against the misuse of advanced technologies and at the same time, prepare to defend against adversaries who might use such advances against us in CogWar.

7.7 THE ROLE OF TECHNOLOGICAL COMPETENCY

NATO must provide military personnel with the education, training, and experience that will prepare them for the defence against CogWar. There is a need to develop a military person's technological competence for understanding the capabilities that advanced technologies provide to both the warfighter and the adversary. To this end, S&T investment needs to be focused on developing training tools that build Social Media expertise, provide wargaming opportunities for military to develop understanding of the technological capabilities and shortfalls of each technology, as well as provide field experience so that the military learns to employ these technologies ethically and effectively.

NATO personnel must acquire an understanding of CogWar and the role that technologies will play in shaping the operational environment. Today, it has become more complicated with the intrusion of misinformation embedded in social media platforms. Information warfare has taken on a new level of meaning and one that is difficult to counter amid the complexity of integrated AI/ML digital networks. Therefore, military personnel must achieve technological competency and understand the capabilities and risks associated with the deployment of advanced technologies such as AI/ML networks, etc., They must also understand the ethical, moral, and legal consequences for integrating advanced technologies as part of their mission plans. Military personnel must be made aware of the gaps and vulnerabilities of these AI/ML networks that may be targeted by adversaries.

Military leaders must be made aware of the ethical consequences associated with extensive AI/ML networks that support social media platforms, AI facial recognition surveillance systems, AI Situational Awareness systems, autonomous weaponized systems, autonomous unmanned systems, AI Robotics, etc., that present significant challenges in the defence against CogWar. These technologies impact civilian, military and society itself and thus play a critical role in how we defend against them in CogWar (Loten and Simons, 2017). Military personnel must understand how adversaries might use these technologies to their advantage if they are going to be able to counter these attacks and mitigate against their influence. Education, training, and experience will prove to be pivotal elements in NATO's CogWar defence strategy for the future.

7.8 CONCLUSION AND THE FUTURE SECURITY ENVIRONMENT

CogWar is aimed at weaponizing information to support the adversary's agenda and will continue to capitalize on technological innovations that support their cause. It is NATO's duty therefore to think defensively in

anticipation of such events. NATO must ensure the safety and security of its allied partner nations and its respective military personnel by developing an S&T defence strategy that will ensure the development of tools, techniques, and technologies in NATO's defence against CogWar.

We anticipate that the emergence and integration of scientific discoveries will continue to provide adversaries with opportunities for the development of new weapons of war. However, we must also take the opportunity to develop defensive measures that will counter the adversary's advance and potential success in CogWar. NATO must be prepared to defend against CogWar across all domains.

The future security environment will continue to challenge NATO with its uncertainty and complexity. NATO and its adversaries will continue to exploit advances and innovation in technologies in the conduct of CogWar. The rapid rate of technological innovation adds to the level of importance in advancing S&T research for defensive technologies.

NATO must provide the guidance for its partner nations and the HFM-ET-356 S&T roadmap will serve as a compass to guide and direct nations to invest in S&T research that will facilitate the development of critical tools and technologies. The Science and Technology roadmap (Chapter 14) will provide the coordinates for mapping out a plan for designing the future defence against CogWar.

7.9 REFERENCES

- Aberman, J. (27 February 2017). Artificial Intelligence Will Change America. Here's How. The Washington Post (Online) Retrieved from https://www.washingtonpost.com/news/capitalbusiness/wp/2017/02/27/artificialintelligence-will-change-america-hereshow/?utm_term=.3e325159efd9
- Arkin, R.C. (1992). Modeling Neural Function at the Schema Level: Implications and Results for Robotic Control. In R.D. Beer, R.E. Ritzmann and T. McKenna (Eds.), Biological neural networks in invertebrate neuroethology and robotics (pp. 383-410). Cambridge, MA: Academic Press.
- Arkin, R.C. (2007). Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture. (technical report GIT-GVU-07-11). Atlanta: Georgia Tech GVU Center. Retrieved from <http://www.cc.gatech.edu/ai/robotlab/onlinepublications/formalizationv35.pdf>
- Bellingcat Investigation Team (19 June 2019). Identifying the Separatists Linked to the Downing of MH17. <https://www.bellingcat.com/news/uk-and-europe/2019/06/19/identifying-the-separatists-linked-to-the-downing-of-mh17/>
- Chandra, R. (2017). An Affective Computational Model for Machine Consciousness. Retrieved from <http://arxiv.org/abs/1701.00349>
- Claverie, B., and du Cluzel, F. (2022). Cognitive Warfare: The Advent of the Concept of "Cognitics" in the Field of Warfare. In Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. (Eds.). Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 2021. NATO STO, Neuilly-sur-Seine, France. Retrieved August 2022 from: <https://hal.archives-ouvertes.fr/hal-03635889/document>

Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. (Eds.) (2022). Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 2021. NATO STO, Neuilly-sur-Seine, France. NATO Collaboration Support Office, pp.8, 1-6, 2022, 978-92-837-2392-9. hal-03635930. Retrieved 10 August 2022 from: <https://www.innovationhub-act.org/sites/default/files/2022-03/Cognitive%20Warfare%20Symposium%20-%20ENSC%20-%20March%202022%20Publication.pdf>

Clayton, J. (13 April 2022). How Facial Recognition is Identifying the Dead in Ukraine. BBC News. <https://www.bbc.com/news/technology-61055319>

Cole, A., and Singer, P.W. (2020). Burn-In. A Novel of the Real Robotic Revolution. Mariner Books, Houghton-Mifflin Harcourt. Boston. New York.

Cummings, M.L., and Guerlain, S. (2007). Developing Operator Capacity Estimates for Supervisory Control of Autonomous Vehicles. Human Factors: The Journal of the Human Factors and Ergonomics Society, 49(1), 1-15. doi:10.1518/001872007779598109.

Cummings, M.L., Clare, A., and Hart, C. (2010). The Role of Human-Automation Consensus in Multiple Unmanned Vehicle Scheduling. Human Factors: The Journal of Human Factors and Ergonomics Society, 52(1), 17-27. doi:10.1177/0018720810368674.

Department of Defense. (2012). Autonomy in Weapon Systems (DoD directive Number 3000.09). Washington, DC: Department of Defense.

Dickson, B. (2021). Adversarial Machine Learning: The Underrated Threat of Data Poisoning. The Machine: Making Sense of AI. Retrieved August 2022 from: <https://venturebeat.com/ai/adversarial-machine-learning-underrated-threat-data-poisoning/>

Dobbyn, C., and Stuart, S. (2003). The Self as an Embedded Agent. Minds and Machines, 13(2), 187-201. doi:1022997315561

Du Cluzel, F. (2021). Cognitive Warfare, a Battle for the Brain. In: Applying Neuroscience to Performance: From Rehabilitation to Human Cognitive STO Human Factors and Medicine (HFM) Panel Symposium 11 – 12 October 2021, Rome, Italy. NATO STO Meeting Proceedings. STO-MP-HFM-334-KN3. NATO STO, Neuilly-sur-Seine, France.

Dutt, N., and TaheriNejad, N. (2016). Self-Awareness in Cyber-Physical Systems. Paper presented at the 29th International Conference on VLSI Design and 15th International Conference on Embedded Systems (VLSID), Kolkata, India. Retrieved <http://ieeexplore.ieee.org/document/7434906/>

Forrest, C. (2015). Chinese Factory Replaces 90% of Humans with Robots, Production Soars. Retrieved from: <https://www.techrepublic.com/article/chinese-factory-replaces-90-ofhumans-with-robots-production-soars/>

Giordano, J., Kulkarni, A., and Farwell, J. (2014). Deliver Us from Evil? The Temptation, Realities, and Neuroethico-Legal Issues of Employing Assessment Neuro-Technologies in Public Safety Initiatives. Theoretical Medicine and Bioethics, 35(1), 73-89. doi: 10.1007/s11017-014-9278-4.

Gregory, J. (2021). Data Poisoning: The Next Big Threat. Security Intelligence. Retrieved August 2022 from: <https://securityintelligence.com/articles/data-poisoning-big-threat/>

Guyader, H. (2021). Cognitive Domain: A Sixth Domain of Operations. In Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. (Eds.). *Cognitive Warfare: The Future of Cognitive Dominance*. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 2021. NATO STO, Neuilly-sur-Seine, France. Retrieved August 10, 2022. <https://hal.archives-ouvertes.fr/hal-03635898/document>

Hao, K. (14 August 2020). A College Kid's Fake, AI-Generated Blog Fooled Tens of Thousands. This is How He Made it. MIT Technology Review. <https://www.technologyreview.com/2020/08/14/1006780/ai-gpt-3-fake-blog-reached-top-of-hacker-news/>

Ishiguro, K. (2021). *Klara and the Sun*. Knopf Publishers, New York, New York.

Koh, P.W., Steinhardt, J. and Liang, P. (2021). Stronger Data Poisoning Attacks Break Data Sanitization. defenses. *Machine Learning*. 111(3): 1-47. December 2021, vs.2. Retrieved August 2022 from: <https://arxiv.org/abs/1811.00741>

Lin, P., Bekey, G., and Abney, K. (2008). Autonomous Military Robotics: Risk, Ethics, and Design. Retrieved from <http://www.dtic.mil/docs/citations/ADA534697>

Lonas, L. (2022). Ukraine Has Used Facial Recognition Tech to Notify Russian Families of Dead Soldiers. The Hill via Nexstar Media Wire. April 18, 2022. Retrieved August 2022 from: <https://www.wavy.com/russia-ukraine-invasion/ukraine-has-used-facial-recognition-tech-to-notify-russian-families-of-dead-soldiers-report/>

Loten, A., and Simons, J. (2017, Jan 04). Leadership Evolves Amid Tech Changes – Management Styles Shift to Embrace Shorter, More Frequent Data-Fueled Development Cycles. Wall Street Journal. Retrieved from <https://search.proquest.com/docview/1855011133?accountid=322>

Masakowski, Y.R. (2020). *Artificial Intelligence and Global Security: Future Trends, Threats, and Considerations*. Emerald Press Publishing, UK.

Masakowski, Y.R. (2022). Leader Development in the 21st Century. In NATO HFM RTG 286, Leader Development for NATO Multinational Military Operations. Chapter 6. August 2022.

Masakowski, Y.R., Smythe, J.S., and Creely, T.E. (2016). The Impact of Ambient Intelligence Technologies on Individuals, Society, and Warfare. *Northern Plains Ethics Journal*, 4(1), 1-11. Retrieved from <http://www.northernplainsethicsjournal.com/NPEJv4n1/The%20Impact%20of%20Ambient%20Intelligence%20Technologies%20on%20Individuals.pdf>

NATO Science & Technology Trends 2020 – 2040. Exploring the S&T Edge. NATO Science & Technology Organization, 2020.

Orinx, K., Struye de Swielande, T. (2021). China and Cognitive Warfare: Why Is the West Losing? Retrieved August 10, 2022, from: <https://hal.archives-ouvertes.fr/hal-03635930/document>

Pappalardo, D. (2022). Win the War Before the War? The French Perspective on Cognitive Warfare. *War on the Rocks*, August 1, 2022. Retrieved August 2022 from: <https://warontherocks.com/2022/08/win-the-war-before-the-war-a-french-perspective-on-cognitive-warfare/>

Porat, T., Oron-Gilad, T., Rottem-Hovev, M., and Silbiger, J. (2016). Supervising and Controlling Unmanned Systems: A Multi-Phase Study with Subject Matter Experts. *Frontiers in Psychology*, 7, 568. doi:10.3389/fpsyg.2016.00568.

Shim, J., and Arkin, R.C. (2012). Biologically Inspired Deceptive Behavior for a Robot. International Conference on Simulation of Adaptive Behavior. From Animals to Animals 12, pp. 401-411.

Steinhardt, J., Koh, P.W., and Liang, P. (2017). Certified Defenses for Data Poisoning Attacks. In NIPS '17 Proceedings of the 31st International Conference on Neural Information Processing Systems, pp. 3520-3532. Retrieved August 2022 from: <https://dl.acm.org/doi/10.5555/3294996.3295110>

Stokes, J., England, P., and Kane, K. (2021). Preventing Machine Learning Poisoning Using Authentication and Provenance.

Troianovski, A. (16 July 2022). Putin Aims to Shape a New Generation of Supporters, Through Schools. New York Times. Retrieved from <https://www.nytimes.com/2022/07/16/world/europe/russia-putin-schools-propaganda-indoctrination.html>

Turner, B. (2022). Chinese Scientists Call for Plan to Destroy Elon Musk's Starlink. Live Science. Retrieved 31 May 2022. <https://www.livescience.com/china-plans-ways-destroy-starlink>

Ullrich, J. (2021). The Five Most Dangerous New Attack Techniques. Presentation at RSA Conference. Retrieved 19 August 2022, from: <https://www.rsaconference.com/Library/presentation/USA/2021/the-five-most-dangerous-new-attack-techniques>

Uppal, R. (31 December 2022). NATO Thrust on AI, Data, Space and Hypersonics as Strategic Disruptor. Future Military Operations. International Defense, Security and Technology (CA, USA). Retrieved from: <https://idstch.com/geopolitics/nato-thrust-on-ai-data-space-and-hypersonics-as-strategic-disruptors-for-future-military-operations/>

Wallach, W., and Allen, C. (2009). Moral Machines: Teaching Robots Right from Wrong. New York: Oxford University Press.

Waltzman, R. (2017). The Weaponization of Information: The Need for Cognitive Security. Retrieved August 2022 from: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

Chapter 8 – SITUATIONAL AWARENESS, SENSEMAKING AND FUTURE NATO MULTINATIONAL OPERATIONS

Benjamin J. Knox

Norwegian Armed Forces Cyber Defence
NORWAY

Yvonne R. Masakowski

US Naval War College
UNITED STATES

8.1 INTRODUCTION

“Victorious warriors win first and then go to war, while defeated warriors got to war first and then seek to win.”

Sun Tzu, “The Art of War,” 5th century China

Success for Sun Tzu meant determining the path of success before you go to war. This meant planning prior to any engagement and applying a “know your enemy” philosophy to potentially avoid war. Sun Tzu’s goal was to “subdue the enemy without fighting” and to achieve this, entailed sensemaking and SA to understand your enemies’ perspectives, capabilities, and strategic objectives. The ‘Art of War’ codifies the philosophies of war adopted by Sun Tzu and reflect the importance of developing strategy and tactics prior to conflict engagement. The concept of winning the battle but losing the war can be understood from this philosophy wherein we may realize a pyrrhic victory, but at a punishing cost that leaves us with a devastating loss of life, wasted resources or high financial costs related to the battle. Leaders must learn to achieve competency in sensemaking and SA if they are to forge effective mission plans and achieve success without incurring severe losses. The importance of this leader competency cannot be overstated as it serves as the foundation for all mission planning. Leaders must evaluate the goodness of information across all domains and in that process, recognize truth, identify trustworthy information, evaluate its value, and assess the reliability information sources, as these elements are the building blocks for mission success and victory in war.

This chapter focuses on the “Sensemaking and Situational Awareness” aspect of the House Model. These processes have considerable implications for how NATO confronts future military operational dimensions, such as the cognitive. Given the dynamic, rapidly evolving nature of warfare, there is a need to consider how information is received, perceived, processed, and transformed from sensemaking of data input to transforming it into SA. Military leaders are presented with a wide array of information from graphical displays, databases, HUMINT, SIGINT, OSINT to name but a few. These information sources encompass a wide array of elements, including human input, technological input, and AI programs. To this end, this chapter will provide a means of understanding how decision makers make sense of data and information from such a complex and vast network.

For this discussion, let us review the House Model and examine its relationship to the topics of sensemaking and SA.

As illustrated in Figure 8-1, the horizontal bars are an examination of the factors that enable and/or block attempts to make sense of ambiguous, uncertain situations.

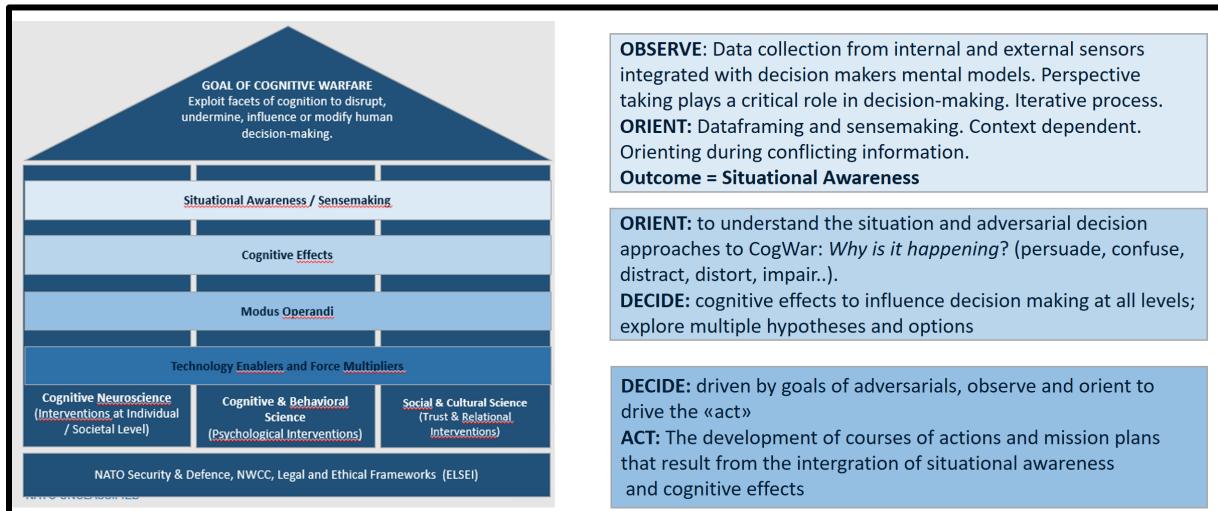


Figure 8-1: The House Model: Sensemaking and Situational Awareness.

8.2 SITUATIONAL AWARENESS: A HUMAN ENDEAVOR

Situational Awareness is a conceptualization of the current situation (Geissler, 2019). It requires experts use a holistic process involving situation recognition and pattern matching to memory structures to make accurate, and when necessary, rapid decisions. In a NATO Defence context, SA is supported by technology enablers that can sense, aggregate and process data at great speed to help build a recognized picture of a war fighting domain.

However, irrespective of the technology resources available, SA remains a human endeavor. It is a cognitive skill to interpret and communicate information in an abstract way, with insight, contextual awareness, and creativity. At any hierarchical level, or at any time point or phase in the awareness building process or perceiving and comprehending, a situation can be affected in a way that can influence decision making. This may be a consequence of own [avoidable] self-inflicted actions, such as poor procedures, behavioral biases, poor memory structures, or novice level pattern matching. Or by actions of an adversary that aim to induce, infer, inflict, or impose an awareness or way to behave upon us. This may occur either directly or indirectly, but it will almost always include the manipulation of ‘input’ data. What or whoever the source is that [mis]shapes our understanding to influence decision making, leading to [un]favorable outcomes, it is the input data going into the brain that is the subject of interest in CogWar. If the input data can be affected, then the effect occurs on the output.

SA requires metacognition for accuracy. Meaning that our level of metacognition can influence SA. The fact that metacognition is a skill, means when it is lacking, we can be targeted and exploited. It can also be trained, and developed to adjust maladaptive thinking behaviors, such as overconfidence in own abilities. The importance of *getting ahead* emerges here as we look to modes of cognitive security to counter CogWar and ensure we are aware of, and resilient to, adversarial metacognitive training that aims to, for example, covertly elicit impulsive and addictive behaviors.

For SA to lead to a level of understanding that can enable better decision making, it requires trusted data input, evaluation of meaningful information, and integration with new knowledge and experience. To achieve this level of understanding in evolving non-linear events, that may or may not have been deliberately interfered with, is reliant on sensemaking ability.

Sensemaking informs and is a prerequisite to decision making. In contrast to SA, sensemaking concerns the process of achieving outcomes such as knowledge of the current data elements, inferences drawn from these data, or predictions made from these inferences. Sensemaking is about the strategies and the barriers encountered that constitute an explanation of a state. Sensemaking requires continuous effort and motivation to understand connections among people, places, and events (the system of systems) to anticipate their trajectories and act effectively.

8.3 COGNITIVE EFFECTS: SCIENCE AND TECHNOLOGY PILLARS

This horizontal bar expresses the need for S&T to contribute to understanding the *Cognitive Effects* an actor will attempt to have on a target audience (group or individual) to cause change. Linking fields of science is what can be transformative in protecting, defending against the cognitive effects of CogWar, as well as ethically and legitimately finding countermeasures.

The effects can be a doctrinal, such as distort, distract, degrade. They can also be more varied and experimental: menace, disorientate, unravel, encourage, nudge, confuse, reduce, doubt, remove. They can be short term (temporary) to include memory loss or gain, creating a state of confusion or clarity, shock or calm, outrage or passivity, lack of coordination or improved group coordination and perception. Effects can also be long term (permanent) such as altering declarative memory or inducing a general lack of, or improvement in, emotional stability. Or in the case of for example instigating a mass psychosis, lack of control over one's actions. Ultimately, the unifying purpose of a 'cognitive effect' is to (passively or actively /overtly or covertly / legally or illegally / invasively or non-invasively) change psychological processes through some form of augmentation or change in cognition that can affect emotion, attention, motivation, or sensory function.

S&T can begin to understand adversarial cognitive effects-based approaches by applying a holistic understanding of the operational environment to any research investigation. Looking at both physical and behavioral aspects of a system of systems in a conflict state and defining it by its associated Political, Military, Economic, Social, Information, Infrastructure (PMESII) elements. Additionally, S&T must consider implications when the operating environment is the mind, these elements can be challenged regarding how we consider effects as the system complexity of PMESII expands and opens opportunities for new ways of planning and delivering known and novel cognitive effects. Any enhancement, modifier or malignantly induced change can have side effects and unintended outcomes. This point is especially salient since it may not be scientifically possible to accurately predict the outcome of an effect due to the dynamic nature of the human nervous system, and isolated mind[s], as an operating environment.

Cognitive effects will need to be studied with 'own' center of gravity as a key component. Considering the mind as a source of strength and balance, we can analyze how it could become an adversarial goal or objective (Ends) and identify what actions/effects can be achieved (Ways), and what resources and requirements an adversary will need to perform the ways (Means), can potentially provide NATO with requisite knowledge to maintain freedom of action, physical strength, and the will to fight.

When we consider effects, and the case for research that contributes to cognitive security, such as building cognitive skills, there is a need to identify effective education and training techniques that focus effort on defending against an adversary who is not only targeting what we think, but also how we think. This means S&T has to focus on capabilities to monitor, evaluate and adapt own cognition and behaviors. These are essential to performance and maintaining clarity of mind when and the adversary is bent on exploiting the competition space between peace and war.

Side cognitive effects (real or perceived) and second order cognitive effects of for example augmentations, whether they be technological, biological, or neurological are serious risk factors that will need a great deal of S&T focus.

8.4 DECISION MAKING AND THE OODA LOOP IN COGNITIVE WARFARE

John Boyd is described as the fighter pilot who changed the art of war (Coram, 2002). When studying military history, Boyd found a common thread: none of the victorious commanders threw their forces head-to-head against enemy forces. Instead, they used deception, speed, fluidity of action, and strength against weakness. Leaders used tactics that disorientated and confused – tactics that, in Boyd's words, caused the enemy "to unravel before the fight."

John Boyd, US Air Force Colonel, was the architect behind the Observe-Orient-Decide-Act (OODA) Loop created during the Korean War in the mid-1950s. Boyd applied the concept of combat operations to the OODA process of decision making. The model accounted for the agility of decision making under conditions of uncertainty in a dynamic environment.

Boyd (1987, p. 18) suggested a similar conclusion in terms of shared orientations: Arrange the setting and circumstances so that leaders and subordinates alike are given the opportunity to continuously interact with the external world, and with each other, in order to more quickly make many-sided implicit cross-referencing projections, empathies, correlations, and rejections as well as create the similar images or impressions, hence a similar implicit orientation, needed to form an organic whole.

He accounted for the need to evaluate information as it unfolded and interacted with information in the environment. Initially, according to Boyd – the cycle was far too dangerous to be fully explained. "If someone truly understands how to create menace and uncertainty and mistrust, then how to exploit and magnify the presence of these disconcerting elements, the Loop can be vicious, a terrible destructive force, virtually unstoppable in causing panic and confusion," he said.

8.5 THE OODA LOOP DECISION MAKING CYCLE

The OODA Loop (Boyd, 1986; 1987; 1996; Coram, 2002; 2004), is a four-step approach to decision making that focuses on filtering data input (Figure 8-2), putting it in context, deciding while knowing that changes may be made when more data becomes available. For those unfamiliar with the OODA loop created by John Boyd (1996, p.3), there are four steps of the OODA loop:

- 1) **Observe** – Data collection phase from multiple sources, i.e., aggregation of information from all sources.
- 2) **Orient** – Filter, analyze, and enrich information, i.e., information is analyzed, evaluated, and prioritized.
- 3) **Decide** – Actionable insights enable best available response, i.e., choosing between options and courses of action.
- 4) **Act** – Execute decision, determine if action was correct i.e., testing hypothesis, executing your decision, and determining if your hypothesis was correct.

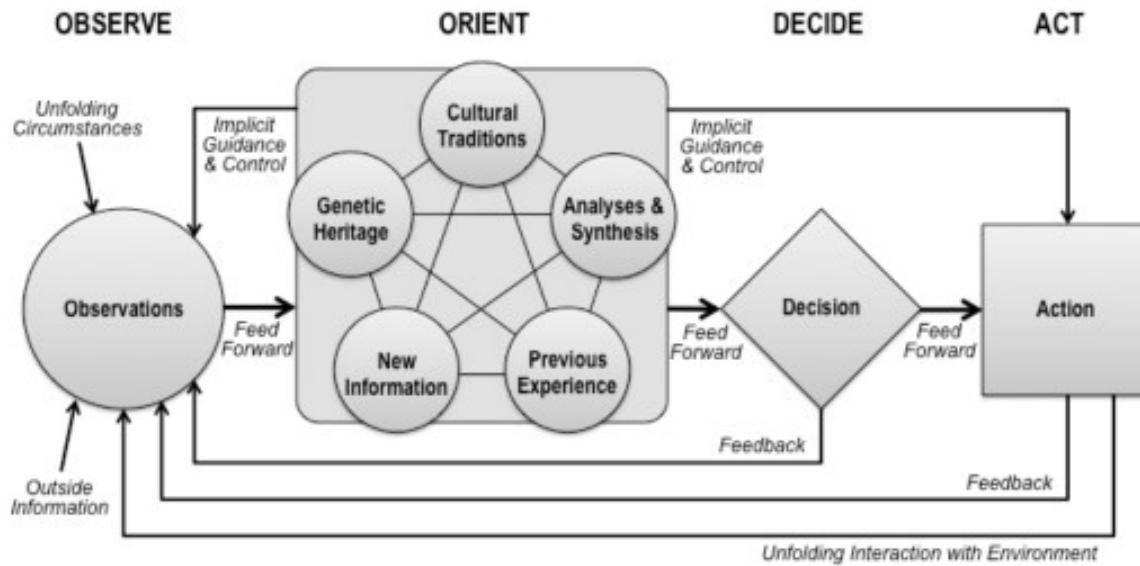


Figure 8-2: The OODA Loop Decision Cycle (John Boyd, 1986).

The OODA loop is a means for understanding the decision-making process. For the military, the OODA loop serves as a framework for decision making. The OODA loop allows decision-makers to adapt to changes as they gather information in real time. This approach to decision making affords them the ability to anticipate threats as it takes advantage of additional data as it is integrated into their mental model. It allows them to test different hypotheses, integrates updated data/information and helps them to select the optimal course of action.

The OODA loop is not a mission planning tool, and although speed is important, understanding it simply as a loop, where doing it faster than your adversary leads you to victory, is missing what Boyd had in mind. One key factor that is highly relevant to our thinking about CogWar is that understanding the OODA loop enables a commander to compress time – that is, the time between Observing a situation and taking an Action. As the commander compresses his own time, he causes time to be stretched out for his opponent, as he is forced to pause, to wonder, to question. Therefore, Boyd included the “Implicit Guidance and Control” from “Orientation” to both “Observation” and “Action” in his model.

For the OODA framework to enhance their decision-making capabilities military commanders need to process information, i.e., Sensemaking, if they are to ensure accurate SA for operational success. To this end, the S&T roadmap highlights the need to develop sensemaking tools, techniques and technologies that will support building SA for human decision-makers.

8.6 IMPLICATIONS FOR THE FUTURE SECURITY ENVIRONMENT

Today, auto designers have developed enhanced tools and technologies embedded in the auto’s interface design such that cars can now park themselves, provide early alerts to drivers of oncoming traffic, and alert the driver to icy road conditions. The vehicle now cognitively augments the human. Military personnel need tools for seeing Over-the-Horizon, as well tools to make sense of the socio-technical operating environment to increase levels and accuracy of SA. Technologies equipped with AI and adaptive ML algorithms have the potential to support sensemaking capabilities for enhanced SA in the future security environment.

Technologies are being designed to enhance medical diagnosis and surgical treatment that may also give rise to military applications in the battlegrounds of the future. Sensemaking and SA technologies merit further exploration and research. There is opportunity for discovery amid the intersection of capabilities provided by designers in the auto industry, medical technologies, and in Robotics and autonomous systems that may facilitate decision-support technologies for future military combat missions. These research topics may further provide opportunities for leveraging capabilities that will enhance the military decision maker's operational readiness. S&T will lead the way to develop tools that will enhance the military's ability to sense-make as a defence against future CogWar.

Orientation is not a new concept for the military. Within this context, military personnel attend to meaningful information in the operational environment and seek opportunities to take the decision advantage. S&T needs to develop technologies that will enhance human Orientation abilities and provide an intuitive understanding of dynamic changes within the operational environment. By so doing, we can potentially help our servicemen and women bypass parts of the OODA cycle, and Act on CogWar at Observation. Today's technology designers must consider the challenges presented in CogWar and provide tools to defend against an adversary that adapts fluidly to technological advances in the CogWar operational environment. Cognitive Superiority demands innovation, being adaptive and prescient if we are to 'get ahead' and take advantage of emergent technologies.

Advances in AI technologies (O'Flanagan, 2018; Masakowski, 2020, 2022a, 2022b) and the power of Quantum Computing will inform and facilitate sense-making and enhanced SA through the design and application of decision-support tools. Similarly, these same advances in emergent AI-enabled technologies will contribute to the complexity and impact of the CogWar environment. As great power competitors and adversaries weaponize AI enabled autonomous systems, the potential threat is elevated in the pursuit of strategic objectives.

It is therefore incumbent upon us to establish and maintain a clear awareness of these future challenges and potential threats. This requires we develop and operationalize the capabilities (tools, technologies, and techniques) to successfully anticipate and orientate us to such advances. Where we can leverage AI autonomous systems, with for example adaptive ML algorithms, to provide the decision advantage for the military commander; we must also explicitly and continuously consider the ethical implications and consequences for these technologies. As a whole-of-society challenge, negotiating and integrating these issues into mission planning must include lawyers, philosophers, ethicists, and society.

The evolution of autonomous unmanned systems has accelerated rapidly and with little time for consideration of the ethical consequences of their application in the military operational environment (Masakowski, 2019). As the introduction and application of AI and ML continues to evolve and transform the character of warfighting, systems with a capacity for self-awareness, and self-organization and self-explanation will be designed to make informed, rational decisions based on logic and reasoning capacities. The human role in sensemaking may well be out-looped and subject to the direction of these advanced agents and/or sentient robots. Indeed, such advancements combined with computational modeling have moved research in the direction of affective machine consciousness (Chandra, 2017; Aberman, 2017). Traditionally, humans do not remove progress but rather continue to explore, invent, and move forward as a society, continuously seeking ways to improve and integrate advances in technology aimed at improving the quality of our daily life and ensuring the security of society. Our adversaries are not no different, only they seek ways to modify advances in technology to their strategic and tactical advantage. We must, therefore, not shy from taking the perspective of the adversaries most dangerous course of action when we plan defence in CogWar. Adversaries will continue to challenge nations by attempting to create chaos, confusion, surprise, shock, and disorientation to keep their strategic opponent at a disadvantage in understanding the situation and impeding their ability to develop effective countermeasures. To this end, nations must strive to develop the tools and technologies to defend against such aspects of CogWar that target our capability to sense-make and build SA.

8.7 REFERENCES

- Aberman, J. (27 February 2017). Artificial Intelligence Will Change America. Here's How. The Washington Post (Online) Retrieved from https://www.washingtonpost.com/news/capital-business/wp/2017/02/27/artificial-intelligence-will-change-america-heres-how/?utm_term=.3e325159efd9
- Boyd, J.R. (1986). Patterns of Conflict. (Unpublished briefing). Retrieved from <http://dnipogo.org/john-r-boyd/>
- Boyd, J.R. (1987). Organic Design for Command and Control. (Unpublished briefing). Retrieved from <http://dnipogo.org/john-r-boyd/>
- Boyd, J.R. (1996). The Essence of Winning and Losing. (Unpublished briefing). Retrieved from <http://dnipogo.org/john-r-boyd/>
- Chandra, R. (2017). An Affective Computational Model for Machine Consciousness. Retrieved from <http://arxiv.org/abs/1701.00349>
- Coram, R. (2004). Boyd: The Fighter Pilot Who Changed the Art of War. Back Bay Books; Reprint Ed. May 10, 2004.
- Coram, R., (2002). Boyd: The Fighter Pilot Who Changed the Art of War. Little, Brown & Company, NY, U.S.
- Geissler, H. (2019). Bless the Fog of War. How Panopticon Will Lose the War in Metropolis. Thesis published by the US Naval War College, Newport, R.I.
- Masakowski, Y.R. (2019) Ethical Implications of Autonomous Systems and Artificial Intelligence Enabled Systems. Institute of Navigation Cognizant Autonomous Systems for Safety Critical Applications Conference. Miami, Fl. September 16 – 17, 2019.
- Masakowski, Y.R. (2020). Artificial Intelligence and Global Security: Future Trends, Threats and Considerations. Emerald Publishing. UK.
- Masakowski, Y.R. (2022a). Artificial Intelligence and Cognitive Warfare. Naval War College Foundation, Newport, RI. 23 February 2022.
- Masakowski, Y.R. (2022b). AI and Global Security: The Influence and Impact of Cognitive Warfare. Navy ROTC: The College of the Holy Cross. Worcester, MA. 01 March 2022.
- O'Flanagan, T.P. (2018). A Breach of Trust: The Impact of Artificial Intelligence on Society and Military Operations. Thesis published by the US Naval War College, Newport, RI. Retrieved August 2022 from: <https://apps.dtic.mil/sti/pdfs/AD1079769.pdf>
- Tzu, S. [496 BC] (1910). SunTzu on the Art of War. Trans. L. Giles. London: Luzac and Co. Retrieved 09 February 2023 from <https://archive.org/details/the-art-of-war-by-sun-tzu-trans.-by-lionel-giles-m.-a.-1910/page/n3/mode/2up>



Chapter 9 – HUMAN-MACHINE TEAMING TOWARDS A HOLISTIC UNDERSTANDING OF COGNITIVE WARFARE

Frank Flemisch

Communication, Information Processing and Ergonomics (FKIE)
GERMANY

9.1 INTRODUCTION

What can we learn from history about cognitive warfare and human-machine teaming? Despite the continuing necessity for physical warfare, there is an increasing tendency in the defence community to think warfare beyond the physical realm. An example is the cyber domain, e.g., as cyber warfare, or in combination with conventional warfare as hybrid warfare, or the cognitive domain, e.g., as Cognitive Warfare (CogWar). What looks revolutionary on the first glance has already a long history, but with AI and autonomous machine capabilities it also enters a new stage, which might have disruptive effects for any future defence operation.

Looking deeply back into history, Dalheim (2020) provided an historical perspective in the description of one of the earliest wooden weapons of war, the Schöningen wooden throwing spears that were excavated between 1994 and 1998 in an open-cast coal mine in the Helmstedt district of Germany (Figure 9-1). These throwing spears, dated between 380,000 and 400,000 years old, represent the oldest preserved hunting weapons of prehistoric Europe yet discovered. (Thieme, 1997; Dalheim, 2020). These spears are not only an early example of weapon technology, but also of Human Factors, for which *Homo heidelbergensis* (Smithsonian, 2022), a pre-runner of *Homo sapiens*, was already able to combine different techniques like cutting to carve and fire to harden an effective tool and adapt it to the individual bearer. These spears are also an early example of Human Systems Integration, which is understood as integration of humans, technology, organization, and environment: Close to the location of the spears, many horse bones were found. Anthropologists reconstructed that obviously a tribe of *Homo heidelbergensis* hunted, rounded up, speared, and ate these horses. Especially the production of the spears, which can be seen as a clever use of or integration with the environment, and the cooperative hunting took a degree of organization, which was not available to other rival species. What we can also derive from hunting techniques of animals, of so-called primitive societies or even from modern hunting traditions is that it was not only about organizing the own tribe, but to disrupt and disorganize the opponent, to trick the flock of prey in a way that they had no chance to escape. This technique represents CogWar at its early stage. It also becomes increasingly clear that these weapons, together with the cognitive development of *Homo* species, was quite disruptive for other animals, one of the first known disruptive technologies as defined by Christensen (1997).



Figure 9-1: One of the Spears of Schoeningen as an Early Example of Human Factors, Human Systems Integration and of Cognitive Warfare (Thieme, 1997).

Given this precedent (Christensen, 1997), we must prepare to defend against CogWar just in case cognitive warfare is as disruptive for us as this early example was for the horses. It becomes increasingly clear that not only the physical layer of these spears, transporting deadly energy over distance and **temporarily out of hand** of the original thrower was revolutionary and highly disruptive, but the cognitive layer of this hunting came was the one which really made a difference in survival of this *Homo* species. Tomasello (2014) describes how human

cognition evolved together with the ability to create and handle such tools, and especially how the cooperation and shared intentionality fostered the evolution of *Homo* towards *Homo sapiens* as one of the most dominant species on this planet. Cooperation and teaming were obviously essential for this early hunting, cooperation and teaming might also be essential for today's challenge of AI-based systems and CogWar. Weapons like these spears became not only a normal part of hunting, but also of warfare:

The necessity of fighting very soon led men to special inventions to turn the advantage in it in their own favour; in consequence of that the mode of fighting has undergone great alterations; but in whatever way it is conducted its conception remains unaltered, and fighting is that which constitutes war. (Clausewitz 1831, 1968)

Thinking before fighting, and about fighting, i.e., cognition about warfare became an integral part of any sophisticated military. Sun Tzu, military philosopher at least well known in China, especially in the Peoples Republic of China, which is considered “a challenge to NATO’s interest, security and values” (NATO, 2022), speaks about “knowing,” which is an essential part of any CogWar: Hence the saying: “If you know the enemy and you know yourself, your victory will not stand in doubt; if you know Heaven and you know Earth, you may make your victory complete” (Tzu, 496 BC).

While the first part of Sun Tzu’s quote is quite familiar for Western ears and cognitions, the second part might sound strange at the first glance but is truly remarkable: It points not only towards weather and terrain, but towards a cognition, which is open to a much bigger, holistic picture than just of yourself and a potential enemy. It might be exactly that feeling of strangeness in our ears or that of our NATO colleagues and comrades, which should make us think twice and ask ourselves: Is there something valuable not only in the first, but also in the second part of Sun Tzu’s insight that could help us to evolve our own cognitive abilities, before a system rival starts to outperform us with a more sophisticated cognition?

Centuries later, Stephen Biko (1971) would carve another mighty weapon of cognitive defence into words, describing a fundamental cognitive relationship between opponents, which applies not only in an asymmetric warfare, but also in a hybrid war of 2022: “The most potent weapon of the oppressor is the mind of the oppressed” (Woods, 1971; Peters, 2018).

Sun Tzu and Stephen Biko each refer to the knowledge, minds, and cognitions of humans. For many centuries, cognition was thought to be a privilege of *Homo sapiens*. This would change with a gradual revolution, starting with the first process-controlled computer Z1 of Konrad Zuse in Berlin, 1936, followed by the Mark I built 1944 by Howard Aiken and the IBM team which was used to support the Manhattan Project. In close relation with this revolution in hardware, another scientific revolution happened regarding the software and scientific model. Norbert Wiener authored his famous book in which he introduced Cybernetics in 1950. It remains one of the most influential books of the twentieth century. Interestingly, Wiener is often misquoted to have written about computers. His book is more general about control and communication mechanism both in animals and machines, and sparked a revolution of system science beyond computers, especially in biology and psychology.

Wiener’s Cybernetics is describing cognition in action, regardless of whether animals, humans, or machines, forming feedback loops which influence or even control situations (for an overview how this applies to safety critical systems see Flemisch et al. 2022). Later, Licklider (1960) sketched the Man/Human-Computer Symbiosis and sparked a whole research stream on joint cognitive systems. Our discussion on AI ties right into this research stream of cybernetics and human-computer symbiosis.

9.2 COGNITIVE WAR AND HUMAN COGNITION

With all the discussions with Artificial Intelligence (AI), it becomes increasingly clear that this is a development towards an Artificial Cognition (Ritter, Barrett, Santoro, and Botvinick, 2017), which forms a joint cognition system in the sense of (Hollnagel and Woods 2005), together with human cognition. That is, Artificial Cognition can be thought of as a hybrid discipline that combines machine behavior and cognitive models that may be inferred from data elicited via experimentation vs directly observed. (Ritter et al. 2017).

Based on Sun Tzu's prescient forecast, it also becomes increasingly clear that it is not enough to look only at one human or one artificial cognition but elevate our view beyond that to a more holistic picture.

Step by Step from the Small to the Bigger Systems

What are integral parts of a more holistic model of CogWar, and where should we start? A good starting point is to look at a single cognition and describe it in a way that it can be applied both to humans and artificial cognition (Figure 9-2).

Figure 9-2 shows a typical loop of perception of and action on a situation. What makes these feedback loops a cognition is that this perception and action is not arbitrary, but with an intent to develop the situation towards a good situation and avoid bad situations. While Figure 9-2 shows a fundamental fork in the road of life, Figure 9-3 shows more detail, especially addressing a fundamental dilemma in any safety and time critical system like in military systems.

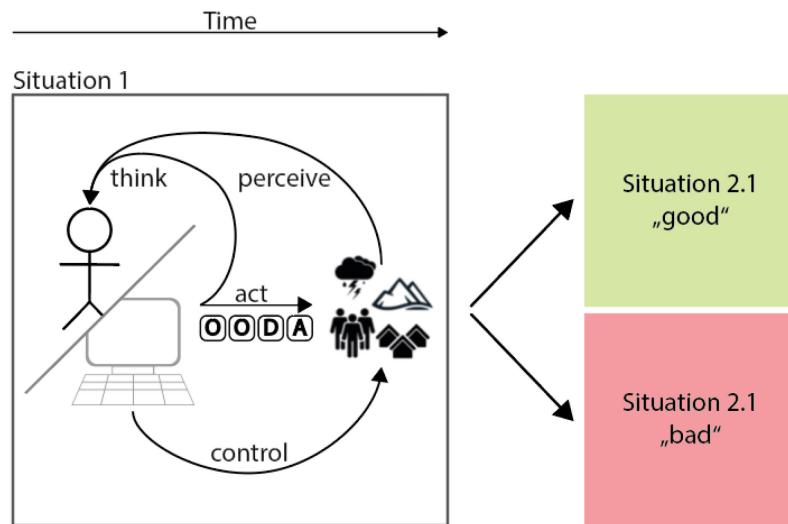


Figure 9-2: Cognitive Loop and Perception-Action Cycle of Humans or Machines. (Inspired by Wiener 1950, including John Boyd's OODA loop, based on Flemisch et al. 2012, Flemisch et al. 2022).

As Clausewitz already describes as "fog of war," there is always uncertainty in information about the situation, e.g., the capabilities and intent of an opponent. Figure 9-3 left shows the most fundamental aspect of uncertainty with the detection of a signal, which might lead to an action and non-action: The signal can be present or absent, and the perception and response can be there and not there, leading to two positive situations "Correct Hit" or

“Correct Rejection,” and two negative states of “Miss” and “False Alarm.” Applied to action and non-action e.g., of military systems, Figure 9-3 right shows “Action” and “Non-Action,” where the valence is still undetermined, and the four possible outcomes “Correct Action,” “Correct Non-Action,” “False Non-Action,” or “False Action.”

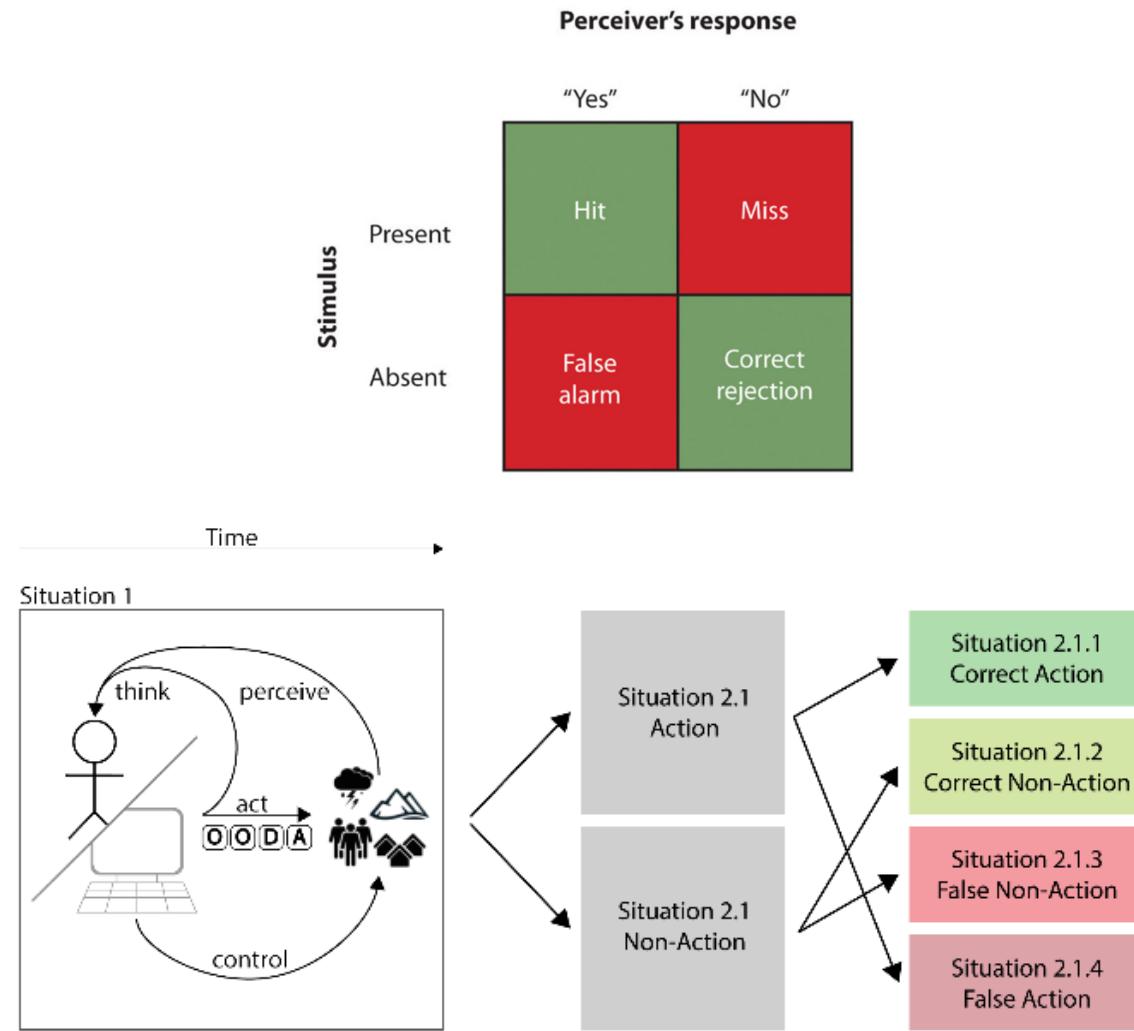


Figure 9-3: Top: Signal Detection Theory; Bottom: Cognitive Loop and OODA Loop of Humans or Machines, with Decision to Action or Non-Action Under Uncertainty (“In the Fog of War”).

An example for this fundamental dilemma is the recommendation of an AI leading to an action or non-action of a soldier, which can cause in a correct or incorrect use or non-use of military action. Even if there is hope that AI might alter this equation, (e.g., Wallace 2018), what makes this dilemma so problematic is time: In military combat, the price for non-action often increases with every second, while the information might still be not reliable enough to determine action to be a correct action. Soldiers sometimes call these dilemma situations “one foot in jail, one foot in the grave.” Ironically, after the combat, e.g., in a court trial, there is ample time to determine all the minute details of law and regulations.

To understand these issues of time and cognition better, over the decades of research models or patterns have been developed which describe how to act on the world and the ability to learn (e.g., Wiener, 1950). Many years later, Damasio (1994) would describe that at least with human cognition, these models and their interactions with the world are also associated, almost inseparable with emotional states and with bodily perception (somatic markers). Kahneman (2011) outlines two systems, (i.e., autonomous, and automatic vs analytical and deliberate) models of human cognition, which work at different speeds and at different cognitive quality.

Another example for the modelling of cognitive processes is the OODA loop (Figure 9-4), originally described by (Boyd, 1996), modelling the decision cycle for military combat/war situations. The OODA loop describes perceiving, thinking, and acting of agents in four stages of decision-making:

- **Observation:** Gathering of outside information and matching them with unfolding circumstances and unfolding environmental interaction.
- **Orientation:** Judging the observation in the light of previous experiences, genetic heritage, cultural traditions, and analyses.
- **Decision:** Selecting one of several hypotheses and putting them to test with reality.
- **Action:** Implementing the decision.

Figure 9-5 shows another important step towards a more holistic model of CogWar: Based on Licklider's concept of human-machine symbiosis, Rasmussen (1983) proposed the term cooperation, Hollnagel and Woods (1983) and Sheridan (2002) describing initial principles, Hoc and Lemoine (1998) and Hoc (2000) described the common ground and know-how-to-cooperate as important parts of developing human-computer cooperation.

A major breakthrough was to think of cognition not only as something separated/assigned to individual agents, but also as Joint Cognition or Joint Cognitive System. Hollnagel also sketches how these Joint Cognitive Systems can be nested, from the small to the big, and already prepared the ground for a system-of-systems approach. Flemisch et al. (2019) described how humans and machine cognition can cooperate on levels with different time frequencies, yet still work together like the blunt end and the sharp end of a spear. Flemisch et al. (2020) extended this view also to conflicts that can happen between agents in cognitive systems, and how these can be mitigated.

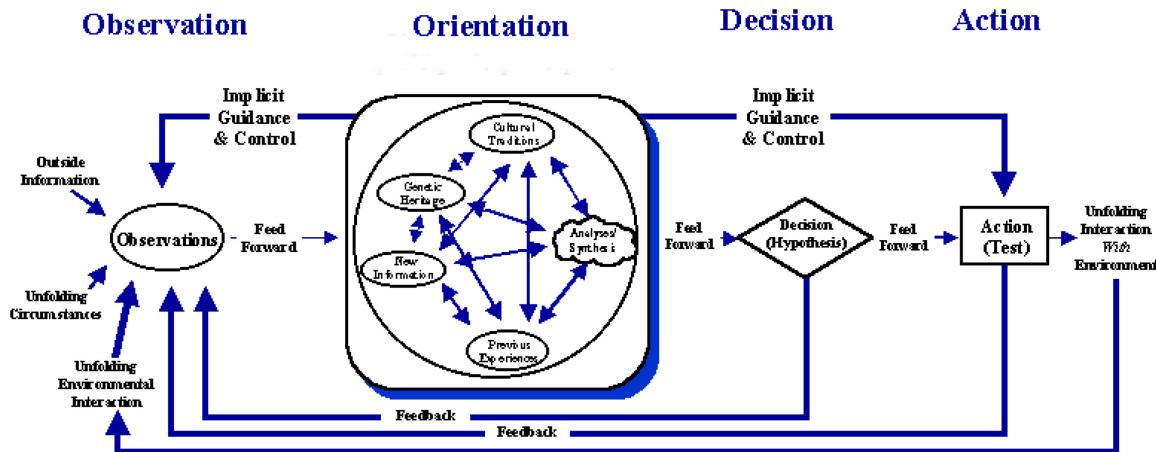


Figure 9-4: A Look into the Details of Cognitive Processes in Individuals or Organizations: Example OODA Loop of Observation, Orientation, Decision, and Action (Boyd, 1996).

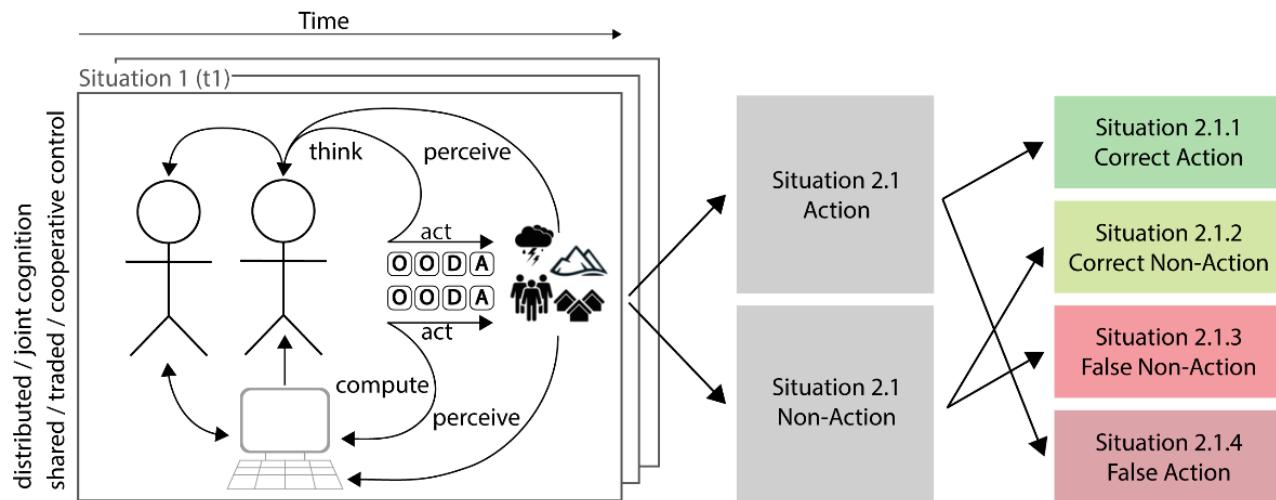


Figure 9-5: Human-Machine System and Cooperation with Other Agents, Forming Joint Cognitive Systems of Interlinked OODA-Loops.

It becomes increasingly clear that the teaming of human and computers, e.g., in the form of AI, will become essential for any form of CogWar, whether offensive or defensive. The more cognitive processes are enabled by computer networks, the more cyber defence becomes important. A similar equation could be true for AI: the more cognitive processes are influenced, hopefully enhanced with AI, the more cognitive (warfare and) defence becomes important. This becomes even more important if the acceleration of the last decades continue (e.g., Rosa, 2013), and fighting at machine speed spreads out from its early beginnings in the realm of fast paced air and space defence systems, also to other domains or even offensive operations. Taking (Kahneman, 2011) seriously, who describes our cognitive systems No. 1 as fast, intuitive and emotional, but also as more vulnerable to mis-judgement compared to the slower but more deliberative and more logical cognitive system no. 2, an essential part of CogWar is about time and speed: Outperform an opponent in a way that he cannot unfold his full cognitive potential, and on the other side of the same coin, design systems with enough time for humans to use their system no 2.

9.3 THE HOLISTIC BOWTIE MODEL

This connection is even more important with the fast interconnectivity between the different layers of our systems, e.g., our defence systems with the political system. With the goal to make this more transparent, Figure 9-6 combines Hollnagel and Woods idea of the joint cognitive system with the idea of a bowtie diagram, originally derived in the incident and accident analysis of safety critical systems and adapted to a holistic bowtie diagram for the design and human systems integration of any system by Flemisch et al. (2022).

Figure 9-6 shows the next step towards a holistic model of CogWar. It puts the core cognitive systems of few human and AI agents in the center, nested by a system-of-systems layer, organizational and societal layers. In the extreme, it is our global environment, sometimes called biosphere, which is nesting and hosting all these layers. The transversal cognitive layer depends on the physical layer and permeates all layers from the small human-machine system to the larger systems like organizations and societies.

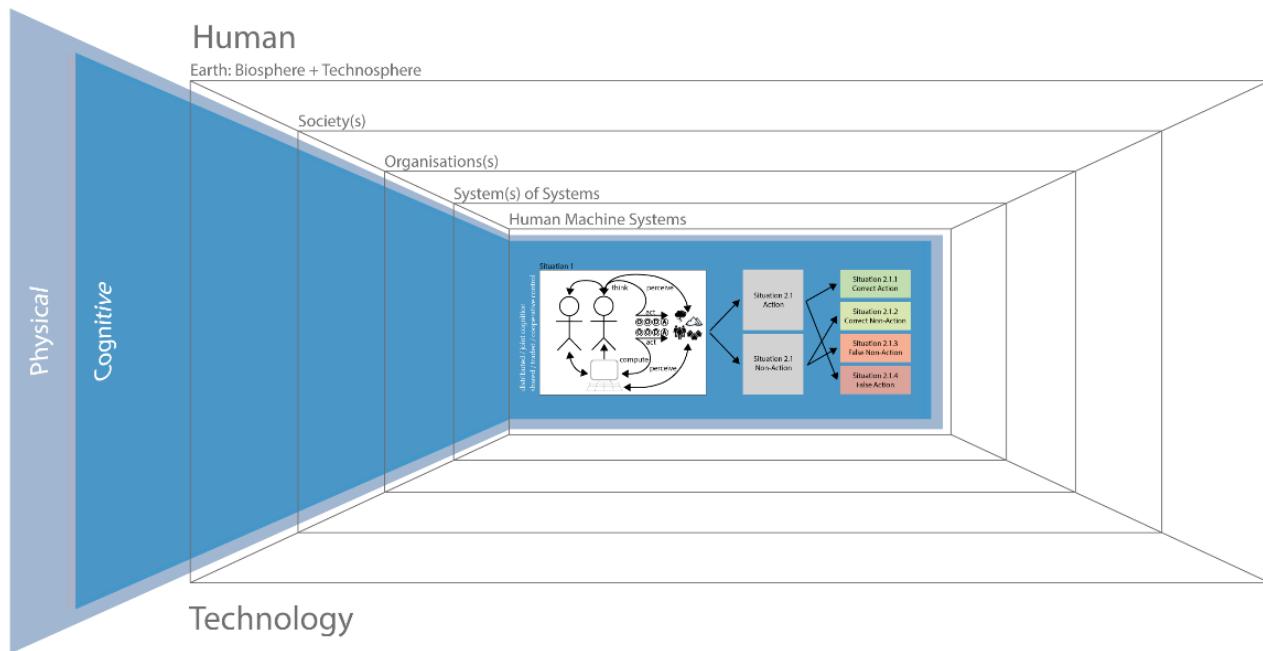


Figure 9-6: Holistic Bowtie Model of Human- Machine Cognition (Adapted from Flemisch et al. 2022).

It becomes increasingly clear, that cognitive processes occur on each of these layers and that these layers mutually influence it other. In these layers from the smallest to the largest, cognition can be considered as distributed and interrelated. Siebert in Flemisch et al. (2022) summarizes Hutchins (1995) theory of distributed cognition by “thinking about cognition in terms of the emergence and interactions of component parts.” The theory of distributed cognition focuses not on how individual actors make decisions considering social and environmental features but focuses on a broader class of cognitive events that surpasses the individual. It is an approach to understanding cognition from a distributed perspective across members of a group, environment and through time. The goal of the holistic bowtie model is aimed at enabling a distributed, holistic perspective on cognition distributed between humans, machines, system-of-systems, organizations, societies, environment, and through time.

Figure 9-7 shows an example how this holistic model can be used. It can help to show essential connections between the layers, e.g., how commensurate transparency helps to cultivate trust between the layers, how authority is distributed and respected, and how ability is enabled, and together with control, leads to a fair accountability for all agents, soldiers, and civilians alike, in this nested system. Figure 9-7 also shows how these essential streams and loops of authority, cognitive ability, and trust, as one of the most essential enablers of our defence cooperation in NATO, might also be attacked and corrupted, and with those cognitive processes be degraded and disturbed. It also provides a map how an adversary’s cognitive processes could be disturbed, disrupted or, if necessary, in defensive action of a major attack, be destroyed.

Damasio (1994) also makes it clear that cognition is combined with our emotions and even bodily feelings. What becomes increasingly clear is that this applies not only for an individual agent, but is connected, from the smallest to the largest, from individuals, groups, human-computer/AI systems up to whole societies. Many of these connections and feedback loops are less understood, described, or remain yet undiscovered. A more holistic model might help to explore those connections. As CogWar might not only affect the battlefield, but all layers up to society and global environment, it will be crucial to understand and consciously shape these connections.

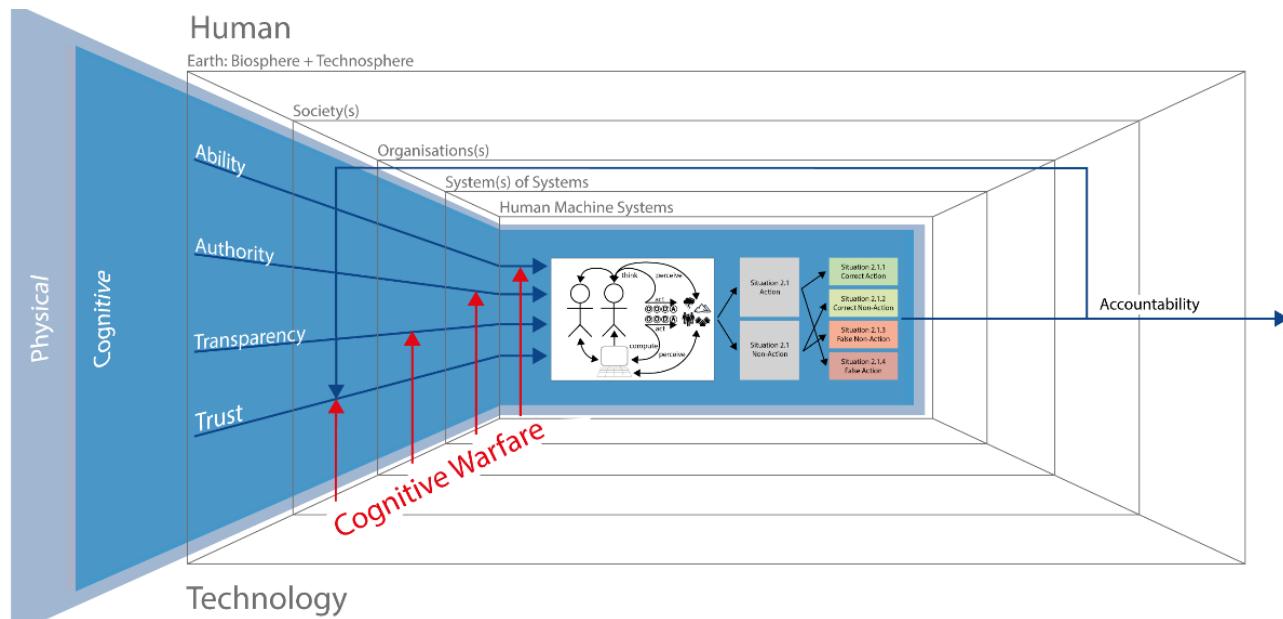


Figure 9-7: Holistic Bowtie Model of Cognitive Warfare, with Examples for Defence and Attack Vectors, and One Feedback Loop from Accountability to Ability, Authority, Transparency, and Trust.

9.4 CONCLUSION AND RECOMMENDATIONS: HOW TO PROCEED WITH COGNITIVE WARFARE AND BEYOND

How holistic, how big should our picture be? Flemisch et al. (2022) describe a commensurate holism, which limits the scope with a pragmatic argument of estimated influence. We should not forget that this might still be a Western tendency to simplify, to focus, while Eastern military philosopher, Sun Tzu's philosophy on warfare is still the basis of Asian/Chinese warfare and taught in Chinese military academies, speaks about nothing less than heaven and Earth.

To understand that Sun Tzu is not only speaking about the weather or the load-bearing capacity of Ukrainian soil, it might also help that Sun Tzu's perspective is related to the Chinese concept of Tianxia 天下 "(all) under Heaven," and is understood as the entire geographical world, including humans and animals. Despite the fact, that it was used for centuries to describe the outreach of the Chinese emperor, it is also a philosophical principle, described e.g., by Daoist philosopher Guanzi how to expand the perspective from a family to a village to a state or an entire world. It was also used in Japanese history as a leitmotiv to unify Japan (by military force and balance of power), and in more recent times, this philosophy was used by Chinese philosopher Zhao Tingyang (2009) to describe a potential global perspective.

We should not leave this potential cognitive revolution towards a holistic perspective, which connects the small with the large, humans with machines/AI's, to our Chinese adversaries. Rather, we proposed the following objectives along short-, mid- and long-term recommendations:

- Do not think CogWar as something only related to human cognition.
- Think CogWar across all levels and in all domains, including space. Think of CW as warfare with and on distributed and joint cognition of humans, machines/AI including networks, organizations, societies, and a global environment.

- Bring and hold together inter- and transdisciplinary teams of soldiers, engineers, human factors and Human Systems Integration specialists, cyber defenders, organizational and societal scientists, and politicians to refine these thinking models, to identify potential attack vectors, and to design and implement potential defence systems.
- Develop and test defence philosophies, doctrines, and systems against cognitive attacks, in an analogous way as we acted on the cyber domain, but even more integrated with individuals, societies, economics, and politics.
- In parallel, constantly work on the narratives, especially the defensive deterrence of NATO against any attack, physical or cognitive.
- In parallel, cooperate with the political side and with arms control: The more we mutually agree on, assert and be able to trust not using certain techniques, the safer it will be for all of us.

If we want to prevent the next war, or at least not lose it, we should seriously consider the lessons of Sun Tzu and not stop at the physical and cognitive layer but think beyond it. Once again, a lesson from history for many nations is that fighting power (e.g., in the sense of van Creveld, 1982), whether physical or cognitive, might not be enough:

*War in its literal meaning is fighting, for fighting alone is the efficient principle in the manifold activity which, in a wide sense, is called war. But fighting is a trial of strength of the **moral and physical forces** by means of the latter. That the moral cannot be omitted is evident of itself, for the condition of the mind has always the most decisive influence on the forces employed in war.* (Clausewitz, 1968, Book 2, Chapter 1)

Today we might talk more about ethics than moral, but the essence is quite similar. We face a system rival China, where at least two senior air force officers obviously have read not only Sun Tzu, but also Clausewitz and Creveld, and wrote about an “Unrestricted warfare” including terrorism, economic and network warfare (超限戰, Qiao et al., 1999). We face a system rival Russia, which is testing a less restrictive warfare in the Ukraine with the threat to escalate to unrestricted warfare. With a clear view in these system rivals, we in NATO are forced, motivated and already engaged to rethink, re-group, balance, and, if necessary, boost up our ethical, cognitive and physical forces, to whatever level necessary (Figure 9-8).

In closing, future consideration about the defence against CogWar should include research on human cognition, artificial cognition, and especially shared, joint cognition in Robotic and Autonomous System design. Future warfare will integrate the human-machine team as part of the cohesive military force and thus, shared Situational Awareness will include AI-embedded Robots. Future research programs must be established to invest in S&T to enhance team performance, including humans and AI, and ensure the integrity and trustworthiness of cooperative systems with autonomous, AI-based functions that will serve as collaborators and partners in the future operational environment.

Let us continue to foster our defensive but cooperative and strong fighting power, physically, cognitively, and ethically. Let us discuss and cultivate a common ground and work on a common balance, from a defensive but strong position to fence off any potential attack, whether physical, cognitive, or ethical. Based on a commonly agreed ethics and a defensive but strong position, let us work together towards physical, cognitive, and ethical peace, on our common home Earth, under the same Heaven.

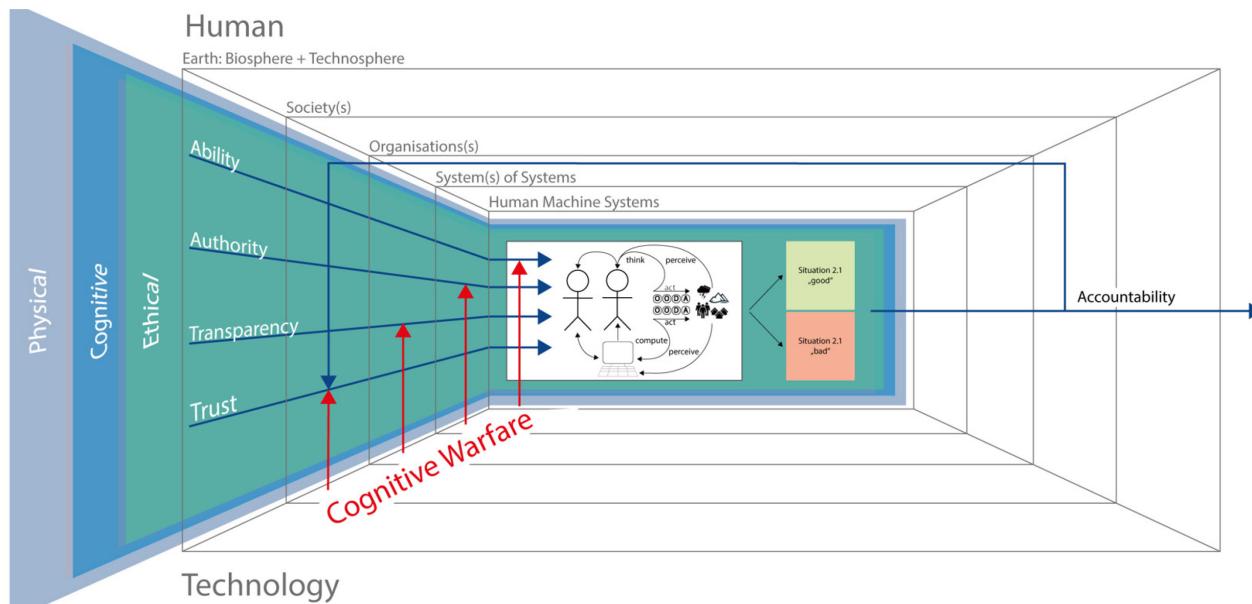


Figure 9-8: Outlook, Holistic Bowtie Model, Including an Ethical Layer into Physical and Cognitive Warfare.

9.5 REFERENCES

Boyd, J.R. (1996). The Essence of Winning and Losing. Ed. C. Richard and C. Spinney. Bluffton, South Carolina. Available online at https://ooda.de/media/john_boyd_-_the_essence_of_winning_and_losing.pdf

Christensen, C.M. (1997). The Innovator's Dilemma. When New Technologies Cause Great Firms to Fail. The Management of Innovation and Change Series. Boston, Mass.: Harvard Business Review Press.

Dalheim, R. (16 September 2020). Schöningen Spears – Mankind's Earliest Wooden Weapons. Retrieved August 2022 from: <https://www.woodworkingnetwork.com/wood/schoninger-spears-mankinds-earliest-wooden-weapons>

Damasio, A.R. (1994). Descartes' Error and the Future of Human Life. *Scientific American* 271(4), p. 144. Doi: 10.1038/scientificamerican1094-144.

Flemisch, F., Abbink, D.A., Itoh, M., Pacaux-Lemoine, M.P., and Weßel, G. (2019). Joining the Blunt and the Pointy End of the Spear: Towards a Common Framework of Joint Action, Human-Machine Cooperation, Cooperative Guidance, and Control, Shared, Traded and Supervisory Control. *Cogn Tech Work* 21(4), pp. 555-568. DOI: 10.1007/s10111-019-00576-1.

Flemisch, F., Baltzer, M., Abbink, D., Siebert, L., Diggelen, J., and Draper, M. (2022). Towards a Dynamic Balance Between Humans and AI-Based Systems: Holistic Bowtie Model for Ability, Responsibility, Authority, Autonomy, Meaningful and Effective Control, and Accountability. In L. Siebert and D. Abbink (Eds.). *Handbook on Meaningful Human Control*. Cheltenham, Gloucester, UK: Edward Elgar (in press).

Flemisch, F., Heesen, M., Hesse, T., Kelsch, J., Schieben, and A., Beller, J. (2012). Towards a Dynamic Balance Between Humans and Automation: Authority, Ability, Responsibility and Control in Shared and Cooperative Control Situations. *Cognition, Technology & Work* 14 (1), pp. 3-18. DOI: 10.1007/s10111-011-0191-6.

Flemisch, F., Pacaux-Lemoine, M.P., Vanderhaegen, F., Itoh, M., Saito, Y., and Herzberger, N. (2020). Conflicts in Human-Machine Systems as an Intersection of Bio- and Technosphere: Cooperation and Interaction Patterns for Human and Machine Interference and Conflict Resolution. In: 2020 IEEE International Conference on Human-Machine Systems (ICHMS). Rome, Italy, 07 Sept 2020 – 09 Sept 2020: IEEE, pp. 1-6.

Hoc, J.M. (2000). From Human-Machine Interaction to Human-Machine Cooperation. In *Ergonomics* 43 (7), pp. 833-843. DOI: 10.1080/001401300409044.

Hoc, J.M., and Lemoine, M.P. (1998). Cognitive Evaluation of Human-Human and Human-Machine Cooperation Modes in Air Traffic Control. *The International Journal of Aviation Psychology* 8(1), pp. 1-32. DOI: 10.1207/s15327108ijap0801_1.

Hollnagel, E., and Woods, D.D. (1983). Cognitive Systems Engineering: New Wine in New Bottles. In *International Journal of Man-Machine Studies* 18(6), pp. 583-600. DOI: 10.1016/S0020-7373(83)80034-0.

Hollnagel, E., and Woods, D. (2005). Joint Cognitive Systems. Foundations of Cognitive Systems Engineering. Boca Raton, Florida: CRC Press. Available online at <https://ebookcentral.proquest.com/lib/subhh/detail.action?docID=263746>

Hutchins, E. (1995). Cognition in the Wild. Massachusetts: MIT Press.

Kahneman, D. (2011). Thinking, Fast and Slow. New York: Farrar, Straus, and Giroux.

Licklider, J.C.R. (1960). Man-Computer Symbiosis. *IRE Trans. Hum. Factors Electron. HFE-1* (1), pp. 4-11. DOI: 10.1109/THFE2.1960.4503259.

NATO (2022). NATO 2022 Strategic Concept. Adopted at the Madrid Summit, 29 – 30 June 2022. Retrieved August 2022 from: <https://www.nato.int/strategic-concept/>

Peters, M. (18 October 2018). The Most Potent Weapon in the Hands of the Oppressor is the Mind of the Oppressed. Red Pepper Magazine. Retrieved August 2022 from: <https://www.redpepper.org.uk/the-most-potent-weapon-in-the-hands-of-the-oppressor-is-the-mind-of-the-oppressed/>

Qiao, L., Santoli, A., and Wang, X. (1999). Unrestricted Warfare. Brattleboro, Vermont: Echo Point Books & Media.

Rasmussen, J. (1983). Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. In *IEEE Transactions on Systems, Man, and Cybernetics SMC-13*(3), pp. 257-266. DOI: 10.1109/TSMC.1983.6313160.

Ritter, S., Barrett, D.G., Santoro, A., and Botvinick, M.M. (2017). Cognitive Psychology for Deep Neural Networks: A Shape Bias Case Study. International Conference on Machine Learning, pp. 2940-2949.

Rosa, H. (2013). Social Acceleration: Columbia University Press.

Sheridan, T.B. (2002). Humans and Automation. System Design and Research Issues. New York: John Wiley and Sons Inc.

Smithsonian Institute, (1 July 2022). Homo heidelbergensis. Human Origins. Smithsonian Institute. Retrieved August from: <https://humanorigins.si.edu/evidence/human-fossils/species/homo-heidelbergensis>

Thieme, H. (1997). Lower Palaeolithic Hunting Spears from Germany. Nature 385, pp. 807-810. DOI: 10.1038/385807a0. Retrieved August 2022 from: <https://www.nature.com/articles/385807a0>

Tingyang, Z. (2009). A Political World Philosophy in Terms of All-Under-Heaven (Tian-xia). Diogenes 56(1), pp. 5-18. DOI: 10.1177/0392192109102149.

Tomasello, M. (2014). A Natural History of Human Thinking. Cambridge, Massachusetts, London, England: Harvard University Press (ProQuest Ebook Central). Available online at <https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=3301383>

Tzu, S. [496 BC] (1910). SunTzu on the Art of War. Trans. L. Giles. London: Luzac and Co. Retrieved 09 February 2023 from <https://archive.org/details/the-art-of-war-by-sun-tzu-trans.-by-lionel-giles-m.-a.-1910/page/n3/mode/2up>

Van Creveld, M. (1982). Fighting Power. German and US Army Performance, 1939 – 1945. Contributions in Military History, 32. Westport, Connecticut: Greenwood Press.

Von Clausewitz, C. (1968). On War. London: Penguin Books.

Wallace, R. (2018). Carl von Clausewitz, the Fog-of-War, and the AI Revolution. Cham: Springer International Publishing.

Wiener, N. (1950). Cybernetics. In Bulletin of the American Academy of Arts and Sciences 3(7), pp. 2-4. Doi: 10.2307/3822945.

Woods, D. (1991). Biko. 3rd rev. ed. New York: Holt.

Chapter 10 – EDUCATION AND TRAINING FOR COGNITIVE WARFARE

J.E. (Hans) Korteling

The Netherlands Organization for Applied Scientific Research (TNO)
THE NETHERLANDS

10.1 INTRODUCTION

The actual and practical execution of CogWar is not simple and may include a range of inherent complexities concerning the concrete, underlying psychological mechanisms and effective psychological strategies and tactics. In addition, according to Verall et al. (2016), compared to the Eastern cultures, the Western world, historically, has been less comfortable with psychological deception as a recognized tool for military influence. Western culture and open democracy are protected by respective government rules with layers of highly valued ethical checks and balances in the open-source, mass-media. Overt lying and feigning of information from sources such as government and/or organizations, is not tolerated nor accepted. However, Western nations and NATO countries have placed a low priority on developing pro-active countermeasures to detect, deter, and defend against CogWar. To date, research studies have focused on information manipulation from a reactive, defensive response to CogWar. For example, Korteling and Duistermaat (2018) concluded that this ad hoc, defensive, and reactive focus may be a risky approach given the deep and long-term nature of hybrid and information campaigns. Our reactive (instead of pro-active) approach may continue our relatively weak and unthreatening position in the world-wide arena. A more pro-active approach will focus on the weakening, destabilization, and undermine the position of the opponent and influence his decisions. This should be done within the boundaries set by our juridical and ethical principles that prevent us from obvious lying, feigning, or massive production and the dissemination of disinformation. In some cases, these boundaries may have a significant limiting consequence for the range of feasible CogWar possibilities.

We contend that a pro-active approach may be more beneficial as it will focus on mitigating and undermining the adversaries' ability to achieve their objectives, as well as weaking and destabilize their sphere of influence on a global scale. NATO should develop defence strategies against CogWar within the legal and ethical boundaries required. NATO and Allied partner nations must develop strategic defence strategies within the legal, juridical, and ethical boundaries of their respective nations. The development of countermeasures requires additional investment in training military personnel to prepare them with the required knowledge, skills, and abilities to defend against CogWar. One must develop measures to detect disinformation and misinformation campaigns at an early stage that may influence public opinion and the mass consciousness. Thus, nations must invest in the development of advanced training tools and methods for education and training personnel to recognize psychological deception and manipulation. Education and training will increase individual's awareness and help to develop resilience with the knowledge and skills acquired to detect and mitigate deception and manipulation. Individuals must acquire the skills to counter the influence of misinformation with reliable, trustworthy, and verifiable facts. This pro-active approach to education and training will require investment in the development of effective training tools but are essential for facilitating the development of military personnel to respond rapidly and effectively.

The development of such advanced training methods and tools is a critical first step in forging each nation's defence against deception operations of CogWar. Virtual technologies and environments provide a means to design scenarios that will help to build the skills necessary to counter the effects of CogWar. Such scenarios in a wargaming virtual environment facilitates the individuals' ability could practice strategic and tactical analysis

across an array of hybrid scenarios based on realistic or imaginary threats (e.g., various forms of strategic gaming). This will increase awareness regarding the possible and current impact of psychological deception, as well as improve the knowledge, experience, capabilities and resilience of military personnel.

To date, however, there is no consensus regarding the best means of training military personnel to defend against CogWar. There is a need to develop a sophisticated tool consisting of many modules, scenarios, and elements aligned with military defence measures such as those of Stratcom. For example, a prototype module might be developed that would include the steps that are essential for the execution of *critical preparatory activities*:

- Analysis of the problem;
- Goal definition;
- Knowing and understanding the target group, their culture, views, and needs;
- Determining other relevant actors or agencies and possible media;
- Historical (context) analysis.

This model could be expanded and tailored in design to address numerous deceptive stratagems (or tactics), scenarios, narratives, and challenges presented in a multi-media platform wherein several social media platforms may be used to verify information, develop risk management procedures, and mitigation strategies could be developed. For example, a model could be developed to focus on the analysis and selection of deceptive tactics or stratagems. This model could be used across media platforms as narratives, messages, with collaborators as a means of developing risk management procedures.

10.2 TRAINING AND EDUCATION

The first question in this respect concerns the specification of adequate training objectives (training goals) and training trajectories, not only for initial training, but also for experts in CogWar. The questions raised are, what skills need to be developed? What are the best methods and formats for this type of training? Training objectives may vary from initial levels of making people aware of the issue and of what is (already) possible, and what can be practically done to more expert-level recurrency team training in realistic scenarios. Several years ago, TNO, in collaboration with the NLDA, organized two workshops focused on discussions concerning the knowledge, practices, policies, and possible scenarios regarding CogWar. These workshops were carried out with participants of the Dutch Armed Forces who were professionally trained on the topic of information operations. These workshops indicated that these professionals do not seem substantially more sophisticated in psychological deception and manipulation than most other well-educated civilians. Specifically, the military's level of knowledge and experience concerning the psychology of subconscious influence and manipulation of information was equally elementary to that of a civilian staff member's level of psychological knowledge (Korteling and Duistermaat, 2018).

Although this was not explicitly investigated or tested, we would place (on a 'best guess') the level of competence of the workshop participants in the two bottom levels of the *Hierarchy of Competence*, i.e., unconscious incompetence and conscious incompetence (see Figure 10-1). This assessment is illustrated by expressions of participants like: "Since we now know that unconscious influence is normal in our daily lives, for instance in commerce and politics, targeted, strategic undermining and manipulation is also business-as-usual for the army." Basic awareness is often highly under-developed, even on the highest levels of political and military decision making (e.g., president Biden emotionally calling President Putin a "war criminal" shortly after the Russian invasion of Ukraine, may be considered very disputable from a psychological point of view.

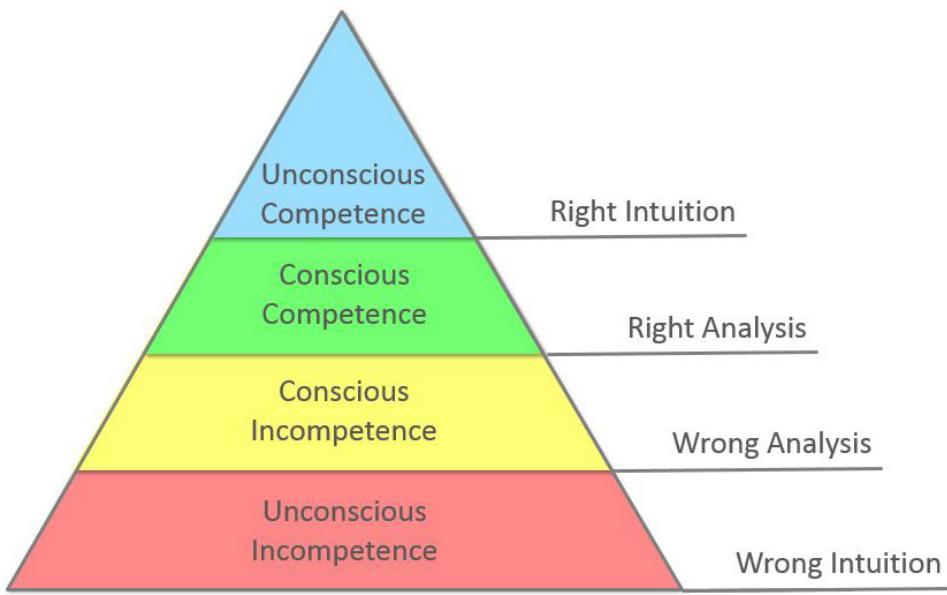


Figure 10-1: Hierarchy of Competence.

This overall lack of knowledge and experience in the military seems to be supported by a brief survey among NATO partners involved in the NATO HFM Panel 356 on CogWar. In this survey we asked our partners (from Canada, France, Italy, Germany, Norway, Sweden, UK, US) the following questions regarding the education and training practices in five fields of information operations that are discerned by the Dutch defence:

- 1) Monitoring the information environment;
- 2) Understanding target groups;
- 3) Countering disinformation/influence;
- 4) Influencing; and
- 5) Strategical Communication:
 - a) *Are there substantial Education and Training practices already carried out in your nation (or other nations you know) and if "Yes" on which ones of the above five fields is this done?*
 - b) *Which types of O&T and which methods/tools (like simulation, gaming, etc.) are used for which kinds of training goals (e.g., board games/constructive simulations/Instruction video's/books for the training goal of Increasing awareness of "OODA hacking" or how to counter disinformation.*

The results of this simple survey on NATO CogWar education and training practices can be summarized as follows:

- No substantial or dedicated education and training on the principles and methods of CogWar:
 - Few initiatives with doubtful results.
 - Governmental initiatives, e.g., debunking misinformation, are minor or negligible.

- CogWar education and training is still an emerging topic in its initial stage:
 - Basic awareness about the impact of internet, cyber, and social media usage.
 - General awareness education is in line with public and academic initiatives not much of dedicated military training.
- Lack of good teaching material and training methods:
 - Wargaming under development (low priority).
 - Some classrooms as well as “hands-on” exercises.

10.3 KNOWLEDGE DEVELOPMENT

The basic level of consciousness on this topic implies that there is a need for defence departments to educate and train military professionals and develop their critical thinking skills if they are to master a range of such competencies. The initial basic training on the development of critical thinking skills would focus on becoming aware of your vulnerabilities (e.g., cognitive bias) and the pervasive effects of influence (including how you yourself are – easily – influenced). Second, skills could be developed by training military personnel how to mitigate the influence of information operations and finally how to practically apply the basic principles to influence others or protect yourself from external influence.

Most prominently, the military should become deeply aware of how deceptive thinking and practices are endemic in a connected, technology-driven international arena. For example, various research projects are being conducted in the Netherlands to expand knowledge, not only regarding the psychological aspects of CogWar, but also related to the physical and informational aspects. Research is being done with military personnel to gain insight on these topics by participating in strategic wargames. There are many types of these games, such as: Matrix gaming, Dilemma games, Connecting-the-dots games, Campaign games, or Interactive scenario-based discussion). Most games are mainly aimed at raising awareness (and some understanding) of the increasing importance and possibilities of hybrid aspects of modern conflicts, which are largely fought in the information domain. What is still lacking in these games is the training of more awareness and insight into the manifold psychological mechanisms of influence (and indoctrination) and how these are translated into concrete activities of psychological deception.

Another topic is how to cope with the emotional impact and stress that may be induced by CogWar and misinformation campaigns. Dealing with these campaigns can be psychologically demanding, cause a lot of distress and therefore undermine cognitive performance. Finally, how to address erroneous data and disinformation on the internet. This may involve detecting hacks and identifying the sources or hidden intentions behind disinformation. However, this is sometimes only possible to a very limited extent due to legal and ethical provisions in the field of managing the public or public data. Simulating data can then offer a solution but it is complex, labor-intensive, and expensive.

To develop effective training and education, good lessons-learned can be drawn from research in (neuro-)cognitive science and other fields of psychology such as, how to influence consumer behavior (Adams, Sartori, and Waldherr, 2007; Cialdini, 1983; Hansen, 2013; Jowett and O'Donnell, 1992). Chapter 11 describes one training toll that has recently been developed by Bergh. Additional educational content can be drawn from neuro-psychological knowledge on how cognitive biases, originating from neural and evolutionary characteristics of the brain, can be exploited to manipulate human thinking and decision making (Heuer, 2013; Janser, 2007; Kahneman, 2011; Korteling, Duistermaat, and Toet, 2018; Korteling, Brouwer and Toet, 2018; Korteling and Toet, 2022).

In addition, valuable insights are also available from the creative professions, such as film set design for physical deception, and from commercial marketing (Verrall et al., 2016). Since our totalitarian opponents are less hindered by ethical and juridical restrictions than we are, this vast body knowledge on influencing human perception, decision making, and behavior can be used to develop more subtle information interventions (Korteling and Duistermaat, 2018). Much attention should be paid to target audience analysis and the methodological aspects of CogWar (e.g., analysis, campaign planning, intervention, risk management, measuring effect). In general, the inclusion of how to apply our deep insights into influencing (or manipulation) human decision making needs to be one of the corner stones of the training courses to be developed.

10.4 CONCLUSION AND RECOMMENDATIONS

Although the allied military remains committed to maintain its capacity for traditional warfare, military leaders recognize that hybrid approaches with an increasing informational and psychological character have become the prevailing mode of conflict. Therefore, military organizations in Western/NATO countries, who strive towards stability, need to rely more heavily on advanced informational and psychological methods and concepts to effectively engage in these hybrid conflicts. However, there seems little awareness, knowledge, or experience to integrate the cognitive aspects of operating in the CogWar dynamic information environment at a sufficient level within the NATO armed forces. In contrast to the former Soviet Union and Russia, the Western world has not yet intensively engaged in developing in-depth knowledge, experience, and adequate tools for CogWar. Improvement of this situation may require progress in the field of recruitment and selection of personnel. However, we must first design the framework for good education and training programs with proper educational content, methods, and didactics. Finally, adequate tools (like simulation and virtual and real-time wargaming) for supporting training and for the defence, preparation, and execution of CogWar must be developed.

10.5 S&T RECOMMENDATIONS

To be implemented now (1 – 2 years):

For the short-term- basic training programs can be implemented focusing on pro-active awareness and more literacy regarding the well-known pervasive effects of military influence, deception and manipulation by the weaponization of information. This includes how we ourselves are – easily – manipulated in our thinking and decision making, for example by the exploitation of our psychological vulnerabilities, such as our cognitive biases. Most prominently, the military should become much more profoundly aware that deceptive thinking and practices are endemic in a connected, information- and technology-driven international arena. Wargaming seems an effective way to promote increased awareness of the complex information environment and for recognizing the interplay of the many forms of influence and deception. It has been shown to be particularly useful for strategically complex problems and offers the possibility to analyze the potential cascading chain of events that emerge because of such actions. An important challenge is that (during the preparation phase) the processing of personal data is only possible to a limited extent – only if there is a legal basis or mandate. This makes it difficult to practice with real data and limits the possibilities in the use of ICT tools. In addition, the narrative to train in the information domain needs to be changed and clearly communicated. Regarding research with more in-depth knowledge and experience must be developed on how psychological influence and deception in a military context works or how the workings may be augmented. This knowledge will facilitate and shape the content and development of more sophisticated training methods and programs to be developed in the next phase.

Next (3 – 5 years):

Practicing within the information environment is essential to acquire the necessary skills for effective maneuvering with information. Apart from the training of the defensive and reactive aspects of CogWar, NATO allies need to foster the practical application of pro-active stratagems and tactics in valid operational contexts. Therefore, in-depth knowledge and experience on the cognitive mechanisms of influence and manipulation, such as how to deal with emotion and distress and how cognitive biases can be exploited for manipulation, must be further developed. Based on this knowledge, the educational methods and content for more sophisticated (than just awareness and literacy) operational readiness training programs and methods need to be extended. In-depth knowledge on the manifold psychological mechanisms of influence (and indoctrination) must be captured in well-structured models. These models will then be applied for the translation of tactical and strategical issues into concrete chains of military CogWar operations. This also concerns a further development of technology supporting the training of how to effectively deal with data, such as social media the large amount of information and communication on the internet. People will have to learn to work effectively with AI technology that may support the detection and identification of misinformation, disinformation and hacks carried out by opponent actors. To train the relevant competencies, this may require the provision of more sophisticated synthetic and simulated data, as well as realistic scenarios, which is difficult, labor-intensive, and therefore, expensive. Finally, more people within the military should be trained to develop critical thinking skills and become “strategic thinkers” across a broad range of relevant (sub)domains. This also requires the development of (selection tools), training methods, and didactic content to train the involved cognitive and communication skills.

Future towards the next level (5+ years):

So, for the first 5 years to come, we must focus on the (further) development of in-depth knowledge, training methods, training content, and probably some basic support tools for CogWar. When this knowledge (and experience) has been sufficiently developed, it will become possible to focus more on the R&D of advanced (support) tools. In this “medium-to-long-term” we need the development of advanced (e.g., AI-endowed) methods and tools to support the military in the integral chain of defensive, pro-active, and offensive CogWar. In this regard, allies will need a coherent framework of different support systems, which is closely and flexibly linked to the operational environment. This approach also includes an overall shell (or framework) for detecting, mitigating, countering, selecting, designing, developing and executing CogWar operations (a “CogWar Engine”). This approach, at least on both the strategic and tactical levels, would prove helpful for the development of technical competencies required for the defence against CogWar. For example, such a model or tool must support certain critical preparation operations, such as: understanding and seeing through the opponent or selecting, preparing and executing certain cognitive tactics (operations, stratagems). Elements of CogWar for which tooling could be developed to support the integral chain of necessary activities in a coherent way are:

- Detection of opposing psychological influence and deception, e.g., recognizing it.
- Disinformation:
 - How to recognize false information.
 - How to mitigate or counter or bend weaponized information, as well as dealing with emotion and distress.
- Analysis and understanding of the opponent (and the other relevant actors).
- Selection and definition of strategic issues for CogWar operations.
- Specification of a strategic or tactical CogWar goal to obtain.

- Analysis of the relevant global and local circumstances.
- Selection and specification of the kind of CogWar operation to use.
- Means (narratives, storyboards, training scenarios), tools and media that may be used.
- Target groups and operation levels on which to act.
- Division of tasks, authorities and responsibilities.
- Execution of CogWar operations (per actor, target, stratagem, timing, means, etc.).
- Orchestrating the whole of the CogWar operation.
- Contextual issues, involvement of the mass and social media.
- Analyses of risks and potential negative outcomes.
- Development of advanced support tools or tooling concepts for different phases/aspects.
- Educate people to become “strategic thinkers.”

In closing, there is a significant amount of research that remains to be done that will focus on the development of advanced training content, methods, and tools that will support the development of military and civilian personnel in the defence against CogWar.

10.6 REFERENCES

- Adams, B.D., Sartory, J., and Waldherr, S. (2007). Military Influence Operations: Review of Relevant Scientific Literature. Report No. CR 2007-146. Toronto: Defence Research and Development Canada. Retrieved August 2022 from: <https://apps.dtic.mil/sti/citations/ADA477201>
- Cialdini, R.D. (1983). *Influence: The Psychology of Persuasion*. New York: Harper.
- Hansen, W.G. (2013). *Influence: Theory and Practice*. Monterey, California: Naval Postgraduate School.
- Heuer, R.J. (2013). Cognitive Factors in Deception and Counter Deception. In: H. Rothstein, and B. Whaley (Eds.), *The Art and Science of Military Deception*, pp. 105-133, Boston/London: Artech House.
- Janser, M.J. (2007). Cognitive Biases in Military Decision Making. US Army War College, Carlisle Barracks, PA.
- Jowett, G and O'Donnell, V. (1992). *Propaganda and Persuasion*, 2nd edition, Newbury Park, CA: Sage Publications, 122-154. <http://people.ucalgary.ca/~rseiler/jowett.htm>.
- Kahneman, D. (2011). *Thinking, Fast and Slow*. London: Penguin Group.
- Korteling, J.E., Brouwer, A.M. and Toet, A. (2018). A Neural Network Framework for Cognitive Bias. *Frontiers in Psychology* 9:1561. doi: 10.3389/fpsyg.2018.01561
- Korteling, J.E. and Duistermaat, M. (2018). Psychological Deception. Report TNO R11532. Soesterberg: TNO Defence, Safety and Security.

EDUCATION AND TRAINING FOR COGNITIVE WARFARE

Korteling, J.E., Duistermaat M. and Toet. A. (2018). Subconscious Manipulation in Hybrid/Psychological Warfare. Report TNO 2018 R11543. Soesterberg: TNO Defence, Safety and Security.

Korteling, J.E. and Toet, A. (2022). Cognitive Biases. In S. Della Sala (Ed), Encyclopedia of Behavioral Neuroscience, 2nd edition, ISBN 9780128216361, Elsevier. pp 610-619. DOI: 10.1016/B978-0-12-809324-5.24105-9.

Verrall, N., Mason, L, Ellis, B. (2016) Military Deception. Baseline Understanding for Contemporary Information Activities. DSTL/TR90060 v1.0. UK: Dstl.

Chapter 11 – SOMULATOR: DEVELOPING COGWAR RESILIENCE THROUGH SOCIAL MEDIA TRAINING

Arild Bergh

Norwegian Defence Research Establishment
NORWAY

11.1 INTRODUCTION

Realistic simulations are beneficial for those preparing for military responsibilities. For the *Trident Juncture* exercise, NATO's Joint Warfare Centre used a commercial software package that provided **Facebook** and **Twitter**-inspired features to provide a social media element in this large, multinational exercise (Tomlin, 2016). Encouraged by the results of this, the C-SPI project at the Norwegian Defence Research Institute (FFI) undertook a research activity aimed at providing an updated social media experience for training purposes. This activity resulted in a complete tool designed for non-IT experts in a range of training and exercise situations. This tool, known as **Somulator**, provides an online service, either through the Internet or on closed networks.

This chapter will summarize the issues that were considered when selecting the core elements of the training tool. Then, we will discuss the feedback received from users that laid the foundations for additional, custom development that were used to integrate the core elements into a complete training solution. Lastly, we will discuss the core lessons learned from this study.

11.2 ISSUES RELATED TO SOCIAL MEDIA TRAINING

Previous chapters have highlighted the challenges that NATO may face from the adversaries' use of social media platforms and technologies in CogWar. There is a need to develop and train military personnel to understand and manage social media effectively. This is especially critical in CogWar where adversaries have weaponized information and disseminate it globally and invisibly across the global digital network on social media platforms.

Thus, given the influence and impact of social media platforms, to train military personnel to understand and manage information presented on social media platforms is no longer optional. Rather, it is an essential competency that all military personnel must achieve as part of CogWar defence. Furthermore, social media is deeply embedded in everyone's daily life, and exerts influence on everyone's perceptions and decisions. Thus, we can no longer ignore or disconnect from information presented in social media, doing so would entail great risks. Nor can we view this as an intelligence or communication specialist issue as the wide dissemination of propaganda, disinformation and misinformation campaigns across global social media platforms affects everyone and must be addressed by each person. Indeed, information has already been weaponized across all media platforms and used by adversaries to target both the military and mass civilian population.

There are many challenges in learning to counter CogWar in the social media environment. For example, although it would be free to open any number of social media accounts on real social media platforms and use them for training, this would immediately run into several issues. First, some social media, like Twitter, display all content by default. This would restrain the ability to train freely on any scenario and being able to fail without fear of causing offence or being ridiculed. Furthermore, most social media platforms ban the use of fake logins.

Military personnel/staff would either break platform rules or face exposure. Unlike other military uses of real-life locations for regular military exercises, these limitations prohibit this approach.

An alternative could be to simply describe a scenario, such as “fake news about an impending attack by a terrorist group is spread through Twitter.” Although this approach is often used in high-level war gaming, this would leave a lot to be desired when training practitioners in different fields. In some ways it would be akin to doing target practice through notes – social media content is chaotic and overwhelming; using a naturalistic setting is thus a better way to start build resilience.

11.3 PROPOSED SOLUTIONS

Given these constraints, we researched how we could achieve a realistic social media simulation that would provide high quality training for a wide array of military personnel, ranging from intelligence cells in the home guard to communications staff in a government department. Attempting to recreate even a subset of a real social media platform’s functionality from scratch would be costly. It would also require the establishment of an ongoing development team to fix bugs. Furthermore, there are different types of social media platforms that each have different affordances (Bergh, 2019, p. 17), training someone on **Twitter** does not necessarily help them on a video-based platform like **YouTube**.

Therefore, we decided to utilize open-source “clones” of several different social media platforms in an overall tool called **Somulator**. **Somulator** integrates five individual web-based applications with custom software to make them suitable for use in training. The term, open source, denotes that one is allowed to modify the software according to one’s needs. For example, we were able to amend newspaper software, so it automatically creates three newspapers for use in training. Each of the five web applications were selected after an evaluation of different products, they are:

- Friendica (Facebook type social media platform, i.e., friends-based platform that allows sharing of many different media).
- Mastodon (Twitter type social media platform, i.e., micro-blogging content) (Figure 11-1).
- Pixelfed (Instagram type social media platform, i.e., photo sharing).
- Peertube (YouTube type social media platform, i.e., video sharing).
- Drupal (Content management software that provides online newspaper functionality).

Each of the four social media platforms implement the key features of the originals. This includes uploading diverse types of content, communicating with, and subscribing to other users, showing content in constantly updated feeds and search results, providing tools for sharing and commenting on information, and so on. The fifth application, Drupal, is a general content management system used by many newspapers and magazines, such as the **Economist**. Like other online newspapers, Drupal has built-in comments and article sharing tools.

What these platforms lack are the advanced machine learning tools used by commercial social media networks to analyze uploaded content and users’ interests which are used to show content that is of interest to the individual users. This is the main aspect of social media that is manipulated for cognitive warfare purposes (Bergh, 2020, p. 17). In a training situation, this will therefore need to be replaced by manually planned and executed deployment of content. This will be discussed briefly at the end of this chapter.

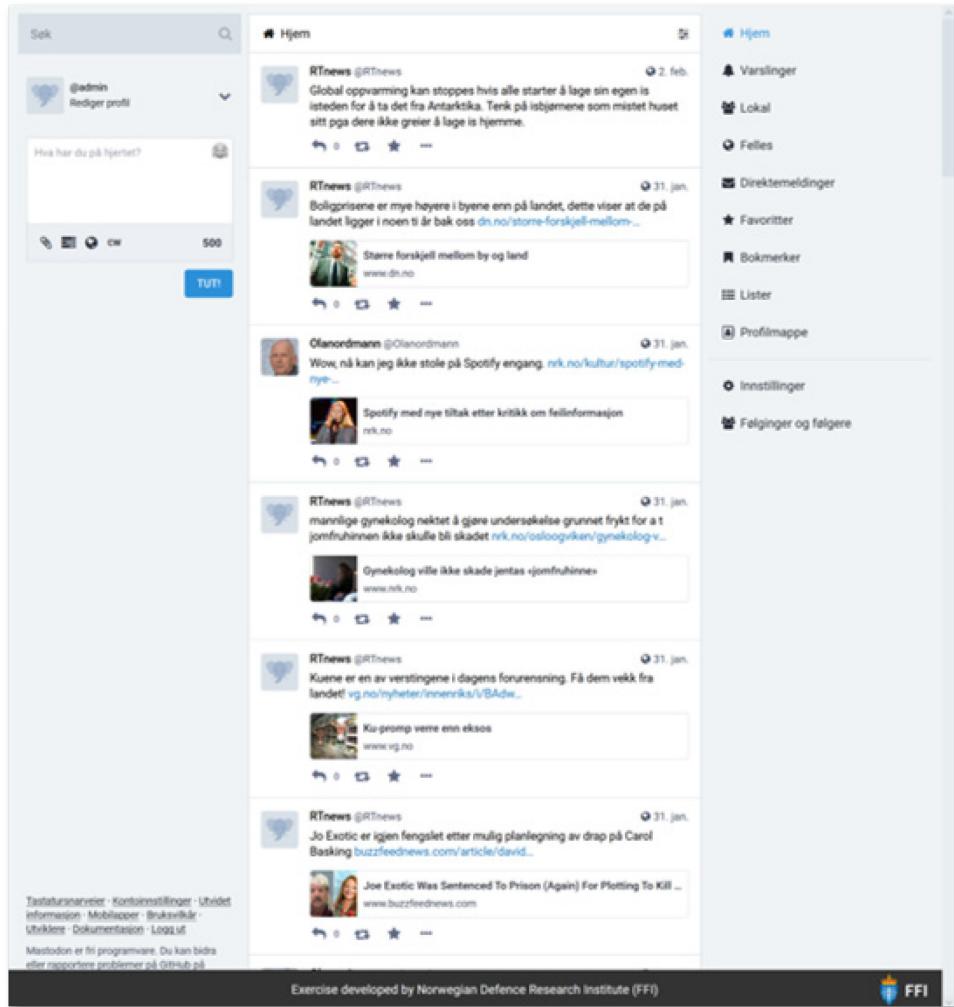


Figure 11-1: Screenshot of Mastodon, the Twitter Clone.

11.4 DESIGN METHODS

11.4.1 Input from Potential Users and Core Goals that Emerged

The decision to utilize existing open-source software that has been tested and is continuously developed was followed by an analysis of what customizations were required to turn these individual, separate applications into a coherent training platform. As a part of this analysis *Somulator* was discussed with different potential stakeholders. These included experienced, regional organizers of media training, staff at NATO's Joint Warfare Centre, workshop, and exercise organizers at national public bodies in Norway, as well as the staff at the Norwegian Cyber Defence and fellow FFI researchers.

Based on these discussions the following key requirements emerged for the different user types. Namely, we developed key requirements for 1) Trainers; and 2) Training event organizers.

11.4.2 Low Threshold for Use

The type of training discussed here is often done by subject specialists who do not necessarily have in-depth IT expertise. A simple method to deploy *Somulator* was therefore required. This requirement was managed by developing an automated means of deploying of *Somulator* after asking just three questions through a regular web page (see Figure 11-2). *Somulator* is thus what is known as “software as a service.” The ease with which *Somulator* can be deployed also means that it can easily be de-commissioned without worrying about the cost of deploying it again. This avoids having to keep services and servers running for longer than required due to re-deployment costs.

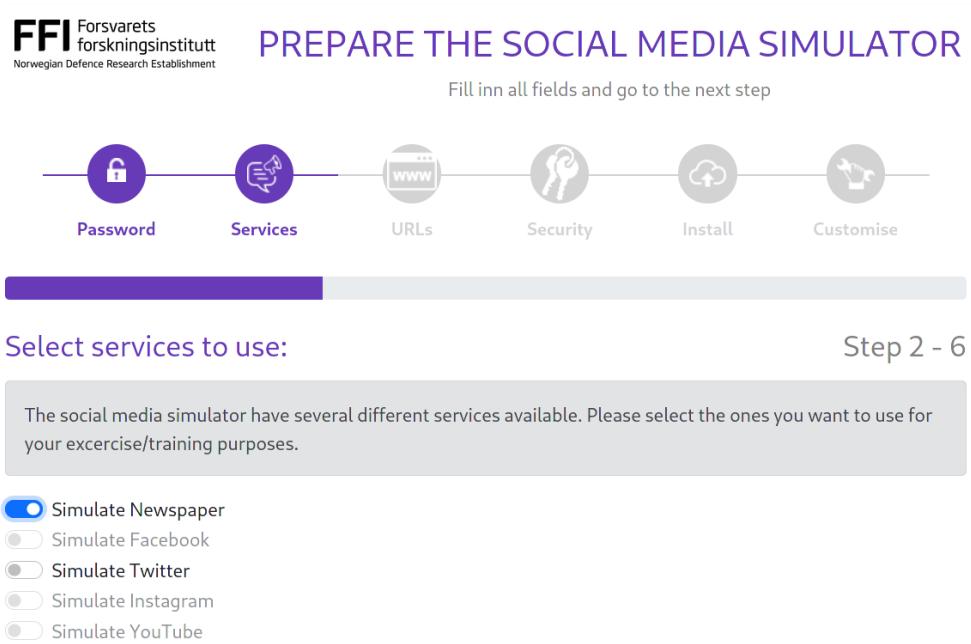


Figure 11-2: Second of the Five Steps When Deploying Somulator.

11.4.2.1 Ease of Organizing Training

Informants with practical training experience highlighted the workload involved in setting up tools for participants to use, typically by creating accounts and emailing login information before the training event. To handle this, a web-based administration tool was developed for *Somulator*. This has, among other things, a built-in registration module where any number of emails can be copied into a text box and accounts will automatically be set up and the new users will be alerted through emails.

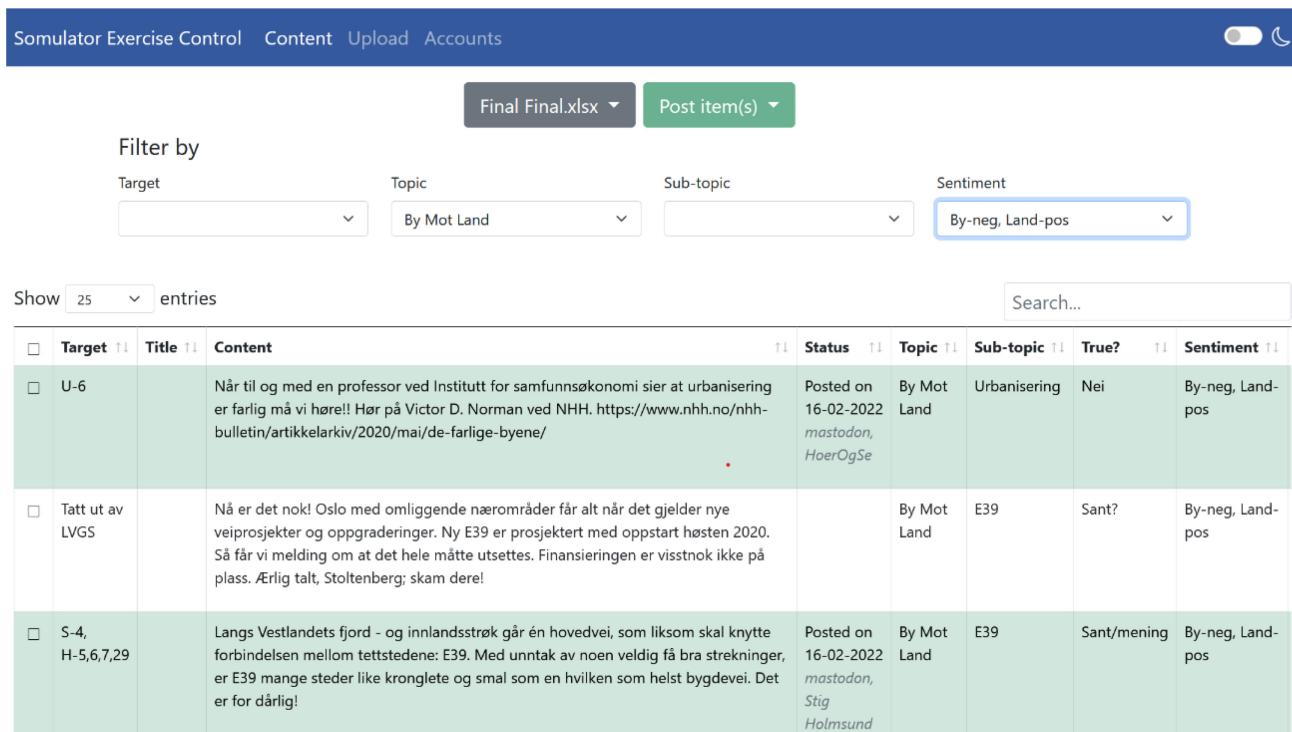
11.4.2.2 Content Control

Finally, trainers needed simple and efficient means by which to control how and when content is published through the different social media platforms. It is the content that will facilitate learning. Content publishing therefore needs to be controlled in such a way that it can tie in with an overarching scenario (Figure 11-3).

Somulator therefore has a module for the “white cell” (also called Excon) to upload and distribute content through the different social media platforms that have been deployed. The main purpose of this tool is:

- 1) To be able to spread copious amounts of content in a brief time, as one experiences it on social media; and
- 2) Choose services and profiles used for diverse types of posts.

The latter is used because different profiles have distinctive characteristics that can change participants’ perception of the shared content. A profile claiming to be a retired general may seem more authoritative on military matters than a home maker’s profile. This is also how real influence campaigns operate.



The screenshot shows the 'Content' tab of the Somulator interface. At the top, there are buttons for 'Final Final.xlsx' (selected), 'Post item(s)', and a toggle switch. Below this is a 'Filter by' section with dropdown menus for 'Target' (empty), 'Topic' (By Mot Land), 'Sub-topic' (empty), and 'Sentiment' (By-neg, Land-pos). There is also a 'Show 25 entries' button and a search bar. The main area displays a table of prepared content items:

Target	Title	Content	Status	Topic	Sub-topic	True?	Sentiment
U-6		Når til og med en professor ved Institutt for samfunnsøkonomi sier at urbanisering er farlig må vi høre!! Hør på Victor D. Norman ved NHH. https://www.nhh.no/nhh-bulletin/artikelarkiv/2020/mai/de-farlige-byene/	Posted on 16-02-2022 <i>mastodon, HoerOgSe</i>	By Mot Land	Urbanisering	Nei	By-neg, Land-pos
Tatt ut av LVGS		Nå er det nok! Oslo med omliggende nærområder får alt når det gjelder nye veiprosjekter og oppgraderinger. Ny E39 er prosjektert med oppstart høsten 2020. Så får vi melding om at det hele måtte utsettes. Finansieringen er visstnok ikke på plass. Årlig talt, Stoltenberg; skam dere!		By Mot Land	E39	Sant?	By-neg, Land-pos
S-4, H-5,6,7,29		Langs Vestlandets fjord - og innlandsstrøk går én hovedvei, som liksom skal knytte forbindelsen mellom tettstedene: E39. Med unntak av noen veldig få bra strekninger, er E39 mange steder like kronglete og smal som en hvilken som helst bygdevei. Det er for dårlig!	Posted on 16-02-2022 <i>mastodon, Stig Holmsund</i>	By Mot Land	E39	Sant/mening	By-neg, Land-pos

Figure 11-3: Prepared Content Ready for Deployment in Somulator.

For researchers:

- **Somulator** is also a tool for researchers to learn more about how CogWar through social media works, and through this research contribute to the development of new training approaches. The features discussed above make it considerably easier to organize casual experiments for different groups that require customized setups. This makes it easier to test ideas with different scenarios/groups. In addition, it is possible to extract the data from an experiment to analyze in retrospect.

For organizations:

- Finally, organizations, whether the armed forces or government agencies tasked with handling crises, have some overarching requirements. Although not clearly spelled out, they emerged during conversations with stakeholders that represented diverse types of organizations.

- First, it would be very costly if a training tool in such a dynamic arena as social media was static. The ability to extend the software is therefore of paramount importance. Somulator is extendable as it uses open-source software that users may freely modify. Furthermore, users actively develop these applications within a large community of developers, who add features over time, thereby, keeping the feature set up to date. The open nature of the underlying social media platforms also means that any custom enhancements are distributed and implemented in the overarching administration tool that can be shared with other organizations.
- Secondly, training tools that users share with other organizations are beneficial in terms of lower costs but also because the pool of people who know the software expands. Interoperability is a key feature to achieve this, and all the social media platforms used in Somulator implement the Activity Pub protocol (Webber et al., 2018). This allows two different organizations using for example Mastodon (the Twitter type platform), to connect these via the Internet if they do joint training at some point. The organization could be two different defence educational outfits or even armed forces from two different NATO member states.

11.5 LESSONS LEARNED AND FUTURE DIRECTIONS

Somulator was evaluated in a pilot experiment where media students from a local high school prepared disinformation-based content and worked in the white cell. Members of a youth wing of an independent defence related Non-Governmental Organization (NGO) participated in the actual experiment.

The key finding from this experiment highlighted the importance of content that feels relevant to the participants, not only in the current experiment but also in relation to their everyday life and work. Social media is deeply embedded in everyone's daily life. Thus, humans filter out irrelevant content, and tailor information streams according to individual interests and relevant needs. Disinformation or propaganda content that seems too outrageous may therefore simply be ignored rather than providing opportunities for learning. This may therefore be more a case of "train as you live" than train as you fight, perhaps an appropriate sentiment given that our cognition straddles everyday life and not only our defence.

This point also shows the need during training to replace the social media platforms' algorithms that continuously evaluate what information you are most likely to prefer, with careful preparation and deployment of information through relevant profiles. Otherwise, the content will have negligible effect on the learning as it will seem to be random information of no particular concern to the individual person undergoing training.

Social media training therefore require considerable preparation in terms of creating relevant content for an experiment or training workshop. The possibility of using machine learning models such as GPT-2 to generate content may provide one way forward, and research is currently taking place to explore how difficult it would be to train Norwegian language models to create copious quantities of disinformation automatically.

Looking ahead, **Somulator** will be used as part of a three-year project funded by the Norwegian DoD. There are also numerous actors within the Norwegian Total Defence who are eager to use **Somulator** in different training contexts.

The results of this pilot study have implications for defence against CogWar. The ability to have AI/ML tools and technologies developed that will facilitate filtering of irrelevant information, detection of fake information, and information that is not valid will be more easily detected and rendered irrelevant to the end user. Thus, the **Somulator** tool that emerged from this research holds great promise in contributing to research and training to defend against CogWar in the future.

11.6 REFERENCES

Bergh, A. (2019). Social Network Centric Warfare: Understanding Influence Operations in Social Media (FFI-Rapport No. 19/01194; p. 65). Norwegian Defence Research Establishment (FFI). <http://hdl.handle.net/20.500.12242/2623>

Bergh, A. (2020). Påvirkningsoperasjoner i sosiale medier – Oversikt og utfordringer (FFI-rapport No. 20/01694; p. 58). Norwegian Defence Research Establishment (FFI). <http://hdl.handle.net/20.500.12242/2724>

Tomlin, G.M. (2016). #SocialMediaMatters: Lessons Learned from Exercise Trident Juncture. Joint Force Quarterly. <http://ndupress.ndu.edu/Media/News/News-Article-View/Article/793264/socialmediamatters-lessons-learned-from-exercise-trident-juncture/>

Webber, C., Tallon, J., Shepherd, O., Guy, A., and Prodromou, E. (2018). ActivityPub-W3C Recommendation. W3C Social Web Working Group, 23rd January.



Chapter 12 – LEGAL AND ETHICAL IMPLICATIONS RELATED TO DEFENCE AGAINST COGNITIVE WARFARE

Lea Kristina Petronella Bjørgul
Norwegian Defence Research Institute
NORWAY

12.1 INTRODUCTION

The sophistication of new digital technologies and advances within artificial intelligence, machine learning, and autonomous systems coupled with the increasingly widespread use of social media has made it possible for actors to reach larger audiences with customized and targeted content at machine speed. This development has arguably altered the character of warfare and given rise to Cognitive Warfare (CogWar). CogWar takes well-known and novel approaches within information, cyber, and psychological warfare to a new level through the implementation of these modern technologies by not only attempting to alter the way people *think*, but also how they *react* to information.

States are increasingly taking advantage of these methods to achieve their strategic objectives. The end goal of CogWar is to gain some sort of advantage over another party. Consequently, the aim of CogWar is arguably the same as within the other warfighting domains; to impose ones will upon another state. This is in line with one of the main elements of Clausewitz's definition of war: "...an act of violence intended to compel our opponent to fulfill our will" (Von Clausewitz, 1968, p. 101). According to Clausewitz, war is conducted for some second-order purpose. States do not go to war simply to commit violence, but to impose their will upon other states. Despite the common aim, the concept of cognitive warfare raises several new legal and moral challenges that should be carefully considered by those involved in determining the status and response to CogWar. These issues should be resolved before NATO decides whether to implement the cognitive domain as its 6th warfighting domain. The challenges in question are both related to the issue of *why* or *if* a war should be fought (*jus ad bellum*), and *how* a war should be fought (the conduct of war or *jus in bello*).

12.2 DEFENDING AGAINST COGNITIVE WARFARE: ISSUES RELATED TO *JUS AD BELLUM*

Several measures are needed to defend against CogWar. Obvious measures include (amongst others) making society more resilient against actions in the cognitive domain across all sectors (civilian and military), to prevent the actions of an adversary to be successful. However, other defensive measures should receive thoughtful treatment. Important examples include deterrence and defensive counterattacks, as well as the problem of attribution (the problem of ambiguity as to the identity of the attacker). Against whom is one to retaliate when the identity of the perpetrator cannot be firmly established? How is deterrence to work if the punitive threat of retaliation cannot be accurately aimed? Ethical reasoning in the form of judgements about good versus harm done, the level of proof required to act, and the matter of *when* and *how* to respond to actions in the cognitive domain will all be of critical importance moving forward.

A specific issue regarding *jus ad bellum* and defensive counterattacks that needs to be investigated is related to Article 5 (The North Atlantic Treaty, 1949, Art. 5). The result of treating the cognitive domain as a warfighting domain is the implication that an action within this domain *can* be characterized as an act of

war, and potentially trigger the right to national self-defence (and Article 5). Consequently, one main issue that the Alliance potentially needs to resolve is: *when should an action within the cognitive domain be considered an unlawful use of force?*

One approach to this challenge is to revisit the debate that took place when NATO declared the cyber domain as an operational domain. The main issue for the participants in this debate was that cyberattacks are non-kinetic, and most importantly, the argument that the existing international frameworks could not accommodate cyberattacks because they do not appear to use physical or violent *means* as they only involve the manipulation of computer code. However, given the potential consequences of cyberattacks, many argued that it was implausible to suggest that no state could ever use military force to protect itself from them.¹ This debate resulted in a definition of force that applies the existing laws of war to actions within the cyber domain only when these actions are likely to result in conventional physical harm (Petkis, 2016, p. 1431; Schmitt et al., 2013, p. 93). More specifically, the threshold suggested for the cyber domain was that actions that *directly*² and intentionally cause significant physical effects, qualify as a use of force (and could potentially trigger the right to national self-defence). Some authors have suggested that this framework can be revised and used to develop legal definitions and metrics for cognitive acts of war (Bernal et al., p. 36).

Although a useful starting point, this definition of force, and the framework suggested for the cyber domain might not be satisfactory for establishing governing principles within the cognitive domain. Several arguments can be made for why the framework suggested for the cyber domain might not be appropriate for the cognitive domain. Most importantly, it appears that many forms of current CogWar will often not involve death and widespread physical destruction. As previously mentioned, the aim of CogWar is to alter the way people *think* and *react* to information. With this aim a state could have several different goals, but one of the most well-known examples is policy change through election influence (such as the Russian influence operation targeting the American public in connection to the 2016 presidential election). Although a significant challenge to modern democracies, these types of actions do not fit the criteria of resulting in “significant physical effects.” One could argue that influence campaigns with the goal of destabilization and encouragement to violence can in fact lead to significant physical effects. However, these effects would be indirect, not direct, as the current consensus encourages (Bjørgul, 2021). The implication of this is of course that very few (if any) cognitive attacks will ever trigger a nation’s right to self-defence. However, the potential consequences of certain types of CogWar (such as influence operations) on democratic stability, raises the question of whether there are other effects than physical harm which should be considered to give rise to a *casus belli*.

In conclusion, CogWar arguably represents a significant and new challenge to our moral and legal understanding of war and the right to self-defence. Consequently, there is a need for critical thinking about when this new type of warfare should be used, and how it should be regulated. One important and difficult challenge for the Alliance moving forward is to think fundamentally new about which actions in the cognitive domain should be considered unlawful actions of war if it decides to implement the cognitive domain as the 6th warfighting domain.³ A framework needs to be developed, from which a set of principles and legal articles can be derived, so that acts of CogWar can be identified and appropriately be responded to.

¹ See for example: Cook, 2010; Roscini, 2010; Silver, 2002; and Eberle, 2013.

² The Tallinn Manual includes both directness (i.e., greater or lesser extent of attenuation in the causal chain) and immediacy (e.g., the sooner the effect manifests) as criteria for assessing the relationship between cyber-cause and physical effect (Schmitt et al., 2013, p. 50).

³ For discussions about adding the cognitive domain as the 6th warfighting domain, see for example: Ottewell, 2020; Janson, 2018; and Elkins, 2019.

This work will likely take time. Academics began the process of defining cyberwarfare as early as in the 1990s (Ashraf, 2021, p. 275), and the first ethical analysis of this new kind of warfare was not published until 2010 (Dipert, 2010). There is no reason to think that dealing with similar issues within the cognitive domain should be a less comprehensive task.

12.3 THE CONDUCT OF WAR: THOUGHTS ON ISSUES RELATED TO *JUS IN BELLO*

The previous section of this chapter dealt some of the most critical issues related to *why* or *if* a war should be fought (*jus ad bellum*). This next section will briefly describe some implications of CogWar on the conduct of war, or the issue of *how* a war should be fought once it has been initiated (*jus in bello*).

One important topic in connection with the conduct of war, which is put under pressure in CogWar, is the issue of whom it is ethical to fight. In conventional war, non-combatants (those who take no direct part in the hostilities), are protected from both direct and collateral injuries. In other words, there should be no direct hostilities directed at civilian populations (Koskenniemi, 2006, para. 374). This is a principle which stands in direct contrast to one of the central elements of CogWar, namely that civilian populations often are the main targets of operations in the cognitive domain. How should this dilemma be approached?

This leads to another important question that needs answering: *Who is, and who isn't a combatant in the cognitive domain?* In traditional warfare civilians may be considered legitimate targets if they directly participate in hostilities. The issue of deciding who is and who is not a combatant in the cognitive domain, and consequently who should be considered legitimate targets, is a puzzling question for several reasons. One complicating aspect is that civilian actors are often used as proxies. One example is the use of PR agencies or influencers in influence operations (Aukia, 2021; Seitz, Tucker and Catalini, 2022; Henley, 2021).

Another prominent issue is that of the kind and degree of force it is ethical to use in different situations. The starting point of this discussion is the *in bello* proportionality principle, which governs the degree and kind of force used to achieve a military goal by comparing the military advantage gained to the expected damage caused to civilians and civilian objects. Taking into consideration that the effects of CogWar are usually not physical damage, how should this comparison be conducted?

12.4 CONCLUSION AND RECOMMENDATIONS FOR FUTURE RESEARCH

CogWar arguably represents a significant and new challenge to our moral and legal understanding of war. Consequently, there is a need for debate regarding how this new type of warfare should be regulated. More research on the normative and legal aspects of CogWar is essential. This should include questions regarding justifications for the resort to military force (*jus ad bellum*) and what may justifiably be done in the use of force (*jus in bello*).

This chapter has pointed to several specific research questions which should be explored to better our understanding of CogWar, as well as its implications for war ethics and international law. First: When should an action within the cognitive domain be considered an unlawful use of force (and potentially trigger the right to national self-defence)? One might begin by considering whether there are secondary effects, other than physical harm, which should be considered that may give rise to a *casus bello*. These issues may lead to another argument regarding whether a *conventional attack* can ever be a proportional response to an enemy cognitive *attack*.

It is also recommended that issues related to *jus in bello* are explored. Specific examples of potential research questions include: What defines who is and who is not a combatant in the cognitive domain? Who is a legitimate target in the cognitive domain? And lastly, how should *in bello* proportionality be evaluated, taking into consideration that the effects of CogWar are usually not physical damage?

In addition to supporting research efforts, NATO should organize a symposium to open the discussion for the development of policies, doctrine, and directives to guide the way ahead for the defence against CogWar. There are significant consequences for the potential abuse of information in the social media environment in CogWar.

Workshops should also be focused on the **Human Element of Cognitive Warfare** and how best to defend people legally and ethically from the influence and impact of CogWar. The workshop may reveal topics related to human fatigue, cognitive impairment, physiological and psychological impacts, stress, anxiety, attention deficit issues, etc., related to CogWar and pave the way to highlighting the results of CogWar that might otherwise remain hidden and unknown. Like the Havana Syndrome, the impact of cognitive attacks may be challenging to prove. Once the evidence is examined, the focus shifts to identifying the level of psychological harm or cognitive impairment and a defensive strategy can be developed to prevent, mitigate and defend against such attacks in the future. So too, there is a need to take a focused examination of the human element that is influenced negatively in CogWar. What are the consequences of such influence? How can we legally and ethically defend against the impact of CogWar? What level of CogWar crosses the Rubicon and defines it as an act of war to which we are legally responsible to defend? These questions must be addressed if we are to mitigate and defend against CogWar.

Lastly, we anticipate that as the level of sophistication increases in advanced technologies such as AI/ML and BMI designs, there will be an exponential increase in the level of adversarial activity to deploy CogWar attacks at an increasing rate. Therefore, it is important to ensure that education and training are done on a continuous basis to ensure military readiness to counter the effects of CogWar. We must advocate for changes in international law that define the parameters of an act of “CogWar”, and establish levels of response, penalty to counter and mitigate the unethical use of technology for CogWar purposes by potential adversaries against NATO forces.

12.5 REFERENCES

- Ashraf, C. (2021). Defining Cyberwar: Towards a Definitional Framework. *Defense & Security Analysis*, 37(3), pp. 274-294.
- Aukia, J. (June 2021). China as a Hybrid Influencer: Non-State Actors as State Proxies. The European Center of Excellence for Countering Hybrid Threats. [20210616_Hybrid_CoE_Research_Report_1_China_as_a_hybrid_influencer_Non_state_actors_as_state_proxies_WEB.pdf](https://hybridcoe.fi/research-reports/20210616_Hybrid_CoE_Research_Report_1_China_as_a_hybrid_influencer_Non_state_actors_as_state_proxies_WEB.pdf) (hybridcoe.fi)
- Bernal, A., Carter, C., Singh, I., Cao, K., and Madreperla, O. (2020). Fall 2020 Cognitive Warfare: An Attack on Truth and Thought. <https://www.innovationhub-act.org/sites/default/files/2021-03/Cognitive%20Warfare.pdf>
- Bjørgul, L. (03 November 2021). Cognitive Warfare and the Use of Force. Stratagem.
- Cook, J. (2010). “Cyberation” and Just War Doctrine: A Response to Dipert. *The Journal of Military Ethics* 9(4), pp. 411-423.

Dipert, R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics*, 9(4), pp. 384-410.

Eberle, C. (2013). Just War and Cyberwar. *The Journal of Military Ethics* Vol. 12(1), pp. 54-67.

Elkins, L. (2019). The 6th Warfighting Domain. OTH. <https://othjournal.com/2019/11/05/the-6th-warfighting-domain/>

Henley, J. (2021). Influencers Say Russia-Linked PR Agency Asked them to Disparage Pfizer Vaccine. *The Guardian*. <https://www.theguardian.com/media/2021/may/25/influencers-say-russia-linked-pr-agency-asked-them-to-disparage-pfizer-vaccine>

Janson, J. (2018). It's Time to Take the Human Domain Seriously. ISCYBERCOM is Our chance. OTH. <https://othjournal.com/2018/05/18/its-time-to-take-the-human-domain-seriously-uscybercom-is-our-chance/>;

Koskenniemi, M. (2006). Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law. United Nations. https://legal.un.org/ilc/documentation/english/a_cn4_1682.pdf

NATO. The North Atlantic Treaty (4 April 1949), Article 5, 63 Stat. 2241, 34 U.N.T.S. 243. https://www.nato.int/cps/en/natolive/official_texts_17120.htm

Ottewell, P. (2020). Defining the Cognitive Domain. OTH. <https://othjournal.com/2020/12/07/defining-the-cognitive-domain/>

Petkis, S. (2016). Rethinking Proportionality in the Cyber Context. *Georgetown Journal of International Law*. Vol 47, No. 4, pp. 1431-1458.

Roscini, M. (2010). Worldwide Warfare – “jus ad bellum” and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law* Vol 14, pp. 85-130.

Schmitt, M.N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

Seitz A., Tucker E., and Catalini M. (2022). How China’s TikTok, Facebook Influencers Push Propaganda. AP News. <https://apnews.com/article/russia-ukraine-eileen-gu-winter-olympics-technology-business-12de242ee53092693c0711b932c1da5c>

Silver, D. (2002). Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter. *International Law Studies* Vol 76, pp. 73-97.

Von Clausewitz, C. (1968). *On War*. Penguin Classics.



Chapter 13 – COGNITIVE WARFARE AND THE HUMAN DOMAIN: APPRECIATING THE PERSPECTIVE THAT THE TRAJECTORIES OF NEUROSCIENCE AND HUMAN EVOLUTION PLACE COGNITIVE WARFARE AT ODDS WITH IDEAS OF A HUMAN DOMAIN

Torvald F. Ask

Norwegian University of Science & Technology
NORWAY

Benjamin J. Knox

Norwegian Armed Forces Cyber Defence
NORWAY

13.1 INTRODUCTION

Advances in neuroscience combined with evolving technological, cyber, and social engineering capabilities converge to form novel methods of influencing human cognition. The potential for weaponizing these methods, to wage war on the cognitive integrity of a target population, has spawned a resurgence of attention to Cognitive Warfare (CogWar). What constitutes CogWar is currently ill-defined and the existing literature arguing for its novelty struggles to make a critical look at existing literature and challenges the wide-ranging and anthropocentric convincing distinction between CogWar and psychological and influence operations (e.g., Claverie et al., 2022). An alternative position found in the literature is that CogWar is an old form of warfare made relevant with novel weapons for influencing cognition at both tactical and mass levels (e.g., Canham et al., 2022; Dahl, 1996, pp. 23-34; Whiteaker and Valkonen, 2022).

While arguing for the novelty of CogWar, some authors have taken issue with the ‘Cognitive Domain’ as a domain of operations (Claverie and du Cluzel, 2022a, 2022b; Cole and Le Guyader, 2020; du Cluzel, 2020; Le Guyader, 2022). The general argument is that a Cognitive Domain is too restrictive as it does not sufficiently encompass the action space in which human thinking and behavior is being weaponized. For instance, one author asks whether the potential threat of biotechnologies and nanotechnologies are addressed by a Cognitive Domain, and whether an individual or a community can be “*solely defined by its cognitive capacities*” (Le Guyader, 2020, p. 3). To address the potential limits of a Cognitive Domain, the authors suggest that we are moving towards a ‘Human Domain’ of operations (Claverie and du Cluzel, 2022a, 2022b; Cole and Le Guyader, 2020; du Cluzel, 2020; Le Guyader, 2022).

This suggestion naturally begs the question of what exactly the Human Domain is. This chapter takes perspective of a ‘human domain’ as it does not a priori align with the trajectory of neuroscience and of human evolution in the context of CogWar. Instead, it argues for S&T approaches that focus on a cognitive domain, where CogWar attacks are directed and hence what needs to be protected.

13.2 THE HUMAN DOMAIN AS DEFINED IN THE LITERATURE

Cole and Le Guyader (2020) argue that the Human Domain is “*the one defining us as individuals and structuring our societies*” (p. 8) and that it is based on many sciences including (but not limited to) “*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 ...” (p. 8). They argue that these sciences are being weaponized by adversaries, that none of the sciences are addressed by other domains of operation and that a Cognitive Domain would not suffice to address them (Cole and Le Guyader, 2020).

One author (Le Guyader, 2020) argues that the Human Domain is based on the Social Sciences and Humanities (SSH), that the SSH do not fall naturally into the five existing domains but can be “*found, simultaneously, in all five current domains*” and that they “*precede, explain, and lead to all domains*” by providing the key ingredients to modern threats and by being “*both inside and outside*” of all domains thus encompassing them. The author then asserts that the “*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*” (Le Guyader, 2020, pp. 3-4).

In an article reviewing several of the threats facing human cognitive integrity (du Cluzel, 2020), the Human Domain was described as not being the military human capital but encompassing “*the human capital of a theater of operations as a whole (civilian populations, ethnic groups, leaders...), but also the concepts closely related to humans such as leadership, organization, decision-making processes, perceptions, and behavior.*” (p. 28). The article then suggests a tentative definition of the Human Domain of operations: “*the sphere of interest in which strategies and operations can be designed and implemented that, by targeting the cognitive capacities of individuals and/or communities with a set of specific tools and techniques, in particular digital ones, will influence their perception and tamper with their reasoning capacities, hence gaining control of their decision making, perception and behavior levers in order to achieve desired effects.*” (Du Cluzel, 2020, p. 33).

Two authors (Claverie and du Cluzel, 2022a, 2022b) argued that the “human enhancement networks”, brought about and facilitated by the increased interconnectedness between humans and information technology, are typical of the Human Domain “*where the ability to solve complex problems is dependent on how information is represented, understood and developed*” (Claverie and du Cluzel, 2022a, p. 7).

In short, and according to the literature, the Human Domain can be understood as everything that involves humans and human societies. It encompasses the cause and outcome of all warfare, and getting an asymmetric advantage requires knowledge in SSH as well as the hard sciences.

There are several issues with this domain as it is currently described. First and foremost, a domain where everything explains everything (like a model consisting of all variables) where one needs to know every SSH, and related science is hardly useful. A Cognitive Domain would be more useful in this regard because it indicates where attacks are directed thus what needs to be protected. Moreover, the explanations and definitions provided by du Cluzel (2020, p. 33) and Claverie and du Cluzel (2022a, p. 7) can be fully addressed by a cognitive domain. Most of the future threats addressed in the literature (du Cluzel, 2020; Le Guyader, 2020) are related to neurobiological and cognitive factors as well as information technology. Thus, to sufficiently address these threats, it will specifically require that focus is allocated to cognitive science, neuroscience, and information technology. One could also argue that the argument for moving towards a Human Domain is too anthropocentric in the sense that it may be a move in the opposite direction of the trajectory of neuroscience and of human evolution.

13.3 COGNITIVE WARFARE AND THE HUMAN DOMAIN: IS A HUMAN DOMAIN AT ODDS WITH THE TRAJECTORY OF NEUROSCIENCE AND HUMAN EVOLUTION?

Developments in neuroscience result from applying common principles for how molecules and materials interact, and how information is represented statistically. Some of these advancements are a result of being able to avoid the bias of thinking about cognition in a human (or anthropocentric) manner, and rather identify the statistical frameworks and models underlying the brain's ability to perceive and understand the world. Examples range from perceiving objects (Nirenberg and Pandarinath, 2012) to complex representations of physical space (Gardner et al., 2022). To understand the neuronal networks that give rise to these statistical models, neuroscientific researchers are developing tools that can be used to manipulate the networks. These tools combine material science with virus technology as delivery mechanisms; being human has little to do with it.

Another problem with conceptualizing an anthropocentric domain is the fact that humans are increasingly becoming cyborgs and merging with technology. At the most extreme, humans are getting implants and replacing organs to attain superhuman abilities (e.g., perceptual, kinetic, etc., Tsui, 2020). If humans are becoming less human over time it begs the question of how relevant a "Human Domain" will be in the future. Cognition is cognition regardless of whether it is occurring in a machine, a human being, or an animal belonging to another species. If one accounts for the possible trajectories that human evolution may take, one could argue that a Human Domain is more restrictive than a Cognitive Domain.

13.4 CONCLUSION AND FUTURE PERSPECTIVES

The conception of a Domain of Operations should be actionable by practitioners and not solely justify the existence of academic pursuits. A Human Domain as it is currently described in the literature is arguably too wide-reaching to be actionable. It is also not clear how it is better at addressing current threats than a Cognitive Domain. The trajectory of neuroscience (including cognitive neuroscience) and human evolution is arguably moving in the opposite direction of that of a Human Domain. To keep up with- and get ahead of the threats associated with these developments, as well as being at the forefront of research that can further understanding of the brain's ability to perceive and understand the world, efforts need to be directed towards S&T that facilitate this. Doing so can lead to anticipatory actions based upon the ability to make sense of how sensory input is transformed, reduced, elaborated, stored, recovered, and used. The outcome is the ability to apply improved and appropriate tools and methods and time relevant defensive strategies in the near and distant future.

Anthropocentric approaches may be a mistake as we risk losing sight of cognition as processes or actions, and how manipulations (positive or negative / offensive or defensive) to these can guide our behavior. The knowledge available in the current neuroscience literature is highly applicable and can be used to develop powerful neuro-ergonomic tools to manipulate brain physiology to alter how individuals experience and interact with the world. This information can be applied by non-academic individuals to improve brain function and optimize performance (e.g., increase dopamine receptors to improve motivation and grit). The same tools can be applied by adversaries to degrade brain function and performance (e.g., reduce dopamine or other neuroactive molecules that facilitate in-group coherence). These dual-use potentials need to be mapped out to effectively defend against them.

For the short term, the HFM-356 House Model can be used as a tool to critically assess existing [grey] literature and analyze perceived CogWar attacks. This will allow for more academic rigor to be applied regarding the how and when CogWar currently occurs, in peace, crises and war.

In mid-term, taking the lead from neuroscience and human evolutionary trajectories, in terms of the opportunities and consequences of human-machine integration, research should proceed by avoiding the biases of ‘humanizing’ CogWar effects and instead focus on the cognitive vectors that become available to affect behavior change. In other words, identifying the how and when can it occur.

Lastly, for the longer term, close collaboration with intra-disciplinary neuroscientists and neuroscience labs (e.g., labs and researchers that has experience with computational-, social-, cognitive-, human-, molecular- and cellular neuroscience, and in using nanotechnological and other material science methods) will be necessary to both get a sufficient SA of the current dual-use potential of neuroscientific tools and for developing sufficient defensive strategies. For instance, understanding how current virus- or molecular-based tools can be applied to manipulate human cognition (e.g., increase the likelihood of risk-taking behaviors) may provide tools for both detecting and molecularly countering such cognitive attacks. This collaborative approach needs to be combined with academically ‘plugging into’ industry technology developers to help understand how developing technologies can facilitate or interact with molecular or more indirect (yet neuro-ergonomic) methods for attacking cognition.

13.5 REFERENCES

Canham, M., Sütterlin, S., Ask, T.F., Knox, B.J., Glenister, L., and Lugo, R. (2022). Ambiguous Self-Induced Disinformation (ASID) Attacks: Weaponizing a Cognitive Deficiency. *Journal of Information Warfare*, pp. 1-17, in press.

Claverie, B., and du Cluzel, F. (2022a). The Cognitive Warfare Concepts. NATO ACT Innovation Hub. Retrieved from: https://www.innovationhub-act.org/sites/default/files/2022-02/COGWAR%20article%20Claverie%20du%20Cluzel%20final_0.pdf

Claverie, B., and du Cluzel, F. (2022b). Cognitive Warfare: The Advent of the Concept of “Cognitics” in the Field of Warfare. In Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. Cognitive Warfare: The Future of Cognitive Dominance. NATO STO, Neuilly-sur-Seine, France., pp. 2, 1-7, 2022, 978-92-837-2392-9. Retrieved from: <https://hal.univ-lyon2.fr/IMS-BORDEAUX-FUSION/hal-03635889v1>

Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. (2022). Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 20201. NATO STO, Neuilly-sur-Seine, France, pp. 8, 1-6. Hal-03635930. Retrieved from: <https://www.innovationhub-act.org/sites/default/files/2022-03/Cognitive%20Warfare%20Symposium%20-%20ENSC%20-%20March%202022%20Publication.pdf>

Cole, A., and Le Guyader, H. (2020). NATO Sixth’s Domain of Operations. FICINT document. Norfolk (VA, USA): NATO ACT Innovation Hub. Retrieved from: <https://www.innovationhub-act.org/sites/default/files/2021-01/NATO%27s%206th%20domain%20of%20operations.pdf>

Dahl, A. B. (1996). Considering a Cognitive Warfare Framework. Command Dysfunction: Minding the Cognitive War, Air University Press: Montgomery, AL. Retrieved from: <http://www.jstor.com/stable/resrep13807.9>

Du Cluzel, F. (2020). Cognitive Warfare. NATO ACT Innovation Hub. Retrieved from: https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_COGWAR%20Final.pdf

Gardner, R.J., Hermansen, E., Pachitariu, M. et al. Toroidal Topology of Population Activity in Grid Cells. Nature 602, pp. 123-128 (2022). DOI: 10.1038/s41586-021-04268-7.

Le Guyader, H. (2022). Cognitive Domain: A Sixth Domain of Operations? In Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. (2022) Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 20201. NATO STO, Neuilly-sur-Seine, France, pp. 4, 1-17, 2022, 978-92-837-2392-9. fffhal-03635907f. Retrieved from: <https://hal.archives-ouvertes.fr/hal-03635898/document>

Nirenberg, S., and Pandarinath, C. (2012). Retinal Prosthetic Strategy with the Capacity to Restore Normal Vision. Proceedings of the National Academy of Sciences of the United States of America, 109(37), pp. 15012-15017. DOI: 10.1073/pnas.1207035109.

Tsui, K. (27 May 2020). Transhumanism: Meet the Cyborgs and Biohackers Redefining Beauty. CNN. <https://edition.cnn.com/style/article/david-vintiner-transhumanism/index.html>

Whiteaker, J., and Valkonen, S. (2022). Cognitive Warfare: Complexity and Simplicity. In Claverie, B., Prébot, B., Beuchler, N., and du Cluzel, F. (2022) Cognitive Warfare: The Future of Cognitive Dominance. First NATO Scientific Meeting on Cognitive Warfare (France) – 21 June 20201. NATO STO, Neuilly-sur-Seine, France, pp.4, 1-17, 2022, 978-92-837-2392-9. Retrieved from: <https://hal.archives-ouvertes.fr/hal-03635948/document>



Chapter 14 – SCIENCE AND TECHNOLOGY ROADMAP BASED ON THE HOUSE MODEL

Janet M. Blatny

Norwegian Defense Research Establishment
NORWAY

Yvonne R. Masakowski

US Naval War College
UNITED STATES

14.1 INTRODUCTION

The HFM-ET-356 has proposed a S&T Roadmap on “Mitigating and Responding to Cognitive Warfare”. The intent was to increase understanding of CogWar and identify S&T that would increase NATO’s and each nation’s ability to defend against it. The process of understanding CogWar enables identification of key areas where S&T can support and affect how NATO’s and Allied nations improve deterrence capabilities and to ensure military readiness and collective defence capabilities (NATO Strategic Concept, 2022). Ensuring military readiness and collective defence capabilities in the context of CogWar will increase military resilience and provide more effective approaches to cognitive security.

There will be second and third order effects that cascade through societies due to the immediate and/or longer-term effects of CogWar. Civil unrest, civil conflicts and political upheavals reflect the influence of CogWar such as evidenced by the COVID-19 pandemic, the US Congressional riots and the Russia invasion of Ukraine. NATO nations must prepare the warfighter to meet the demands of future CogWar effects via education, training, and technology development.

The “House Model” (Figure 14-1) provides an illustration of the cross-cutting multidisciplinary topics that need to be addressed in this regard. The scientific fields that overlap and/or intersect with critical applied operational military dimensions of CogWar, such as enabling technologies, *modus operandi*, cognitive effects, and processes of sensemaking, and SA, represent a critical aspect of this report. NATO must be prepared to understand and address the potential impact along these convergent S&T areas, as adversaries will most surely view them as vulnerabilities and opportunities for further exploitation. Each of the horizontal bars in the model has the potential to enable the emergence of disruptive military capabilities. This report focuses on the assessment of S&T topics and their potential impact on future NATO military operations.

The S&T roadmap guides:

- Technological and socio-technological efforts necessary to give NATO nations the advantage when faced with dangerous and unpredictable security threats, and opportunities presented by CogWar and its associated processes and activities.
- NATO in the development of its CogWar S&T defence strategy, policies, doctrine, and directives to deter, identify, and defend against CogWar.

The S&T road map is further aligned with NATO’s S&T priorities, “Advanced Human Performance and Health,” “Cultural, Social & Organizational Behaviors”, “Information Analysis & Decision Support”, (NATO, 2016).

The “House Model” (Figure 14-1) presents principal topics of S&T pertaining to CogWar. It serves as a strategic framework for developing short- and long-term perspectives on research programs, depending upon S&T knowledge requirements concerning own or adversarial approaches. By illustrating the multidisciplinary scientific topics and the intersection of these key areas, the model serves as a tool for guiding increased S&T investments.

SCIENCE AND TECHNOLOGY ROADMAP BASED ON THE HOUSE MODEL

When the House Model is viewed with the Observe, Orient, Decide, and Act (OODA) decision cycle model, it is possible to gain further insight and understanding of the cooperation between the evolution of science and the operational military community (Figure 14-2 and call-out box, below).

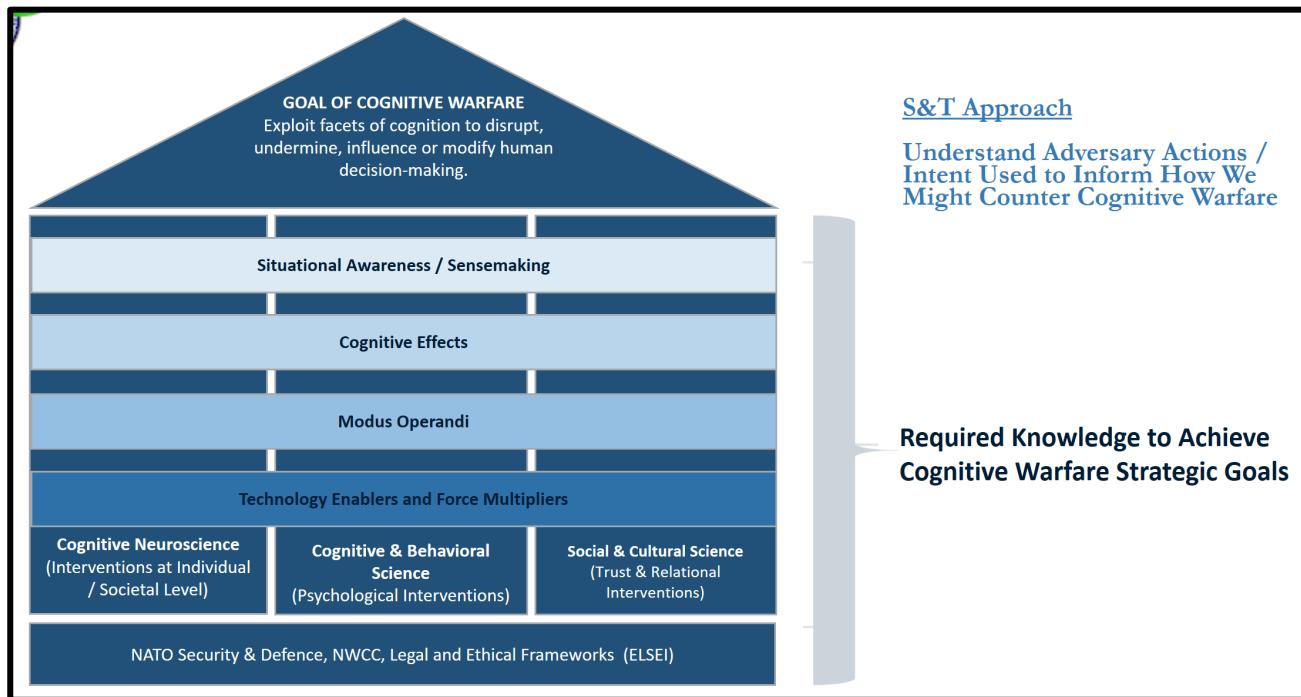


Figure 14-1: The House Model Proposed by HFM-ET-356.

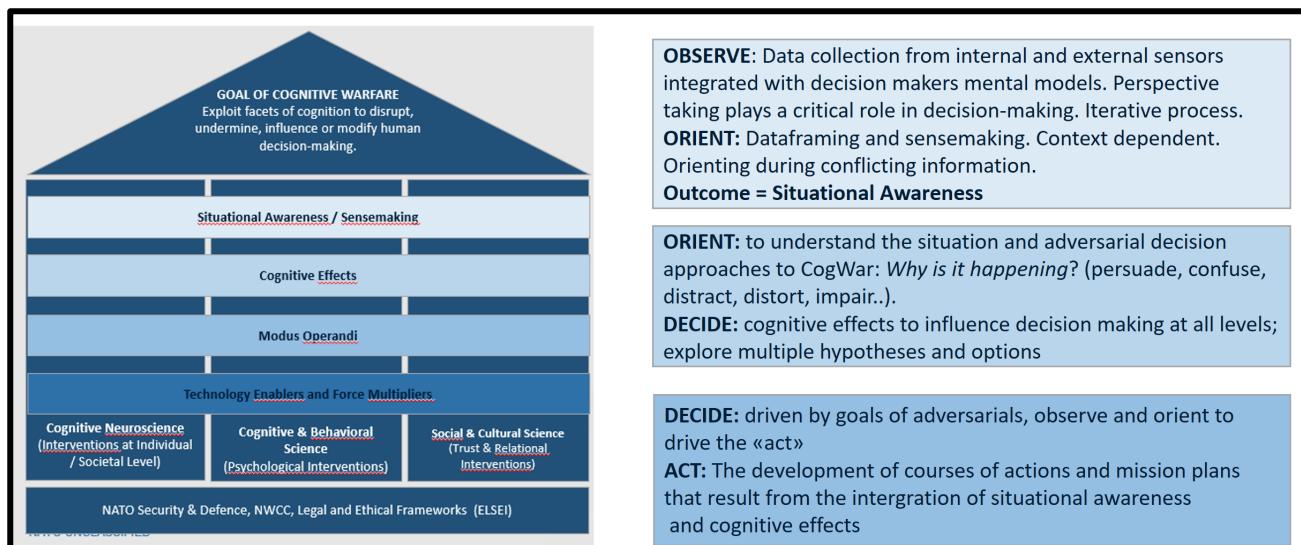


Figure 14-2: The Link Between the House Model and the Observe, Orient, Decide and Act (OODA) Loop.

Enablers and Force Multipliers

Situational Awareness (SA) / Sensemaking: Examination of the factors that enable or block attempts to make sense of an ambiguous situation. Sensemaking informs and is a prerequisite to decision making. It requires trusted data input, evaluation of meaningful information, integration with knowledge and experience to achieve an understanding of evolving non-linear events.

Cognitive Effects: Describes the effects an actor may try to create on a target audience IOT achieve desired goal. Could be doctrinal effect verbs, e.g., distort, distract, etc., or more elaborate descriptions, e.g., degrade TA's trust in democratic institutions or politicians, persuade TA to believe A instead of B, etc. Related to neurobiology the effects could be to, for example, injure or impair cognitive functions, stimulate emulative functions, or trigger social contagion.

Modus operandi: Examination of adversary methods and stratagems to generate the desired effect on the target/target audience, including when methods/stratagems are employed to exploit 'cognitive openings' and other opportunities for intervention (i.e., how and when). This effort is also concerned about the synchronization of activities by adversaries to psychologically prime and target. A better understanding of when and how adversaries conduct CW provides insights on the development and validation of countermeasures and defensive strategies.

Technology Enablers and Force Multipliers: Use technology to enable the actor to utilize one, two or all of the three knowledge pillars simultaneously, in pursuit of the goal. This aspect enables the above aspects. e.g., EDTs ICT CIS / Big Data / AI & ML / Social Media / Directed Energy / Biotech / Nanotech, etc.

Technological developments in areas such as AI/ML, BMI, system integration, modelling, quantum computing, adaptive algorithms, neuroscience, biotechnology, human enhancement, and human augmentation will have significant impact on the future of conflict and competition. Individually these developments present both performance opportunities and challenges (NATO S&T Trends, 2020) across all operational domains. The intersection of these advances in technology will yield new military capabilities giving operational and strategic advantage, as well as potentially unforeseen disruptive effects. The integration of advanced technology and systems within the social, organizational, and cultural environment will contribute to the complexity of CogWar.

It is important NATOs gains a better understanding of the vulnerabilities and exploitability of technology, digital eco-systems, human cognition, and other human vulnerabilities that can be targeted by adversaries to manipulate and shape human understanding, behaviors, and decision making. S&T will remain a strategic imperative as technologies continue to advance and evolve, contributing to new methods of CogWar.

14.2 OVERVIEW OF OVERALL FUTURE S&T AREAS

Chapters presented in this report reflect an analytical discussion of S&T topics, military operational requirements, and their relevance and importance in the defence against CogWar as illustrated in each pillar and horizontal bar of the House Model (Figure 14-1). The House Model may be read top-down (defensive perspective or bottom-up (offensive perspective). The HFM-356 Team focused solely on the defensive perspective.

The Three pillars identify the fields of knowledge required to influence a Target Audience (TA). These are **Cognitive Neuroscience** (how brain functions to integrate an individual's knowledge, experience, and information to make an informed decision), Cognitive and Behavioral Science (psychological knowledge related to sensemaking, decision making, which may be influenced by aspects of human behavior) and **Social and Cultural Science** (socio-technical mechanics of individuals/societies, psycho-social effects, interventions). The horizontal bars identify enablers and force multipliers of the knowledge pillars: the SA and Sensemaking factors, the Cognitive Effects, the *modus operandi*, and the specific Technology Enablers and Force Multipliers. The horizontal aspects show the interdependence between the pillars of knowledge. They also present opportunities to consider the “**how and when**” S&T knowledge needs.

The triangle at the top states the Goal of CogWar on an individual and societal level according to the HFM-ET-356. “The goal of CogWar is to exploit facets of cognition to disrupt, undermine, influence or modify human-decision making.” Changing perception or cognitive capability is a means to an end, the end being creating favorable conditions for achieving own strategic goals.

The fundamental bar represents strategic, ethical and legal guidelines for NATO security and defence.

14.3 COGNITIVE NEUROSCIENCE, BEHAVIORAL, AND SOCIAL AND CULTURAL PILLARS

14.3.1 Pillar One: Cognitive Neuroscience

Pillar One is concerned with the micro-cognitive methods that affect cognitive abilities such as sensemaking and decision making. These cognitive processes are equally context sensitive and must adapt to situational complexity. Cognition is a complex process as it reflects brain functions that integrate an individual's knowledge, experience, and the information processed to make an informed decision. There are cognitive constraints that may interfere with these processes such as fatigue, cognitive bias, and emotion. Adversaries may influence each of these cognitive processes at multiple levels such as biological, mechanistic, and socio-technical influences.

There is extensive research in Brain-Machine interfaces (BMI) to support military operations and the neuroscience and brain research chapter (Grigsby and McKinley, Chapter 6) summarizes the development and evolution of enhanced BMI capabilities. As BMI research advances, there is the potential for intrusion, manipulation, and modification to human cognitive processes, as well as adversaries inducing deliberate emotional and behavioral responses to achieve their objectives. While BMI systems are designed to reduce cognitive workload and enhance attention and vigilance capabilities, such advances do so at increased cognitive risk. The evolution of BMI will yield further opportunities for adversaries to conduct CogWar on a new level. There is a need to develop defence systems that guard and defend against malevolent data input into the human BMI as adversaries may target human attention and emotional responses to alter behaviors in support of their military objectives. *The subjective experiences of those equipped with BMI to facilitate optimized cognitive performance and enhanced Situational Awareness must be investigated from a defensive perspective to ensure that vulnerabilities, biases and potential harm are not being introduced.* The BMI connectivity to command and control is further elaborated in Chapter 14.3.4. Nations must anticipate the evolution of the CogWar battlespace with a focus on ensuring the safety and security of individuals, warfighters, and the civilian population, as well as future military command and control systems and ensure national resilience.

CogWar also addresses the impact of advanced neuroweapon attacks such as the “Havana Syndrome” attack of US Embassy personnel in Cuba (Dilanian, 2022; Giordano, 2021, 2022; Moore, 2022; Terra, 2021). Symptoms

such as memory loss, lack of cognitive processing capabilities, fatigue, dizziness, et al., are among the symptoms experienced by Embassy personnel. Cognitive impairments, whether temporary or long term, reflect the need to invest in the development of tools and technologies that will detect, deter, and defend against the weapons of CogWar.

14.3.2 Pillar Two: Cognitive and Behavioral Science

The Cognitive and Behavioral Science (CBS) pillar represents the psychological knowledge related to sensemaking, and decision making, which may be influenced by aspects of human behavior such as communication, affect, and persuasion. As CogWar targets human vulnerabilities, it is easy to recognize the potential for manipulation in this regard.

Researchers need to assess the gaps and vulnerabilities along these dimensions and find novel approaches to defending information networks and human cognitive capacities. NATO nations need to understand the elements in the OODA-loop decision chain (Chapter 9) and determine how best to defend decision making and socio-cultural attacks and manipulations at all levels (Figure 14-2). For example, SA and sensemaking are linked within the first “O” of the OODA-Loop and refers to the “Observe” phase. During the Observe phase, it is important to learn what is happening and gain clarity regarding the meaning, motivation, and uncertainty of the situation (Chapter 9).

14.3.3 Pillar Three: Social and Cultural Science

The application of interdisciplinary methods to better understand structural and institutional factors in social, cultural, economic, and political contexts that uphold, shape, constrain and/or empower individual and collective behavior is needed. The social and cultural sciences offer insight into and can help inform the development of both offensive and defensive facets of CogWar, particularly at the meso- and macro- levels of analysis (i.e., characteristics of social interaction between groups and organizations through large-scale societal interactions).

Pillars Two and Three are concerned with macro-cognitive problems, such as anticipating events and adapting to dynamic contexts, uncertainty, and increased complexity. Where cognition can be individual or shared among individuals (e.g., teams, organizations, society), it is a macro-cognitive issue. Micro-cognitive research may benefit by being contextualized by macro-cognitive theory and method (Klein, et al. 2003).

Chapter 4 provides a comprehensive list of theories related to the social and cultural aspects related to CogWar. These theories facilitate our understanding of the role of socio-cultural aspects that may be used to influence and shape CogWar. However, the following suggestions are potential areas of investigation to better understand how to counter the impact of CogWar along the Social and Cultural Science pillar (Lauder, Chapter 4).

- Countering amplification and exploitation of social and political divides.
- Countering dissemination of rumors, gossip, and disinformation to generate mass anxiety and uncertainty.
- Countering exploitation of cognitive errors in decision making – the maskirovka/operational masking used to gain indirect control of a target’s decision-making process.
- Building societal resilience to disinformation.

The socio-cultural aspects of warfare are relevant for the conduct of CogWar. Russia “justified” the invasion of

the Ukraine as an act of defending Russian citizens from a Ukraine Nazi movement that threatened Russia's citizens. This manipulation of social and cultural aspects serves as a tool to be weaponized by adversaries in CogWar. It remains for nations to understand how adversaries may use these theories and practices as weapons for conducting future CogWar.

14.4 SENSEMAKING AND SITUATIONAL AWARENESS: PRECURSORS TO ACHIEVING DECISION SUPERIORITY

The Sensemaking, SA bar illustrates its role in the OODA-loop decision-making framework (Chapters 8 and 9) and the importance of integrating information that is trustworthy, reliable, and emanates from a valid and certified source. Adversaries are conducting information warfare and psychological operations across all elements and domains of information platforms. Data poisoning of datasets being used to train ML algorithms highlights the need to develop software tools to defend against the introduction of uncertified, poisoned datasets. Thus, it is important to ensure that the tools and technologies used in *a priori* steps for human sensemaking and SA processes are based upon accurate data.

John Boyd's OODA-loop (Chapter 9) (Figure 14-3) germinated from the iterative, adaptive decision-making processes experienced by fighter pilots in military combat operations. The model describes the interaction of the human's perceptions and cognitive processes related to observing, orienting, and modifying according to dynamic changes in the environment. Pilots in such dynamic air combat settings had to continually modify their actions. Such agile, adaptive behavior is humanistic and facilitates cognitive processes that are essential for survival in a combat environment. So too, human cognitive resilience is essential for decision making across all domains. In addition, such adaptive behavior extends to human-human teams, as well as human-machine teams. Indeed, human-machine teaming is an important element within the OODA-decision cycle loop. Chapter 9 on human-machine teaming highlights the need to understand CogWar from the individual perspective, the team level, as well as understand the adversaries' perspectives.

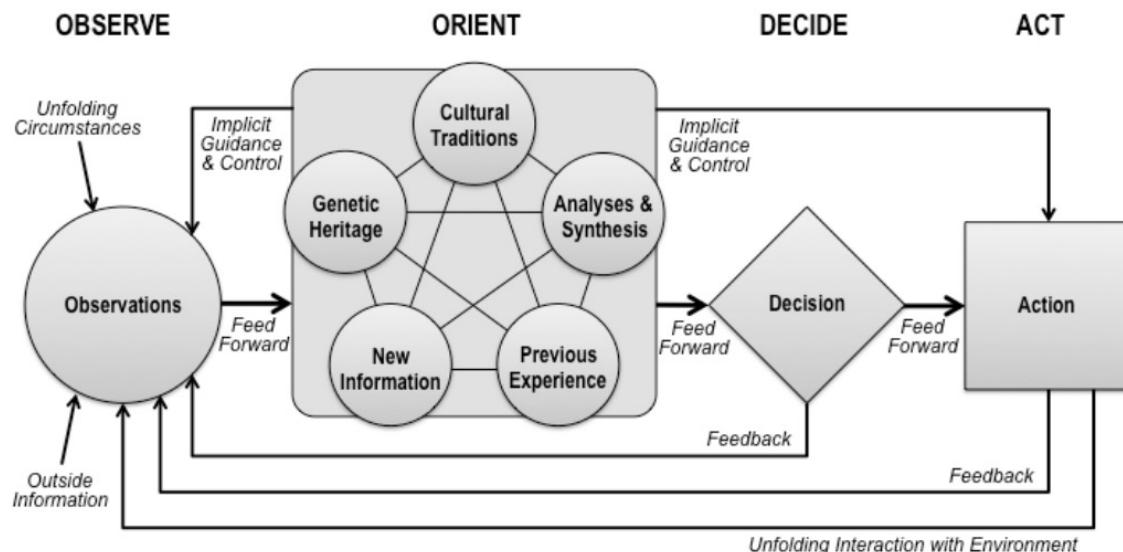


Figure 14-3: OODA-Loop of Observation-Orientation-Decision-Action (Boyd's).

14.5 COGNITIVE EFFECTS AND *MODUS OPERANDI*

The second bar, ‘Cognitive Effects’ relates to the second “O” (i.e., Orient) in order to understand the situation and the adversaries’ decision approach to CogWar. *Why is it happening?* Adversaries design CogWar to their strategic advantage and aim to create chaos, confusion, disruption, distortion and undermine democracies and social order.

Modus operandi is the deliberate, rigorous, and scientifically informed examination of methods, stratagems, and other patterns of behavior designed and operationalized by adversaries to generate the desired psycho-social effect on an audience, including activities employed to psychologically prime and create cognitive openings and other opportunities for adversarial intervention (i.e., pre-propaganda). *Modus operandi* is not limited in scope to the examination of specific tactics or tools, such as using a loudspeaker or a fraudulent social media account but is concerned with the holistic application and synchronization of a range of methods and resources across the dimensions of the information environment.

The *modus operandi* in the third horizontal bar is linked with the “D” (i.e., Decide) course of action. How to counter CogWar? What methods and strategies might be employed to undermine, mitigate, interfere with CogWar? How to reduce risks associated with defence against CogWar and minimize second and third order effects?

14.6 TECHNOLOGY ENABLERS AND FORCE MULTIPLIERS

The Technology Enabler and Force Multipliers, the fourth horizontal bar, links with the entire OODA loop. Technology enables the user (or the adversary) to take advantage of all three pillars in pursuit of their goal.

ICTs have changed warfare, not least with regards to enabling actors to infiltrate the cognitive dimension of the IE more effectively. Malign actors are systematically employing overt and covert influence and interference methods to shape and manipulate the SA and decision-making process on all levels – from the international political level to the military strategic, operational, tactical and sub-tactical level. Even in remote and less developed areas, most people have Internet access, smartphones and social media accounts. This enables them to document and share observations and information about their surroundings including military equipment, troop movements and tactics. In addition, most troops have social media accounts, even if they may not use their devices on the battlefield. Commercially available drones, facial recognition software, AI, geo-tagging and satellite imagery have added another layer of both risks and opportunities to be analyzed, mitigated and exploited by all parties, civilian and military, in areas of conflict.

The permeation of ICTs in the AO poses obvious risks to operational security (OPSEC), information security (INFOSEC) and freedom of maneuver for any part in any conflict. For example, in the aftermath of the downing of Malaysian Airlines MH17 over Ukraine in 2014, Bellingcat was able to identify and document Russian personnel, equipment, tactics and locations using operational security intelligence (OSINT) techniques including mapping of videos, images and social media accounts belonging to both civilians and Russian troops.¹ For all parts of an armed conflict today, ICTs offers vast opportunities for intelligence gathering, improved SA, battle damage assessment, shaping of the battlefield and deception. However, as with all technology, the flipside of increased opportunity is increased risk.

¹ <https://www.bellingcat.com/news/uk-and-europe/2019/06/19/identifying-the-separatists-linked-to-the-downing-of-mh17/>

Other examples of technological enablers are AI/ML, adaptive algorithms, autonomous systems, system integration, unmanned systems, digital/cyber networks, modelling, quantum computing, deep fakes, neuroscience, facial recognition, biotechnology and human enhancement/augmentation (Chapter 5).

Below are examples of how technological enablers can impact CogWar.

14.6.1 Adaptive Command and Control, Brain-Machine Interfaces and SA

The development of adaptive command and control networks and systems will offer distinct advantages for future military operations. The BMI will enable the development of an agile command and control (C^2) capability (Chapter 7). These advantages do not come without risk. Whereas the advanced C^2 environment can facilitate enhance connectedness across all domains, cyber, space, maritime, land and air, and in a full multinational context, technology alone cannot ensure total defence and security. There are societal, cultural, organizational, political, and global challenges to be met, as well as considering that humans are part of all operations (human factors).

The NATO's defence and information environment must address the vulnerabilities associated with BMI's that will become part of the global C^2 environment (Chapter 6). This entails understanding the complexity of the operational and information environment in which these BMI systems will be employed, and their interactions with the entire system; people/individuals, society, organizations, technology, and their respective policies, legal and ethical constraints (Chapter 12) also to guide military personnel and ensure the safe distribution of such technologies. As military personnel become equipped with embedded BMI, there is a need to develop defence mechanisms to ensure the security of brain interfaces to defend against hacking of these systems at a system, group and/or at an individual level. AI/ML technologies and BMI will continue to be designed to augment human capacities including cognitive, sensory, and physical abilities. However, there is a need to address the safety and security of such advances that may have potential long-term impact on the cognitive processes and health of the individual.

The call-out box below provides an example of technological advances within brain research and its ethical/legal implications relevant for CogWar measures and that will have an impact on the development of future adaptive C^2 network (Binnendijk, Marler, and Bartels, 2021).

Example of Technological Advances within Brain Research Relevant for CogWar Measures.

Brain research has yielded advances in the treatment of patients with Parkinson's disease with brain interfaces to facilitate psychomotor response, that is used for Deep Brain Stimulation (DBS) (Arlotti, et al. 2021). The intersection of the multidisciplinary sciences such as cognitive science, neuroscience, and genomics will give rise to new medical treatments to minimize the effects of Alzheimer's, Multiple Sclerosis, et al., as well as give rise to advances in BMIs that soldiers will be equipped with for specific knowledge, skills, and abilities. This may sound like science fiction; however, the reality of such transformational technology lends itself to dual-use design that is continuously being exploited by China, which has already conducted human experimentation to create biologically enhanced super soldiers (Dilanian, 2020). Rather, each technological advance in neuroscience, brain science, genomics and BMI is examined for its dual-use application in China's military defence arsenal. NATO nations abides by ethical requirements to ensure human subject safety and seek to identify potential medical treatment benefits associated with technological advances.

C² must be considered within the complex socio-political- technological system as technologies evolve within the geopolitical and societal environments and are used by people within the framework of their respective organizations. Thus, command and control systems consisting of with AI/ML algorithms and BMI connected to individual soldiers, become part of a matrix of national and international security systems that are vulnerable to adversarial manipulation, hacking, and cyber/cognitive attacks.

Digital AI/ML networks must be capable of self- defence and detect, deter intrusions from external networks aimed at manipulating, poisoning data, and/or regulating the networks themselves. The C² environment is one that is robustly designed as a collection of C² nodes which provides access to information, aimed at sharing and distributing information within the network. *It is essential to ensure the security of such networks to avoid and mitigate any vulnerabilities such as data poisoning, networks, manipulation of information and attacks within the networks themselves.*

Building an understanding of the situation requires analysis and data framing, testing hypotheses along a range of perspectives to ensure an accurate understanding of events as they develop, adapting to changes in the environment and maintaining the ability to share awareness among NATO nations.

14.6.2 Human-Machine Teaming and Training

Chapter 9 on human-machine teaming highlights the need to understand CogWar from the individual perspective, as well as understanding the adversaries' perspectives. Human-machine teaming will enhance military capabilities and speed information dissemination, analysis, and decision making. War gaming, joint military exercises, and simulated virtual war gaming exercises provide a means for the military to gain experience with these advanced technologies, as well as assess their shortcomings, and human relationship (cognition). At the operational level, it is critical to understand the capabilities and shortfalls of these technologies. The range of human actors, adversaries, enemies, and adversarial AI intelligent agents may also need to play a role that should be included in these wargaming exercises. For the military leader, there are potentially ethical and moral consequences related to the deployment of future weaponized, autonomous systems that may yield unintended second and third order consequences. All aspects of war gaming should be exercised as part of military training and education.

Military personnel must also be educated in the development of critical thinking skills, the influence of cognitive biases and how to overcome these, as well as trained in the development of analytical skills for effective decision making. Their failures will teach them to recognize the impact of their cognitive biases and help them to become more aware of the impact of perceptual and cognitive biases that mislead and misinform them in their decision making.

There is a need to develop adaptive, applied training tools that will provide users with hands-on experience that can be used on an individual level, as well as shared with teams and/or across organizations to develop skills to counter the impact of CogWar misinformation and disinformation campaigns. Training tools (Chapter 11) that can be shared with organizations provide unique benefits associated with the training of teams and groups of people that can gain insight and expertise on propaganda, disinformation/misinformation, PsyOps, and InfoOps campaigns.

14.7 ETHICAL AND LEGAL IMPLICATIONS

As future military environment unfolds, replete with advanced technologies, human performance and challenges in the CogWar environment, there is a need to consider ethical and legal challenges associated with the deployment of technology as part of decisions made by humans. For example, those associated with the

deployment of weaponized, autonomous systems, and advanced robots making decisions formerly made by humans (Chapter 12). The ground and fundamental bar in the House Model addressing ethical and legal policies and guidelines needs to consider such aspects.

Policies related to the role and ethical and legal responsibilities of military personnel working in fast tempo operations where human-machine teaming collaboration is aimed at reducing workload and accelerating the decision cycle (Chapter 14.3) should be developed. What happens when things go wrong, and the intelligent AI-enabled machine made the error? How to handle the collateral damage of such errors? These are but a few of the ethical and legal questions raised that must be addressed by policy makers, doctrine authors and war game designers, and allow humans the opportunity to gain experience and insight regarding how best to work in human-machine teams ethically and effectively (Chapter 12). NATO may need to address some of these initiatives as formal doctrine in the future C² environment as netted BMI systems may become an integral part of the future C² environment.

Several strategic documents outline the need and goal for defending against CogWar and lay at the foundation of the House Model (i.e., the bottom horizontal bar: “NATO Security and Defence, NWCC, and Legal and Ethical Frameworks (ELSEI)”). Among these documents, are the NATO Warfare Capstone Concept (NWCC) and therein, the Warfare Development Initiative Cognitive Superiority. The ethical and legal aspects, as well as the Conduct of War and Law of Armed Conflict (von Clausewitz, 1968, and UN Charter, should be considered when combating CogWar (Chapter 12).

14.8 CONCLUSION AND RECOMMENDATIONS

This roadmap report summarizes the intersection of S&T topics illustrated by the House Model that require further investment in the development of human skills and advanced technologies to defend against CogWar. It is also critical to address the need for the E&T of military personnel to learn how best to implement, integrate and ethically deploy autonomous systems, advanced AI/ML digital networks etc. into the operating environment. There is also a need to develop the ethical and legal policies, directives, and guidance necessary for the ethical deployment of advanced technologies in the defence against future CogWar.

The S&T road map provides a means of examining the House Model linked with the OODA decision loop. The goal of the CogWar is to exploit facets of cognition to disrupt, manipulate, influence or modify human decision making. Defence against CogWar calls for S&T activities involving the following cross-cutting areas:

Pillars:

- Cognitive Neuroscience (Including AI/ML, et al.);
- Cognitive and Behavioral Science; and
- Social and Cultural Science.

Bars:

- Situational awareness and sensemaking;
- Cognitive effects;
- *Modus operandi*; and
- Technology and force multipliers.

Recommendations for S&T investment will be discussed further in Chapter 15.

14.9 REFERENCES

Arlotti, M., Colombo, M. Bonfanti, A., Mandat, T., Lanotte, M.M., Pirola, E., Borellini, L., Rampini, P., Eleopra, R., Rinaldo, S. Romito, L., Janssen, M.L.F., Prior, Al, and Marceglia, S. (2021). A New Implantable Closed-Loop Clinical Neural Interface: First Application in Parkinson's Disease. Retrieved July 18, 2022, from: <https://www.frontiersin.org/articles/10.3389/fnins.2021.763235/full>

Binnendijk, A., Marler, T., Bartels, E.M. (2021). Brain-Computer Interfaces: US Military Applications and Implications, an Initial Assessment. RAND Corporation. Retrieved 18 July 2022, from: https://www.rand.org/pubs/research_reports/RR2996.html

Dilanian, K. (2022). Havana Syndrome Symptoms in Small Group Most Likely Caused by Directed Energy Attacks Says US Intel Panel of Experts. Retrieved July 18, 2022, from: <https://www.nbcnews.com/politics/national-security/havana-syndrome-symptoms-small-group-likely-caused-directed-energy-say-rcna14584>

Giordano, J. (2021). Nations Must Come Together to Tackle Havana Syndrome. Retrieved August 2022 from: <https://www.nationaldefensemagazine.org/articles/2021/10/15/nation-must-come-together-to-tackle-havana-syndrome>

Giordano, J. (2022). Embassy Encephalopathy: Findings, Effectors, and Ethical Address. Video Presentation at UTSW's Havana Syndrome Webinar. February 11, 2022. Retrieved August 2022 from: https://www.youtube.com/watch?v=ix_Kscvk-6g

Klein, G., Ross, K.G., Moon, B., Klein, D.E., Hoffman, R. and Hollnagel, E. (2003). Macro-Cognition. Intelligent Systems, IEEE. 18. 81-85. 10.1109/MIS.2003.1200735.

Moore, T. (2022). For Your Ears Only: What Is Really Behind Havana Syndrome. Retrieved August 2022 from: <https://www.smh.com.au/national/for-your-ears-only-what-s-really-behind-havana-syndrome-20220506-p5aj70.html>

NATO (2016). AC/323-D(2016)0008-COR1 (INV). 2017 NATO Science & Technology Priorities.

NATO (2022). NATO Strategic Concept 2022. Adopted at the Madrid Summit, 29 – 30 June 2022. <https://www.nato.int/strategic-concept/index.html>

NATO STO (2020). NATO Science &Technology Trend Report, 2020. Science & Technology Trends 2020 – 2040. Exploring the S&T Edge. NATO Science & Technology Organization. NATO Science & Technology Organization, Neuilly-sur-Seine, France. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

Terra, J. (2021). Havana Syndrome the Perfect Disease for a Post-Truth World. Retrieved August 2022 from: <https://balkaninsight.com/2021/11/30/havana-syndrome-the-perfect-disease-for-a-post-truth-world/>

Von Clausewitz, C. (1968). On War. London: Penguin Books.



Chapter 15 – CONCLUSION AND RECOMMENDATIONS

Janet M. Blatny

Norwegian Defense Research Institute
NORWAY

Yvonne R. Masakowski

US Naval War College
UNITED STATES

15.1 INTRODUCTION

Cognitive Warfare (CogWar) presents an emerging battlespace used to influence and shape global security environments in novel ways.

Defensive CogWar must be approached from a socio-technical systematic perspective, including technological developments, as well as human and organizational factors.

The next decade will produce advances in AI/ML technologies that will significantly alter the conduct of war and impact how NATO conducts military operations. CogWar is not new, but what is emerging is an area of operations that needs to be understood and a more nuanced, academic, and operational picture of the full extent of its current capabilities and future potential must be established. This includes how CogWar shapes the geopolitical environment, affects military operations, impacts global economics, commercial enterprises, distribution of resources (e.g., food, energy, and materials) and how information may be misused within global digital networks. It is essential to understand the social, cultural, cognitive, and behavioral context of the environment in which CogWar is executed.

NATO STO HFM Exploratory Team (ET) 356 “Mitigating and Responding to Cognitive Warfare” aimed to increase the understanding of how to defend against CogWar, and to increase NATO’s defence, security and resilience. The HFM-ET-356 team developed the “House Model” (Chapter 2) as the foundation for an S&T Strategic Roadmap and made links to the operational Observe, Orient, Decide, and Act (OODA) cycle. The House Model presents seven S&T knowledge fields and enablers that are inter-relational:

Pillars:

- Cognitive Neuroscience.
- Cognitive and Behavioral Science.
- Social and Cultural Science.

Bars:

- Situational Awareness and Sensemaking.
- Cognitive Effects.
- *Modus operandi*.
- Technology and Force Multipliers.

These seven areas provide the basis for more in depth research activities that need to be explored within NATO STO and its Panels and Groups in order to identify and deliver effective countermeasures to CogWar. The combination and intersection of multi-disciplinary topics in the House Model, gives rise to methods for influencing and destabilizing offensive CogWar processes. Despite several definitions of CogWar, the HFM-ET-356 uses the following:

CONCLUSION AND RECOMMENDATIONS

The goal of CogWar is to exploit facets of cognition to disrupt, undermine, influence and/or modify human decision making in accordance with the adversaries' strategic and tactical objectives.

Recommendations for research to defend against CogWar are provided in the following sections.

15.2 EMERGING TECHNOLOGIES AND COGNITIVE WARFARE

CogWar impacts all domains and dimensions of military operations. Technology is one main enablers and force multiplier in both offensive and defensive CogWar (House Model Figure 2-1, Chapter 2).

The effects of CogWar will impact “Trust” at every level of C² and present challenges in decision making. The adversaries’ *modus operandi* could use technological advances to their strategic advantage. NATO nations should collaborate to:

- Conduct research on the impact of cognitive-inspired AI/ML machines that can affect all stages of the OODA decision cycle.
- Develop certification doctrine and training dataset sources to ensure that valid, reliable datasets are used for development of AI/ML algorithms.
- Develop and design technologies that will contribute to overall accuracy and trust of information and evaluate the validity and reliability of the information.
- Develop validation tools to ensure accurate, reliable, and trustworthy datasets/information before they are integrated into nations’ networks and into NATO’s military C² systems.

Future designs of technological systems and networks will alter the role of the human in the OODA decision cycle. AI/ML adaptive robots will be designed with human-like cognitive processing. As these systems become more cognitively capable, there will be more human and AI machine collaboration as “equal partners.” Decision making will no longer be the singular capability of the human. Therefore, “trust” between humans and human-machines becomes an important element in CogWar and decision making. NATO nations need to:

- Defend against manipulation of advanced AI machine/technologies that may interfere with sensemaking capabilities.
- Identify and act to close the vulnerability gaps within the OODA decision-making cycle, where human and AI machine converge to build SA.
- Research, design and provide cognitive security interventions to ensure defence against second and third order CogWar effects.

15.3 FUTURE HUMAN SYSTEMS, FACTORS, AND PERFORMANCE AND COGNITIVE WARFARE

Education plays a pivotal role in the development of leaders who will be capable of ethically deploying advanced technologies in the operational environment. Technologies and tools that will enhance human performance and capabilities must be understood by those using these advanced tools. Future military operations will see an increase in human-machine teaming wherein machines will be collaborators, and decision makers. Emerging and advanced technologies will expand military capabilities, but these advances do not come without risk. The military must educate their personnel to understand the ethical and legal implications of

human-machine teaming and deploying such technologies. The evolution of such advanced tools, technologies, and systems will reconfigure the battlespace, as well as the role of the human in the decision-making cycle. NATO nations need to develop:

- Training and education methods and tools for military personnel at all levels (tactical, operational, and strategic) regarding the capabilities and shortfalls of each advanced technology that will be used in the operational environments. This is to include understanding the importance of ethical decision making relating to the role of modern technologies in the operating environment.
- Training scenarios, including various (simulated) environments and operations (multi-domain), to evaluate defence processes given adversaries' potential *modus operandi* and attempts to affect sensemaking and SA.

Using false information to gain strategic advantage is not new, however, new technologies afford adversaries a means of initiating misinformation and disinformation campaigns on a global scale. Adversaries seek to manipulate the mass population and leverage extremist's causes to their strategic advantage. NATO nations need to:

- Counter the impact of adversarial cognitive intrusions and influence effects.
- Ensure NATO nations understand human vulnerabilities and the role cognitive security can play in defending against CogWar.

Decision making is iterative and based upon a process of continually updating data input associated with environmental changes (Chapter 9). NATO nations need to:

- Develop tools that will design, facilitate, and enhance accurate sensemaking, SA, and decision making. As well as validate data, to support Cognitive Superiority.

The inability to overcome the emotional impact and influence induced by CogWar campaigns may induce fatigue, emotional distress and negatively impact performance. Thus, NATO nations need to:

- Develop strategies and tactics to mitigate the emotional impact of CogWar to reduce the threat to judgment, decision making, physical and mental exhaustion.

Misinformation campaigns are effective in inducing distrust within society and elevates the level of social pressure on individual and communities. Current internet /software systems and tools do not provide a means of validating the source of information. NATO nations need S&T to:

- Develop tools that facilitate the ability to detect socio-technical manipulations and ensure the dissemination of valid information.
- Develop defensive, agile, resilient digital networks that can defend against fake news, manipulation of socio-cultural aspects, political elections, intrusions on government, economic, and policies.
- Develop defensive tools and techniques to detect, deter, and counter intrusions and manipulations.

Humans make errors in judgment that often are based on misinformation or non-factual reasoning. NATO nations need S&T to:

- Examine the impact of CogWar on human cognitive processes, emotional processes, cognitive workload, fatigue, vigilance, and safety.
- Develop training and education material to enhance human cognitive processes and critical thinking skills.

CONCLUSION AND RECOMMENDATIONS

- Conduct research on human fatigue, emotional stress, and the influence of cognitive bias for human decision making.
- Develop tools for accelerating the decision cycle, reducing chaos, eliminate the fog of war and reduce information overload, and reduce cognitive dissonance.

Advances in BMI have revealed gaps in the understanding of how to defend against manipulation and hacking of the human brain. NATO nations need to:

- Research on the use of neuro-enhancing techniques to boost attention and enhance decision making.
- Develop the means to identify and deter both passive and active cognitive attacks via neuro-interference and secure BMIs.
- Address barriers-to-adoption of Counter-CogWar neurotechnology.
- Counteract the development and effects of “neuro-weapons.”

Human Factors research includes methods for assessing cognitive workload in humans. Task analysis methods and physiological measures are often used to evaluate impact of interfaces, equipment, and technological advances. Cognitive workload analysis and task analysis methods provide an objective measure of assessment. This is especially effective when these assessments are linked with psychophysiological measurements, such as heart rate, eye movements, and pupil dilation. Eye movements and changes in pupil dilation provide valuable information regarding how users interact with complex visual displays. Pupil changes also serve as an indication of level of cognitive processing. NATO nations need to:

- Assess human brain and cognitive processes, including cognitive modelling, human performance assessment, cognitive workload analysis, eye movement/tracking research, and the evaluation of cascading consequences for the integration of advanced technologies

CogWar represents a significant and new challenge, as it also targets the civilian population, to our moral and legal understanding of war. NATO nations should determine:

- If CogWar actions trigger Article 5 – the right to national self-defence (e.g., conventional attack as a proportional response to an adversary’s cognitive attack).
- How to deal with CogWar attacks against civilians as non-combatants.
- Question the legal principles required to establish levels of response, penalty to counter and mitigate the unethical use of technology for CogWar.

15.4 CONCLUDING REMARKS

The S&T recommendations presented in this report are provided to increase the ability of NATO nations to defend against CogWar. This report highlights S&T gaps and provides recommendations for investing in future S&T within NATO nations. This report also echoes the recommendations of NATO’s strategic documents, including NATO’s (2020 – 2040) S&T Tech Trend Report.

It is incumbent upon NATO to ensure the ability to collaborate, cooperate and defend against future CogWar. Failure to do so will have global cascading consequences.

REPORT DOCUMENTATION PAGE			
1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-HFM-ET-356 AC/323(HFM-356)TP/1120	ISBN 978-92-837-2433-9	PUBLIC RELEASE
5. Originator	Science and Technology Organization North Atlantic Treaty Organization BP 25, F-92201 Neuilly-sur-Seine Cedex, France		
6. Title	Mitigating and Responding to Cognitive Warfare		
7. Presented at/Sponsored by	This technical report documents the findings of HFM Exploratory Team 356.		
8. Author(s)/Editor(s)	Y.R. Masakowski and J.M. Blatny		9. Date March 2023
10. Author's/Editor's Address	Multiple		11. Pages 146
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	Artificial intelligence; Autonomous; Cognition; Cognitive warfare; Enhancement; Human performance; Machine learning; Military; Neuroscience; Social and behavioral; Social and cultural; Warfighter		
14. Abstract	<p>The NATO STO HFM-ET-356 performed an assessment of the Science and Technologies (S&T) required to mitigate and defend against Cognitive Warfare (CogWar). CogWar has emerged replete with security challenges due to its invasive and invisible nature and <i>where the goal is to exploit facets of cognition to disrupt, undermine, influence, or modify human decisions</i> (proposed by HFM-ET-356). CogWar represents the convergence of a wide range of advanced technologies along with human factors, used by NATO's adversaries in the 21st century battlespace. CogWar is a risk to global defence and security and threatens human decision making.</p> <p>The ET-356 proposed a S&T Road map to guide NATO and Allied Partners in future research activities and investments. The proposed Road map is based on a “House Model,” and linked to the Observe, Orient, Decide, and Act (OODA) decision cycle. The Model represents seven main S&T knowledge areas and enablers that are cross-cutting related: <i>Pillars</i>: Cognitive Neuroscience, Cognitive and Behavioral Science, Social and Cultural Science; and <i>Bars</i>: Situational Awareness and Sensemaking, Cognitive Effects, modus operandi, and Technology and Force Multipliers.</p> <p>This work underpins the NATO Warfighting Capstone Concept and its Warfare Development Initiative Cognitive Superiority, and the NATO Strategic Concept 2022.</p>		





BP 25

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



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 et 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

PORUGAL

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 sil 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 Bakanlıklar – 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>).



BP 25

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



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 sil 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 Bakanlıklar – 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>).