NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

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

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

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.

Edited by:

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

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.

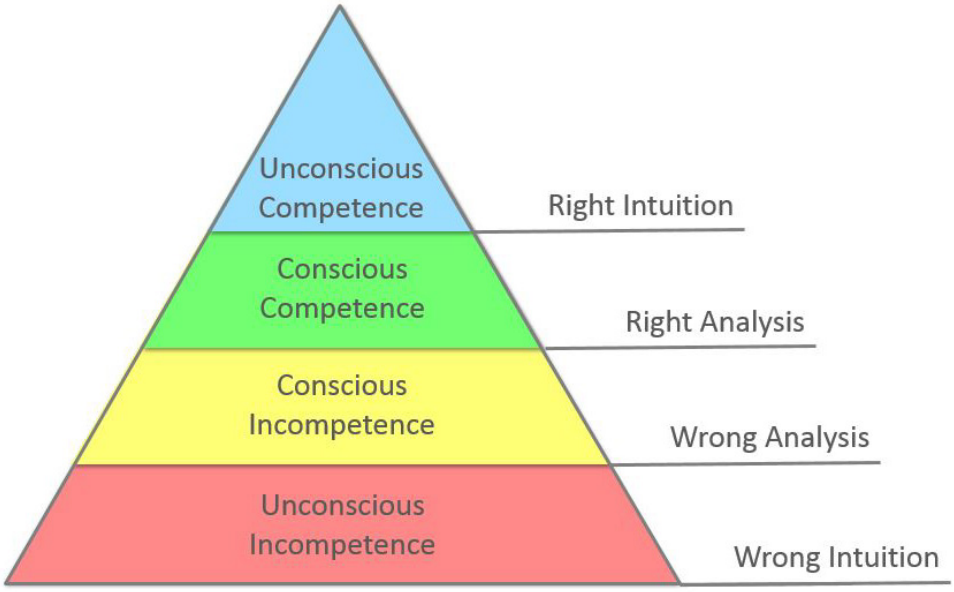

Figure 10-1: Hierarchy of Competence.

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.

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.