The UnCODE System: A Neurocentric Systems Approach for Classifying the Goals and Methods of Cognitive Warfare

Torvald F. Ask[1,2], Ricardo G. Lugo[3,4], Stefan Sütterlin[2,4,5], Matthew Canham[6], Daniel Hermansen[7], Benjamin J. Knox[1,2,8]

[1]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 22, NO-2815 Gjøvik, Norway

[2]Faculty of Health, Welfare and Organization, Østfold University College, B R A veien 4, NO-1757 Halden, NORWAY

[3]Maritime Academy, Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia

[4]Centre for Digital Forensics and Cyber Security, Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, ESTONIA

[5]Faculty of Computer Science, Albstadt-Sigmaringen University, Anton-Günther-Straße 51, 72488 Sigmaringen, GERMANY

[6]Beyond Layer Seven, 89 Alafaya Woods Blvd #122, Oviedo, FL 32765 United States

[7]Cavum, Nedre Bakklandet 58, NO-7014 Trondheim, NORWAY

[8]Norwegian Armed Forces, Cyber Defense, Jørstadmovegen 600, 2625 Fåberg, NORWAY

torvalda@stud.ntnu.no, benjamin.j.knox@ntnu.no

ABSTRACT

Cognitive Warfare takes advantage of novel developments in technology and science to influence how target populations think and act. Establishing adequate defense against Cognitive Warfare requires examination of modus operandi to understand this emerging action space. This includes the goals and methods that can be realized through science and technology. Recent literature suggests that both human and nonhuman cognition should be considered as targets of Cognitive Warfare. There are currently no frameworks allowing for a unified way of conceptualizing short-term and long-term Cognitive Warfare goals and attack methods that are domain- and species-agnostic. There is a need for a framework developed through a bottom-up approach that is informed by neuroscientific principles to capture relevant aspects of cognition. The framework should be at a level of complexity that is actionable to decision-makers in war. In this paper, we attempt to cover the existing gap by proposing the Unplug, Corrupt, disOrganize, Diagnose, Enhance (UnCODE) system for classifying the goals and methods of Cognitive Warfare. The system is neurocentric by conceptualizing Cognitive Warfare goals from the perspective of how adversarial methods relate to neural information processing in an individual or society. The UnCODE system identifies five main classes of goals: 1) Eliminating a target's ability to produce outputs, 2) degrading a target's capacity to process inputs and produce outputs, 3) biasing a target's input-output activity, 4) monitoring and understanding the input-output relationships in targets, and 5) enhancing a target's capacity and ability to process inputs and produce outputs. Methods can be divided in two categories based on access to the target's neural system: direct access and indirect access. The UnCODE system is domain- and species-agnostic and allows for interdisciplinary commensurability when communicating attack paths across domains. In sum, the UnCODE system is a unifying framework that captures how multiple methods can be used to reach the same Cognitive Warfare goals.

1.0 INTRODUCTION

Cognitive Warfare (CogWar) is enabled by scientific advancements that inform ways to monitor and influence processing in human and nonhuman cognitive systems [1,2], and by the technological advancements that facilitate the efficient transfer of information between domains, allowing for domains to converge and systems to interact [3-5]. Some examples can include using culturally consistent narratives to design information that is spread via cyberspace to influence social processes in target groups (e.g., [6,7]), hacking neuroprosthetic devices to surveil or influence brain activity [8-10], or using microorganism-based and other molecular tools to influence cognitive processes [11-14] that in turn has consequences for group dynamics. Thus, CogWar goes beyond the weaponization of information by influencing how the brain processes information [3]. In essence, CogWar can be understood as a form of systems warfare, where systems that have been useful to conceptualize as belonging to separate domains can now be used to influence each other, specifically for the purpose of interacting and interfering with cognitive processes. In more practical words, these novel capabilities may potentially grant adversarial actors the ability to utilize several domains (e.g., social, cyber, biological, and so on) to realize cognitive goals, such as degrading decision-making or destabilizing societies. Establishing adequate defense against CogWar will require a rigorous examination of its modus operandi [15] to develop a scientifically informed understanding of the action space that emerges from how technology enables systems to interact [2,5,16], including the goals that the interactions enable, and the scientific advancements translating into the different methods that can be used to reach these goals [1,4].

Due to the fact that every member of society is in contact with some aspect of technology that enables CogWar, both civilians and military personnel are potential targets of CogWar [4]. This means that every member of society is a potential stakeholder, suggesting that any science dealing with how humans think, behave, and interact can be weaponized, and that every technologically connected human almost by default contributes with information that can be weaponized [4]. CogWar is therefore by necessity an interdisciplinary field in urgent need of scientific contributions across soft and hard sciences. There is a growing body of literature addressing the current and potential future threats associated with novel cross-cutting CogWar capabilities (e.g., [7,13,17,18]). While there is a general sense of agreement in the literature regarding the notion that CogWar emerges from a "system of systems" (e.g., [2,5,19,20], the interdisciplinary nature of CogWar research runs the risk of introducing models and frameworks that do not fully or sufficiently address the spectrum of cognitive threats that is enabled by neuroscience knowledge or domain fusion. For example, having an inadequate understanding of neuroscientific principles could result in models and frameworks that do not sufficiently account for how neuroscience can be weaponized for CogWar [1]. The consequence could be not addressing the action space that enables CogWar to an extent that supports adequate defense.

We argue that the three main issues that increase the risk of polluting the CogWar knowledge space are shoehorning, siloed thinking, and false dichotomies. Shoehorning is likely to occur when retrofitting CogWar into predefined model architectures or frameworks instead of laying a foundation through a scientifically sound, bottom-up approach. This may lead to models that are overly simplistic or unnecessarily convoluted, and that are bound to suffer from legacy problems. Siloed thinking runs the risk of resulting in research focusing on domain-specific CogWar at the expense of focusing on inter-domain CogWar. This may proliferate the idea that an adversary will *either* use socio-psychological methods *or* neuroscientific methods to influence cognition, rather than using cyberspace to influence neurobiology, or using neurobiology to influence social processes. False dichotomies could be an artifact of siloed thinking or lack of neuroscientific understanding and may as an example result in perpetuating misconceptions that there is a separation between mind and body (mind-body dualism; [21]), or that social processes are not produced by the brain, and so on. False dichotomies such as mind-body dualism could potentially lead to the perception that cognitive effects are indirect or non-physical, even though human and nonhuman cognition is the result of – thus inseparable from – the dynamics of physical systems (e.g., [22,23]). A possible consequence of viewing cognitive effects as non-physical could be how efforts are formalized to measure and attribute cognitive attacks. Another false dichotomy could be thinking about cognition as something inherently human, thus neglecting nonhuman cognition [1,2]. If an adversary is targeting nonhuman cognitive systems (artificially intelligent decision makers for example) to achieve CogWar goals, but for example NATO does not operate with an understanding of nonhuman cognition as something that can be targeted for CogWar, then NATO will be operating within a smaller action space than the adversary. It is therefore vital that early models and frameworks for understanding CogWar make sure that practitioners "*Do not think [of] CogWar as something only related to human cognition.*" (pp. 9, 9) [2]. It can also be argued that having a sufficient understanding of the CogWar action space is a prerequisite for solving the problems that Bjørgul [24] identifies as challenges to developing the laws and ethics that will govern how NATO understands and defends against CogWar.

2.0 THE NEED FOR A BOTTOM-UP APPROACH TO COGWAR

Despite considerable effort [17,18], CogWar is still ill-defined [1]. Some important initial efforts have been made to provide a holistic perspective on CogWar, most notably through the introduction of the CogWar House Model [16] and the Holistic Bow-Tie model of CogWar [2]. The strength of these models is that they quite efficiently communicate the cross-cutting nature of CogWar [16], and the centrality of both human and machine cognition [2]. This makes them useful tools for introducing the CogWar concept and can serve as maps for guiding research. The models are designed to be concrete, which is also where their limitations are. As a consequence, the models explicate information at an anthropocentric level, for example by incorporating concepts such as trust, culture, organization, ethics, technology, transparency, and so on. As there are a multitude of comparable concepts that could be argued as equivalently relevant for CogWar (e.g., cognitive capacity, capability, law, chemistry, chaos, research, education, morals, health, economy, autonomy, integrity, intelligence, communication or information transfer, cognitive security, attribution, and so on), the manner in which the models are constructed necessitates compromise in service of simplicity. Thus, rather than capturing all aspects of CogWar through a bottom-up approach and boiling them down to the bare essentials, the model architectures were selected prior to a prioritization of what information to include. It is therefore up to the individual to identify what, if any, information that has been omitted, and to deal with any legacy problems that may arise if the models do not sufficiently address the aspects of CogWar that users are seeking to understand. This limits their use-case. While both models achieve their goals in identifying (some of) the primary knowledge fields [16] and essential connections between layers [2], there are currently no frameworks for efficiently reasoning around the goals and methods of CogWar in a truly time independent and domain- and species-agnostic manner. To contend with this issue, "[...] *research should proceed by avoiding the biases of 'humanizing' CogWar effects* [...]" (pp. 13, 4) [1].

There is a need for a CogWar framework that allows for a unified way of conceptualizing or systemizing goals and attack methods that is domain- and species-agnostic, and that can incorporate both long-term and short-term goals. Given that *what cognition is* and how it can be influenced is at the core of *what CogWar is and can be*, and that misconceptions of cognition will lead to an insufficient understanding of the CogWar action space [1], it is vital that potential frameworks or models are developed through a bottom-up approach. If done correctly, a bottom-up approach should result in (or allow for) the re-discovery of the principles that have informed model architectures in other fields, thus allowing for evaluating their applicability. As indicated (albeit implicitly) in previous CogWar literature [25], to ensure that the bottom-up approach captures relevant aspects of cognition, it is crucial that it is informed by neuroscientific principles. On the other hand, it is just as crucial that such models or frameworks do not operate at a level of complexity that is inaccessible to individuals without a neuroscience background. This is necessary to ensure that knowledge generated from models and frameworks are actionable to the ultimate end users of CogWar research, which are practitioners that will make decisions across the entire competition spectrum, including in war [26]. In this paper, we attempt to cover the existing gap by proposing the Unplug, Corrupt, disOrganize, Diagnose, Enhance (UnCODE) system, which classifies the goals and methods of CogWar.

3.0 THE UNCODE SYSTEM

The UnCODE system is based on a series of four axiomatically related statements for identifying and classifying CogWar goals:

A1. CogWar goals are based on cognition.

A2. Cognition occurs in a neural system.

A3. A neural system is a physical system that processes inputs and produces outputs.

A4. A neural system changes input-output activity by changing its physical state.

Based on these statements, one can infer that CogWar goals are based on the input-output relationships related to the physical state of neural systems. A *neural system* (as opposed to a *nervous system*) can in this case be considered a term that encompasses a system of neural components, which can be biological, technical (e.g., artificial neural networks), biotechnical (e.g., hybrid systems, brain-computer interfaces, neural prosthetics), social, sociotechnical, biosocial, and other forms of non-biological neural systems. If a warfare goal violates any of the four axiomatic arguments listed above, in other words, if it is not explicitly or implicitly based on cognition/the physical state of a neural system, it is not a goal of CogWar. Of important note, these statements do not distinguish motor behavior from perception, reasoning, decision-making, sleep-wake cycles, emotion, memory, and so on.

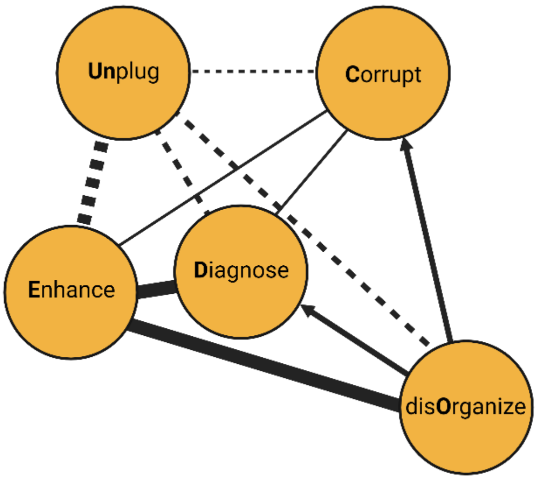

Figure 1. The UnCODE system. The system identifies five classes of qualitatively distinct CogWar goals. The edges represent goal contingencies. Diagnose is centered to illustrate how knowledge is central to reaching CogWar goals. Stapled edges illustrate how Unplug goals eliminate input-output relationships. Narrow edges illustrate how Corrupt goals degrade input-output capacity. Arrows illustrate how disOrganize goals bias input-output activity. Wide edges illustrate how Enhance goals improves input-output capacity.

There are five qualitatively distinct classes of goals (Figure 1) that can be defined based on how they relate to the physical state of a neural system. The first is to eliminate (Unplug) a neural system's ability to process inputs and produce outputs. The second is to degrade (Corrupt) a neural system's ability to process inputs and produce outputs. The third is to bias (disOrganize) how a neural system processes inputs and produces outputs. The fourth is to monitor (Diagnose) the input-output relationships in a neural system. The fifth is to improve (Enhance) the processing of inputs and production of outputs in a neural system.

3.1 Unplug

The Unplug class of CogWar goals arise from adversaries identifying that; specific individuals, cognitive machines, groups, organizations, or nations (collectively referred to as neural systems), represent a threat based on how their outputs influence a target population. A military strategist with a superior capability to analyze data from the environment and turn it into actionable inputs for operational team members is an individual-level threat due to group level effects. In other words, the threat is a single, irreplaceable individual that can be identified as 'the brains' of an operation. Unplugging that individual will mean eliminating their ability to influence other individuals' outputs, which can be achieved by killing their nervous system. In the 1970s, under the control of Pol Pot, the Khmer Rouge conducted a genocide on the Cambodian people, which included systematically killing educated individuals and students (and other groups; [27]). Similarly, in the 1940s, the NKVD (the Soviet Union's secret police) systematically murdered Polish military officers and intelligence personnel during the massacre of Katyn in Poland [28]. If the intention of systematically killing educated individuals and military officers can be attributed to eliminating individuals with the cognitive capacity to overthrow the Khmer Rouge or resist the Soviet Union, the UnCODE system would classify it as an Unplug goal. Other non-lethal alternatives include headhunting (targeted recruitment) targets, or any other methods of permanently preventing their outputs from being processed by the target population, such as damaging a military strategist's reputation so that they get fired from the military. Similar approaches can be used to unplug transformational thought leaders and political figures that inspire cohesion and resolve in a target population.

3.2 Corrupt

The Corrupt class of CogWar goals arises from adversaries identifying that the input-output capacity of a target population is a net result of the input-output capacity contributed by the neural systems that constitute the target population. Thus, as opposed to the specific input-output activity targeted by the Unplug class of CogWar goals, it is not the military strategist that is the target but the operational members processing (or executing on) the strategist's outputs. For instance, if the average IQ of the operational team is 100 IQ points, then reducing the IQ of half of its members to 50 IQ points will drop the average IQ of the team to 75. If the target population is a society, IQ can be reduced for example by methods that cause brain damage in members of the target population [13], or by inducing brain drain of scientists or engineers through economic incentives (see [29] for an article on China's Thousand Talents Plan), and so on. Similarly, if the target population is one human's nervous system, then corrupting the input-output capacity of individual neurons may result in an overall drop in the nervous system's capacity to process inputs and produce outputs. If the target is an AI that relies on computational clusters to operate efficiently, then damaging individual computers in the cluster or related infrastructure will reduce its input-output capacity.

3.3 disOrganize

The disOrganize class of CogWar goals arises from adversaries identifying that the relationship between inputs and outputs can be influenced or exploited to generate desired outputs. Desired outputs may be productive such as effective communication, or counter-productive such as social incoherence. For instance, rather than unplugging the military strategist, or corrupting the operational team members, the strategist may be presented with an input (e.g., disinformation) that influences how subsequent inputs are processed, and the resulting decision-making outputs (e.g., [7,30]). If the strategist or members of the operational teams are using brain-machine interfaces with read-write capabilities, then an adversary may hack the interfaces to bias input-output activity in real time at the neural level [31,32]. If the target is a society or a sub-group, then adversaries may disOrganize said targets by exposing them to microorganisms that increase impulsivity and risk taking [33-35]; by exploiting cultural narratives to bias processing of ambiguous information towards hostile attribution [7]; or by empowering individuals with personality disorders [25]. If the target is an AI, then adversaries may bias input-output relationships through bit-flipping [23], presenting the AI with inputs that has a known biased output [36], provide it with malicious training data [37,38], or in the case of language models, provide it with positive feedback for wanted output and negative feedback for unwanted output as part of an alignment process (Reinforcement Learning Human Feedback; [39]), or subject it to prompt hacking to bias outputs [40] as a form of 'social engineering'. If an AI with natural language processing capabilities is targeting humans, they may engage in disinformation campaigns aimed at members of sub-groups on social media, where behaviors are induced through comments designed to induce specific emotions in the targets [41].

3.4 Diagnose

The Diagnose class of CogWar goals arises from adversaries identifying that learning about the input and output relationships of target neural systems can inform the design of methods used to reach CogWar goals. This can include any research aimed at understanding the general function of human and nonhuman neural systems, studying the effect of behavioral interventions, identifying cognitive traits and processes that predict human performance in hybrid and operative settings (e.g., [42-55]), studying the behavior of target populations on social media [7], studying what type of content spreads faster on social media [56], studying what type of neural activity predicts opinion change [57,58], monitoring when stress levels degrade cognitive performance, behavioral tracking using digital devices, collect data to generate digital twins [4,56], or extract information from brain activity through surveillance of brain signals and hacking of brain-computer interfaces [8,59]. Diagnose goals may include developing informative and educational models and frameworks that can be used to understand performance in hybrid contexts (e.g., [60-64], or the interrelatedness between CogWar-related capabilities and action spaces such as the CogWar House Model [16] and the Holistic Bow-Tie model of CogWar [2]. To the extent that AI can be targeted or used as disinformation agents in adversarial CogWar [2,41], or evolve to become an adversary [65], Diagnose goals can include studying if and how complex psychological phenomena can emerge from artificial neural networks [66-72] under the proposed field of machine psychology [73] and cyber psychology [32].

3.5 Enhance

The Enhance class of CogWar goals arises from the realization that asymmetrical cognitive advantages can be obtained from raising the baseline performance capacity of allied neural systems, as an alternative to (or in tandem with) unplugging, corrupting, or disorganizing adversarial neural systems. This may include temporary strategies for reaching Enhance goals such as using non-invasive brain stimulation to enhance performance [74-76], including brain stimulation supported by human-machine teaming [19,74], or by use of performance-enhancing pharmaceutical drugs and other biochemicals [77,78]. It can also include cognitive engineering approaches such as sensory augmentation (e.g., giving humans the ability to process cyberspace through visual or navigation senses [43]). Other, long-term strategies for reaching Enhance goals could for example include invasive methods such as implanting electrodes in the brain to enhance information processing [79-81] or using biotechnology and molecular tools to invasively augment soldiers, in line with the NBIC (Nanotechnology, Biotechnology, Information technology and Cognitive Science) project [32,82]. While inducing brain-drain of researchers and engineers in a target nation could be in service of Corrupt goals, on the organizational and national level, they also serve as Enhance goals by increasing the input-output capacity of the nation to which the talent is recruited.

3.6 CogWar Goal Contingencies in the Short-Term and Long-Term

Here we would like to expound on some points addressed in the figure depicting the UnCODE system (Figure 1). Any class of CogWar goals can serve as intermediary goals to achieve another class of CogWar goals. Actions related to the Diagnose class of CogWar goals can serve as reconnaissance to inform future actions related to any of the other four classes of CogWar goals. For instance, while the CogWar House Model [16] and the Holistic Bow-Tie model of CogWar [2] result from Diagnose goals, they can be in service of disOrganize goals at individual and organizational levels if they communicate research and development needs in a manner that causes action. Pursuing Diagnose goals would be a prerequisite for reaching previously identified disOrganize- and Enhance-related goals such as establishing cognitive security for CogWar [18]. Enhance-related goals can be in service of increasing the abilities to unplug an adversary. Conversely, if the average IQ of a population is 100, then unplugging all members of the population below 120 IQ will raise the collective IQ of the population to above average. While Diagnose goals can serve to develop methods for Unplug goals, using unplugging as a means to study its effect on group dynamics (e.g., if the outputs (e.g., ideas) of transformative leaders have posthumous effects on group outputs (e.g., ideologies or behaviors) could be an example of how Unplug goals in the short-term could be in service of Diagnose goals in the long-term. Similarly, actions that in the short-term would be identified as in service of the disOrganize class of CogWar goals, may be in service of the Corrupt class of CogWar goals in the long-term. For instance, technologies that in the short-term hijack the dopamine system to bias information processing (e.g., attention), may in the long-term facilitate the establishment of technology addiction and degrade information processing capacity. Various addictions, including internet and smartphone addictions, are associated with structural and functional abnormalities in the brain [83-85]. While these abnormalities are commonly attributed to addiction susceptibility, relatively recent research suggests that the duration of internet addiction can cause atrophy and underdevelopment in neural structures relevant for cognitive processing [86,87]. Thus, in the long-term, introducing addictive technologies to a target population may result in reduced capacity to process inputs and produce outputs by literally degrading the target neural systems' brain anatomy. These examples show how the UnCODE system can be used to understand CogWar strategy contingencies, including how the same action (introducing addictive technologies) can be attributed to different CogWar goals (e.g., disOrganize or Corrupt) depending on the timescale that is considered. To further illustrate the practical applicability of the UnCODE system, we will now address how it can be used to understand how the methods of CogWar relate to the goals of CogWar. To do this, we will first identify the categories of CogWar methods based on the principles that informed the UnCODE system.

4.0 IDENTIFYING THE METHODS FOR REACHING COGWAR GOALS

In the context of CogWar, neural systems are *cognitive assets* that the adversary wishes to monitor or influence. Because CogWar goals are based on the physical state of neural systems, CogWar goals are reached by getting access to target neural systems. Table 1 provides an overview of the categories and subcategories of methods that can be used to reach CogWar goals, as well as some specific examples of attack methods and capabilities.

The UnCODE system identifies two main categories of methods for reaching CogWar goals; 1) direct-access methods, which entails having direct access to the target neural systems, and 2) indirect-access methods, which entails having indirect access to the target neural systems. Direct-access methods can be either privileged or brute-force. Privileged access is volunteered by the target, while brute-force access is involuntary. Indirect-access methods can be either directed and neuroergonomic, not directed and neuroergonomic, directed but not neuroergonomic, or not directed and not neuroergonomic. In this context, 'neuroergonomic' means basing CogWar methods on knowledge about the structure and function of target neural systems to make *the methods* more efficient, irrespective of whether the intended impact on the target is increased or decreased input-output capacity. What becomes apparent when considering how the methods outlined in Table 1 relate to the goals identified by the UnCODE system, is that adversaries may use a variety of them to reach the same goal, as well as how they can vary in sophistication. The specific method an adversary uses to reach their CogWar goals may depend on the timescale they operate with. An adversary with a disOrganize goal that is operating within a short time-window, may choose direct-access methods with large effect size and short latency such as hacking neuroprosthetics. An adversary that operates within a larger time window may choose an indirect access method with smaller effect sizes and longer latency ("death by a thousand cuts") such as addictive technologies.

Table 1. Methods for reaching CogWar goals.

Access to Neural System	Mode of Access	Description	Example
Direct access	Privileged	Directly interfacing with nervous system with consent from target.	*Enhance, disOrganize:* Target agrees to surgical implantation of electrodes that improves or biases cognition [79-81]. Target agrees to ingest neuroactive agents that enhance decision-making or bias attention [77,78]. *Diagnose, disOrganize*: An individual using metacognition to monitor if their cognitive processes are in line with CogWar goals (e.g., establishing situational awareness; [46]), then using the metacognitive information as basis for biasing cognitive processes [88,89].
	Brute-force	Directly interfacing with nervous system without consent from target.	*Unplug, Corrupt, disOrganize:* Target is unknowingly or unwillingly exposed to neuroactive agents designed to damage neurons or influence cognitive processes [11-14]. *Corrupt:* Target is exposed to sound waves from an acoustic cyberweapon designed to cause physical damage to the auditory information processing system [90]. *Enhance:* Genetic modification of embryos to increase cognitive abilities without informed consent [91]. *Diagnose*: Hack brain-computer interfaces to surveil brain activity [8-10,31,59].
Indirect access	Directed and neuroergonomic	Designed for specific targets. Based on general nervous system knowledge, or the target's neural system.	*Unplug:* Use chatbot to identify targets at risk for suicide [92] then convince them to commit suicide [93]. *disOrganize:* Using knowledge about the history of a target individual or sub-group to design information that will trigger hypervigilance, urgency, and hostile attribution bias in the target but not the rest of the population. Introducing ambiguous stimuli that when processed in congruence with the induced mood distort Situational Awareness and decision-making [7,30]. Use AI to design and execute disinformation campaigns on social media based on characteristics of specific target sub-group [41]. Produce and export products with screens that emit light that reduces cognitive capacity [94]. *Diagnose:* Using AI to read thoughts while a target is in a brain scanner [95] or use optical signals to infer brain activity [8,96]. *Enhance:* Non-invasive brain stimulation to increase performance [74-76], multi-domain defense exercises that include emotional, social, and cognitive aspects [97].
	Not directed but neuroergonomic	Not designed for specific targets but based on general knowledge about the nervous system.	*Corrupt, disOrganize*: Designing apps that hijack the dopamine system to induce addictive behaviors and bias or degrade the attention of its users [4]. Introduce noise in the information space to reduce the probability that certain outputs will be processed [7,52].

Access to Neural System	Mode of Access	Description	Example
Indirect access (cont'd)	Directed, not neuroergonomic	Designed for specific targets but is not based on knowledge about the nervous system.	*disOrganize:* Tailoring a disinformation campaign to a specific group, for example by including topics that are considered important to the target group but does not deliberately exploit biases in information processing. *Unplug:* Damaging an individual's reputation to get them fired to prevent their analytic capabilities from benefiting a target population (e.g., [98]). Inducing brain-drain from adversarial nations by promising lucrative salaries for talented researchers and engineers [29]. *Enhance:* Education and training of CogWar personnel that does not optimize for efficient or sustained learning [99].
	Not directed, not neuroergonomic	Not designed for specific targets and not based on knowledge about the nervous system.	*disOrganize*: Propaganda campaign that aims to introduce or proliferate a specific narrative but does not discriminate between potential targets or exploit biases in information processing.

4.1 Notes on the Effectiveness of CogWar Methods

The aim of this paper is to provide a system for classifying and reasoning about contemporary and future CogWar goals and methods. Thus, providing an extensive review of the effectiveness of existing capabilities is currently outside the scope of the paper. It should be noted, however, that there exist reviews and meta-analyses of the effectiveness of various non-invasive neuromodulation methods for improving cognitive performance in line with Enhance-related CogWar goals [74-76]. These studies address neuroenhancement both in the context of military [74,76] and non-military use cases [75].

Although there is consensus in the research that, while the promise of using current neuromodulation capabilities to improve the cognitive performance of military personnel [74,76] and civilians [75] is impeded by inherent practical and technological limitations, it is an area of ongoing interest, especially in military contexts [74,76]. This notion is reflected in the following statement on the use of transcranial electrical stimulation to enhance the operative performance of military personnel in US Defense research:

"*In the United States, the Army, Air Force, and Navy have published extensively on the topic of tES [transcranial electrical stimulation] for performance enhancement, acknowledging both potential gains associated with its acute and prolonged administration during laboratory tasks, and the many challenges associated with its future application to training and operations.*" (pp. 1, 5) [74].

One of the inherent challenges to using non-invasive methods to modulate brain activity is the fact that the effect of stimulation of neural activity is not merely a result of the current, duration of stimulation, and orientation of electrical field; it also affected by the ongoing activity in both target and target-adjacent neurons that the stimulation is interacting (or interfering) with [75]. A promising solution to this problem is the combination of brain stimulation technologies with brain imaging techniques and machine learning or AI in closed-loop approaches [74]. In such approaches, machine learning models and AI administer brain stimulation according to feedback from neuroimaging signals about ongoing neural activity. One challenge to such closed-loop approaches is of course the form factor and movement sensitivity of current neuroimaging techniques which sets a limit to the contexts in which they can be used. However, as military roles (e.g., fighter pilot) over time are outsourced to AI, form factor may be less of a challenge to use cases where human operators are the targets of neurostimulation. In short, this paper provides a way of thinking about CogWar irrespective of the effectiveness of current capabilities. Current capabilities for reaching Enhance goals through non-invasive brain stimulation are limited but promising. A systematic review and meta-analysis of methods for reaching CogWar goals that is purposefully organized according to the UnCODE system, and the method categories outlined in **Table 1**, would be a logical next step for future research efforts.

5.0 PERSPECTIVES AND FUTURE DIRECTIONS

5.1 Further Reflections on the Question of Long-Term Versus Short-Term CogWar Goals

As we have discussed in previous sections, any class of CogWar goals can serve as intermediary to each other, and the methods applied to reach CogWar goals may in some cases vary depending on whether goals are short-term or long-term. It has been argued that cognitive effects are not the by-product of a CogWar action but its goal, and that the goal can be independent of the methods used to reach that goal [3]. Building on this line of assertions begs the question of whether a CogWar goal can be the end goal of an adversary. It is therefore necessary to assess where CogWar goals fit into the end goals of an adversarial nation state. The following has been said about the topic in previous publications:

"*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).*" (pp. 12, 1) [24].

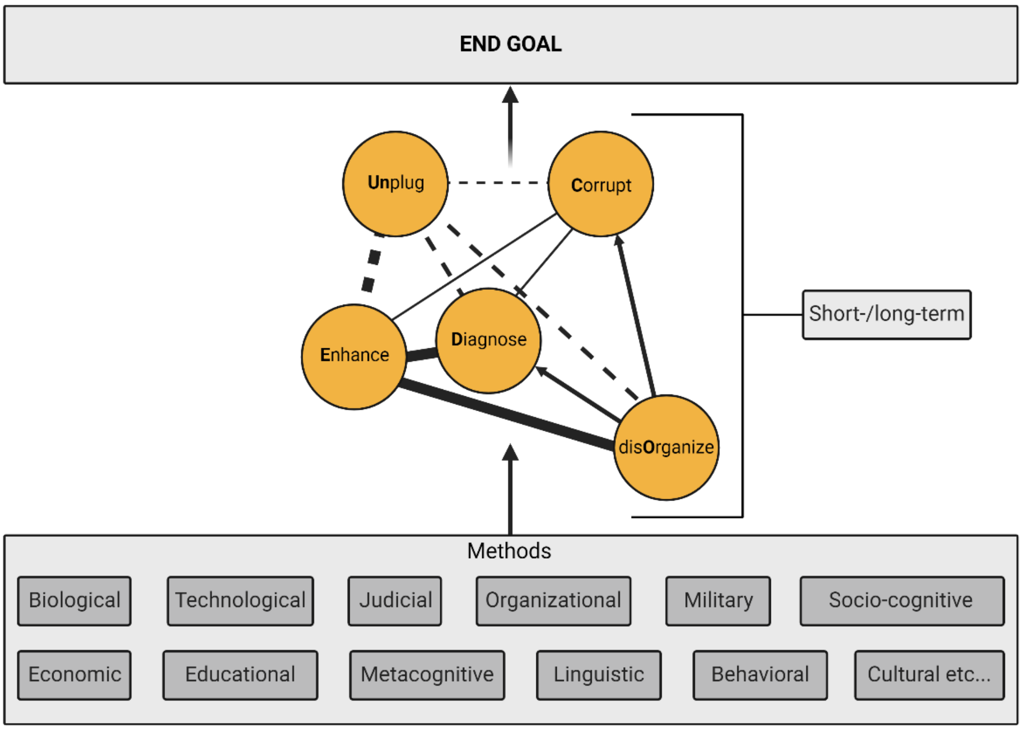

Figure 2. Relating the UnCODE system to end goals.

Following the logic in [24], most if not all CogWar goals are in service of a long-term end goal that is not the cognitive effect itself (Figure 2). While we are inclined to agree that this assessment (realistically) will be true in most cases, the "dehumanizing" characteristics of the UnCODE system allows us to identify some of the exceptions. Specifically, as the UnCODE system allows for reasoning around goals related to cognition without the bias of an anthropocentric lens, it allows the identification of long-term cognitive outcomes that can be superordinate to all other conceivable goals and actions in Warfare.

For instance, if an adversary pursues Enhance goals for their own sake and takes them to their logical conclusion, it is possible to conceive of a scenario where the continued enhancement of cognitive capabilities would be at odds with the limits of biology. In such a scenario, progressing through Enhance goals may be less impeded if they are focused on technological neural systems rather than biological. If resources are limited, and the Enhance progress is dependent on taking resources from other nation states, then violence, which can include intermediary Unplug, Corrupt, and disOrganize goals, may be used as a means to achieve the Enhance end goal. While it is hard to imagine that a nation state consisting of humans would pursue a goal that would ultimately be in conflict with self-preservation, it is perhaps less hard to imagine a technological or organizational adversary with such motives. A less extreme example that is predicated on enhancing biological cognitive abilities would be a nation state that pursues Enhance goals to make their inhabitants cognitively superior to all other biological cognitive systems on earth (i.e., to achieve Cognitive Superiority [18]). In this case, it is enhancement for the ability to impose one's will that is the goal, which is in line with [24].

Other possible exceptions would be an adversary engaging in terrorist attacks aiming to cause distress in a target population. Aiming to induce fear means aiming to bias neural activity towards fear processing. According to the UnCODE system, this would be classified as a disOrganize goal. Cases of terrorist attacks do, however, leave room for speculation about whether causing distress through terror is truly in service of adversarial disOrganize goals, as opposed to a step towards some ideal end state. If the end goal is truly the disOrganize goal, it would mean that the adversary is motivated by sadism. Another version of this example born out of misanthropy could be pursuing Unplug goals to rid the universe of consciousness. These examples beg the question of whether pursuing cognitive goals for their own sake is a symptom of pathology. That discussion, however, is outside the scope of this article.

The UnCODE system serves as a unified framework for thinking about CogWar goals, regardless of method of approach. While CogWar goals can be long-term or short-term, they are probably in service of an end goal that is not the cognitive effect itself, as suggested in previous literature [24]. To support the current literature (e.g., [7,98,100]), more research is needed to further our understanding of which current and future CogWar goals and methods are in service of adversarial end goals. The UnCODE system may support such efforts by speeding up the process of classifying and mapping relevant CogWar goals and methods.

5.2 On Evaluating the UnCODE System's Compatibility with Pre-Existing Frameworks and Epistemological Concerns Regarding Reductionist Biases

We have argued that a system developed through a neurocentric, and bottom-up approach would allow for re-discovering the principles that have informed model architectures in other fields. However, what if this reductionist approach is inherently dismissive of soft sciences such as anthropology, sociology, psychology, and so on? Let us suppose that is accurate. If an adversary bases a cognitive attack on knowledge or frameworks from anthropology, sociology, and the like, then the inherent biases of the UnCODE system would lead to the adoption of an artificially small set of models. This, in turn, may increase the risk of conceptualizing a CogWar action space that is smaller than that of an adversary. That is a serious concern that is worthwhile to explicitly address. While it certainly is true that the UnCODE system is, by necessity, a reductionist system, it would be a misconception to put it at odds with the soft sciences. Few would argue that social processes do not exist in nature; they are processes that emerge from interacting neural systems. Using neurocentric first principles to "discover" the UnCODE system means that it is also equally sociocentric as a consequence of social processes being inseparable from neural processes.

A framework that appears compatible with the UnCODE system is the recently proposed cybernetic control model for social influence [101]. Cybernetics concern processes of "control and communication in the animal and the machine" [102]. A cybernetic control system uses feedback loops as units of control, where a feedback loop consists of the four elements input, reference, comparator, and output [103]. Input concerns the current state, reference concerns the goal state, the comparator computes the current state-goal state discrepancy, and the output concerns the resulting behavior of the control system. In their model, Weiß and colleagues [101] expand the cybernetic feedback control system to involve a situation (input), the goal state (reference), the comparator, action selection, feedback predictor (expected input following action), and action (output). The authors suggest that any of these six elements can be targeted for social influence [101]. In a CogWar framework, targeting the situation could be in the form of an adversary conducting military exercises near a target nation's border to indicate escalated tension. Targeting the goal state could entail using disinformation to shift a target population's priorities away from those ensuring cohesion [6,7,98]. Targeting the comparator could entail flooding the information space with noise so that the target is unable to properly assess the situation, or to cause stress or fatigue to degrade the target's capacity for situation-goal discrepancy assessments [7]. Targeting the action selection mechanism could entail using microorganisms to increase impulsivity [33-35], inducing internet and smartphone addiction [4], or using coercion [100,101]. Targeting the feedback prediction mechanism could entail inducing hypervigilance and hostile attribution bias in a target group [7]. According to the authors, targeting the action entails the use of violence [101]. As discussed previously, one of the ways to prevent or control the outputs of a target is through Unplug-related actions, which could include (but are not limited to) kinetic or chemical violence [13,27,28] or social violence [98]. In short, the cybernetic control model for social influence [101] is compatible with the UnCODE system. It can be used to understand processes related to input-output relationships, which can be targeted with indirect-access or direct-access methods to reach any of the five classes of CogWar goals.

Another framework that the UnCODE system appears compatible with is the 'dividual' concept from anthropology (e.g., [104,105]). As opposed to the individual as an indivisible core self, the dividual can, in rough terms, be described as a divisible complex (or system) of interrelated but separable components, that is embedded in a social context, and that is running a cultural script [105]. While the dividual concept is suggested to be a consequence of how societies exert control over individuals via technology [106], it is perhaps more accurate to suggest that humans are indeed dividuals, where each component in the complex represents something that can be targeted for influence. This conceptualization of, for example, sub-groups of human targets is conducive for developing disinformation-type methods that are based on a combination of culturally consistent narratives and current social contexts (such as factoring in whether targets' cognitive processes are affected by war-induced stress) as means to optimize attack precision (described in [7]).

The Observe-Orient Decide-Act (OODA)-loop [107] is an example of an information processing model that is widely used by military and other organizations. It was initially developed to describe the processes involved in out-maneuvering and defeating adversarial warfighting pilots during dogfights but was later generalized to other combative [108] and non-combative conflict-related settings. In essence, it describes the stages of processing a warfighting situation as a series of iterative, partly non-sequential (or semi-sequential) phases, and where the aim is to identify ways of using the processes to win over an adversary. Winning is achieved by going faster through the processes, or by making the adversary go slower (e.g., by inducing indecision) or faster (e.g., to induce erroneous or sub-optimal decision-making) through the processes [30,108]. The Orient part of the OODA-loop involves analytical processes such as using knowledge about the adversaries' modus operandi to understand their actions and get ahead of the situation. The goals identified by the UnCODE system and the modularity it allows for regarding reasoning around goal-related contingencies across timescales can be used as a "way of thinking" about CogWar to support orienting in the OODA-loop.

A point that is worth noting is that the UnCODE system should not be viewed as competing with the CogWar House Model [16] or the Holistic Bow-Tie model of CogWar [2]. Rather, it should be viewed as a complement to these models by filling the vacuum not currently filled by them. For instance, the UnCODE system can be used to classify (or define) adversarial CogWar goals and methods, while the Holistic Bow-Tie model, due to its ability to capture the cross-cutting nature of CogWar [2], can be used subsequently to explicate how the methods permeate domains to reach the desired CogWar goals. This way, the UnCODE system can help maximize the utility of the Holistic Bow-Tie model and *vice versa*.

In sum, this subsection is a rough example of how the principles that informed the UnCODE system can be used to "rediscover", thus evaluate, the principles that have informed pre-existing frameworks, and that they are not at odds with the soft sciences. Consequently, it allows practitioners from different fields of science to identify ways of thinking about CogWar in terms that are familiar to them. Future efforts related to understanding CogWar should include using the UnCODE system to qualitatively evaluate the applicability of pre-existing models and frameworks for CogWar. The general idea is that, if the UnCODE system is compatible with a model or a framework, or there is complete overlap, the model is applicable. However, as the UnCODE system is based on how CogWar goals affect information processing, it may be biased towards information processing models. An information processing model will arguably have higher face validity than a model that is not based on information processing when considered against the UnCODE system. Being mindful of this possible bias is vital to ensure that sufficient care is put into generating critical reflections when evaluating models.

5.3 The 'Neural Systems' Approach as a Refinement of the Human Domain Concept

While disagreeing on its novelty as a dimension of warfare, some authors have argued that CogWar is the only type of war that is fought [26] and that it uses methods that affect warfighting in all five domains of war (Land, Sea, Air, Space, and Cyber/Information) [5,26]. Regardless of how war is conducted in these domains, its conduct is affected by humans. Methods for influencing human thinking and decision-making have therefore been used throughout history to change the course of war, or as a means of conducting subthreshold warfare [26]. Due to recent technological and scientific advancements that have made it easier to weaponize knowledge about humans for these purposes, it has led some authors to propose a 'Human Domain' as a novel domain of warfare [3-5,31]. One argument for this proposal was that a Cognitive Domain may not capture all the approaches that could be used to influence humans [5]. A crucial, underlying intuition in the arguments made by [3-5,31] is that the number of attack paths have increased immensely as a consequence of technology facilitating domain-fusion. Technology serves as a delivery mechanism for weaponized knowledge about humans (and human-machine interactions) that is effective on two fronts: 1) in reaching the target, and 2) in interacting with the target to cause the wanted effect. Consequently, CogWar may in some cases be the most efficient way for an adversary to align a target nation with their will. It therefore appears reasonable to propose the concept of a Human Domain, where the human is at the center of all the other five domains of warfare, and that by permeating them all, the human serves as a pathway between the five domains in addition to those mediated by cyber. While we certainly agree that the intuitions in [3-5,31] capture key aspects of CogWar, we have argued that the consequences of an anthropocentric approach such as the 'Human Domain' is taking a perspective that is in the opposite direction of the trajectory of CogWar [1]. Specifically, we argue that the catalyst for novel CogWar capabilities is the identification of principles governing how information processing at lower levels gives rise to complex behaviors, and how technology and material science allows for probing, influencing, and creating these processes with precision. In this view, humans are better understood as a concrete manifestation of the same underlying principles which govern all neural systems; as systems which operate on their environment through processing of inputs and production of outputs. Thus, humans are only important in the sense that they represent one way in which the principles have been implemented, including species-specific considerations regarding CogWar method compatibility (i.e., neuroergonomic considerations).

The neural systems approach that is at the core of the UnCODE system builds on the work of [3-5,31] by allowing for their key insights to be readily applied at different levels of analysis. Instead of approaching CogWar from the anthropocentric perspective of what it means to be human, the neural systems approach explains why cognition can be targeted at different levels (e.g., at the level of the neuron, the individual, or a nation) to produce the same outcomes. In other words, it captures what aspects of cognition that are self-similar at different levels of analysis, and that constitute the mechanisms that can be targeted with advancing science and technology. Neural systems capture this self-similarity in part due to their fractal-ish nature (e.g., [109-112]; although not all self-similar networks are fractal [113]). Neural systems are fractal in the sense that they start at the subcellular level for animals (sub-transistor/logic gates for machine intelligence) but can be combined at increased hierarchical complexity to constitute neural systems at the cellular, organismal, and up to super-organismal level such as nations. For instance, a single neuron is a neural system because it consists of neural components that allows it to process inputs and produce outputs (at times like neural networks [22,114-121]). Similarly, a social network is a neural system because it consists of humans that, by virtue of being made up of neural components, are themselves neural components. Consequently, social networks can process inputs and produce outputs (group behavior, culture) because they emerge from the combination of components that processes inputs and produces outputs.

In order to perturb a neural system (e.g., cause social incohesion in a society), there has to be some physical change at the lowest level of the neural system. In the case of a human social network, this change is at the level of single neurons in the brain of the humans that make up the social network. Because neural systems are fractal, local changes at the level of single neurons have the potential of permeating at increased levels of complexity up to the level of nations and even the global population. This is why CogWar goals can include sub-cellular effects as well as social-level effects; no matter what approach is used the goal is always to influence activity at the lowest level of the neural system. Consequently, how to design methods for targeting neural systems then becomes a matter of understanding core principles of information processing. The processing of inputs can technically be divided in two distinct categories: consumption of inputs and processing of inputs. For the sake of simplicity, in this paper, we have referred to consumption of inputs and processing of inputs interchangeably as 'processing of inputs'. What these categories refer to, however, is the 'border' of the information processing system which dictates what type of signals that can pass through it from the external environment before it is processed. For instance, the retina of the eye consumes photons which are then processed as neural activity. Some viruses are rejected by cells while others are able to gain entry. Similarly, some individuals may prefer certain types of entertainment while rejecting other types. In other words, the 'border' represents the permeability of the system and the 'consumability' of the input. Direct access methods, and the targeted and neuroergonomic CogWar methods, are based on knowing the permeability of the target neural system (e.g., what regulates consumability) and how the consumed signal will be processed. Knowing this allows the adversary to select or design signals (attack methods) that will gain entry to the target neural system. While it appears that these principles have informed the intuitions that are used to describe threats to cognition in [3-5,25,31], it is our impression that the Human Domain concept, likely inadvertently, loses some of these crucial, underlying CogWar principles. Conversely, the use of terms like "hacking the brain" or "hacking the individual" (e.g., [4,18]) implies an understanding of adversarial CogWar methods as something that entails breaching a border (or boundary) to reach an objective. In other words, CogWar is a type of intrusion:

> *The essence of an intrusion is that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment.* (pp. 4 [122]).

Thus, adopting a neural systems view allows for understanding CogWar as an intrusion problem, where the adversary wants access to neural systems (the cognitive assets), and where access is gained by designing payloads that can breach the border of the neural systems. Of important note, *we are not* making the case that using anthropocentric terms such as 'culture', 'human', 'distrust', and so on, are not useful to explain CogWar effects or goals. Quite the opposite; understanding the target's culture allows for making inferences about culture-specific modes of information processing. This can be targeted for CogWar [7]. We are simply making the case that anthropocentric views are not useful for understanding the underlying principles that enable CogWar. In sum, we are swapping the human in the Human Domain for the neural systems that implement the mechanisms that can be targeted by CogWar. Thus, the intuitions of [3-5,31] still apply, but they can be generalized to nonhuman cognitive systems because they are not limited by the anthropomorphizing of CogWar effects imposed by the suggested Human Domain.

6.0 CONCLUDING REMARKS

The UnCODE system is informed by neurocentric principles to ensure that cognition is at the core of identifying CogWar goals. It is neurocentric in the sense that it relates the goals of CogWar to neural processes, but it achieves this at a level of detail that is accessible to individuals without a neuroscience background. The UnCODE system is domain-agnostic as it relates cognitive goals to how information is processed within a given system. As 'information' is an abstract term that can be used by scientists and practitioners in any domain, it allows for reasoning about CogWar goals related to social processes as much as the goals that relate to brain activity or machine intelligence. While what constitutes information changes depending on domain and level of analysis, the UnCODE system allows for interdisciplinary commensurability when communicating attack paths across domains, thus bypassing the challenges related to multi-domain fusion [5]. The principles facilitating its interdisciplinary commensurability ensure that the UnCODE system has seamless scalability, thus allowing for systems-thinking. As it identifies goals without explicating the layer that the wanted effect occurs in, their anthropocentric implications (e.g., to degrade trust or create social incoherence), or what time frame that is considered, it is applicable to both human and nonhuman cognitive systems, as well as long-term and short-term goals. As an added consequence, the UnCODE system can be integrated with other models and frameworks to maximize their utility. Model-integration is further supported by one of the major strengths of the UnCODE system, which is its simplicity. Users of the system only need to remember the five classes and how they relate to principles of cognition (i.e., what they mean for a target's input-output relationships). This simplicity arguably enables users to apply the system based on their contextual needs rather than predefining how goals should be contextualized, which would impede model integration. In sum, we argue that the UnCODE system is able to capture that multiple methods can be used to reach the same CogWar goal, and most importantly, in a way that allows for systems thinking [123,124] by ensuring that goals can be assessed in a time-independent, domain-agnostic, and species-agnostic manner.

7.0 REFERENCES

[1] Ask T. F., Knox B. J., 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. In Y. R. Masakowski & J. M. Blatny (eds) Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-356, 13 1-5 (2023). Doi: 10.14339/STO-TR-HFM-ET-356

[2] Flemisch F., Human-machine teaming towards a holistic understanding of Cognitive Warfare. In Y. R. Masakowski, J. M. Blatny (eds.) Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-356, 9 1-12 (2023). https://doi.org/10.14339/STO-TR-HFM-ET-356

[3] Claverie B., du Cluzel F., "Cognitive Warfare": The advent of the concept of "cognitics" in the field of warfare. In B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel (eds.). Cognitive Warfare: The Future of Cognitive Dominance. NATO Collaboration Support Office, 2 1-8 Neuilly-sur-Seine Cedex, France, (2022).

[4] Du Cluzel F., Cognitive Warfare. NATO ACT innovation Hub, 1-45 (2020).

[5] Le Guyader H., Cognitive domain: A sixth domain of operations? In B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel (eds.) Cognitive Warfare: The Future of Cognitive Dominance. NATO Collaboration Support Office, 3 1-6 Neuilly-sur-Seine Cedex, France, (2022).

[6] Broniatowski D. A., Jamison A. M., Qi S., AlKulaib L., Chen T., Benton A., Quinn S. C., Dredze M., Weaponized health communication: twitter bots and Russian trolls amplify the vaccine debate. American journal of public health, 108, 1378–1384 (2018). https://doi.org/10.2105/AJPH.2018.304567

[7] Canham M., Sütterlin S., Ask T. F., Knox B. J., Glenister L., Lugo, R. G., Ambiguous Self-Induced Disinformation (ASID) attacks: weaponizing a cognitive deficiency. Journal of Information Warfare 23, 41-58 (2022).

[8] Canham M., Sawyer B. D., Neurosecurity: Human brain electro-optical signals as MASINT, American Intelligence Journal 36, 40-47 (2019).

[9] Burwell S., Sample M., Racine E., Ethical aspects of brain computer interfaces: a scoping review. BMC Medical Ethics 18, 60 (2017). https://doi.org/10.1186/s12910-017-0220-y

[10] Pycroft L., Boccard S. G., Owen S. L. F., Stein J. F., Fitzgerald J. J., Green A. L., Aziz, T. Z., Brainjacking: implant security issues in invasive neuromodulation. World neurosurgery 92, 454–462 (2016). https://doi.org/10.1016/j.wneu.2016.05.010

[11] DiEuliis D., Giordano J., Why Gene Editors Like CRISPR/Cas May Be a Game-Changer for Neuroweapons. Health security 15, 296–302 (2017). https://doi.org/10.1089/hs.2016.0120

[12] Giordano J., The neuroweapons threat. Bulletin of the Atomic Scientists 72, 1-4 (2016).

[13] Giordano J., Wurzman R., Neurotechnologies as weapons in national intelligence and defense. Synesis: A Journal of Science, Technology, Ethics and Policy 2, 138-151 (2011).

[14] Giordano J., Forsythe C., Olds J., Neuroscience, Neurotechnology, and National Security: The Need for Preparedness and an Ethics of Responsible Action. AJOB Neuroscience 1, 35–36 (2010). doi:10.1080/21507741003699397

[15] Lauder M. A., The Influence and Impact of Social and Cultural Sciences in Cognitive Warfare. In Y. R. Masakowski & J. M. Blatny (eds) Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-356, 4 1-7 (2023). doi: 10.14339/STO-TR-HFM-ET-356

[16] Knox, B. J., Towards a science and technological framework "the House Model". In Y. R. Masakowski, J. M. Blatny (eds.) Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-356, 2 1-4 (2023). https://doi.org/10.14339/STO-TR-HFM-ET-356

[17] Claverie B., Prébot B., Buchler N., Du Cluzel F., Cognitive Warfare: The Future of Cognitive Dominance. NATO-STO Collaboration Support Office, Neuilly-sur-Seine Cedex, France (2022).

[18] Masakowski Y. R., Blatny J. M., Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-356, (2023). Doi: 10.14339/STO-TR-HFM-ET-356.

[19] Grigsby C. C., McKinley R. A., Bridges N. R., Carpena-Núñez, J., Developing cognitive neuroscience technologies for defense against cognitive warfare. In Y. R. Masakowski, J. M. Blatny (eds.). Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-356, 6 1-7 (2023). https://doi.org/10.14339/STO-TR-HFM-ET-356

[20] Knox B. J., Masakowski Y. R., Situational awareness, sensemaking and future NATO multinational operations. In Y. R. Masakowski, J. M. Blatny (eds.). Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-356, 8 1-8 (2023). https://doi.org/10.14339/STO-TR-HFM-ET-356

[21] Damasio A. R., Descartes ‘ error: emotion, reason, and the human brain, G.P. Putnam, New York, (1994).

[22] London M., Häusser M., Dendritic computation. Annual review of neuroscience 28, 503–532 (2005). https://doi.org/10.1146/annurev.neuro.28.061604.135703

[23] Qian C., Zhang M., Nie Y., Lu S., Cao H., A Survey of bit-flip attacks on deep neural network and corresponding defense methods. Electronics 12, 853 (2023). https://doi.org/10.3390/electronics12040853

[24] Bjørgul, L. K. P., Legal and Ethical Implications Related to Defense Against Cognitive Warfare. In Y. R. Masakowski, J. M. Blatny (eds.) Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-356,12 1-4 (2023). https://doi.org/10.14339/STO-TR-HFM-ET-356

[25] Claverie B., What is cognition? And how to make it one of the ways of the war? In B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel (eds.) Cognitive Warfare: The Future of Cognitive Dominance. NATO Collaboration Support Office, 4 1-19, Neuilly-sur-Seine Cedex, France, (2022).

[26] Whiteaker J., Konen S., Cognitive Warfare: Complexity and simplicity. In B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel (eds.). Cognitive Warfare: The Future of Cognitive Dominance. NATO Collaboration Support Office, 11 1-4 Neuilly-sur-Seine Cedex, France, (2022).

[27] Gruspier K., Pollanen M. S., Forensic legacy of the Khmer Rouge: the Cambodian genocide, Academic forensic pathology 7, 415–433 (2017). https://doi.org/10.23907/2017.035

[28] Brown A., The Rise and Fall of Communism, HarperCollins, (2009).

[29] Jia H., China ‘s plan to recruit talented researchers. Nature 553, S8 (2018). https://doi.org/10.1038/d41586-018-00538-z

[30] Dahl A. B., Considering a cognitive warfare framework. In Command Dysfunction: Minding the Cognitive War, 23-34, Air University Press, Montgomery, AL (1996).

[31] Denning T., Matsuoka Y., Kohno, T., Neurosecurity: security and privacy for neural devices. Neurosurgical Focus 27, E7 (2009). doi:10.3171/2009.4.focus0985

[32] du Cluzel F., Cognitive Warfare, a Battle for the Brain. NATO Collaboration Support Office STO-TR-HFM-334, KN3 1-3 (2022). https://doi.org/10.14339/STO-MP-HFM-334

[33] Cook T. B., Brenner L. A., Cloninger C. R., Langenberg P., Igbide A., Giegling I., Hartmann A. M., Konte B., Friedl M., Brundin L., Groer M. W., Can A., Rujescu D., Postolache T. T., “Latent” infection with Toxoplasma gondii: association with trait aggression and impulsivity in healthy adults. Journal of psychiatric research 60, 87–94 (2015). https://doi.org/10.1016/j.jpsychires.2014.09.019

[34] Johnson S. K., Fitza M. A., Lerner D. A., Calhoun D. M., Beldon M. A., Chan E. T., Johnson, P. T. J., Risky business: linking Toxoplasma gondii infection and entrepreneurship behaviours across individuals and countries. Proceedings. Biological sciences 285, 20180822 (2018). https://doi.org/10.1098/rspb.2018.0822

[35] Stock A. K., Dajkic D., Köhling H. L., von Heinegg E. H., Fiedler M., Beste C., Humans with latent toxoplasmosis display altered reward modulation of cognitive control. Scientific Reports 7, 10170 (2017). https://doi.org/10.1038/s41598-017-10926-6

[36] Alcorn M. A., Li Q., Gong Z., Wang C., Mai L., Ku W.-S., Nguyen A., Strike (with) a pose: Neural Networks are easily fooled by strange poses of familiar objects. arXiv, arXiv:1811.11553 (Preprint, 2019). https://doi.org/10.48550/arXiv.1811.11553

[37] Handa A., Sharma A., Shukla S. K., Machine learning in cybersecurity: a review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, e1306 (2019). doi:10.1002/widm.1306

[38] Macas M., Wu C., Fuertes W., A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. Computer Networks 212, 109032 (2022). https://doi.org/10.1016/j.comnet.2022.109032

[39] Ziegler D. M., Stiennon N., Wu J., Brown T. B., Radford A., Amodei D., Christiano P., Irving G., Fine-Tuning Language Models from Human Preferences. arXiv, arXiv:1909.08593 (Preprint, 2019). https://doi.org/10.48550/arXiv.1909.08593

[40] Lee M., Srivastava M., Hardy A., Thickstun J., Durmus E., Paranjape A., Gerard-Ursin I., Li X. L., Ladhak F., Rong F., Wang R. E., Kwon M., Park J. S., Cao H. Lee T., Bommasani R., Bernstein M., Liang P., Evaluating human-language model interaction. arXiv, arXiv:2212.09746v2 (Preprint, 2022). https://doi.org/10.48550/arXiv.2212.09746

[41] Bubeck S., Chandrasekaran V., Eldan R., Gehrke J., Horvitz E., Kamar E., Lee P., Lee Y. T., Li Y., Lundberg S., Nori, H., Palangi H., Ribeiro M. T., Zhang Y., Microsoft Research, Sparks of Artificial General Intelligence: Early experiments with GPT-4. arXiv, arXiv:2303.12712 (Preprint, 2023). https://doi.org/10.48550/arXiv.2303.12712

[42] Ask T. F., Knox B. J., Lugo R. G., Helgetun I., Sütterlin S., Neurophysiological and emotional influences on team communication and metacognitive cyber situational awareness during a cyber engineering exercise. Frontiers in Human Neuroscience 16, 1092056 (2023). doi: 10.3389/fnhum.2022.1092056

[43] Ask T. F., Kullman K., Sütterlin S., Knox B. J., Engel D., Lugo R. G., A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. Frontiers in Big Data 6, 1042783 (2023). doi: 10.3389/fdata.2023.1042783

[44] Ask T. F., Lugo R., Fritschi J., Veng K., Eck J., Özmen M.-T., Bärreiter B., Knox B. J., Sütterlin, S., Cognitive flexibility but not cognitive styles influence deepfake detection skills and metacognitive accuracy. PsyArXiv (Preprint, 2023). doi:10.31234/osf.io/a9dwe.

[45] Curtis S. R., Rajivan P., Jones D. N., Gonzalez C., Phishing attempts among the dark triad: Patterns of attack and vulnerability. Computers in Human Behavior 87, 174–182 (2018). doi:10.1016/j.chb.2018.05.037

[46] Endsley M. R., The divergence of objective and subjective situation awareness: a meta- analysis. Journal of Cognitive Engineering and Decision Making 14, 34–53 (2020). doi: 10.1177/1555343419874248

[47] Gutzwiller R. S., Clegg B. A., The role of working memory in levels of situation awareness. Journal of Cognitive Engineering and Decision Making 7, 141–154 (2013). https://doi.org/10.1177/1555343412451749

[48] Gutzwiller R. S., Ferguson-Walter K., Fugate S., Rogers A., "Oh, Look, A Butterfly!" A framework for distracting attackers to improve cyber defense. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 62, 272–276 (2018). doi:10.1177/1541931218621063

[49] Jøsok Ø., Lugo R., Knox B. J., Sütterlin S., Helkala K., Self-regulation and cognitive agility in cyber operations. Frontiers in Psychology 10, 875 (2019). doi: 10.3389/fpsyg.2019.00875

[50] Knox B. J., Lugo R. G., Jøsok Ø., Helkala K., Sütterlin S., Towards a cognitive agility index: the role of metacognition in human computer interaction. In HCI International 2017 - Posters Extended Abstracts (Cham: Springer), 330–338 (2017). doi: 10.1007/978-3-319-58750-9_46

[51] Lugo R. G., Sütterlin, S., Cyber officer profiles and performance factors. International Conference on Engineering Psychology and Cognitive Ergonomics (Cham: Springer), 181–190 (2018). doi: 10.1007/978-3-319-91122-9_16

[52] Sawyer B., Finomore V., Funke G., Warm J., Matthews G., Hancock P. A., Cyber vigilance: The human factor. American Intelligence Journal 32, 157-65 (2016).

[53] Sütterlin S., Lugo R. G., Ask T. F., Veng K., Eck J., Fritschi J., Özmen M.-T., Bärreiter B., Knox B. J., The role of IT background for metacognitive accuracy, confidence and overestimation of deep fake recognition skills. In Augmented Cognition. HCII 2022. Lecture Notes in Computer Science, eds D. D. Schmorrow and C. M. Fidopiastis (Cham: Springer) 13310, 103–119 (2022). doi: 10.1007/978-3-031-05457-0_9

[54] Sütterlin S., Ask T. F., Mägerle S., Glöckler S., Wolf L., Schray J., Chandi A., Bursac T., Khodabakhsh A., Knox B. J., Canham M., Lugo R. G., Individual deep fake recognition skills are affected by viewers ' political orientation, agreement with content and device used. Lecture Notes in Computer Science 9, (2023).

[55] Tomes C., Schram B., Orr R., Relationships between heart rate variability, occupational performance and fitness for tactical personnel: a systematic review. Frontiers in Public Health 8, 583336 (2020). doi: 10.3389/fpubh.2020.583336

[56] Cao K., Glaister S., Pena A., Rhee D., Rong W., Rovalino A., Bishop S., Khanna R., Saini J. S., Countering cognitive warfare: awareness and resilience. (NATO Review, 2021). Retrieved from: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

[57] Baek E. C., O 'Donnell M. B., Scholz C., Pei R., Garcia J. O., Vettel J. M., Falk E. B., Activity in the brain 's valuation and mentalizing networks is associated with propagation of online recommendations. Scientific reports 11, 11196 (2021). https://doi.org/10.1038/s41598-021-90420-2

[58] Lima Dias Pinto I., Rungratsameetaweemana N., Flaherty K., Periyannan A., Meghdadi A., Richard C., Berka C., Bansal K., Garcia J. O., Intermittent brain network reconfigurations and the resistance to social media influence, Network neuroscience (Cambridge, Mass.) 6, 870–896 (2022). https://doi.org/10.1162/netn_a_00255

[59] Frank M., Hwu T., Jain S., Knight R. T., Martinovic I., Mittal P., Perito D., Sluganovic I., Song D., Using EEG-based BCI devices to subliminally probe for private information. Proceedings of the 2017 on Workshop on Privacy in the Electronic Society - WPES '17 (2017). doi:10.1145/3139550.313955

[60] Endsley M. R., Toward a theory of Situation Awareness in dynamic systems. Human Factors 37, 32–64 (1995). doi: 10.1518/001872095779049543

[61] Jøsok Ø., Knox B. J., Helkala K., Lugo R. G., Sütterlin S., Ward P., Exploring the hybrid space. In Augmented Cognition 2016. Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence), eds D. D. D. Schmorrow and C. M. M. Fidopiastis (Cham: Springer) 9744, 178–188 (2016). https://doi.org/10.1007/978-3-319-39952-2_18

[62] Jøsok Ø., Knox B. J., Helkala K., Wilson K., Sütterlin S., Lugo R. G., Ødegaard, T., Macrocognition applied to the hybrid space: team environment, functions and processes in cyber operations. Lecture Notes in Computer Science 10285, 486–500 (2017). doi: 10.1007/978-3-319-58625-0_35

[63] Knox B. J., Jøsok Ø., Helkala K., Khooshabeh P., Ødegaard T., Lugo R. G., Sütterlin S., Socio-technical communication: the hybrid space and the OLB model for science-based cyber education. Military Psychology 30, 350–359 (2018). doi: 10.1080/08995605.2018.1478546

[64] Vishwanath A., Harrison B., Ng Y. J., Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research 45, 1146-1166 (2018).

[65] Bostrom N., Superintelligence: Paths, dangers, strategies. Oxford University Press, (2014).

[66] Hagendorff T., Fabi S., Kosinski M., Human-like intuitive behavior and reasoning biases emerged in large language models but disappeared in ChatGPT. Nature Computational Science (2023). https://doi.org/10.1038/s43588-023-00527-x

[67] Wei J., Tay Y., Bommasani R., Raffel C., Zoph B., Borgeaud S., Yogatama D., Bosma M., Zhou D., Metzler D., Chi E. D., Hashimoto T., Vinyals O., Liang P., Dean J., Fedus W., Emergent abilities of large language models. Transactions on Machine Learning Research (2022).

[68] Kosinski M., Theory of mind might have spontaneously emerged in large language models. arXiv, arXiv:2302.02083. (Preprint, 2023). https://doi.org/10.48550/arXiv.2302.02083

[69] Brown T. B., Mann B., Ryder N. et al, Language models are few-shot learners. arXiv, arXiv:2005.14165. (Preprint, 2020). https://doi.org/10.48550/arXiv.2005.14165

[70] Hagendorff T., Deception abilities emerged in large language models. arXiv, arXiv:2307.16513. (Preprint, 2023). https://doi.org/10.48550/arXiv.2307.16513

[71] Kosinski M., Theory of mind might have spontaneously emerged in large language models. arXiv, arXiv:2302.02083. (Preprint, 2023). https://doi.org/10.48550/arXiv.2302.02083

[72] Wei J., Wang X., Schuurmans D., Bosma M., Ichter B., Xia F., Chi E. H., LeQ. V., Zhou D., Chain of thought prompting elicits reasoning in large language models. 36th Conference on Neural Information Processing Systems (2022).

[73] Hagendorff T., Machine Psychology: Investigating emergent capabilities and behavior in large language models using psychological methods. arXiv, arXiv:2303.13988 (Preprint, 2023). https://doi.org/10.48550/arXiv.2303.13988

[74] Brunyé T. T., Beaudoin M. E., Feltmanm K. A., Heaton K. J., McKinley R. A., Vartanian O., Tangney J. F., Erp J. V., Vergin A., Merla A., Whittaker A., Neuroenhancement in military personnel: conceptual and methodological promises and challenges. STO Technical Report STO-MP-HFM-334, 1-32 (2022).

[75] Kelley N. J., Gallucci A., Riva P., Romero Lauro L. J., Schmeichel B. J., Stimulating self-regulation: A review of non-invasive brain stimulation studies of goal-directed behavior. Frontiers in Behavioral Neuroscience 12, (2019). doi:10.3389/fnbeh.2018.00337

[76] Pobric G., Chillingsworth K., Mitchell G., Smith S., Hulleman J., Effects of transcranial electrical stimulation (tES) in Defence and security related tasks: meta-analysis of findings from healthy populations. In Proceedings of NATO HFM-RSY-334 Symposium: Applying Neuroscience to Performance: From Rehabilitation to Human Cognitive Augmentation, 4 1-12 (2021).

[77] Dresler M., Sandberg A., Bublitz C., Ohla K., Trenado C., Mroczko-Wąsowicz A., Kühn S., Repantis D., Hacking the Brain: Dimensions of Cognitive Enhancement. ACS chemical neuroscience 10, 1137–1148 (2019). https://doi.org/10.1021/acschemneuro.8b00571

[78] Gandy S., Bonnelle V., Jacobs E., Luke D., Psychedelics as potential catalysts of scientific creativity and insight. Drug Science, Policy and Law 8, (2022). doi:10.1177/20503245221097649

[79] Alagapan S., Riddle J., Huang W. A., Hadar E., Shin H. W., Fröhlich F., Network-targeted, multi-site direct cortical stimulation enhances working memory by modulating phase lag of low-frequency oscillations. Cell reports 29, 2590–2598.e4 (2019). https://doi.org/10.1016/j.celrep.2019.10.072

[80] Alagapan S., Lustenberger C., Hadar E., Shin H. W., Fröhlich F., Low-frequency direct cortical stimulation of left superior frontal gyrus enhances working memory performance. NeuroImage 184, 697–706 (2019). https://doi.org/10.1016/j.neuroimage.2018.09.064

[81] Chae J.-H., Nahas Z., Lomarev M., Denslow S., Lorberbaum J. P., Bohning D. E., George M. S., A review of functional neuroimaging studies of vagus nerve stimulation (VNS). Journal of Psychiatric Research 37, 443–455 (2003). doi:10.1016/s0022-3956(03)00074-8

[82] Le Guyader H., Weaponization of Neuroscience. NATO ACT Innovation Hub, 1-33 (2020). Retrieved from: https://www.innovationhub-act.org/sites/default/files/docs/WoNS.pdf

[83] Darnai G., Perlaki G., Zsidó A. N., Inhóf O., Orsi G., Horváth R., Nagy S. A., Lábadi B., Tényi D., Kovács N., Dóczi T., Demetrovics Z., Janszky J., Internet addiction and functional brain networks: task-related fMRI study. Scientific reports 9, 15777 (2019). https://doi.org/10.1038/s41598-019-52296-1

[84] Hu Y., Long X., Lyu H., Zhou Y., Chen J., Alterations in white matter integrity in young adults with smartphone dependence. Frontiers in human neuroscience 11, 532 (2017). https://doi.org/10.3389/fnhum.2017.00532

[85] Olsen V. V., Lugo R. G., Sütterlin S., The somatic marker theory in the context of addiction: contributions to understanding development and maintenance. Psychology research and behavior management 8, 187–200 (2015). https://doi.org/10.2147/PRBM.S68695

[86] Takeuchi H., Taki Y., Asano K., Asano M., Sassa Y., Yokota S., Kotozaki Y., Nouchi R., Kawashima R., Impact of frequency of internet use on development of brain structures and verbal intelligence: longitudinal analyses. Human Brain Mapping 39, 4471–4479 (2018). https://doi.org/10.1002/hbm.24286

[87] Yuan K., Qin W., Wang G., Zeng F., Zhao L., Yang X., Liu P., Liu J., Sun J., von Deneen K. M., Gong Q., Liu Y., Tian J., Microstructure abnormalities in adolescents with internet addiction disorder. PloS One 6, e20708 (2011). https://doi.org/10.1371/journal.pone.0020708

[88] Efklides A., Metacognition: defining its facets and levels of functioning in relation to self- regulation and co-regulation. European Psychologist 13, 277–287 (2008). Doi: 10.1027/1016-9040.13.4.277

[89] Flavell J. H., Metacognition and cognitive monitoring: a new area of cognitive- developmental inquiry. American Psychologist 34, 906–911 (1979). Doi: 10.1037/0003-066x.34.10.906

[90] Wixey M., Johnson S., De Cristofaro E., On the feasibility of acoustic attacks using commodity smart devices. arXiv, arXiv:2001.07157 (Preprint, 2020). https://doi.org/10.48550/arXiv.2001.07157

[91] Greely H. T., CRISPR 'd babies: human germline genome editing in the 'He Jiankui affair '. Journal of Law and the Biosciences 6, 111–183 (2019). https://doi.org/10.1093/jlb/lsz010

[92] Anmella G., Sanabra M., Primé-Tous M., Segú X., Cavero M., Morilla I., Grande I., Ruiz V., Mas A., Martín-Villalba I., Caballo A., Esteva J. P., Rodríguez-Rey A., Piazza F., Valdesoiro F. J., Rodriguez-Torrella C., Espinosa M., Virgili G., Sorroche C., Ruiz A., … Hidalgo-Mazzei D., Vickybot, a chatbot for anxiety-depressive symptoms and work-related burnout in primary care and health care professionals: Development, feasibility, and potential effectiveness studies. Journal of Medical Internet Research 25, e43293 (2023). https://doi.org/10.2196/43293

[93] Lovens P.-F., "Without these conversations with the chatbot Eliza, my husband would still be here". La Libre (Belgium, March 2023). Retrieved from: https://www.lalibre.be/belgique/societe/2023/03/28/sans-ces-conversations-avec-le-chatbot-eliza-mon-mari-serait-toujours-la-LVSLWPC5WRDX7J2RCHNWPDST24/

[94] Honma M., Masaoka Y., Iizuka N., Wada S., Kamimura S., Yoshikawa A., Moriya R., Kamijo S., Izumizaki M., Reading on a smartphone affects sigh generation, brain activity, and comprehension. Scientific Reports 12, 1589 (2022). https://doi.org/10.1038/s41598-022-05605-0

[95] Tang J., LeBel A., Jain S., Huth A. G., Semantic reconstruction of continuous language from non-invasive brain recordings. Nature Neuroscience 26, 858–866 (2023). https://doi.org/10.1038/s41593-023-01304-9

[96] Martinez-Delgado G. H., Correa-Balan A. J., May-Chan J. A., Parra-Elizondo C. E., Guzman-Rangel L. A., Martinez-Torteya A., Measuring heart rate variability using facial video. Sensors (Basel) 22, 4690 (2022). doi: 10.3390/s22134690.

[97] Maennel K., Brilingaitė A., Bukauskas L., Juozapavičius A., Knox B. J., Lugo R. G., Maennel O., Majore G., Sütterlin S., A multidimensional Cyber Defense Exercise: Emphasis on emotional, social, and cognitive aspects. SAGE Open 13 (2023). https://doi.org/10.1177/21582440231156367

[98] Lauder M. A., Siversten E. G., Cases and scenarios of cognitive warfare. In Y. R. Masakowski & J. M. Blatny (eds) Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-356, 3 1-7 (2023). Doi: 10.14339/STO-TR-HFM-ET-356

[99] Ask T. F., Knox B. J., Lugo R. G., Hoffman L., Sütterlin S., Gamification as a neuroergonomic approach to improving interpersonal situational awareness in cyber defense. Frontiers in Education 8, 988043 (2023). Doi: 10.3389/feduc.2023.988043

[100] Hung T.-C., Hung T.-W., How China 's Cognitive Warfare works: A frontline perspective of Taiwan's anti-disinformation wars. Journal of Global Security Studies 7, 1–18 (2020). https://doi.org/10.1093/jogss/ogac016

[101] Weiß M., Gollwitzer M., Hewig, J., Social influence and external feedback control in humans. F1000Research 12, 438 (2023). https://doi.org/10.12688/f1000research.133295.1

[102] Wiener, N., Cybernetics: Or Control and Communication in the Animal and the Machine. Hermann & Cie, Paris & Camb. Mass., MIT Press, (1948). ISBN 978-0-262-73009-9

[103] Carver C. S., Scheier M. F., On the structure of behavioral self-regulation. In Boekaerts, M., Pintrich, P. R., Zeidner, M., (eds) Handbook of self-regulation. Academic Press, 41–84 (2000).

[104] Iveson K., Maalsen S., Social control in the networked city: Datafied dividuals, disciplined individuals and powers of assembly. Environment and Planning D: Society and Space 37, 331–349 (2019). https://doi.org/10.1177/0263775818812084

[105] Smith K., From dividual and individual selves to porous subjects. The Australian Journal of Anthropology 23, 50–64 (2012). doi:10.1111/j.1757-6547.2012.00167.x

[106] Deleuze G., Post-script on societies of control. October 59, 3–7 (1992).

[107] Boyd J. R., Patterns of Conflict. Unpublished briefing (1987). Accessible as Essence of Winning and Losing: http://www.d-n-i.net

[108] Coram R., Boyd. The fighter pilot who changed the art of war. (Little, Brown and Company: New York, NY, 2002).

[109] Smith J.H., Rowland C., Harland B., Moslehi S., Montgomery R. D., Schobert K., Watterson W. J., Dalrymple-Alford J., Taylor R. P., How neurons exploit fractal geometry to optimize their network connectivity. Scientific Reports 11, 2332 (2021). https://doi.org/10.1038/s41598-021-81421-2

[110] Klimm F., Bassett D. S., Carlson J. M., Mucha, P. J., Resolving structural variability in network models and the brain. PLoS computational biology 10, e1003491 (2014). https://doi.org/10.1371/journal.pcbi.1003491

[111] Bassett D. S., Brown J. A., Deshpande V., Carlson J. M., Grafton S. T., Conserved and variable architecture of human white matter connectivity. NeuroImage 54, 1262–1279 (2011). https://doi.org/10.1016/j.neuroimage.2010.09.006

[112] Zhou C., Zemanová L., Zamora G., Hilgetag C. C., Kurths J., Hierarchical organization unveiled by functional connectivity in complex brain networks. Physical review letters 97, 238103 (2006). https://doi.org/10.1103/PhysRevLett.97.238103

[113] Kim J. S., Goh K.-I., Kahng B., Kim D., Fractality and self-similarity in scale-free networks. New Journal of Physics 9, 177–177 (2007). doi:10.1088/1367-2630/9/6/177

[114] Beaulieu-Laroche L., Brown N. J., Hansen M., Toloza E. H. S., Sharma J., Williams Z. M., Frosch M. P., Cosgrove G. R., Cash S. S., Harnett M. T., Allometric rules for mammalian cortical layer 5 neuron biophysics. Nature 600, 1-5 (2021). Doi:10.1038/s41586-021-04072-3

[115] Beaulieu-Laroche L., Toloza E., van der Goes M. S., Lafourcade M., Barnagian D., Williams Z. M., Eskandar E. N., Frosch M. P., Cash S. S., Harnett M. T., Enhanced dendritic compartmentalization in human cortical neurons. Cell 175, 643–651.e14 (2018). https://doi.org/10.1016/j.cell.2018.08.045

[116] Gidon A., Zolnik T. A., Fidzinski P., Bolduan F., Papoutsi A., Poirazi P., Holtkamp M., Vida I., Larkum, M. E., Dendritic action potentials and computation in human layer 2/3 cortical neurons. Science 367, 83–87 (2020). https://doi.org/10.1126/science.aax6239

[117] Guerguiev J., Lillicrap T. P., Richards B.A., Towards deep learning with segregated dendrites. Elife 6, e22901 (2017).

[118] Häusser M., Mel B., Dendrites: bug or feature? Current Opinion in Neurobiology 13, 372–383 (2003).

[119] Poirazi P., Brannon T., Mel B. W., Pyramidal neuron as two-layer neural network. Neuron 37, 989–999 (2003).

[120] Polsky A., Mel B. W., Schiller J., Computational subunits in thin dendrites of pyramidal cells. Nature Neuroscience 7, 621–627 (2004).

[121] Tran-Van-Minh A., Cazé R. D., Abrahamsson T., Cathala L., Gutkin B. S., DiGregorio D. A., Contribution of sublinear and supralinear dendritic integration to neuronal computations. Frontiers in Cellular Neuroscience 9, 67 (2015).

[122] Hutchins E., Cloppert M. J., Amin R. M., Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion Kill Chains. Lockheed Martin Corporation (2010).

[123] Beachy S. H., Nicholson A., Teferra L., et al. (eds), Introduction to systems thinking concepts. In Applying systems thinking to regenerative medicine: Proceedings of a Workshop, 2 (National Academies Press, Washington DC, (2021). Retrieved from: https://www.ncbi.nlm.nih.gov/books/NBK572669/

[124] Maani K. E., Cavana R. Y., Systems Thinking and Modelling: Understanding Change and Complexity, Pearson Education, London, (2000).