Eksplorium *p*-ISSN 0854-1418
Volume 46 No. 1, May 2025: 1243–1270 *e*-ISSN 2503-426X

Cognitive Warfare: The Mind as a Battlefield

[1]Claudio Paya Santos (Correspondence Author), [2]Luigi Martino, [3]Raquel Ibañez Lopez, [4]Roger Sanz Gonzalez

[1]Valencia International University, Spain

claudio.paya@professor.universidadviu.com

https://orcid.org/0000-0002-1908-9960

[2]Khalifa University Abu Dhabi, Bologna University, Italy

luigi.martino3@unibo.it.

https://orcid.org/0000-0002-7417-2898

[3]Reseint

info@reseint.eu

[4]Valencian International University, Spain

rsanzg@professional.universidadviu.com

https://orcid.org/0009-0006-1419-2367

Article Received: 05 May 2025, Revised: 07 June 2025, Accepted: 15 June 2025

Abstract: Cognitive warfare constitutes a rapidly emerging domain in modern military strategy, wherein the battlefield transcends physical spaces to target the cognitive faculties of individuals and societies. This study explores the strategic mechanisms and ramifications of cognitive warfare, with particular attention to psychological operations, information manipulation, and neuropsychological tactics that shape perception, decision-making, and behavior. Through the examination of contemporary literature and illustrative case studies, the paper offers a comprehensive analysis of cognitive warfare's growing influence in geopolitical conflict and its associated ethical dilemmas. Ultimately, this work highlights the pressing need to protect mental sovereignty amid the rise of digital and psychological manipulation.

Keywords: Cognitive warfare, psychological operations, information warfare, perception manipulation, ethics.

1. INTRODUCTION TO COGNITIVE WARFARE

War has long been understood as a territorial struggle involving physical and economic strength. Over the decades, the definition of warfare has gradually expanded to include cyber, economic, and bio-warfare as strategic avenues to harm the enemy's interests where interpretation can vary greatly (Ganji et al., 2013). In this vein, the rapid advancement of Artificial Intelligence (AI) and media-processing technology has recently given new meaning to warfare. In addition to its capabilities to hack into critical infrastructures such as satellites, power plants, airports, and trains, the same technology can be weaponized against an enemy's populace utilizing their social media for subversion (Sanz., et al., 2024) The new field of cognitive warfare will reshape our understanding of warfare, similar to the paradigm shift foreseen for psychological warfare but from a more cell-based perspective (Espinoza, 2024).

The previously weaponized technology of the media, in combination with the AI revolution, has opened a new field of warfare that is referred to as cognitive warfare (CW). Whereas traditional warfare takes place in the material battlefield with fire, noise, and destruction, CW is a notion of weaponized social media and the internet to conduct information warfare to

neutralize the enemy's decision-maker's mental domain (i.e., observation, orientation, decision, and action) without a conventional attack. CW is estimated to reshape our future military thinking and decision-making and put us into uncharted territories if left unchecked. The informal definition of CW includes the use of information, communication technologies, and psychological operations to manipulate the adversary's cognition by biasing its perception and interpretation of reality to gain advantages. The goals are to alter the information acts of individuals, which may result in unintended, uncontrollable outcomes; and to leverage automatic information processing based on behavioral data to influence the goals, self-identity, and past experience of individuals after plausibility testing.

2. HISTORICAL CONTEXT OF COGNITIVE WARFARE

A recent online editorial identifies three dimensions of warfare which include physical warfare, digital warfare and cognitive warfare. It is said it is the first time that cognitive dimension has reached the stage of being recognised as a variable, measurable, important input to equations of warfare. Physical warfare is described as the more traditional form of warfare "with weapons made of steel, gunpowder and explosives" and the battlefield as concrete geographic territory. The second dimension, digital warfare, is described as "a new kind of warfare, waged on virtual battlegrounds with computer code and computer networks" where the battlefield is a cyberspace territory. The third and new dimension, cognitive warfare, destroys the enemy's will to fight, rendering its physical and digital capabilities useless (Martino, 2021:2023: Editor, 1999). Clear examples are provided about cognitive warfare skies which detach the enemy's minds from the earth and conquer them with pamphlets of psyops on weekends and then nudge them with advertisements. The conclusion is that an intelligent army must utilise all three dimensions of warfare but if one dimension were to be chosen and developed first and foremost, cognitive warfare, the newest and least-known dimension, would be the safest option (Payá, 2023).

The editorial has been widely celebrated and vigorously debated on digital platforms. Following are a few noteworthy points. Firstly, cognitive warfare will attract attention of both defence and intelligence operation sides, including psychological operations and influence operations which will see and be forced to react to the shaped calamities of cognitive warfare under the assumptions that cognitive operations should affect enemy individuals and groups' capabilities of understanding and willingness to act politically (Luque et al., 2023). It is also anticipated cognitive warfare will offer new spaces for adversary intelligence collection and deception activities and operational opportunities to use non-coercive intelligence approaches under conditions where coercion is difficult (Martino 2024a).

3. THEORETICAL FRAMEWORKS

Cognitive Warfare (CW) is described as a use of means, methods, and information in conflict conducted with a primary goal of affecting the cognitive behavior and decisions of the adversary. Doctrines of global leaders do communicate such awareness, yet tangible approaches for observing or indicating expressions of CW are limited. By seeking a cognitive landscape perspective of conflict, CW can be up to a transdisciplinary inquiry on a mindset level. As such, the initial phase of CW analysis tends to move up to an actor's perspective, and

the distinctions of observation instruments currently needed may be limited to indications of intent or largescale narratives (targeted or focused sub-country campaigns). Developing an exclusive methodology of CW is not easy. Currently broadly available tools such as heuristic modeling or big-data EDA are in some ways applicable to small to mid-scale CW analyses or link-scales of communication flows (Payá et al, 2023). Without external help, however, parsing the individual narratives producing conflict is likely to be very labor-intensive and left to private, artistic optimism.

Cognitive warfare competes for the best cognitive narratives within the cognitive territory in doing so, affecting long-term behaviors of said minds. Unlike other forms of contest such as cyberwarfare or economic warfare, CW does not rest on "owned" infrastructures conducting attack/defense but searches to affect/influence minds through communication construed as competitive narratives (Payá et al., 2018). In addition, such communications often embody contending meaning systems that define basic odds and rules of each community - mind-space in a broader sense - possibly affecting engagement in the conflict well before it evolves to kinetic forms (Alberto Gomez & Whyte, 2021). Successfully disentangling such complex+large-scale architectures might be the best prime-intent observations in sorting CW from other types of information warfare, nonetheless bearing mental-considerations for early carry-over application. Unlike existing network and textual analyses focusing on narrative structures, immersive perspectives will be taken in considering usages of dialogue/monologue as prime communicative means of CW depending upon the scale of conflict par-verbal aspects other than purely content ones.

The challenges of a mindset perspective on warfare consist of tackling stubborn specification or formalization of the vague notion if compared to the physically accessible arena-ground of war, knowledge to accommodate the problem domain as it expands far beyond pure natural observation, thus well organized research for its better essence identification considerations. The first effort of a tender system-theoretic formulation is proposed cautiously as a modest start towards an articulation of the notion with cognitive findings distilled from general endeavors.

3.1. Psychological Operations

Psychological operations (PsyOps), one of the earliest overt forms of influence operation, often come to mind when thinking of cognitive warfare. While PsyOps tend to be associated with broadcasting propaganda in some wartime radio and television broadcasts, the term spans official and unofficial, military and nonmilitary, government and commercial, mass and personal message creation and dissemination with the goal of changing thoughts and behavior. PsyOps is a subset of influence and information operations (IO) that specializes in behaviors and attitudes and employs strategic communication (M. Scanzillo & M. Lopacienski, 2015). Unlike military PsyOps that attempt to manage domestic perceptions and garner international sympathy, influence operations, as discussed here, operate primarily through nonmilitary actions with the goal of changing behaviors and awareness. These operations include deception, psychological manipulation, and social engineering through a range of public and private actions to achieve desired goals by changing perceptions and guiding decisions.

Behavioral change, however, is harder than thought and often produces dangerous, unintended consequences.

The psychology of shame illustrates the difficulties of inducing desired behavior. Individual and social behavior is not always rational, and decisions are shaped by mental shortcuts, biases, heuristics, and rules of thumb. Desired behavioral change can be induced through the removal of an individual's procedural grounding. Where only specious reasons remain, resulting behavior is entirely pragmatic and irrelevant. Where internalized behavioral justification is replaced by an unsustainable stance, major efforts to justify past behavior and shame and guilt follow. These emotions prompt change; alternatives emerge. This is the desired end state in the majority of IO. Persuaders seek to craft messages that maximally trade off the control of the first, indisputable ground and the regulation of its fearfully-close repercussions. If successful, controlled shame induces a new behavioral fixation on conversational grounds that are manipulated by the sender. Inducing unwanted behavioral change is no easy task. Simply communicating fearsome truths is rarely sufficient. Where a target's perception is starkly counteraligned with reality, entrenched, socially negotiated behavior often follows. Treating decision makers in this manner runs the risk of double-reversal toward the disfavored decision, a move that is almost always more than animated by cynicism and anger. Any fearsome truth or desired behavioral change will plausibly be hailed or dismissed as nonsense if inconsistent with social consensus. Overriding consensus to effect external convergence is exceptionally difficult and against the established norms of international behavior—despite the case for exerting this leverage convincingly (Editor, 2018).

3.2. Information Warfare

Information Warfare (IW), "the cornerstone of neoinformation warfare," refers to "action taken to gain advantage over an opponent by the malicious use of information and/or information systems." IW can be considered effort to target and manipulate the information environment. IW encompasses a variety of tactics and leveraging some of the tools of war that do not fall into the traditional military categories of kinetic (e.g., attacks that cause physical damage). IW can be divided into two kinds of military operations: Information Attack and Information Defence. Information Attack consists of offensive information operations, including information disruption, information destruction, and information denial. Information Attack aims at achieving information dominance over an adversary while preventing or reducing damage to national information resources and facilities (Wei-Cheng Wang, 2003). For example, a campaign of cyber attacks on crucial infrastructure may create temporary disruption. Information Defence consists of defensive information operations with an intent to limit the destructive effect of enemy information attacks while retaining capability to conduct information attacks against the enemy (Rodríguez et al., 2023). Immediately after a major information attack, the defender usually has to focus the effort on recovering and restoring the information assets while hunting down the attackers and defending against follow-on assaults. Information Attack/ Information Defence can be waged individually, but integrated and complementary applications of these two components provide more dynamics than either component employed separately. In this context, a military action can escalate to IW warfare, that is, the application of IW.

3.3. Cognitive Psychology

The psychological implications of cognitive warfare merit attention, particularly those that have emerged in light of technological advances. Also, cognitive biases must be explored in greater detail due to the significant effects they can produce in wartime cyber propaganda situations, as well as the psychological and cultural factors influencing human and machine interactions (Liz 2024; Delgado 2024). Finally, it is important to also examine how the physical imprint of the cognitive landscape can be reconstructed in order to inquire from a memory's past what it can do in the present. To that a failure narrative framework for visual experiences forms as a multi-sensory data visualization application able to recursively reconstruct the landscape of human cognitive imagery past. It will be argued that cognitive warfare research and technology also advance beyond the arm of information warfare. Hence, it is necessary to conceptualize and develop a contemporary understanding of cognitive warfare that includes a focus on flexibility: this cognitive molding also requires diligence and adaptability to the idiosyncratic qualities of local cognition. Following this line of thinking, this essay attempts to examine how these emerging technologies will broadly shape future cognition, while also looking at the most relevant appropriate initiatives. Contemporary cognitive warfare needs to bring together many emerging points of interest as a means of framing general reasoning about this domain. Publicly accessible information on human cognition and social interactions is more abundant than ever. How can such information be accessed, used and understood as knowledge? Collectively the rational thinking of many combine to form a memory landscape – or cognitive map – though can these imprints of cognition gradually learn to understand abstract information? The affordances and affordance bias in action interfacing human perception at a distance is a critical consideration for communicating stimuli persistence, coherence and amplification. The language explanation becoming knowledge construct weaknesses in society could frame state or commercial influence on identity.

4. MODERN APPLICATIONS

Establishing storytelling, controlling perceptions, and leveraging effects are the cornerstones of cognitive warfare's modern applications. The latter is best positioned within the information domain and has evolved into a key feature in the strategic competition between states and nonstate actors. It describes an organization's capability to create and shape its information environment through a theatre of information effects, developing the noosphere to achieve advantages. The noosphere is envisaged as a collective, shared, and distributed network of minds operating on information, beliefs, and narratives, articulated by various means, tools, and platforms.

These include evolving AI tools, semi-automated bots, trolls, and information groups leveraging social media platforms, as well as traditional state-sponsored media. Cognitive set of technologies from data understanding to data visualization can be applied towards generating information effects such as political derailing via high credibility information laundering, tendentious biasing towards ideological beliefs or cultural paradigms via state media narratives, and infrastructure debilitation via psychophysical mismatching and emotional contagion.

They may also be employed further down the information engagement action-cycle towards the management of these effects. These technologies equipped with understanding of human cognition may be asked to assess the likelihood, efficacy, impact, propagators, amplifiers, and/or remedial solutions of a proposed story, narrative framework, or concurrent debate in terms of the understanding, attention, and perception of a key target audience. Cognitive agents can widen, shift, and elevate the frontier of taking impact and understanding towards the generation of deeper, trickier, and latently troubling depictions of news, players, agencies, or events of concern. These technologies likewise allow for the scaleup of management actions, enhancing traditional influence operations through perceptual exposition, marginalization, and integration of heterogeneous influencer ensembles.

Whereas the focus of modern applications is on enacting impacts, cognition provides a foundation to also counter cognitive challenges, informed detection being the starting point to replication. Platforms such as detection, voice generation, and image synthesis are examples of cognitive tools that aim to neutralize the effects of cognitive warfare panorganisms. Cognitive responses are not hoped for silver bullet interventions, but augments to a classical methodological toolkit for understanding information and beliefs to build resilient populations that detect, evolve, and adapt to challenges.

4.1. Social Media Manipulation

Discussion of cognitive warfare inevitably begins with the images that dots and electrons create in the brains of those who are compromised - compelling images of both what they believe and what they believe the world around them to be. These images in turn constrain the actions and motives of the compromised. In a world of media where dots and electrons are effective military weapons and initiatives of national power, the cognitive battlespace has grown tremendously. Organizations that surmount social networks can influence social connectivity, community norms, identity, hence cognition, and movement within a society, deeply challenging the concept of “free opinion.” They do this vast scale without conventional social networking tech, whose extensive exploitation earlier has exacerbated these shortfalls. The possibility of effective cognitions weapons is tightly co-evolved with these challenges, constraining their very definitions and remedy options (Oates, 2020).

High values of social contestation required to keep in mind the interests of national security. However, it has become difficult to convince audiences of this case, particularly audiences who are already compromised. After all, assumptions of a particular norm of 21st century information warfare stem, a world where anyone could freely have an opinion, largely without risk of manipulation or enforcement. These new technologies, whose workings constrain discussion of any vantage point, work neither with the expectation that everyone is free to have it opinion nor with claims of decisive military advantage in control of cognition. They suppose instead a deep incapacity to engineer cognition itself, particularly the cognitions that shape contest for co-nationalized communities.

The global information struggle must be discussed in terms of warfare against cognitive weaponry rather than social media. The latter is very much an enclave that creates terms of agency in which its freedoms can be afforded. Acknowledging the limits of such agency even

raises the question of sociality itself, as news and media consumption become substrates for calculating human behavior. New thinking is required about both knowing the world and controlling its representation, in a world with globalization of doubts and data moat visualizations of a novel order. Above all, the indifference of armies of social contestation presents a loss of innocence outside the West.

4.2. Disinformation Campaigns

The original definition of disinformation is "disinformation is falsified or manipulated information intentionally created or disseminated to mislead." The objective is to manipulate perceptions and create confusion, doubts, and division amongst the targeted audience, sowing misinformation. Disinformation is now more easily accepted due to technological advancements, facilitating the diffusion of such falsehoods with a few clicks (Editor, 2018). Disinformation arrived on social media and traditional online platforms at the very beginning of their rise. This was, in a way, natural as these platforms inherited their predecessors' liabilities. A widely read analyst coined this phenomenon "ubiquitous information pollution." Today, despite the increased attention given to the disinformation problem, platforms and publishers, reeling under public backlash, still act as an easily exploited digital Wild West where disinformation thrived in its initial days (Martino 2024b; 2018).

Current literature broadly distinguishes between propaganda, misinformation, and disinformation, broadly following the definition that propaganda refers to untruthful but not unintentional information, misinformation refers to untruthful and unintentional information, and disinformation refers to both untruthful and intentional information. Information transmission can also be divided into three categories: true information, false information, and mixed information, which leads to types of cognitive manipulation – persuasion, deceit, and confusion. Social media helps manipulate public perceptions by massively disseminating false information and then limiting the discussion of the eventual truth (Aslama Horowitz, 2019). An example is the disinformation campaigns against COVID-19 with fixed patterns or templates the tactics used to attack a narrative, both prevention and cure. Recombinant Wars: The Unanticipated Impacts of Improving the Way Information Wars are Fought, propaganda to sow confusion in real time, creating emanations of false credibility to proliferate around the disinformation narrative (crystallizing), and the inescapable democratization of social media and the vast array of other visual and participatory media commonly used today (imbuing).

4.3. Cyber Warfare

Cyber operations are a unique class of warfare characterized by several factors, including low cost, reliance on concealment, generation of disproportionate effects, and access to a global and relatively systematic weapon base. They are fluid, transparent, and often one-sided, yet dynamic and asymmetrical. In cyberspace, a very small actor can generate disproportionate effects by exploiting systemic vulnerabilities. The massive investment of Fortune 500 companies in defensive security measures alongside constant assaults on their data suggests a best-effort strategy, leaving the most lucrative and damaging exploits in the hands of well-resourced actors familiar with the latest in malware and deception techniques. Consequently,

the asymmetrical access to offensive tools is one possible explanation for the contemporary cyber battle environment (Alberto Gomez & Whyte, 2021).

Furthermore, when new actors begin to exploit a new vector, there is often no equivalent counter-attack available in response. Due to the open nature of cyberspace, those exposed to the new capability are at a significant disadvantage until they fully understand the exploit. New unknown exploits tend to produce the largest and most asymmetric advantage, following a similar logic to the rise of the industrial age. As usability increases, even state-supported actors with no highly-technical talent will be able to execute highly-effective exploits. Current information warfare is more akin to a fifth-generation warfare, wherein media control is difficult and all actors live together in a combined physiology, than a traditional warfare of precision tools with targeted and strategic impact (L Bibighaus, 2015).

Moreover, though the domain is accessible to all, its geography is fundamentally asymmetric. Exactly as second-movers in the industrial age, most actors began with tools of mass hacking that invalidated all previous analytic strategies. The return of the Trojan Horse as a form of attack warrants a paradigm-changing response strategy. Attack vectors in cyberspace are not precisely understood, and which logic to use for response is not apparent. Malevolent actors with access to multiple vectors are more asymmetric in effect than are any national actors. Though the outcome is a violation of sovereignty, a nation-state with the capacity to respond to an act of war against its critical infrastructures may find, upon successful retaliation, collateral damage to the private sector and greater armed forces of the adversary. This possibility of asymmetric consequence invites caution around cyber-reactive capability clear strategies for identifying cyber-attackers.

5. COGNITIVE BIASES AND THEIR IMPACT

According to 78.8% of respondents, cognitive biases can be basic rules, evolutionary by-products, or irrational beliefs that promote non-optimal decision making in the context of human cognition. Here are examples of individual cognitive biases and suggestions for dealing with them.

By confirmation bias, people often place greater emphasis on information that supports their belief and do not consider contrary evidence. To combat confirmation bias, generating counterarguments to one’s beliefs can alleviate its effects and increase accuracy. Group decision making can also lessen these effects. Members of groups who initially hold the same preference are encouraged to examine arguments against the alternative preference. The group members are then asked to generate new arguments, resulting in greater consideration of contrary information.

Anchoring occurs when information is provided that is irrelevant to the judgmental task at hand. Recipients of irrelevant information tend to treat this as a starting point, which can lead to insensitivity to subsequent irrelevant information. Generally, the more incongruous information provided, the more biased responses become. To combat anchoring, recipients can be alerted to the potential anchoring, which increases resistance to bias. Other groups can also be involved to generate different answers before discussion.

Overconfidence can produce a tendency to believe too strongly in subjective knowledge. 78.8% of respondents regarded it as a very serious bias. Merely encouraging individuals to consider possible disconfirming evidence can help limit overconfidence. The best remedial approach involves accounting for one's own fallibility and interacting with others whose knowledge differs considerably.

Attraction is an unexpected bias in which the introduction of an inferior option can favor a dominant one. This paradoxical bias is not intuitive. Further knowledge of the phenomenon can address this bias when choices are to be made.

By using statistically rigorous methods, decision makers often mistakenly regard some options as better than others. When designing the process of constructing a decision model, care must be exercised to prevent excessive analysis.

5.1. Confirmation Bias

Cognitive biases describe irrational gaps in human perception, recall, judgement, and reasoning. Many biases skew estimation and predictive processes in multiple domains. Given that the domain is contextually irreverent, successful strategies for reducing biases have been of wide interest. However, while some cognitive distortions are avoidable or reducible, others—in particular, those affecting beliefs—are reasonably considered to be largely unmodifiable, at least by simple methods. Importantly, confirmation bias is one example of a cognitive bias that has recently been implicated in the development and persistence of extreme, harmful beliefs such as conspiracy theories and disinformation beliefs. Biases in evaluation can take a number of forms. In a standard sense, different processes can be tasked to judge the reliability of information or sources. Attention and evaluation can differ depending on whether evidence confirms or contradicts different beliefs. Finally, confirmation bias in belief can be construed as the tendency to avoid integration of information that, while considered reliable, does not support the belief, as more information can be integrated. Such evidence exclusion can use an exculpatory or confirmatory rationale, by which attention or belief in other evidence can be reevaluated. For what topics or beliefs confirmation bias occurs, and why, questions of consequence arise.

'Confirmation bias' describes an extensive variety of processing phenomena. Confirmation bias is sometimes cast in a broad sense and other times is restricted to narrow processes exclusively pertaining to evidence-consistent evaluations or behavior. Confirmation bias denotes normative 'influence' that is compatible with accuracy or neutrality of assessment, but fines infractions for the excessive effects other properties can have on anticipated behavior like those broadly termed 'misuse' or 'misweighting'. Analyses of problematic biases and distortions of reasoning consequence knowledge in artificial intelligence, science, and professionals have been focused in epistemology and theorized in social theory.

5.2. Anchoring

Numerous cognitive biases have the potential to be exploited in warfare or as weapons. The principle of anchoring suggests that decision-making can be influenced if an externally provided value precedes it. This could involve cases where an initial value is provided before

asking questions which, under normal circumstances, would have yielded different values. Such anchors influence estimates, predictions, and even choices in ways not logically connected to the options being exhibited. Although anchors need not be extreme, obvious, or relevant, explorations of the effects of strong anchors in the real world have generally focused on their more obvious manifestations.

Anchors can be manipulated in two ways. First, they can be given along with a question so that when responding to the question, there is a specific estimate or initial value to begin with. For example, "What is the price of a Bentley car?" This is generally understood as asking for a single value, say, 20,000, which in this particular case is likely to be an underestimate. Other reads of a question could lead to higher estimates. It has been found that anchors occurring earlier during the processing of the event generally influence decision-making. For example, anchoring can occur at the level of perception (Danielle K. Ongchoco et al., 2023). It has also been demonstrated that the immediate pre-exposure to a number can adversely affect decisions made years afterwards and regardless of knowledge or experience about the event being decided upon.

Also known as "the anchoring effect," the anchoring bias is a widely studied phenomenon, demonstrating how an initial piece of information—a purported fact presented before making an estimate—biases responses in a systematic fashion. For instance, estimates of the proportion of countries in the United Nations that are African were causally influenced by the spin of a rigged wheel, which landed on either 10 or 65. Moreover, the anchoring effect appears to be strong even when the anchor is not credible or informative (Yasseri & Reher, 2019).

5.3. Framing Effects

Framing effects provide a means of engaging cognitive warfare by activating or suppressing a reasoning pathway. By strategically framing the perception of information, media can sway the ultimate decisions made. For instance, the full quote by President Franklin Delano Roosevelt at his first inauguration says: "The only thing we have to fear is fear itself." The quote suggests that fear must not be permitted to propagate, as it would distort perception and reasoning. This description brings to light the real nature of fear, and how it can adjust agents' interpretation of the information, obstructing logical reasoning.

Framing effects likely occupy a niche position somewhere between the elementary techniques of emotional warfare on one end and the advanced techniques of propositional manipulation on the other. In their primitive manifestations, frames are a tool for the guidance of an interpretation humanoids provided with language. It is so innate that the approach may be overlooked as a means of manipulating choices; yet at the same time, it can yield substantial results (Duane Saner, 2008). For instance, Yin Shun offered a simple yet elegant resolution to the debate between free will and predestination. Free will is the capacity to change the fate. Even with karmic conditions fixed, it is capable of producing karmic conditions not envisaged before. By prompting agents to provide conflicting definitions of freedom, the discussion may lead nowhere. Instead, directing attention towards the broadest definition showing that free will is indeed inherent in the affairs of individuals can settle the debate amiably.

Even though reasonable framing is a pleasant aid in cognition, unreasonable framing could bias cognition. Some frames, especially when deployed along with an access prime, can outrightly fan out perception guiding toward alternative assimilation or accommodation pathways. In this case, agents can subconsciously perceive information somewhat differently and draw different conclusions (R. Mandel & V. Kapler, 2018).

6. TARGETING THE MIND: STRATEGIES AND TACTICS

While information and emotion are both critical for influencing behavior, how each of them does so is less well understood. Designed by members of academia in collaboration with the CIA, an understanding of propaganda developed in World War II transformed American understanding of mass communications, many principles of which are still in use today (Editor, 2018). However, an understanding of emotional warfare and how it works, along with its limitations, remains under-developed. The last critical phase of the IRD/USIA operations to stage a counter87467127295-rypto broadcastoplay masterfully combined information and emotion with several policies and strategies.

Aiming to win the runine call, experts there developed a penalty mind-guided plan focusing attention on emotional information. A swathe approach to play this masterfully naturally drew upon multiple behavioral and cognitive pathways to trigger the value of interest and value indelible bias. The most robust behavioral path was to create an enduring value by informing on values—their effects were local, or not widely due to scarcity. To build high trains of interest, a back-and-forth cryptos would ideally be operated. This, they thought, would work in terms of behavior like, “Today, we must yield to the foe of the party like to show it to be immense. Either aide, there must be heirs and nurse on chances target worth par asoulment of the cryl of droop.” The limit on how many satirical cryptos could be played in succession appeared to be not humans but company acquisition limits on the number of machine cryptos that could have, as a fair use exemption should exist internationally for each company.

An international news desk to gather and distribute takes globally first used it to assemble machine-crafted snarkification from sources, usually agreeing with the planned shape but interpretation otherwise. Placed in a cryptographic scheme, cryptos were lawfully published in free press to be traded for major and respected satirical comments by a civil, fair use exemption, machine hardware high bar. Tracers were easily paraled back to the source’s targeting location, even with anonymizing agents if any contract with total unwritten targets was all-consuming. Then, thanks to plot gats, like larger film studios and international agents, magnifying glass shape substitutes could be made and seeped into earlier broadcasts of inflation drives or discourse hold ups (Espinoza, 2024).

6.1. Narrative Construction

Humans are storytelling animals, socialized from an early age into the art of narrative engagement. All available forms of communication, including one’s own body, the human voice, video-based or digital output, can be used to tell a story in attempts to persuade others to make sense of events, for the benefit of themselves or for others (L. Winter, 1989). Some stories work better than others in this regard, owing to culture. Stories become myths (ideologies) if they are successful in soothing fears, redirecting anxiety, providing legitimacy,

and explaining the inexplicable. Myths provide meaning and a sense of order in an otherwise anarchic world. A classic case of how stories come to define a mythical order is the cinema boom of the American West from the 1880s to the 1930s. Whether the account came from the vantage point of Hollywood, or of the disempowered, the primal themes were similar and directly relevant to the transformation of culture.

However, as in the symbol-based generalizations asked of the machinations of knowledge, there are specific and pre-eminent limits on the type and range of stories that can be told and shared. This cognitive dimension derives from the process and operations of representational coherence; abilities for memory binding, association, groupings, and interaction inherent in the working of human consciousness. These cognitive processes are what render factual narratives possible, in the sense that actual events can be encoded, stored, and recalled from memory. They are also limits, though, as full understanding and appreciation of the armed voyeuristic workings of the details of power are beyond human expression and grasp. Affective processing is also cognitively encoded and constructed, communicated and embodied, constrained and determined by the same symbolic and linguistic structures.

6.2. Emotional Appeals

This section discusses the potential psychological operations platforms and techniques that might be leveraged by states and non-state actors in modern conflicts. The cognitive dimension of modern warfare has, broadly, two intertwined frameworks of analysis: the visual and audio-visual dimensions of social media; a wide range of social media devices and platform affordances repurposed for cognitive warfare; and the political, economic, and social relational, sociotechnical, and temporal frameworks or filters within which audio-visual content and interpretation compete for attention. The general approach has been grounded in how ‘cognitive warfare’ is conceptualized.

Cognitive warfare refers to the use of insights and tools from psychology and economics to sway human cognition, behavioral dispositions, and social and political phenomena visioned as relating to (and at least partly determined by) cognition (Editor, 2018). Cognitive warfare both draws on and partly overlaps with information warfare that operates through the communicational dimension and the contextually variable frame of reference through which information is selected and understood.

The object of information warfare is to influence a situation so that the settled state of affairs is calculated to be congruent with one side’s preferred interpretation as potential ‘victors’. The win-lose outcome is established by a kind of vestibule of legitimacy or standing that garners the means through which more continued harm upon the ‘enemy’ than upon oneself. While the battleground in cognitive warfare might prospectively be global, especially so given the affordances of social media, the more embedded local frames of reference or lenses through which the battleground has been propagandized and sullied remains unexplored.

6.3. Manipulation of Perception

The manipulation of perception is a broad set of techniques to affect what is seen and what is remembered. Deception of sight relies on the manipulation of light to create illusions. Given

one way in which cognition can be disturbed, memory can be altered and beliefs can be put in doubt (Espinoza, 2024). Acts performed much in view of many people may be certain, but still may not be believed. The manipulation of perception is a vital part of cognitive warfare. The battle for perceptions is already waged on a massive scale. Low-cost communications means there is continual reporting of all major events in many circumstances, including war. The individual perceives some of these occurrences, but most of them are outside perception or attention. Evaluation takes place only in that part of a person's mind where perception happens. Pre-existing beliefs and preferences about the world constitute understanding. The majority of these events are forgotten shortly after they occur. Perception and memory, highlighting the factors affecting them, affect understanding and thus also behavior. As events and facts outside a person's control are reported and spread, more subtle means are possible. Techniques based on the alteration of perceptions and beliefs therefore also need to contend with other more well-entrenched means of achieving the same goals. In the popular imagination, certainty is the currency of intelligence. A century of relentless research in philosophy and behavioral science should have taught otherwise (Editor, 2018). The balance between skepticism and credulity is at the heart of intelligence tradecraft and the art of persuasion. By necessity, practical techniques have proceeded from the observation of the behavior of very smart individuals. These techniques happen to put individuals in a frame of mind in which they become sensitive to the manipulation of their own cognitions. Everything else, from computer generation and using false digital identities to the production of statistical hallucinations, is ancillary. A full understanding of thought and its workings is not needed. What is needed are suggestions on how thought works, correct and not, and ways to put individuals in conditions where they could be manipulated. That hope was fed by computer-generated speech, machine learning, and algorithmically produced phantasms: ways of manipulating behavior and perception that did not focus on belief and cognition. However, it is belief, rather than direct manipulation that is the mind's barrier against unconsidered credulity.

7. CASE STUDIES

Understanding the manifestation of cognitive warfare requires a focus on specific examples in which the idea can be applied as a framework to understand the unfolding of events. This section includes key case studies of cognitive warfare including propaganda in the United States, more modern examples in the U.S. Presidential Election, and events in the Brexit referendum.

No discussion of cognitive warfare would be complete without examining the use of propaganda during the Cold War. In many ways, the Soviet Union became the first actor to recognize the potential of propaganda as a weapon against the mind—organizing and implementing propaganda campaigns that relied on real-world events, social media, and other tactics now standard to modern cognitive warfare. The United States had its own information warfare capabilities, of course, but many were rudimentary compared to the sophisticated means employed by Soviet agents and defending the sentiment against leftist ideology in American life. Such campaigns targeted both elite and popular discourse, spreading false and misleading ideas to journalists and other opinion-makers while inciting or amplifying social grievances. Ideas ranging from climate change to race riots passed along by Soviet-sponsored

outlets and proxy actors entered mainstream discussion and were adopted and propagated by academics, celebrities, politicians, and journalists—unlike material threats, many of these ideas enjoyed a certain immunity against state intervention.

In the U.S. Presidential Election, there was a varying degree of engagement with different modes of information warfare. Such engagement could possibly have been achieved through cat videos or memes, but instead, a concerted effort was made to build a narrative and escalate tensions surrounding racial inequality in the U.S. As such, racial grievance groups were given power in the electorate. Compounding the effects of actions by state and private agents, key figures in American life—including politicians, journalists, celebrities, and academics—amplified and responded to such information campaigns.

The U.S. Presidential Election also shows how modern information warfare differs from its older counterparts. In the age of information, information is transmitted in a more decentralized and faster manner than in previous times. Simple, meme-like formats are more effective than long, complicated analyses, a secular instead of a religious moral universe in rhetoric, bright colors and striking visuals instead of long newspaper articles. All these differences rendered countermeasures taken by authorities for the 1940s ineffective in the face of modern cognitive warfare.

7.1. The Cold War Propaganda

The ideological war reflected on the pages of the Review following the breakout, development and "raging" of the cold war up to the signing of the Helsinki Final Act. During the studied period, the leaders of the Ministry of Interior paid special attention to keeping the level of effective interior propaganda high, being influenced by national and international political factors. The sharp ideological struggle and psychological war led to the emergence of long-lasting, deep images of the enemy. The rivalry between the US and the Soviet Union polarized international and domestic politics, as it had been during the years of the Second World War. The cold war confrontation led to the unnatural, forceful division of countries and tragedies for various societal classes in the Eastern bloc. The 1960s show some "hectic," controversial elements. The conflicts among international and domestic actors and pressures meant that it was not easy for the Soviet Union of its allies to find a decent and applicable response to events like those in Hungary, Poland, etc. Approaching the end of the studied period, the issue of radio stations was increasingly on the agenda, as in the early days of the cold war. The everyday propaganda of the Eastern bloc depicted the darkest picture of Western societies to make the Eastern reality look brighter. Control was extraordinarily strict near the iron curtain to prevent defection: vigilance campaigns were carried out, potential cases were investigated from the beginning, border guards were treated with great care, etc. Self-praise and self-deception created an era of intellectual breathlessness for many intellectuals.

7.2. The 2016 U.S. Presidential Election

In the lead-up to the 2016 U.S. presidential election, Russian actors sought to exploit American society's vulnerabilities during a contentious election season. These efforts have attracted extensive scrutiny in the last several years, resulting in a lively, ongoing debate about how best to characterize their impact and, more importantly, what can be done about them. Since the

2016 election, legislators and companies have made a number of proposals to counter the threat of foreign influence operations, and many states have adopted new legislation that attempts to regulate social media companies or increase the exposure of "fake news." Notably, however, no comprehensive approach has yet been implemented that is designed to address the full arc of behavior exhibited by the Kavun team and like-minded actors (Maréchal, 2017).

To inform future efforts at countering cognitive warfare campaigns, a case study of the Russian actors' operations conducted during the 2016 U.S. presidential election unveiled significant evidence that suggests the likely online behavior of similar teams. This evidence includes information from government investigations, disclosures from social media companies, and third-party research. The case study additionally applied both the cyber and psychological elements of the SMART framework to assist in structuring the analysis. While the 2016 U.S. presidential election also produced important governance lessons and next steps for tech companies, the cognitive warfare aspects of the campaign and the mitigation options explored in this study will likely be of greater interest to future researchers and policymakers focused on similar threats. That said, the cognitive warfare aspects of the campaign were in many ways too complex to model directly at the time of the election. The case study application of SMART will hopefully spur further analysis of the campaign as more information becomes public and events unfold in ways that allow for a wider variety of modeling. Even so, the findings generated by the case study will still be of value for mapping out potential future influence campaigns of a similar style.

Given the overwhelming amount of ongoing cognitive warfare in society today, avenues for future analysis are limited only by imagination. Teams that attempted to use manipulated content to influence social media conversations during a U.S. national election were examined. One team, nicknamed the "Kavun," engaged in relatively sophisticated operations on social media platforms and internet forums in English and Arabic.

7.3. Brexit Referendum

Many legal and political initiatives taken by the EU involve a shift in the level of policy concern about issues, raising them to a more salient, supranational level of aggregation. There has been a strong cognitive campaign in favor of 'European' roles for policy concerns that previous accepted national settings. The empirical opportunities to explore the processes and consequences of identity change in the European context are almost limitless (Goodwin et al., 2018). The Brexit referendum provides a very rare case to observe the relative consequences of two very different types of message framing.

Before the referendum, it was undeniable at least two frame effects were to be considered. First is the frame feature. The debate since the autumn of 2015 has exposed a prime frame embedding a strong issue salience shift. Although the concept of a frame is not very precise, in contrast to message and theme, in this analysis a frame is conceived as a feature of the message that compresses a larger number of cues and relies on a cognitive schemata that is more or less shared among a certain group of individuals and that helps them to understand the issue. The 'for' and 'against' frames looked relatively settled, and the tone was set with a 'camps' campaign style. The supportive or opponent markers of 'in' and 'out' could influence whole

groups of campaign events that were directly coded with ‘for’ and ‘against’ frames. In a world of sampled actions of limited time and perfect recall, it is unlikely that campaigns can create effects entirely free from this priming base. The structure and results of the referendum movement and campaign exercises were consistent with language, in particular with a recent category coherent to linguistic or textual structure. The ‘EU stables’ refer to the targets of the self-act, be it the EU or specific EU policy aspects. The major exit choices were all access in previous analyses based on the types and arguments of such self-act choices, suggesting that English rhetoric was well-structured with regards to its mention space.

The relatively low salience of the frames, together with its long-suit edge, provides an especially nice case for the investigation of indirect frame sway by spillover style effects. In the days leading up to the referendum, no events directly aimed at fostering voluntary narrows in ‘EU stables’ were open to sampling. Nevertheless, during this period, the anti-Brexit group found room for promoting cognitive reappraisals of close antinomy or opposition to public action ‘in’. This was successfully coupled with the campaign style of the ‘in’ standard. Inference to much broader framing-minded differences was granted by the finding of the prominence of these posts as well as their positive tone and widespread. The systemically constrained referendum campaign yielded a highly angled wedge by construction. The conditions of the bouts along with the earlier set frame exhibition periods are likely to have carved irreversible whetstone wedge for processing the cognitive reversal. The deliberation capabilities of individuals seem better at reappraising broader than highlighted exposure frames.

8. ETHICAL CONSIDERATIONS

The emergence of technologies that target the human brain and central nervous system has prompted efforts toward targeted changes in belief, judgement, or decision-making. As the nature and capabilities of technologies have evolved, fears about their potential misuse have prompted scientific communities to engage proactively on the ethical challenges these raise: should they be developed, to what ends, how might they be regulated, and what kinds of safeguards should be put in place? Domestically, the focus is often on protections for civil society against the efforts of actors within states. Internationally, there has been concern primarily about illicit attempts by states or non-state groups to acquire chemical or biological weapons, and how states might act collectively to prevent and respond to such action.

Among the technologies and capabilities of concern discussed by the scientific community are those that fuse the measurement and/or manipulation of brain signals through imaging or other modalities with physical, physiological, or psychophysical interventions. Applications include restoration of function following neurological disorders (therapeutic or primary brain-computer interface), augmentation of normal function (enhancement or primary Brain Computer Interface), and elicitation of changes in function (disruption or non-primary Brain Computer Interface) (N. Munyon, 2018). These have the potential, when applied across contexts, to either enhance or disrupt individual or societal cognition, perception, emotion, or behavior. Evidently, there is great promise in developing the technology to restore function for individuals who suffer from debilitating conditions. However, many in the scientific

community acknowledge concern over dual-use implications of restoration technologies, and the potential utility they might have in worse-case scenarios.

8.1. Moral Implications

The weaponization of cognitive vulnerabilities raises moral questions around cognitive warfare, its regulation, and its permissibility. Military research and development into psychological and cognitive warfare are growing rapidly and the effects of its use are already being felt around the world. Additionally, an arms race is underway to make techniques more effective and harder to defend against. Weaponizing cognitive vulnerabilities is currently unregulated. All material warfare techniques have received scrutiny at one point, and efforts to regulate or proscribe them have occurred post-invention. There are pressing questions about whether, on the balance of foreseeable harms and benefits, cognitive warfare techniques merit regulation, where the burden of proof to justify their permissibility would lie, and what form regulation should take (Kate Devitt, 2022). The proposed moral consideration asks whether cognitive warfare techniques might avoid cross-temporal regret and needless suffering, in virtue of producing better-assisted choices and favorable behavioral shifts. While input to cognition is an obvious target of attack, informatic infrastructure and the culture buildings on them should not escape notice. Information warfare, cultural warfare, and cognitive warfare, beyond their over-reporting of attention economy dynamics, inject content supporting conspiracy ideation and opportunistic epistemic contagion into more direct agential and relational conduits (Reichert, 2019). The attacks being inflicted by these indirect alterable agents, unmoored from interpretable volition and remorselessly producing hate, division, and violence, are perhaps more tentatively and tractably contemplated than the classic take in ethical philosophy of existential risk and unfair choice.

8.2. Responsibility of Information Providers

When human beings engage in social situations involving a common mode of discourse, they expect to understand what is meant by words, phrases, and sentences in order to make inferences without undue difficulties. They also expect that all parties will do their best not to mislead each other in their discourse and to assist each other to understand what they mean by their words and phrases. Such expectations form a cooperative principle with specific conversational maxims governing the performance of the act of discourse. Four basic maxims govern the performance of acts of discourse: quantity, quality, relation, and manner. Other associated conversational maxims elaborate on these four maxims to ensure the cooperative principle is followed. A virtual community is an arena in which individuals act, and verbal discourse is a basic part of such an arena. Responsibility of the planning and implementing of discourse formation on the Internet in practice is relative since individuals have control over the nature and contents of their part of the discourse formation.

Virtual communities on the Internet serve as a model case to analyze the issues of ensuring a discourse commons where responsibility for feeding information into the commons does not merely consist of its taking place on the Internet, but also of the feeding agents adopting certain discourse ethics. Such discourse ethics obligates those adopting it to frame the contents of their part of the discourse formation in such a way that individuals who go to their part of the

discourse commons get the type of information they know it is in their own best interests to obtain. Information providers who adopt the ideal discourse ethics in practice take a variety of forms in existing virtual communities. Some of them are individuals who adopt a personal news service or online magazine editor position, and frame the contents of their discourse as such a news commentator or editor in their own discourse commons. In this case, the opinions of news gathering and filtering processes are deployed by these individuals. Other information providers adopt a more interactive form to take the role of a discourse agent position in the discourse commons, filtering and organizing the myriad clues muzzily popping up out of the discourse commons.

As a result of their efforts, individuals are brought a better formed part of the discourse commons consisting of more or less relevant comments on the idea or clue they set out on looking for. Still other information providers take the most complex and elaborate form of representing themselves as an active voluntary discourse agent combining both roles to create, organize, and frame a discourse commons in which either scholars or hobbyists in a certain academic field or a community of interest can gather together taking part on an equal footing. The ethical responsibility of such elaborate community planners is of course heavier than that of the former individuals. Failure to act responsibly in feeding information into the commons amounts to the gaming of the discourse commons.

9. COUNTERMEASURES AGAINST COGNITIVE WARFARE

In the face of cognitive warfare, a concerted effort to build resilience against cognitive warfare is needed, one that spans various sectors and disciplines: media literacy education, critical thinking, and the creation of competitive messaging frameworks. Strong provisions must be established to address the challenges of misinformation and malinformation, specifically issues that public and policy awareness or education can help to combat. This will require the promotion of media literacy and critical thought as lower stakes, ubiquitous educational realms. At an institutional level, independent journalism and media should have the resources and protection they need to compete in the marketplace of ideas. This can take the form of funding, expertise, access to technology, or legal considerations such as antitrust actions against monopolistic information feeds. Deep learning models for framed detection and source authentication should be piloted in the platforms that take ownership of hosting and aggregating contested information. Provisions for designing illustrative competition should be included if a plague of severity warrants it. These requirements all bear consideration, and many should be worked into a cogent and wide-reaching set of policy recommendations for both parliamentary and private consideration.

As is often the case, heightened awareness brings new vigilance but not rest. The preparedness of any institutions or organizations that can be mobilized to combat a wide range of cognitive assaults rests on an understanding of them in advance. Institutional vulnerabilities should be accounted for, and pre-approved plans and strategies to counteract attacks should be worked into possible scenarios.

Much has been made of tacit recognition as a facet of human agency's relationship to the interpretation of information. A sociological basis that composes shared modes of meaning-

making is salient in the practice of meaning-making. Leverage may be gained through deliberate alternative deployment as scaffolding whereby recognized modalities are utilized nonstandardly. Individual cognition is both individual and conventional. The publicly known shared uptake and response models of gradual surprise with amplification and boredom is where an implicit sociality of public knowledge taps into the scaffolds of semantic generation. This means spaces of tacit understanding absolutely dictate the terms on which given content can be reacted to. Calculus both coacts with representation practices and hosts heretofore spilling place-based induced change. Facilitating a public understanding of possible messaging frameworks holds that each individual has a further interpretive skill to hold content in ways inaccessible to computation. Public knowledge support will enable competitively framing beliefs to spontaneously emerge and stem alienation amongst target classes. Baseline engagement is assured. So, to take a potential point of starting victory, monied interests in engineering and alternative energy development have cultivated a negative political mood and misrecognition of the relative urgency and epochal scope.

9.1. Media Literacy Education

Disinformation tactics have been employed by individuals and groups for many years, and there have always been attempts to combat them. We all need tools to inoculate ourselves against damage from the impact of disinformation. Knowing how propaganda works is a first step in building resilience against it. It is hoped that educators around the world will take up the questions and challenges posed within this initiative to better prepare students for their role as critical consumers and disseminators of information. The mind, as such, has always been crucial in warfare. In the current, globally interconnected and digital world, the domains and weapons of cognitive warfare have changed, even if they have not been novel. Information has long been recognized as a weapon or a target in military operations: industrial and infrastructure services may be attacked in order to damage the military or service delivery of an adversary. By analogy, ‘cognitive warfare’ may be used to weaken the enemy’s potential to identify combatants and combat strategies, or the legitimacy of the cause or effort. The mind may be targeted, led astray, or confused by weaponized information (Berkman, 2018). It is proposed ‘cognitive warfare’ as a core form of information warfare, making the mind expressly a battlefield.

Cognitive warfare (CW) is presented, in part, at these overlapping levels of complexity: 1. the overarching proposal of CW as a fundamental mode and level of contemporary DDR, extended for immediate empirical assessment; 2. the underlying rationale for CW, drawing on hindsight, projection and forecast, leading to its conceptualization; and 3. the indeterminate means and modalities that may characterize the practice of CW. The focus is on matters of definition rather than the historical narrative of contemporary interests in this issue of information warfare (McQueeney, 2014). Currently, a 21st century rendition of information warfare promoted and run by state and agency actors, particularly in socially-mediated digital (and other) domains, is termed CW; with its pursuits characterized as weaponized information, misinformation, disinformation, and propaganda.

9.2. Critical Thinking Skills

Critical thinking is considered one of the most important skills among professions and is a focus of many societies. Teaching methods to improve critical thinking have proliferated in many educational institutions. Yet, when viewed broadly, critical thinking is not convenient. For example in investment or political institutions, it is often considered unwise to suggest views contrary to the consensus. Moreover, inspiring a universal urge to cultivate critical thinking in leadership can lead to disarray. Thinking in unconventional ways for too long is hard to contain to only small subgroups. However, in corporations the CEO or a key owner can usually shape the framework within otherwise engaged personnel set up cognitive schemata to enhance productivity as expected by the corporation.

The suicide of well regarded executives during corporate collapses misconceived the interdependence of cultural and cognitive constituents of thinking. Desired ideas, mental models or frames must be instilled among the personnel. These must imbibe religiously, somewhat like those on the crusades or on the other hand those in an inquisitional setting. Much depends on leaders obviously, but there are constraints on what choices are taken or condoned. While these collective cognitive and moral frameworks can be formulated explicitly, they are often implicit and instinctive. Changes in leadership or thinking are usually extremely difficult. Intensification of change efforts can, of course, backfire simply because these lead to strengthening of the old frameworks that make the change more distant rather than bringing it closer.

In the Cold War the USA and USSR had difficulty countering each other's social barriers to perception and thinking even with costly efforts. The fall of the Berlin wall was unexpected on both sides for this reason. However one side can take on an unexpected shift or change to the old dominant and cherished style. The cognitive defence of nations, corporations and people and how understanding can be created of all cognitive barriers in a system is universally important. Increasing the competency of an organisation's ability to absorb alternative views and adversarial ideas is of growing importance. To ensure it, an integrated coevolution of moral and cognitive systems, these latter having both cultural and technological foundations, is increasingly important.

10. FUTURE TRENDS IN COGNITIVE WARFARE

Cognitive warfare will be a battlefield for minds, as thoughts and perceptions - and even those who have them - blend, blur and merge, while massively disrupted and manipulated by hordes of intelligent and impossible to control digital entities and agents in the near future (Théron & Kott, 2019). While continuing to mostly ignore cognitive attacks, many military, intelligence, and law enforcement agencies currently recognize the cognitive domains in capacities like SIGINT, HUMINT or PSYOP. At a conceptual level, military organizations are aware that cognitive warfare can be part of conflict strategies. However, literature, models, and procedures to focus the topic, train and hone skills, or test countermeasures either do not exist or are being discarded as too mundane. Partially due to the lack of immediate effect, cognitive warfare is still significantly behind the technical challenges, crisis, and responses, that other domains like cyber, space, or tangled are facing. But these other domains (and more broadly STEAM) are

increasingly cognitive and brain-influencing by their nature and the social connections, new info, and knowledge they create, amplify, and engage with individual and collective cognition. Neuromorphic networks, systems, and technologies are looming in the R&D horizon, already design cerebral protocols, recreating abnormal evolutions of human-like intelligence to simulate mood, faking data memories, hindrances, and outputs of machine learning, and building new type agent education pipelines.

Independently of who wins the race to achieve this quantitative and qualitative leap of intelligence, its existence would generically threaten existing and emerging cyber, global control, and growth monopolies and empires, as it fundamentally means the end of the novelty paradigm upon which social and economic dynamism is continuously produced and consumed for the past half a century (Mayer, 2018). To this end, it could favor an intelligence clearing action: identify, select, and remand the most dangerous antagonistic agents. The two key multi-dimensional and interactive classes of cognitive threat agents are those autonomous intelligent goodware, that randomly changes and combines behavioral libraries and models, equipped with or able to auto-learn disruptive capabilities, privacy breaching rules, false information simulation protocols, and online human likeness; and the massive intelligent information hygiene software and lexicon fixers, that mangles OS code, and device firmware, corrupts algorithms, obfuscates data, and limits accessibility and flow of info. Merging these capabilities would have unprecedented consequences for life and civilization on the planet and their competition and ownership could allow new economic, political, and ideological paradigms to flourish.

10.1. Artificial Intelligence and Cognitive Warfare

The revolution in AI, specifically deep-learning neural networks on powerful computing systems, catalyzed a rush to integrate AI into numerous applications. AI is already deeply integrated into society and weapons systems like fighter aircraft, missiles, and naval units. Many military actors, recognizing the importance of AI, ramped up efforts to develop military applications for AI (Hallaq et al., 1970).

Emerging AI systems in defense applications are still overly basic and naive. AI systems face scrutiny from informed individuals, both inside and outside of military organizations. AI/ML systems may be ineffective due to the selections made in training, or unintentional biases can be designed into algorithmic heuristics. It is too late to take a pen-and-paper approach to manually inspect AI for flaws. Groups outside a developer's organization can reverse-engineer an algorithm and make it act outside of its original intentions, causing military applications to fail catastrophically.

A symbiotic relationship can expect to exist following the development of trustworthy and effective AI systems. Threats to AI systems from other AI systems can be expected as the value of nations' AI increases. AI systems can also enable attacks on trusted systems to manipulate their behaviors or outputs. The military must establish norms regarding the use, reliability, and robustness of AI systems (Feldman et al., 2019).

Military conflicts' rapidly changing nature is an underlying enabler of full-spectrum AI strategy. Nations with poor AI will lose conflicts against opponents that leverage AI faster and

more effectively. Significant alteration of military culture, doctrine, and processes is necessary for industries and nations to harness AI effectively. Nations need full-spectrum AI cadences to increase velocity and recursiveness of AI decisions, development, and generation against the complexity of conflicts and threats changing military needs.

10.2. The Role of Big Data

Large volumes of data available today far exceed what was previously possible. This vast volume of data, stemming from diverse sources such as social networks, cyber scans, mobile devices, public announcements, and other evolving media, has qualitatively and quantitatively changed and is expected to grow in the days ahead. There is a pressing need to assimilate as much of that data into something that is timely, discoverable, and actionable, providing tools necessary for systemic analysis for immediate and future requirements. Only as much information is needed that is known to be outdated, erroneous, inaccurate, incomplete, or otherwise not relevant to context.

The role of Big Data is elucidated through these two viewpoints—technologically and sociologically. Technically, it describes advanced processes adopted for the collection and automated analysis of Big Data on open analytic techniques using statistical and machine learning processes adopted in AI systems designed to counter adversarial machine learning. Sensing AI is contrasted to the tactical analytics-enabled version that not only handles but leverages deception. Overall, while Big Data sources and analytics are reviewed, there is also a fusing component that integrates entity detection, name matching, similar moniker detection, co-reference resolution, relation extraction, and fuzzy temporal analysis. How all these together contribute to the larger vision of Command, Control, Communications, Computers, Intelligence based probabilistic predictive risk mapping is described (Gangi, 2025). Given the usage of knowledge graphs or graphs learned from knowledge in the embedding space for such lower dimensional analytical and interpretability readiness of macro-level knowledge on news and geopolitical scoping is discussed.

At the sociological level, using political-science-based game theory insights, the adversarial nature of Big Data is described detailing how the misuse of Big Data by agencies, CMOs, and institutions of countries lead to sub-oscillation echo chambers in willingness-to-divulge privacy needed for a current AI system. How such echo chambers are examined for a MATURE and CINDERELLA model in terms of two parameters— relative capacity-knowledge signified by how much the agents know and the agent-agent interaction type in the form of egoistic/friendly and reciprocally secretive/honest that elicit infopolitical responses enabling utility—is described. Further, trade-offs between response-burden and knowledge-mellowness, and developmental variations for long-time scales are discussed based on which modifications are suggested to mitigate echo chambers for smoother maps.

11. INTERNATIONAL PERSPECTIVES ON COGNITIVE WARFARE

The mental frame of cognitive warfare has become a popular topic of interest for strategists and public authorities. A strong interpretation on how to combat interference of this sort has been offered by French authors, especially through a seminal work. They see cognitive warfare as part of a total war approach. This viewpoint is supported by the suggestions that certain

countries consider their international competition to be total war in scope, which includes not only a societal approach to cyber and hybrid warfare but also a social-psychological approach to warfare. However, this total war view on cognitive warfare has not yet received as much credibility among other groups, and this prompts concern about gaps in understanding. This may be a precondition that leaves an opening for cognitive warfare scholars to interpret strategically narrow definitions in an extreme manner. The need for clarification and specification of cognitive warfare, in order for the international discourse to come up with a more balanced understanding is evident.

Approaches in cognitive warfare are analyzed based on the more generative parameters of intent, methods, and means. This mapping is the starting point for a discussion of what an internationally accepted discourse on cognitive warfare might look like. It is argued that a non-reporting low-intent approach to primary covert methods is the most plausible course of action, although such an international attendance is not evident at present. In the absence of an established international cognitive warfare discourse this is an area with a known aperture and a known delivery channel. Certain countries and non-state actors are exploiting the gap that is laid bare by the lack of an internationally accepted discourse. Cognitive warfare has clearly become a multipolar process (González, 2023).

The framing of cognitive warfare is still in progress and should be seen as a study undertaken as part of a natural course of events, with a more strategic model on the cognitive environment of warfare ending phases being possibly the most plausible outcome. One plausible closing of the framing process is focused on cognitive warfare mechanisms that target specialist and micro-centers of the cognitive domain and environment. This would be a summary of cognitive system vulnerability.

11.1. Global Responses

The onus is on leaders of other states – notably those with democratic institutions – not to collude with a US government that resorts to the terrific wonder; more subtly, it falls to them to devise some mechanism for a gradual but decisive attenuation of current terrorism of the US type, states still envisaged in a somewhat antiquated paradigm of nation-states, military buildup, allied military confrontations, and limited conventional warfare that can cater for victory. In tech industry, academics allied with big IT will assist to rally public support for a slightly–updated project to end US unilateralism in launching wars (Delgado et al., 2019; Editor, 2003). Once there is acknowledgement of the fact that cognition is convoluted and inefficient to non-expert minds, that an effective technology of mass cognitive manipulation is at hand, and that the intense cognitive warfare against one's people by an elite is endemic to the times, able and willful minds capable of formidable counter-measures to disarming the elite's unassailable position can be expected to engage despite the fact that that position once entrenched cannot be divested in combat but at the cost of devastation on an unbelievable scale and on a completely altered future. In pragmatic terms, talk of warfare, however it may be differentiated qualitatively from conventional state action, functionalism and curve-fitting notwithstanding, is likely to be regarded with disdain, as it is traditional to consider warfare an activity innate to nations or states, and conventional states act at national and international systemic levels. Further, hobbled by antiquated paradigms of military organization,

comprehension, struggle, and victory, non-conventionally warring entities are anticipated to be swept off. Added to this is the trivialization of warfare, exhibited by television networks formatting coverage as entertainment and by some academics writing groundless articles comparing political constituencies to impoverished armies with no means to wage war (Delgado et al., 2019).. If it is the case that the widening gulf between cognitive sophistication and intelligence promulgated by this elite and the absence of it or cynical tolerance of it in the rest is fast becoming unbridgeable, the machinations of the elite will be self-destructive if not unravelled. If it is only the decision-making of this elite that is subject to an extraordinary alteration in kind, and this is conducive to states and societies' current comfort, there can be much greater catastrophes still unimagined in the near future, though identifiably menacing forces are culturally distant, already perceptible, unguided by convention.

11.2. Comparative Analysis of Strategies

A comparative analysis of two strategic sub-categories across the two case studies is provided. First, the effect of cyber influence exploitation on domestic political processes and then the employment of malicious cyberoperation to assist interstate cyber aggression are examined. Four elements of comparison are presented: (1) mode of influence and operational function, (2) vulnerabilities exploited, (3) escalation potential, and (4) countermeasures. By mapping these four elements of comparison onto the each of the two case studies' strategic sub-category, a detailed evaluation on how they compared across the overall set of assessments can be achieved. On the basis of the strategic assessments made against the two case studies, the comparative analysis is assessed.

With regard to the Russian cyber influence exploitation that affected the US Presidential election in 2016 and the downing of Malaysian Airlines flight MH17, it is important to compare the use of social media misinformation and cyber-misinformation, attributing the incident to Ukrainian security forces through hack-and-leak operations. The former seeks to influence or fuel domestic political processes in order to benefit a target state's political stance and to disrupt political reform presently sought by another, who is designated as a rival state. The former's operational function is to amplify divisive issues, magnify factual disagreements and spread misinformation that may have a negative effect on the balance of power, such as in the case of affecting election results that favor a Russian-stances political appointment. As an election interference banner, more attention is paid to a set of facilities influencing the domestic political processes of the target state than to improving its own advantage to achieve the goal. As such, it could be claimed that the Russian cyber influence exploitation contrast with the prior perspectives on its geographical limitations and scrutiny on planning steps. The operational effect of the US Presidential election affair compares with model templates of prior strategic assessment made with regard to domestic cyber influence exploitation. Overall, it is expected that newly developed operational approach would be examined, challenged and debated further within an acyclic evolution of an operational environment of malicious usage.

12. CONCLUSION

Psychological warfare is commonly referred to a battle for hearts and minds (Editor, 2018). The underlying assumption is straightforward: if the desired mental state could be induced, the

intended behavioral consequence should follow. But inducing the desired mental state is never simple, and there are many reasons to believe that it is harder than envisaged in this simplified model. The psychology of shame illustrates some of the essential difficulties that should be reckoned with in the pursuit of inducing behavioral change.

Several human beings of various ages and cultures would remember a similar shameful experience: being ridiculed for face-plants after a poorly executed gymnastics performance in elementary school. The sensation of being observed with disdain is typical of the emotion evoked by this exposure to public ridicule, and shameful memories also frequently consist of components suggestive of sadism and belittlement. Shame should be understood as a social and self-conscious emotion that is usually experienced in situations of negative evaluation and moral transgression, which have an effect on the self (Fenici, 2017). Constructivist psychologists have uncovered that respondents often misconstrue the term "shame," producing results that are inconsistent with their manifestly shameful behavior. The study of shame induces a realization of how complex is the web of mental states and states of mind that is of core interest in understanding psychological warfare (Delgado et al., 2019). The cognitive structure underlying shame further highlights that the catchphrase “mind as a battlefield” is simplistic and misleading. The sophistication, complexity and heterogeneity of mind states additionally enact the challenge of inferring and altering belief states.

In the pursuit of understanding the self and its non-observable affairs, the knowledge of the mind has been a pursuit of humanity. Its understood secrecy, astonishing range of formats of representation, and the great accuracy or distortion in the reported experience - from perfect retentive memories to the blankness due to an Alzheimer's episode - have rendered this human endowment a fertile ground for exploration, experimentation and abuse. The essential plea is for researchers, social networkers and governments, to use democratic procedures to frame a better global order that could ensure the basic and their privacy rights, and by extension social peace.

REFERENCES:

[1] Bibighaus, D. L. (2015). How Power-Laws Re-Write The Rules Of Cyber Warfare. *Journal of Strategic Security,* 8(4), 39–52. http://www.jstor.org/stable/26465214

[2] Delgado Moran, J. J.; Mazurier, P.A. & Payá Santos, C. A. (2019). The race to securitize the arctic in a post-cold War scenario. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 4(1), 59-64. http://hdl.handle.net/10272/17180

[3] Delgado-Moran, J. J.; (2024). Acoso y agresión en las nuevas tecnologías: ciberacoso / ciberodio. AlmaMater. Cuadernos de Psicosociobiología de la Violencia: Educación y Prevención, nº 5, Dykinson, pp. 107-122. https://doi.org/10.14679/3315

[4] Editor, IBPP (2018) "Psychological Warfare and the Kingdom of Shame," International Bulletin of Political Psychology: Vol. 18 (2) , Article 1. https://commons.erau.edu/ibpp/vol18/iss2/1

[5] Editor, IBPP (2003) "Political Authority and Social Cognitions on the War on Terrorism with Global Reach: Airport Security, Terrorism Contingent on a United States-Led Attack on Iraq, Smallpox Vaccinations," International Bulletin of Political Psychology: Vol. 14 : Iss. 8 , Article 5. https://commons.erau.edu/ibpp/vol14/iss8/5

[6] Editor, IBPP (1999) "The Eritrea-Ethiopia War: How Helpful are Psychological Theories of Warfare?," International Bulletin of Political Psychology: Vol. 6 (7) , Article 4. https://commons.erau.edu/ibpp/vol6/iss7/4

[7] Espinoza, M. (2024). Weaponization of Conscience in Cybercrime and Online Fraud: A Novel Systems Theory. *Scientific Bulletin*, *29* (1), 2024. 17-25. https://doi.org/10.2478/bsaft-2024-0003

[8] Feldman, P., Dant, A., & Massey, A. (2019). Integrating Artificial Intelligence into Weapon Systems. Computer Science. Artificial Intelligence. https://doi.org/10.48550/arXiv.1905.03899

[9] Fenici, M. (2017). Rebuilding the Landscape of Psychological Understanding After the Mindreading War. *Phenomenology and Mind,* (12), 142–150. https://doi.org/10.13128/Phe_Mi-21113

[10] Ganji, M., Dehghantanha, A., Izura-Udzir, N. and Damshenas, M. (2013) Cyber Warfare Trends and Future. Advances in Information Sciences and Service Sciences. 5(13) Busan, Korea.

[11] Gangi Guillén, G, K. (2025). Derechos humanos y derecho penal en la era de la inteligencia artificial: retos y propuestas. *Cuadernos de RES PUBLICA en derecho y criminología*, https://doi.org/10.46661/respublica.11635.

[12] Goodwin, M., Hix, S., & Pickup, M. (2020). For and Against Brexit: A Survey Experiment of the Impact of Campaign Effects on Public Attitudes toward EU Membership. *British Journal of Political Science*, *50*(2), 481–495. doi:10.1017/S0007123417000667

[13] Gomez, M., & Whyte, C. (2021, December 8). Unpacking Strategic Behavior in Cyberspace: A Schema-Driven Approach. https://doi.org/10.31235/osf.io/hfsru

[14] González Trigo, N, A. (2023). El agente encubierto ante la criminalidad organizada transnacional. *Cuadernos de RES PUBLICA en derecho y criminología,* (1). https://doi.org/10.46661/respublica.8062

[15] Hallaq, Bilal, Somer, Tiia, Osula, Anna-Maria, Ngo, Kim and Mitchener-Nissen, Timothy (2017) Artificial intelligence within the military domain and cyber warfare. In: 16th European Conference on Cyber Warfare and Security 29-30 Proceedings of 16th European Conference on Cyber Warfare and Security ISBN 9781510845190.

[16] Horowitz, M.A. (2019). Disinformation as warfare in the digital age: dimensions, dilemmas, and solutions. Journal of Vincentian Social Action: Vol. 4: Iss. 2, Article 5. https://scholar.stjohns.edu/jovsa/vol4/iss2/5

[17] Kate Devitt, S. (2022). Bad, mad, and cooked: Moral responsibility for civilian harms in human-AI military teams. *Computers and Society* https://doi.org/10.48550/arXiv.2211.06326

[18] Liz Rivas, L. (2024).Violencia y agresión entre iguales a través de las TICS: Cyberbulling. AlmaMater. Cuadernos de Psicosociobiología de la Violencia: Educación y Prevención, nº 5, 2024, Dykinson, pp. 89-105. https://doi.org/10.14679/3314

[19] Luque Juárez, J. M., Payá Santos , C. A., & Arenas Morales, F. (2023). Contexto de las políticas de seguridad ciudadana. *Cuadernos de RES PUBLICA en derecho y criminología*, (2), 69–82. https://doi.org/10.46661/respublica.8293

[20] Maréchal, N. (2017). Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communication, 5*(1), 29-41. https://doi.org/10.17645/mac.v5i1.808

[21] Martino, L. (2024a). Cybersecurity in Italy. Governance, Policies and Ecosystem. Springer Nature. https://doi.org/10.1007/978-3-031-64396-5

[22] Martino, L. (2018). La quinta dimensione della conflittualità. L'ascesa del cyberspazio ei suoi effetti sulla politica internazionale. Politica e Società, [online] 1, pp.61–76. doi:https://doi.org/10.4476/89790.

[23] Martino, L. (2021). Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza. *IAI Papers*, [online] 21(13). Available at: https://www.iai.it/sites/default/files/iaip2113.pdf.

[24] Martino, L. (2023). La guerra nel XXI secolo: la dimensione cyber e il conflitto russo-ucraino. In: *La guerra tiepida: Il conflitto ucraino e il futuro dei rapporti tra Russia e Occidente*. Rome: Luiss University Press.

[25] Martino, L. (2024b). International Law, State Sovereignty and Competition in the Digital Age. *Rivista di filosofia del diritto internazionale e della politica globale*, Vol. 21, Nº. 2, 2024. https://dialnet.unirioja.es/descarga/articulo/10098952.pdf

[26] Mandel DR and Kapler IV (2018) Cognitive Style and Frame Susceptibility in Decision-Making. Front. Psychol. 9:1461. doi: 10.3389/fpsyg.2018.01461

[27] Mayer, M. (2018). Artificial Intelligence and Cyber Power from a Strategic Perspective. IFS Insights; April. https://brage.bibsys. no/xmlui/bitstream/handle/11250/2497514/IFS%20Insights_4_2018_Mayer.pdf

[28] McQueeney, K. (2014). Disrupting Islamophobia: Teaching the Social Construction of Terrorism in the Mass Media. *International Journal of Teaching and Learning in Higher Education*, 26(2), 297-309. https://scholarworks.merrimack.edu/crm_facpub/3

[29] Munyon CN (2018) Neuroethics of Non-primary Brain Computer Interface: Focus on Potential Military Applications. Frontiers. Neurosci. 12:696. doi: 10.3389/fnins.2018.00696

[30] Oates, S. (2020). The easy weaponization of social media: why profit has trumped security for U.S. companies. Digi War 1, 117–122 https://doi.org/10.1057/s42984-020-00012-z

[31] Ongchoco, J.D.K., R. Walter-Terrill, & B.J. Scholl, (2023).Visual event boundaries restrict anchoring effects in decision-making, Proc. Natl. Acad. Sci. U.S.A. 120 (44) e2303883120, https://doi.org/10.1073/pnas.2303883120

[32] Payá-Santos, C. A. (2023). El desempeño de la inteligencia en España en el ámbito público, empresarial y académico. *Revista Científica General José María Córdova*, *21*(44), 1029–1047. https://doi.org/10.21830/19006586.1222

[33] Payá Santos, C. A, & Delgado Morán, J. J;. Martino, L; García Segura, L, A.; Diz Casal, J, & Fernández Rodríguez, J, C. (2023). Fuzzy Logic analysis for managing Uncertain Situations. *Review of Contemporary Philosophy* Vol 22 (1), 2023 pp. 6780 -6797. https://doi.org/10.52783/rcp.1132

[34] Payá Santos C., Delgado Morán J. J, & Mazurier P. A. (2018). Individual terrorism as a response to the distorted phenomenon of cultural identity. En J. Ramírez & G. Abad-Quintanal (Eds.), Cross-cultural dialogue as a conflict management strategy. *Advanced*

sciences and technologies for security applications. (pp. 34-45). Springer. https://doi.org/10.1007/978-3-319-77231-8_4

[35] Payá Santos, C. A; Rodríguez González, V; Domínguez Pineda, N. Z; Diz Casal, J; Fernández Rodríguez, J. C. & Delgado Morán, J. J. (2025). Role of the Human Factor in the Cybersecurity Ecosystem. *Journal of Information Systems Engineering and Management*,10(4). https://doi.org/10.52783/jisem.v10i4.8983

[36] Reichert, B. (2019). Moral Disengagement and the Support for Military Force: A Review. Business and Public Administration Studies, 2019, Vol. 12, No. 1 37 Published by the Washington Institute of China Studies. All rights reserved.

[37] Rodríguez González, V., Payá, Santos., C, A., & Peña Herrera. B. (2023). Estudio criminológico del ciberdelincuente y sus víctimas. *Cuadernos de RES PUBLICA en Derecho y criminología,* (1) 95-107. https://doi.org/10.46661/respublica.8072.

[38] Saner, Lelyn Duane (2008) Framing in the Wild: Expressions of Decisions in Real-World Situations. Doctoral Dissertation, University of Pittsburgh. http://d-scholarship.pitt.edu/id/eprint/7425

[39] Sanz González, R, Luque Juárez, J, M.ª, Martino, L, Liz Rivas, L, Delgado Morán, J, J, & Payá Santos, C, A. (2024) Artificial Intelligence Applications for Criminology and Police Sciences. *International Journal of Humanities and Social Science.* Vol. 14, No. 2, pp. 139-148. https://doi.org/10.15640/jehd.v14n2a14

[40] Scanzillo, Thomas M. and Lopacienski, Edward M., (2015). "Influence Operations and the Human Domain" *CIWAG Case Studies.* 13. https://digital-commons.usnwc.edu/ciwag-case-studies/13

[41] Steven L. Winter, (1989). The Cognitive Dimension of the Agon Between Legal Power and Narrative Meaning, 87 Mich. L. Rev. 2225 https://repository.law.umich.edu/mlr/vol87/iss8/6

[42] Théron, P. & Kott, A. (2019). When Autonomous Intelligent Goodware will Fight Autonomous Intelligent Malware: A Possible Future of Cyber Defense, "MILCOM 2019 IEEE Military Communications Conference (MILCOM), pp. 1-7, https://doi.org/ 10.1109/MILCOM47813.2019.9021038.

[43] Yasseri, T. & Reher, J. (2022). "Fooled by facts: quantifying anchoring bias through a large-scale experiment," *Journal of Computational Social Science,* Springer, vol. 5(1), pages 1001-1021, https://doi.org/10.1007/s42001-021-00158-0