USI Occasional Paper

No. – 3 – 2024

# Impact of Technology Enabled Cognitive Operations in Hybrid Warfare

Lieutenant General (Dr) RS Panwar, AVSM, SM, VSM (Retd)

## Introduction

Warfare conducted in the cognitive domain is not a new phenomenon. Sun Tzu's maxim of 'Winning Without Fighting', which essentially entails subduing the enemy by attacking his will, is perhaps the most widely quoted maxim related to warfighting in the cognitive domain. The Psychological Operations (Psyops), public affairs, and Military Information Support Operations functions laid down the in United States (US) Information Operations (IO) Doctrine,[1] the Reflexive Control Concept of Russia[2] and the Three Warfares Strategy of China[3] are all different flavours of cognitive domain operations. The Indian Army's (IA) Doctrine on Information Warfare (IW) of 2010[4] includes psychological warfare as one of its three main components. A Joint Doctrine on Perception Management and Psyops was published in 2010 by the Headquarters Integrated Defence Staff.[5] The most recent manifestation of the cognitive domain operations during an armed conflict is in the form of the so-called narrative wars being orchestrated in the ongoing Russia-Ukraine conflict.

Cognitive warfare as a term, however, is recent in the literature on modern warfare, with a 2020 North Atlantic Treaty Organisation (NATO) sponsored study by the same name giving a degree of formality to it.[6,7,8] The work of Dr James Giordano and his team at Georgetown University, US, is one of the primary reference documents for this study, and the NATO Innovation Hub, which has been set up by its Allied Transformation Command based out of Norfolk, US, continues to pursue and evolve the concept of cognitics in warfare.[9]

**NATO's theory of cognitive warfare includes within its ambit the use of neuro-weapons as well. NATO's stated objective for conducting cognitive operations is "To change not only what people think, but how they think and act".**

There is a qualitative difference, however, between NATO's notion of cognitive warfare and all the other psychological warfare concepts and doctrines listed above. Simply stated, while the other concepts involve the use of information weapons, NATO's theory of cognitive warfare includes within its ambit the use of neuro-weapons as well. NATO's stated objective for conducting cognitive operations is "To change not only what people think, but how they think and act". The 'What people think' part of this objective involves distorting or disrupting information to influence adversary brains. On the other hand, the 'How they think' part refers to the use of neuro-weapons, which physically target the brain to degrade its information processing capability.

In this paper, the use of the term cognitive operations is preferred over cognitive warfare, though the latter is also used at times largely in a synonymous sense. Moreover, cognitive operations are addressed here from a perspective which is more relevant for the Indian Armed Forces and, in general, this term will simply imply 'Operations in the cognitive domain'.

To begin with, cognitive operations are contextualised as a component of the closely related notions of hybrid warfare and grey zone warfare. The relevance of these operations to the military domain are then discussed and it is explained how, as part of IO, they are a component of Multi-domain Operations (MDO), i.e., military operations conducted in a multi-dimensional battlespace. Thereafter, the impact of three emerging disruptive technologies, namely, cyber, Artificial Intelligence (AI) and Neuroscience and Technology (NeuroS/T) on the conduct of cognitive operations is analysed. Finally, after giving an overview of the cognitive operations doctrines and capabilities of some major players, a few broad recommendations are given on what steps India, and particularly the armed forces, need to take to build up effective capabilities in this potent new domain of warfare.

## Cognitive Warfare in 21st Century Battlespace

It is widely believed that the character of warfare is undergoing a transformational change in the 21st Century. One of the primary causes for this transformation is the expansion of the battlespace from the physical to the information and cognitive realms. The weapons used in the expanded portion of the battlespace are largely non-kinetic in character. While elements of non-kinetic warfare have always been employed by nation states in conflict scenarios, it is the increasing potency of offensive cyber operations as well as cognitive operations that has propelled the notion of non-kinetic operations into prominence over the last couple of decades.

**It is widely believed that the character of warfare is undergoing a transformational change in the 21st Century. One of the primary causes for this transformation is the expansion of the battlespace from the physical to the information and cognitive realms.**

**Cognitive Operations: A Potent Weapon in Hybrid Warfare.** In general, all warfare waged by a state is a 'Whole-of-Nation Endeavour', carried out by leveraging Comprehensive National Power (CNP) in all its forms. The Diplomatic, Informational, Military and Economic paradigm, depicted in Figure 1, nicely captures the main elements of CNP.[10] Here the military element represents kinetic operations, while the diplomatic, informational and economic realms are non-kinetic in flavour. Because of the increased effectiveness of non-kinetic operations, leading military strategists have coined new terms for the synergetic employment of kinetic and non-kinetic means of waging war, such as Hybrid Warfare (US)[11], Unrestricted Warfare (China)[12] and New Generation Warfare (Russia)[13], all of which are largely synonymous in meaning, it may be noted that there is a role for the military in two of the non-kinetic elements as well, namely, Military IO and Military Diplomacy. Cognitive Operations are a very potent means of warfare within the Informational element of CNP, the other two elements being cyber operations and Electronic Warfare (EW).

**Cognitive Operations are more Effective in the Grey Zone.** It is important to note that hybrid warfare spans the entire spectrum of conflict. Grey zone warfare, on the other hand, encompasses all the means adopted by states and non-state actors in the operational space between peace and all-out conflict to achieve politico-military objectives. In general, non-kinetic operations, and particularly cognitive operations, have greater relevance in the grey zone, while kinetic operations are more effective during all-out conflicts. That stated, there is a role for both forms of warfare across the full spectrum of conflict. A state may carry out cognitive operations against an

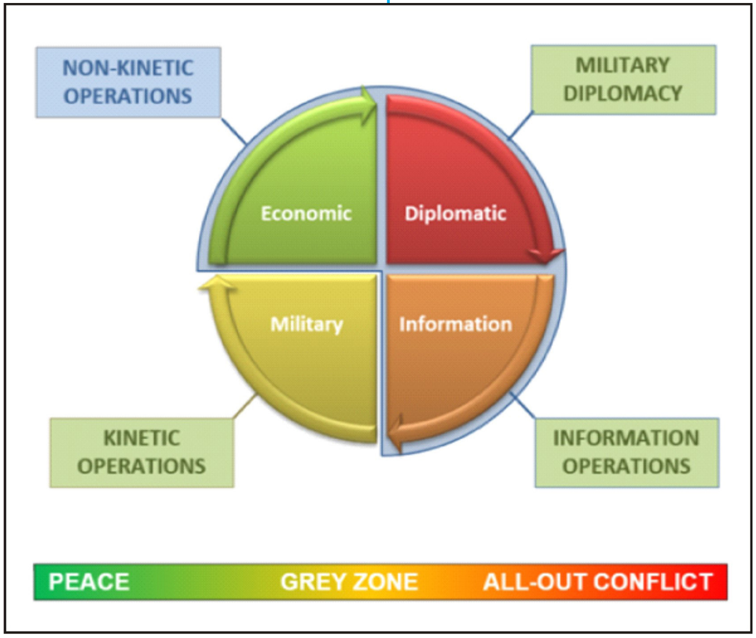


Figure 1

adversary state independently using multiple agencies at its disposal, or as a component of MDO in support of military objectives.

## Cognitive Operations in the Military Context

**While most cognitive operations are likely to be conducted below the threshold of armed conflict, they can have significant impact during all-out conflicts as well, either independently or to facilitate military operations.**

While most cognitive operations are likely to be conducted below the threshold of armed conflict, they can have significant impact during all-out conflicts as well, either independently or to facilitate military operations. Arguably, the armed forces of a state would need to play a significant role in their conduct across the spectrum of conflict. These days most militaries, including the Indian, refer to a five-dimensional battlespace construct, comprising the land, sea, air, space, and cyberspace domains, with operations in this battlespace being referred to as MDO. In this five-dimensional construct, cyberspace should be understood in its wider sense as Info space, encompassing within its ambit the Electro-Magnetic (EM) and cognitive domains as well.[14] These three types of operations may be collectively referred to as 'Military IO' (Refer Figure 2).

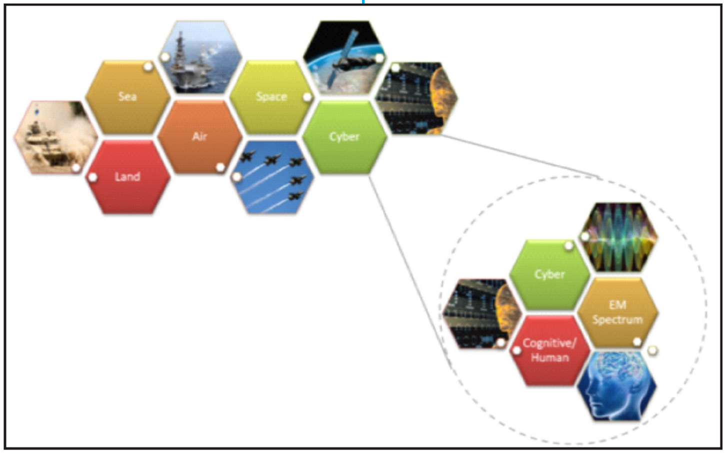


Figure 2

**Military IO: Primary Components**. Figure 3 below differentiates amongst the three primary components of IO: the weapon in the case of EW is EM energy which targets electronics in machines, for cyber operations it is a piece of malicious code targeted against data and software, and for psychological/ cognitive operations the weapon is the message designed to create effects in human minds.[15]

**Cognitive Operations: A Spectrum of Capabilities**. Cognitive operations in the military context include several conceptually different capabilities: Psyops convey selected information - not necessarily truthful - to foreign audiences in order to influence their behaviour; Public Information (PI) aims to inform foreign as well as domestic audiences; military deception is meant to deliberately mislead adversary

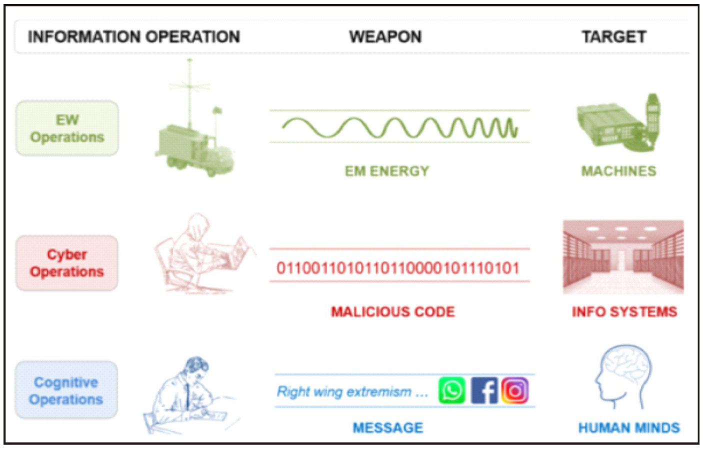


Figure 3

military decision makers; military diplomacy involves relationship building with foreign publics and military audiences; and civil-military operations are activities carried out to influence the civilian populace for achieving operational objectives, and are best characterised as actions that convey meaning. It is important to note that each of these capabilities involves messaging in some form or the other. While kinetic warfare is restricted to the physical realm, IO manifest across the physical, information and cognitive realms, as indicated on Figure 4.

## Cognitive Operations in Cyberspace

Let us now delve into how cognitive operations may be undertaken by suitable agencies, not restricted to the military, during all phases of conflict.

Over the last three decades or so, the global information infrastructure has tremendously improved, with its reach touching almost every individual across the world through cyberspace, with social media platforms and broadcast media being the primary means of information dissemination. Cyberspace and cyber technologies, therefore, have a central role to play in the conduct of state-on-state cognitive operations. The synergetic use of cyber and cognitive operations is often referred to in the literature as Cyber Influence Operations (CIO) (Refer Figure 5).

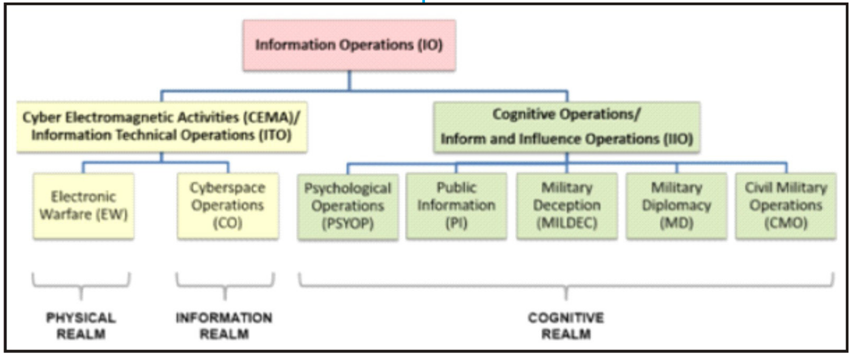

Information Operations (IO)
Cyber Electromagnetic Activities (CEMA)/ Information Technical Operations (ITO)
Cognitive Operations/ Inform and Influence Operations (IIO)
Electronic Warfare (EW)
Cyberspace Operations (CO)
Psychological Operations (PSYOP)
Public Information (PI)
Military Deception (MILDEC)
Military Diplomacy (MD)
Civil Military Operations (CMO)
PHYSICAL REALM
INFORMATION REALM
COGNITIVE REALM

**Figure 4**

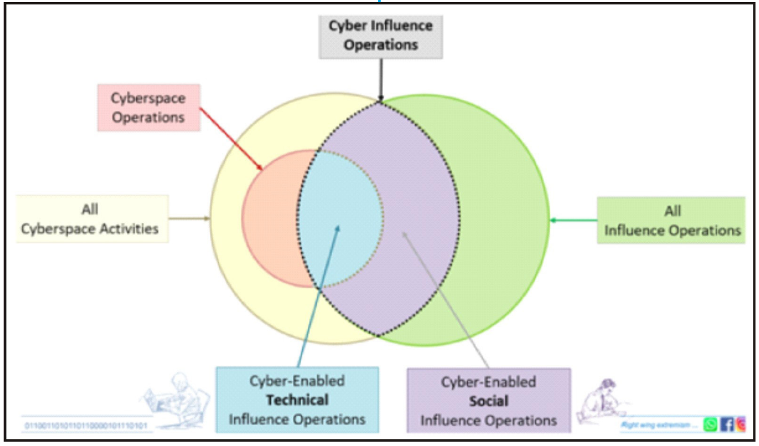

Cyber Influence Operations
Cyberspace Operations
All Cyberspace Activities
All Influence Operations
Cyber-Enabled Technical Influence Operations
Cyber-Enabled Social Influence Operations

**Figure 5**

**CIO: An Overview**. In colloquial terminology, CIO are generally referred to as disinformation campaigns or narrative wars carried out over social media. However, there is much more to CIO than this restricted understanding. CIO are a rather complex confluence of cyber and cognitive operations. It is emphasised here that not all CIO require the use of specialist cyber expertise. Some CIO merely use cyberspace as a medium, e.g., dissemination of preferred narratives through social media platforms, requiring expertise only in the art of generating narratives. Others require cyber operations expertise, e.g., a Cambridge Analytica type of operation.[16] The former CIO are referred to as Cyber-enabled Social Influence Operations while the latter are termed as Cyber-enabled Technical Influence Operations (CeTIO).[17]

**CIO: Multiple Dimensions.** One may abstract three operational dimensions while conceptualising cyber influence strategies. The first dimension relates to the level of precision with which the target audience is selected: general, social-demographic, and psychographic, in increasing order of precision. The type of effect which the influence strategy is expected to have on the target audience, i.e., positive, distractive, or negative, constitutes the second dimension. The third dimension denotes the intensity of the operation across the spectrum of conflict, i.e., peace, low-intensity conflict full-blown conflict. This dimension also governs the intrusiveness of attacks: as the level of conflict escalates, intrusiveness of CeTIO capabilities is likely to increase.[18]

> **Cyber influence tools and techniques will rarely be applied in isolation, and often a combination of multiple techniques would be used for achieving specific malicious objectives. Such coordinated uses of influence techniques are referred to as influence stratagems.**

**CIO: Techniques and Stratagems.** CIO involve a host of complex techniques and stratagems[19], mostly underpinned by social science disciplines such as psychology, philosophy, linguistics, anthropology, and sociology, which need to be mastered. The term 'Stratagem' differs from 'Strategy', in that it implies the use of deceit and trickery with the aim of outwitting an adversary. Cyber influence tools and techniques will rarely be applied in isolation, and often a combination of multiple techniques would be used for achieving specific malicious objectives. Such coordinated uses of influence techniques are referred to as influence stratagems. Some of the more significant techniques and stratagems are listed in the figure below, and a few of these are elaborated upon as under:

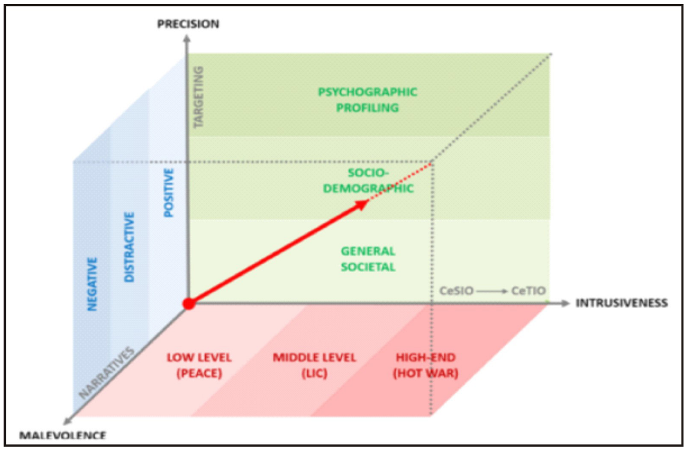


**Figure 6**

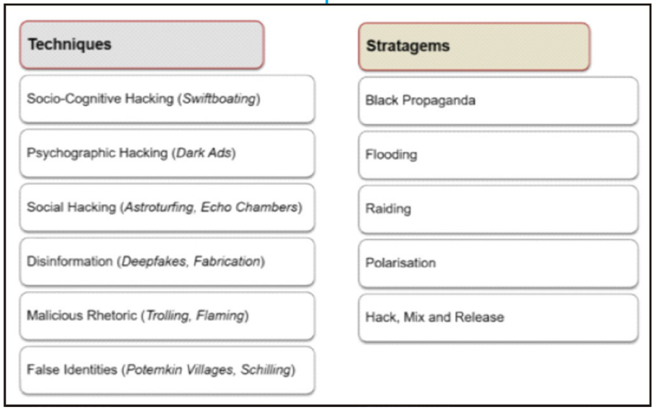
- **Socio-Cognitive Hacking.** Here the cognitive vulnerabilities of a group are exploited to influence behaviour. Swift boating, wherein, politicians are subjected to a smear campaign just before elections giving no time to offer counters, is an example of this technique. Rumour-mongering to incite hate between religious or ethnic groups is another example of socio-cognitive hacking.

- **Psychographic Hacking.** This involves targeting individuals based on their psychographic profiles. Dark Ads, i.e., ads visible only to specific individuals and designed to influence them based on, for instance, their political leanings are a good example of psychographic hacking.

- **Black Propaganda.** In 'White Propaganda', the source is known, the propaganda is pursued openly, and the information disseminated is fairly accurate; in contrast, the objective of 'Black Propaganda' is to deceive the target audience by falsifying information and obfuscating its origin; 'Grey Propaganda' lies somewhere in between these two extremes. Cyberspace provides an ideal medium for executing the stratagem of black propaganda, using techniques such as 'Disinformation and False Identities'.

- **Hack, Mix and Release.** In the 'Hack, Mix, and Release' stratagem, restricted documents are first hacked by using CeTIO techniques such as spearfishing and malware; thereafter, selected information is tainted using disinformation techniques, and then released to the public. A combination of fake news, bot-supported social media distribution, memes and trolls may be used to amplify the effect of this stratagem.

**CIO vis-à-vis Offensive Cyber Operations.** It is pertinent to point out here that CIO are quite different in flavour from offensive cyber operations, since these two types of operations are often conflated with each other. All influence operations, including CIO, require expertise primarily in social science disciplines. Some CIO may not need cyber expertise for their execution, e.g., smear campaigns carried over broadcast media or social media platforms. Others such as hack, mix and release operations would indeed require a synergetic use of cyber and influence expertise. Offensive cyber operations such as attacks on critical infrastructure, on the other hand, require sophisticated cyber expertise, which is underpinned by information and communication technologies. Organisations and expertise needed to execute CIO and offensive cyber operations are very different in character. Therefore, from considerations of specialisation, the structure of organisations tasked to conduct these operations must be given careful thought.



| Techniques | Stratagems |
|---|---|
| Socio-Cognitive Hacking (*Swiftboating*) | Black Propaganda |
| Psychographic Hacking (*Dark Ads*) | Flooding |
| Social Hacking (*Astroturfing, Echo Chambers*) | Raiding |
| Disinformation (*Deepfakes, Fabrication*) | Polarisation |
| Malicious Rhetoric (*Trolling, Flaming*) | Hack, Mix and Release |
| False Identities (*Potemkin Villages, Schilling*) | |

**Figure 7**

**Offensive cyber operations such as attacks on critical infrastructure, on the other hand, require sophisticated cyber expertise, which is underpinned by information and communication technologies.**

**Cognitive Operations in the Ongoing Russia-Ukraine Conflict.** In the ongoing Russia-Ukraine conflict disinformation campaigns, or the so-called narrative wars, are being aggressively conducted by both sides over broadcast and social media. The central theme on almost all western media platforms is designed to paint President Putin as a war criminal and characterise the conflict as a brutal, unprovoked aggression by Russia. Russia and its sympathetic media outlets, on the other hand, call the conflict a special military operation instigated primarily by NATO expansion. Allegations of war crimes are freely traded by both sides. Specific actions taken by the two sides are discussed extensively in the literature.[20,21,22,23]

## Impact of AI on Cognitive Operations

AI is a field of research that seeks to build computing technologies which possess aspects of human perception, reasoning, and decision-making. Machine Learning, a subset of AI, involves the use of computing power to execute algorithms that learn from data. Over the last decade, significant improvements in machine learning capabilities have been enabled by advances in computer processing power, the rise of Big Data, and the evolution of deep learning neural networks. While distinct from human intelligence, AI excels at narrow tasks and has exceeded human capabilities in several fields. Malign actors are increasingly exploiting machine learning systems to precisely target audiences, shape global public opinion, and sow social discord. AI-enhanced disinformation operations have the potential to significantly exacerbate political polarisation, erode citizen trust in societal institutions, and blur the lines between truth and lies.

**Technology.** AI technologies can be used in a variety of ways for the conduct of cognitive operations. A few applications of AI that have so far proved to be very impactful in this domain are as under:

- **Deepfakes.** Machine learning techniques can generate highly realistic fake images, audio, and video known as 'Deepfakes'. The use of generative adversarial networks is one technique which makes these synthetic media capabilities possible.[24] It has been used to create extraordinarily realistic artificial faces for bot accounts, and generate fake content that, when timed strategically, can destabilise governance and geopolitics.

- **AI Powered Bots.** AI-powered bots excel at creating large volumes of content, ranging from articles and social media posts to videos and memes. They leverage natural language processing and machine learning algorithms to generate content that is challenging to identify as disinformation. By mimicking human behaviour over social media platforms, AI-powered bots can rapidly spread disinformation, creating the illusion of widespread support for a particular narrative.

**AI-driven disinformation campaigns can exploit existing societal divisions, promote political polarisation, and amplify dissent within an adversary state.**

- **Microtargeting and Personalisation.** AI can analyse vast amounts of user data to identify specific demographics or individuals susceptible to manipulation. By tailoring disinformation campaigns to target these groups, AI can increase the effectiveness of spreading false information and influencing opinions.

- **Generative Artificial Intelligence and Large Language Models (LLMs).** Generative AI refers to a class of AI systems that can autonomously produce new content, such as text, images, or even videos, based on patterns and information learned from vast datasets. LLMs, a subset of generative AI, specifically focus on processing and generating human-like text, making them very valuable for producing disinformation for dissemination by bots. Examples of LLMs include OpenAI's Generative Pre-trained Transformer, Google's Bidirectional Encoder Representations from Transformers and Anthropic's Claude.[25]

## Impact

AI, in particular generative AI, poses several security risk implications at national and international levels, as under:

- **Undermining Political Stability.** AI-driven disinformation campaigns can exploit existing societal divisions, promote political polarisation, and amplify dissent within an adversary state. Such campaigns can undermine the stability of political institutions, sow distrust in government, and create conditions conducive to unrest or regime change.

- **Interference in Electoral Processes.** AI-powered bots and disinformation tactics can be employed to interfere with electoral processes in adversary states by spreading false narratives, influencing public opinion, and potentially manipulating voting behaviours.

- **Economic Destabilisation.** AI-powered disinformation campaigns can target economic stability by spreading false information about a nation's financial health, economic policies, or trade relationships, leading to market fluctuations, loss of investor confidence, and overall economic destabilisation.

- **Military Deception and Misdirection.** AI can contribute to military deception by creating realistic but fabricated scenarios. False intelligence reports, AI-generated deepfake videos, or manipulated satellite imagery can be disseminated to mislead an adversary about military intentions, deployments, or capabilities.

- **Strategic Miscalculation.** Misinformation attacks targeted at disrupting military communication between adversaries can increase the fallibility of strategic weapon systems. Generative AI, by blurring the line between real and fake content, can make it harder to signal benign intentions to adversaries, further aggravating the security dilemma.

- **Distorting Perceptions of Reality**. The convergence of disinformation campaigns and generative AI poses a formidable threat to the integrity of truth and the stability of societal perceptions. This synergy has given rise to what scholars refer to as the 'Liar's Dividend', i.e., a phenomenon where the proliferation of falsehoods erodes trust in information sources and distorts reality, which would have a severe adverse impact on governance as well as security of states.[26]

## Leveraging Neuro S/T for Cognitive Operations

It was stated at the outset that NATO's stated objective for conducting cognitive warfare is 'To change not only what people think, but how they think and act', by resorting to the use of neuro-weapons. Both of these facets are depicted in the Figure 8 below.

**Attack Surface Covers Entire Populations**. In conventional warfare, as per the principles of International Humanitarian Law (IHL), targets of physical attacks are limited to combatants. In contrast, the notion of cognitive warfare which is being practiced and evolved by nations envisages the targeting of combatants as well as civilians, with the attack surface extending to whole adversary populations. While some of the attack vectors such as inform and influence operations may be benign in nature, others such as subversive black propaganda and neuro weapons could lead to physical harm to the victims including civilians, which throws up ethical issues.

**While some of the attack vectors such as inform and influence operations may be benign in nature, others such as subversive black propaganda and neuro weapons could lead to physical harm to the victims including civilians, which throws up ethical issues.**

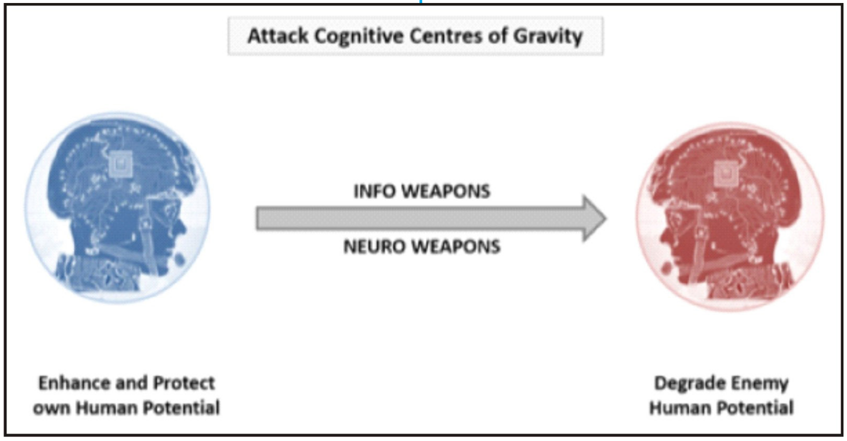

Attack Cognitive Centres of Gravity
INFO WEAPONS
NEURO WEAPONS
Enhance and Protect own Human Potential
Degrade Enemy Human Potential

**Figure 8**

**Information Weapons Exploit Brain Limitations**. Information weapons take advantage of several types of vulnerabilities of the human brain to achieve the desired effects. For instance, the human brain has limited capacity for processing information. Thus, it attempts to take shortcuts to arrive at conclusions, that leads it to believe repetitive messages, get convinced by any evidence presented even if false, and makes conclusions which align with its cultural and societal belief system. Furthermore, human emotions distort reasoning and interfere with balanced decision making. All these limitations are exploited by information weapons employed in cognitive operations.[27]

**Cognitive Warfare and the Human Domain**. NATO seems to be seriously considering adding a 'Cognitive Domain' as the sixth domain of warfare. Going even further, some military strategists have opined that a cognitive domain would be too restrictive, and that the sixth domain which deserves to be added to the battlespace construct is the 'Human Domain'. This view is based on the contention that every individual is embedded in an environment and maintains relationships within a society characterised by a set of beliefs and values. It is these relationships, beliefs and values which can be effectively attacked by conducting cognitive operations.[28]

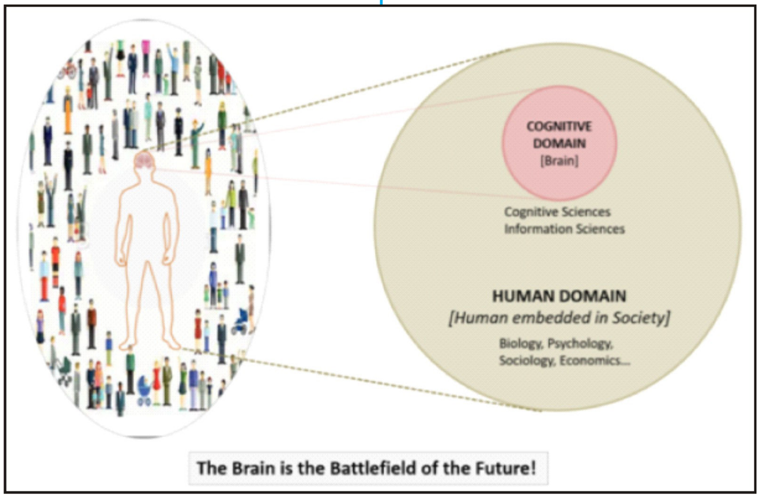


**Figure 9**

**Employment of Neuro Weapons for Cognitive Warfare.** A look will now be taken at the second main facet of cognitive operations, namely, the employment of neuro-weapons.[29] These weapons are powered by a basket of disciplines grouped together under the head of NeuroS/T, which employ Directed Energy (DE) as well as nano and bio technologies in conjunction with knowledge of cognitive sciences (Nanotechnology, Biotechnology, Information Technology, and Cognitive Science Technologies) to physically degrade the brain's cognitive abilities. Here one can draw an analogy from the way cyber weapons on one hand, and EW and DE weapons on the other, respectively target information systems. While cyber weapons target software including data on information systems, EW/DE weapons directly disrupt or destroy the hardware. Similarly, while CIO distort and manipulate information fed to the human brain, neuro-weapons target the brain itself.

**These capabilities may be used to either enhance the performance of own combatants, creating the sci-fi equivalents of super-soldiers, or they may be used to degrade the fighting potential of adversary combatants.**

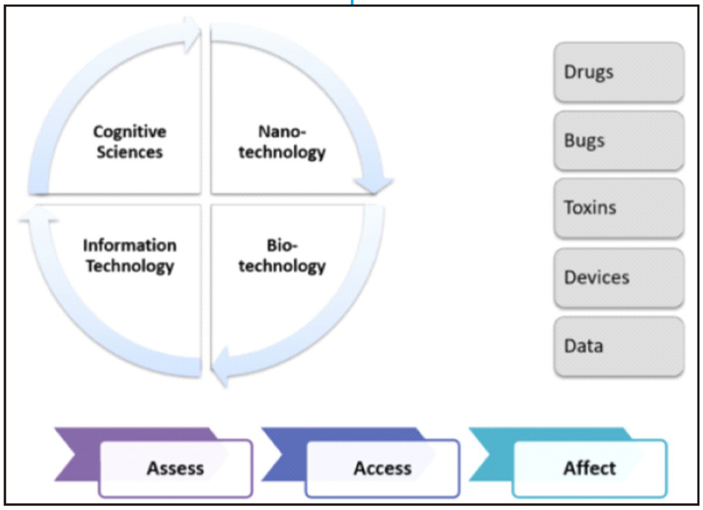


**Figure 10**

The spectrum of capabilities which are powered by NeuroS/T is catchily captured in the five terms: drugs, bugs, toxins, devices and data. These capabilities may be used to either enhance the performance of own combatants, creating the sci-fi equivalents of super-soldiers, or they may be used to degrade the fighting potential of adversary combatants. These may also be employed for targeting adversary civilians, though this would raise ethical issues.

**Performance Enhancers.** For enhancing the performance of soldiers, the term 'Drugs' here implies the employment of pharmacological agents such as stimulants to increase attention spans, enhance memory and reduce fatigue; eugeroics to induce wakefulness during extended engagements, and nootropics to boost cognitive performance. Devices translate to getting neuro feedback from the brain using electroencephalogram and brain imaging techniques, and enhancing brain performance using electric and magnetic transcranial modulation techniques.

Another facet of performance enhancement involves Brain-Computer Interfacing either through intrusive methods by inserting electrodes or merely by using electrical signals.[30]

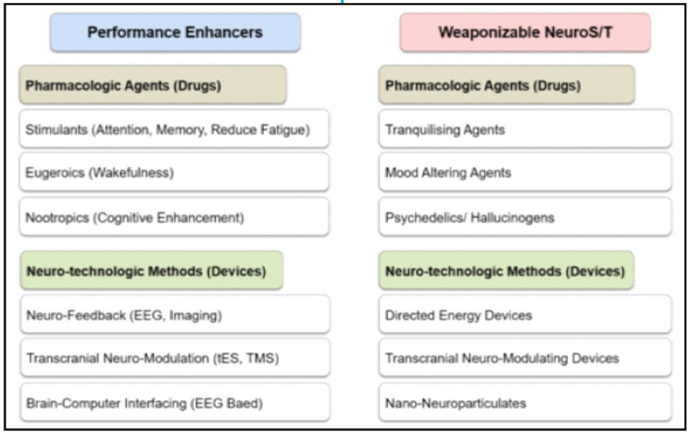

Performance Enhancers
Weaponizable NeuroS/T
Pharmacologic Agents (Drugs)
Stimulants (Attention, Memory, Reduce Fatigue)
Eugeroics (Wakefulness)
Nootropics (Cognitive Enhancement)
Neuro-technologic Methods (Devices)
Neuro-Feedback (EEG, Imaging)
Transcranial Neuro-Modulation (tES, TMS)
Brain-Computer Interfacing (EEG Baed)
Pharmacologic Agents (Drugs)
Tranquilising Agents
Mood Altering Agents
Psychedelics/ Hallucinogens
Neuro-technologic Methods (Devices)
Directed Energy Devices
Transcranial Neuro-Modulating Devices
Nano-Neuroparticulates

**Figure 11**

**Weaponising NeuroS/T.** For degrading adversary combat capabilities, drugs such as tranquilizers, mood altering agents and hallucinogens may be used to great effect. On the devices front, DE weapons are believed to have been already operationalised, for example, in the widely reported Havana Syndrome case, wherein, US and Canadian diplomats posted in Cuba are suspected to have been targeted using microwave or ultrasound DE weapons. Transcranial modulation devices or even nano-neuroparticulates may be used to target specific sets of neurons. Bugs and toxins refer to biological warfare using toxic substances such as sarin gas and other nerve agents. Data refers, for instance, to the psychographic profiling of individuals to subsequently target them using either information or neuro-weapons to attack individual vulnerabilities.

**It is important to consider legal and ethical issues associated with this cognitive warfare, most of which have their genesis in the fact that not just combatants but civilians, from individuals to groups to whole societies, may be in the firing line of such operations.**

## Cognitive Warfare: Legal and Ethical Issues

It is important to consider legal and ethical issues associated with this cognitive warfare, most of which have their genesis in the fact that not just combatants but civilians, from individuals to groups to whole societies, may be in the firing line of such operations. Some of these issues are discussed below.

**Freedom of Press.** As stated in an earlier section, PI aims to inform foreign as well as domestic audiences with factually correct information presented with a balanced perspective. The question which comes up is, in the interests of national security, should a certain degree of control be exerted by the state over broadcast media? In the Ukraine conflict, even the so-called liberal West has exhibited no qualms in exerting a great degree of control over the media and in banning Russian media outlets such at Russia Today and Sputnik.

**Psyops against Domestic Audiences.** The Indian Joint Doctrine on Perception Management and Psyops of Mar 2010 makes a surprising statement, as follows: “Psyops are conducted against friendly forces and civil population as well as adversary’s forces and hostile populations”. In this paper, Psyop is taken to mean operations which convey selected information - not necessarily truthful - to foreign audiences in order to influence their behaviour. The ethical question which needs to be addressed is: Should half-truths and lies ever be systematically fed to domestic audiences even in the interest of national security? Classified information of course cannot be made public. However, there is only a thin line between classified information and deliberately concealed unpalatable facts.

**Cognitive Warfare against Adversary Populations.** While disseminating disinformation amongst an adversary population in support of military operations should be acceptable, ethical lines are blurred when a state exploits societal fault-lines to create dissension and unrest, perhaps leading to violent protests and deaths. The use of disinformation by states is looked down upon with disdain by the so-called liberal democracies. Yet some states, including India's adversaries, unhesitatingly resort to such means. The following question, therefore, comes up: Should disinformation be countered with truthful narratives alone, or would that be a losing defensive strategy, and a more offensive stance needs to be adopted?

**Employment of Neuro-Weapons.** Employment of NeuroS/T for performance enhancement to create super-soldiers, as well as to target adversary soldiers and civilians, throw up further ethical conundrums. While temporary enhancement, e.g., by using stimulants, may be acceptable, biological enhancement of a permanent nature, such as by employing Clustered Regularly Interspaced Short Palindromic Repeats technology to genetically modify humans, will likely be looked at from an ethical perspective as having crossed a red line. While international conventions already exist which ban the employment of chemical and biological weapons, the same is not true yet for neuro-weapons which use DE and transcranial-modulation.

**Chinese influence operations are conducted using non-cyber platforms such as broadcast media and Confucius Institutes, as also Cyber Influence Operation which play a major role in the overall strategy.**

**International Law.** IHL as it exists today strives to protect civilians during armed conflicts. However, IHL principles have been formulated against the backdrop of kinetic warfare. In contrast, in the context of cyberattacks debates have been ongoing globally for almost two decades now to figure out how international law applies in cyberspace, without much progress. Taking a cue from this, arriving at an international consensus on legal and ethical issues associated with cognitive warfare, which is much more nebulous in character, would likely present itself as an almost intractable problem.

## Cognitive Warfare Capabilities of Major Powers

This section gives an overview of the cognitive warfare capabilities of some states from which India might draw some lessons.

**Russia.** Russia, arguably, may be credited with the best demonstrated prowess in cyber and cognitive warfare, which it terms together as IW. Notable demonstrations of this expertise are its cognitive operations in Estonia, Georgia, Ukraine, as well as interference in presidential elections in the US, France, and Germany.[31] Russia's strategic thought on cognitive warfare is captured in its concepts of 'Active Measures' (Influence operations), Maskirovka (Deception), reflexive control and the frequently quoted Gerasimov Doctrine.[32,33,34] The Glavnoye Razvedyvatelnoye Upravlenie, notably, its Unit 54777, Federal Security Service, Foreign Intelligence Service and non-state actors such as the Internet Research Agency are all involved in Russian IO[35].

**China.** Influence operations in China are coordinated and executed by the United Front Work Department, the Propaganda Department, the Ministry of State Security, and the People's Liberation Army Strategic Support Force[36]. China's 'Three Warfares Strategy', comprising psychological, media and legal warfares, is well known.[37] Chinese influence operations are conducted using non-cyber platforms such as broadcast media and Confucius Institutes, as also CIO which play a major role in the overall strategy. The media houses in China being almost entirely state-owned or controlled, online platforms of media organisations such as Xinhua, China Global Television Network and the People's Daily are focused towards influencing foreign audiences over western social media platforms.[38] China initiated its Brain Project in 2016[39], one of the three primary global research projects in NeuroS/T, together with US Defence Advanced Research Projects Agency's (DARPA) research the European Union's Brain Science Project.

**United States.** The US was the first to develop the concept of military IO with PSYOP as a core function, and several other inform and influence functions such as public affairs, military diplomacy, and civil-military operations.[40,41,42] It has significant psyops forces in the form of psyops groups and battalions.[43] In the field of NeuroS/T, DARPA is at the forefront of research on brain sciences and is a main lead in the NATO projects on cognitive warfare.

**Pakistan.** The Pakistani Armed Forces apparently have no doctrine or military units specifically tasked for psyops. However, unlike India, it does have an effective tri-services Directorate of Inter-Service Public Relations (ISPR) with objectives in the cognitive domain specified across the spectrum of conflict. Another obscure think tank, namely, Command Eleven, plays a significant role in furthering the psyops' objectives of its Armed Forces.[44] The strength of the ISPR establishment is estimated to be 4,000 personnel, with a budget of several thousand crore.

## Way Forward for India

India has several fault-lines, along religious, ethnic, cultural and caste boundaries; and its primary adversaries, namely China and Pakistan, both possess formidable cognitive warfare capabilities for exploiting these fault-lines. It is imperative, therefore, for India and its Armed Forces to develop requisite strategy, doctrine, organisations, and expertise to deter its adversaries and deliver strategic effects in the cognitive realm.

**Ethical issues highlighted above need to be addressed while formulating India's overall strategy. As a nation India need to take a call on whether it would like to conduct ethically questionable cognitive operations against adversary civilians.**

**Strategy and Ethics.** Ethical issues highlighted above need to be addressed while formulating India's overall strategy. As a nation India need to take a call on whether it would like to conduct ethically questionable cognitive operations against adversary civilians. In extreme cases, these could involve subversion of dissatisfied populace in the adversary state aimed at instigating them to secede. While taking such a call, India must keep in mind that its adversaries evidently have shown no compunction in resorting to such black operations against India.

**Apex Organisation.** India's cognitive operations strategy must necessarily adopt a whole-of-government approach. Ministries and agencies which have roles to play in the conduct of cognitive operations beyond India's borders are the Ministry of Defence/Armed Forces, external facing agencies, i.e., Ministry of External Affairs/Research and Analysis Wing, and the Ministry of Information and Broadcasting. The Ministry of Home Affairs must focus on developing an effective defensive strategy to counter the cognitive onslaught by its adversaries. Finally, the Defence Research and Development Organisation and other research institutions must be leveraged for the development of neuro-weapons. Being a multi-agency effort, India needs to evolve a potent apex level organisation for coordinating all cognitive warfare lines of effort. A notional architecture for such an organisation is depicted in Figure 12.

**Role of the Armed Forces.** A distinction has been made in an earlier section between cognitive operations conducted in support of military operations and those which are targeted directly against adversary populations independently. The former should fall squarely within the charter of the Armed Forces.

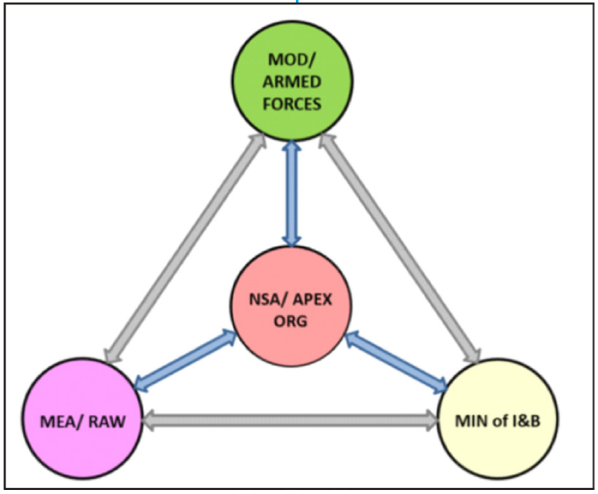


**Figure 12**

The current capabilities in this area are on a rather weak footing. Within the Army, the erstwhile Additional Directorate General PI, now renamed as Additional Director General (Stratcom) exists at the Integrated Headquarters of Ministry of Defence (Army) level, supported by IW appointments at various formation headquarters, all tenanted on a single tenure basis. In terms of capability development, IW courses conducted at the Army War College provide some exposure to IO disciplines, including cyber and EW. Organisational set-ups and training in the Air Force and Navy are understandably on a lower scale. Units specifically dedicated to the conduct of cognitive operations do not exist as yet. Thus, the present resource within the Armed Forces devoted to cognitive operations is arguably too limited to counter the likes of the People's Liberation Army Strategic Support Force and other Chinese capabilities, as well as Pakistan's ISPR. Therefore, the following recommendations are made:

- Structured training of armed forces personnel in cognitive operations disciplines needs to be considerably enhanced, including conduct of courses at graduate, post graduate and doctoral levels. Towards this end, a tri-Service centre of excellence should be set up. For officers, cognitive operations profiles must be created based on multiple tenures, while for other ranks, creation of separate trades is warranted.

- A tri-service Defence Cognitive Operations Agency must be set up on a pilot basis to cultivate expertise in various cognitive warfare disciplines and carry out operations. After the pilot phase, cognitive operations units and groups must be raised as needed.

- The armed forces need to take a lead in steering research in NeuroS/T, including the establishment of a brain project.

- Since cognitive warfare is conducted against adversary states with political objectives similar to those which justify the employment of kinetic military force, perhaps the Armed Forces need to play a key role in the conduct of cognitive operations, not only in support of military operations but also for carrying out operations in the grey zone below the threshold of armed conflict.

## Conclusion

In conclusion it may be stated that nation states are very likely to increasingly adopt non-kinetic means of warfare in the grey zone to achieve their political objectives rather than resort to all-out military conflicts. This is especially true for both Pakistan and China, the former because it is weak militarily, and the latter because it strives to be a global power and would not want to get bogged down in a war of attrition with India.

Amongst the various non-kinetic options, cognitive operations in all its forms, suitably enabled by cyber operations, have the maximum potential for achieving strategic effects below the threshold of all-out conflict. It is a matter of concern that, unlike its adversaries, India as a nation in general and the armed forces in particular have perhaps not paid enough attention to developing capabilities in the cyber and cognitive domains. Evolving doctrinal thought, upgrading the Defence Cyber Agency to a Cyber Command, setting up a Defence Cognitive Operations Agency, and making transformative changes in the human resource policies to develop the right level of specialisation in these warfighting domains, are some of the measures which need to be implemented on top priority.

**Nation states are very likely to increasingly adopt non-kinetic means of warfare in the grey zone to achieve their political objectives rather than resort to all-out military conflicts.**

## Endnotes

[1] US DoD Joint Publication 3-13, Information Operations, Nov 2014, Accessed 04 Jan 2024, https://irp.fas.org/doddir/dod/jp3_13.pdf

[2] Posard, M. N. et al, From Consensus to Conflict, RAND Corporation Research Report, 2020, pp. 2-3, Accessed 04 Jan 2024, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA700/RRA704-1/RAND_RRA704-1.pdf

[3] John Costello and Joe McReynolds, China's Strategic Support Force: A Force for a New Era, Washington, National Defence University Press, China Strategic Perspectives, No 13, Oct 2018, pp. 28-29, Accessed 04 Jan 2024, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf

[4] HQ Army Training Command, Information Warfare Doctrine for Indian Army, 2010 (classified)

[5] HQ Integrated Defence Staff, Perception Management and Psychological Operations, 2010 (unclassified; presently not available online)

[6] Alonso et al, Cognitive Warfare, NATO Innovation Hub and John Hopkins University, 2020, Accessed 05 Jan 2024, https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf

[7] NATO, Countering cognitive warfare: awareness and resilience, NATO Review, 20 May 2021, Accessed 04 Jan 2024, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

[8] NATO, Cognitive Biotechnology: opportunities and considerations for the NATO Alliance, NATO Review, 26 Feb 2021, Accessed 04 Jan 2024, https://www.nato.int/docu/review/articles/2021/02/26/cognitive-biotechnology-opportunities-and-considerations-for-the-nato-alliance/index.html

[9] Giordano, James, Neurotechnology in National Security and Defence, pub. CRC Press, Taylor & Francis Group, 2015, Accessed 04 Jan 2024, https://www.amazon.in/Neurotechnology-National-Security-Defense-Considerations/dp/1482228335 (Paid version)

[10] US Joint Chiefs of Staff, Strategy, US Joint Doctrine Note 1-18, 25 Apr 2018, Accessed 04 Jan 2024, https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_18.pdf

[11] Hoffman, Frank. Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, Virginia: Potomac Institute for Policy Studies, Arlington, Virginia, US, 2007, Accessed 05 Jan 2024, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

[12] Liang, Qiao & Xiangsui, Wang, Unrestricted Warfare, Beijing: PLA Literature and Arts Publishing House, Feb 1999, Accessed 05 Jan 2024, https://archive.org/details/unrestricted-warfare-by-qiao-liang-and-wang-xiangsui

[13] Derleth, James, Russian New Generation Warfare: Deterring and Winning the Tactical Fight, US Army Military Review, Sep-Oct 2020, Accessed 05 Jan 2024, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-20/Derleth-New-Generation-War-1.pdf

[14] Panwar, R. S., Grey Zone Operations in the Infospace Dimension: Imperatives for India, Future Wars, 19 Oct 2021, Accessed 04 Jan 2024, https://futurewars.rspanwar.net/grey-zone-operations-in-the-infospace-dimension-imperatives-for-india/

[15] Ibid

[16] Confessore, Nicholas, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, The New York Times, 04 Apr 2018, Accessed 04 Jan 2024, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[17] Panwar, R. S., Cyber Influence Operations - A Battle of Wits and Bits: The Cauldron of Concepts and Terminologies, 13 Oct 2020, Accessed 04 Jan 2024, https://futurewars.rspanwar.net/cyber-influence-operations-a-battle-of-wits-and-bits-the-cauldron-of-concepts-and-terminologies/

[18] Panwar, R. S., Cyber Influence Operations - A Battle of Wits and Bits: Targets, Techniques and Stratagems, 27 Oct 2020, Accessed 04 Jan 2024, https://futurewars.rspanwar.net/cyber-influence-operations-a-battle-of-wits-and-bits-targets-techniques-and-stratagems/

[19] Ibid

[20] Panwar, R. S., Ukraine Conflict: Fascinating Operations in Cyberspace, Future Wars, 05 Apr 2022, Accessed 04 Jan 2024, https://futurewars.rspanwar.net/unkraine-conflict-fascinating-operations-in-cyberspace/

[21] Osadchuk, Roman & Carvin, Andy, Undermining Ukraine, Atlantic Council, Feb 2023, Accessed 02 Mar 2024, https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Undermining-Ukraine-Final.pdf

[22] Algarni, Ahmed D., Information Operations in the Russia-Ukraine War, International Institute of Iranian Studies, 24 Jan 2023, Accessed 02 Mar 2024, https://rasanah-iiis.org/english/wp-content/uploads/sites/2/2023/01/Information-Operations-in-the-Russia-Ukraine-War.pdf

[23] Demus, Alyssa et al, The Nightingale versus the Bear, RAND Corporation, 12 Oct 2023, Accessed 02 Mar 2024, https://www.rand.org/pubs/research_reports/RRA2032-1.html

[24] Anderson, Martin, The Future of Generative Adversarial Networks in Deepfakes, Metaphysic, 25 Jul 2022, Accessed 02 Mar 2024, https://blog.metaphysic.ai/the-future-of-generative-adversarial-networks-in-deepfakes/

[25] Toner, Helen, What Are Generative AI, Large Language Models, and Foundation Models? Centre for Security and Emerging Technology, 12 May 2023, Accessed 04 Jan 2024, https://cset.georgetown.edu/article/what-are-generative-ai-large-language-models-and-foundation-models/

[26] Schiff, Kaylyn Jackson et al, The Liar's Dividend: The Impact of Deepfakes and Fake News on Trust in Political Discourse, SocArXiv x43ph, Centre for Open Science, DOI: 10.31219/osf.io/x43ph, 19 Feb 2021, Accessed 04 Jan 2024, https://ideas.repec.org/p/osf/socarx/x43ph.html

[27] Oie, Kevi S. & McDowell, Kaleb, Neurocognitive Engineering for Systems' Development in Neurotechnology in National Security and Defence, Ed. Giordano, James, CRC Press Taylor and Francis Group, 2015, pp. 36-38, Accessed 04 Jan 2024, https://www.routledge.com/Neurotechnology-in-National-Security-and-Defense-Practical-Considerations/Giordano/p/book/9781482228335

[28] Claverie, Bernard & Cluzel, François, The Cognitive Warfare Concept, NATO Innovation Hub, 2021, pp. 7-8, Accessed 04 Jan 2024, https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf

[29] Giordano, James et al Redefining Neuroweapons Emerging Capabilities in Neuroscience and Neurotechnology, PRISM 8, No 3, NDU Press, Jan 2020, Accessed 05 Jan 2024, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2053388/redefining-neuroweapons-emerging-capabilities-in-neuroscience-and-neurotechnolo/

[30] Ibid

[31] Brattberg, Eric & Tim Maurer, Tim, Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks, Carnegie Endowment for International Peace, 23 May 2018, Accessed 05 Jan 2024, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

[32] Aurelian Stoica, Aurelian, From Social Influence to Cyber Influence: The Role of New Technologies in the Influence Operations Conducted in the Digital Environment, International Journal of Cyber Diplomacy / 2020, Volume 1, Issue 1, pp. 29, Accessed 06 Jan 2024, https://ijcd.ici.ro/documents/24/2020_article_4.pdf

[33] Bartles, Charles K. Getting Gerasimov Right, Military Review, Jan-Feb 2016, Accessed 05 Jan 2024, https://community.apan.org/cfs-file/__key/docpreview-s/00-00-00-11-18/20151229-Bartles-_2D00_-Getting-Gerasimov-Right.pdf

[34] Thomas, Timothy L., Russia's Reflexive Control Theory: Manipulating an Opponent to One's Advantage, The MITRE Corporation, Jun 2019, Accessed 06 Jan 2024, https://apps.dtic.mil/sti/pdfs/AD1157096.pdf

[35] Bowen, Andrew S. Russian Cyber Units, Congressional Research Service, 02 Feb 2022, Accessed 05 Jan 2024, https://crsreports.congress.gov/product/pdf/IF/IF11718

[36] Panwar, R. S., China's Strategic Support Force and its Implications for India - Part II: Organisational Structures for Information Operations, Future Wars, 16 Jun 2020, Accessed 06 Jan 2024, https://futurewars.rspanwar.net/chinas-special-support-force-and-its-implications-for-india-part-ii/

[37] Cheng, Dean, Winning Without Fighting: The Chinese Psychological Warfare Challenge, The Heritage Foundation, 11 Jul 2013, Accessed 06 Jan 2024, https://thf_media.s3.amazonaws.com/2013/pdf/bg2821.pdf

[38] Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion, Insikt Group, 06 Mar 2019, Accessed 06 Jan 2024, https://www.recordedfuture.com/china-social-media-operations/

[39] Elsa B. Kania, Minds at War: China's Pursuit of Military Advantage through Cognitive Science and Biotechnology, NDU Press, Prism 8, No. 3, Jan 2020, Accessed 06 Jan 2024, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf

[40] US DoD Joint Publication 3-13.12, Military Information Support Operations, 07 Jan 2010, Accessed 05 Jan 2024, https://info.publicintelligence.net/JCS-MISO.pdf

41 US DoD Joint Publication 3-61, Public Affairs, 17 Nov 2015/ 19 Aug 2016, Accessed 05 Jan 2024, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_61.pdf

42 US DoD Joint Publication 3-57, Civil Military Operations, 09 Jul 2018, Accessed 05 Jan 2024, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_57.pdf

43 Psychological Operations (United States), Wikipedia, Accessed 05 Jan 2024, https://en.wikipedia.org/wiki/Psychological_operations_(United_States)

44 Panwar, R. S., IW Structures for the Indian Armed Forces - Part III: Organisation Structures in Other Defense Forces, Future Wars, 14 Apr 2020, Accessed 05 Jan 2024, https://futurewars.rspanwar.net/iw-structures-for-the-indian-armed-forces-part-iii/

### About the Author

**Lieutenant General (Dr) RS Panwar, AVSM, SM, VSM (Retd)** holds a doctorate in Computer Science from Indian Institutes of Technology Bombay, and is a Distinguished Alumnus of this premier Institution. A graduate of the National Defence College, he has tenanted important assignments including GOC 101 Area, Commandant Military College of Telecommunication Engineering, Cdr 81 Sub Area and Cdr Electronic Warfare Brigade. His current work focuses on technology driven future warfare as relevant to the Indian Armed Forces. He is also an active participant in Track 2 diplomacy initiatives at the international level in responsible use of military Artificial Intelligence.

## About the USI

The United Service Institution of India was founded in 1870 by a soldier scholar, Colonel (later Major General) Sir Charles MacGregor 'For the furtherance of interest and knowledge in the Art, Science and Literature of National Security in general and Defence Services, in particular'. It commenced publishing its Journal in 1871. USI also publishes reports of its members and research scholars as books, monographs, and occasional papers (pertaining to security matters). The present Director General is Major General BK Sharma, AVSM, SM** (Retd).

Price: ₹ 350.00

United Service Institution of India (USI)

Rao Tula Ram Marg, Opposite Signals Enclave, New Delhi-110057
Tele: 2086 2316/ Fax: 2086 2315, E-mail: dde@usiofindia.org