Cognitive Centric Warfare: Modelling Indirect Approach in Future Warfare

K Takagi

Colonel, Japan Ground Self-Defense Force, Tokyo, Japan
Graduate School of Media and Governance, Keio University, Tokyo, Japan
Fellow, Hudson Institute, Washington, D.C., United States of America

E-mail: ktakagi@hudson.org

Abstract: *With the development of science and technology, warfare has become a multi-domain operation that includes land, sea, air, space, cyber, electromagnetic waves, and human cognition. Nonetheless, existing research has not examined the relationship between each of these domains and the cognitive domain. Hence, this paper explores how cognitive influence on adversaries can be exerted from multiple domains. This paper analyses the case of the war in Ukraine in which the latest science and technology were used. This article finds that attacks on human cognition are exerted from all domains and provides a comprehensive model of cognitive influence on the adversary.*

Keywords: *Cognitive Warfare, Information Warfare, War in Ukraine, Latest Science and Technology, Multi-Domain Operations, Cognitive Domain*

Introduction

Since ancient times, war has been a battle of wills between the two parties involved, and humans have fought in the domain of cognition. In the 6th century B.C., Sun Tzu insisted on the importance of surrendering the enemy without resorting to force. In the 5th century B.C., Thucydides argued that three elements of war were fear, honor, and interest. In the early 19th century, Clausewitz (1989) stated that war is an act to force one's will on the enemy. Thus, the cognitive aspects of human beings in war are central to war theories.

An enemy's recognition that he or she has lost the war is an important requirement for the end of the war. Very rarely in the history of warfare has there been a case, such as Carthage's defeat to Rome, where a city is removed without a trace, the entire population is enslaved, and the state physically annihilated. In many cases, the will of the involved parties has determined the continuation and end of a war.

Sun Tzu and Basil Liddell-Hart argued for the importance of an indirect approach strategy that avoids physical warfare and affects the enemy's will. However, Sun Tzu and Liddell-Hart did not offer specific suggestions on how to do so. Furthermore, the rapid development of science and technology in recent years—particularly information and communication technology, social media, and artificial intelligence—has rapidly changed indirect approach methods.

ISSN 1445-3312 Print/ISSN 1445-3347 Online

With the development of science and technology, warfare has become a multi-domain operation that includes the traditional physical domains of land, sea, and air, as well as the relatively new technological domains of space, cyber, and electromagnetic waves, and even human cognition. Operations in each domain are conducted across the board, as aircraft attack targets on the ground and at sea, and cyber means target weapons on land, sea, air, and space. In the same way, attacks are carried out from all domains, targeting the domain of human cognition. Nevertheless, existing research on information operations and the cognitive domain has not explored the relationship between the domains of land, sea, air, space, cyber, and electromagnetic waves and the domain of human cognition.

Given this situation, the research question of this article is how cognitive influence on an adversary is exerted from multiple domains: land, sea, air, space, cyber, electromagnetic, and cognitive domains.

To this end, this article analyzes the case of the Ukrainian War, a large-scale war between nations in which the latest science and technology are used, and extracts examples that influence the adversary's cognition from the land, sea, air, space, cyber, electromagnetic, and cognitive domains. To plan operations in warfare, it is necessary to integrate and synchronize all domains. Hence, this paper systematizes the extracted cases to provide a comprehensive model of the methods of cognitive influence on the adversary.

In doing so, this paper modifies the Five Ring Model proposed by John Warden, taking into account the recent development of information and communication technology, in addition to the fact that human cognition is central to war. The Three Ring Model proposed by this paper consists of three domains: the cognitive domain (consisting of political leaders, military decision makers, and the population); the informational domain (consisting of the information and communication infrastructure); and the physical domain (consisting of the military forces).

This article first discusses the literature review on related concepts and then analyses the cases of the war in Ukraine. Then, this article systematizes the cases and presents the model.

Literature Review

Concepts influencing adversary cognitions and their history

Methods of exerting psychological influence on the leaders, armies, and populations of adversaries to achieve strategic effects without the use of physical means have evolved with the development of technology. These techniques became particularly active in the 1920s, when radio was developed (Rid 2020). Subsequently, this concept has been expressed in various forms, including political warfare, information warfare, influence operations, and cognitive warfare.

The oldest of these is political warfare, used by the U.S. Central Intelligence Agency (CIA) during the Cold War. Political warfare is a concept that encompasses information warfare, which involves the dissemination of a mixture of true and false information, and includes regime overthrow activities (Paterson & Hanley 2020).

In those days, paper media were often used to disseminate information to the opposing side. For example, in the 1950s, the CIA flew balloons into East Germany and distributed booklets containing accusations of repressive regimes in the East (Rid 2020). Another famous piece of disinformation spread by the Soviet Union during the Cold War was that HIV (human immunodeficiency virus) was a man-made virus created by the U.S. military (Rid 2020). In 1983, a Soviet-funded Indian newspaper published this disinformation, which was then repeated in newspapers around the world throughout the 1980s. The paper method has been used well into the 21st century. On 21 March 2003, the Coalition of the Willing distributed two million leaflets during the war in Iraq (McCardle 2022).

In this context, information and communication technologies, such as the Internet, have been actively used since the 1990s. Information warfare is a term that came into wide use in the 1990s, when information and communication technologies were developed. It is a concept that encompasses both the technological aspect, which targets computers, communication networks, and other information and communication devices, and the human cognitive aspect. The former is a concept similar to cyber warfare, while the latter refers to the manipulation of human cognition through disinformation and other means. However, when the term ‘information warfare’ is used, the definition is not constant, sometimes focusing on the technological aspect, and sometimes with only the human cognitive aspect in mind (Blannin 2022; Golovchenko, Hartmann & Adler-Nissen 2018).

The latter concept, which focuses on human cognition, is cognitive warfare (Hutchinson 2022; Takagi 2022a, 2022b). Cognitive warfare is an interdisciplinary approach that combines social science and new technologies and has attracted increasing attention worldwide in recent years (Pappalardo 2022). In particular, China has frequently used the term ‘cognitive’ in recent years, including ‘cognitive domain operations’ (Beauchamp-Mustafaga 2019).

China’s cognitive warfare, with a view to the latest neuroscience and direct machine-brain connections in the future, consists of cognitive inhibition, cognitive formation, and cognitive control (Dong 2020). ‘Cognitive inhibition’ refers to concealing one’s own behavior and weakening or depriving the enemy of situational awareness. ‘Cognitive shaping’ refers to providing the enemy with disinformation to induce him or her to make decisions and act in accordance with his or her own expectations. ‘Cognitive control’ refers to modifying the enemy’s decision-making mechanisms or directly tampering with the outcome of the enemy’s decisions. However, Chinese researchers have not stated specifically how this is to be done, and the feasibility of this with current technology is not certain.

Another term used is ‘influence operations’, which refers to efforts to cognitively influence foreign targets in peacetime and wartime to change their attitudes, behaviours, and decision-making (Saressalo & Huhtinen 2022). This includes using social media to interfere in other countries’ elections. Influence operations are also a concept that focuses on the cognitive aspects of human behaviours, similar to cognitive warfare in China.

Methods of influencing adversaries’ cognitions and their history

As described above, political warfare, information warfare, cognitive warfare, and influence operations have various definitions and have developed with the advancement of technology, but they all have in common that information is used as a weapon and strategic effects are achieved through non-physical means. In physical combat, bullets destroy and kill adversaries, while in non-physical combat, information is the bullet. Here, the bullet is a mixture of true and false information transmitted for strategic purposes, and such information can be expressed in various forms, such as propaganda, disinformation, and narratives.

Propaganda also has a variety of definitions, and although no universal definition has been obtained, there is agreement among many researchers that it achieves its objectives by interweaving true and false information (Milton 2022). For example, Wilbur (2022) argued that propaganda is defined as a concept inseparable from ideology and a deliberate and systematic attempt to shape and manipulate human cognition and induce adversaries to behave in some way. Wilber (2022) insisted that disinformation is always propaganda.

Disinformation is malicious and false information. However, information disseminated in information warfare, for example, does not necessarily have to be false information, but a mixture of true and false information is considered effective. The DIIM matrix is useful and allows information to be classified according to its correctness and maliciousness (Newman 2022).

Numerous studies exist on propaganda and disinformation. Some of them cover recent events, such as Russian and Chinese intervention in the U.S. presidential and midterm elections since 2016 (Kliman *et al.* 2020), and those on disinformation spread during the Russian invasion of Ukraine since 2014 (Lupion 2018; Roman, Wanta & Buniak 2017; Khaldarova 2021). These studies showed that the Internet and social media played an important role in the spread of disinformation in the 2010s.

Strategic narratives are the means by which political actors construct meaning about the past, present, and future of international politics and shape the behaviour of domestic and foreign actors (Miskimmon, Roselle & O'Loughlin 2013). Strategic narratives do not emerge spontaneously but are created by political actors with specific intentions and are intended to influence others. There is also a temporal element to them, which invokes the past to understand the present and predict the future. Furthermore, it is a statement about who the actors are and what order they want.

Methods of Indirect Approaches Based on the Latest Science and Technology

As mentioned, there are a variety of concepts and methods that influence the cognition of adversaries. Previous studies mentioned above have shown that the development of those concepts is closely related to the development of information and communication technologies. However, the concepts in these previous studies do not mention activities using all domains, including land, sea, air, space, cyber, and electromagnetic waves.

In order to explore methods using the latest science and technology, this section analyses recent cases in the war in Ukraine to extract methods that use all domains to influence the cognition of the adversary, allies, and international communities.

Activities in the Cognitive Domain

Narratives play a central role in influencing the cognition of adversaries. Effective narratives are those that resonate with the audience. For example, Ukraine has continually asserted the narrative of a vibrant, democratic Ukraine in the face of an authoritarian Russian invasion (Kuleba 2022).

The examples made by Ukraine, the United States, and NATO countries in the war in Ukraine demonstrate the importance of information transparency, accusations of illegal activities committed by adversaries, countering disinformation, and showing off the war record and courage of friendly forces to create and spread an effective narrative.

Transparency of information

Democracies can gain advantages by weaponizing transparency on a large scale (Berntsen & Fedasiuk 2022). The Biden administration's strategic release of classified information before Russia's invasion of Ukraine is an effective example of promoting transparency (Abdalla *et al.* 2022).

On February 18, 2022, at a press conference just before Russia launched its invasion of Ukraine, President Joe Biden stated that he was "convinced" that Russian President Vladimir Putin had "made the decision" to invade Ukraine (White House 2022). On February 23, the day before the Russian invasion, U.S. Secretary of State Antony Blinken clearly stated that he expected Russia to invade Ukraine the next day (Walton 2022). This approach was expected to deter war (London 2022), gain support in the international community (Duss 2022), and refute Russian claims of a special military operation, not war (Kolesnikov 2022).

Interagency cooperation is essential to weaponize information transparency (Berntsen & Fedasiuk 2022). It also requires prompt declassification and timely release of information (Abdalla *et al.* 2022). Accurate release of information is necessary, as it is counterproductive if released information is false (Kuldkepp 2022; Abdalla *et al.* 2022).

Furthermore, the protection of information sources is always a top priority (Abdalla *et al.* 2022). Concerning the release of classified information by the U.S., the source of the information seemed to be not HUMINT but rather intercepted communications (Walton 2022). This means electronic sources may have facilitated the rapid release of information.

Accusations of illegal activities committed by the adversaries

It is effective to accuse the adversaries of illegal activities and to reveal the involvement of the adversary's leadership in the illegal acts. By doing so, the adversary loses the support of the international community and friendly countries gain the support of the international community. In today's world of disinformation, it is important to painstakingly collect evidence of responsibility for war crimes (Coleman 2022).

When Ukrainian forces retook the Ukrainian city of Bucha at the end of March 2022, they found numerous civilian bodies and mass graves. Russia claimed that this was a Ukrainian fabrication. In response, Western media used commercial satellite images to prove that the bodies and mass graves lying in the streets of Bucha had existed since the Russian military occupation (Lin-Greenberg & Milonopoulos 2022).

The Ukrainian government also created a mechanism for Ukrainian citizens to provide information to the government through an official government app (Abdalla *et al.* 2022) Many Ukrainian citizens used the app to provide the government with evidence of Russian military movements and illegal activities. The U.S. military and U.S. intelligence agencies also continuously provided Ukraine with information on Russian military actions, operational plans, and evidence of Russian military misconduct (Abdalla *et al.* 2022). Ukraine made this information public on government websites and published evidence of Russian military atrocities to the international community.

Countering disinformation from adversaries

As disinformation abounds in times of war, it is necessary to provide appropriate counterarguments and to win the support of the international community. During the war in Ukraine, Russia released false economic statistics to cast doubt on the effectiveness of its economic sanctions (Demarais 2023). Russia also made claims that food and energy insecurity in emerging economies was caused by Western economic sanctions, not Russia's blockade of the Black Sea (Demarais 2023). In 2022, this disinformation was spread and gained support, especially in African countries (Julian-Varnon 2022).

In recent years, the development of artificial intelligence has made it possible to create elaborate images and videos known as deep fakes. On March 2, 2022, shortly after Russia invaded Ukraine, a video emerged of Ukrainian President Volodymyr Zelensky calling on the Ukrainian people to surrender. This fake video quickly spread across various social media platforms and was picked up and reported by the international media (Byman *et al.* 2023).

Countermeasures against such disinformation include real-time efforts to identify and ban accounts that spread false information, and the need for government intelligence agencies to actively engage in dialogue with civil society so that citizens can fact-check and verify information (Ivan *et al.* 2021).

In mid-February, just prior to the start of the invasion of Ukraine, Russia falsely announced that it had begun withdrawing its troops from the Ukrainian border. In response, the Secretary General of NATO showed commercial satellite images and clarified that this announcement was false (Lin-Greenberg & Milonopoulos 2022). Satellite imagery has rapidly increased in accuracy in recent years and is effective in detecting false information.

Showing off friendlies' achievements and courage

Showing friendly achievements and courage is effective in boosting the morale of allies and discouraging the war effort of opponents. It also has the effect of spreading its advantage to the international community and winning support. On May 11, 2022, the Ukrainian Defense Ministry's Twitter account posted the success of artillery attacks on Russian troops crossing the river. The tweet received over 14,000 likes and about 2,000 retweets (Helmus 2023). Also on the same day, a tweet by a Ukrainian soldier received many likes and retweets and became a central source of information for news outlets such as *Newsweek* and *France24* (Helmus 2023).

The courage and strong leadership of a leader is also important in boosting the morale of one's people and soldiers and in winning the support of the international community. During the Russian invasion, Ukrainian President Zelensky remained in the capital city of Kyiv and distributed selfies to inspire his people and to appeal to the international community for support (Kuleba 2022).

Operations in the Space, Cyber, and Electromagnetic Domains

Activities in the space, cyber, and electromagnetic domains are important in influencing human cognition. Information that contributes to creating narratives is collected mainly through activities in the space, cyber, and electromagnetic domains. In addition, the spread of disinformation and signalling through cyber means are effective in influencing the perceptions of adversaries. Also in the human cognitive domain, how quickly and accurately political leaders and military forces make decisions is an important factor. Sending misinformation and data and imposing complexity on adversaries can achieve relative superiority in the quality and speed of decision making.

Gathering information that contributes to creating narratives

To form a persuasive narrative, it is necessary to collect evidence for it. In particular, if an adversary is engaged in illegal activities, it is necessary to collect information on such illegal activities through activities in all domains. Among these, space, cyber, and electromagnetic means are important. For example, during the war in Ukraine, satellites acquired evidence of Russian military atrocities in Bucha. The U.S. obtained secret information about Russia's start of the war by intercepting communications.

Spreading disinformation and signalling by cyber means

Cyber and electromagnetic activities can interfere with an adversary's decision-making. Rovner (2022) noted that many of Russia's cyberattacks in the war in Ukraine were aimed at influencing public opinion by spreading disinformation, in addition to information theft. Wilde (2022) also stated that Russian cyber operations were aimed at the cognition and perception of Ukraine and the international community.

Before the war in Ukraine, articles pointed out that, with the start of the war, Russia could launch a massive cyberattack against the power grid, causing massive power outages and leaving millions of Ukrainians without heat and electricity in the bitter cold (Alperovitch 2022). In fact, on December 23, 2015, a Russian cyberattack caused the lights in western Ukraine to go out simultaneously, affecting 225,000 Ukrainian households (Lee, Assante & Conway 2016). Sending signals through such cyber activities can influence perceptions of other countries or people (Iasiello 2021).

Sending false information and data

The act of sending false information to enemy forces to deceive and confuse them has existed since ancient times, but the methods have changed with the development of information and communication technology. During the Russian invasion, Ukrainian hackers set up fake accounts of attractive women and tricked Russian soldiers into sending them photos. The Ukrainian military used the photos to determine the location of the Russian base, which it then shelled and destroyed (Ankel 2022).

Sending the wrong data can also be effective against artificial intelligence, which has been widely used in the military domain in recent years. With the development of deep learning technology, machine learning using large amounts of data is improving the quality of artificial intelligence. Taking advantage of this, sending data contaminated with the enemy's training data can confuse the opponent's machine learning and can reduce the quality of the artificial intelligence.

Adding complexity to adversaries

The use of decoys and other means to create the appearance of the presence of units or assets that do not exist is an age-old technique. In addition to conventional decoys, numerous unmanned weapons can be used in the future. In addition, operations in the space, cyber, and electromagnetic domains can deceive an adversary's ISR activities. Such activities can add complexity to an adversary's decision-making and can provide a relative advantage in decision quality and speed.

Maintaining and interfering with communications infrastructure

Since information dissemination is critical, it is necessary to maintain communication infrastructures. In addition, it is effective to sabotage communication infrastructures to disrupt the dissemination of information by the adversary. Russia launched cyberattacks against the Ukrainian government, military, and critical infrastructure computer systems at the beginning of the invasion of Ukraine, causing some Ukrainian systems to malfunction (Cattler & Black 2022). KA-SAT, used by Ukraine's military and intelligence agencies, also ceased functioning. In response, Ukraine maintained its information and communication infrastructures with the support of U.S. cyber forces and high-tech companies (Detsch & Yang 2022). As a result, Ukraine was able to quickly disseminate information to the world.

Methods in the Physical Domain

An important prerequisite for the creation and dissemination of effective narratives is the legitimate activity of friendly forces in the physical domain. In addition, the display of intent through physical troop actions is a traditional method of exerting cognitive influence on adversaries.

Legitimate activities of friendly forces

In today's wars, the battlefield is becoming more transparent (Barno & Bensahel 2022). In the age of information and communication technology development, the military is constantly operating under the watchful eye of many smartphones. In these situations, friendly troops and soldiers must always act lawfully. Such legitimate activities will lead to the support of the international community for their country and its allies. In addition, to counter disinformation, it is necessary to actively disseminate information that friendly forces are not engaged in illegal activities.

Diversion, intimidation, and declaration of intent through physical troop actions

In influencing the cognition of the opponent, the traditional physical domains of operations, the land, sea, and air domains, are still important. Psychological influence on the opponent through false troop movements, diversionary tactics, and surprise attacks are traditional methods that have been used repeatedly since prehistoric times. In addition, threats and statements of intent through physical military actions sometimes have a significant psychological impact on the opponent.

For example, from late 2021 to early February 2022, Russian forces surrounded Ukraine from the north, east, and south and conducted military exercises to intimidate Ukrainian leaders and citizens. Such intimidation, however, did not cause the Ukrainian government and people to give in.

Modelling

To plan operations in war, it is necessary to integrate and synchronize land, sea, air, space, cyber, electromagnetic, and cognitive means. To this end, this article proposes a model that synthesizes the methods in all domains described so far and integrates methods that influence the opponent's cognition.

Modelling the attack target: Three-Ring Model

Colonel John Warden of the U.S. Air Force developed the Five Ring Model in 1988 (Chun 2012). This model was used in planning for the Gulf War. In this model, enemy target groups are composed of five concentric circles according to their character. The closer to the centre of the concentric circles, the more important the target is. At the time of the Gulf War, the concentric circles representing Iraq were, from the centre, leadership, key industries, infrastructure, population, and combat forces.

The leadership, which is the most central in the Five Ring Model, consists of a group of individuals who have the power to decide how to start, sustain, and end the war and function as the nation's brains. The direct destruction of this, or the disabling of the chain of command and communication, would paralyse the entire nation.

The second circle, which encompasses the leadership, consists of key industries, which include oil, gas, power plants, and research facilities. The third circle is infrastructure, which includes the nation's basic industries and transportation networks—such as roads, bridges, and railroads. For the military as well as for the private sector, the loss of these would make survival difficult. The fourth circle is the people, and as Douhet (1921) once theorized, if they are targeted and bombed, the people may claim the cease-fire and overthrow their government. The fifth circle is the combat troops, who are the furthest from the centre of the circle. This indicates that it is inefficient to target the combat troops for attack.

In addition to the fact that human cognition is central to warfare, this article modifies the Five Ring Model to take into account the recent development of information and communication technology.

Considering Clausewitz's theory of the trinity of war—consisting of the people, the government, and the military—this paper places government leaders, military decision makers, and the people equally at the centre of the circle (1989). First of all, war is an extension of politics, and it is politics that determines the beginning and end of war. Given that Iraq was a despotic state at the time and maintained a strong police force, the people as the target of the attack were relatively undervalued in the Five Ring Model during the Gulf War. In constructing a generalized model, the leadership and the people should be treated equally as actors who determine the beginning and end of a war. Democracies, and even dictatorships, cannot wage war without the support of the people. Both Xi Jinping and Putin have a great interest in gaining public support. In addition, it is the military that wages war, and decision making by military commanders is also an important factor. For this reason, the model in this paper centres on the cognitive domain, which consists of the cognitions and decisions of government leaders, military decision makers, and the population.

The information and communication infrastructures are extremely important as a means for these decision makers to communicate their decisions to end units and others, and for these decision makers to gather information for decision making. If the information and communication infrastructure is destroyed, decision makers will not know what is going on and will not be able to make decisions. They also would not be able to communicate their intentions to the end units, and the military and the nation would be paralysed. For this reason, the information domain, composed of information and communication systems, is of secondary importance and is the second circle surrounding the cognitive domain. While the second circle in Warden's model is key industries and the third circle is infrastructure, this paper's model places special emphasis on the information and communication infrastructure as the second circle.

Furthermore, in today's world of advanced information and communication technology, where many news stories are distributed simultaneously around the world, support or opposition from the international community is also an important factor. The reactions of the international community influence citizens and national leaders. Therefore, it is necessary to incorporate the international community into the model.

The outermost is the physical domain, which is composed of physical combat forces. Directly attacking physical forces, as in John Warden’s model, is not a good approach because human lives on both sides will be lost. Therefore, the physical domain as a target of attack should be avoided as much as possible.

As described above, this paper proposes the Three-Ring Model: the cognitive domain consisting of political leaders, military decision makers, and the population; an information domain consisting of information and communication infrastructure; and a physical military force.

Modelling the method of attack

Then, this article models how the methods based on the latest technology listed in the previous section will work against the model consisting of the three rings described above. The following figure (**Figure 1)** shows the overall actions of the friendlies to influence the cognition of the adversary. Influencing an adversary’s perception is not done solely by cognitive means. It is a synthesis of operations in the traditional physical domains of land, sea, and air, as well as in the information-related domains of space, cyber, and electromagnetic waves, and the cognitive domain.

The right side of the model represents each specific friendly action. From the top are actions in the traditional physical domains of land, sea, and air, followed by actions in the information-related domains of space, cyber, and electromagnetic waves, and at the bottom are actions in the cognitive domain. Thus, **Figure 1** models the cross domain and comprehensive action of friendly actions in the cognitive, informational, and physical domains against the adversary’s cognitive, informational, and physical domains.

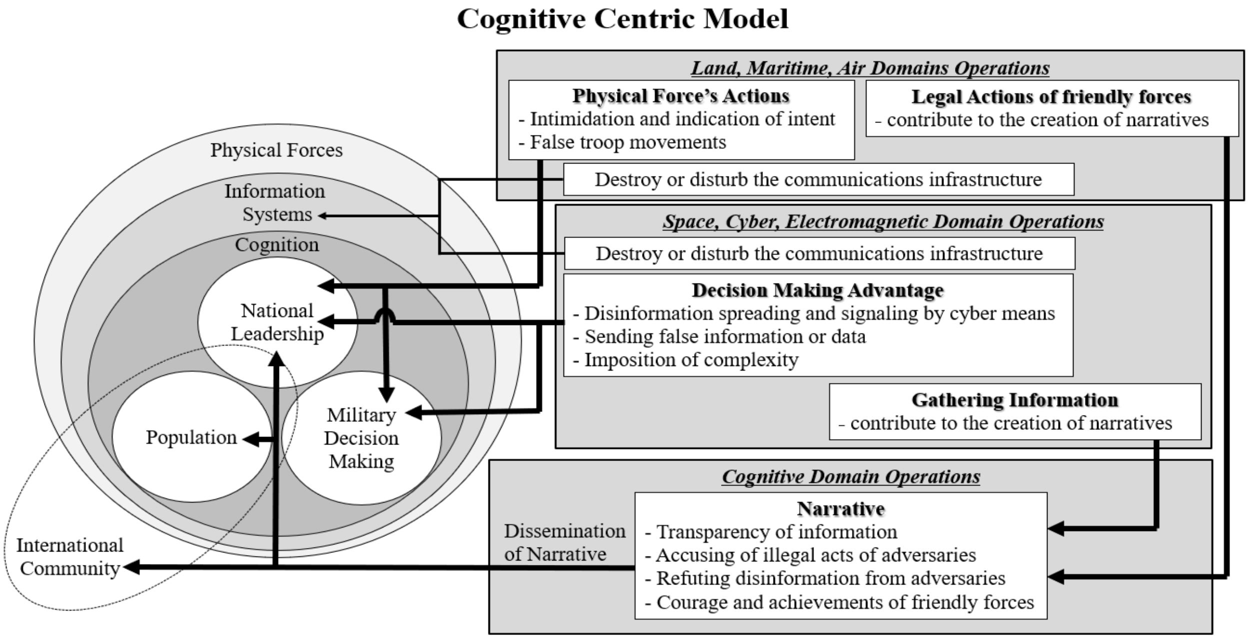
Cognitive Centric Model
Land, Maritime, Air Domains Operations
Physical Force’s Actions
- Intimidation and indication of intent
- False troop movements
Legal Actions of friendly forces
- contribute to the creation of narratives
Destroy or disturb the communications infrastructure
Space, Cyber, Electromagnetic Domain Operations
Destroy or disturb the communications infrastructure
Decision Making Advantage
- Disinformation spreading and signaling by cyber means
- Sending false information or data
- Imposition of complexity
Gathering Information
- contribute to the creation of narratives
Cognitive Domain Operations
Dissemination of Narrative
Narrative
- Transparency of information
- Accusing of illegal acts of adversaries
- Refuting disinformation from adversaries
- Courage and achievements of friendly forces
Physical Forces
Information Systems
Cognition
National Leadership
Population
Military Decision Making
International Community

Figure 1: Cognitive centric model

Operations in the cognitive domain

Operations in the cognitive domain are conducted by disseminating narratives to the national leaders, the population, and the international community. In generating narratives, it is effective to utilize information transparency and to accuse the adversary of illegal activities, as the West and Ukraine did during the war in Ukraine. It must also properly refute disinformation from the adversary. Narratives that show off the achievements and bravery of friendly forces are important to discourage opponents' will to fight and to gain support from the international community.

Operations in space, cyber, and electromagnetic domains

Operations in the space, cyber, and electromagnetic domains can assist operations in the cognitive domain and can directly influence the perceptions of adversaries. As the U.S. and Ukraine in the war in Ukraine used satellites to admissions evidence of Russian military atrocities and communications intercepts to obtain secret information about Russia's start of the war, intelligence gathering to generate effective narratives can be conducted by satellites, cyber means, and electromagnetic waves.

Cyber and electromagnetic means can be used to spread disinformation, and send signalls, and to influence political and military decision makers in adversaries. Sending false information and data by cyber and electromagnetic means can also deceive and confuse adversary forces. In addition, false deception through space, cyber, and electromagnetic means can impose complexity on an adversary's decision making. These can provide a relative advantage in the speed and quality of decision making.

Operations in the physical domain

Operations in the physical domain can also assist operations in the cognitive domain and can influence an adversary's perceptions. Direct combat against the opponent's physical forces should be avoided because of the human casualties on both sides, and priority should be given to influencing the perception of the opponent.

In a transparent battlefield in recent years, physical forces must operate legitimately and must contribute to the creation of a favourable narrative. In addition, diversion and intimidation through physical force actions to communicate intentions to the adversary are traditional and effective methods. In addition, destroying or disturbing the enemy's communications infrastructure through the information and physical domains can also be effective in interfering with the enemy's decision making.

Conclusion

This article explores how cognitive influence on an adversary can be exerted from multiple domains: land, sea, air, space, cyber, electromagnetic, and cognitive domains. To this end, this paper analysed the case of the war in Ukraine, a large-scale war between nations in which the latest science and technology was used, and extracted cases that influenced the adversary's cognition from the multiple domains. The analysis of the case studies revealed that the attacks on the domain of human cognition are conducted from all operational domains: land, sea, air, space, cyber, electromagnetic waves, and cognitive domains.

To plan military operations, it is necessary to synchronize operations in all domains. To this end, this paper provided a diagrammatic and comprehensive model of the methods of cognitive influence on the adversary. In doing so, this paper modified the Five Ring Model proposed by John Warden, taking into account the fact that human cognition is central to warfare and the recent development of information and communication technology, and proposed the Three Ring Model consisting of the cognitive, information, and physical domains.

War is a battle of wills on both sides. The purpose of war is not to kill and destroy the enemy but to bring it to it's knees and to make it believe that it has lost. It is also necessary to win the hearts and minds of the people of the other country and of the international community. To achieve this, it is necessary to focus on human cognition, not on physical aspects. For these reasons, the concept of Cognitive-Centric Warfare is needed.

References

Abdalla, NS, Davies, PHJ, Gustafson, K, Lomas, D & Wagner S 2022, 'Intelligence and the war in Ukraine: Part 1', *War on the Rocks*, 11 May, viewed 2 June 2024, <https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/>.

Alperovitch, D 2022, 'How Russia has turned Ukraine into a cyber-battlefield', *Foreign Affairs*, 28 January, viewed 2 June 2024, <https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield>.

Ankel, S 2022, 'Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says. Days later, the base was blown up', *Insider*, 5 September, viewed 2 June 2024, <https://www.businessinsider.com/ukraine-hackers-create-fake-profiles-russia-troops-share-location-ft-2022-9>.

Barno, D & Bensahel, N 2022, 'The other big lessons that the US Army should learn from Ukraine', *War on the Rocks*, 27 June, viewed 2 June 2024, <https://warontherocks.com/2022/06/the-other-big-lessons-that-the-u-s-army-should-learn-from-ukraine/>.

Beauchamp-Mustafaga, N 2019, 'Cognitive domain operations: The PLA's new holistic concept for influence operations', *China Brief, The Jamestown Foundation Global Research & Analysis*, vol. 19, no. 16, 6 September, viewed 2 June 2024, <https://jamestown.org/program /cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/>.

Berntsen, G & Fedasiuk, R 2022, 'To defeat autocracy, weaponize transparency', *War on the Rocks*, 23 August, viewed 2 June 2024, <https://warontherocks.com/2022/08/to-defeat-autocracy-weaponize/ >.

Blannin, P 2022, 'Modeling information warfare: Visualising definitions, fundamental characteristics, and foundational theories of contemporary information warfare', *Journal of Information Warfare*, vol. 20, no. 3, pp. 90-107.

Byman, DL, Gao, C, Meserole, C & Subrahmanian, VS 2023, 'Deepfakes and international conflict', *Brookings*, January, viewed 2 June 2024, <https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf>.

Cattler, D & Black, D 2022, ‘The myth of the missing cyberwar: Russia’s hacking succeeded in Ukraine—And poses a threat elsewhere, too’, *Foreign Affairs*, 6 April, viewed 2 June 2024, <https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar>.

Chun, CKS 2012, ‘John Warden’s Five Ring Model and the indirect approach to war’, *Theory of war and strategy*, Strategic Studies Institute, U.S. Army War College, Chapter 11, pp. 295-308.

Clausewitz, CV 1989, *On War*, revised edn., Princeton University Press, Princeton, NJ, US.

Coleman, F 2022, ‘To prosecute Putin for war crimes, safeguard the digital proof’, *Foreign Policy*, 10 April, viewed 2 June 2024, <https://foreignpolicy.com/2022/04/10/prosecute-putin-war-crimes-evidence-bucha-safeguard-digital-proof/>.

Demarais, A 2023, ‘Russia sanctions: 10 lessons and questions for what comes next’, *Foreign Policy*, 24 February, viewed 2 June 2024, <https://foreignpolicy.com/2023/02/24/russia-sanctions-war-ukraine-lessons-putin-energy-gas-oil/>.

Detsch, J & Yang, M 2022, ‘Russia prepares destructive cyberattacks’, *Foreign Policy*, 30 March, viewed 2 June 2024, <https://foreignpolicy.com/2022/03/30/russia-cyber-attacks-us-ukraine-biden/>.

Dong 2020 (董治强), ‘认知作战从隐蔽迷惑到攻芯控脑’, 解放军报, 17 September, viewed 2 June 2024, <http://www.81.cn/jfjbmap/content/2020-09/17/content_271042.htm >.

Duss, M 2022, ‘The war in Ukraine calls for a reset of Biden’s foreign policy’, *Foreign Affairs*, 5 May, viewed 2 June 2024, <https://www.foreignaffairs.com/articles/ukraine/2022-05-04/war-ukraine-calls-reset-bidens-foreign-policy>.

Golovchenko, Y, Hartmann, M & Adler-Nissen, R 2018, ‘State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation’, *International Affairs*, vol. 94, no. 5, pp. 975-94.

Helmus, TC 2023, ‘The Ukrainian Army is leveraging online influencers. Can the US military?’, *War on the Rocks*, 1 March, viewed 2 June 2024, <https://warontherocks.com/2023/03/the-ukrainian-army-is-leveraging-online-influencers-can-the-u-s-military/>.

Hutchinson, B 2022, ‘Strategic cognition war’, *Journal of Information Warfare*, vol. 21, no. 3, pp. 74-83.

Iasiello, E 2021, ‘What is the role of cyber operations in information warfare?’, *Journal of Strategic Security*, vol. 14, no. 4, pp. 72-86.

Julian-Varnon, K 2022, ‘Ukraine’s story can find listeners in Africa’, *Foreign Affairs*, 30 August, viewed 2 June 2024, <https://foreignpolicy.com/2022/08/30/ukraine-russia-war-africa-diplomacy-zelensky/>.

Khaldarova, I 2021, 'Brother or 'other'? Transformation of strategic narratives in Russian television news during the Ukrainian crisis', *Media, War & Conflict*, vol. 14, no. 1, pp. 3-20.

Kliman, D, Kendall-Taylor, A, Lee, K, Fitt, J & Nietsche, C 2020, 'Dangerous synergies', *Center for a New American Security*, May, viewed 2 June 2024, <https://www.cnas.org /publications/reports/dangerous-synergies >.

Kolesnikov, A 2022, 'Will Putin lose Russia? His grip on power rests on fantasy and fear', *Foreign Affairs*, 3 March, viewed 2 June 2024, <https://www.foreignaffairs.com/russian-federation/will-putin-lose-russia>.

Kuleba, D 2022, 'The fight for Ukraine is forging a new world. If Ukraine prevails against Russia, the global movement toward a more empowered and freer digital world will accelerate', *Foreign Policy*, 27 April, viewed 2 June 2024, <https://foreignpolicy.com/2022/04/27/ukraine-war-internet-metaverse-cyber-cryptocurrency/>.

Kuldkepp, M 2022, 'Stop falling for Russia's delusions of perpetual victory', *Foreign Policy*, 10 May, viewed 2 June 2024, <https://foreignpolicy.com/2022/05/10/russia-blind-spots-ukraine-propaganda/>.

Lee, RM, Assante, MJ & Conway, T 2016, 'Analysis of the cyber attack on the Ukrainian power grid', *SANS ICS and the Electricity Information Sharing and Analysis Center*, 18 March.

Lin-Greenberg, E & Milonopoulos, T 2022, 'Boots on the ground, eyes in the sky. How commercial satellites are upending conflict', *Foreign Affairs,* 30 May, viewed 2 June 2024, <https://www.foreignaffairs.com/articles/ukraine/2022-05-30/boots-ground-eyes-sky>.

London, D 2022, 'To reveal, or not to reveal. The calculus behind US intelligence disclosure', *Foreign Affairs*, 15 February, viewed 2 June 2024, <https://www.foreignaffairs.com/articles/ukraine/2022-02-15/reveal-or-not-reveal>.

Lupion, M 2018, 'The gray war of our time: Information warfare and the Kremlin's weaponization of Russian-Language digital news,' *Journal of Slavic Military Studies*, vol. 31, no. 3, pp. 329-53.

McCardle, G 2022, 'PSYOPS and paper bombing the enemy', *The SOFREP Media Group*, 17 December, viewed 2 June 2024, <https://sofrep.com/news/psyops-and-paper-bombing-the-enemy/>.

Milton, D 2022, 'Truth and lies in the Caliphate: The use of deception in Islamic State propaganda', *Media, War & Conflict*, vol. 15 no. 2, pp. 221-37.

Miskimmon, A, Roselle, L & O'Loughlin, B 2013, *Strategic Narratives: Communication Power and the New World Order*, Routledge, New York, NY, US.

Newman, H 2022, 'Information warfare: Leveraging the DMMI matrix cube for risk assessment', *Journal of Information Warfare*, vol. 21, no. 3, pp. 84-102.

Pappalardo, D 2022, '"Win the war before the war?": A French perspective on cognitive warfare', *War on the Rocks*, 1 August, viewed 2 June 2024, <https://warontherocks.com/2022/08/win-the-war-before-the-war-a-french-perspective-on-cognitive-warfare/>.

Paterson, T & Hanley, L 2020, 'Political warfare in the digital age: Cyber subversion, information operations and "deep fakes"', *Australian Journal of International Affairs*, vol. 74, no. 4, pp. 439-54.

Rid, T 2020, *Active Measures: The Secret History of Disinformation and Political Warfare,* New York, Farrar Straus & Giroux, New York, NY, US.

Roman, N, Wanta, W & Buniak, I 2017, 'Information wars: Eastern Ukraine military conflict coverage in the Russian, Ukrainian and US newscasts', *The International Communication Gazette*, vol. 79, no. 4, pp. 357-78.

Rovner, J 2022, 'Sabotage and war in cyberspace', *War on the Rocks*, 19 July, viewed 2 June 2024, <https://warontherocks.com/2022/05/intelligence-and-war-does-secrecy-still-matter/>.

Saressalo, T & Huhtinen, A 2022, 'Information influence operations: Application of national instruments of power', *Journal of Information Warfare*, vol. 21, no. 4, pp. 1-15.

Takagi, K 2022a, 'New tech, new concepts: China's plans for AI and cognitive warfare', *War on the Rocks*, 13 April, viewed 2 June 2024, <https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/>.

—2022b, 'The future of China's cognitive warfare: Lessons from the war in Ukraine', *War on the Rocks*, 22 July, viewed 2 June 2024, <https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/>.

Walton, C 2022, 'Can intelligence tell how far Putin will go?', *War on the Rocks*, 28 February, <https://warontherocks.com/2022/02/lessons-of-cold-war-intelligence-for-ukraine-today/>.

White House 2022, 'Remarks by President Biden providing an update on Russia and Ukraine', 18 February, viewed 2 June 2024, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/18/remarks-by-president-biden-providing-an-update-on-russia-and-ukraine-2/>.

Wilbur, DS 2022, 'Using junk mews to build an agenda for violence: Russian propaganda targeting American right-wing extremists', *Journal of Information Warfare*, vol. 21, no. 4, pp. 1-15.

Wilde, G 2022, 'Assess Russia's cyber performance without repeating its past mistakes', *War on the Rocks*, 21 July, viewed 2 June 2024, <https://warontherocks.com/2022/07/assess-russias-cyber-performance-without-repeating-its-past-mistakes/>.