CLAWS

ISSN 23939729

NO. 99

2023

MANEKSHAW PAPER

The Dogs of War

Multidomain Mercenaries Operating in the Ukraine War

PR Kumar

CENTRE FOR LAND WARFARE STUDIES

Field Marshal Sam Hormusji Framji Jamshedji Manekshaw, better known as Sam "Bahadur", was the 8th Chief of the Army Staff (COAS). It was under his command that the Indian forces achieved a spectacular victory in the Indo-Pakistan War of 1971. Starting from 1932, when he joined the first batch at the Indian Military Academy (IMA), his distinguished military career spanned over four decades and five wars, including World War II. He was the first of only two Field Marshals in the Indian Army. Sam Manekshaw's contributions to the Indian Army are legendary. He was a soldier's soldier and a General's General. He was outspoken and stood by his convictions. He was immensely popular within the Services and among civilians of all ages. Boyish charm, wit and humour were other notable qualities of independent India's best known soldier. Apart from hardcore military affairs, the Field Marshal took immense interest in strategic studies and national security issues. Owing to this unique blend of qualities, a grateful nation honoured him with the Padma Bhushan and Padma Vibhushan in 1968 and 1972 respectively.

Photographs courtesy: The Manekshaw family/FORCE

Field Marshal SHFJ Manekshaw, MC
1914-2008

CLAWS Occasional Papers are dedicated to the memory of Field Marshal Sam Manekshaw

MANEKSHAW PAPER No. 99, 2023

The Dogs of War
Multidomain Mercenaries Operating in the Ukraine War

PR Kumar

Centre for Land Warfare Studies
New Delhi

KNOWLEDGE WORLD
KW Publishers Pvt Ltd
New Delhi

Editorial Team : CLAWS

ISSN 23939729

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone: +91-11-25691308 Fax: +91-11-25692347
email: landwarfare@gmail.com; website: www.claws.in
CLAWS Army No. 33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To establish CLAWS as a leading Think Tank in policy formulation on Land Warfare, National Security and Strategic Issues.

Disclaimer: The contents of this paper are based on the analysis of materials accessed from open sources and are the personal views of the author. The contents, therefore, may not be quoted or cited as representing the views or policy of the Government of India, or the Ministry of Defence (MoD) (Army), or the Centre for Land Warfare Studies.

www.kwpub.in

Published in India by

Kalpana Shukla
KW Publishers Pvt Ltd
4676/21, First Floor, Ansari Road, Daryaganj, New Delhi 110002
Phone: 011 43528107 email: kw@kwpub.in • www.kwpub.in

Contents

The Dogs of War: Multidomain Mercenaries Operating in the Ukraine War

"Being a mercenary, … we just go wherever there's a mixture of money and trouble, and everyone in the galaxy is a potential customer".

– Howard Tayler

General

A mercenary is a hired professional soldier who fights for any state or nation without regard to political interests or issues.[1] Ever since warfare took on an organised form, institutionalised, political standing armies somewhere around the mid-17th century (mainly Westphalian states), often supplemented their military forces with mercenaries for their protection and furtherance of their national interests. Today, we see in most countries, corporate honchos, feudal landlords, housing societies and even wealthy individuals hiring security personnel to protect their families, business interests, and property. It's a risky and well-paid job. Some mercenaries make $500 to $1,500 per day. Interrogators are rumoured to make up to $14,000 per week. The salary ranges from $89,000 to $250,000 per year.[2] Astonishingly, we can see advertisements in prominent national newspapers in the USA and Europe and even the BBC, since the war started, inviting mercenaries for astronomical sums varying from $1,000 to $2,000 per day, for select jobs like extracting families from conflict areas in Ukraine.[3] Employer, experience, expertise, specialty, location, and danger potential ultimately determine the pay check. In this mix, there are idealists fighting for a cause, patriots, nationalists and even unpaid cannon fodder, who fight with nil or negligible pecuniary benefits.

UN Accepted Definition of Mercenaries[4]

- A mercenary is any person who:
  - is specially recruited locally or abroad in order to fight an armed conflict;
  - does, in fact, take a direct part in the hostilities;
  - is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of what promised or paid to combatants of similar ranks and functions in the armed forces of that Party;
  - is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict;
  - is not a member of the armed forces of a Party to the conflict; and
  - has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.
- A mercenary shall not have the right to be a combatant or a prisoner of war.

Mercenaries and the Laws of War

Historically, the law of war[5] has little to say about mercenaries. The term was not defined in Treaty Law, nor did the law of war establish "mercenary" as a distinct status with a special legal character. Before 1977, international legal regulation of mercenaries was limited mainly to a requirement based in the law of neutrality to prevent States from creating/forming mercenary groups. In 1977, the First Additional Protocol to the Geneva Conventions (API) significantly changed the law for mercenaries by withholding from a mercenary "the right to be a combatant or a prisoner of war".

Both Russia and Ukraine are signatories to API. Therefore, each is bound by Article 47[6] in the current armed conflict. Additionally, Ukraine is also a party to the 1989 International Convention against the recruitment, use, financing, and training of mercenaries. The 1989 Convention created a criminal law regime for mercenaries, which identifies and defines criminal offences, establishes rules of jurisdiction, and obligates enforcement measures. Furthermore, it expands the Article 47 definition of "mercenary" by removing the condition that a mercenary actually takes part in hostilities. Russia is not party to the 1989 Convention. Thus, unlike Ukraine, Russia is not subject to the Convention's obligations, such as the requirements to criminalise mercenary offences (Article 5), cooperate in prevention of

such offences (Article 6), and notify the UN Secretary-General of potential violations (Articles 8 & 10).[7]

For a variety of reasons, including narrowness of definition, and 'volunteer fighters who may not fight for private gains', legal experts say that application of the law in Ukraine may well turn out to be unworkable.[8] These operators do not fall strictly under the definition of 'mercenaries' as per UN convention, which incidentally is being increasingly questioned due to the changing nature and character of war, and widespread employment in most confrontations and conflicts. The status of non-kinetic, cognitive fighters waging war from their homes like hackers, Information Influence Operations (IIO) operators, drone operators sitting thousands of miles away—even tech giants like Meta, Google, Elon Musk who are participating and certainly influencing the war even strategically—needs clarity. Some amongst them may be getting paid, corporates are advancing their company and financial interests, and some may be 'lone wolf' warriors. Ethical and legal questions will need to be answered—are they soldiers or mercenaries? Does the Geneva Convention apply to them? Can they be prosecuted or even neutralised/killed in their homes far away? Would they be better categorised under the broader term 'Grey Zone Warriors'?

Mercenaries Gain Fame. While mercenaries are as old as warfare, their employment gained international attention due to the immense popularity of the 1980 Hollywood cult film titled the "Dogs of War"[9] (based on a phrase from William Shakespeare's play, 'Julius Caesar': "Cry, 'Havoc!', and let slip the dogs of war",[10] which literally means 'the havoc accompanying military conflict'. The movie shows a small mercenary unit of soldiers privately hired to depose the President of a fictional African country modelled after Guinea-Bissau, Guinea-Conakry, Equatorial Guinea and Angola (as they were in the late 1970s), so that a British tycoon can gain access to a platinum deposit.

Western Biased Narrative. The West led by the USA has dominated the 'information war and perception management' during the Ukraine conflict, and hence most reports on the war including employment of mercenaries are one-sided. Inputs on employment and the role of mercenaries employed by Ukraine are scant even when scanning Russian official and online media publications.

Mercenary Operations and Participation: Overview. Both Ukraine and Russia have boasted of staggering numbers of foreign volunteers and mercenaries willing to join the biggest conflict in Europe since World

War II. On 06 March 2022, Ukraine announced that some 20,000 people from 52 countries had applied to fight in the newly formed 'International Legion of Territorial Defence of Ukraine'. They reportedly include Americans, Canadians, and several European nationalities. "The whole world today is on Ukraine's side, not only in words but in deeds",[11] the Foreign Minister, Dmytro Kuleba, told Ukrainian television. Days later, the Russian Defence Minister, Sergei Shoigu, claimed that some 16,000 men from the Middle East had applied to fight for Russia.[12] "As for the mercenaries from all over the world being sent to Ukraine, we see that they do not conceal it, the Western sponsors of Ukraine, the Ukrainian regime, do not hide it,"[13] Putin said, in a meeting with his top security advisers. "That's why if you see that there are people who are willing to come as volunteers, especially not for money, and help people residing in Donbas, well, we need to meet them halfway and assist them in moving to the combat zone".[14] The infusion of outsiders and "irregular forces" has further complicated an already messy multidomain conflict. The battlefield in Ukraine is incredibly complex, with a range of violent non-state actors, private military contractors, foreign fighters, volunteers, mercenaries, extremists, and terrorist groups, not to forget the non-kinetic warriors involved in information warfare and perception management, apart from the political, diplomatic, economic manoeuvrings by all players, exacerbating an already chaotic global geostrategic economic security environment. The war has engulfed the world, and has exacerbated bilateral and multilateral tensions, caused economic misery—even recession—heightened fault lines specially between the three global powers (USA, China and Russia), and could precipitate a nuclear conflagration. The trigger could well be initiated by planned or rogue actions by multidomain mercenaries.

Russian Employment of Mercenaries

Most ex-colonial powers, USA and Russia, sell weapons and systems to many unstable regions of the world specially Africa and the Middle East. Russian 'guns-for-hire' have been seen in 5 of the 17 African countries that abstained on the first UN vote on Ukraine: The Central African Republic, Madagascar, Mali, Mozambique and Sudan. Many more of the abstentions, or no-shows, are buyers of Russian arms. These include Algeria, Angola, Sudan and Uganda, according to data collected by the Stockholm International Peace Research Institute (SIPRI). Western intelligence agencies and media showcase Putin's reliance on Yevgeny Prigozhin (oligarch billionaire considered Putin's right-hand man), the Wagner Group, and other private military contractors to

Wagner Mercenaries. Source: Alexander Nemenov, AFP via Getty Images.

supply mercenaries.[15] According to the Centre for Strategic and International Studies (CSIS), Russian employment of mercenaries with proven military operations includes 30 countries in four continents, from Venezuela to Libya and Afghanistan. The group has been active over the past eight years in Ukraine, Syria and African countries, and has repeatedly been accused of war crimes and human rights abuses.[16] Even prior to the commencement of actual operations of the Ukraine war, US and British intelligence spoke of a thousand Wagner mercenaries, including senior leaders, initially deployed to the eastern parts of Ukraine.[17]

Genesis of the Wagner Group and Its Role in Ukraine. A 51-year-old former Russian special forces officer, and member of the Glavnoye Razvedyvatelnoye Upravlenie (GRU), Russia's military intelligence

service, Lt Col Dmitri Utkin, is thought to have founded the Wagner Group and given his own former call-sign 'W/Vagner'.[18] The Wagner Group first saw action during Russia's annexation of Crimea in 2014, says Tracey German, professor of Conflict and Security at King's College, London. "Its mercenaries are thought to be some of the 'little green men' who occupied the region", she says. "Running a mercenary army is against the Russian constitution", she adds.[19] "However, Wagner provides the government with a force which is deniable. In the weeks leading up to Russia's invasion of Ukraine, it is thought that the Wagner Group mercenaries carried out "false flag" attacks in eastern Ukraine to give Russia a pretext for attacking. Messages have appeared on Russian social media recruiting mercenaries by inviting them to 'a picnic in Ukraine'.[20]

Wagner chief Yevgeny Prigozhin, centre, with soldiers in what they said was a salt mine in Soledar, Ukraine, in an image released on January 12, 2023. Source: NBC News.[21]

Who Funds the Wagner Group? The BBC has stated that Wagner Group "is spending more than $100 million each month in Ukraine".[22] Even though the group faces further economic sanctions, Wagner Group's influence and presence inside Russia has increased due to the Russian military suffering multiple setbacks. Some suggest Russia's

military intelligence agency, the GRU, secretly funds and oversees the Wagner Group. Mercenary sources have told the BBC that its training base in Mol'kino in southern Russia is next to the Russian army base.[23] Initially, however, Russia consistently denied the Wagner Group's connection with the state. The BBC investigation that identified Ukraine's links to the Wagner Group also links Yevgeny Prigozhin, the oligarch known as "Putin's chef", who as per British Intelligence also funds the Wagner Group.[24] Prigozhin is thought to make money from Wagner Group operations abroad. The US Treasury says he uses its presence to enrich mining companies which he owns, and has placed them under sanctions. An unnamed White House spokesman told Reuters that Mr. Prigozhin may want the Wagner Group to capture Bakhmut so they can control the salt and gypsum mines in the area.

Current Wagner Operations in Ukraine. Regarding the personnel on the ground, the United States and UK government estimate that the private military contractor has 50,000 personnel in Ukraine,[25] consisting of 10,000 contractors and 40,000 convicts recruited from Russian prisons, which has also been acknowledged by Reuters. They have been heavily involved in Russian efforts to capture the city of Bakhmut, in eastern Ukraine. Ukrainian troops report that Wagner fighters are attacking in large numbers over open ground with heavy casualties. The video link[26] purportedly showing fresh mass graves of Wagner mercenaries in a graveyard for their fighters, is tagged for viewing. After Russia captured Soledar in the outskirts of Bakhmut, a row broke out between the Russian Defence Ministry and Wagner Group about attributing credit.[27] At first, the defence ministry did not even mention the group. However, it then conceded that its mercenaries had played a "courageous and selfless" role.

The Noose Tightens around Wagner Group. Since the Wagner Group has accepted military equipment and violated UN Security Council resolutions, the United States has announced that they would implement further sanctions on Wagner; at the same time, the Biden administration is taking steps "to designate Wagner as a military end user", reported by Politico. In doing so, the Department of Commerce will prevent the Wagner Group from accessing any equipment based on United States technology, preventing the private military contractor from using such equipment in Ukraine. There are repeated calls from Ukraine and the West, led by the USA, for holding the Wagner Group mercenaries accountable for war crimes.

Ukraine's Mercenaries

Apart from the 'International Legion of Territorial Defense of Ukraine' mentioned above, the famous **Azov Regiment**,[28] a militia has drawn controversy for its alleged continuing association with both far-right groups and neo-Nazi ideology, including using controversial symbols linked to Nazism, and allegations that members of the group are participating in torture and war crimes. Since 2014, criticism of the Azov Regiment has been a recurring theme of Russian politics. In 2016, Amnesty International and Human Rights Watch received several credible allegations of abuse and torture by the regiment. Reports published by the UNHCR documented looting of civilian homes and unlawful detention and torture of civilians between September 2014 and February 2015 "by Ukrainian armed forces and the Azov regiment in and around Shyrokyne".[29] President Putin has categorised them as inhuman neo-Nazis, who have perpetrated many human rights violations including killings of Russian-speaking Ukrainians residing in the Donbas region. In fact, Putin attributes one of the reasons for the invasion to 'de-nazification' of Ukraine by removing far-right elements, the primary forces being the Azov militia. The Special Operations Detachment "Azov"—also known as the Azov Regiment and formerly the Azov Battalion—came into the limelight since 2014, as a unit of the National Guard of Ukraine based in Mariupol, in the coastal region of the Sea of Azov, from which it derives its name. The regiment had an estimated 900 to 2,500 combatants in 2017-2022. Most of the unit members are Russian speakers and come from the Russian-speaking regions of Ukraine. It also includes members from other countries. In the ongoing war, they gained the reputation of being very hardy, professional and tactically sound fighters who fought for every inch of territory during the siege of Mariupol, and made their final stand at Mariupol's Azovstal steel plant. Rumours suggests that a number of senior commanders from NATO were holed up there, but not substantaited. A significant amount of Azov fighters, including the regiment's commander since 2017, Denys Prokopenko, surrendered to the Russian forces on orders from Ukrainian high command.

Are Proclaimed Terrorists Joining the War, by Invitation from Both Sides.[30] There are disturbing news inputs, which are not being denied, of jihadists being invited to join the war in Ukraine for a handsome payment (a few thousand dollars a month) from Northern Syria. Al-Mayadeen—a pan-Arabist satellite news television channel based in Beirut, Lebanon—states that: "Radical Islamic terrorists in Idlib/Syria are among those foreigners

seeking to reach Ukraine to fight the Russians. Radical Islam is a political ideology that has been called Islamo-Fascist, and shares commonalities with the Nazi militias in Ukraine. Both the Nazis in Ukraine and the terrorists in Idlib are fighting the Russians. The most powerful terrorist force in Idlib is Hayat Tahrir al-Sham (HTS), a coalition of Islamist groups made up of Syrian and foreign fighters, and dominated by Al-Qaeda affiliate known as Jabhat-al-Nusra.[31] While Chechen Islamic scholar Salakh Mezhiev has pronounced the Russian invasion of Ukraine a 'jihad', which should be fought "for the Koran, for God", in order to save Islam and Russia against the 'filth' of NATO forces,[32] Russia has allowed Chechen strongman Ramzan Kadyrov to send in units of his Muslim volunteer fighters into Ukraine, whose operations have gone viral on social media.[33] Muslims of diverse national and ethnic backgrounds are playing a central role. Muslim clerics in Russia have backed Vladimir Putin's offensive and tried to rally the support of Russia's estimated 20 million or more Muslims (at least 14 per cent of the country's population). Ironically, Russian Muslims find themselves pitted against fellow Muslims defending Ukraine. Chechens are fighting on both sides.[34] "The main problem is the foreign fighters, they have nowhere to go", said Sinan Ülgen, a former Turkish diplomat and analyst with Carnegie Europe. "Sending the terrorists to Ukraine is one solution that the US and NATO are using. Just as the Obama administration used the Al-Qaeda terrorists to fight the Syrian government for regime change, those same terrorists can be utilized to fight the Russians in Ukraine and Idlib".[35]

Impact of Mercenaries in the War

Inputs indicate that the estimates of mercenaries on ground by both Ukraine and Russia are high, but this is more a wishlist than reality. Over time, foreign fighters have the potential to be "force multipliers", if highly trained and motivated, especially if former Special Forces (SF) personnel are fighting. SF are trained and well versed in hybrid warfare (irregular urban and rural insurgency) and can even be used for strategic operational tasks. There will be major issues of communication (language) and interoperability, training, coordination and synergy of action impacting optimal employment. Generally, mercenaries are not trusted with critical and latest weaponry and fight with old degraded weapons. US reports indicate that within the first ten days of the war, mercenaries operated by Russia quickly suffered losses. By the first few days, about two hundred mercenaries, some of whom belonged to the Wagner Group, had already died on the battlefield. However, in today's

world of information warfare and perception management, many volunteers come for the adventure, glory and 'social media recognition', are barely and rarely trained, serve as "cannon fodder", and generally cause more embarrassment and damage; their ineptitude can cause sudden losses leading to adverse tactical situations, impacting morale and even in some cases the future of the conflict. Capture of mercenaries and subsequent publicity is not good for either nation.

Ukraine's Militias and Mercenaries Have Made Significant Tactical and Operational Impact. Interestingly, the Ukrainian population have shown remarkable resilience, fighting spirit, cohesion, tactical acumen and ability to endure warfighting conditions. Ukraine has obviously anticipated an offensive manoeuvre from Russia, and have got its armed forces and militia and even civilian volunteers trained and armed for such occasion. There are reports in the media of NATO trainers from Europe and USA training Ukrainian troops and volunteers for tactical operations, as also in NATO armaments and equipment since Russia seized Crimea. There are also reports of mercenaries from all over Europe and even the USA who are fighting for Ukraine.[36] The results are on ground for all to see. They have contributed in large measure to bringing the Russian onslaught to a slow and agonising battle of attrition, in which they have by Western accounts inflicted far greater damage to men and material and suffered far less attrition. They quickly learnt, adapted, deployed tactically and effectively employed 'easy to handle' munitions like the Javelin, hand-held anti-aircraft/helicopter missiles, drones and loitering munitions, thereby creating an asymmetry when pitted against highly trained tank and gun crews, and other troops. It is a unique case of a motley crew of civilians, militias and mercenaries using sophisticated easy to use weapons versus highly trained troops following conventional methods and platforms, contributing to Ukraine's ability to stall the mammoth Russian war machine. The role of mercenaries and non-kinetic warriors showcases the impact and effectiveness of ingenuous hybrid/grey zone warfare in a conventional war. It has also visibly demonstrated how a vastly conventional, asymmetrically superior force (Russia) can be fought to a standstill by a resolute, mobile, small team of soldiers/mercenaries/volunteers equipped with light manoeuvrable weapon systems fighting a multidomain, hybrid tactical battle. It must be stated that while the Russians are slowly learning, inputs coming from the battle for Bakhmut indicate employment of mercenaries en masse without much tactical manoeuvre, resulting in large casualties.

Strategic Contribution by the Kinetic Mercenaries? Mercenaries/ militias from both the Russian and Ukrainian sides have been more effective in fighting in urban areas like Kyiv, Mariupol, Kharkiv, Soledar and the Donbas region. The essential question is whether mercenaries will alter the conflict's course, or even have operational or tactical impact. While evaluation can only be done later, so far the effect of mercenaries has been reported and felt at the strategic level. However, in case the war gets protracted into a long-winded insurgency campaign like in Iraq, Afghanistan and Vietnam (the West led by the USA are quite happy to prolong the war indefinitely, as long as it's with Ukrainian and mercenary blood), mercenaries would certainly gain more relevance. Already there are credible reports of effective and frequent Ukrainian resistance inside Russian-held territory. Forays across the Russian border also cannot be ruled out. These actions are more effectively and proactively activated by irregular forces/mercenaries.

The Non-Kinetic, Cognitive Mercenaries (Grey Zone Warriors)

Overview. Non-Kinetic warfare is a comprehensive operational concept that is applied in interlaced, overlapping and integrated electromagnetic spectrum, information and cyber space to enable the achievement of non-kinetic environment superiority. **Cognitive warfare** is non-kinetic, and embodies the idea of 'combat without fighting'.[37] Mastering the cognitive domain constitutes a new and major stake indispensable to the generation of combat power. By integrating all the elements available in the information, cyber and psychological domains and creating a force multiplier effect, not only by manipulating the perception of the target population but also by ensuring that the desired reaction is achieved. Here, the human mind becomes the battlefield. It is weaponisation of public opinion by an external entity. Its impact is frightful—everyone turns into a weapon. It has the potential to fracture and fragment an entire society, so that it no longer has the collective will to resist an adversary or even pushes the weaker side to continue to face a stronger opponent despite facing heavy losses in conventional warfare like Ukraine, its people and its armed forces.

Apart from the state' multidomain operations, both Russia (Belarus, allies) and Ukraine (NATO, the USA and her allies) have accepted the role of non-state players, corporates, groups and individuals extensively prior and during the War for non-kinetic, multidomain operations.

Over the ages, the term 'mercenary'—including its definition by the UN—applied to non-state kinetic warriors, later war also turned kinetic. The

relevance, execution and acceptance of war encompassing multiple domains, including cognitive and non-cognitive, has been accepted globally only in the 21st century. Experts and defence analysts possibly would feel more comfortable calling these fighters being engaged in 'grey zone warfare'. I have included them under 'non-kinetic mercenary' category to highlight the fact that these independent actors also engage for financial reasons or to further their agendas, and many operate internationally and follow no national boundaries, and can have strategic consequences. A compelling and strategically impactful assistance is providing the facilities of Starlink (3,667 terminals were donated by SpaceX and a further 1,333 sponsored by USAID)[38] for or without pecuniary benefits to Elon Musk (reportedly based on a tweet by Ukraine's Vice Prime Minister and Minister of Digital Information, Mykhailo Fedorov to tech and media giants). Starlink is providing Ukraine profound real-time IIRT (Information, Intelligence, Reconnaissance and Targeting) capabilities, as well as post-strike damage assessment capabilities, which is altering the status of the War.

Moreover, non-kinetic activities can cause material damage and physical casualties like inciting panic, riots, migration, and even jamming air, sea and land activity communication nodes causing paralysis and accidents. Similarly, hacking into financial and banking networks too can cause extensive turbulence. For example, use of Starlink for spreading rumour of a strike using an area weapon/or a tactical nuclear device in a city/town, can cause large-scale panic, migration and accidents leading to casualties. Similarly, a cyber attack on civil aviation communication links or electric grid can cause crashes and lifesaving equipment to stop, causing casualties.

Information Influence Operations (IIO)

There are four factors that allow the US/NATO/Ukraine narrative to dominate globally. First, the differences between NATO's and Russia's doctrine for cognitive warfare; second, implementation of NATO's experience gained through biannual exercises; third, strategic use of social media and channels under the control of the US and the West (virtual monopoly) as also large number of diplomats, think tanks, journalists and experts for creating favourable perceptions globally; and fourth, carefully planned IIO to elicit the desired reactions from the Ukrainians, Russians and the target population globally.[39] The NATO's cognitive warfare doctrine focuses on altering perceptions of societies and is not restricted to contested zones only. On the other hand, the Russian doctrine focuses more on the

area of conflict. In the Russian Gerasimov Doctrine,[40] the goal is to weaken the enemy state from within, using multidomain operations with special focus on information warfare, and emphsising on grey zone operations both by state and non-state players.

Ukraine's/NATO's Modus Operandi. The US/NATO/Ukraine narrative is carefully planned to project that the Ukrainians are giving a tough fight to the Russians and are winning despite disadvantages. Russian losses are shown as its defeat in the conflict, and Russian involvement in committing war crimes and violation of human rights is being drummed to international audiences repeatedly. In this warfare, the first movers have the advantage. Russia's external disinformation efforts have been largely ineffective because Ukrainian messages are being transmitted quickly to the target allied population who are already sceptical of the Russian media. The Western powers gained advantage over the Russian narrative by releasing intelligence regarding the Russian operations before they occurred. Besides, carefully selected videos, images have greater impact. The videos and images of 13 Ukraine soldiers on Snake Island asking the Russian warship to buzz off, Russian farmer on tractor capturing a Russian-tank and an old couple daring the Russian soldiers, have more impact than videos showing destruction of Russian arms depot, etc., to strengthen the determination of Ukrainians to face the Russians boldly. The world treats them as heroes. In aggregate, these campaigns enable Ukrainian messaging to dominate Western opinion and have been decisive in eliciting foreign military aid. Now Ukraine is going in for crowd-funding that would give a further boost to its narrative. To further the narrative, all stops have been pulled out specially of non-state actors; numerous players from independent media (tv, print, social), social media watchers and influencers, large IT companies like Meta, Google, have been harnessed for perception management and information warfare.

It needs serious evaluation that a "weaker opponent could achieve strategic victory bypassing the traditional battlefield, if it is fought successfully". This has great relevance for India, which is facing two adversaries especially China who is using its 'Three Warfares' doctrine against India to gain advantage in this domain. Our systems have to be geared up sufficiently for cognitive warfare, and to deny advantages to our adversaries. India's National Security Advisor, Ajit Doval stated that "the civil society is the new frontier of warfare, and it is the common people, their thinking, their perceptions, their sense of well-being, and their perception of their own governments, that can impact the will of the nation".[41] This calls for an

effective national and strategic organisation, and awareness programme for all citizens to understand its various dimensions and repercussions that can enable them to counter the misinformation pushed in by our adversaries, and also be capable of prosecuting offensive cognitive operations.

The beauty of non-kinetic operations is that there are no strict delineations between armed forces, government agencies, corporates or even individuals. Attribution is ambiguous, thus making proportionate response difficult. One cannot stop or legislate rules for the mind and cyber. Passionate nationalists or mercenaries merge into cognitive operations making identification of government sponsored or motivated individuals participating in non-kinetic warfare almost impossible, which is exactly what is happening in the Ukraine conflict. A clear illustration of its dominance is that virtually nothing much is being reported from the battlefields of Ukraine, but yet the Ukraine war dominates the net and hence the global mind.

To put it bluntly, IIO hacks the mind and brain. While cyber operations have thus far been limited, information operations have been in full flow from all sides. Russia, China and even Pakistan are certainly very advanced in exploiting information for strategic purposes. Russia is fighting to challenge the West's longstanding narrative dominance. While it has so far lost the Ukraine perception war, unlike what the USA and NATO feel, Russia is slowly consolidating its own narrative of the West's hypocrisy of democracy, continuous eastward movement of NATO despite assurances to the contrary, actual strictures on free markets, illiberal actions based on historic events since WWII, especially against the Global South and autocratic/illiberal governed nations. The increasing number of nations who abstained during the UN resolution is a fair test of Russian increasing influence, and economic realities. To fight and win information wars against foreign adversaries, long-term credibility is essential.

Cyber Warfare

The impact of cyber warfare conducted by non-state actors will be judged later; however, the proliferation of third-party, non-state cyber actors in the Ukraine war has important, and potentially negative, implications for the future. Ironically, the US is leading in setting a global precedent. The standards/precedent set by bigger powers and political leaders are more effective than formal agreements. The ongoing conflict in Ukraine has drawn in hackers vowing to conduct cyber attacks on behalf of both parties to the conflict. On the Ukrainian side, the government has called on hackers to join

its "IT Army" and there are indications that around 400,000 individuals have volunteered to provide their services. Additionally, hacktivist groups have independently taken up cyber arms against Russian interests. A similar dynamic exists on the Russian side. Notably, the Conti-ransomware group announced its backing of the Russian government and warned of cyber attacks against critical infrastructure. The Sandworm group, which has links to Russian military intelligence (GRU), is also involved.[42] Further details are enumerated below.

The Russia Story. The much-feared and hyped Russian "cyber blitzkrieg" has not happened in Ukraine. Russia has sophisticated cyber capabilities, and her hackers have worked their way into Ukrainian networks for many years. It is also unlikely that everything the Russians may be doing has been made public. Russia's Information Security Doctrine of December 2016 covered strategic deterrence, the information security of government agencies, critical national infrastructure and citizens, the armed forces and countering the threats posed by rival states, terrorists and criminals. The three main Russian intelligence agencies (the FSB, GU/GRU and SVR) have offensive cyber capabilities. A military commentary declared that dominance in cyberspace and military power are prerequisites for victory in modern war.[43] Russia appears not to have prioritised developing the top-end surgical cyber capabilities needed for high-intensity warfare. Most of the detected attacks are relatively unsophisticated and uncoordinated from individual and group hackers, compared to the methods designed by the US and several of its allies for high-intensity warfare and/or strategic surgical effect.[44]

The Ukrainian conflict started with the invasion of Crimea by Russian troops. As the conflict continued, Ukrainian and Russian hackers engaged in tit-for-tat cyber attacks while maintaining them at low intensity. In December 2015 and December 2016, the cyber attacks on the Ukrainian power grid showed that cyber capabilities could be used to escalate the conflict. Experts have generally reached a consensus that while the conventional kinetic war is ongoing in full swing, there is yet to be any significant cyber attack on Ukraine's infrastructure, intelligence, or communication systems. The rationale for low-key cyber activity could be that Putin did not want to destroy infrastructure on territory that he later planned to occupy as disabled systems can be expensive to repair, and may also take time to become fully functional; also take time; or it could be that he did not want to shut it down, for example, Ukrainian government computer systems which can be used to gather intelligence in wartime; the real possibility is that the decision to

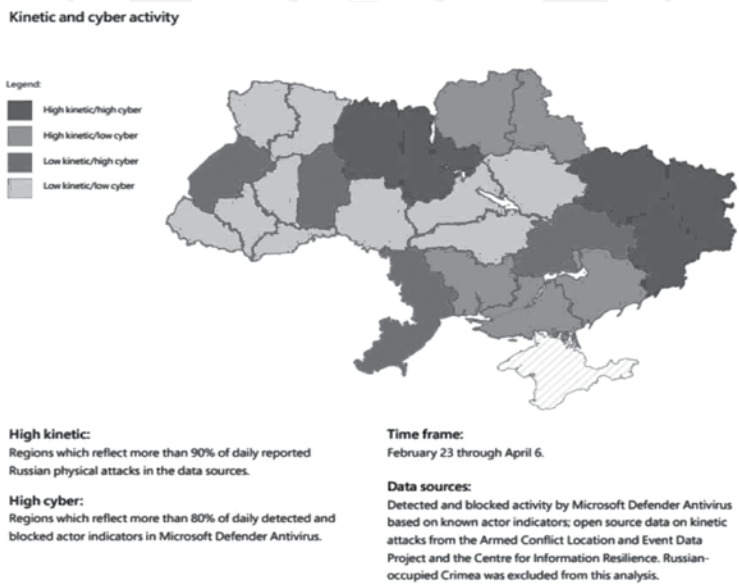
invade Ukraine was taken at the highest level and didn't trickle down the chain of command until it became too late to undertake cyber attacks that take months to organise. The probability of wanting a quick kinetic victory for the world to see the military might of Russia appears thin, given the slow pace of operations, and his inability to take any major city, specially Kyiv. Russia might also be wary of better cyber and technological capabilities of the West and watching how the US and NATO intelligence services have pushed back against the Kremlin's disinformation campaigns. So far, the cyber attacks have been relatively basic DDoS, or distributed denial-of-service attacks. Hackers have bombarded Ukrainian government websites with so much traffic that servers are forced to go offline for a period of time. And these kinds of attacks, though effective for short-term disruption, are not really like new or impressive cyber capabilities.[45] There have been stray reports of Russian cyber mercenaries deploying wiper malware to delete data that's been held by the Ukrainian government agencies and by at least one financial institution. This is a more sophisticated form of attack, but one that was largely thwarted. Possibly of greater significance is the cyber cooperation and coordination achieved under the leadership of the USA of governments and businesses in Ukraine, Europe, the Baltic States, and Poland, and coordination with the non-government hackers.

Can Russia Step Up Its Cyber War as Stalemate Continues/or in Desperation? Russia certainly has much better and potent capabilities. It could ramp up its assault on Ukraine and target Western nations to inflict on them the same kind of chaos wrought by sanctions, for example, by targeting companies and financial markets, or even target healthcare systems and power networks.[46]

Russian Pre-war Actions. Before the invasion began, Ukraine has been under a continuous barrage of cyber attacks. Since 15 February 2022, Ukraine experienced more than 3,000 DDoS attacks till 24 February. In January 2022 itself, wiper malware, a malicious software that erases the targeted computer's hard drive was detected in Ukrainian government and private sector networks.[47] There were a number of espionage attacks on high-value targets. New malware was distributed through phishing campaigns. Text messages were sent to personnel of Ukraine's 53rd and 54th Mechanised Brigades near the frontline, informing the soldiers that Russian units deployed in Donbas would attack on 22 February. The messages called on Ukrainian servicemen to desert their posts to save their lives in a psychological warfare tactic. On 23 February, Ukrainian

government websites of Cabinet Ministers, Federal Security Service of Ukraine, Defence Ministry, Parliament, and the Ministry of Foreign Affairs were hit with relatively unsophisticated and short-lived Distributed Denial-of-Service (DDoS) attacks. In the early phase of the conflict, some ATMs in Ukraine were unable to dispense cash. On the morning of the invasion, most crucially, hackers jammed the satellite signal of Viasat Inc., which delivered broadband satellite Internet services to Ukraine and some other parts of Europe.[48] Viasat provides Internet service to the Ukrainian army and several Western militaries. It is suspected that the cyber attack on Viasat was carried out to compromise Ukraine's command-and-control systems. The attack was marginally successful. Online inputs as also Western intelligence agencies attribute the majority of attacks to non-governmental voluntary groups or lone wolf warriors.

Cyber Warfare Continues. Since then, the cyber war is continuing between Russia and Ukraine. Russian hackers are actively supporting Russian military's strategic and tactical objectives. Kinetic and cyber military operations have been directed towards similar military targets. High intensity military actions frequently overlapped with concentrated cyber operations during the first two months of the invasion. Kinetic and cyber activity map is given below.



Source: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Source: https://github.com/curated-intel/Ukraine-Cyber-Operations

Russian ransomware operators offered their services to the government, threatening to retaliate against governments that sought to punish Russia. These seem to be loosely controlled proxy groups and not a unified effort. A Ukrainian member of the Russian-linked Conti-ransomware group, for instance, leaked the group's internal chat logs to counter the pro-Russian effort.[49]

Hacking of Apps Used for Artillery Fire Support. To speed up the process of calling in artillery fire support, Ukrainian artillery units were using apps in their smartphones. Russian hackers hacked the app easily, geo-located artillery batteries accurately and brought down devastating counter battery fire to destroy the guns.

Deployment of Malware and Salient Threat Actors. Russia deployed additional destructive malware from its arsenal of cyber weapons regularly aimed at Ukraine government agencies, operational units and networks, economic hubs. Some of the destructive malware identified are HermeticWiper (23 February), WhisperGate (13 January), IsaacWiper (24 February), CaddyWiper (14 March), RURansomWiper (1 March), DoubleZero (17 March). Salient threat actors, to name some, are UNC1151 (Belarusian-Phishing campaigns, hacking large areas including military personnel, defacing websites), APT28, Gamaredon, DanaBot, Sandworm, Strontium and many more.[50] Russians in turn were subjected to massive

cyber attacks. To illustrate, on 02 March 2022, Russia's cyber defence agency gave an alert that 17,500 IP addresses and 174 internet domains were involved in DDoS attacks on Russian sites and provided private organisations with mitigation measures.

Russia's control of cyberspace has been hampered by global tech companies that:

- created a strategic digital blockade of Russia.
- kept free and unrestricted internet content available to Russian citizens.
- ensured that the internet was still accessible through satellite broadband.
- counteracted Moscow's information warfare.
- prevented numerous cyber attacks on Ukraine's government and infrastructure.

Mercenary Internet Giants Showcase Their Ability to Shape the Global Security Environment

Even before Ukraine's Vice Prime Minister and Minister of Digital Information, Mykhailo Fedorov sent tweets to Apple, Google, Netflix and Starlink asking for help, global tech companies were working to protect the internet; from its undersea cables to the 29 billion devices connected to it and the 2.5 quintillion bits of data created and carried on it daily—from the impact of the conflict. Global tech companies like Facebook (Meta), Google, Twitter were able to step in with a speed and agility that individual countries did not possess, helping to neutralise Russia's digital strategy**.** If global tech companies can use their agility and innovation to counter aggression and authoritarianism, their potential to be a power is unparalleled. And as they diversify their infrastructure, products and services, their role and influence in determining the future of the free, global and interoperable internet will only increase. To illustrate, Twitter has officially stated that it will downrank or not promote Sputnik and RT content. Microsoft has said that its Bing search engine is not going to send users any content on Russian state media unless it is proved that the user actually wanted the to go. Google news has said that they will no longer feature Kremlin news content in news searches and Facebook has outrightly blocked Russian state media content, reportedly at the request of governments. This has not necessarily gone down well with many nations or public observers of the social media as it has far-reaching implications on freedom of social media, for which there are particularly zealous activists. This has highlighted the urgency and necessity to establish international protocols to ensure global giants act

responsibly, fairly with accountability, failing which there are significant risks to the international order. In fact, it appears that on numerous occasions, it has been tech companies rather than governments that have taken the lead in controlling the Internet based on their perceptions and biases.

Official Russian Response to Ukraine and the West's Cyber Operations. Russian Ministry of Foreign Affairs has clearly stated that persons involved in cyber aggression against Russia will face serious consequences.[51] On 29 March, TASS reported that Russia will seek liability for those involved in cyber aggression against the country. The Ministry specifically added that "an army of cyber mercenaries, which pursue concrete combat tasks that border on terrorism, is waging a war against Russia, and will be held accountable".[52] Russia has stated that "Ukrainian special detachments of information and technical influence, trained by the United States and other NATO member states, wage cyber war involving anonymous hackers and provocateurs, who follow orders of Western coordinators supporting the Kiev regime". The statement added that, "We are faced, in fact, with the war waged by cyber-mercenaries, who have concrete warfare tasks, which often border on open terrorism".[53]

Disinformation and Psychological Operations (PSYOPs) in Ukraine. PSYOP's influences mind starting from the leaders, force commanders and troops to the common man. It relies on the ability to collect information (mainly available online and in social media), analyse it, and rapidly exploit the information environment, which is increasingly being done by non-combatants/hackers/cyber warriors. The competition for influence has a distinct first-mover advantage. Research shows that simply countering fake news with accurate information is not enough due to cognitive bias and disinformation effects (echo chamber), whereby repeated information can change people's perceptions of past events. It is therefore critical to engage with adversarial narratives before they gain traction, which can generate credibility, especially when corroborated by outside observers.[54]

Russia's PSYOPS campaign relies on both state-sponsored networks and private operators to spread disinformation.[55] Internally, Russia is targeting its citizens by blocking Western social media and news platforms while simultaneously pushing pro-invasion propaganda. Interestingly, here, too, individual citizens and groups have taken the lead, specially the ultra-nationalists. This has created a constrained information environment and has further divided the country between those who rely on state sponsored media and those who use VPNs to circumvent censorship.

Interestingly, Russia's external disinformation efforts have been largely ineffective. Such activity is likely to step up in tempo, breadth and strength as the on-the-ground military situation trends towards stalemate. Efforts at disinformation will increase with the passage of time, as Russia tries to recapture lost media space and create new spaces and storylines, with focus on nations not directly involved in the conflict like the Global South, Middle East, South and South-East Asia.

Conclusion

Mercenaries have always been participants during any competition, confrontation and conflict between nations. The scope and role of mercenaries has now widened to include kinetic and non-kinetic (grey zone) warriors/participants. Interestingly, in the Ukraine war, the role of the non-kinetic, cognitive vertical is increasingly taking centre stage during all stages of conflict—pre-war-ongoing war-attrition stage. The non-kinetic mercenary has provided strategic support compared to the tactical contribution by the fighting mercenaries. The role and impact of mercenaries in a total war scenario has been limited as of now; however, as the conflict drags on in an attrition phase, kinetic mercenaries could prove to be strategic force multipliers. A combination of the two could prove to be decisive.

Notes

1. *Encyclopedia Britannica* and Wikipedia. Accessed on August 5, 2022.
2. "How much do mercenaries make?", Calendar.Canada.ca, available at https://www.calendar-canada.ca/faq/how-much-do-blackwater-mercenaries-make. Accessed on February 23, 2023.
3. "Private military firms see demand in Ukraine war", bbc.com, March 9, 2022, available at https://www.bbc.com/news/world-us-canada-60669763. Accessed on February 17, 2023.
4. "International Convention against the Recruitment, Use, Financing and Training of Mercenaries", from UN HR Office of the High Commission, General Assembly resolution 44/34 adopted December 4, 1989, available at https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-against-recruitment-use-financing-and. Accessed on May 3, 2022.
5. *Encyclopedia Britannica*, available at https://www.britannica.com/topic/law-of-war and accessed on March 15, 2023. Also see, "The laws of war in a nutshell", October 19, 2016, International Committee of the Red Cross (ICRC), available at https://www.icrc.org/en/document/what-are-rules-of-war-geneva-conventions. Accessed on March 18, 2023. Read Wikipedia: "The law of war is the component of international law that regulates the conditions for initiating war (*jus ad bellum*) and the conduct of warring parties (*jus in bello*). Laws of war define sovereignty and nationhood, states and territories, occupation, and other critical terms of law. Among other issues, modern laws of war address the declarations of war, acceptance of surrender and the treatment of prisoners of war; military necessity, along with *distinction* and *proportionality*; and the prohibition of

certain weapons that may cause unnecessary suffering.[1][2] The *law of war* is considered distinct from other bodies of law—such as the domestic law of a particular belligerent to a conflict—which may provide additional legal limits to the conduct or justification of war." Available at https://en.wikipedia.org/wiki/Law_of_war. Accessed on December 22, 2022.

6. Geneva Convention relative to the Protection of Civilian Persons in Time of War of 12 August 1949: "A mercenary shall not have the right to be a combatant or a prisoner of war. Has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces."
   ART. 47: *Inviolability of rights*
   — Protected persons who are in occupied territory shall not be deprived, in any case or in any manner whatsoever, of the benefits of the present Convention by any change introduced, as the result of the occupation of a territory, into the institutions or government of the said territory, nor by any agreement concluded between the authorities of the occupied territories and the Occupying Power, nor by any annexation by the latter of the whole or part of the occupied territory.
7. Robert Lawless, "Are Mercenaries in Ukraine?", Lieber Institute, West Point, Articles of War, March 21, 2022, available at https://lieber.westpoint.edu/are-mercenaries-in-ukraine/. Accessed on April 13, 2022.
8. "EXPLAINER—Is it legal for foreigners to fight for Ukraine?" Read more at: https://economictimes.indiatimes.com/news/defence/explainer-is-it-legal-for-foreigners-to-fight-for-ukraine/articleshow/90195649.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. Accessed on March 18, 2023.
9. Wikipedia, "Dogs of War" (1980 Hollywood film), available at https://en.wikipedia.org/wiki/The_Dogs_of_War_(film). Accessed on November 15, 2022.
10. Wikipedia, "The dogs of war" (phrase), available at https://en.wikipedia.org/wiki/The_dogs_of_war_(phrase). Accessed on November 15, 2022.
11. Prakash Nanda, "Russia-Ukraine War Ignites The 'Dirty Battle' Of Foreign Mercenaries, Private Army & Crazy Volunteers", November 13, 2022, in *The EurAsian Times*, available at https://eurasiantimes.com/russia-ukraine-war-ignites-the-dirty-battle-of-foreign-mercenaries/. Accessed on February 25, 2023.
12. Ibid.
13. Ibid.
14. Robin Wright, "Will Mercenaries and Foreign Fighters Change the Course of Ukraine's War?", April 22, 2022, available at https://www.newyorker.com/news/daily-comment/will-mercenaries-and-foreign-fighters-change-the-course-of-ukraines-war. Accessed on April 21, 2022.
15. "Putin's Chef or Successor? Yevgeny Prigozhin, the Russia Oligarch, Leading a 'Brutal' Fight in Ukraine", February 13, 2023, News 18, available at https://www.news18.com/news/world/russia-wagner-group-ukraine-war-yevgeny-prigozhin-vladimir-putin-7069381.html. Accessed on February 20, 2023.
16. "What is Russia's Wagner Group of mercenaries in Ukraine?", BBC Group, April 6, 2022, available at https://www.bbc.com/news/world-60947877. Accessed on April 13, 2022.
17. "British intelligence says Russia's Wagner Group deployed to eastern Ukraine", Reuters, March 29, 2022, available at https://www.reuters.com/world/europe/british-intelligence-says-russias-wagner-group-deployed-eastern-ukraine-2022-03-28/. Accessed on December 18, 2022.
18. John Dobson, "Putin's shadowy 'foreign legion' expands his geopolitical influence", November 20, 2022, *The Sunday Guardian*, available at https://sundayguardianlive.com/world/putins-shadowy-foreign-legion-expands-geopolitical-influence. Accessed on January 9, 2023.
19. n. 16.

20. "War in Ukraine: How Russia is recruiting mercenaries", BBC News—Russia-Ukraine War, March 12, 2022, available at https://www.bbc.com/news/world-europe-60711211. Accessed on November 18, 2022.
21. NBC News of January 13, 2023. Available at https://www.nbcnews.com/news/world/russia-ukraine-war-wagner-yevgeny-prigozhin-putin-chef-soledar-rcna65471. Accessed on February 1, 2023.
22. Ellis Clay, "The Role of Wagner Group in Ukraine", December 25, 2022, The Institute of World Peace, available at https://theowp.org/reports/the-role-of-wagner-group-in-ukraine/. Accessed on January 28, 2022.
23. n. 20.
24. n. 14.
25. n. 16.
26. https://www.nytimes.com/2023/01/24/world/europe/wagner-group-cemetery-russia-ukraine.html?smid=url-share
27. Evan Gershkovich and Ian Lovett, "Report on the Ukraine War", *Wall Street Journal*, February 12, 2023, available at https://www.wsj.com/articles/russias-wagner-group-claims-gains-near-bakhmut-in-eastern-ukraine-77faa1cd
28. "Profile: Who are Ukraine's far-right Azov regiment?", Al Jazeera, March 1, 2022, available at https://www.aljazeera.com/news/2022/3/1/who-are-the-azov-regiment. Accessed on August 19, 2022. Also see, "Azov Movement", Stanford Center for International Security and Cooperation, available at https://cisac.fsi.stanford.edu/mappingmilitants/profiles/azov-battalion. Accessed on January 2023.
29. "Report on the human rights situation in Ukraine 16 November 2015 to 15 February 2016" *(PDF). Office of the United Nations High Commissioner for Human Rights*, February and May 2016, available at https://www.ohchr.org/sites/default/files/Documents/Countries/UA/Ukraine_13th_HRMMU_Report_3March2016.pdf. Accessed on June 10, 2022.
30. Dr. Adil Rasheed, "Jihadists, White Supremacists Vex Russia–Ukraine War", IDSA Comment, March 28, 2022, available at https://www.idsa.in/idsacomments/jihadists-white-supremacists-vex-russia-ukraine-war-arasheed-280322. Accessed on November 15, 2022. Also see, Steven Sahiounie, "Terrorists from Syria go to Ukraine to fight Russia: will Turkey suffer?". Source: Al Mayadeen, March 8, 2022, available at https://english.almayadeen.net/articles/blog/terrorists-from-syria-go-to-ukraine-to-fight-russia:-will-tu. Accessed on December 5, 2022.
31. Ibid.
32. Robert D. Crews, "Muslims are Fighting on Both Sides in Ukraine", *The Washington Post*, March 10, 2022.
33. Ibid.
34. Neil Hauer, "Chechens Fighting Chechens in Ukraine", March 3, 2022, *New Lines Magazine*, available at https://newlinesmag.com/reportage/chechens-fighting-chechens-in-ukraine/. Accessed on March 18, 2023.
35. Dr. Adil Rasheed, n. 30.
36. "US Mercenaries in Custody Reveal Corruption in Ukrainian Army", published on June 20, 2022**,** available at https://www.telesurenglish.net/news/US-Mercenaries-in-Custody-Reveal-Corruption-in-Ukrainian-Army-20220620-0001.html. Accessed on January 27, 2023.
37. Paraphrased from Martti Lehto and Gerhard Henselmann, "Non-kinetic Warfare—The new game changer in the battle space", *ResearchGate*, March 2020, available at https://www.researchgate.net/publication/339943524_Non-kinetic_Warfare_-_The_new_game_changer_in_the_battle_space_316_Non-kinetic_Warfare_-The_new_game_changer_in_the_battle_space. Accessed on August 25, 2022. Also read, "Countering cognitive warfare: awareness and resilience", May 20, 2021, NATO Review, available at https://www.nato.int/

docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html. Accessed on August 31, 2022.
38. "SpaceX, USAID deliver 5,000 satellite internet terminals to Ukraine", Reuters, April 6, 2022, available at https://www.reuters.com/technology/spacex-usaid-deliver-5000-satellite-internet-terminals-ukraine-2022-04-06/. Accessed on November 17, 2022.
39. S. D. Pradhan, "Role of cognitive warfare in Russia-Ukraine conflict: Potential for achieving strategic victory bypassing traditional battlefield", May 8, 2022, timesofindia.indiatimes.com, available at https://timesofindia.indiatimes.com/blogs/ChanakyaCode/role-of-cognitive-warfare-in-russia-ukraine-conflict-potential-for-achieving-strategic-victory-bypassing-traditional-battlefield/. Accessed on January 31, 2023.
40. Ofer Fridman, "On the "Gerasimov Doctrine: Why the West Fails to Beat Russia to the Punch", October 4, 2019, NDU Press, available at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1981229/on-the-gerasimov-doctrine-why-the-west-fails-to-beat-russia-to-the-punch/. See also, Molly K. McKew, "The Gerasimov Doctrine: It's Russia's new chaos theory of political warfare: And it's probably being used on you", Politico.com, September/October 2017 issue, available at https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/. Both articles accessed on February 25, 2023.
41. "Civil society, the new frontiers of war, can be manipulated to hurt a nation's interests: Ajit Doval", indianexpress.com, January 31, 2023, available at https://indianexpress.com/article/cities/hyderabad/ajit-doval-nsa-warfare-civil-society-7619555/. Accessed on January 31, 2023. Also see, "Subverting civil society is new frontier of war: NSA Ajit Doval", timesofindia.indiatimes.com, November 13, 2021, available at https://timesofindia.indiatimes.com/india/subverting-civil-society-is-new-frontier-of-war-nsa-ajit-doval/articleshow/87675717.cms. Accessed on January 31, 2023.
42. Erica D. Lonergan, "Cyber Proxies in the Ukraine Conflict: Implications for International Norms", CFR, March 21, 2022, at https://www.cfr.org/blog/cyber-proxies-ukraine-conflict-implications-international-norms. Accessed on December 18, 2022.
43. Ministry of Defence, "Превосходство в киберпространстве становится одним из условий победы в войнах", April 22, 2019, available at https://function.mil.ru/news_page/country/more.htm?id=12227079@egNews. Accessed on January 28, 2023.
44. Maj Gen PK Mallick, VSM (Retd), "War in Ukraine: Are Russia's Cyber Warfare Capabilities Overhyped?", May 2, 2022, VIF India, available at https://www.vifindia.org/article/2022/may/02/war-in-ukraine. Accessed on August 24, 2022.
45. Jessica Brandt and Adrianna Pita, "How is Russia conducting cyber and information warfare in Ukraine?", March 3, 2022, Brookings Institute, available at https://www.brookings.edu/podcast-episode/how-is-russia-conducting-cyber-and-information-warfare-in-ukraine/. Accessed on May 3, 2022.
46. Elizabeth Gibney, "Where is Russia's cyberwar? Researchers decipher its strategy", March 17, 2022, *Nature Magazine*, available at https://www.nature.com/articles/d41586-022-00753-9. Accessed on April 25, 2022.
47. Maj Gen PK Mallick (Retd), n. 44.
48. Katrina Manson, "The Satellite Hack Everyone Is Finally Talking About", March 1, 2023, Bloomberg, available at https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/?leadSource=uverify%20wall. Accessed on March 18, 2023.
49. Brandon Valeriano et al., "Putin's Invasion of Ukraine Didn't Rely on Cyberwarfare. Here's Why", Cato Institute, March 7, 2022, available at https://www.cato.org/commentary/putins-invasion-ukraine-didnt-rely-cyberwarfare-heres-why
50. Ibid.
51. Russian News Agency, TASS, March 29, 2022, available at https://tass.com/politics/1429201?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com. Accessed on April 26, 2022.

52. Ibid.
53. Ibid.
54. Zara Abrams, "The role of psychological warfare in the battle for Ukraine", June 1, 2022, American Psychological Association, available at https://www.apa.org/monitor/2022/06/news-psychological-warfare. Accessed on December 25, 2022.
55. "Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses", November 3, 2022, OECD, available at https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/. Accessed on January 4, 2023.

SUBSCRIBE NOW

SUBSCRIPTION RATES

IN INDIA
☐ Rs. 500 /- per copy

SAARC COUNTRIES
☐ US $ 15 per copy

OTHER COUNTRIES
☐ US $ 20 per copy

☐ Rs. 1000 /- Annual Subscription (2 issues)

TO SUBSCRIBE SEND YOUR REQUEST TO

Centre for Land Warfare Studies (CLAWS)
RPSO Complex, Parade Road, Delhi
Cantt, New Delhi - 110010
Tel: +91-11-25691308
• Fax: +91-11-25692347 • Army: 33098
E-mail: landwarfare@gmail.com
www.claws.in

The paper examines the role of mercenaries operating in the Ukraine War. As per the UN definition, 'mercenary is a hired professional soldier who fights for any state or nation without regard to political interests or issues'. With war having become multi-domain—operations involving both kinetic and non-kinetic operations, the author examines the role and impact of both type of mercenaries. The cognitive mercenary, be it in the domain of information, cyber and economic warfare, as an individual (Elon Musk) or corporates (META and Google), are playing an equally important role in the war.

Both Ukraine and Russia have boasted of staggering numbers of foreign volunteers and mercenaries willing to join the biggest conflict in Europe since the Second World War. The paper details the kinetic mercenary operations from both sides including the much-touted activities of the infamous 'Wagner Group' and 'Azov Regiment/Militia'.

Cognitive warfare which is non-kinetic, and embodies the idea of combat without fighting, has also been covered in detail specially in the domains of Information Influence Operations (IIO), cyber warfare and psychological operations (PSYOPS). The Author contends that while the mercenaries have had some limited tactical success on ground (more so from the Ukrainian side), so far, their role has not had an operational or strategic impact.

Lieutenant General **PR Kumar**, PVSM, AVSM, VSM (Retd) is an alumnus of the National Defence Academy and was commissioned into the Regiment of Artillery on 15 December 1976. The General Officer in his illustrious career spanning 39 years has a very judicious mix of Command, Staff and Instructional Appointments in varied operational environments. He was the DG Army Aviation, before superannuating from the appointment of Director General of Military Operations (DGMO) in end 2015. He continues to write and talk on international and regional geo-political, security and strategic issues.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy oriented in approach.

CLAWS Vision: To establish CLAWS as a leading Think Tank in policy formulation on Land Warfare, National Security and Strategic Issues.

Website: www.claws.in Contact us: landwarfare@gmail.com

Rs 100.00 US $ 5.00

KW KNOWLEDGE WORLD

KW PUBLISHERS PVT LTD

www.kwpub.in