www.dsalert.org | info@dsalert.org

# DEFENCE & SECURITY ALERT

Committed to Defence and Security Worldwide

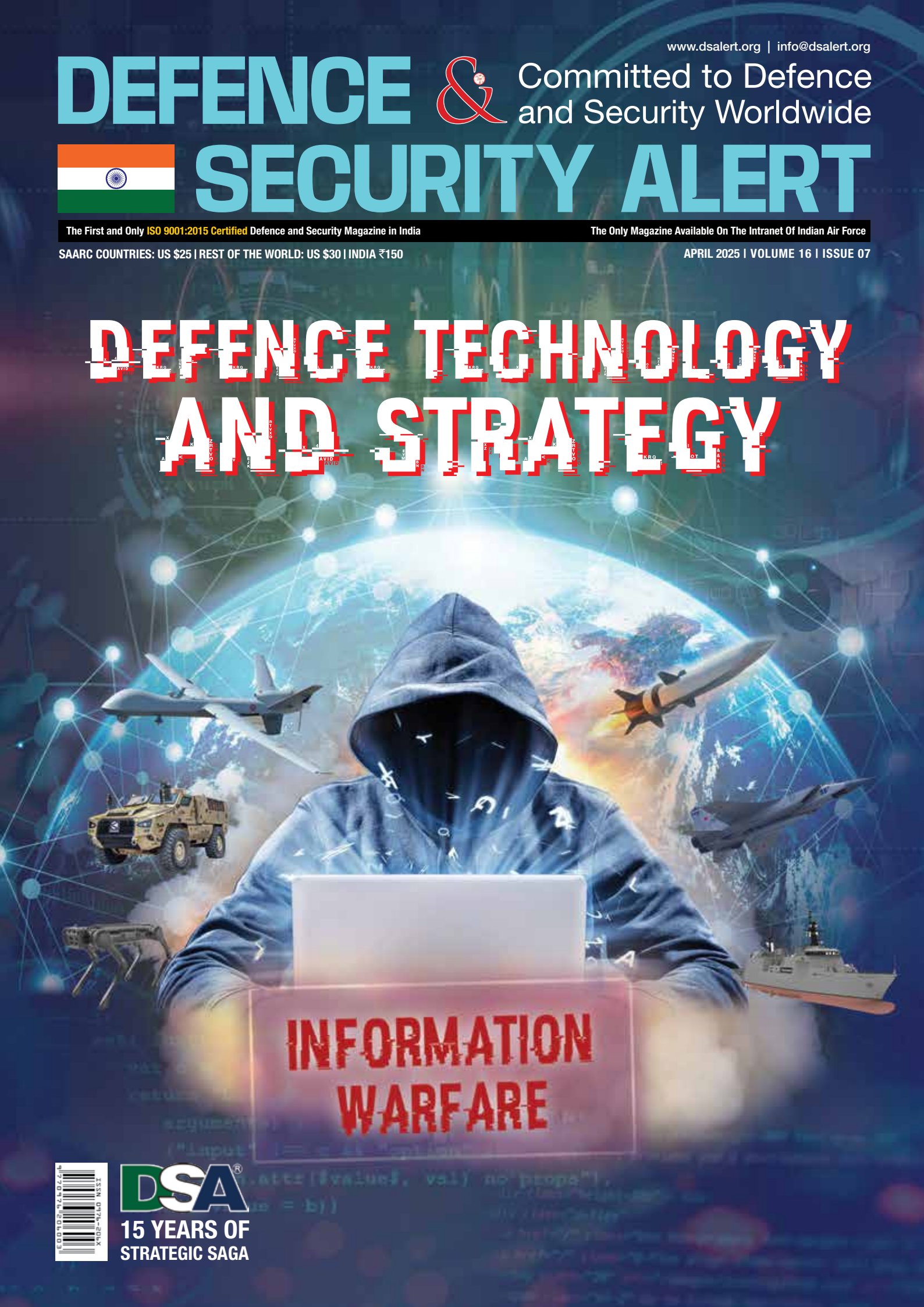
The First and Only ISO 9001:2015 Certified Defence and Security Magazine in India

The Only Magazine Available On The Intranet Of Indian Air Force

SAARC COUNTRIES: US $25 | REST OF THE WORLD: US $30 | INDIA ₹150

APRIL 2025 | VOLUME 16 | ISSUE 07

# DEFENCE TECHNOLOGY AND STRATEGY




DSA®

15 YEARS OF
STRATEGIC SAGA

15 YEARS OF STRATEGIC SAGA

APRIL

# CONTENTS


06 **Leveraging Technology Enhanced Security**
Brig Dr Anil Sharma (Retd.)

14 **Drone: A Knight on the Battlefield**
Colonel Utkarsh Singh Rathore

18 **DeepSeek: A Cursed Boon**
Antonio Delgado
Joel Norris

22 **India's Rise in Jet Engine Manufacturing**
Suman Sharma

30 **India And The Art of Information War**
Marc Cohen

33 **Information Warfare in Modern Military Strategy**
Ashutosh Kumar

38 **Information Warfare: Russia-Ukraine Conflict**
Arjun Singh Dyarakoti
Dr. Siddhardha Kollabathini

44 **Deepfake Warfare: Reinforcing Security**
Ummed Meel

# INFORMATION WARFARE: RUSSIA-UKRAINE CONFLICT

**While Russia may have emerged as a very dominant player in deploying the strategies of information warfare through various means, Ukraine has also adapted to information warfare strategies to counter the Russian narrative and influence public opinion, both at the domestic and international levels.**

**ARJUN SINGH DYARAKOTI**

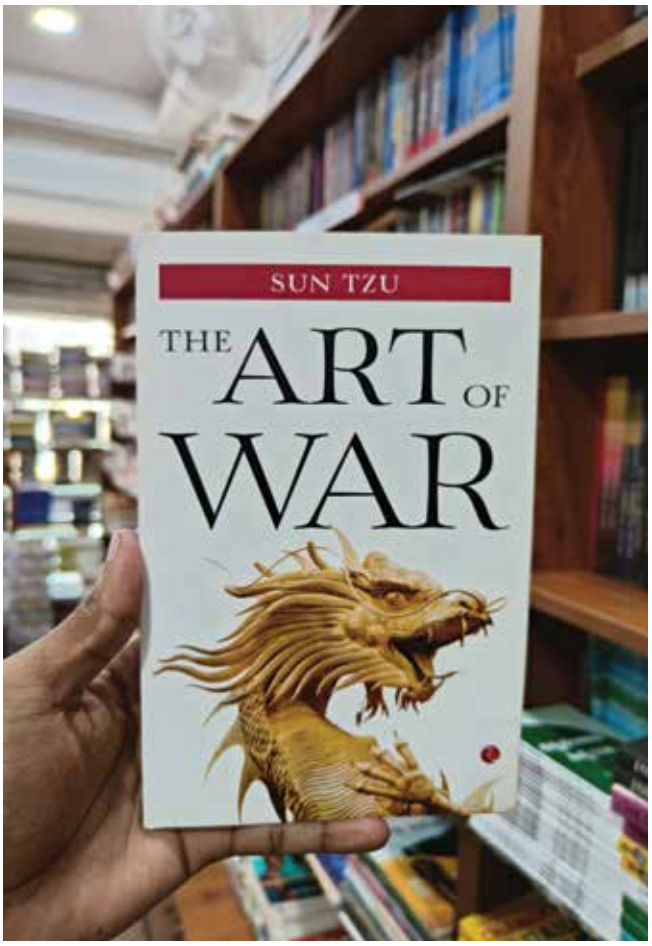
The author is pursuing PhD in International Politics from Central University of Gujarat and simultaneously working as Research Assistant at Rashtriya Raksha University, Gandhinagar.

**DR. SIDDHARDHA KOLLABATHINI**

Author holds a PhD and M Phill from the School of International Studies, Jawaharlal Nehru University (JNU) and currently works as Research Assistant at Rashtriya Raksha University, Gandhinagar.

Information is one of the most significant factors in determining the course of action of an individual or a group of people. The accuracy and the right portion of information received guides the decision-making, which ultimately influences the outcome of the events. Information warfare constitutes the dissemination, exploitation or fabrication of information, misinformation or disinformation during or before the conflict to achieve a winning edge over the adversary by its strategic utilisation. According to a US Air Force's paper titled "Cornerstones of Information Warfare" published in 1997, Information Warfare (IW) has been defined as "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions, and exploiting our own military information functions". Air Marshal Anil Chopra (Retired) has categorised IW in three categories: offencive, defecsive and exploitative, based on how they are employed during warfare. Considering the significance information warfare has come to acquire in modern-day conflicts, Maj Michael Knapp, US Air Force argues, "Success in the information domain is the main contributor to winning (modern) conflicts."

Information has been used as a weapon of war to achieve favourable results by warring parties since ancient times. Sun Tzu's 'Art of War' lays emphasis on the importance of having prior information as a prerequisite for winning the war. In Ramayana, the information gathered by Hanuman and its subsequent utilisation was instrumental in guiding the Vanarsena to fight against the mighty Ravana. Similarly, in Mahabharata when Krishna convinced Yudhisthir to announce the news of the demise of an elephant named Ashwatthama to the Guru Dronacharya to mislead him into believing that it was his son who was dead; this deception




Master the art of strategy with "The Art of War " by Sun Tzu

**Information has been used as a weapon of war to achieve favourable results by warring parties since ancient times**

The Cold War between the US and the Soviet Union which endured for nearly half a century

A majority of Russians regret the fall of the Soviet Union, purporting to miss the unity it brought

and strategic usage of information changed the course of Mahabharata war altogether. In medieval times as well, the deployment of spies to gather actionable intelligence was a prevalent practice in the enemy territory to leverage it against them, particularly in times of conflicts, which continues to be also one of the common practices in modern times as well.

The modern-day information communication-related technologies and various emerging platforms of information propagation have made Information Warfare and its various offshoots even more powerful than ever before. How effectively these data resources are transposed to information resources and used contextually, relevantly and meaningfully can alter the very course and outcomes of war. A classic example in this regard is the Cold War wherein, neither the United States of America (USA) nor the Union of Soviet Socialist Republics (USSR), ever directly confronted the other militarily, yet the former emerged victorious. The strategic use of information as propaganda was one of the various factors that propelled the USA's chances of victory.

As technology advanced, from personal computers to laptops to cell phones, the internet widely became accessible to the public; social media emerged and sophisticated advancements in artificial intelligence are underway. These changes have not only brought about tremendous proliferation in the availability of

information but also in the way it is disseminated and perceived. Both State and Non-State actors exploit this information to achieve their strategic objectives. For example, When Estonia was cyber attacked (one of the means of waging Information warfare) in 2007; these attacks indicated Russia's ability to use information as a tool to influence Estonia's actions to its advantage. The alleged involvement of Russia in meddling in the US election in 2016 also brought to the fore how the strategic usage of information could play a very important role in determining electoral outcomes. India continues to face the two fronts Information Warfare from Pakistan and China, thereby necessitating a strong counter and safeguard mechanism.

The ongoing Russia-Ukraine crisis, which began in 2022 has also witnessed the extensive usage of information as an instrument of warfare by both parties involved to get the strategic leverage in the battlefield and beyond. This included the deployment of not just the conventional means of waging information warfare, but also social media, Artificial Intelligence (AI), usage of bots and deepfakes among other latest technologies. Against this backdrop, this article aims to briefly analyse and examine the different ways in which both Russia and Ukraine have resorted to Information Warfare to get a strategic advantage in the course of the war over one another.

## RUSSIA'S INFORMATION WARFARE

Much of the academic discussion on the ongoing Russian-Ukraine crisis has held that Russian Army General Valery Gerasimov expounded new information warfare operations empowered with Social Media and Artificial Intelligence for Moscow. Russia has taken this strategy forward to prevent Ukraine from joining NATO long before 2014. This was evident in the support given by Russia to the Ukrainian pro-Russian leader Viktor Yanukovych in 2013, wherein social media and broadcast channels played an important role, foiling all the attempts carried out to make a political coup d'etat

**Both State and Non-State actors exploit this information to achieve their strategic objectives**


Estonia Cyberattack 2007

Chief of the General Staff of Russian Armed Forces Valery Gerasimov

a success. Furthermore, Russia's social media and broadcast media projected the narrative of external management of Ukraine by the EU, NATO, the USA and the whole western world. Besides, Russia's social media and broadcast media came with the news that the Heavenly Hundred (people who died during the 2013-2014 Ukraine internal crisis) were killed by the government installed by the mediated European foreign ministers. These narratives were strongly projected by Russia on the grounds of protecting the public order in the aggression regions of Ukraine close to the Russian border, particularly in "Crimea".

All these narratives are carried forward and Russia strengthened its position that Ukraine is to be blamed for the things that happened post-2013 and eventually, cyber attacked Ukrainian critical information infrastructure in early 2022. Subsequently, Russian President Putin appeared on Russia's social media and broadcast media addressing the Russian and Ukranian public that, "Russia will carry out a special military operation in Ukraine to demilitarise and denasify Ukraine" and launched a ground confrontation with Ukraine in 2022. Afterwards, Russian media was successful in projecting Ukraine as an instigator having a stubborn attitude towards joining the EU, particularly NATO, without taking into account the security apprehensions of Russia, thereby leaving the latter with no other option but to launch a special military operation as a preventive security measure against Ukraine.

Although Russia appeared bleak in justifying its cause in its confrontation with Ukraine at the beginning of the Russia-Ukraine conflict in 2022, it eventually nearly succeeded in making its narrative the dominant one. This is evident in the way states in Africa, Asia and South America continents reacted throughout the on-going Russian-Ukraine conflict. For instance, China informed Russia, within 5 months of the start of the Russia-Ukriane crisis, that Beijing is willing to deepen cooperation with Russia. Even though it might appear exaggerated while analysing the above timeline of incidents from the information warfare perspective, however, it remains a fact that many states across the globe are discreetly supportive of Russia in the on-going Russia-Ukraine crisis. Eventually, Russia's information warfare progressed to such a degree that at one critical stage of the crisis the narrative "peace in Ukraine, when it comes, will be on Moscow's terms, those of Russia," prevailed as the most viable logical solution for bringing peace.

## UKRAINE'S INFORMATION WARFARE

While Russia may have emerged as a very dominant player in deploying the strategies of information warfare through various means, Ukraine has also adapted to information warfare strategies to counter the Russian narrative and influence public opinion, both at the domestic and international levels. Following the Euromaidan protests in Ukraine and the Russian annexation of Crimea in 2014, Ukraine has intensified efforts to strengthen the Information Warfare framework. Ukraine Crisis Media Center (UCMC), an NGO founded in 2014, aims to spread


Figurines with computers and smartphones are seen in front of the words "Cyber Attack", binary codes and the Ukrainian flag, in this illustration taken 15 February 2022

information related to events in Ukraine in a manner which promotes Ukraine's national interest and dispels the propaganda against it. The "Stop Fake" initiative was started by Kyiv with the same purpose in 2014 to counter fake news and disinformation. Ukraine has also worked on strengthening its cyber resilience to counter the cyber-attacks from Russia in collaboration with the EU and NATO.

Since the beginning of the recent crisis in 2022, Ukraine has used social media platforms such as Twitter, Instagram and Telegram extensively to counter the Russian narratives, with the Ukrainian President and the officials of his government at the forefront. This includes not only the dissemination of information critical to the on-going conflict, but also the simplest form of humour and memes[2] to boost the morale of soldiers, influence public opinion, ridicule the enemy and combat war fatigue. Hashtag campaigns like #ArmUkraineNow and #StandWithUkraine became very popular in the initial months to garner international support in favour of Ukraine.

The "I Want to Live" campaign launched by Ukraine in September 2023 to provoke and encourage Russian soldiers to surrender had an instrumental role to play in capturing the psychological space of the enemy. The drone footage showcasing Russian soldiers surrendering their weapons and raising their hands has been circulated widely to lure more soldiers to surrender. The Military Intelligence Service of Ukraine also intercepted the phone calls of the Russian soldiers made to their family members. The clippings of these phone calls and similar personal communications are then circulated in social media to influence the enemy's operations in favour of Ukraine.

**Peace in Ukraine, when it comes, will be on Moscow's terms, those of Russia**

Ukraine has also utilised Artificial Intelligence to further its own narratives and counter the ones propagated by Russia. The usage of US-based Clearview's AI by the Ukrainian Army for facial recognition during the conflict is a significant case in point. This software has been used by officials to "detect infiltrators at checkpoints, process citizens


The Standing with Giants team are hopeful that the presence of the 'I want to live' tribute may help promote the amazing work of the charity Ukraine Relief

With Russian full-scale invasion, Ukraine has applied AI on the battlefield, to document the war and to defend itself against Russian cyber and information warfare


Ukrainian Startup Osavul Secures $3M Funding to Combat Disinformation with AI

who lost their IDs, identify and prosecute members of pro-Russia militias and Ukrainian collaborators", thereby utilising the information received as a "secret weapon". Furthermore, Ukraine's "IT Army", which was formed right after the beginning of the war in 2022, has also had various cyber-attacks against the Russian government and its functionaries. This has further been bolstered by the support of various volunteers from around the world. Two Ukraine-based start-ups namely, Osavul and Mantis Analytics, have countered various disinformation campaigns against Ukraine with the help of AI. These above measures undertaken are indicative of the fact that Kyiv has taken up Information Warfare as an important war strategy to neutralise and weaken Russia, even if it may not have been successful in trying to achieve its stated objectives many of the times.

## CONCLUSION

We live in a digital era which is characterised more by information abundance than that of information scarcity. This makes information warfare a lot more sophisticated as a strategy to get the desired output, especially when the widespread access to technologies makes information access way easier. Russia-Ukraine conflict since 2022 has brought the significance of Information Warfare to the forefront, not only in terms of determining material gains but also in building the public perception, support and narrative and ultimately augmenting the winnability in the conflict. Given the various fronts, Information Warfare has come out to be played by both countries during the conflict; it offers immense war lessons in understanding how information warfare can be leveraged to the fullest while riding on the back of modern technology.