How Geo-Strategy, Warfare and War-Tech have Changed in 2022: A Review of Events Which Shaped the New Paradigms of Warcraft

Mr Shaurya Dhakate[@]

Abstract

The year 2022 arrived with fresh opportunities and challenges for the world, transforming the way nations dealt with each other in the process of safeguarding their interests. The article looks back at the year to see how nations behaved in conflicts, what new strategic challenges emerged, and the development of new state of the art war-tech. It attempts to look at the events based on the level of significance they hold pertaining to the change in the global order, including territorial disputes, cyber warfare, war and recent development of war-tech. It concludes with the significant changes in the belief system around the world when it comes to how wars will be fought in the near future. These changes are a result of the paths that nations took in 2022 to gain strategic advantage over their adversaries.

A Categorised Flashback

The year 2022 witnessed most countries in the world starting to move on and trying to forget the losses suffered in the last two years of the Covid pandemic. The global economy suffered a great hit from the circumstances and the it might take years to recover. When the year 2021 came to an end, the pandemic started to wane making way for newer challenges. With the dawn of the new year, fresh opportunities and challenges awaited us, transforming the way nations dealt with each other, in the process of safeguarding their own interests. It is with this background that

[@]**Mr Shaurya Dhakate** is an independent researcher and geopolitical analyst. He holds Pol Sc (Hons) from University of Delhi along with work and writing experience with various defence think tanks. His principal research areas include Disruptive Warfare, Cyberspace, Airpower and Global Diplomacy.

Journal of the United Service Institution of India, Vol. CLII, No. 630, October-December 2022.

the article looks back at the year 2022 to assess how nations behaved in conflicts, what new strategic challenges emerged, and the development of new state of the art war-tech around the world.

To make comprehending the gravity of events easier, the article has colour-coded the events based on the level of their significance towards the changes in the global order. Yellow stands for territorial disputes not escalating to use of arms and the use of 'lawfare'. Orange signifies use of cyber warfare and hacktivism. Red, being a well-accepted code for danger, denotes use of firepower and skirmishes escalating to war and recent development of war-tech. To that end, the ensuing paragraphs will address every significant international event that has changed the meaning of the word we know as 'War'.

Red: Battles of Belonging and Modernisation of Arms

Use of firepower. The month of February 2022 saw one of the biggest wars and significant human rights violations in Europe when Russia invaded parts of Ukraine beginning with massive fly-bys by fighters and bombers in Ukraine's cities and marching-in of tanks and BMPs from across the IB. The war has affected many countries adversely and has left a dent on the global economy in various sectors. The war in Ukraine was not the only use of arms that 2022 saw. In January 2022, a Saudi led coalition undertook air strikes in Yemen in response to the Houthis attack on the UAE. The attack employed precision guided munitions which were developed in the United States (US). One of the weapons used by the Houthi rebels was the Burkan-3. With the increase in flow of arms for non-international armed conflicts, advanced weapon systems have significantly grown in the inventories of various rebel and militant groups in recent years.

Much later, in August, with the visit of the US House of Representative's Speaker Nancy Pelosi to Taiwan, the People's Republic of China (PRC) demonstrated aggressive behaviour and military posturing in the high seas. Following Pelosi's visit, the Taiwan strait saw quick upsurge of tensions arising out of insecurity amongst the Chinese. "The Chinese leadership now believes that Washington is using Taiwan as a strategic asset to contain the mainland within the first island chain in the Western Pacific. In this context, Beijing has opted to use military means short of war—

such as live-fire exercises off the coast—to deter independence and to potentially prepare for non-peaceful reunification. The mainland has also used diplomatic, economic, and other tools to exert pressure—for example, by poaching Taiwan's diplomatic allies, conducting cyber-attacks against the government, detaining Taiwanese politicians and activists, and imposing embargo on Taiwanese products".[1]

Going back to February, the Russian invasion gave us amazing insights on what motivates leaders to take difficult steps when their national interests are threatened and what potential shapes modern territorial conflicts may take when things get chaotic. The present scenario of the war is what geo-political and international relations theorists call the '*spiral model'*, in which the parties to a conflict treat each other with equal hostility. These types of escalatory spirals can become very dangerous even though there's no nuclear war. Till June, the Russian forces did not succeed in achieving full air dominance in the region; it lost what is believed to be more than 160 aircrafts which accounted for about 10 percent of its fleet. In the third phase of the war, the Kharkiv Region saw counter offensives by the Ukrainian side. Earlier, Ukraine's use of arms and airpower was mostly defensive. The nation in the first two quarters of the year, was defending for survival whereas now it's fighting for survival and the struggle doesn't seem to stop in the near future. With Russian withdrawal from Kherson and its occupation by Ukrainian forces, the conflict is taking mysterious proportions.

Developments in arms and war-tech. The year saw birth and evolution of many arms and technologies. There is a race for introduction of newer weapons amongst countries, with plans to upgrade their airpower by modernising their equipment, in preparation for potential conflicts.

- North Korea in January tested a rail borne ICBM. "The missiles fired from rail cars appeared to be a solid-fuel short-range weapon, the North has apparently modelled after Russia's Iskander mobile ballistic system".[2]

- Tu-160M 'White Swan' strategic bomber was unveiled by Russia. The strategic importance of this addition is huge to the country keeping in mind its recent confrontations and for any possible conflict with NATO forces in the future.

- Israel's C-Dome defence system is the naval variant of the Iron Dome Air defence system, which is an all-weather system, used to intercept and destroy short range rockets and missiles.

- Launch of NROL-85 US Reconnaissance Satellites by Space-X was conducted in April 2022. "NRO Launch 85 (NROL-85) is the fourth dedicated Falcon 9 mission that SpaceX will carry out for the National Reconnaissance Office (NRO)".[3]

- German KF-51 Panther Main battle tank was unveiled in 2022; the 'Panther' is a lethal, highly protected, and fully digitised piece of equipment.

- BAS-750 Unmanned Helicopter is developed by Russian company Rostec. It can do long range communications and has capability to carry heavy payloads while flying for long distance and long duration.

- Autonomous Flying Wing Technology Demonstrator is developed by the DRDO, and flew its maiden flight in July 2022. It is India's new indigenously developed UCAV. It operated in full autonomous mode and was a stepping stone for the fully autonomous aircraft to be built in the future.

Orange: From Fire-power to Wire-power

We may recall that in the initial months of the year, a novel virus, this time a software virus and not a biological one, was gaining popularity. The Pegasus spyware, of Israeli origin, was said to be infiltrating into IT devices of politicians, military personnel and journalists, posing a privacy breach as well as a risk of leak of official secrets and confidential information concerning national security. In late January, the Global cyber security outlook released by the world economic forum stated that ransomware attacks increased by 151 percent, making cyber space an even more dangerous place to be in, not only for the netizens but also for the governments. Later, in February after the war began in Europe, the hacktivist group '*Anonymous*' declared a cyber-war against Russia and targeted its various e-assets and digital infrastructure.

After 1991, the global conflict underwent a metamorphosis and hibernated under the layers of software and algorithms. Since

then, the world has been exposed to the nefarious threat to international and psychological peace - cyber threats. Internet was born in 1983, only to see the first virus in 1986, just three years after its birth. The jump in technological advancement is infinite with no zenith of sophistication. It is never certain what kind of technology would be developed to eclipse its predecessor, but it is always certain that a counter-tech will emerge to give the former one a death blow. Unregulated money transfers, digital currency transfers, and data transfers concocted opaque corridors made of algorithmic cement to ensure concealed conduct of capital during conflicts.

In December 2021, there was a breach of security of four US Defence and Security firms by a Chinese hacker group in order to intercept sensitive and classified communications. In March 2022, "Hackers linked to the Chinese Government penetrated the networks belonging to government agencies of at least 6 different US states in an espionage operation. Hackers took advantage of the *Log4j* vulnerability to access the networks in addition to several other vulnerable internet-facing web applications".[4]

In April 2022, Chinese hacker group targeted about seven power grids in north India, similar to other past attacks which targeted critical infrastructure and sectors like defence and space. "US based cyber threat intelligence company, Recorded Future, released a report saying it had found evidence that at least seven Indian State Load Dispatch Centres (SLDCs) and an Indian subsidiary of a multinational logistics company were targeted by a China-linked group that it has codenamed TAG-38".[5]

"If it were measured as a country, then cybercrime — which is predicted to inflict damages totalling $6 trillion USD globally in 2021 — would be the world's third-largest economy after the US and China. Cybersecurity Ventures expect global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined".[6]

Cyber espionage is the most widely used and quotidian variant of this group of pathogens. Nations always wanted to eavesdrop on adversary's policy making portals; this is the way it's done now. This often involved using botnets and spear phishing to target systems. These are very similar to the MITM or 'Man in The Middle' attacks. Spear phishing can be distinguished from regular phishing as the former targets an individual whereas the latter uses a broad strokes approach, often through emails and apps. When heads of governments or important organisations are targeted, it is referred to as 'Whale-Phishing'. "A Russian organised cybercrime group, Fancy Bear, targeted Ukrainian rocket forces and artillery between 2014 and 2016. The malware was spread via an infected android application used by the D-30 Howitzer artillery unit to manage targeting data. Ukrainian officers made wide use of the app which contained the X-Agent spyware. This is considered to be a highly successful attack, resulting in the destruction of over 80 percent of Ukraine's D-30 Howitzers".[7]

When such penetration techniques aim to bring down certain electronic infrastructure or equipment, they are called Cyber Sabotage. Siblings of it are the Denial of Service (DoS) attack and the Distributed Denial of Service (DDoS) attack, which can not only cause disruptions in a system but can block others from operating it. A very notorious example of this is the Stuxnet virus. "Stuxnet was a worm that attacked the Iranian nuclear program. It is among the most sophisticated cyber-attacks in history. The malware spread via infected Universal Serial Bus devices and targeted data acquisition and supervisory control systems. According to most reports, the attack seriously damaged Iran's ability to manufacture nuclear weapons".[8] The end manifestation of this attack is a kinetic energy damage.

Another species is the Structured Query Language (SQL) Injection attack. "SQL is the code used to communicate with a database. In an SQL injection attack, the hacker writes vindictive SQL code and inserts it into a victim's database, in order to access private information".[9]

These virtual attacks on people, groups, society, nation, or humanity as a whole can actually be placed in 'red' category as they possess the power to control the use of nuclear weapons/ energy and cause disruptions in air, maritime and space domains

at any point of time. But neither are these capabilities visible nor have they been employed in large scale as yet and the year has only seen such capabilities being used either as a trial or to satisfy geo-political and activist agendas.

Yellow: Geo-political Tussles and Lawfare

This part of the analysis explores various issues that emerged during the year pertaining to territorial disputes, maritime conflicts, boundary issues and most importantly Lawfare.

People's Liberation Army (PLA) at the Borders and High Seas. India faced challenges arising out of boundary disputes with China and its increasing presence in the Indian Ocean Region (IOR), which it is aiming to strengthen by doing bilateral pacts with nations in the IOR. In January, it was reported that China was building a strategically important bridge at the Pangong Tso Lake. The site of construction was approximately 20 km from Finger-8 of the lake and it is east of the Khurnak Fort. The bridge is at the narrowest part of the lake and connects the two sides, which, when completed, will make crossing of tanks and armoured vehicles of PLA easier and faster. This move came out of the standoff that began in May 2020 and in retaliation to Indian Army occupying the heights of the Kailash Range in the Chushul Sub-sector on the southern banks of the lake. This move gave Indian Army a clear view of China's Moldo Garrison (military base).

In April, China signed a strategic pact with the Solomon Islands which evoked protests from Australia and the US. "The relationship between the world's most populous country and this Pacific archipelago of 700,000 people was thrust into the spotlight this year when word leaked that they had struck a secret security agreement. The United States and its allies fear the pact could pave the way for the establishment of a Chinese military base in the strategically valuable island chain".[10] Further, the presence of the Chinese surveillance ship at Hambantota, despite diplomatic protests from the Indian Government, is an indication of the Chinese influence in our littoral neighbourhood.

The Nord Stream 2 pipelines. It has been in the news a lot in 2022. The 1,234 km long natural gas pipeline runs from Russia to Germany through Baltic Sea. There were several warnings issued by Moscow to Berlin of stopping the pipeline to warn it of the

increasing interference in Russian operations in Ukraine. Towards the end of September, authorities of Sweden and Denmark said that there were a number of explosions at pipe A of Nord stream 2 and pipe A and B of the Nord Stream 1 pipeline, which caused significant gas leaks. “The European Union considers the incident to be intentional sabotage”.[11]

In the geo-political and geo-strategic parlance, the F-16 fleet sustenance package deal between the US and Pakistan might be a move to rescind the Trump-era ban to extend aid and indulge in arms deal with Pakistan, but it brings challenges for both the parties in the global arena. New Delhi is pressurising Washington to reconsider its plan to go ahead with the US $450 million deal as it might give Pakistan an upper hand in any future aerial combat with India, especially in case India has a two-front war with China and Pakistan. Pakistan Air Forces’ Falcons are already a good match for IAF’s fleet, which they now seek to upgrade and extend the life through a sustenance package, adding punch to versatile and potent machine. The past deals and the future ones involve advanced targeting pods and electronic warfare pods, which might not be necessary to fight the terrorist groups in the subcontinent as no group has in their possession a 4+ generation fighter which fights with electronic warfare.

Today, using law as a weapon for achieving ulterior motives is no doubt a cunning move. Many nations are relying on using loopholes in international laws to stop the developing and underdeveloped nations from growing their economies and militaries.

China likes to follow the old playbooks and stringently follows the Sun Tzu maxim that ‘*defeating the enemy without fighting is the pinnacle of excellence’*. The PRC uses law as an instrument to destroy its adversaries, which increased significantly in 2022. It used it belligerently in the South China Sea through which almost one-third of the world’s maritime trade passes. Xi’s increasing lawfare has been receiving very minimal global outrage, even after many nations are aware of its passive impact. Another example is US’s Countering America’s Adversaries Through Sanctions Act (CAATSA), which is a federal law and through which Washington DC can impose sanctions on any country which has ‘significant transactions with Iran, North Korea or Russia’. It has come to limelight after the Ukraine war, and when the US warned

India that it'll impose sanctions on it for purchasing Russia's S-400 surface to air missile system. However, CAATSA waiver in the case of India was approved by the US House of Reps on 14 Jul 2022.

Conclusion

There have been significant changes in the belief system around the world when it comes to how wars will be fought in the near future. These changes are a result of the paths that nations took this year to gain strategic advantage over their adversaries. The heavy use of fire arms in the Russo-Ukraine war made the world apprehensive that if the conflict escalates to a world war, would the nuclear-powered nations be compelled to launch their nuclear arsenals. In the first quarter of the year, when talks and diplomatic efforts failed to stop the war in Ukraine, the hope of peaceful resolution of disputes slowly started vanishing and with increased deployment and use of firearms in other parts of the world, it completely disappeared. The year saw recurrent firing of ICBMs by North Korea, airstrikes in Yemen, violation of international laws by China over the airspace and maritime domain of Taiwan with continued geo-political and strategic issues in Europe over the Ukraine war.

The cyber space is another war zone which lit up this year. The fact that it did not come into the limelight a lot is because it does not have direct consequences on the lives of people. Manipulating this, the PRC targeted various high value infrastructures in India and abroad. If these attacks were not stopped at the right time, they would've been in the news for a longer time and the trajectory the events of this year took would have been different.

Tomorrow's wars will involve some of the greatest technology that man has developed so far, since the greatest inventions of humankind were born during conflicts. When countries strive for their survival, the best minds and the best resources are coupled together to bring new weapons and their counter-shields to the world, be it physical or virtual.

A lesson that remains with us after this analysis is that in the coming decades, waiting for slow build-up of conflict may not happen and that conflicts could erupt after certain redlines are

breached. We have seen Russia getting insecure of losing its 'buffer zone', which separates it from direct contact with NATO, and China going berserk after Nancy Pelosi's visit to Taiwan.

Another lesson that emerges from the Russo-Ukraine conflict is that nations have to fight their wars on their own, with, maybe,some external support from its allies or those who have a direct involvement in giving a certain direction to the conflict. A final lesson that emerges is that nuclear sabre rattling will not go down well with any nation, including iron-clad allies and the world in general abhors those who threaten nuclear attacks. A nation which uses even the low-yield TNWs, is likely to become a pariah in the world. Only conventional kinetic and non-kinetic power may be acceptable in warfare.

"El poder es unacombinacion de todosloselementos de unaestructura, la debilidadencualquier element puede conducer al colapso total de la structura"
(Power is a combination of all elements of a structure, weakness in any one element can lead to total collapse of the structure).

Endnotes

[1] Paul Haenle, Nathaniel Sher, How Pelosi's Taiwan Visit Has Set a New Status Quo for U.S-China Tensions, August 17 2022, Carnegie Endowment for International Peace.

[2] "North Korea says it test launched missiles from train", the Hindu, January 15, 2022.

[3] William Graham, Falcon 9 launches NROL-85 mission for National Reconnaissance Office, April 17 2022, NASAspaceflight.com

[4] Centre for Strategic and International Studies, Significant Cyber attacks since 2006, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents, accessed on 03.05.2022.

[5] Binayak Dasgupta, Hindustan Times, "Chinese hackers targeted 7 Indian power hubs, govt says ops failed", April 08 2022. Accessed on 03 04 2022.

[6] Steve Morgan in Cybercrime To Cost The World $10.5 Trillion Annually By 2025, November 13 2020, cybersecurityventures.com, accessed on May 06 2022.

[7] "Cyber warfare", Imperva, https://www.imperva.com/learn/application-security/cyber-warfare/ , accessed on May 14, 2022.

[8] "Cyber warfare", Imperva, https://www.imperva.com/learn/application-security/cyber-warfare/, accessed on May 14, 2022.

[9] Carmen Ang, The Most Significant Cyber Attacks from 2006-2020, by Country, May 10 2021, Visualcapitalist.com accessed on May 14, 2022.

[10] Michael E. Miller, "China's growing reach is transforming a Pacific island chain", August 11, 2022, The Washington post.

[11] "Nord Stream leaks: Sabotage to blame, says EU". BBC News. 28 September 2022. Accessed on 29 September 2022.