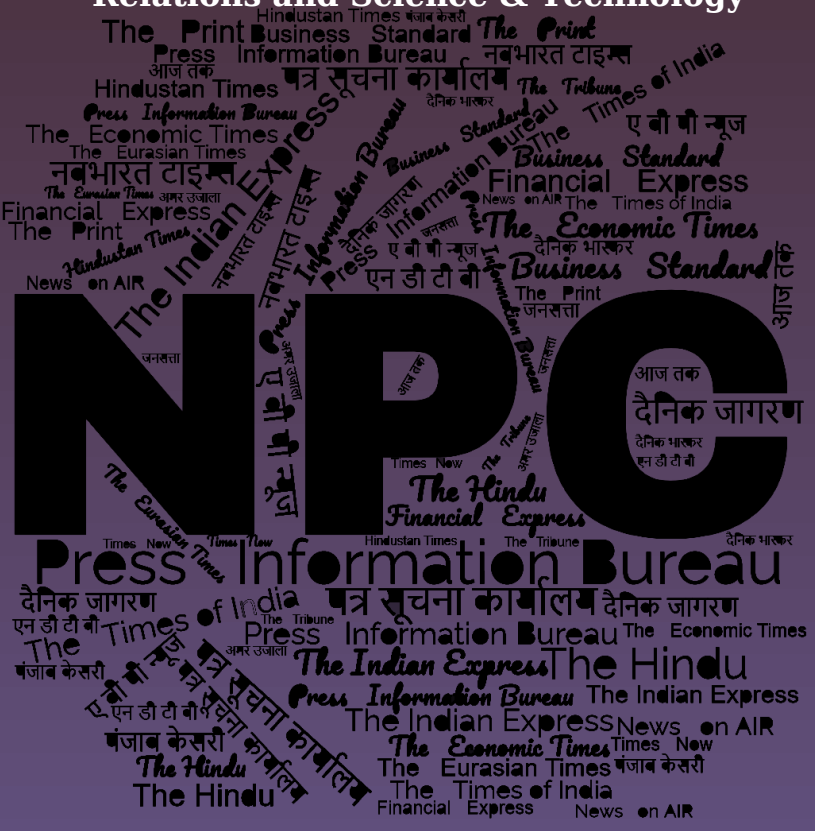
जुलाई
July
2023

खंड/Vol. : 48 अंक/Issue : 139
25/07/2023

समाचार पत्रों से चयित अंश
Newspapers Clippings

डीआरडीओ समुदाय को डीआरडीओ प्रौद्योगिकियों, रक्षा प्रौद्योगिकियों, रक्षा नीतियों, अंतर्राष्ट्रीय संबंधों और विज्ञान एवं प्रौद्योगिकी की नूतन जानकारी से अवगत कराने हेतु दैनिक सेवा

A Daily service to keep DRDO Fraternity abreast with DRDO Technologies, Defence Technologies, Defence Policies, International Relations and Science & Technology



रक्षा विज्ञान पुस्तकालय
Defence Science Library
रक्षा वैज्ञानिक सूचना एवं प्रलेखन केंद्र
Defence Scientific Information & Documentation Centre
मेटकॉफ हाउस, दिल्ली - 110 054
Metcalfe House, Delhi - 110 054

CONTENTS

DRDO News

DRDO Technology News

REPUBLICWORLD.COM

Mon, 24 Jul 2023

Unveiling India's Directed Energy Weapons: A Game-Changing Military Technology

India's Air Chief Marshal Vivek Ram Chaudhuri recently sparked curiosity and excitement within the defence community when he mentioned the successful tests and deployment of Directed Energy Weapons (DEWs) and hypersonic weapons during a public event in Delhi. Although he later clarified that these weapons were tested by various countries. However, according to Colonel (Retd) D.R. Semwal, DEWs are indeed part of India's security infrastructure. DEWs, which use concentrated laser, microwave, or particle beams to strike targets with lethal force, offer unmatched accuracy, low cost per shot, and lightning-fast attacks. Such weapons seem to be the key to neutralizing the challenge posed by virtually 'unstoppable' hypersonic missiles, Air Vice Marshal (Retd) BM Tyagi said. Meanwhile, the secretive nature of India's DEW program raises intrigue and highlights the country's focus on cutting-edge military technology.

While India has not officially declared the existence of DEWs within its arsenal, various tests conducted by the Defence Research and Development Organization confirm their presence in the country's security architecture. Notably, India's DEW development efforts date back to at least the early 2000s. The Laser Science and Technology Centre (LASTEC), a Delhi-based DRDO lab, achieved a full-scale technology demonstration of DEWs at the Hindon Air Base near Delhi in 2001. This demonstration reportedly impressed the country's top leadership and showcased the potential of these advanced weapon systems.

Veiled in Secrecy: KALI and DURGA projects

According to various defence experts, development and research for these advanced weapon systems have been ongoing for decades, with several defence organizations like DRDO, CHESS, BARC, and ADB contributing to their success. One area where India's DEW technology has been publicly mentioned is in the development of anti-drone systems. These systems are designed to detect and neutralize hostile drones, either by disrupting their communication signals or physically disabling them with laser beams.

Meanwhile, classified defence programs KALI and DURGA have been at the forefront of people’s imagination when it comes to Directed Energy Weapons under development in India. However, as per the information available on public domain, the Kilo Ampere Linear Injector (KALI) is supposedly a high-power electron accelerator project developed by the DRDO. It is believed to be designed to generate a high-intensity electron beam to be used for various applications, including directed energy weapons research. The project was initiated in the early 1980s with the primary objective being to explore its potential for directed energy weapons and advanced scientific research.

Directionally Unrestricted Ray-Gun Array or DURGA on the other hand, is another directed energy weapon development program led by the DRDO. Like KALI, information on DURGA is also kept limited to the public due to its status as a classified project. However, the name "DURGA" suggests that the program involves the development of a powerful ray-gun array, implying that it is focused on directed energy weapons technology.

DEWs worldwide and India's competition

India's progress in DEWs is parallel to other major powers' efforts, like China and Russia. China boasts multiple ground-based laser weapons and microwave systems, while Russia's 'Peresvet' and 'Zadira' demonstrate their commitment to advanced laser technologies. The US remains a global leader in DEW research, with plans to increase power levels and deployment in the coming years.

As India continues its research and development of DEWs, the technology will play a significant role in the military capabilities of the future. While the secrecy surrounding these advancements fuels curiosity, it also signifies India's commitment to maintaining its edge in the ever-evolving realm of military technology. As the nation continues its journey into the unknown, DEWs remain a pivotal element in safeguarding India's security and interests.

https://www.republicworld.com/india-news/general-news/unveiling-indias-directed-energy-weapons-a-game-changing-military-technology-articleshow.html

THE HINDU

Mon, 24 Jul 2023

Training Programme for DRDO, INAS Personnel Begins at IIM-Visakhapatnam

A training programme for Defence Research and Development Organisation (DRDO) scientists and Indian Naval Air Squadrons (INAS) officers was inaugurated on the campus of Indian Institute of Management-Visakhapatnam here on Monday.

The 16 DRDO scientists started their five-day capacity building programme on project uncertainty and risk management whereas the 10 INAS officers started their six-day training programme.

DRDO former director general K.S. Varaprasad attended the event as chief guest. He emphasised the importance of gaining managerial skills as one grows in the organisation. He stressed the significance of project management in the timely delivery of projects. He also highlighted the need to multiply human resources by networking with different organisations; better participation of academic institutes; and engaging students in development activities for efficient execution of projects.

He also noted that AI and autonomous machines are going to play a significant role in the future and underscored the significance of proper technology forecast and the need to invent disruptive technologies.

https://www.thehindu.com/news/cities/Visakhapatnam/training-programme-for-drdo-inas-personnel-begins-at-iim-visakhapatnam/article67116259.ece

FINANCIAL EXPRESS
Read to Lead

Mon, 24 Jul 2023

Over 30,000 Defence Items by DPSUs on Srijan Portal Offered to the Industry Including MSMEs for Indigenisation: MoS Defence Ajay Bhatt

More than 30,000 defence items by defence public sector units (DPSUs) and services on the Srijan portal have been offered to the industry including MSMEs to become partners in the indigenisation process, said Ajay Bhatt, Minister of State in the Defence Ministry in a written reply to a question in the Lok Sabha. The value of defence production crossed Rs 1 lakh crore for the first time ever during FY23, the minister informed.

To promote the participation of MSMEs and startups in the development of defence technology, the government offers schemes such as Innovations for Defence Excellence (iDEX), Technology Development Fund (TDF), and Make procedure under Defence Acquisition Procedure (DAP) 2020.

“The DAP 2020 provides special provisions to encourage MSMEs and startups. Moreover, Public Procurement Policy for MSEs Order, 2012 has been implemented at DPSUs under which the price preference is given to MSME bidders under certain conditions,” said Bhatt.

The Minister stated the government’s role in promoting local defence manufacturing and innovation by initiatives such as Innovations for Defence Excellence (iDEX), Technology Development Fund (TDF), and procedure of procurement under Defence Acquisition Procedure (DAP) 2020.

Further, Innovations for Defence Excellence (iDEX) — an initiative by the Defence Ministry — was launched in April 2018 to foster innovation and technology development in Defence and Aerospace by engaging Industries including MSMEs and startups. iDEX offers funding and other support for research and development activities.

So far, iDEX has connected 3 ministries, 16 DPSUs, and 19 incubators, with over 6800 applicants for the positions, as per the iDEX dashboard.

“Moreover, the Public Procurement Policy for MSEs Order, 2012, was implemented at the defence public sector units, or DPSUs, under which the price preference is given to MSME bidders under certain conditions,” Bhatt said in the Parliament.

The Ministry of Defence, which is among the largest buyers of products from MSMEs, nearly doubled its online procurement of goods and services from MSMEs and other sellers in the financial year 2022-23 from the previous fiscal via the Government e-Marketplace (GeM)

marketplace. The ministry made purchases worth Rs 28,732.9 crore in FY23, up by 90.4 per cent from Rs 15,090.8 crore worth of goods and services bought in FY22, according to GeM data.

https://www.financialexpress.com/industry/sme/msme-over-30000-defence-items-by-dpsus-on-srijan-portal-offered-to-the-industry-including-msmes-for-indigenisation-mos-defence-ajay-bhatt/3184162/

Hindustan Times

Mon, 24 Jul 2023

IAF Base in Prayagraj to be Hub for Transport Aircraft C295 Spares

An Indian Air Force (IAF) base in Prayagraj will be the spares hub for the its latest C295 transport aircraft, which is at the heart of a key Make in India programme, a defence ministry statement said on Monday. The 24 Equipment Depot, Air Force Station, Manauri in Prayagraj has been designated as the central stock holding depot for C295 spares.

Air Commodore Angshuk Pal, who is commanding the air force station, on Monday inaugurated the exclusive warehousing facility for C-295 assemblies and parts.

In September 2021, the defence ministry signed a ₹21,935-crore project with Airbus Defence and Space to equip the IAF with 56 C295 aircraft to boost self-reliance in the defence manufacturing sector. Tata Advanced Systems Limited and Airbus are jointly executing the programme.

The aircraft was ordered as a replacement for the IAF's fleet of ageing Avro-748 planes that entered service in the early 1960s. The first 16 C295 aircraft will be delivered to the IAF by Airbus in flyaway condition from Spain, and the remaining 40 will be assembled in India. The first plane is set to be delivered to the IAF in September followed by the second one in May 2024.

All 16 flyaway aircraft will be delivered between September 2023 and August 2025, while the first Made in India C295 will roll out of the Vadodara facility in September 2026 and the remaining 39 by August 2031,

In October 2022, Prime Minister Narendra Modi laid the foundation stone of the manufacturing facility being set up by the Tata-Airbus combine at Vadodara. The C295 will be the first military aircraft to be manufactured in India by a private consortium.

https://www.hindustantimes.com/india-news/indian-air-force-base-in-prayagraj-designated-as-spares-hub-for-c295-aircraft-in-make-in-india-programme-101690214474808.html

NEWS18

Mon, 24 Jul 2023

From Combat Management to Military-Grade Security, How WESEE Powers Navy's Aatmanirbharta

From its modest beginnings with Project-16 frigates, WESEE (Weapons and Electronic Systems Engineering Establishment), previously known as WESO, has now emerged as a formidable force overseeing Combat Systems Integration across the Indian Navy's diverse platforms.

Established in 1978, WESEE has played a crucial role in successfully integrating a wide range of weapons and electronic systems into various naval vessels, submarines, aircraft, and aircraft carriers, making it an indispensable backbone of the Navy's quest for self-reliance (Aatmanirbharta).

WESEE's Management Board is chaired by the Secretary of the Department of Defence (R&D) and comprises senior functionaries from DRDO, MoD, MoD(Finance), the Chief of Materiel (COM) of the Indian Navy, and the Director General of WESEE. Projects are assigned to WESEE by the Naval Headquarters through a second-tier committee called the Programme Management Committee, which includes representatives from directorates of Naval Headquarters, DRDO, MoD, and MoD (Finance).

A Navy Commander highlighted the critical role of WESEE, stating, "Despite having a diverse arsenal of weapons and systems from friendly nations, relying on them for integration into our naval platforms is not a viable option. Sharing sensitive data about our platforms raises concerns that cannot be ignored. This is where an organization like WESEE becomes indispensable. Their team of experts handles local integration, ensuring that our sovereignty and security remain intact. WESEE empowers us to maintain self-reliance and safeguard our nation's interests."

INCEPTION AND MILESTONES

WESO's primary objective was to create a group of system engineers capable of integrating the diverse range of equipment on board ships. With just 20 naval officers, scientists, and staff, the organisation began operating from a rented house in Safdarjung Enclave before moving to 'Metcalfe House' in Civil Lines, New Delhi.

The successful integration of systems on the Godavari class ship laid the foundation for a permanent systems integration establishment, and on 31 May 1985, WESEE was officially established as the successor to WESO.

WESEE's notable achievements include System Integration of Project-16A (Brahmaputra class), Project-15 (Delhi class), Project-25A (Kora class), and Project-1241RE (Veer class) ships, along with the development of the Modular Data Bus (MDB) and the Modular Interface for Ship-borne Systems (MISS boxes). The IT&IW Group within WESEE conceptualized, designed, and deployed an indigenous encryption system for Secure Email, which is still in use today. Additionally, their Combat Management System (CMS) assists officers on warships in making decisions based on integrated inputs.

A NERVE CENTRE ONBOARD WARSHIPS

The Combat Management System by WESEE acts as the nerve centre on board warships by integrating all sensors such as radars, sonars, EW systems and AIS, with weapons like guns, missiles, torpedoes and rockets.

It can also exchange information with other platforms via the ship's Data Link equipment. The CMS has evolved over the years, transitioning from CAIO systems to Commercial-Off-the-Shelf (COTS) high-performance hardware and operating systems, ensuring strategic independence and reliability.

Making decisions lies entirely with the officers, but with CMS, they now have a technologically backed system that aids them in reviewing and determining the optimal use of weapons or systems for superior outcomes, explains the officer. "Here at WESEE, our role revolves around seamless data integration, ensuring a robust system to receive, employ, analyse, and transmit data as per the need of the hour."

CYBER SECURITY ADVANCEMENTS

WESEE has been at the forefront of securing the digital space for the Indian Maritime force. Apart from developing security suites and solutions for force systems, WESEE ventured into the uncharted quantum domain to address emerging challenges. They established a state-of-the-art Quantum Communications Lab in 2020, and within the same year, achieved a significant milestone by developing the first-ever Quantum Safe Algorithm, primed for prototype testing. Other groundbreaking solutions from WESEE include the Linkryptor — a customised hardware for secure Tactical Communication, and a Cross Domain Solution enabling secure information exchange between networks of different trust levels.

LOOKING TOWARDS THE FUTURE

While WESEE has been instrumental in making the Navy self-reliant and future-ready, it is now considered the gateway of technology in the Indian Navy. As the Navy enjoys a strategically relevant position as a 'Preferred Security Partner in the IOR', its technological dominance among the three Services is a key factor. However, challenges such as the proliferation of powerful and affordable technologies and disruptive innovations threaten this status. WESEE's mission is to push the boundaries in 'Disruptive and Transformational Technology' domains, paving the way for excellence and innovation within the fleet.

"WESEE has established itself as the beacon of excellence and a source of innovative ideas and products that enabled the fleet both to grow and operate optimally. WESEE's endeavour now is to pursue and push the technology frontiers in 'Disruptive and Transformational Technology' domains," said a Captain rank officer from WESEE.

https://www.news18.com/india/from-combat-management-to-military-grade-security-how-wesee-powers-navys-aatmanirbharta-8408443.html

THE ECONOMIC TIMES

Mon, 24 Jul 2023

Gravity of Cyber Risks will Increase with Disruptive Technologies such as Artificial Intelligence: NSA Ajit Doval at BRICS Meet

National Security Advisor Ajit Doval participated in the 'Friends of BRICS' meeting in Johannesburg in South Africa on Monday.

Apart from BRICS, the following Friends of BRICS countries - Belarus, Burundi, Iran, UAE, Saudi Arabia, Egypt, Kazakhstan and Cuba - also participated in the meeting.

Sources said the issue of cybersecurity was discussed at length in the meeting.

They said NSA Doval highlighted that the gravity of cyber risks will increase exponentially with the advent of disruptive technologies such as Artificial Intelligence, Big Data and Internet of Things.

He also highlighted the linkages between cyber criminals and terrorists including the use of cyber space for financing, money laundering, radicalizing, lone wolf attacks, recruitment and secured communications, the sources said. The NSA, the sources said, noted that younger populations were particularly susceptible to the spread of extremist ideologies through the use of social media sites because they are technology savvy and have impressionable minds.

They said Doval highlighted the need for collective efforts to deal with challenges emanating from cybersecurity.

He said the Global South in particular needed to overcome limitations of resources. In this endeavour, India will always remain at the forefront, working closely with the Global South, Doval said, according to sources.

They said NSA also held several bilaterals with his counterparts from BRICS and Friends of BRICS countries.

https://economictimes.indiatimes.com/news/defence/gravity-of-cyber-risks-will-increase-with-disruptive-technologies-such-as-artificial-intelligence-nsa-ajit-doval-at-brics-meet/articleshow/102088025.cms

REPUBLICWORLD.COM

Mon, 24 Jul 2023

5 Lessons from Ukraine Conflict: The Evolution of Aerial Warfare and India's Preparedness

By Yuvraj Tyagi

In the wake of the conflict in Ukraine, critical shortcomings in planning, perceptions, weapon systems, and tactics related to peer-to-peer aerial warfare have been exposed. These challenges can largely be attributed to the world's predominant focus on asymmetric warfare, leading to surprises for both Ukraine and Russia as they encountered unique technological advances in the conflict.

Shortly after the announcement of President Putin's 'Special Military Operation' against Ukraine in February 2022, both Ukraine and Russia felt the brunt of shortcomings in defence against technologically advanced weapons. Notably, in asymmetric warfare, only the dominant military force advances on the battlefield, specifically in technology. However, in a peer-to-peer conflict, "both sides have the liberty to do so", Colonel Sant Pal told Republic. Meanwhile, some lessons from the war between Russia and Ukraine validate the concepts that the Indian Air Force has already adopted.

1) Modern Air Defence Systems rule out Theater-Wide Air Superiority

In traditional warfare, air superiority refers to absolute control over the skies within a specific theater of conflict. It grants the dominating air force the freedom to operate while severely limiting or suppressing enemy air operations. However, the landscape of modern air defense has evolved, making the attainment of theaterwide air superiority impossible.

The versatility and effectiveness of modern Air Defence (AD) systems have reshaped the dynamics of air superiority. Advanced systems like the Patriot and the S-300, along with shorter-range systems like NASAMS and Pantsir, can now operate in 'dark' mode, presenting a formidable challenge to achieving complete air superiority.

2) Modern Air Defence dramatically reduces air power effectiveness

The effectiveness of modern Air Defence (AD) systems compels the attacking fighters and bombers to adopt a strategy of launching bombs and missiles from standoff ranges. This approach ensures their safety but comes with some drawbacks. Standoff attacks, involving costly

ammunition like cruise missiles and glide bombs, prove more expensive than unguided ammunition used in close-range attacks (rockets, bombs).

Furthermore, the smaller warhead size and lower speed of long-range guided ammunition result in reduced destructive power, making it less efficient when targeting hardened enemy installations. In summary, the long-range use of air power has become less effective in the face of advanced AD systems.

3) No role for armed drones in peer-to-peer aerial warfare

Following the stabilisation of the battlefront in October 2022, Ukraine faced a harsh reality: medium-sized armed drones, like the Turkish Bayraktar TB-2, proved highly vulnerable when deployed in heavily contested airspace. Despite initial enthusiasm over their capabilities, these drones were easily shot down during active combat operations. Consequently, Ukraine shifted their use to safer roles, such as performing reconnaissance in lightly contested areas of the battlefront.

India's strategic intent to heavily invest in US Predator drones raises questions in light of the Ukrainian experience. With two peer adversaries, China and Pakistan, and no hegemonic ambitions, India's border regions would become highly contested areas during hostilities. In such a scenario, deploying Predator drones along these borders would present significant challenges. The survival time of these drones in the face of advanced enemy defenses and countermeasures would likely be limited.

The Ukrainian conflict highlights the need for a prudent approach to drone deployment, particularly in peer-to-peer aerial warfare. Instead of relying solely on armed drones for offensive actions, nations must consider their vulnerability in contested airspace and potential alternatives. While drones have proven invaluable for reconnaissance and surveillance missions, their use in direct combat must be carefully evaluated in high-risk environments.

4) Need for long-range Air-To-Air Missiles

During the Ukrainian conflict, the supply of modern US and NATO Air Defence (AD) systems to Ukraine thwarted Russia's attempts to establish air superiority over significant portions of Ukrainian airspace. Instead, Russia managed to gain air superiority only over a relatively narrow 100-kilometer strip along the 1000-kilometer battlefront.

To achieve this limited air superiority, Russia strategically deployed its S-300 and S-400 long-range Integrated Air Defence Systems (IADS) in close proximity to the battlefront. Continuous 24x7 patrolling by Russian Su-35S and Su-30SM fighters further supported their efforts. These fighters were equipped with various types of air-to-air missiles, enabling them to engage and neutralize Ukrainian aircraft below.

A key tactic employed by Russian forces involved using a single Anti-Radiation Missile (ARM) to destroy any Ukrainian Air Defence radar that came into operation. By disrupting radar capabilities, Russia aimed to diminish Ukraine's situational awareness and hamper their air defence response. The deployment of long-range air-to-air missiles and ARMs played a critical role in establishing air superiority over the limited territory controlled by Russia.

In contrast, the Indian Air Force (IAF) faces challenges with regard to long-range air-to-air missiles. The IAF’s stock of long-range ARMs is limited, potentially impacting its ability to counter adversaries in a similar manner to Russia's approach in Ukraine, Air Vice Marshal BM Tyagi told Republic.

5) Need for multi-layered Air Defense

The conflict in Ukraine has highlighted the effectiveness of multilayered mobile air defense systems in countering a wide range of threats, including ballistic missiles, cruise missiles,

aerodynamic targets, artillery rockets, and shells. Unlike single-layer systems, the deployment of multiple AD layers makes it significantly harder for attackers to penetrate the defense. For instance, attacking fighters and cruise missiles can attempt to avoid detection by flying at low altitudes, while medium-range systems can use terrain masking to reduce their detection range.

A key strategy to bolster the efficacy of AD cover involves deploying missile systems equipped with different types of seekers, AVM BM Tyagi added. This approach makes it more challenging for incoming missiles to evade detection and interception, enhancing the overall defense capability.

The Indian Air Force has recognized the importance of a layered defense and has acquired various types of AD systems to fortify its capabilities. However, there remains an ongoing assessment of whether the quantity of systems acquired is adequate and whether their networking and integration meet operational requirements. India has made significant strides in missile technology and now stands as a self-sufficient nation in this field. The indigenously developed AD missile systems are expected to bridge any potential gaps and further bolster the country's air defense capabilities.

https://www.republicworld.com/india-news/politics/5-lessons-from-ukraine-conflict-the-evolution-of-aerial-warfare-and-indias-preparedness-articleshow.html

Mon, 24 Jul 2023

The Indian Navy's Arabian Sea Exercise is a Reality Check for Pakistan

By Aditya Bhan

In perhaps its most extensive display of operational capability in recent years, the Indian Navy conducted what it described as, "a coordinated deployment of more than 35 aircraft in the Arabian Sea" early last month. The mission included two aircraft carriers, multiple warships, submarines, and in excess of 35 frontline planes amidst China's increasing forays into the Indian Ocean.

The exercise represented a major milestone in the Indian Navy's quest for heightened maritime security and power projection capability in the Indian Ocean Region (IOR) and beyond. To truly appreciate its strategic significance, however, it must be viewed against the backdrop of the Pakistan Navy's augmentation of its surface fleet in recent years.

Pakistan's build-up

While Pakistan's submarine acquisition plans are frequently discussed in India's maritime circles, the country's augmentation of its navy's surface fleet has largely eluded the attention of New Delhi's naval mandarins, despite indicating Islamabad's new ambition to enhance its navy's ability to project power in the IOR.

The exercise represented a major milestone in the Indian Navy's quest for heightened maritime security and power projection capability in the Indian Ocean Region (IOR) and beyond.

For instance, consider the Zulfiquar-class frigates—also called F-22P frigates—which the Pakistan Navy commissioned in 2009. Modelled on the 2200-2500 tonne-class Chinese Type 053H3 frigates, operated by the People's Liberation Army Navy, these ships predate the considerably larger Tughril-class (Chinese Type 054A) frigates manufactured subsequently for the Pakistan Navy. The Pakistan Navy presently operates four Zulfiquar-class frigates, with the first three built in China, and the remaining vessel—PNS Aslat—constructed in Pakistan through transfer of

technology (see Figure 1). Not designed for any specified role, these are multi-mission guided missile frigates that can conduct anti-submarine warfare as well as anti-surface warfare (ASUW). They can additionally be utilised in an air defence role.

The multi-mission characterisation is also true for the technologically superior 4,000 tonne displacement Tughril-class stealth frigates, although with enhanced air defence capabilities. Two of these—PNS Tughril and PNS Taimur—were commissioned into the Pakistan Navy in 2022, and the remaining two—PNS Tippu Sultan and PNS Shah Jahan—in May 2023 (see Figure 2).

As the author had discussed in a recent brief, the Tughril-class—with its long-range missiles, improved radar and electronic warfare suite, and sensors—was developed by the Chinese to boost both air defence as well as ASUW capabilities. When operated with the Pakistan Navy's MILGEM/Jinnah-class corvettes, offshore patrol vessels (OPV 1900), and CH-4 medium-altitude long-endurance drones, the Tughril-class is aimed at enhancing the Pakistan Navy's footprint in the IOR rather than remaining limited to coastal defence and sea denial during war.

The Arabian Sea drill

The mega exercise involved the Indian Navy's aircraft carriers, INS Vikramaditya and the recently-commissioned INS Vikrant, as its mainstay. The flagships served as mobile airfields for a broad variety of aircraft such as the MiG-29K fighter aircraft (see Figure 3) and helicopters like the MH60R, Kamov, and Advanced Light Helicopters.

The drills demonstrated smooth integration of the two aircraft carriers operating with a varied flotilla of ships, submarines, and aircraft, displaying India's technological acumen in the maritime domain. The skilful display underscored New Delhi's commitment to protecting India's national interests, preserving regional stability, and fostering collaborative ties in the maritime sphere. Notably, these were the first mammoth drills with the two aircraft carriers in participation post the induction of the indigenously-constructed INS Vikrant in September 2022 .

The drills validated the Indian Navy's flexibility in situating the aircraft carriers in the vast expanse of the IOR and beyond. This provides enhanced operational manoeuvrability, prompt reaction to emerging challenges, and sustained deployment of air power to protect India's interests across the world; it serves consequently as a convincing testament of the centrality of sea-based air power in sustaining sea control. In this context, Indian Navy Spokesperson Commander Vivek Madhwal aptly mentioned that, as India continues to buttress its security architecture, "the significance of aircraft carriers will remain paramount in shaping the nation's defence strategy and promoting regional stability."

Conclusion

While Pakistan's augmentation of its navy's fleet of surface combatants is significant, their numbers and capabilities are not yet sufficient to credibly challenge the Indian Navy's control of the high seas. Although the Pakistan Navy's interest in novel technologies and weapons systems is notable, the Indian Navy maintains sizeable numerical superiority and wields much better capabilities, as was on show during the Arabian Sea exercise.

The skilful display underscored New Delhi's commitment to protecting India's national interests, preserving regional stability, and fostering collaborative ties in the maritime sphere.

For all its soaring ambitions, therefore, the Pakistan Navy has long remained a defensive force and will likely continue as such over the foreseeable future. Given its stated aims to protect Pakistan's maritime interests, deter aggression at and from the sea, provide disaster relief, participate in the development of coastal communities, and contribute to global efforts in maintaining a good maritime order, the core of the Pakistan Navy's approach will remain reliant on the enhancement of

its Anti-Area Access-Denial (A2/AD) capabilities. These would aim to limit and delay the enemy and deny them a free hand, using platforms like those belonging to the Tughril-class.

Nevertheless, the Indian Navy must monitor the shift in the Pakistan Navy's maritime strategy, which has, in recent years, begun to aspire for increased and lasting presence in the IOR rather than remaining limited to coastal defence and sea denial during war. From a force adopting an offensive sea denial strategy, which required the supremacy of submarines and missile-carrying maritime patrol aircraft, the latter is now gearing towards enhanced power projection in the IOR with the periodic induction of surface vessels of higher displacement and featuring the required capabilities.

https://www.orfonline.org/expert-speak/the-indian-navys-arabian-sea-exercise-is-a-reality-check-for-pakistan/

THE ECONOMIC TIMES

Mon, 24 Jul 2023

Taiwan Air Raid Drills Simulate Response to China Missile Attacks

Taiwan held air raid drills simulating its response to Chinese missile attacks in several cities on Monday, the same day the island's military kicked off its annual war games.

Self-ruled Taiwan holds frequent defence drills in the face of increasing military and political pressures from China, which regards the island as its territory.

Preparation efforts also extend to its civilian population, with authorities stepping up drills in cities, citing lessons learned from Russia's invasion of Ukraine where the street-to-street warfare appears to be part of the defence strategy playbook.

"Because of the ongoing Ukraine-Russian war, the importance of the drill is for our residents to know how to evacuate," said Tsai Yin-fong, who organised Monday's evacuation in Taipei's Neihu district.

Residents in seven counties across northern Taiwan were subjected to emergency scenarios as part of Taiwan's "Wan An" air defence exercises, which translates to "everlasting peace".

As the sirens sounded in Neihu to signal an incoming missile attack, volunteers guided residents to nearby underground evacuation shelters, where they crouched to the ground and covered their eyes and ears. In Taipei's southeastern Nangang district, firefighters simulated putting out a blaze caused by a missile attack on a train station, aiming their hoses at the building, and then rescuing a civilian from it.

Government employee Wu Kai-te, who had hidden in an underground parking lot as part of the drill, said these exercises were necessary because of China's military threats.

"Taiwan's international situation is more special because of the China factor," the 37-year-old told AFP. "It's very practical for the public and it teaches us the right poses to take to avoid more damage during a missile attack."

The air raid drills will continue across Taiwan until Thursday.

Taiwan is also currently holding its largest annual military drills, known as "Han Kuang" (Han Glory), to simulate how it would fend off an attack from Beijing's army.

Fighter jets and transport planes took off Monday from bases across the island, with Taiwan's defence ministry saying that the exercises "showcased the formidable capabilities of our air force".

But drills scheduled for Tuesday in the southern Taitung airport were cancelled as Typhoon Doksuri in Southeast Asia edges closer to Taiwan.

Beijing's sabre-rattling against Taiwan has intensified in recent years, with near-daily incursions by warplanes into the island's air defence zone. The Chinese military has also held two massive drills in waters around Taiwan, simulating targeted strikes and a blockade of the island.

https://economictimes.indiatimes.com/news/defence/taiwan-air-raid-drills-simulate-response-to-china-missile-attacks/articleshow/102082548.cms

DECCAN HERALD

Mon, 24 Jul 2023

Pakistan, US Agree to Enhance Bilateral Defence Ties

Pakistan and the US on Monday agreed to further enhance their bilateral relations, including in the defence field, at a meeting between a top American general and Pakistan's army chief General Asim Munir.

US Central Command (Centcom) chief General Michael Erik Kurilla held a meeting with Chief of Army Staff (COAS) General Munir, according to a statement issued by Pakistan Army's media wing Inter-Service Public Relations (ISPR).

They discussed matters of mutual interest, regional security situation and defence cooperation between Pakistan and the US.

"The visiting dignitary acknowledged and appreciated Pakistan Army's successes in (the) fight against terrorism and Pakistan's continued efforts for bringing peace and stability in the region," the statement said.

It stated that both sides reiterated the desire to further enhance bilateral relations in all fields.

The important meeting comes days after the two countries urged the interim Afghan government to prevent the use of its soil for terrorist attacks on other countries.

https://www.deccanherald.com/international/world-news-politics/pakistan-us-agree-to-enhance-bilateral-defence-ties-1240242.html

Science & Technology News

BW BUSINESSWORLD

Mon, 24 Jul 2023

Rising Cyber Threats Need Robust Defence Mechanism: Sanjay Katkar, Quick Heal Technologies

In today's digital age, where technology has permeated every aspect of our lives, the importance of cybersecurity cannot be overlooked, as cyber threats have become increasingly sophisticated and

pervasive. Constantly evolving tactics, the use of advanced techniques such as ransomware, phishing attacks and data breaches to target individuals, businesses and even governments are rampant.

Sophos's report "The State of Ransomware 2021" states that in 2020, the average cost of a ransomware attack on businesses reached close to Rs 8.5 crore, a 200 per cent increase from the previous year. While, the "Cost of a Data Breach Report 2020" by IMB security revealed that in 2020, the average data breach cost was USD 3.86 million and it took an average of 280 days to identify and contain a breach.

According to Microsoft's Global Tech Support Scam Research, 31 per cent of Indians lost money to cyberattacks in 2022. Every day, citizens in the state of Gujarat alone collectively lose Rs 1 to 1.2 crore to online financial fraud, according to the cyber cell of Gujarat CID. Thus, the consequences of these attacks can be devastating, ranging from financial loss to reputational damage and, in some cases, even endangering lives.

Expanding Attack Surfaces

According to Sanjay Katkar, Joint Managing Director of Quick Heal Technologies, "One of the key challenges in today's cybersecurity landscape is the ever-expanding attack surface. With the proliferation of Internet of Things (IoT) devices, cloud computing and the widespread adoption of mobile devices, we have seen an exponential increase in the number of entry points for cybercriminals to exploit. Mobile device usage has become pervasive."

According to Statista's report on the number of smartphone users worldwide from 2016 to 2023, as of 2021, there were over 3.8 billion smartphone users worldwide which is expected to reach 4.3 billion by 2023.

The number of IoT devices is also increasing at a rapid pace. By 2025, there will be over 75 billion connected IoT devices worldwide, as per Statista's report on "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025." It is essential for organisations to be proactive in their approach to cybersecurity, continuously monitoring and securing all interconnected devices and systems, Katkar said.

Katkar also said that we face an array of sophisticated threats such as ransomware, advanced persistent threats (APTs) and zero-day vulnerabilities, which are exploited by attackers. Also, Google's Project Zero revealed that a total of 18 zero days came to light in the first half of 2022 itself, half of which were variants of old ones.

These threats are often highly targeted, seeking to exploit specific weaknesses within an organisation's defences. It is no longer sufficient to rely solely on traditional antivirus software. Instead, a multi-layered approach to security is necessary, incorporating advanced threat detection technologies, behavioural analytics and real-time threat intelligence.

Another significant challenge in the evolving cyber threat landscape is the rise of nation-state-sponsored attacks. State-sponsored hacking activities have gained prominence, with governments leveraging cyber espionage and cyber warfare as tools for political and economic advantage. These attacks can have severe implications for national security and require a robust defence mechanism that can detect and mitigate such threats effectively.

The SolarWinds attack, attributed to Russian state-sponsored hackers, affected numerous government agencies and organisations, highlighting the severity of nation-state threats (Source: Cybersecurity and Infrastructure Security Agency (CISA), "Activity Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organisations)." Closer to home, All India Institute of Medical Sciences (AIIMS), one of the premier healthcare institutions in the country, has suffered cybersecurity breaches twice this year.

Another cyberattack targeting the CoWIN portal exposed the personal data of several Indian citizens – including high-profile political leaders – who had uploaded their information on the vaccination platform.

Collaboration between governments, private sector organisations and cybersecurity experts is crucial to combatting these complex threats.

Harnessing Technology for Security

The evolving landscape of cyber threats requires adapting and enhancing defence mechanisms constantly. Traditional security approaches are needed in combating these sophisticated attacks and need a proactive and multi-layered defence strategy that encompasses technology, people and processes. Effective cybersecurity requires a holistic approach that addresses both preventive and responsive measures.

Machine learning and artificial intelligence enhance cybersecurity capabilities. According to a survey by Capgemini, "Reinventing Cybersecurity with Artificial Intelligence: The New Frontier in Digital Security," 61 per cent of organisations have implemented AI in their cybersecurity strategies to detect and respond to threats effectively.

Katkar believes that organisations must invest in cutting-edge technologies that can detect and mitigate cyber threats in real time. Machine learning and artificial intelligence are revolutionising the field of cybersecurity, enabling to analyse vast amounts of data and identify patterns that indicate potential threats. By leveraging these technologies, organisations proactively detect and neutralise threats before they cause significant damage.

Beyond Antivirus

Technology alone is not enough in preventing security lapses in the digital world. Cybersecurity is a shared responsibility and it requires a collaborative effort from individuals, businesses and governments. It is essential to educate and raise awareness among individuals about the risks and best practices to protect themselves online. Individuals can take preventive measures to protect themselves. According to Google, using two-factor authentication can prevent 99.9 per cent of automated attacks on Google accounts. Basic measures such as using strong passwords, keeping software up to date and being cautious of suspicious emails or links can go a long way in preventing cyberattacks.

For businesses, it is crucial to prioritise cybersecurity and establish robust protocols to safeguard their data and systems including implementing strong access controls, conducting regular vulnerability assessments and training employees on cybersecurity best practices.

Additionally, organisations must be prepared for the worst-case scenario by developing an effective incident response plan. Governments also play a vital role in creating a secure digital ecosystem, which is why they need to enact and enforce robust cybersecurity regulations that promote information sharing, collaboration and accountability.

The evolving landscape of cyber threats demands a proactive and robust approach to cybersecurity. "As individuals, organisations and nations, we must recognise the importance of investing in advanced defence mechanisms, continuously updating our systems and staying informed about the latest threats. Cybersecurity is not a luxury, it is a necessity in our interconnected world," Katkar said.

https://www.businessworld.in/article/Rising-Cyber-Threats-Need-Robust-Defence-Mechanism-Sanjay-Katkar-Quick-Heal-Technologies/24-07-2023-485346/

THE TIMES OF INDIA

Tue, 25 Jul 2023

ISRO to Launch Singapore Satellite, Six Others on July 30

Amid the ongoing Chandrayaan-3 mission, Isro is also gearing up to launch the PSLV-C56 rocket that will carry a Singapore satellite (DS-SAR), along with six co-passenger satellites, from the first launchpad of the Sriharikota spaceport at 6.30 am on July 30.

Isro's commercial arm NewSpace India Ltd (NSIL) procured the PSLV-C56 to deploy the 360-kg DS-SAR satellite from DSTA & ST Engineering, Singapore, the space agency tweeted on Monday.

The six co-passenger satellites are VELOX-AM, a technology demonstration microsatellite, atmospheric coupling and dynamics explorer (ARCADE), an experimental satellite, SCOOB-II , a 3U nanosatellite flying a technology demonstrator payload, NuLIoN by NuSpace, an advanced 3U nanosatellite enabling seamless IoT connectivity in both urban & remote locations, Galassia-2, a 3U nanosatellite that will be orbiting at the low earth orbit, and ORB-12 STRIDER, a satellite developed under an international collaboration, according to Isro.

Singapore's DS-SAR satellite carries a synthetic aperture radar (SAR) payload developed by Israel Aerospace Industries (IAI). This allows the DS-SAR to provide for all-weather day and night coverage, and capable of imaging at one metre resolution at full polarimetry.

DS-SAR is developed under a partnership between Singapore's Defence Science and Technology Agency (DSTA) representing the Government of Singapore and ST Engineering. Once deployed, it will be used to support the satellite imagery requirements of various agencies within the Singapore government. ST Engineering will use it for multi-modal and higher responsiveness imagery and geospatial services for their commercial customers.

https://timesofindia.indiatimes.com/india/isro-to-launch-singapore-satellite-six-others-on-july-30/articleshow/102092060.cms