

April
2022

समाचार पत्रों से चयित अंश Newspapers Clippings

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

खंड : 47 अंक : 73 19 April 2022

Vol. : 47 Issue : 73 19 April 2022



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

S. No.	TITLE		Page No.
	DRDO News		1-2
	DRDO Technology News		1-2
1.	Ajit Doval inaugurates exercise to strengthen cybersecurity system	<i>The Tribune</i>	1
	DRDO On Twitter		2
	Defence News		3-18
	Defence Strategic: National/International		
2.	सरकार ने लेफ्टिनेंट जनरल मनोज सी पांडे को अगला थल सेनाध्यक्ष नियुक्त किया	<i>Press Information Bureau</i>	3
3.	Government appoints Lt Gen Manoj C Pande as next Chief of Army Staff	<i>Press Information Bureau</i>	4
4.	Army Commanders' Conference to assess border situation, discuss aspects of Ukraine conflict	<i>News On AIR</i>	5
5.	Indian Army brainstorm operational situation along China border	<i>The New Indian Express</i>	5
6.	Russia-Ukraine war: India assesses impact on defence supply from both nations	<i>Deccan Herald</i>	6
7.	Counter-drone systems should be part of 'smart' air defence network	<i>Financial Express</i>	7
8.	Way forward for Project 75(I) and MDL	<i>Financial Express</i>	9
9.	Expanding Chinese cyber-espionage threat against India	<i>Observer Research Foundation</i>	12
10.	What is Iron Beam, the Star Wars-like missile defense system tested by Israel?	<i>India Today</i>	15
11.	हाइपरसोनिक मिसाइलों को अपग्रेड करने के लिए AI का इस्तेमाल करेगा NASA, रूस के लिए खतरे की बात	<i>News 18 Hindi</i>	16
	Science & Technology News		19-20
12.	Scientists resurrect ancient enzymes to improve photosynthesis	<i>Science Daily</i>	19

The Tribune

Mon, 18 Apr 2022

Ajit Doval inaugurates exercise to strengthen cybersecurity system



National Security Adviser Ajit Doval on Monday inaugurated the National Cyber Security Incident Response Exercise along with National Cyber Security Coordinator Lt Gen (Retd) Rajesh Pant and DRDO Secretary Satheesh Reddy.

National Security Adviser Ajit Doval on Monday inaugurated the National Cyber Security Incident Response Exercise along with National Cyber Security Coordinator Lt Gen (Retd) Rajesh Pant and DRDO Secretary Satheesh Reddy.

Doval, in his address, drew attention to the launch of a large number of digital services by the government which had heightened the need to safeguard cyberspace.

The hybrid exercise will last 10 days to train senior management and technical personnel of government organisations and agencies on contemporary cyber threats and handling cyber incidents and response, stated an official news release.

The programme is being conducted by the National Security Council Secretariat (NSCS) in association with Data Security Council of India (DSCI) as the knowledge partner and supported by the DRDO.

The platform for training is being provided by CyberExer Technologies, an Estonian cybersecurity company accredited for globally conducting several large cyber exercises.

The participants will be trained on various key cyber security areas such as intrusion detection techniques, malware information sharing platform, vulnerability handling and penetration testing, network protocols and data flows and digital forensics.

NCX India will help officials to better understand cyber threats, assess readiness and develop skills for cyber crisis management and cooperation.

Over 140 officials to be trained

- The hybrid exercise will last 10 days to train senior management and technical personnel of govt organisations on contemporary cyber threats and handling cyber incidents
- Over 140 officials will be trained through training sessions, live fire and strategic exercises
- The participants will be trained in key cyber security areas such as intrusion detection techniques and malware information sharing platform.

<https://www.tribuneindia.com/news/nation/ajit-doal-inaugurates-exercise-to-strengthen-cybersecurity-system-387471>

DRDO On Twitter



DRDO
@DRDO_India

...

NCX 2022 National
[#CyberSecurity](#) Exercise,
organised by NSCS, was
inaugurated by Shri AjitDoval,
NSA in the presence of Chairman
DRDO, CISC, NCSC & renowned
cyber experts. In his address, Dr
Satheesh Reddy emphasised on
the need of robust cyber security
technology measures.



A. Bharat Bhushan Babu and NCSC India

5:37 PM · Apr 18, 2022 · Twitter for iPhone

Defence Strategic: National/International



Press Information Bureau
Government of India

Ministry of Defence

Mon, 18 Apr 2022 7:25 PM

सरकार ने लेफ्टिनेंट जनरल मनोज सी पांडे को अगला थल सेनाध्यक्ष नियुक्त किया

वर्तमान में सेना के उप प्रमुख लेफ्टिनेंट जनरल मनोज सी पांडे को सरकार ने अगला सेनाध्यक्ष नियुक्त किया है। इस पद पर उनकी नियुक्ति 30 अप्रैल, 2022 की दोपहर से प्रभावी होगी। 06 मई, 1962 को जन्मे लेफ्टिनेंट जनरल मनोज सी पांडे को 24 दिसंबर, 1982 को भारतीय सेना की कोर ऑफ इंजीनियर्स (द बॉम्बे सैपर्स) में कमीशन दिया गया था। 39 वर्षों से अधिक समय की अपनी लंबी और विशिष्ट सेवा अवधि के दौरान श्री मनोज सी पांडे ने विभिन्न कमानों, अधिकारी पदों और प्रशिक्षण सम्बन्धी नियुक्तियों पर काम किया है। लेफ्टिनेंट जनरल मनोज सी पांडे ने अपनी कमान की नियुक्तियों के दौरान पश्चिमी युद्ध क्षेत्र में एक इंजीनियर ब्रिगेड की कमान संभाली है, उन्होंने हमलावार फौजी दस्ते के साथ काम किया है और इसके अलावा जम्मू-कश्मीर में नियंत्रण रेखा पर एक पैदल ब्रिगेड के साथ उनकी सेवाएं भी शामिल हैं। श्री मनोज सी पांडे की अन्य महत्वपूर्ण कमांड नियुक्तियों में पश्चिमी लद्दाख के ऊंचाई वाले क्षेत्र में एक माउंटेन डिवीजन तथा एलएसी के साथ और पूर्वी कमान के काउंटर इंसर्जेंसी ऑपरेशन क्षेत्र में एक कोर की कमान संभाली।



लेफ्टिनेंट जनरल के रैंक पर मनोज सी पांडे अंडमान और निकोबार कमान के कमांडर-इन-चीफ और कोलकाता में पूर्वी कमान के जीओसी-इन-सी के पद पर सेवारत रहे हैं और ये उनकी सेना के उप प्रमुख के रूप में कार्यरत होने से पहले की महत्वपूर्ण नियुक्तियां हैं।

लेफ्टिनेंट जनरल मनोज सी पांडे राष्ट्रीय रक्षा अकादमी के पूर्व छात्र हैं और उन्होंने केम्बरली (यूके) के स्टाफ कॉलेज, महू के आर्मी वार कॉलेज और नई दिल्ली में राष्ट्रीय रक्षा कॉलेज से अपनी पढ़ाई पूरी की है।

लेफ्टिनेंट जनरल मनोज सी पांडे को उनकी उत्कृष्ट सेवा के लिए परम विशिष्ट सेवा मेडल, अति विशिष्ट सेवा मेडल और विशिष्ट सेवा मेडल से सम्मानित किया गया है।

<https://pib.gov.in/PressReleasePage.aspx?PRID=1817880>



Press Information Bureau
Government of India

Ministry of Defence

Mon, 18 Apr 2022 7:25 PM

Government appoints Lt Gen Manoj C Pande as next Chief of Army Staff

Government has appointed Lt Gen Manoj C Pande, presently Vice Chief of the Army Staff, as the next Chief of the Army Staff with effect from the afternoon of April 30, 2022. Born on May 06, 1962, Lt Gen Manoj C Pande was commissioned on December 24, 1982 in the Corps of Engineers (The Bombay Sappers) of the Indian Army. During his long and distinguished service spanning over 39 years, he has served in a variety of Command, Staff and Instructional appointments. The Command appointments of Lt Gen Manoj C Pande include Command of an Engineer Brigade in the Western Theatre, as part of Strike Corps and an Infantry Brigade along with Line-of-Control in Jammu & Kashmir. Other important Command appointments include a Mountain Division in the high-altitude area of the Western Ladakh and Command of a Corps, deployed along the LAC and in Counter Insurgency Operations area of Eastern Command.

In the rank of Lt General, the officer has held important appointments including that of Commander-in-Chief of the Andaman & Nicobar Command and as the GOC-in-C of the Eastern Command at Kolkata before getting appointed as the Vice Chief of the Army Staff.

Lt Gen Manoj C Pande is an alumnus of National Defence Academy and has undergone courses at Staff College, Camberley (UK), Army War College, Mhow and National Defence College, New Delhi.

For his illustrious service, Lt Gen Manoj C Pande has been conferred with Param Vishisht Seva Medal, Ati Vishisht Seva Medal and Vishisht Seva Medal.

<https://pib.gov.in/PressReleasePage.aspx?PRID=1817865>



NewsOnAIR

Mon, 18 Apr 2022

Army Commanders' Conference to assess border situation, discuss aspects of Ukraine conflict

Army Commanders' Biannual Conference is all set to kickstart today in New Delhi. During the five-day conference, the top brass of the Indian Army will take stock of the situation along the borders, and discuss various aspects relating to the Russian-Ukraine conflict.

The Army Commanders' Conference is an apex level biannual event that is held in April and October every year, and for this year it is scheduled from 18-22 April 2022 in the national capital. Army Commanders' Conference is an institutional platform for conceptual level deliberations, culminating in making important policy decisions for the Indian Army.

Discussion to review border situation

The apex level biannual event is an institutional platform, in which senior leadership of the Indian Army reviews the operational situation along the active borders, assesses threats in the entire spectrum of conflict and undertakes an analysis of capability voids to further focus on capability development & operational preparedness plans. As per the official statement by the Indian Army, discussions on aspects pertaining to infrastructure development in border areas, modernisation through indigenisation, induction of Niche tech and assessment of any impact of the Russia – Ukraine conflict are also scheduled to take place. Further, various agenda points sponsored by regional commands will be deliberated upon by the senior commanders apart from proposals concerning improving works, financial management, introducing e-vehicles, and digitisation in the Indian Army. Notably, as a part of the conference, Boards of Governors meetings of the Army Welfare Education Society (AWES) and Army Group Insurance Fund (AGIF) will be organised. On the fourth day of the conference, Defence Minister Rajnath Singh is also expected to interact with the senior commanders and address the Conference on 21 April 2022. The conference is also a formal forum for senior leadership of the Indian Army to interact with the senior functionaries of the Department of Military Affairs and Department of Defence during the Ministry of Defence Interaction Session.

<https://newsonair.com/2022/04/18/army-commanders-conference-to-assess-border-situation-discuss-aspects-of-ukraine-conflict/>



**THE NEW
INDIAN EXPRESS**

Tue, 19 Apr 2022

Indian Army brainstorm operational situation along China border

Top commanders of the Indian Army on Monday brainstormed the operational situation along the country's borders. The army leadership will also discuss issues pertaining to intelligence,

operational logistics, human resources and modernisation during the ongoing commanders' conference.

"It was the Military Operations day on Monday and the operational situation was discussed by the top brass." This included the deployment and the operational situation along the Line of Actual Control with China, the Line of Control and other areas," a source said.

India and China have been on a protracted standoff along the Line of Actual Control in Eastern Ladakh since May 2020. Although the situation has seen de-escalation, the deployment of personnel by both sides continues in Hot-Spring area, Depsang and Demchok.

Another issue the army is set to brainstorm is the implications of the protracted conflict between Russia and Ukraine on India's defence plans. Apart from Defence Minister Rajnath Singh, senior army commanders are expected to attend the conference.

The commanders are set to "review the operational situation along active borders, assess threats in the entire spectrum of conflict and undertake analysis of capability voids to further focus on capability development and operational preparedness plans". The Army Commanders' Conference is an apex level biannual event which is held in April and October every year. Also, the conference is an institutional platform for making important policy decisions.

<https://www.newindianexpress.com/nation/2022/apr/19/indian-army-brainstorm-operational-situationalong-china-border-2443655.html>



Mon, 18 Apr 2022

Russia-Ukraine war: India assesses impact on defence supply from both nations

India is assessing the implication of the Russia-Ukraine conflict on its security environment as well as supply of military hardware from both the warring nations.

The assessment of any impact of Russia-Ukraine war is on the agenda, as the Indian Army commanders assembled for a four-day-long conference in New Delhi on Monday. Defence Minister Rajnath Singh is also expected to interact with the commanders during the conclave, which is being led by Chief of Army Staff Gen M M Naravane.

The commanders are expected to assess impact on supply of defence equipment and spares from both Russia and Ukraine and discuss ways to deal with any disruption in supply and services in the wake of the conflict between the two nations, sources told DH on Monday.

India's dependence on Russia for military hardware was built over decades. A 2020 report by the Stimson Centre based in Washington DC estimated that 90 per cent of defence equipment, weapons and platforms presently used by the Indian Army had originated from Russia. Nearly 86 per cent of the defence equipment currently in military service in India had origins in the former Soviet Union nation.

Russia, according to the sources, might not be able to deliver the second unit of the S-400 Triumf air defence missile systems to India on time due to its military operations in Ukraine and the

sanctions imposed by the United States and other western nations on it. However, some training equipment and simulator for the second unit have already arrived. Russia had in December 2021 delivered the first of the five S-400s India procured for \$5.43 billion.

New Delhi, however, is more worried about disruptions in supply of spares from Ukraine, particularly for some of the tanks and missile systems currently being used by the Indian Army and for gas turbine engines of some of the Indian Navy warships.

The commanders, according to the sources in New Delhi, are expected to review the situation along the India-China Line of Actual Control (LAC), where soldiers of the two nations are still engaged in a stand-off that started two years ago with the communist country's People's Liberation Army (PLA) amassing large number of troops along the disputed boundary between the two nations, prompting counter-deployment by the Indian Army.

New Delhi has been assessing the possibility of China trying to take the advantage of geopolitical churning triggered by Russia-Ukraine conflict and stepping up its belligerence, not only along the disputed boundary between the two nations in the Himalayas, but also in the South China Sea, the East China Sea and the Taiwan Strait. The commanders over the next few days will review the Indian Army's preparedness to respond to any bid by the Chinese PLA, not only along the western sector, but also in the middle and the eastern sector of the long disputed boundary between the two nations.

A spokesperson of the Ministry of Defence said that the senior leadership of the Indian Army would review the operational situation along the active borders during the conference, apart from assessing threats in the entire spectrum of conflict. The commanders would also analyse capability voids to further focus on capability development and operational preparedness plans, added the spokesperson.

<https://www.deccanherald.com/national/russia-ukraine-war-india-assesses-impact-on-defence-supply-from-both-nations-1101809.html>



Mon, 18 Apr 2022

Counter-drone systems should be part of 'smart' air defence network

Assigning the manufacturing of a drone detection system to a private Indian industry designed by state-run organizations marks the pivotal moment of a joint first step towards defence indigenization. Notably, Defence Minister Rajnath Singh's handing over of Transfer-of-Technology (ToT) documents on April 7 also came close on the heels of the Ministry of Defence's (MoD) third list of 100 items to be procured/developed/manufactured domestically and not through imports. This bears the seriousness of the effort towards attaining defence indigenization.

From a pure technology and doctrinal perspective, the armed forces should now consider integrating counter-drone systems as a part of a larger highly networked, 'intelligenized' and 'informationized' environment— approaches that are employed by potential adversaries. Counter drone systems could also be airborne on other drones themselves, rather functioning as smaller

Airborne Early Warning (AEW) systems fused with larger AEW aircraft and other ground-based Counter-UAV platforms.

Webbed into a larger and highly dense network connecting ground, sea-based, airborne, space and individual combatants, allow C-UAVs to evolve from standalone platforms to be a part of a bigger setup that enhances situational awareness of both the frontline combatants and military decision makers.

With a new concept of operations fuelled by new technologies (AI, Machine Learning, Big Data, Quantum Computing and Quantum Communications), the government should now undertake a study of whether the new techno-military doctrines are relevant to India. Simultaneous development of other relevant technologies like Directed Energy Weapons (DEW) should continue, standardized to be compatible with other C-UAVs.

Depending on the battlefield needs and doctrines, the C-UAVs can also deploy 'hard-kill' options like missiles and guns either attached as a part of the system or direct other batteries or ground-based units to undertake fire. But arming all units with such portable and easy to deploy systems is vital as battlefield drones, both big and small, are likely to be used in nearly all scenarios. India is creating Integrated Battle Groups (IBG) with mixed armour, infantry, artillery, mechanised infantry, combat engineers, signals and air defence units, where C-UAVs of various sizes should be deployed with each arm.

Adversaries target not only fighting formations but also support and combat support units to degrade overall military fighting capability, especially during large force-on-force contacts. And while bigger armed drones can be taken down with missiles and guns, advanced soft-kill options like Radio Frequency (RF) jamming, spoofing and possibly hacking are equally effective. It is the capability to develop non-kinetic hard and soft-kill systems that reflect the industrial and technological advancement of a country. Also used in cyber and space warfare which are poised to be the next battlefield frontiers, developing electronics and electronic hardware manufacturing capability that go into soft-kill systems is crucial and should be a larger focus under the government's 'Aatmanirbharta' aim.

For instance, millimetre microwave radars (MMR) that transmit radio frequencies at short wavelengths are said to be effective against smaller swarm drones. China recently tested vehicle mounted box launched swarm drones, released through multiple tubes stacked together, that once in the air in a group of dozens, deploy wings and can work together to perform a variety of tasks.

Possibly AI-enabled, they can overwhelm an air defence system or a ground formation drawing their fire, act as loitering munitions to take out well-defended targets, provide mass air surveillance capability, acting as a smaller part of its Communications Coordination Command Control Intelligence Surveillance and Reconnaissance (C4ISR) network to provide enhanced situational awareness. This is in line with China's 'informationized' and 'intelligenized' warfare doctrines.

The possibilities are endless and taking out well networked small swarm drones are equally limited. This is where non-kinetic hard and soft kill systems come in. India should therefore develop an industrial capability to manufacture hi-tech electronics like powerful lasers, RF jammers, MMR and microwave weapons that can simultaneously disable swarm drones.

While this pertains to just counter-drone systems, drone manufacturing capability itself can be enhanced in India. While structures like arms, upper and lower sidings, fixed/retractable landing gears, internal support and payload carriers are manufactured in India, propellers and motors are largely imported from China, Taiwan and Germany. India even lags in electronics and avionics

systems like speed controllers, GPS modules, power distribution boards, signals receivers, flight controllers, telemetry modules, communication devices and GPS hardware that go both into drone and counter-drone systems.

Our capability in building our own Electro-Optical IR/Thermal systems, Synthetic Aperture Radar and Medium Powered Radars leaves a lot to be desired for. Promoting MSMEs that develop and manufacture these can lead to massive economic benefits too. Over the next 15 years, the Indian Army plans to induct UAVs down to the battalion level, while the Indian Air Force aspires to have at least six 18-fleet squadrons of both armed and unarmed UAVs. With Requests for Information/Requests for Proposal (RFI/RFP) estimated to be to the tune of 100 a year, developing these advanced electronics in-house reduces imports, with India possibly becoming their exporter to the very countries we buy them from!

To sum up, India first needs to evolve a basic academic understanding of where counter-drone and drone systems fit in the larger scheme of things involving emerging technologies, military concepts, industrial capabilities and adversary nations' capabilities. This should be a joint effort between the government, services, industry and academia.

Secondly, defence indigenization should not be looked at as a standalone effort but as a larger goal towards becoming industrially advanced with hi-tech and electronics manufacturing leading the charge. Drones and counter-drone systems use these very systems and having an integrated approach automatically synergizes efforts by all stakeholders, effecting the Comprehensive National Power and a 'whole of nation' approach that can withstand any adversity.

<https://www.financialexpress.com/defence/counter-drone-systems-should-be-part-of-smart-air-defence-network/2494887/>



Mon, 18 Apr 2022

Way forward for Project 75(I) and MDL

By Cmde Arun Kumar

Project 75(I) is the second part of Phase I of the 30-year submarine building plan, approved by the CCS in Jul 1999, which was to be executed in the period 2000-15. Under this, six submarines of an appropriate design, preferably of a derivative of 877EKM like the Amur 1650 (Russia), were to be built in the period as stated above. Project 75 was the first part which was started in Oct 2005 and is nearing completion, with the sixth Kalvari class boat of Scorpene design to be delivered to the Navy by the end of this year.

Early Negotiations

As per the 30-year plan, discussions to identify the platform for P-75I were initiated with the Russian side in November 1999, which continued through December 2001. By then, it was understood that broad agreements on design specifications and transfer of design and build technology for Amur 1650 had been reached. Representatives of MDL and L&T also participated in this.

Consequently, follow-on actions to progress the project were taken up with the competent authority. It was towards the end of 2003. However, due to the announcement of early General elections in May 2004, the case was kept in abeyance until a new Government at the Centre was formed after the elections. The UPA formed the new Government at the Centre, and a review of all ongoing cases was undertaken, and as a result, P75(I) receded into the background. The contract for the Scorpene design with M/S DCN of France was concluded for P75 in Oct 2005, and construction activities with a delay started in MDL in real earnest only in 2010. Despite the initial hiccups, this programme has progressed well and will be complete by the end of this year.

Reformation of NSQRs for P75 (I)

As per the original approval of the 30-year plan, the two projects in Phase I viz; P75 and P75(I) were to have designs from Western Sources (Scorpene selected) and of Eastern (Russia) Origin for P75(I). In Phase II (2016-30), 12 submarines were to be made of a totally indigenous design incorporating the best of both the above-mentioned designs. However, since Project 75(I) as envisaged could not be progressed in parallel, as mandated by the 30-year plan, and due to a considerable time-lapse, the NSQRs for P 75(I) were reformed to include Air Independent Propulsion System (AIPS). The primary role for the boats under P75 (I) was the capability to attack targets ashore and deep inland; as such, a Land attack missile was integral to the QRs. The inclusion of AIPS created a dilemma in that the Russians did not have an AIPS, and the other contenders from the West did not have a sub-launched land attack missile. Thus the project stalled and could not be actively pursued.

Two lines of production

At the time of the initial discussions, since boats of two designs were to be built simultaneously, two production lines were under consideration. These were the established MDL and L&T that had gained experience building hull sections for a special project. The choice of two lines then was imperative since MDL would be fully loaded with P 75 and could not undertake series construction of 12 boats. Even to execute the P 75, an infrastructure upgrade in MDL was needed, and as understood, sums in hundreds of crores were budgeted. In addition, skill sets that had been lost due to the abandonment of the 5th & 6th SSKs of Shishumar class boats in the mid-80s needed to be created afresh. Just as a side effect, we lost trained manpower to South Korea, which was starting the production of conventional submarines.

Revival of P75 (I)

Once the P75 was truly underway, attention was once again turned to P 75(I) with the amended QRs. However, with the introduction of the new DPP of 2016, the concept of Strategic Partner Initiative (SPI) involving the Private Sector was introduced, and P75 (I) was earmarked as the first project to be undertaken with an SP. After many deliberations and fits and starts, two SPs were shortlisted viz; MDL and L&T. (One wonders why so many years were needed to decide this as way back in 2003 itself, it was clear that only these two had capabilities for submarine construction). It was also decided to go the competitive route to select the design collaborator. Accordingly, five potential collaborators viz; Rosoboronexport (Russia), Navantia (Spain), Daewoo (South Korea), DCN Naval Group (France) and Thyssenkrupp Marine Systems (FRG) have been shortlisted. The two SPs were asked to negotiate a tie-up with any one of the five collaborators and make a joint bid to the MOD for final selection. In my view, this is a harebrained scheme wherein a yard is to negotiate the technology transfer with each of the five collaborators and then decide on a bid with the selected partner. The induction of technology is a 'user' function and not that of the yard. The user should have done this activity at NHQ. Be that

as it may, except for DSME (South Korea), all others showed hesitancy to participate due to the RFP's conditions.

Further, it was not clear how a private yard would ensure the secrecy and integrity of the information without a sovereign guarantee. As of present, as understood, the matter rests here. The urgency to progress the project needs no emphasis as already the project is 20 years in arrears. The matters should be progressed with alacrity even if the RFP has to be tweaked to accommodate the concerns of the collaborators.

In the case of P75, the user first selected the Collaborator and the Yard MDL (Only one). During the negotiations with the Collaborator, the MDL team sat on the side of the MOD. Once that was complete, the yard had a clear idea of design transfer and collaboration costs and was in a firm position to bid for the total cost as the Principal Contractor. Accordingly, the next stage of negotiations was between the user (MOD) and the MDL for the total cost of the Project/boat. The success of this model was the fruition of the contract in the production and delivery of six boats of Scorpene design. This, in my view, is the only viable working model to follow.

Future Exploitation of Assets in MDL

The upgraded infrastructure created in MDL for P 75 has already gone idle, with the 6th submarine Vaghsheer in the final stages of construction. It would be a great folly to let this strategic asset go to waste without further orders. As stated earlier herein, in the initial stages of the implementation of Phase I of the 30-year plan, there was a necessity for a second line, but in the present circumstances, the same no longer holds. Further, the MDL has created the capacity to undertake a series of construction of 11 boats with the conversion of the Alcock yard to submarine building and the East Yard. This is a strategic defence asset of the Government of India and cannot be allowed to idle. The multiplicity of yards in such a vital sector is a luxury even the United States cannot afford. They have only two yards, viz; Newport and the Electric boat division at General Dynamics, which make strategic and tactical boats. In our case, we already have the Ship Building Centre dedicated to the Strategic Programme.

Continuation of Series Production

The 30 Year plan had envisaged a strategic vision of creating indigenous capability in the design and construction of conventional submarines in concert with the private sector. That aim remains valid even today. With the construction of 18-24 boats under the plan does not mean its end but a continuation of series construction to enable replacements as the older boats become due for retirement (Decommissioning). The capabilities thus created must remain alive and viable at all times. The intervals of outputs may be staggered to balance the yard loading and meet the force level requirements at any given time. What cannot be allowed, at any cost, is the non-utilisation of a strategic asset created at great costs not only in monetary terms but also in terms of skill sets and expertise either due to redundancy or demand. Our investments must be thus tuned to ensure capacity utilisation as an assembly line.

Way Forward

The goals and aim of the 30-year submarine building plan were well-considered and strategic in thought and nature. They must be implemented for our Navy to be self-sufficient (Atma Nirbhar) in meeting its own requirements of submarine force levels. In due course, it could also mean the ability to export submarines. Strategic assets like in MDL for the construction of submarines must be kept loaded and in activity mode at all times. This will not only ensure the survival and viability of these assets but also nurture innovation in the long run. Accordingly, since MDL is already selected as the SP, it must be nominated as the lead yard (Principal Contractor) for P75

(I) with a work-sharing relationship with L&T (The other SP). This will allow the rules of DPP to be also met. Redundancy built for just the sake of it may not be prudent in the present case. Work-sharing will also help reduce the delivery periods and, in some measure, mitigate the inordinate delay the 30 Year plan has suffered. The Contract for the Transfer of Design and Build technology must be between the user and the Collaborator (Principal Collaborator). We must not forget that Phase II is looming ahead.

<https://www.financialexpress.com/defence/way-forward-for-project-75i-and-mdl/2495190/>



Mon, 18 Apr 2022

Expanding Chinese cyber-espionage threat against India

On 6 April 2022, American cybersecurity firm, Recorded Future revealed that Chinese state-sponsored hackers had targeted India's power grids in Ladakh. A part of China's cyber espionage campaign, the sustained targeting of the power grids was possibly aimed at collecting information on India's critical infrastructure or preparing for their sabotage in the future. What technical information the hackers had collected through this breach remains unknown. However, this targeting of the power grids and cyber-espionage campaign fits in the broader pattern of China's systematic pursuit of offensive cyber operations against India for more than a decade.

India is not alone. Several countries, including the Netherlands, United Kingdom, Australia, and the United States, and businesses like Vodafone and Microsoft have revealed China's unabated campaign to steal trade and other sensitive data.

China's cyber espionage against its adversaries

The US Cybersecurity and Infrastructure Security Agency, for instance, in its overview of China's cyber activities, has noted that Beijing conducts extensive hacking operations globally, targeting the health and telecom sector, critical infrastructure providers, and enterprise software providers, stealing intellectual property and confidential information. These targets provide valuable leads for subsequent "intelligence collection, attack, or influence operations". The biggest and most recent such hack for cyber-espionage purpose was the breach of the Microsoft Exchange Server by the Hafnium state-sponsored hacking group in March 2021. The group exploited Microsoft's email software vulnerabilities to target US government departments, defence contractors, policy think tanks, and infectious disease researchers, amongst others.

Not just cyber attacks, China has even utilised overseas business contracts and activities to pursue its cyber-espionage campaign. A crucial part of this campaign is the telecom network and fibre optic communications infrastructure provided by Chinese companies like China Telecom, Huawei, and ZTE. The litany of spying instances involving Chinese companies, mostly Huawei, as listed in Table 1, establishes this trend. No wonder, for a long time, policymakers in the United States had been warning and recommending to exclude Chinese firms such as Huawei and ZTE from any critical communication backbone.

Table 1: Select recent incidents of Chinese cyber-espionage worldwide

Month & Year	Country	Target	Incident
2010	The Netherlands	KPN mobile phone network	A hidden backdoor by Huawei on the Netherlands's largest mobile network KPN allowed Huawei to gain unlimited access to call records and customer data, including the conversations made by government ministers. A risk-analysis report by Capgemini consultancy on KPN's telecom network revealed this instance of espionage.
January 2017	Ethiopia	African Union (AU) headquarters	Technicians at the AU headquarters building in Addis Ababa discovered that a backdoor inserted by China allowed the transfer of data every night from computers in the building to servers in Shanghai for five years. Beijing had constructed the building. In 2020, reports again noted that China-based hackers had been filching security camera footage from inside the AU headquarters building.
April 2019	Italy	Vodafone telecom network	Vodafone Group acknowledged that it had found vulnerabilities with Huawei equipment deployed for the carrier's Italian business. The vulnerabilities, which had been running for years, could have given Huawei unauthorised access to the carrier's fixed-line network in Italy.
August 2020	Papua New Guinea	National Data Centre	A report from the Australian government and Papua New Guinea's National Cyber Security Centre noted that the latter's National Data Centre, built by Huawei in 2018, is marred by various cybersecurity issues, which exposed secret government files to being stolen.
October 2020	United Kingdom	National telecom network	UK intelligence agency, Government Communications Headquarters, discovered a 'nationally significant' vulnerability in Huawei equipment. The vulnerability was so severe that it was withheld from the company.

Source: *Compiled by authors*

China uses cyber espionage to fulfil several objectives. According to the latest US intelligence community assessment, these cyber-espionage operations often target those sectors which provide potentially rich “follow-on opportunities for intelligence collection, attack, or influence operations.” China uses information ferreted from these sources i) to boost its domestic manufacturing capabilities, and ii) to produce lower-cost imitations of popular western brands/products and, thereby, attain a competitive advantage.

The example of China's theft of US' F-35 stealth fighter aircraft data is well-documented. But there are many other cases where China has sought competitive intelligence on the foreign business rivals of Chinese companies in multiple sectors, including defence, technology, oil and energy, automobile, and telecommunications.

Target India

While India has so far not proved such an attractive target for China's commercial cyber espionage, things may be changing.

In March 2021, a Singapore-based company, CyFirma, revealed that a Chinese state-backed hackers' group had targeted the information technology systems of two Indian vaccine makers—Bharat Biotech and the Serum Institute of India (SII). These companies' vaccines have been the most critical element of India's national vaccination programme and vaccine diplomacy. Chinese hackers' targeting of SII is significant when examining the reach of its vaccine, Oxford-AstraZeneca/Covishield, which is being used in 183 countries, as against almost half-reach of China's flagship Sinopharm vaccine (used in 90 countries). Prime Minister Narendra Modi's description of India as the “pharmacy of the world” vividly brings the country's

comparative advantage over China. Therefore, Chinese hackers may be trying to bridge that gap by targeting the vaccine makers to steal commercially valuable data.

A Singapore-based company, CyFirma, revealed that a Chinese state-backed hackers' group had targeted the information technology systems of two Indian vaccine makers—Bharat Biotech and the Serum Institute of India (SII).

Therefore, we can expect China to broaden its range of targets for commercial cyber-espionage reasons to include sectors like services where India has a comparative advantage. Another potential target includes India's start-up innovation ecosystem, where India has barred Chinese investments.

But beyond commercial considerations, China's cyber-espionage campaigns also demonstrate its coercive tactics.

The targeting of the power grids in Ladakh in the middle of the prolonged border stand-off is clearly aimed at sending a political message and signalling that Beijing can open other non-military fronts in the bilateral security competition. Pertinently, this is the second such attack on India's power sector by Chinese hackers.

In October 2020, in one of the worst power outages, large parts of Mumbai witnessed a widespread blackout, which affected suburban train services and hospitals. Months later, Recorded Future noted that a China-linked hacker group, "RedEcho," had breached the Indian power sector, which may have caused Mumbai's power outage—a charge refuted by a Maharashtra government's technical audit committee examining the incident. But Recorded Future added that besides the power sector, Chinese hackers also targeted two Indian ports and some parts of the railway infrastructure. Coming in the wake of the violent Galwan Valley clash between the Indian and Chinese militaries in June 2020, this targeting of India's critical infrastructure suggested a combination of intimidation and retribution.

The targeting of the power grids in Ladakh in the middle of the prolonged border stand-off is clearly aimed at sending a political message and signalling that Beijing can open other non-military fronts in the bilateral security competition.

Moreover, the extent of Chinese persistence in targeting India is shown by the Advanced Persistent Threat 30 (APT30) vector. This threat actor's espionage operation ran for a decade before its discovery in 2015. It harvested information from the Indian computer networks on geopolitical issues relevant to the Chinese Communist Party, such as the India–China border dispute, Indian naval activity in the South China Sea, and India's relations with its South Asian neighbours.

Conclusion

In responding to this widening Chinese cyber-espionage activity, India is hardening its cyber defences and undertaking its own offensive cyber operations. But it needs to do more. For one, it needs to start outlining technical evidence to attribute these attacks to Chinese state-sponsored hackers—something which the national security establishment has resisted, even as the technical community in India and abroad has presented that evidence.

New Delhi also needs a dedicated mechanism to monitor these offensive operations. While respective intelligence and security agencies do trace foreign spying campaigns against India, this kind of cyber activity is often treated as a cyber breach or incident, focusing on the target and activity, but without linking it to the broader Chinese cyber-espionage campaign, the involvement of state-sponsored hacking groups and the trends in their targeting of Indian

computer networks. Perhaps the Defence Cyber Agency can take the initiative to collaborate with the civilian technical community to track these operations. This will send a definite message that Beijing's mischief is not going unnoticed and is being systematically tracked as part of India's comprehensive cyber posture.

<https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india/>



Mon, 18 Apr 2022

What is Iron Beam, the Star Wars-like missile defense system tested by Israel?

Films have always been a source of inspiration behind new discoveries, technological advancements, and unique designs. Israeli engineers and scientists have now revealed a Star Wars-like laser beam that can target incoming missiles and render them useless. The Israeli prime minister says, "It may sound like science fiction, but it's real."

Dubbed Iron Beam, the technology, a laser missile-defense system, can reportedly intercept drones, mortars, rockets, and anti-tank missiles.

Israel has been known for its technological advancement in weaponry and is one of the biggest global exporters of arms. The Iron Beam is part of the country's aerial defense system alongside its highly advanced rocket-intercepting Iron Dome. Claimed to be the world's first energy-based weapons system, it uses a laser beam to shoot down incoming UAVs, rockets & mortars.

Naftali Bennett in a tweet said, "Israel has successfully tested the new "Iron Beam" laser interception system. This is the world's first energy-based weapons system that uses a laser to shoot down incoming UAVs, rockets & mortars at a cost of \$3.50 per shot."

Israel has successfully tested the new "Iron Beam" laser interception system.

This is the world's first energy-based weapons system that uses a laser to shoot down incoming UAVs, rockets & mortars at a cost of \$3.50 per shot.

What is Iron Beam?

In a video released by the Israeli government, the Iron Beam system is shown targetting an incoming rogue Unmanned Aerial Vehicle (UAV), which is then destroyed mid-air before it is able to attack. The test was conducted last month in the Negev Desert.

The video, which was highly edited and set to music, appears to show a laser beam shooting out of a ground station, hitting the targets and smashing them into small pieces.

While the country has released very few details about the laser system's effectiveness, it is expected to be deployed on land, in the air, and at sea. The goal is to deploy the laser systems around Israel's borders over the next decade to protect the country against attacks. The announcement of the new system was aimed at sending messages to Palestine and Iran.

Why does Israel need Iron Beam?

Part of a series of systems meant to intercept everything from long-range missiles to rockets launched from just a few kilometers (miles) away, Iron Beam has been designed to complement the Iron Dome system, which has emerged as a costly technology for the country.

Israeli PM Naftali Bennett had in February acknowledged that the Iron Dome defense system is too expensive and the country is speeding the rollout of laser technology to help protect it from rocket attacks. The Iron Dome defense system is too expensive and the country is speeding the rollout of laser technology to help protect it from rocket attacks. If it is possible to intercept a missile or rocket with just an electric pulse that costs a few dollars, we will have nullified the ring of fire that Iran has set up on our borders," Bennett had told the Institute for National Security Studies at Tel Aviv University.

The Iron Dome system, unveiled a decade ago, has been a great success, with a 90% interception rate against incoming rocket fire, however, it has been equally expensive. The Israeli prime minister had said that Iron Dome is limited by its high price, which is partly underwritten by the United States. Bennett said someone in Gaza can fire a rocket toward Israel for a few hundred dollars, but it costs tens of thousands of dollars to intercept it.

The new system, as claimed by the Israeli government, will cost just \$3.50 per shot.

Will other Countries get Iron Beam?

Israel has been known to be a major arms exporter to countries across the world, including India, which uses Israeli Tavor assault rifles, the Negev and the B-300 anti-tank rocket launchers, and Phalcon AWACS systems among others. "This new generation of air defense can also serve our friends in the region," Bennett has said in the past, hinting that the technology could be used by other countries as well.

The country is working on a "laser wall" against missiles, rockets, and drones that can be used by Israel and other countries against threats from Iran, which has developed long-range missiles capable of striking Israel.

<https://www.indiatoday.in/science/story/what-is-iron-beam-the-star-wars-like-missile-defense-system-tested-by-israel-1938825-2022-04-18>



Mon, 18 Apr 2022

हाइपरसोनिक मिसाइलों को अपग्रेड करने के लिए AI का इस्तेमाल करेगा NASA, रूस के लिए खतरे की बात

रूस और यूक्रेन के बीच जंग (Russia-Ukraine War) चल रही है. रूस अपने शक्तिशाली मिसाइलों से यूक्रेन पर हमले कर रहा है. इस बीच अमेरिकी स्पेस एजेंसी नासा (NASA) ने हाइपरसोनिक जेट इंजन को और डेवलप करने के लिए कृत्रिम बुद्धिमत्ता (Artificial Intelligence) को लागू कर रहा है. इससे प्लेन,

स्पेस लॉन्चिंग और मिसाइल हथियारों में क्रांति लाई जा सकती है. यूक्रेन में जंग के बीच रूसी राष्ट्रपति व्लादिमीर पुतिन (Vladimir Putin) के लिए ये चिंता की बात है, क्योंकि अमेरिका इस जंग में यूक्रेन की मदद कर रहा है. 50 दिनों की जंग में अमेरिका यूक्रेन को अब तक 13 हजार करोड़ की सैन्य मदद भेज चुका है.

आइए जानते हैं क्या है आर्टिफिशियल इंटेलिजेंस और हाइपरसोनिक इंजन कैसे करेगा काम...

□ क्या है आर्टिफिशियल इंटेलिजेंस?

आर्टिफिशियल इंटेलिजेंस कंप्यूटर विज्ञान की वह शाखा है, जो कंप्यूटर के इंसानों की तरह व्यवहार करने की धारणा पर आधारित है. इसके जनक जॉन मैकार्थी हैं. यह मशीनों की सोचने, समझने, सीखने, समस्या हल करने और निर्णय लेने जैसी संज्ञानात्मक कार्यों को करने की क्षमता को सूचित करता है.

□ कब हुई थी इसकी शुरुआत?

आर्टिफिशियल इंटेलिजेंस पर रिसर्च की शुरुआत 1950 के दशक में हुई थी. आर्टिफिशियल इंटेलिजेंस का अर्थ है- कृत्रिम तरीके से विकसित बौद्धिक क्षमता. इसके ज़रिये कंप्यूटर सिस्टम या रोबोटिक सिस्टम तैयार किया जाता है, जिसे उन्हीं तर्कों के आधार पर संचालित करने का प्रयास किया जाता है, जिसके आधार पर मानव मस्तिष्क कार्य करता है.

□ हाइपरसोनिक मिसाइल क्या होते हैं?

हाइपरसोनिक मिसाइलें ऐसी मिसाइलें होती हैं, जिनकी स्पीड साउंड की स्पीड से 5 गुना या उससे ज्यादा तेज होती है. ये मिसाइलें परमाणु हथियार ले जाने में सक्षम और मेनुरेबल टेक्नोलॉजी, यानी हवा में रास्ता बदलने की क्षमता से लैस होती हैं. अंडरग्राउंड हथियार गोदामों को तबाह करने में हाइपरसोनिक मिसाइलें सबसोनिक क्रूज मिसाइलों से ज्यादा घातक होती हैं. डिफेंस एक्सपर्ट्स के मुताबिक, अपनी बेहद हाई स्पीड की वजह से हाइपरसोनिक मिसाइलें ज्यादा विध्वंसक होती हैं.

□ हाइपरसोनिक ग्लाइड व्हीकल क्या है?

हाइपरसोनिक ग्लाइड व्हीकल को एक रॉकेट से लॉन्च किया जाता है। लॉन्च होने के बाद ग्लाइड व्हीकल रॉकेट से अलग हो जाता है और टारगेट की ओर कम से कम मैच 5 की गति से ग्लाइड करता है यानी बढ़ता है

□ रूस ने यूक्रेन पर कब किया हाइपरसोनिक मिसाइलों का इस्तेमाल?

रूस ने कहा है कि उसने 19 मार्च को पश्चिमी यूक्रेन के इवानो-फ्रांकिवस्क इलाके में एक हथियार गोदाम नष्ट करने के लिए अपनी हाइपरसोनिक मिसाइल 'किंझल' का इस्तेमाल किया. 20 मार्च को भी रूस ने दक्षिणी यूक्रेन के माइकोलाइव इलाके में एक फ्यूल डिपो पर दूसरा हाइपरसोनिक मिसाइल हमला किया. जानकारों के मुताबिक, दुनिया में पहली बार किन्हीं दो देशों के बीच लड़ाई में हाइपरसोनिक मिसाइल का इस्तेमाल हुआ है.

□ नासा हाइपरसोनिक मिसाइलों को कैसे अपग्रेड और ऑप्टिमाइज कर रहा?

नासा ने एक हाइपरसोनिक कम्प्यूटेशनल कोड विकसित किया है, जिसे VULCAN-CFD नाम दिया गया है. जिसका नाम आग के रोमन देवता के नाम पर रखा गया है, जो यह बताता है कि हाइपरसोनिक गति पर इंजनों के अशांत वायुप्रवाह में आग कैसे व्यवहार करता है.

□ अमेरिका कब से हाइपरसोनिक मिसाइल बनाने में जुटा है?

अमेरिका 2011 से ही हाइपरसोनिक मिसाइल बनाने में जुटा है और कई मिसाइलों के टेस्ट कर चुका है. लॉकहीड मार्टिन ने हाल ही में अमेरिकी सरकार के साथ हाइपरसोनिक कंवेशनल स्ट्राइक वेपन और AGM-1831 एयर लॉन्चड रैपिड रेस्पॉन्स वेपन बनाने के लिए करार किया है. अमेरिका के पास पहली हाइपरसोनिक मिसाइल के 2023 तक आने की संभावना है. अमेरिका के मुताबिक, पिछले 5 वर्षों में चीन सैकड़ों हाइपरसोनिक मिसाइलों का टेस्ट कर चुका है, जबकि अमेरिका ने ऐसे कुल 9 टेस्ट ही किए हैं.

□ चीन हाइपरसोनिक मिसाइलों में कहां है?

चीन D-17 हाइपरसोनिक मिसाइल बनाने के करीब है. वह 2018 में ही लिंगयुन-1 नामक हाइपरसोनिक मिसाइल का टेस्ट कर चुका है. साथ ही DF-ZF हाइपरसोनिक मिसाइल बनाने के करीब है और स्टैरी स्काई-2 नामक मैक 6 स्पीड (करीब 7000 किमी/घंटे) वाली हाइपरसोनिक मिसाइल का भी टेस्ट कर चुका है.

□ हाइपरसोनिक मिसाइलों के मामले में कहां है भारत?

भारत भी कई वर्षों से हाइपरसोनिक मिसाइल बनाने में जुटा है. DRDO ने 2020 में एक हाइपरसोनिक टेक्नोलॉजी डेमोंस्ट्रेटेड व्हीकल (HSTDV) का सफल परीक्षण किया था. रिपोर्ट्स के मुताबिक, भारत HSTDV का इस्तेमाल करके अपनी हाइपरसोनिक क्रूज मिसाइल बनाने की ओर बढ़ रहा है. साथ ही भारत रूस के सहयोग से ब्रह्मोस-II मिसाइल के विकास में जुटा है, जोकि एक हाइपरसोनिक मिसाइल है. ब्रह्मोस-II की रेंज 1500 किमी तक होगी और स्पीड साउंड से 7-8 गुना ज्यादा (करीब 9000 किमी/घंटे) होगी. इसकी टेस्टिंग 2024 तक होने की उम्मीद है. इनके अलावा फ्रांस, ब्रिटेन जैसे देश हाइपरसोनिक मिसाइल बनाने में जुटे हैं. वहीं नॉर्थ कोरिया भी हाइपरसोनिक मिसाइल बनाने का दावा कर चुका है.

<https://hindi.news18.com/news/world/america-russia-ukraine-war-nasa-applies-artificial-intelligence-to-optimize-new-3800mph-hypersonic-engine-all-you-need-to-know-4200407.html>

Scientists resurrect ancient enzymes to improve photosynthesis

A Cornell University study describes a breakthrough in the quest to improve photosynthesis in certain crops, a step toward adapting plants to rapid climate changes and increasing yields to feed a projected 9 billion people by 2050.

The study, "Improving the Efficiency of Rubisco by Resurrecting Its Ancestors in the Family Solanaceae," published April 15 in *Science Advances*. The senior author is Maureen Hanson, the Liberty Hyde Bailey Professor of Plant Molecular Biology in the College of Agriculture and Life Sciences. First author Myat Lin is a postdoctoral research associate in Hanson's lab.

The authors developed a computational technique to predict favorable gene sequences that make Rubisco, a key plant enzyme for photosynthesis. The technique allowed the scientists to identify promising candidate enzymes that could be engineered into modern crops and, ultimately, make photosynthesis more efficient and increase crop yields.

Their method relied on evolutionary history, where the researchers predicted Rubisco genes from 20-30 million years ago, when Earth's carbon dioxide (CO₂) levels were higher than they are today and the Rubisco enzymes in plants were adapted to those levels.

By resurrecting ancient Rubisco, early results show promise for developing faster, more efficient Rubisco enzymes to incorporate into crops and help them adapt to hot, dry future conditions, as human activities are increasing heat-trapping CO₂ gas concentrations in Earth's atmosphere.

The study describes predictions of 98 Rubisco enzymes at key moments in the evolutionary history of plants in the Solanaceae family, which include tomato, pepper, potato, eggplant and tobacco. Researchers use tobacco as the experimental model for their studies of Rubisco.

"We were able to identify predicted ancestral enzymes that do have superior qualities compared to current-day enzymes," Hanson said. Lin developed the new technique for identifying predicted ancient Rubisco enzymes.

Scientists have known that they can increase crop yields by accelerating photosynthesis, where plants convert CO₂, water and light into oxygen and sugars that plants use for energy and for building new tissues.

For many years, researchers have focused on Rubisco, a slow enzyme that pulls (or fixes) carbon from CO₂ to create sugars. Aside from being slow, Rubisco also sometimes catalyzes a reaction with oxygen in the air; by so doing, it creates a toxic byproduct, wastes energy and makes photosynthesis inefficient.

Hanson's lab had previously tried to use Rubisco from cyanobacteria (blue-green algae), which is faster but also reacts readily with oxygen, forcing the researchers to try to create micro-compartments to protect the enzyme from oxygen, with mixed results. Other researchers have tried to engineer more optimal Rubisco by making changes in the enzyme's amino acids, though little was known about which changes would lead to desired results.

In this study, Lin reconstructed a phylogeny -- a tree-like diagram showing evolutionary relatedness among groups of organisms -- of Rubisco, using Solanaceae plants.

"By getting a lot of [genetic] sequences of Rubisco in existing plants, a phylogenetic tree could be constructed to figure out which Rubiscos likely existed 20 to 30 million years ago," Hanson said.

The advantage of identifying potential ancient Rubisco sequences is that carbon dioxide levels were possibly as high as 500 to 800 parts per million (ppm) in the atmosphere 25 million to 50 million years ago. Today, heat-trapping CO₂ levels are rising sharply due to many human activities, with current measurements at around 420 ppm, after staying relatively constant under 300 ppm for hundreds of millennia until the 1950s.

Lin, Hanson and colleagues then used an experimental system developed for tobacco in Hanson's lab, and described in a 2020 *Nature Plants* paper, which employs *E. coli* bacteria to test in a single day the efficacy of different versions of Rubisco. Similar tests done in plants take months to verify.

The team found that ancient Rubisco enzymes predicted from modern-day Solanaceae plants showed real promise for being more efficient.

"For the next step, we want to replace the genes for the existing Rubisco enzyme in tobacco with these ancestral sequences using CRISPR [gene-editing] technology, and then measure how it affects the production of biomass," Hanson said. "We certainly hope that our experiments will show that by adapting Rubisco to present day conditions, we will have plants that will give greater yields."

If their method proves successful, these efficient Rubisco sequences could be transferred into crops such as tomatoes, as well as those from other plant families, such as soybeans and rice.

The study was funded by the U.S. Department of Energy.

<https://www.sciencedaily.com/releases/2022/04/220418164926.htm>

