समाचार पत्रों से चयित अंश
Newspapers Clippings

दैनिक सामयिक अभिज्ञता सेवा

A Daily Current Awareness Service

रक्षा विज्ञान पुस्तकालय
Defence Science Library
रक्षा वैज्ञानिक सूचना एवं प्रलेखन केन्द्र
Defence Scientific Information & Documentation Centre
मेटकॉफ हाऊस, दिल्ली 110054
Metcalfe House, Delhi-110054

Business Standard

Sun, 14 May, 2017

Defence looking up for L&T

Exports at highest ever, company expects shipbuilding turnaround in next two financial years

Engineering conglomerate Larsen & Toubro (L&T) may finally be scripting its defence story after winning a ~4,500-crore order for self-propelled guns recently.

The current financial year and the next will be significant for the company with an expected new defence manufacturing policy, fresh orders and rising defence exports.

“Over the next five years a sizeable number of orders would have been booked and revenues would have started to grow dramatically,” Jayant Patil, head of defence and aerospace and member of the heavy engineering board of L&T, told Business Standard.

L&T in April signed a contract with Hanwha Techwin of South Korea for execution of the 155mm/52 Cal tracked self-propelled gun programme for the Indian army. “A lot of action is expected this year. Six or seven large programmes of between ~500 crore and ~15,000 crore are expected to be placed with Indian companies to kick off Make in India,” Patil said.

The locally manufactured K9 VAJRA-T opens a long-term revenue stream for L&T through repeat orders and export opportunities, wrote Renu Baid and Nayan Parakh in an IIFL research note.

The new defence procurement policy allows 100 per cent repeat orders, beyond which special approvals are required. “This project, we hope, should see a repeat of the current order,” Patil said.

L&T also stands to gain from the proposed new defence manufacturing policy, which has raised hopes of long-term commitments in certain defence programmes with chosen private domestic manufacturers.

Over the medium term, defence could contribute five-10 per cent of L&T’s order book, according to Baid of IIFL. L&T’s order inflow in OctoberDecember was ~34,890 crore and its order book ~2.58 lakh crore.

“In the last financial year we crossed ~1,000 crore defence order inflow through exports. We see exports growing over the coming years,” Patil said.

L&T is also hopeful its loss-making shipbuilding facility will be out of the red in the next two financial years. L&T is one of two bidders for a landing platform dock contract that is expected to open this year. “Any large naval order will provide a 10-year revenue visibility for the shipbuilding facility,” Baid added.

the pioneer

Sun, 14 May, 2017

INS Darshak completes Hydrographic survey of Lanka’s Weligama Bay

With the objective of forging closer maritime ties with the neighbouring countries, the Indian Navy has carried out the maiden joint hydrographic survey of Sri Lanka’s Weligama Bay and southern coast.

Hydrographic survey data for more than 7,000 nautical miles was collected during a two-month-long exercise and details of the survey were handed over to the Sri Lankan Navy at a ceremony in Colombo on Friday.

Giving details of the survey, Navy spokesman DK Sharma said, here on Saturday, the successful completion of the maiden joint survey with Sri Lanka marks a new beginning in the bilateral relations. He said Indian ship INS Darshak was on a two-month-long deployment in Sri Lanka to carry out the exercise.

Interestingly, Sri Lanka had on Wednesday rejected China's request for its submarine to dock at Colombo next week, after a similar visit in 2014 triggered strong protest from India. China has been making consistent efforts to make inroads into the island nation.

Meanwhile, Sharma said that the survey operations were undertaken in three phases and the ship also visited Colombo and Galle harbour. A Chetak helicopter was also deployed as part of the data collection exercise. The ship and its survey motor boats fitted with multi-beam systems were extensively deployed and the hydrographic survey data for more than 7,000 nautical miles was collected, he added.

Officers onboard the INS Darshak also imparted training on various aspects of hydrographic survey to some Sri Lankan naval officers. Indian Navy conducts these surveys with other littoral countries in the Indian Ocean to enhance the naval capabilities of these nations and foster more robust relations with them.

As part of this endeavour, Navy's frontline missile destroyer INS Rajput paid a three-day visit to Myanmar as part of efforts to boost cooperation between navies of the two countries. During the visit, 35 Indian naval officers visited the Myanmar Naval Training Command. The ship was on an operational turnaround from May 11 to May 13, the spokesman said.

नईदुनिया

Sun, 14 May, 2017

OBOR सम्मेलन आज, भारत करेगा बहिष्कार, कहा- क्षेत्रीय अखंडता की उपेक्षा करता है सीपीईसी

बीजिंग। चीन के रविवार से शुरू हो रहे वन बेल्ट-वन रोड (सिल्क रोड) योजना के सम्मेलन का भारत बहिष्कार करेगा। भारत ने शनिवार देर रात इस आशय की घोषणा कर दी। ऐसा वह इस योजना के अंतर्गत आने वाले चीन-पाकिस्तान इकोनोमिक कॉरीडोर (सीपीईसी) के गुलाम कश्मीर (पाक के कब्जे वाले कश्मीर) से गुजरने के विरोध में कर रहा है। अप्रैल में चीन के विदेश मंत्री वांग ई ने भारत के सम्मेलन में हिस्सा लेने का भरोसा जताया था।

भारत ने अपने बयान में कहा है कि इस मामले में अपनी सैद्धांतिक स्थिति के तहत हम चीन से उसके इस पहल पर सार्थक बातचीत का आग्रह कर चुके हैं। हम चीन की तरफ से सकारात्मक उत्तर की प्रतीक्षा कर रहे हैं। कोई भी देश संप्रभुता और क्षेत्रीय एकता पर उसकी मुख्य चिंताओं को नजरअंदाज करने वाली परियोजना को स्वीकार नहीं करेगा।

राष्ट्रपति शी चिनफिंग के ड्रीम प्रोजेक्ट वन बेल्ट-वन रोड पर चीन दो दिवसीय अंतरराष्ट्रीय सम्मेलन आयोजित कर रहा है। इस प्रोजेक्ट के तहत चीन सड़क, रेल, जल और वायु मार्ग से यूरोप और अफ्रीका से संपर्क बढ़ाएगा। इससे वह दुनिया के सुदूर हिस्सों को अपनी व्यापारिक गतिविधियां से जोड़ेगा, कच्चा और तैयार माल भेजेगा व मंगवाएगा।

चीन ज्यादा देशों की उपस्थिति को सम्मेलन की सफलता से जोड़कर देख रहा है। इसी के चलते वह भारत सहित सभी प्रमुख देशों को सम्मेलन और वन बेल्ट-वन रोड प्रोजेक्ट से जोड़ने की कोशिश कर रहा है। अमेरिका और जापान, चीन के साथ अपने मतभेदों को दरकिनार करते हुए इस सम्मेलन में हिस्सा ले रहे हैं। सम्मेलन में रूसी राष्ट्रपति व्लादिमीर पुतिन समेत 29 देशों के प्रमुख हिस्सा लेंगे।

अमेरिकी विरोध को नकारा

सिल्क रोड योजना पर हो रहे सम्मेलन में चीन सभी देशों के शामिल होने का स्वागत करता है। चीनी विदेश मंत्रालय ने यह बात अमेरिका की उस चेतावनी पर कही है जिसमें सम्मेलन में उत्तर कोरिया के भाग लेने से गलत संदेश जाने की आशंका जताई गई है। फिलहाल अमेरिका इस सम्मेलन में हिस्सा ले रहा है। परमाणु बम और मिसाइल परीक्षण के

मुद्दे पर उत्तर कोरिया और अमेरिका, दक्षिण कोरिया व जापान के बीच इन दिनों तनातनी चरम पर है। संयुक्त राष्ट्र सुरक्षा परिषद ने उत्तर कोरिया पर व्यापक आर्थिक प्रतिबंध लगाए हुए हैं।

दैनिक जागरण

Sun, 14 May, 2017

चीन की वन बेल्ट-वन रोड परियोजना

वैश्विक अर्थव्यवस्था पर अपनी धाक जमाने के लिए चीन द्वारा शुरू की गई वन बेल्ट-वन रोड (ओबोर) का दो दिवसीय सम्मेलन आज से शुरू होने जा रहा है। यह परियोजना सड़क, रेल, जल और वायु मार्ग से 68 देशों को जोड़ेगी। पांच साल में इस परियोजना में 800 अरब डॉलर का निवेश होगा।

68 इतने देशों को जोड़ेगी ये परियोजना

4.4 अरब परियोजना से जुड़ने वाले देशों की आबादी

5 लाख करोड़ डॉलर परियोजना की कुल अनुमानित लागत

40% वैश्विक अर्थव्यवस्था होगी प्रभावित

16 चीन के 27 प्रांतों में से इतने प्रांतों से होकर गुजरेगी यह परियोजना

------ सिल्क रोड इकोनॉमिक बेल्ट ------ सिल्क रोड समुद्री मार्ग

लगेंगे चार दशक

वैसे तो परियोजना 30 से 40 साल में पूरी होगी, लेकिन 2049 में मौजूदा चीन (पीपुल्स रिपब्लिक) अपने सौ वर्ष पूरे करेगा। इस वर्ष को मील का पत्थर बनाने के लिए यह परियोजना इस वर्ष तक पूरी करने का लक्ष्य रखा गया है।

पांच साल में 800 अरब निवेश

2013 से अब तक चीन वन बेल्ट वन रोड परियोजना में 60 अरब डॉलर खर्च कर चुका है। अगले पांच वर्षों में चीनी सरकार इसमें 600 से 800 अरब डॉलर का निवेश कर सकती है। चीन के नेशनल डेवलपमेंट एंड रिफॉर्म कमीशन के मुताबिक 2013 से 2016 के बीच इस परियोजना के तहत चीन में 1.8 लाख नौकरियां पैदा हुईं। चीनी कंपनियों ने 60 अरब डॉलर निवेश किया और सरकार को 1.1 अरब डॉलर का टैक्स भी चुकाया।

आधारभूत संरचनाओं का निर्माण

- चीन से दक्षिणी यूरोप के बीच सड़क मार्ग, जो नीदरलैंड से होकर गुजरेगा।
- चीन के शंघाई बंदरगाह से वेनिस के बीच जल मार्ग जो भारत व दक्षिण अफ्रीका से होकर गुजरेगा।
- इसके साथ बंदरगाह, सड़कें, रेलवे, हवाईअड्डे, बिजली संयंत्र, तेल व गैस की पाइपलाइन, मुफ्त व्यापार क्षेत्र और आईटी व टेलीकॉम क्षेत्र बनाए जाएंगे।
- अंतरराष्ट्रीय ऑडिट कंपनी पीडब्लूसी के मुताबिक 250 अरब डॉलर की कुछ परियोजनाएं पूरी चुकी हैं और कुछ निर्माण के चरणों में हैं। परियोजना की लागत पांच लाख करोड़ रहेगी।

प्रमुख बेल्ट व सड़क परियोजना

1. **मॉस्को-कजान उच्च-गति रेलवे** : मॉस्को से बीजिंग को जोड़ने वाली सात हजार किमी लंबी हाई-स्पीड रेल के लिए पहली लाइन 770 किमी लंबी बिछाई जाएगी।
2. **खोरगोस द्वार** : चीन व कजाख सीमा पर बने कार्गो हब पर सालाना दस लाख कंटेनर उतारे जाएंगे।
3. **तेहरान रेल लाइन** : 2016 में चीन से पहली मालगाड़ी तेहरान पहुंची।
4. **चीन-पाकिस्तान मार्ग** : 46 अरब डॉलर की लागत में प्रस्तावित इकोनॉमिक कॉरीडोर चीन को पाकिस्तान के ग्वादर बंदरगाह से जोड़ेगा।

विरोध भी कम नहीं

- द. चीन सागर में चीनी गतिविधियों को देखते हुए कई देश जल मार्ग के इस रूट के खिलाफ हैं।
- चाइना पाकिस्तान इकोनॉमिक कॉरीडोर (सीपीईसी) के खिलाफ भारत अपना प्रतिरोध जाहिर कर चुका है। यह मार्ग पाक अधिकृत कश्मीर से होकर गुजरेगा जो भारत को मंजूर नहीं है।
- सीपीईसी की सुरक्षा पर भी सवाल उठाए जा रहे हैं क्योंकि यह पाकिस्तान में आतंकी संगठन तालिबान के क्षेत्र से होकर गुजरेगा।

चीन को नफा-नुकसान

आर्थिक

नफा

पड़ोसी देशों के साथ व्यापार बढ़ाने में मदद मिलेगी। उद्योगों के ज्यादा उत्पादन का निर्यात होगा। आधिकारिक मुद्रा रेनमिनबी के अंतरराष्ट्रीय मूल्य को सुधारा जा सकेगा।

नुकसान

एशिया और अफ्रीका के कई देश आर्थिक व राजनीतिक अस्थिरता से गुजर रहे हैं। ऐसे देशों में इस परियोजना पर कोई संकट आने पर पूरी परियोजना के निष्फल हो जाने की आशंका है। विशेषज्ञों के मुताबिक चीन का विदेशी निवेश का पुराना रिकॉर्ड खराब रहा है।

राजनीतिक

नफा

विशेषज्ञों का मानना है कि यह कदम राजनीतिक लक्ष्यों को साधने का चीन का प्रयास है ताकि वह कई देशों से मित्रता कर सके। विशेषज्ञ इसकी तुलना मार्शल प्लान से कर रहे हैं, जिसमें अमेरिका ने द्वितीय विश्व युद्ध के बाद पश्चिमी यूरोप के पुनर्निर्माण में मदद की थी जिसके बाद अमेरिका सुपरपावर बनकर उभरा।

नुकसान

अगर परियोजना सफल हुई तो चीन अमेरिका की जगह सुपरपावर देश बन सकता है। लेकिन इसके विशालता के कारण विशेषज्ञों को इसके असफल होने का खतरा ज्यादा नजर आ रहा है। अगर ऐसा हुआ तो चीन की साख पर बट्टा लग जाएगा।

the pioneer

Sun, 14 May, 2017

Stolen US NSA's cyber weapons invade world

Nearly hundred countries, including India, were hit by what is believed to be the biggest-ever recorded cyberattack that used "cyber weapons" stolen from the US' National Security Agency to lock up computers and hold users' files for ransom. The cyberattack was first reported from Sweden, Britain and France, US media outlets reported.

An increase in activity of the malware was noticed on Friday, security software company Avast reported, adding that it "quickly escalated into a massive spreading". Within hours, over 75,000 attacks have been detected worldwide, the company said. Meanwhile, the MalwareTech tracker detected over 100,000 infected systems over the past 24 hours.

Security researchers with Kaspersky Lab have recorded more than 45,000 attacks in 99 countries, including the UK, Russia, Ukraine, India, China, Italy, and Egypt. In Spain, major companies, including telecommunications firm Telefonica, were infected. The most disruptive attacks were reported in the UK, where hospitals and clinics were forced to turn away patients after losing access to computers. The US Computer Emergency Readiness Team (USCERT) under the Department of Homeland Security said it has received multiple reports of WannaCry ransomware infections in many countries around the world.

The ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. It demands users pay $300 worth of cryptocurrency Bitcoin to retrieve their files, though it warns that the payment will be raised after a certain amount of time. The malware spreads through email. Individuals and organisations are discouraged from paying the ransom, as this does not guarantee access will be restored, the USCERT said.

According to it, ransomware spreads easily when it encounters unpatched or outdated software.

A Microsoft spokeswoman said that the company was aware of the reports and was looking into the situation.

According to The Wall Street Journal, the malware believed to be behind the attacks encrypts data on infected computers and essentially holds it for ransom. "Known as WannaCry or Wanna Decryptor, the so-called ransomware programme homes in on vulnerabilities in Microsoft Windows systems," the daily said.

However, there may be good news as a researcher claimed to have discovered a "kill switch" that can prevent the spread of the ransomware. The researcher tweeting as @MalwareTechBlog, said the discovery was accidental, but that registering a domain name used by the malware stops it from spreading. In a statement, international shipper FedEx said it has been badly hit by the cyber attack.

"Like many other companies, FedEx is experiencing interference with some of our Windows-based systems caused by malware. We are implementing remediation steps as quickly as possible," it said.

"This event should serve as a global wake-up call — the means of delivery and the delivered effect is unprecedented," Rich Barger, the director of threat research at security firm Splunk, said in a separate statement. The Department of Homeland Security (DHS) said it is actively sharing information related to this event and stands ready to "lend technical support and assistance as needed to our partners, both in the United States and internationally".

The DHS has a cadre of cyber security professionals that can provide expertise and support to critical infrastructure entities, it said in a statement. The malware was made available online on April 14 through a dump by a group called Shadow Brokers, which claimed last year to have stolen a cache of "cyber weapons" from the National Security Agency (NSA). At the time, there was scepticism about whether the group was exaggerating the scale of its hack. Whistleblower Edward Snowden blamed the NSA for not preventing the global cyber attack. "Despite warnings, (NSA) built dangerous attack tools that could target Western

software," Snowden said. "Today we see the cost." "If @NSAGov had privately disclosed the flaw used to attack hospitals when they *found* it, not when they lost it, this may not have happened," he said.

Some cyber security experts and privacy advocates said the massive attack reflected a flawed approach by the US to dedicate more cyber resources to offence rather than defence, a practice they argued makes the internet less secure. PTI

THE TIMES OF INDIA

Sun, 14 May, 2017

AUTO COS TO HOSPITALS: NONE SPARED

WHAT IS RANSOMWARE

- The malware shutting down computers worldwide is **known as WannaCry** and variants of that name
- This type of malware is **called ransomware as it first scrambles a victim's files and then demands a payment** to unscramble them

HOW DOES IT WORK

- WannaCry seems to be deployed via a **worm — a programme that spreads by itself** between computers
- Once malware is inside an organisation, **it will find vulnerable machines** and infect them too
- Infections reported in **99 countries, including Russia and China. In UK, hospital systems badly hit**

HOW THE HACKERS STRUCK

- The ransomware **exploits a weakness in Microsoft Windows systems** that was identified by the US National Security Agency and given the name EternalBlue
- But NSA's code was among a cache stolen by a hackers' **group known as The Shadow Brokers**, who then attempted to sell it in an online auction
- The hackers' group later made the tools freely available in April, saying it was a **"protest" about US President Donald Trump**
- Microsoft had by then already released a software upgrade fixing the issue (experts think the **NSA may have tipped Microsoft off**)
- But not all users were prompt in installing the upgrades

HOW THEY FELL FOR IT

- **Cyber extortionists tricked victims** into opening malicious attachments to spam emails that appeared to contain legitimate files
- The ransomware encrypted data on the computers, demanding payments of **$300 to $600** via the digital currency bitcoin to restore access

GOVT AGENCIES/ COMPANIES AFFECTED GLOBALLY

- **Britain's National Health Service (NHS)**
- Russian interior ministry (about 1,000 computers)
- Spain's communications giant Telefonica
- Spain's power firm Iberdrola
- FedEx in the US
- **Japanese carmaker Nissan's plant in England (left)**
- German rail operator Deutsche Bahn
- **French automaker Renault halted production** at several sites in Europe

GLOBAL IMPACT

- A cybersecurity firm said it had seen **75,000** cases of the WannaCry attack
- **Asian nations still assessing impact**, full extent of which may not be known till at least Monday

THE HINDU

Sun, 14 May, 2017

India largely safe from cyberattack

By Yuthika Bhargava

While no major incident of the worldwide ransomware attack has been reported from India so far, Gulshan Rai, the Cyber Security Chief in the PMO, said a better impact assessment would be possible only on Monday when offices open.

The Indian Computer Emergency Response Team (CERT— In), which on Saturday issued an advisory asking organisations to install updates to Windows systems, had, in fact, released a vulnerability note with a "Severity Rating of High" on March 15 for "a possible remote exploitation of this vulnerability." The agency advised that the patch released by Microsoft be applied. Over 70 countries have been hit by the cyberattack.

"We have been checking hundreds of systems since we were alerted to this cyberattack. The attacks seem to be the result of a vulnerability in the Microsoft windows OS, and we released a patch," Mr. Rai told The Hindu . "We understand that systems in Andhra Pradesh are affected, but so far our assessment is that there isn't much impact," he added.

THE HINDU

Sun, 14 May, 2017

Researcher accidentally finds 'kill switch' for cyberattack ransomware

The attacks used a technique known as ransomware that locks users' files unless they pay the attackers a designated sum in the virtual currency Bitcoin.

A cybersecurity researcher appears to have accidentally discovered a "kill switch" that can prevent the spread of the WannaCry ransomware — for now — that has caused the cyberattacks wreaking havoc globally, they told AFP on Saturday.

The researcher, tweeting as @MalwareTechBlog, said the discovery was accidental, but that registering a domain name used by the malware stops it from spreading.

I will confess that I was unaware registering the domain would stop the malware until after i registered it, so initially it was accidental.

"Essentially they relied on a domain not being registered and by registering it, we stopped their malware spreading," @MalwareTechBlog told AFP in a private message on Twitter.

The researcher warned however that people "need to update their systems ASAP" to avoid attack.

"The crisis isn't over, they can always change the code and try again," @MalwareTechBlog said.

Friday's wave of cyberattacks, which affected dozens of countries, apparently exploited a flaw exposed in documents leaked from the U.S. National Security Agency.

The attacks used a technique known as ransomware that locks users' files unless they pay the attackers a designated sum in the virtual currency Bitcoin.

Affected by the onslaught were computer networks at hospitals in Britain, Russia's interior ministry, the Spanish telecom giant Telefonica and the US delivery firm FedEx and many other organisations.

French carmaker Renault also announced it was attacked. A spokeswoman said the company was "doing what is needed to counter this attack."

Unfortunately however, computers already affected will not be helped by the solution. So long as the domain isn't revoked, this particular strain will no longer cause harm, but patch your systems ASAP as they will try again. The malware's name is WCry, but analysts were also using variants such as WannaCry.

Global scope

Forcepoint Security Labs said in a Friday statement that the attack had "global scope" and was affecting networks in Australia, Belgium, France, Germany, Italy and Mexico. In the United States, FedEx acknowledged it had been hit by malware and was "implementing remediation steps as quickly as possible."

Also badly hit was Britain's National Health Service, which declared a "major incident" after the attack, which forced some hospitals to divert ambulances and scrap operations. Pictures posted on social media showed screens of NHS computers with images demanding payment of $300 (275 euros) in Bitcoin, saying: "Ooops, your files have been encrypted!"

It demands payment in three days or the price is doubled, and if none is received in seven days, the files will be deleted, according to the screen message. A hacking group called Shadow Brokers released the malware in April claiming to have discovered the flaw from the NSA, according to Kaspersky Lab, a Russian cybersecurity provider. Kaspersky researcher Costin Raiu cited 45,000 attacks in 74 countries as of Friday evening.

THE HINDU

Sun, 14 May, 2017

NASA not taking humans on first flight of new rocket

Feasibility studies rule out the idea

NASA has dropped the idea of putting astronauts aboard the first integrated flight of the Space Launch System rocket and Orion spacecraft - Exploration Mission-1 (EM-1).

This is the first in a broad series of exploration missions that plans to take humans to deep space, and eventually to Mars.

NASA's original plan was to launch the test flight without crew, but in February, reportedly at the request of the Donald Trump administration, NASA began an effort looking at the feasibility of putting crew aboard EM-1.

"After weighing the data and assessing all implications, the agency will continue pursuing the original plan for the first launch, as a rigorous flight test of the integrated systems without crew," NASA said in a statement on Saturday.

However, engineers will apply insights gained from the effort to the first flight test and the integrated systems to strengthen the long-term push to extend human presence deeper into the solar system.

NASA determined it is technically capable of launching crew on EM-1, but after evaluating cost, risk and technical factors in a project of this magnitude, it would be difficult to accommodate changes needed to add crew at this point in mission planning.

The effort confirmed that the baseline plan to fly EM-1 without crew is still the best approach to enable humans to move sustainably beyond a low-Earth orbit.

"We appreciate the opportunity to evaluate the possibility of this crewed flight," NASA acting Administrator Robert Lightfoot said.

"The bipartisan support of Congress and the President for our efforts to send astronauts deeper into the solar system than we have ever gone before is valued and does not go unnoticed. Presidential support for space has been strong," Lightfoot added.