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

THE TIMES OF INDIA

Mon, 15 May, 2017

New agency to push arms buys, production

By Rajat Pandit

Govt to Set Up Specialised Def Procurement Organisation

India does not get enough bang for its buck in the arms business. With this in min d, the defence ministry is now looking to create a specialised defence procurement organisation (DPO) to streamline mega arms acquisitions as well as leverage them to build a robust defence industrial base (DIB) in the country.

Defence ministry sources said creation of the DPO as "a strategic imperative for longterm self-reliance" would be the second big-ticket defence reform to be set in motion after the "strategic partnership (SP)" policy is finalised to boost the private sector's role in defence production.

The SP policy, under which select Indian private sector companies will be nominated to jointly produce weapons systems with global armament companies, is slated for discussion in the defence acquisitions council (DAC) meeting to be chaired by defence minister Arun Jaitley on Monday , as was earlier reported by TOI.

"Once the SP policy is hopefully cleared this month, the focus will shift to setting up the DPO. Jaitley has already received detailed presentations on the DPO, whose main aim will be to use India's arms procurement clout to build a strong DIB," said a source.

The "professional and empowered" DPO, which was recommended by the Pritam Singh committee, will "amalgamate" what the defence ministry currently does in "a fragmented and isolated manner" by integrating the longwinded and cumbersome arms acquisitions, offsets, defence production and other such processes.

"Vested with some autonomy , the DPO will function as the powerful executive arm of the defence minister-led DAC.After the DPO is approved by the Cabinet, it will take around two years to take full shape. It will also have legal, costing and contracting experts, who are largely missing in the existing system," he said.

India still acquires 65% of its military hardware and software from abroad, which not only places it in a strategically vulnerable position, but also ensures its enduring and embarrassing tag of being the world's largest arms importer.

This is primarily due to the sloppy performance of DRDO and its 50 labs, five defence PSUs, four shipyards and 41 ordnance factories as well as the failure to enthuse the private sector to enter defence production in a major way over the years.

The Modi government, after it came to office in May 2014, launched a major `Make in India' drive in the defence production sector but it's yet to translate into anything concrete on the ground.“There has been some improvement with the new Defence Procurement Procedure giving top priority to the new indigenous design, development and manufacturing (IDDM) category . We hope the SP policy and DPO, working in conjunction, will catalyse the defence-industrial ecosystem in the country,“ said the source.

THE ASIAN AGE

Mon, 15 May, 2017

‘Technology transfer key to defence tieup’

DAC likely to take up strategic partnership issue today

New Delhi: The degree of willingness to engage in transfer of technology (ToT) will be the main criteria in deciding whether a foreign defence company can qualify to partner an Indian company to manufacture military equipment under the long-awaited strategic partnership (SP) model, the government has said in a power-point presentation made to Indian defence industry honchos behind closed-doors on Thursday.

“ToT remains the main factor in selection of the OEM,” says the presentation on the planned guidelines to select strategic partners, comprising Indian military equipment making companies and foreign OEMs. The foreign defence company will then be the designated original equipment manufacturer (OEM) to pair the Indian strategic partner.

The presentation, titled “Revitalising Defence Industrial Ecosystem”, made by an Indian Navy officer was part of a 90-minute-long interaction between the government team led by defence minister Arun Jaitley and Indian defence industry officials. The SP model issue is now expected to be taken up in the Defence Acquisition Council meeting on Monday.

In evaluating ToT, the considerations will include “range, depth and scope of technology transfer offered in identified areas, extent of indigenous content proposed, extent of eco-system of Indian vendors/ manufacturers proposed, measures to support SP in establishing system for integration of platforms, plans to train skilled manpower, and extent of future research and development planned in India,” the presentation said.

Other critical criteria that will be considered will be the willingness of the foreign company to help develop an ecosystem in India.

In the PP presentation, only four segments — single engine fighter aircraft, helicopters, submarines and armoured fighting vehicles/main battle tanks — have been identified leaving out the fifth segment — ammunition and macro process management of issues — that found mention in the earlier government documents.

However, the presentation points out that the defence ministry may “add more segments or subdivide the existing ones as the SP model matures”.

While six strategic partners will be shortlisted from among Indian companies for each segment, preferably two or more OEMs would be shortlisted for each segment. And “even if one OEM is shortlisted, the process will be taken forward”.

Finally, only one strategic partner will be selected per segment to maintain focus on core areas.

"One potential SP can engage with any or all OEMs, but finally submit only one offer in collaboration with any one of the shortlisted OEMs," the presentation said.

Besides the technical and financial requisites, aspects like "wilful default, debt restructuring and non-performing assets" will be considered while selecting the strategic partner. In the final run, the selection will be based on a combination of price bids and segment specific capabilities of the companies.

While the defence ministry will undertake the process to select strategic partners and OEMs in each segment separately, both will be undertaken concurrently.

The SP model is a government-led effort to persuade broader participation of the private sector in defence manufacturing under the "Make in India" framework in order to ensure greater self-reliance and dependability of supplies essential to meet national security objectives.

Mon, 15 May, 2017

Indian warships in Malaysia to step up maritime cooperation

Two warships of the Indian Navy on Sunday reached Malaysia on a six-day visit as the force aims to further deepen bilateral maritime cooperation including effectively containing piracy in the Indian Ocean Region.

The ships — INS Shivalik and INS Jyoti — are part of an overseas deployment to the South East Asia and Southern Indian Ocean in sync with India's 'Act East Policy'.

"The visit of the Indian Naval Ships seeks to underscore India's peaceful presence and solidarity with friendly and harmonious countries towards ensuring good order in the maritime domain and to strengthen existing bonds between India and Malaysia," Navy Spokesperson Capt DK Sharma said.

Indian naval assets have been increasingly deployed in recent times to address the main maritime concerns of the region. In addition, as part of the Indian Government's vision of SAGAR (Security and Growth for All in the Region), the Indian Navy has also been involved in assisting countries in the Indian Ocean Region with surveillance of the exclusive economic zones, search and rescue operations and other capacity-building and capability-enhancement activities.

Mon, 15 May, 2017

Nearly 1,000 evacuated from Rajouri after Pak resorts to heavy shelling

So far, three relief camps have been made operational and 28 others notified in wake of expected migration from affected villages

Jammu: Pakistani army violated the ceasefire along the Line of Control (LoC) in Rajouri sector of Jammu and Kashmir early on Sunday, damaging buildings and forcing the evacuation of nearly 1,000 border dwellers, following which Indian troops 'retaliated strongly'.

Around 6.45am, the Pakistani troops started shelling using long-range 82 mm and 120 mm mortars, besides firing from small arms and automatic weapons, defence spokesperson Lt Colonel Manish Mehta said, adding Indian army posts retaliated strongly.

This is the fourth ceasefire violation by Pakistan in four days and the second in Rajouri district in two days.

Rajouri deputy commissioner Shahid Iqbal Choudgary said fresh a ceasefire violation has been reported in Chitibakri area of Chingus in Rajouri.

“More than seven villages have been affected,” he said.

Police and district officials evacuated 996 people from areas along the Line of Control to relief camps.

Fifty one schools in Nowshera sector have been closed for an indefinite period while 36 in Manjakote and Doongi zones have been closed for three days, affecting 4,600 students, he added.

At least two civilians, including a minor girl, were killed and nine people, including four solmills diers, were injured on Saturday as Pakistan pounded 35 villages and Indian posts with mortars along the LoC in Rajouri.

So far, three camps have been made operational and 28 others notified in wake of expected migration from affected villages, Choudhary said.

“Six ambulances have been pressed into action for shifting of injured and treatment. One mobile medical unit was stationed at Nowshera and another deputed to forward areas,” the deputy commissioner said.

Around 120 officers from various departments have been deployed to organise facilities at relief camp.

The district administration has provided immediate relief and financial assistance to the kin of the deceased and to the injured, he said.

A control room has been established in the office of SDM Nowshera for coordination.

THE ECONOMIC TIMES
WWW.ECONOMICTIMES.COM

Mon, 15 May, 2017

India Skipping OBOR Meet a Strategic Move

By DipanjanRoy Chaudhury

One Belt One Road Encompasses South Asia Sans India, Bhutan: In its current form, initiative has no less implications than China-Pakistan Economic Corridor

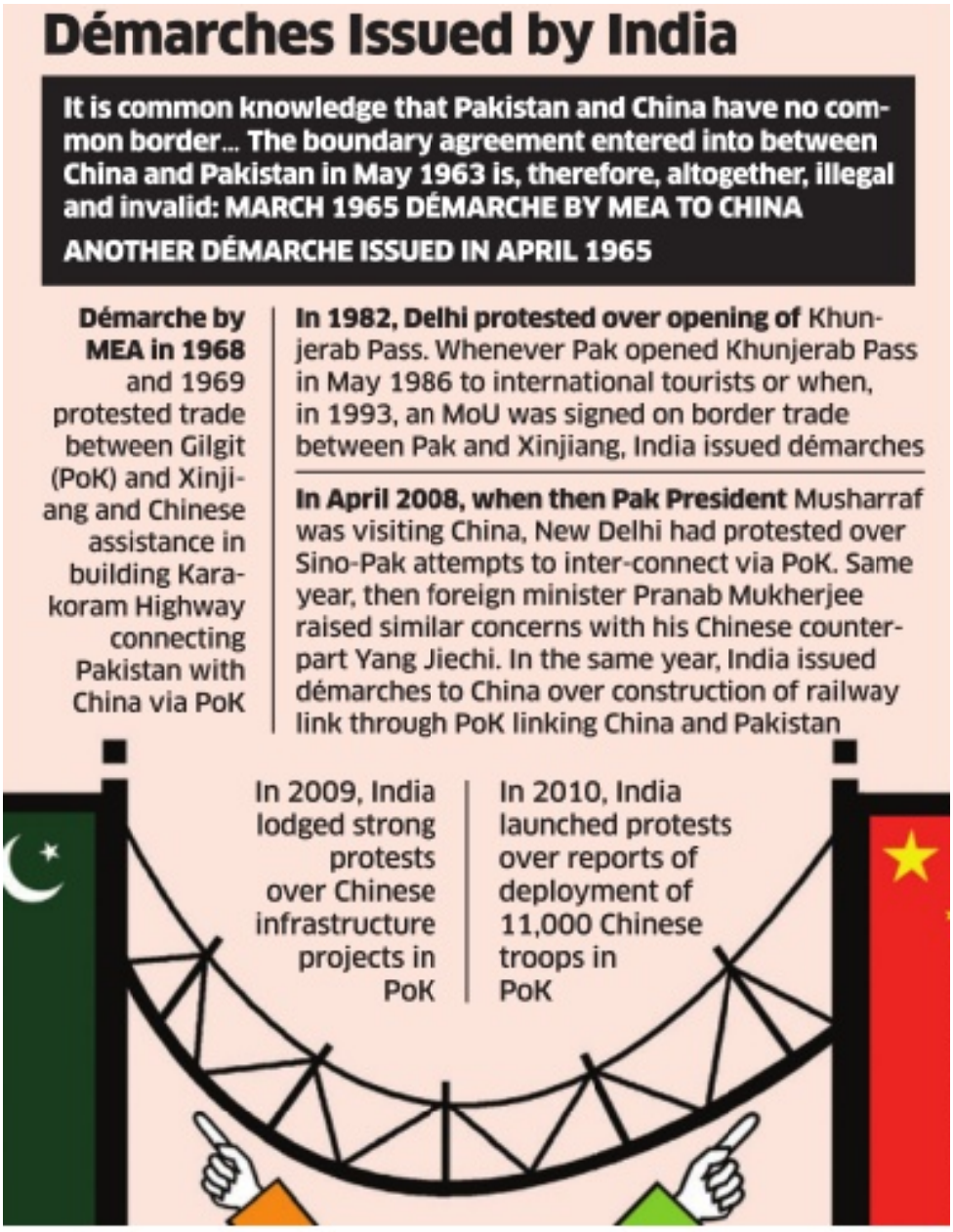
New Delhi has been issuing strong demarches to Beijing since 1961

India's decision to skip the May 14-16 One Belt One Road (OBOR), or Belt and Road Initiative (BRI), Summit in Beijing is a strategic call with the mega connectivity initiative in its current form having no less implications than the ChinaPakistan Economic Corridor.

OBOR encompasses all of South Asia sans India and Bhutan, and enhances China's strategic heft in the same countries where India also has huge stakes, including in connectivity initiatives and infrastructure projects launched in the past three years.

Beijing, people familiar with OBOR said, did not take Delhi into confidence when it decided to implement projects in South Asian countries. Such projects have strategic implications for New Delhi during times of conflict, according to an insider . India, in keeping with its principle of taking local sentiments on board, is also in the process of implementing several connectivity initiatives, both through bilateral as well as sub-regional groups -such as the Bangladesh-Bhutan-India-Nepal Motor Vehicles Agreement and the Bay of Bengal Initiative for MultiSectoral Technical and Economic Cooperation. Also, the Chabahar Port project and the International North South Transportation Corridor are likely to enhance India's footprints in Russia, Central Asia, Iran, Afghanistan and Europe.

ET has learnt that India has been issuing strong demarches to Beijing since 1961 at each and every stage of Chinese engagement with PoK. The first such demarche was issued by the Indian Ambassador to China one year before the 1962 Sino-Indian War.Subsequent communications were issued in 1963, 1965, 1968, 1969, 1982, 1983 and protests were continuously registered since 2008 when China and Pak agreed to construct the first mega infrastructure project in PoK.



THE ECONOMIC TIMES
WWW.ECONOMICTIMES.COM

Mon, 15 May, 2017

No Desire to Impose Our Will on Others: Chinese Prez

Chinese President Xi Jin ping pledged $124 billion on Sunday for his new Silk Road plan to forge a path of peace, inclusiveness and free trade, and called for “the abandonment of old models based on rivalry and diplomatic power games“. Speaking before an audience that included Russian President Vladimir Putin, Xi said his government has “no desire to impose our will on others".

But he called for “economic integration" and cooperation on financial regulation, antiterrorism and security - fields in which China's heft as the world's No. 2 economy would make it a dominant player. A total of 29 world leaders are attending the two-day meet, but attendee countries continue to be sceptical of China's final goal. Putin called for further negotiations on the project. -OPB

THE HINDU

Mon, 15 May, 2017

Alert sounded on malware

IT Ministry asks stakeholders to protect digital payments ecosystem

The IT Ministry has reached out to key stakeholders like RBI, National Payments Corporation of India, NIC and UIDAI (Aadhaar) to advise them to protect their systems against 'WannaCry' ransomware to ensure that the digital payments ecosystem in the country is protected.

The Ministry of Electronics and Information Technology has also instructed cyber security unit CERT-In to gather information of 'WannaCry' ransomware that has wreaked havoc across sectors like healthcare and telecommunications in more than 100 countries.

Over the weekend, the ransomware hit systems in over 100 countries, including Russia and the U.K., in one of the most widespread cyber attacks in history. It infected computers running on older versions of Microsoft operating systems like XP, locking access to files on the computer.

The cyber criminals have demanded a fee of about $300 in crypto-currencies like Bitcoin for unlocking the device.

Security patch

Microsoft has introduced a security patch to tackle the situation, and consumers across the globe have been advised to download the solution at the earliest.

Noting that no reports have been formally received so far related to the ransomware attack, MeitY said a few systems of the Police Department in Andhra Pradesh were impacted and that the State government has been informed to follow the advisory by the Indian Computer Emergency Response Team (CERT-In).

"MeitY is keeping a close watch on the developments on the ransomware and is working in close coordination with all relevant agencies," it said in a statement. The Ministry has also reached out to the Department of Telecom to alert internet service providers to secure their networks.

Besides, it has also requested Microsoft India to inform all its partners and customers to apply the relevant patches.

In Spain, major companies including telecommunications firm Telefonica have been 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 HINDU

Mon, 15 May, 2017

Defying warnings, North Korea fires yet another missile

The weapon, which experts say may represent a new missile with a long range, flew 700 km and landed 97 km south of Russia's Vladivostok region.

North Korea, defying calls to rein in its weapons programme, fired a ballistic missile that landed in the sea near Russia on Sunday, days after a new leader in South Korea came to power pledging to engage Pyongyang in dialogue.

The U.S. military's Pacific Command said it was assessing the type of missile that was fired but it was "not consistent with an intercontinental ballistic missile". The U.S. threat assessment has not changed from a national security standpoint, a U.S. official said.

Japanese Defence Minister Tomomi Inada said the missile could be a new type. It flew for 30 minutes before dropping into the sea between North Korea's east coast and Japan. North Korea has consistently test-fired missiles in that direction.

Call for sanctions - A U.S. official, speaking on condition of anonymity, said the missile landed 97 km south of Russia's Vladivostok region, prompting the White House to reference Moscow in a statement about the incident. "With the missile impacting so close to Russian soil in fact, closer to Russia than to Japan the President cannot imagine that Russia is pleased," the White House said, referring to U.S. President Donald Trump. The launch served as a call for all nations to implement stronger sanctions against North Korea, it added. North Korea is widely believed to be developing an intercontinental missile tipped with a nuclear weapon that is capable of reaching the United States. Mr. Trump has vowed not to let that happen.

The missile flew 700 km and reached an altitude of more than 2,000 km, according to officials in South Korea and Japan, further and higher than an intermediate-range missile North Korea successfully tested in February from the same region of Kusong, northwest of its capital, Pyongyang.

An intercontinental ballistic missile is considered to have a range of more than 6,000 km. Experts said the altitude reached by the missile tested on Sunday meant it was launched at a high trajectory, which would limit the lateral distance it travelled. But if it was fired at a standard trajectory, it would have a range of at least 4,000 km, experts said. Kim Dong-yub of Kyungnam University's Institute of Far Eastern Studies in Seoul said he estimated a standard trajectory would give it a range of 6,000 km. "The launch may indeed represent a new missile with a long range," said Jonathan McDowell of the Harvard Smithsonian Center for Astrophysics, referring to the estimated altitude of more than 2,000 km. "It is definitely concerning."

THE HINDU

Mon, 15 May, 2017

North Korea missile launch a challenge for South's new leader

North Korea's missile test on Sunday, which Tokyo said could be of a new type of missile, is a direct challenge to the new South Korean president and comes as U.S., Japanese and European navies gather for joint war games in the Pacific. David Wright, co-director of the Global Security Program at the Union of Concerned Scientists, said the launch may have been of a new mobile, two-stage liquid-fuelled missile North Korea displayed in a huge April 15 military parade.

South Korea, Japan and the U.S. swiftly condemned the launch, which jeopardises new South Korean leader Moon Jae-in's willingness for dialogue with the rival North.

"The President expressed deep regret over the fact that this reckless provocation... occurred just days after a new government was launched in South Korea," said senior presidential secretary Yoon Young-chan. "The President said we are leaving open the possibility of dialogue with North Korea, but we should sternly deal with a provocation to prevent North Korea from miscalculating."

Russia concerned - Speaking in Beijing, Dmitry Peskov, Russian President Vladimir Putin's spokesman, told reporters Putin and Chinese President Xi Jinping had discussed the situation on the Korean peninsula, including the latest missile launch, and expressed "mutual concerns" about growing tensions.

Japanese Prime Minister Shinzo Abe told reporters that the launch was "absolutely unacceptable" and that Japan will respond resolutely. Japan's Foreign Minister Fumio Kishida said he and his South Korean counterpart agreed that "dialogue for dialogue's sake with North Korea is meaningless".

North Korea's past satellite rocket launches have been called clandestine tests of ICBM technology, but it is not believed to have tested a true intercontinental ballistic missile yet. The U.S. has called North Korean ballistic and nuclear efforts unacceptable and has swung between threats of military action and offers to talk as it formulates a policy. The North's state media said on Saturday that the nation will bolster its nuclear capability unless the United States abandons its hostile policy.

The launch also comes as troops from the U.S., Japan and two European nations gather near Guam for drills that are partly a message to North Korea. The *USS Carl Vinson*, an aircraft supercarrier, is also engaging with South Korean navy ships in waters off the Korean Peninsula, according to Seoul's Defence Ministry.

Mr. Moon, the first liberal leader in Seoul in nearly a decade, said as he took his oath of office that he'd be willing to visit the North if the circumstances were right. Mr. Trump has also said he'd be "honoured" to talk with leader Kim Jong-un under favourable conditions. On Saturday, a top North Korean diplomat in charge of U.S. relations, Choe Son-hui, told reporters in Beijing that Pyongyang would be willing to meet with the Trump administration for negotiations "if the conditions are set." She did not elaborate.

hindustantimes

Mon, 15 May, 2017

N Korea fires missile, US calls for tougher sanctions

Washington: US President Donald Trump called for tougher sanctions against North Korea after it tested an intermediate range ballistic missile on Sunday. He also sought to provoke a response out of Moscow by saying the projectile landed closer to Russia than Japan, the usual target of Pyongyang's belligerence.

The missile travelled farther than any tested successfully by North Korea and was the first after the election of a new president in South Korea, Moon Jae-in, who has favoured engagement with Pyongyang and has said he is willing to travel there if circumstances are right.

It rose to a height of about 1,240 miles, according to the Japanese defence ministry, and between 435 and 500 miles from the launch site. Experts told The Wall Street Journal that if launched at the conventional angle, it could have travelled 2,800 miles, far enough to reach a US military base in Guam.

But it was Russia that the president had in mind, as the White House statement showed: "With the missile impacting so close to Russian soil – in fact, closer to Russia than to Japan – the President cannot imagine that Russia is pleased." The statement went on to reiterate America's "ironclad commitment to stand with our allies in the face of the serious threat posed by North Korea" and call for "all nations to implement far stronger sanctions against North Korea".

The reference to Russia was seen as an attempt to manipulate Moscow to say or do more, in continuation with Trump's effort to first outsource the problem with North Korea to its strongest ally and patron China. Trump has said he would like Beijing to use its "considerable influence" over North Korea to deal with Kim Jong-Un, adding, as a possible motivator the threat of United States prepared to act unilaterally if needed.

The Russian defence ministry said in a statement that the North Korean missile "didn't pose any danger" to Russia, according to the Russian news agency Interfax, as it landed a "significant" distance from the coast.

The ministry said in the statement the early warning system had tracked the "ballistic target" "for 23 minutes before it fell into the central part of the Sea of Japan, some 500 km from the territory of Russia".

The Indian EXPRESS

Mon, 15 May, 2017

WannaCry ransomware: Everything to know about the global cyberattack

By Nandagopal Rajan

WannaCry, a crypto-ransomware that is also called WannaCrypt, affected at least 45,000 computers in the world

The worst ransomware attack the world has ever seen has just been thwarted, or so it might seem, with a $10 web domain. WannaCry drove thousands to tears around the globe, and held out a stark warning about the vulnerabilities of our digital, inter-connected, existence.

What exactly happened?

WannaCry, a crypto-ransomware that is also called WannaCrypt, affected at least 45,000 computers spread over 74 countries, including India, on Friday. The WanaCrypt0r 2.0 bug encrypts data on a computer within seconds and displays a message asking the user to pay a ransom of $ 300 in Bitcoins to restore access to the device and the data inside. Alarmingly, the attack also hit the National Health Service of the United Kingdom, stalling surgeries and other critical patient care activity across the British Isles, and making confidential patient information and documents inaccessible.

But what is ransomware? How is it different from other malicious software?

There are many types of malware that affect a computer, ranging from those that steal your information to those that just delete everything on the device. Ransomware, as the name suggests, prevents users from accessing their devices and data until a certain ransom is paid to its creator. Ransomware usually locks computers, encrypts the data on it and prevents software and apps from running.

How was the attack ultimately brought under control? What could potentially have happened otherwise?

The attack was brought under control by an "accidental hero", a security researcher who wants to be identified only as MalwareTech, who discovered a hard-coded security switch in the form of a link to a nonsensical domain name. He bought the domain name for $10.69, and this triggered thousands of pings from affected devices, thus killing the ransomware and its spread. If this had not been discovered, millions of computers worldwide could theoretically have been locked within a few days, affecting all kinds of services globally. Within hours of this attack, many surgeries were reported to have been put off, x-rays cancelled, and ambulances called back — just in the UK, where at least 40 hospitals under NHS were affected. It had been long feared that an attack of this nature could bring public utilities or transport systems to a halt, forcing the government to pay a huge ransom to normalise services — for a few hours on Friday, that day appeared to have arrived.

Who was behind the attack and what was their motivation?

It isn't known yet. However, it is widely accepted that the hackers used the 'Eternal Blue Hacking Weapon' created by America's National Security Agency (NSA) to gain access to Microsoft Windows computers used by terrorist outfits and enemy states. Since over a thousand computers in the Russian Interior Ministry, as well as computers in China, were hit, some of the state- or quasi-state actors suspected of carrying out largescale break-ins of computer systems in the United States will, on this occasion, start as not being immediate suspects. Interestingly, the NSA tool was stolen in April by a group called Shadow Broker, who seemed unhappy with US President Donald Trump, whom they said they had voted for.

How secure are Indian databases such as banks or UID (Aadhaar)?

The attack was specifically targeted at Microsoft Windows devices. Microsoft claims it "released a security update which addresses the vulnerability that these attacks are exploiting" in March itself, and advised users to update their systems in order to deploy the latest patches. However, in India, where most official computers run Windows, regular updates might not be a habit, and hence the vulnerability could be very high. A lot of personal data online are now connected to the Aadhaar data of over a billion Indians. Pradipto Chakrabarty, Regional Director, CompTIA India, said that the linking of Aadhaar to bank accounts, income-tax and other sensitive information increases the "threat surface". "Since the user's bank account is linked with his Aadhaar number, the ransomware can potentially lock down the account and make it unusable unless a ransom is paid," Chakrabarty said. Amit Nath, Head of Asia Pacific, Corporate Business, at F-Secure Corporation, said the success of the WannaCry ransomware attack could give hostile nation states a reason to create cyber weapons where there's no hope of ever recovering the data. "That's the worst case scenario," Nath said.

Given the manifest vulnerabilities of the digital age, what, if anything, can you do to protect yourself?

A post attributed to Phillip Misner, Principal Security Group Manager, Microsoft Security Response Center, said some of the attacks were using "common phishing tactics" like malicious attachments, and asked users to

be cautious while opening attachments. The least you can do is stop clicking links that you don't trust, and stop downloading software from unknown sources.

F-Secure highlights the need for a four-phase approach to cybersecurity: Predict, Prevent, Detect, and Respond. Predict by performing an exposure analysis; prevent by deploying a defensive solution to reduce the attack surface; respond by determining how a breach happened and what impact it had on systems; and detect by monitoring infrastructure for signs of intrusion or suspicious behaviour.

THE HINDU

Mon, 15 May, 2017

IIT Bombay gives a leg-up to thermal imaging technology

By Jayant Sriram

Develops India's first infrared sensors

Night-vision devices like goggles or telescopes are a key part of modern military and security operations. Whether you've seen them in movies or television shows or read about them in novels, the concept has been around for a number of years. What is less known, perhaps, is that while the Indian Army relies heavily on these devices for a range of operations, they have never been produced indigenously.

A team of scientists from IIT-Bombay has now made a key breakthrough in developing India's first infrared sensors for thermal imaging. The research started in 2010, with funding from the Defence Research and Development Organisation. The details of the work have been published in the prominent journal Current Science in April 2017.

Multiple applications

The technology, the scientists say, can be used for a range of applications such as night vision, surveillance and — going beyond military and security operations — even in the detection of cancers.

"The successful development and demonstration of indigenous infrared sensors to image human objects is a major milestone for the Indian scientific community," says Subhananda Chakrabarti, of IIT-B's department of electrical engineering, where the infrastructure for creating the sensor was developed.

In an air-conditioned room in the department, Prof. Chakrabarti and his team are able to use the sensor to capture startlingly clear images of human subjects, even when the room is in complete darkness. The sensor captures the thermal signature emanated by a subject and is accurate to the point of picking up minor temperature differences: put your hand on a cold surface for two seconds for instance, and that spot on your palm registers darker on the camera.

"This will make the indigenous thermal imaging or night vision technology affordable and cheaper and will serve as a perfect example of Made In India. This project could, perhaps, be the first significant development in the push for indigenous military equipment production. According to Prof. Chakrabarti, the DRDO spends about Rs. 1,000 crore per year on importing night-vision devices for Indian soldiers and has been searching for an indigenous solution for over two decades.