समाचार पत्रों से चयित अंश
Newspapers Clippings

दैनिक सामयिक अभिज्ञता सेवा

A daily Current Awareness Service

Vol. 42 No. 169 05 December 2017

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

the pioneer

Tue, 05 Dec, 2017

Imported Fighters: Forlorn IAF

By Abhijit Bhattacharyya

Can the retired IAF fleet be replenished by suitable replacement?

Theoretically. But in reality, a delusion as successive rulers have set precedent. Discuss. Doubt. Delay and denude the force

From the beginning of 1947, the Indian Air Force (IAF) is a battleground of dual connotations owing to its 100 per cent foreign origin assets. Thus, alphabet "I", though implying "Indian", could also be "I for Imported", thereby being referred to as "Imported Air Force." That certainly cannot give any pleasure to Indians. Before moving further, therefore, it must be remembered that whereas the need/assessment of/for quality, quantity and type of combat aircraft is planned, proposed, projected by institutional procedure of IAF, all decisions of import are taken by the civil administration of the incumbent Government.

Let us, therefore, see where IAF stands, banking on authentic open source info. According to Jane's *World Air Forces-2017* (page 254-269): In March 2016, then Vice Chief of IAF (now Chief) stated publicly that "our numbers are not adequate to fully execute an air campaign in a two-front scenario…..The squadrons are winding down." It further reported: "With the exception of Sukhoi-30 MKI, which experienced serviceability problems, notably engine failure — IAF assets are ageing and it is essential that the inventory is speedily refurbished, upgraded, or as preferred by IAF, replaced type by type." Foreigners are more concerned, and aware, of IAF plight.

The perilous fallout of the Indian establishment's traditional procrastination and complacency was severely criticised by the Parliamentary Standing Committee on Defence which "expressed concern over IAF's decreasing squadron strength and noted in December 2014 that 'shockingly', Pakistan Air Force has 26 squadrons of operational combat fleet" and that "the country's security requirements are being compromised by ignoring consistently widening gap between sanctioned and existing strength." The Indian Parliament verdict: "Security requirements being compromised."

It further came to light that a "substantial number of MiG fighters (most MiG-21s, all MiG-23 interceptors, MiG-25 Reconnaissance) have retired" and "Parliamentary Standing Committee on Defence" report stated that "14 squadrons of MiG-21 and MiG-27 will retire by 2024." The alarming scenario is, in effect, "11 existing squadrons will remain, which are likely to be joined by 13 Sukhoi-30 squadrons by 2020. Therefore, only 24 squadrons are expected to be operational by 2020, unless substantial orders are placed for more Sukhoi-30s." IAF sanctioned strength of 42 squadron becomes 24 squadron? How far is 2020? In less than 36 months, the "theoretical 42 squadron IAF" will turn into a "ground reality of 24"? Can the retired IAF fleet be replenished by suitable replacement? Yes, theoretically. But in reality, a grandeur of delusion as successive past rulers have set precedent. Discuss. Debate. Doubt. Delay and denude the force, crying for deployment. The IAF is professional, not politicised. Hence they are warning of a two-front threat/war. Do rulers know how to thwart?

Indeed, the cumulative effect of past wrongs appear to have piled up so adversely that human resources, too, appear contaminated. Thus, "in April 2015, a report tabled by the Parliamentary Standing Committee on Defence stated that IAF is facing a crisis in fighter pilot numbers that is almost as serious as that facing its combat fleet, with a fighter aircraft to pilot ratio of 1:0.81 (Pakistan's ratio is 1:2.5 and the United States is 1:2)." According to the world air force almanac, "In March 2015 it was claimed that the IAF officer shortage was only 152, but this apparently small deficiency can be attributed to the fact that the number of squadrons has fallen, and thus, on paper, the authorised establishment strength has followed suit. It is estimated that a more realistic figure of pilot shortage is about 600…..mid-2016." True or untrue, no alarm bells are ringing.

Can't we see the monumental negligence by/of ruling class and gross neglect of forces? Can the civilian rulers escape "irresponsibility" or "unaccountability?" Have we forgotten humiliation of Indian Army in October/November 1962? Do we recall names of "guilty men of 1962?" Hope history does not repeat itself.

In this scenario, can one then blame the public statement of then Air Chief in February 2016 that "Rafale has been selected as L1 (lowest bidder). It is a replacement. It is important that we have the medium multi-role combat aircraft (MMRCA) and we need to have it in the quickest possible time." That for "MMRCA and Sukhoi-30, the requirements are slightly different. And they have their own capabilities. They complement each other but do not replace each other."

In fact, any sensible observer, with functional antenna, will tell the reality quoting open source information-index. Thus, in May 2016, it was reported in Parliament that there were "34 occasions between April 01, 2014 to March 31, 2016 when the Sukhoi-30 MKI aircraft were forced to land on single engine due to mid-air engine problems."

To make matters worse for IAF, even the plan to acquire 214 fifth-generation fighter aircraft (FGFA), which was confirmed in October 2011, through an Indo-Russian co-development programme, is nowhere near action-station; Indian payment of US $ 250 million towards the project notwithstanding.

Is IAF, therefore, becoming an "orphan/destitute?" Is it caught in the midst of "force structure decision making complicated by politics, oversensitivity to past corruption in procurement projects, conflicting budget priorities, continuing problems of indigenous systems, bureaucratic delays in tendering processes, and entry of US as a major commercial and political factor in procurement decisions?"

One thing is clear. And none should have any illusion about it. In a multi-billion dollar fighter deal, where six foreign vendors bid and five lose, one instantly creates five implacable foes, "the vanquished", and one shaky/nervous "victor", who too cannot be seen to be overtly friendly. Importing India must be prepared to be terrorised and traumatised by foreign losers/vendors.

The entire acquisition imbroglio, therefore, boils down to "perception management" which need not be based on truth and facts. When Indo-US transport aircraft deals are made, no questions are asked because it is "Foreign Military Sales." When Indo-Soviet transactions brought Sukhoi-7, MiG-21, 23, 25, 27 and 29, they were a "Government to Government" deal. However, even though "India and France signed an inter-governmental agreement on September 23, 2016 for purchase of 36 Rafale fighters in flyway conditions" to at least partially mitigate critical shortages of the rapidly depleting fleet strength of the beleaguered IAF, politics supersedes all. Then there is the prevailing grave threat of the China-Pakistan axis. Historically, India's forte has been civil war, not war. Late General Sundarji's laconic definition/description of India's ruling class still stands: "The blind men of Hindustan."

(The author is alumnus, National Defence College, and Member, Aeronautical Society of India/M.AeSI. Views are personal)

Business Standard

Tue, 05 Dec, 2017

A test for the defence minister

Ms Sitharaman's decision on whether to kill the BMS project or not will reveal her commitment to building real indigenous capability in defence

By Ajai Shukla

Senior Indian Army generals, who grew up before smartphones became a part of our daily lives, are blundering in scrapping as "too costly" the ~5,000-crore project to indigenously design and develop a Battlefield Management System (BMS). More tech-savvy junior officers understand the importance of the

BMS, which will provide frontline combat soldiers with a real-time tactical picture of the battlefield to help them deal with "the fog of war". But generals call the shots, and now a defence ministry okay is all that is needed to cancel this promising initiative.

The success of the US Army in Gulf war I (1991), when Saddam Hussein's well armed and battle hardened Iraqi Army folded in less than 96 hours, amply demonstrated the power of a networked force. The defence ministry must also evaluate the army's wish to foreclose the BMS in the light of the Chinese BMS (named Qu Dian) which began deployment 10 years ago. Even Pakistan is working on their own BMS named Rehbar. If the Indian military wishes to avoid the fate of Hussein's forces, it too must network its battlefield units securely and robustly.

Then there is the need to prioritise "Make" category projects — including the BMS, there are only three in the pipeline. These harness Indian defence industry to develop "complex, high-tech systems", with the government reimbursing 80 per cent of the development cost. Such projects build design and development skills and systems integration capability, which is far more important than "Make in India" projects, which merely involve assembling imported components and systems to blueprints provided by a foreign "original equipment manufacturer" (OEM) under "transfer of technology". Defence Minister Nirmala Sitharaman's decision — whether to kill the BMS "Make" project or nurture it — will be a revealing indicator of her commitment to building real indigenous capability in defence.

Why is the BMS more important than buying the tanks and guns for which the army wants to save its money? A BMS is a "force multiplier" that uses information and communications technology (ICT) to enhance the effectiveness of the field force and the weapons they operate? An example of this in civilian life is Google Maps. Buying a fast (and expensive) car has limited benefits in terms of reaching one's destination sooner, but Google Maps' software does that more effectively. It chooses the fastest route by "crowd sourcing" traffic conditions, with user inputs updating this dynamic element in real time. This allows for the most efficient use of the road. Extrapolating this cheap and commonsensical solution to the battlefield, the "crowd-sourcing" of inputs from friendly elements on the battlefield — soldiers, weapons systems or surveillance devices that form a part of one's own force — builds up a common operating picture of the battlefield that is updated in real time. The "battlefield transparency" this creates enables soldiers and combat commanders to react to emerging situations faster than the enemy. Network centricity is all about being faster on the OODA loop – the action sequence of Observe, Orient, Decide, Act – than the adversary. In non-military terms that means being quicker in picking up and identifying the enemy, deciding how and with what weapons to engage him, and then actually doing so. A strong BMS system that provides battlefield transparency, and enables the immediate use of firepower and manpower, creates greater combat effect than expensive tanks, guns or fighter aircraft that are unable to use their capabilities to full effect.

Although creating a BMS combat network would be cheaper than buying weapons platforms, it still requires the expenditure of significant sums. In 2011, the defence ministry approved the BMS for an overly optimistic ~350 crore. Other worldwide benchmark projects indicate $1.5-2.0 billon in initial investments towards developing BMS-type "force multiplier "capabilities.

Today, the combined cost quoted by the two "development agencies" (DAs) – one, a consortium of Tata Power (Strategic Engineering Division) and Larsen & Toubro; the other between Bharat Electronics Ltd and Rolta India – is a more realistic ~5,000 crore. This would be paid out over five years, but the army is unwilling to earmark even ~1,000 crore per year for this revolutionary project, which would harness India's demonstrated skills in information technology. Given the range of technologies that it would galvanise, the BMS would be not just a "force multiplier" for the military but equally for the ICT economy.

Why does developing two BMS prototypes cost so much? The other ICT-based networks the army is developing — such as the "artillery command, control and communications system", which integrates fire support from artillery guns; or the "battlefield surveillance system" that integrates surveillance systems — are basically software systems. These will ride on a communications network called the "tactical communications system" (TCS), which is being developed as a separate "Make" programme. The BMS, however, is intended for the combat soldier, who would outpace communications networks like the TCS, especially in situations

like an advance into enemy territory. The BMS, therefore, requires its own communications backbone, built on sophisticated "software defined radio" (SDR) that provides enormous flexibility with its ability to function on disparate "wave forms". This means the BMS must have advanced communications technology, on which the information technology component is fully integrated. All these must be engineered as part of the project. The US Army tried in vain to ride its BMS on a generic radio, the Joint Tactical Radio System. Some $15 billion later, they realised the hardware and software had to be engineered together in a "system of systems" approach. Each element and device in the BMS has to be planned for SWAP (size, weight and power), and a range of waveforms have to be created.

The day of reckoning for the BMS is December 29, when the two DAs must submit their "detailed project reports", including final price estimates, to the Defence Production Board (DPrB), which the defence secretary currently heads. The ministry is currently squeezing the DAs to bring down their prices by over 30 per cent, even if that means reducing the scope of the BMS project. It is mind-boggling to see a government that claims to be committed to defence preparedness and indigenisation haggling with defence industry over a project that would bring to the Indian military a "revolution in military affairs", albeit three decades after it transformed the US military's way of warfare. It is time for Ms Sitharaman to step in and end this nonsense.

The Statesman
PEOPLE'S PARLIAMENT, ALWAYS IN SESSION

Tue, 05 Dec, 2017

Defence ministry needs an image overhaul

By Harsha Kakar

Over the years and for many reasons, the defence ministry (MoD) has been viewed as a stumbling block in national security, rather than being the prime mover. It has been viewed as being antagonistic to the armed forces, rather than a supporter. Amongst all the ministries of the government, it has faced the most flak for this reason.

The UPA regime refused to clear any defence deal, creating capability shortfalls and leaving the armed forces with such shortages of ammunition that even fighting a ten-day war was difficult. For years, A K Anthony only saw the Bofors ghost lurking around each corner, viewed every deal with suspicion and worried about his clean image being damaged. It led to the ministry losing even the basic respect it deserved.

The present government appeared to begin on a positive note, with Prime Minister Modi addressing the Rewari veterans' rally, promising to pay special attention to the military and its veterans. He gained full support in his campaign. With no defence minister at the helm for prolonged periods, the MoD continued with its antics. It gave false details to the pay commission, without clearing it from service headquarters leading to servicemen being degraded in status and salary in the seventh pay commission report, which the government accepted despite strong objections from the service chiefs. It was the joint decision of the service chiefs against issuing the letter of acceptance which compelled the PMO to step in.

Other issues which dominated headlines were letters degrading the status of the armed forces vis-a-vis their civilian counterparts, refusing to process their case for the grant of NFU (Non-Functional Upgradation), propelling a group to approach the courts for a decision and even supporting government decisions on cancellation of rations. It has claimed to be studying the Reddy commission report a year after it was submitted. It kept silent while veterans were hounded out of Jantar Mantar, not once but twice, and has ignored OROP anomalies.

Every day there are reports of war widows, including those of gallantry awardees and aged veterans challenging the government in courts for their rightful pensions, being denied by the accounts department of the MoD finance. This despite having obtained justice from the Armed Forces Tribunal (AFT). Some officers

sitting in MoD prefer to challenge these humane and just decisions of AFTs in higher courts, while the defence minister keeps quiet, adding to the suffering of widows and veterans.

Are these deliberate actions or accidental or being done to compel service headquarters to waste time and reams of paper only on resolving non-issues? It is a fact that those who serve in the MoD have little knowledge of matters military, seek privileges which flow from being a part of the armed forces but battle to remain at their helm. The impression being conveyed to the nation is that the MoD is a monster, seeking to dominate the services, subdue their voice and lower their status, while denying them the capabilities they need to ensure national security.

For every ill, the MoD is blamed, because as an organisation it has neither amalgamated the service HQs nor have its representatives as a part of it. Yet it continues to take decisions impacting the armed forces with a lack of understanding and knowledge. Publicly it is visualised as being aloof, uncaring, unresponsive and insensitive.

At the same time, the present defence minister has shown her desire to interact more with service chiefs and veterans than her predecessors and appears to be concerned about service-related issues. She is possibly the first defence minister in a long time with minimum outside responsibilities and hence is able to devote complete attention to the armed forces. If this is the truth, then the MoD must make efforts to change its image from that of an opponent to one of a friend in the eyes of the common Indian, who supports the armed forces because of its sacrifice and commitment.

The first action that the defence minister must take is to direct her staff to stop approaching higher courts, especially in cases of pensions and disability issues which concern war widows and veterans. Unless special focus is given to veteran and war widows' welfare, the ministry would continue to be criticised for being insensitive. If George Fernandes, as defence minister, could threaten sending erring defence ministry officials to Siachen, she could do the same with those adding to the agony of war widows and veterans.

The next action is to withdraw the challenge of the government in the NFU case. It would resolve much of the anger which presently permeates throughout the service and would be an immense morale booster. On similar lines is the case of 'Military Service Pay (MSP)' for Junior Commissioned Officers (JCOs), a small issue but one that has immense impact on morale.

The veteran community today stands with the serving. Those in service today are veterans of tomorrow. A positive approach to their problems, resettlement and pensions would enhance the image of the MoD and of the government.

The minister must pull up ordnance factories for their tardiness and hold them accountable for their lapses, especially their poor-quality products. Decisions on defence procurements must be based more on service HQ inputs than on suggestions of her scientific advisor, who would invariably support the DRDO in its development. This would not be difficult as both these organisations directly function under her ministry.

Finally, the armed forces need to be amalgamated into the MoD. By keeping them away, they are neither in decision making, nor are their interests ever considered, only enhancing the swelling anger against the ministry. Functionally too, the present system is obsolete, especially for a rising superpower.

The MoD needs to alter its image, which has in recent times been negative. Nirmala Sitharaman has proved to be an able administrator and has indicated a desire to act. But unless she puts in concerted efforts to change the outlook of her own staff, the MoD would continue to face criticism.

(The writer is a retired Major-General of the Indian Army.)

\

THE ASIAN AGE

Tue, 05 Dec, 2017

India invites Russia for joint defence manufacturing

By Smita Sharma

Seeking redefined ties with Russia in the multilateral changing times, India today called for the bilateral relations that are 'neither transactional nor based on convenience'. Vijay Gokhale, Secretary (Economic Relations), Ministry of External Affairs, asked Russia, the biggest arms supplier to India, to become a partner in Indian defence manufacturing.

"This is the opportune time to move from a buyer-seller format to joint production and investments under our Prime Minister's 'Make in India' initiative, in order to bring a new dynamism to our military-technical cooperation," said Gokhale. He was addressing the second meeting of the India-Russia Heads of Think-Tanks Forum at the Indian Council of World Affairs here.

Without naming China's Belt and Road Initiative (BRI), Vijay Gokhale also reiterated India's objection to it on grounds that it connects to China-Pak Economic Corridor (CPEC) passing through PoK.

"It is important for such initiatives to be open, inclusive, transparent and financially sustainable. It is also essential that such initiatives are taken by all states with due sensitivity in respect of the sovereignty and territorial integrity of states, so that they are net contributors to regional stability and prosperity," stressed Gokhale.

Last month at a public event, Russian envoy to India Nikolay Kudashev had said his country viewed BRI as an 'economic venture' and hoped that Delhi-Beijing could hold a dialogue on it like 'two adults' to resolve their differences.

the pioneer

Tue, 05 Dec, 2017

India Seeks Russia Push in Its Bid for NSG Membership

Citing India's impeccable record on non-proliferation, Secretary Economic Relations Vijay Gokhale on Monday sought Russian push for New Delhi's membership in the Nuclear Supplier's Group (NSG).

Speaking at the Second Meeting of the India-Russia Heads of Think-Tanks Forum, Gokhale said with Russia being India's premier supplier in nuclear power production, it is, therefore, natural expectation from New Delhi to bank on its active support for an early membership.

India will reactivate its NSG membership application once again this year to be discussed during its June 2018 Plenary Session. China is the only country that is opposing India's NSG membership on the grounds that New Delhi has not signed the Non Proliferation Treaty (NPT), one of the clauses for the membership.

However, India's NSG membership claim is based on the waiver it got in 2008 from the elite group. Apart from engaging with China directly on this issue, India is also seeking support from other countries. With Russia being India's closest ally, India wants Moscow to use its influence with China to give up its resistance.

"India and Russia are responsible space powers. In a significant development, India actively supported a Russian sponsored resolution on 'Further Practical Measures on Prevention of Arms Race in Outer Space'. We also have an impeccable record on non-proliferation, and we have taken a conscious decision to strengthen the global non-proliferation regime.

"Our export controls are now concordant with the requirements of all multilateral export regimes. Russia's consistent support for

India's efforts to seek membership is greatly valued. Membership of the NSG remains a priority for India. It is closely linked to our economic development and requirement for clean energy. As our premier supplier in the area of nuclear power production, it is, therefore, our natural expectation to bank on Russia's active support for an early membership," Gokhale said.

On another touchy issue of regional connectivity, and China's push for Belt Road Initiative, Gokhale made it clear that while India supports regional and international moves it is also essential that such initiatives are taken by all States with due sensitivity in respect of the sovereignty and territorial integrity of countries. He added India believes that Russia understands its position in this regard.

Talking about the dynamics of India-Russia relationship, Gokhale said the past relationship of the two countries should not transmute into a passive present partnership.

MAIL TODAY

Tue, 05 Dec, 2017

Why India needs robust space law

A Long-Awaited draft on Indian space law has finally been unveiled. It is called the Space Activities Bill, 2017, and its main objective is to "promote and regulate space activities in India." The need for such a legislation has been felt for a long time since India, despite having made deep inroads into space sector over the years, did not have any legislation so far. The absence of a regulatory or legal framework became more apparent in the past few years, with growing interest of private sector in space and growth of space start-ups in Bengaluru. The involvement of private sector in core space activities such as building and launching satellites is inevitable for any space agency for growth and wider utilisation of space technologies. Such a multi-player space sector needs a full-fledged regulatory framework.

Researchers have found an imbalance in the brain chemistry of young people addicted to smartphones and the Internet, according to a new study done at Korea University in Seoul.

They used magnetic resonance spectroscopy (MRS) to gain unique insight into their brains. MRS is a type of MRI that measures the brain's chemical composition. The study involved 19 young people diagnosed with the addiction and 19 healthy volunteers. Researchers used standardised Internet and smartphone addiction tests to measure the severity of the addiction.

Questions focused on the extent to which internet and smartphone use affects daily routines, social life, productivity, sleeping patterns and feelings. The key difference between those addicted and normal youth was in the levels of a neurotransmitter in the brain that inhibits or slows down brain signals and another chemical that causes neurons to become more electrically excited.

The draft made public by the Department of Space (DoS) allows private players to fabricate and launch satellites and participate in other space-related activities. This is a welcome move. Till now private companies have only been a supplier of components, fuel and other parts to the Indian Space Research Organisation (ISRO). However, the entry of private sector in space business will be governed by a regulatory mechanism proposed in the bill. It is proposed that all powers to licence private players to launch and operate 'space objects' will rest with the Union government (read DoS). And these powers will be quite sweeping. DoS will not only have powers to "grant, transfer, vary, suspend or terminate licence" but also have powers to inspect books of accounts and other documents of licensees and seek all information about partners, directors, etc.

This is particularly worrying because 'space activity' under this proposed law not only covers launch of satellites but also "use of space objects" as well as "operation, guidance and entry of space object into and from outer space and all functions for performing the said activities."

This would technically mean even data companies handling satellite imagery or universities operating ground facilities for their micro satellites may also need licence. If this is going to be so, it is a recipe for a new 'licence raj'. Another disconcerting note is the fact that DoS will be the regulator. This will amount to grave conflict of interest, because DoS through ISRO is also a service provider as well as a commercial operator through Antrix. At present, one person heads three offices — Space Commission chairman, DoS secretary and ISRO chairman. If the bill goes through, the same person will also be India's space regulator.

The bill is a clear indication that the government does not want a separate, independent regulatory authority for the space sector. In its present form the draft bill may not be music to the ears of existing private players and potential investors. In any case, much will be revealed in the rules and regulations. For instance, the quantum of licence fee to be charged, time frames for approvals and procedures for inspection of books, etc, are all critical issues. The writer is a science journalist

The Indian EXPRESS
JOURNALISM OF COURAGE
NEW DELHI WWW.INDIANEXPRESS.COM

Tue, 05 Dec, 2017

'Need to understand cyber threats before fighting them'

At IEThinc, experts discuss emerging threats to national security in the fast-changing digital world.

The confluence of national security and cyberspace is a dark area. A panel of experts — comprising Abhinav Kumar, IG Operations, Western Command, BSF Chandigarh; Sanjeev Tripathi, former chief, R&AW; Lt Gen. D S Hooda (retd), former Northern Army Commander; and Sandesh Anand, Cyber Security Consultant, Synopsys Inc — discussed the implications and challenges it poses. The discussion was moderated by Sushant Singh, Associate Editor, The Indian Express. Edited excerpts

What exactly does cybersecurity/ cyberspace mean? How has the nature of cybersecurity changed in India? What is the future trajectory and vulnerabilities?

Sandesh: We often joke that we should stop calling it cyber and start calling it cider, as none of us know the actual history behind it; where the word came from. I think the commonly accepted definition of cybersecurity is any information that you store or use in a digital format. It could be social media profile, a website a company runs and a database of the information the government has, among others. When you have this information stored, the process of securing it could be loosely called cybersecurity. The threats can come from many different places. We need to understand who are these people that are a threat to us. I want to classify the threats into three or four broad categories. There are many ways of categorisation. The way I will do it today is by motivation of the so-called hackers. In the technical world, the first is the script kiddie amateurs or curious individuals who spend time on the internet and are not a threat to the nation but they may become dangerous. The second category is that of actual cybercriminals. They have criminal motives to cause financial fraud or personality damage and make profit out of it. The third are the hacktivists or people with a message and a political viewpoint, and the way they propagate their viewpoints is through breaching security of various organisations. Fourth is nation-states trying to further their agenda using cyber attacks. With the Brexit, the definition of cyberattacks has gone up. When we spoke of stuxnet virus, few years ago, it was hardcore subverting of technical systems to gain information. But what happened in the US elections last year is influencing voters' mind to change voting behaviour.

The internet we use is some software being used by someone. Traditionally, the way software was used is to develop it or to outsource your development activity to a company and they would write the software for you. The way the world has moved over 5-7 years is about 80 per cent of the source code that is being used on your website is not actually written by you. It could be a third-party software or an open source, as we do not know the owner of it or piggybacking on another person's software.

Radicalisation from cyberspace remains a big challenge for societies like India particularly with the onset of digital tools as boundaries of national security have completely collapsed. But radicalisation has been a threat to india even earlier, as the hardware and software would be nothing without the human-ware. As someone who has dealt with it at very close quarters, how does radicalisation work in India? How should we view role of internet in it & how do we view the possibility of cooperating with other countries or global internet giants to deal with this problem?

Tripathi: In the last 15-20 years, with the IT revolution, the pace of radicalisation has increased by leaps and bounds. Earlier, it was confined to a particular segment of poor people in rural areas, now propagation of ideology through social media is expanded to urban areas and educated Muslim youth are getting affected. It gained momentum after the US action in collusion with Pakistan to counter Soviet influence in Afghanistan and US action with NATO allies in Iraq, Syria and Libya. While the action in Afghanistan led to the formation of Taliban, that strengthened Al-Qaeda, the dismantling of Saddam regime in Iraq and weakening of the Assad regime in Syria led to the rise of ISIS. Strangely & subsequently, the US had to take military action in Afghanistan to overthrow them, marginalising Al-Qaeda and killing their leader. And also in Iraq & Syria, they are fighting against the ISIS. The rise of ISIS and Al-Qaeda should be seen in a wider perspective as growth of radical Islamic ideology or jhadi terrorists in different parts of the world. Various jihadi groups have similar ideologies and common objectives such as Bokoharam in Nigeria,

Al Shabab in Somalia, Jemaah Islamiya in Indonesia, TTP in Pakistan and Abu Sayal group etc. They have to be defeated militarily, financing needs to be checked, they are using latest means of communication which should be checked by intelligence organisations.

How do you view the threat from cyber to national security? How vulnerable is India?

Hooda: The threat is very serious. In 2007, Estonia as the whole country had to be electronically shut down, Russia and Ukraine is a classic example of how you make use of cyber warfare. Misinformation, propaganda. Russia annexed Cremia leaving NATO and the US confused about what their response should be. Another dimension is that we can take measures only if we understand the complete nature of the threat. I think we are looking at it mostly in one part, cyber crimes/espionage, protecting critical assets, power, banking system but the part we need to look at is human part. Every time we are connected via internet, a lot of data is being collected about us. It is expedited as the cost of storing data is halved every 15 months. For instance, in 2011, there was an Austrian law student, namely Max Shrim. He asked Facebook for all his personal data that was stored about him. So, a legal battle ensued, but the EU lost it. He was given a CD with 1,200 pages of PDF, that's the kind of data that is being stored about all of us by Google, Amazon and FB. You say, how can one look at such huge amounts of data and that is where machine learning comes in. It uses and analyses this data properly. It's called psychographic profiling. So the governments and commercial companies know everything about you — preference, ideological leanings, friends, relatives and children, among others. In India, we have no control over data. There are no privacy laws and you don't own your data. Google and FB are the owners and they can use it anywhere in the world without paying any royalty. For a legal problem, a court in California has to be accessed is the clause given. That's one are we need to look at when we talk of cyberspace and national security. It is here that individual security intersects with the security of a nation.

Taking on from where Gen Hooda left, maintenance of law and order, internal security threats are increasingly emanating from cyber tools. You are in Chandigarh you saw what happened in Baba Ram Rahim case. And it goes pure hackers as Sandesh said. We also have the Russian example and I was astonished to learn of 2 fake profiles created to organise actual protests in the US where people came out & protested for 2 different ideologies. As Gen Hooda said is this a growing danger in India? The external meddling influencing Indian politics? Spreading socio-economic disaffection and as a senior

police official, what is the conversation? What is the discussion on the subject? Among peers, how are you looking at critical, social & economic subversion among communities?

Kumar: The fact that cyber space will be any less dysfunctional than the real world is a misplaced expectation. Cyber space is going to be a mirror of the real world with all its warts, fissures and all. We should be prepared for that. On threat related to the cybersecurity, the first question in my mind is what is its analogue in the real world. When you have ransomware, what is its counterpart in the real world. Similarly, impersonation, theft, robbery, or using cyber tools to influence elections or political opinion… step back a bit. Do we think it did not happen earlier? I think not. Right through the 50s & 60s during the height of cold war, the game was played using different tools. Now, it is being played with digital tools. I see cybercrime as a sub-set of cybersecurity, which, I believe, is a larger issue. Police forces across the country are struggling to adapt. It is not going to happen overnight. We need a radical change in the way we recruit & train our forces if we want to meaningfully counter the threat of cybercrime and cyber security. Also, I think without serious investment in basic policing, I don't think cyber policing or cutting-edge policing would succeed. Lot of capacity building in basic policing is needed.

Although you say that there are parallels about what has happened in the physical world but there are defining characteristics why those parallels fail at certain points. One is sovereignty issues. Companies that are operating may not be under the nation's sovereignty, as physical contact is not required. Secondly, the accelerated speed at which information travels. Example of Kashmir after Burhaan Wani's death is due to the speed of information travels which is not happening in the real world. So, with these changes, what are the kind of systems, institutional changes that police would require to tackle this situation?

Kumar: Almost all police forces have set up cyber crime cells at least at the headquarters level. Slowly, the more progressive police, especially in the southern states, are rolling out cybercrime cells at district levels also. Ideally, I would like to see that all police stations have a cell like we have PCR vans attached with each station. The spread of online, internet activity, the smart phones shows it has to be integrated with mainstream policing.

Tripathi: Many of these things have been happening from earlier times like cyber operations. Now, better tools are available which are being used. For example, dismantling of USSR was done by cyber operations only. Similarly, growth of radical ideology was happening earlier too but now with better tools, the interested parties are making better use than the authorities to counter that.

Is shutting down internet the only response? Darjeeling, 45 days? Kashmir, 30 days? And India is No. 1 for international shutdowns in the last three years. Is this the only response the establishment has?

Tripathi: I don't think it should be. There should be a counter-narrative available. It should not appear as a government propaganda.

Hooda: The internet shutdowns, I think the problem is that we have not been able to develop a counter-narrative. So, social media is used to spread all kinds of anti-government, anti-security forces propaganda to mobilise crowd.

When you were in Kashmir, when all these incidents were happening, were you recommending the shutdowns in time? And what was the role of cybercrimes in radicalisation and spreading violence in Kashmir in real terms?

Hooda: The classic case is of Burhan Wani, an absolute creation of the social media. I don't think he had committed a single crime. But on social media, the way his messages were sent out he became such a big hero that his death led to one of the biggest protests in Kashmir in recent times. So, you see that happening with other terrorists today. Zakir Musa, for example. Every time he gives a 3-4 min video message, it goes viral in valley.

But what can an ordinary citizen, companies, organisations and governments do to protect their technology assets? What do you recommend?

Sandesh: I will add a 4th dimension: As a society, what can we do. First of all, there is no replacing the government or state action. There are few things a citizen can do. Basic training and skill building. As we become more digital and people begin using these tools, they can be educated on how to protect data. As a citizen, the onus is on us to learn this. As informed citizens, we can demand better of our service providers. If you are using websites from your telecom providers or banks that are insecure and you know them to be insecure, please make noise about it.

Are our laws modern enough? Do we again and again need IPC or CrPC, a new Ranbir Penal Code? Is that also a problem, as you have constantly written about it?

Kumar: Experience of our police forces with IT Act has not been a happy one. We have attracted a lot of flak & most of them quite justified from civil society because of mindless application of 66A of the IT Act. I don't think that was the original intent of the framers of the Act. I am sure they didn't visualise some enterprising SHO wanting to curry favour with local political dispensation decides this is how I want to build my credibility of ruling party's man. IPC is a comprehensive act in terms of dealing with a range of human behaviour. So, how to adapt it to digital world will remain a challenge. Given the proclivities & problems of grassroot policing, I would say that we need to tread carefully. There is always a demand from a section of society for tough laws for emerging problems. Nirbhaya problem we introduced death penalty, has it made any dent? I think we need to tackle digital illiteracy on a war footing. Some counties in California have introduced teaching of coding to primary class.

The Ministry of Defence has announced formation of a cyber agency, initially planned to be a cyber command. There is low moral threshold for doing cybercrime activities besides intelligence gathering, covert operations, poll warfare, low-intensity provisions. So, what role do you see? Would it be offensive capabilities the cyber division would have? What would it really do? For example, in the last scenario, where there was a Chinese threat and Pakistan threat. What would the agency do?

Hooda: Today, structurally it is required. The NTRO (National Technical Research Organisation) was mandated to look after critical infrastructure in India, less defence forces. So, it looks after everything else less defence forces. So, one is protection of critical infrastructure of MoD, the 3 services is required to be undertaken today by some agency. I think the cyber agency will do this, there is little bit of weakness here as all 3 services are individually looking at it. So, that's the defensive part and certainly, secondly, you have to develop offensive tools to counter or carry out cyber attacks when you are threatened. There is also a larger role, cyber threats are actually a sub-set of information warfare. Tools have now changed. How you will use information, deny it to adversary, protect it, will depend on an amalgamation of intelligence agencies government agencies, military, & that's the ultimate role I see for the cyber command & not looking purely at cyber threats.

MAIL TODAY

Tue, 05 Dec, 2017

Kim the boaster

N Korea's Hwasong-15 missile intended to reach 'whole US mainland' broke as it re-entered earth's atmosphere

A Newly-Constructed missile North Korean officials said could reach the 'whole US mainland' failed during testing this week. The presumed powerful Hwasong-15 intercontinental ballistic missile (ICBM) broke apart in the air Wednesday as it re-entered into the earth's atmosphere, a US official told Fox News.

Eugene Lee, a South Korean spokesperson of the ministry of unification, who deals with North Korean affairs, said the Seoul government believes the "North hasn't crossed the 'red line' in weapons development yet because it hasn't perfected its ICBMs", according to the report. Back in July, North Korea also launched its Hwasong-14, which successfully flew 580 miles before it crashed into the Sea of Japan.

Officials confirmed the Hwasong-15 missile was 'significantly more' powerful than the Hwasong-14. South Korea's military said the latest missile flew 950 kilometers (600 miles) before splashing down in waters near Japan. It is potentially capable of striking targets as far as 13,000 kilometers (8,100 miles), which would put Washington within reach. Despite the break, the launch of the new ICBM was celebrated Friday with a massive public rally and fireworks in capital Pyongyang. North Korean leader Kim Jong-un also thanked workers during a visit to a factory that built the tires for a huge vehicle used to transport the ICBM.

Kim complimented workers for manufacturing the largesize tires for the 9-axle missile truck without relying on imported equipment. The leader called for efforts to raise production to 'satisfy the daily-increasing needs in developing the country's economy and beefing up national defense capabilities', the North's official Korean Central News Agency said on Saturday. Kim in September tasked the Amnokgang Tire Factory to make the tires for the 'great event in November', the agency reported.

hindustantimes.com

Tue, 05 Dec, 2017

US, South Korea kick off massive joint air exercise

Tensions Rise: North Korea has labelled the exercise an 'allout provocation'

Seoul: Hundreds of aircraft including two dozen stealth jets began training on Monday as the United States and South Korea launched a massive combined air force exercise.

The war games come a week after North Korea test-fired its most powerful missile ever, an intercontinental ballistic missile (ICBM) that may be able to target the US eastern seaboard. The five-day drill called Vigilant Ace, is meant to improve the allies' wartime capabilities and preparedness, South Korea's defence ministry said.

The US Seventh Air Force sent major strategic military assets, including an unusually large number of the latest generations of stealth fighter jets, for the annual training in the Korean Peninsula. They include six F-22 and 18 F-35 stealth fighter jets. About 12,000 US military personnel are participating. In total, 230 aircraft will be flying at eight US and South Korean military installations in the South.

An official at the South Korean defence ministry, who spoke on condition of anonymity, corrected his earlier statement that the exercise was the biggest ever.

Some local media report that B-1B bombers will also join aerial drills, but officials did not confirm their participation.

The training, held each year in late fall, is not in response to any incident or provocation, the Seventh Air Force said in a statement.

North Korea's state media said the drill pushes the Korean Peninsula "to the brink of nuclear war."

Pyongyang will "seriously consider" countermeasures against the drill, and the U.S. and South Korea will "pay dearly for their provocations," the Korean Central News Agency said before the start of the exercises.

2 Airline crews 'saw N Korea missile test'

The crew of a Cathay Pacific flight and pilots of two different Korean Air planes saw what they believe to be North Korea's latest missile test last week.

Cathay said on Monday that the flight from San Francisco to Hong Kong reported witnessing the apparent re-entry of the ICBM that North Korea launched before dawn on Wednesday.

The missile was far from the plane, and operation was unaffected, Cathay said, adding that it had informed other carriers and relevant authorities.

"At the moment, no one is changing any routes or operating parameters," the airline said.

Korean Air pilots on two different planes also reported seeing flashes of light believed to be the North Korean missile when they were flying over Japan, airline spokesman Cho Hyun-mook said.

The flights, one from San Francisco and the other from Los Angeles, were both headed for Incheon, the main airport serving Seoul, South Korea.

THE ASIAN AGE

Tue, 05 Dec, 2017

N-ARMED PYONGYANG POSES REAL DANGER: US

Washington, Dec. 4: A nuclear-armed North Korea poses the real danger to the world including its allies China and Russia, US National Security Advisor Lieutenant General H.R. McMaster said on Monday.

Pyongyang acquiring nuclear weapons "would be the most destabilising development" in the post-World War II period, he told Fox News.

"It is something that places us at direct risk, but places the world at risk. This is a regime that's never met a weapon that it hasn't proliferated. It's a regime who's said clearly its intentions are to use that weapon for nuclear blackmail and then to quote, "reunify" the peninsula under the red banner," Mr McMaster said.

Mr McMaster said the other grave concern is that he (Mr Kim) would proliferate or sell off these weapons to others. — *PTI*

Business Standard

Tue, 05 Dec, 2017

China's A.I. Advances Help Its Tech Industry, and State Security

By Paul Mozur and Keith Bradsher

Beijing — During President Trump's visit to Beijing, he appeared on screen for a special address at a tech conference. First he spoke in English. Then he switched to Mandarin Chinese.

Mr. Trump doesn't speak Chinese. The video was a publicity stunt, designed to show off the voice capabilities of iFlyTek, a Chinese artificial intelligence company with both innovative technology and troubling ties to Chinese state security. IFlyTek has said its technology can monitor a car full of people or a crowded room, identify a targeted individual's voice and record everything that person says.

"IFlyTek," the image of Mr. Trump said in Chinese, "is really fantastic."

As China tests the frontiers of artificial intelligence, iFlyTek serves as a compelling example of both the country's sci-fi ambitions and the technology's darker dystopian possibilities.

The Chinese company uses sophisticated A.I. to power image and voice recognition systems that can help doctors with their diagnoses, aid teachers in grading tests and let drivers control their cars with their voices. Even some global companies are impressed: Delphi, a major American auto supplier, offers iFlyTek's technology to carmakers in China, while Volkswagen plans to build the Chinese company's speech recognition technology into many of its cars in China next year.

At the same time, iFlyTek hosts a laboratory to develop voice surveillance capabilities for China's domestic security forces. In an October report, a human rights group said the company was helping the authorities compile a biometric voice database of Chinese citizens that could be used to track activists and others.

Those tight ties with the government could give iFlyTek and other Chinese companies an edge in an emerging new field. China's financial support and its loosely enforced and untested privacy laws give Chinese companies considerable resources and access to voices, faces and other biometric data in vast quantities, which could help them develop their technologies, experts say.

China "does not have the stringent privacy laws that Western companies have, nor are Chinese citizens against having their data collected, as (arguably speaking) government monitoring is a fact of China," analysts with the research firm Sanford C. Bernstein wrote in a report in November.

Already, China's companies have at times edged out foreign rivals. IFlyTek has won major competitions for speech recognition and translation. Two years before Microsoft did, Baidu, the Chinese internet search company, created software capable of matching human skills at understanding speech. This year the Shanghai-based start-up Yitu took first place in a major facial recognition contest run by the United States government.

IFlyTek and other Chinese companies say they follow China's laws and protect user data. But they agree that the sheer number of users in China, plus the government's single-minded drive to dominate the new technology, puts them at an advantage. "China has entered the artificial intelligence age together with the U.S.," said Liu Qingfeng, iFlyTek's chairman, at the Beijing conference. "But due to the advantage of a huge amount of users and China's social governance, A.I. will develop faster and spread from China to the world."

An iFlyTek spokeswoman said the company had yet to receive required permission from officials in Anhui, the Chinese province where it is based, to speak with the foreign news media.

IFlyTek is portrayed in the Chinese media both as a technology innovator and as an ally of the government. Last year iFlyTek helped prevent the loss of about $75 million in telecommunications fraud by helping the police target scammers, according to The Global Times, a nationalist tabloid controlled by the Communist Party. Its article quotes a Chinese security official as saying collecting voice patterns is like taking fingerprints or recording people with closed-circuit television cameras, meaning the practice does not violate their privacy.

"We work with the Ministry of Public Security to pin down the criminals," said Liu Junfeng, the general manager of the company's automotive business, at a conference in September.

Where iFlyTek gets its data is not clear. But one of its owners is China Mobile, the state-controlled cellular network giant, which has more than 800 million subscribers. IFlyTek preloads its products on millions of China Mobile phones and runs the hotline service for China Mobile, which did not respond to a request for comment.

"Data is gold," said Anil Jain, a professor who studies biometrics at Michigan State University. "These days you cannot design an accurate and robust recognition system for anything" without data.

Cars could be another major market, iFlyTek believes. China is pioneering a push into self-driving cars, which could heavily depend on voice technology. In September, iFlyTek introduced a new product, a glowing ellipsoid that mounts on a dashboard and listens for questions that it can check online, like a car-mounted Siri.

"We have to understand if the car is our friend, if there is an emotional connection," Mr. Liu said.

Through a third-party supplier, a few hundred thousand of the four million cars that the Volkswagen Group sells in China annually will be equipped next year with iFlyTek voice recognition technology, said Christoph Ludewig, a spokesman for the German automaker.

The New York Times News Service