PROTECTING
INDIA'S HERITAGE.

It has been our duty to strengthen a country that has a strong history. And we have consistently done so for the past 6 decades using cutting edge technology and class of service. Needless to say our response has always been prompt. Through our dedication and support we've helped secure the heritage of billions in India with peaceful grounds and safer skies.

RAFALE
INTERNATIONAL
DASSAULT AVIATION • SNECMA • THALES

60 YEARS. 5 AIRCRAFT TYPES. 1 NATION.
www.rafale.co.in

TOOFANI I MYSTERE IV I ALIZE I JAGUAR I MIRAGE 2000

DEFENCE AND DIPLOMACY

VOL. 6 NO. 3 • APRIL-JUNE 2017

DEFENCE AND DIPLOMACY

IN PURSUIT OF NATIONAL SECURITY

VOL. 6 NO. 3 ISSN 2347 - 3703 APRIL-JUNE 2017

JOURNAL OF THE CENTRE FOR AIR POWER STUDIES

DEFENCE AND DIPLOMACY

IN PURSUIT OF NATIONAL SECURITY

VOL. 6 NO. 3 ● APRIL-JUNE 2017

CENTRE FOR AIR POWER STUDIES

VISION

To be an independent **centre of excellence on national security** contributing informed and considered research and analyses on relevant issues.

MISSION

To encourage independent and informed research and analyses on issues of relevance to national security and to create a pool of domain experts to provide considered inputs to decision-makers. Also, to foster informed public debate and opinion on relevant issues and to engage with other think-tanks and stakeholders within India and abroad to provide an Indian perspective.

CONTENTS

Book Reviews

EDITOR'S NOTE

The power of the internet is a rapidly increasing phenomenon, almost unbridled in scope. One can only wonder what the morrow brings. There is no gainsaying that the internet has changed our lives and made them far more efficient. Unfortunately, the human tendency to get the better of an adversary in every possible way extends to the use of the internet as well. The social media has also mushroomed but has brought in its wake misuse of the media. Privacy that was taken for granted only a few years ago, is now a major concern. Worse, there is a requirement to balance security and privacy. Therein lies the 'privacy paradox'. In our lead article on the subject, **Gp Capt Ashish Gupta** explains the concept of privacy as it has evolved and questions whether attempts to breach it were inevitable. In a battle between security and privacy, security will take pride of place even in a society that places individual privacy as a near fundamental right. The author also suggests that much work lies ahead.

Since times immemorial, intelligence has been a war-winning factor and considerable resources are expended to gain useful information about the adversary. In the internet age, we have to ensure the safety and security of data from the time it is created, through the transmission system and till it is received by the appropriate agency. The adversary is only too keen to tap into the data. For long, it was supposed that a computer system that is part of a secured computer network and is isolated from unsecured networks, social media, etc, would be safe. We call it air gapping of computers. **Dilipraj** argues that air gapping may, by itself, no longer permit us to assume any

such thing and shows how the US has developed or is developing tools to beat the system that so far was considered to be impervious. He describes some of the measures being developed but the list cannot be complete.

Even before President Trump assumed office in January this year, many wondered about the extent that he would live up to regarding his electoral promises. The president took a number of decisions from the first day itself. Many statements and pronouncements were made. There were many U-turns as well, particularly in relation to his approach towards Russia and China. **Hina Pandey** looks at the president's first 100 days in office, with particular reference to US-Iran relations. To begin with, the president stated that the nuclear deal was a bad deal, but possibly as a result of good advice, he is now reconciled to it. The US Department of State has certified that Iran was following the dictates of the Joint Comprehensive Plan of Action (JCPOA). With little love lost between the US and Iran, and the US openly siding with Saudi Arabia and Israel, the future is uncertain.

The exuberance of North Korea in showcasing its missile might and nuclear capability led to the US and South Korea agreeing to the placement of the Theatre High Altitude Air Defence (THAAD) system in South Korea. **Debalina Ghoshal** examines the possible change in China-South Korea relations. China vociferously objected to the deployment and resorted to petulant behaviour and bullying tactics like banning TV series, impeding tourism to South Korea, closing down stores and banning specific imports. However, North Korea indulged in open and provocative defiance. With China not intervening to control North Korea, the US and South Korea certainly have a strong case for deployment of the missiles.

The growth and mushrooming of terrorism in Pakistan must be a subject of interest to us. In an incisive article, **Shreya Talwar** describes the growth of the Tehrik-e-Taliban Pakistan (TTP). The year 2017 has been particularly bloody for Pakistan. Possibly the worst instance was in February this year when 92 people were killed and over 200 injured at a shrine in Karachi. The TTP claimed credit for the attack. The Pakistanis' assertion that they are

themselves the victims of terrorism is justified but then they are also the sponsors of terror in other countries. The Pakistan Army has made many determined efforts to combat the TTP but the latter remains a potent force. Shreya traces the history of the TTP, its growth, goals and objectives, and the strategies employed for survival. The recruitment, funding, resort to organised crime and its linkages with other terrorist organisations are also addressed.

Space is a recognised domain of warfare. In a future war, we can expect satellites to be targeted through hard or soft kills, and attacks on our ground stations that support our space activities. Possibly, one answer is to ensure redundancy but there will be cost penalties. Does the answer lie in a deterrent capability? **Wg Cdr Anand Rao's** description of our efforts at Anti-Satellite (ASAT) technology makes interesting reading. He categorically states that China has an extant capability, is improving on it, and we should develop our own capability in the field. In a clear and unambiguous manner, the author gives the reader a good feel for the subject.

This journal seldom discusses the nuances of India's foreign policy. In this issue, an exception is made and **Dr Stuti Banerjee** explores our maritime outlook. She tells us of our rich maritime traditions and the need for us to keep a continuous watch on our maritime borders. The maritime domain is gaining in importance and there are traditional and non-traditional threats to counter. Our policy should seek the acceptance of the countries in the Indian Ocean Region for a policy of 'shared security and shared prosperity'. The policy is unexceptionable.

The last article is by **Gp Capt RK Narang** who discusses the civil aviation scene in India, with particular reference to 'Make in India'. The UDAN scheme for affordable flights was inaugurated by our prime minister on April 27, 2017. The important question is as to whether we have a viable 'Make in India' programme. The author looks at the requirements of what should become a burgeoning sector and makes suggestions on what should be done.

In our Book Review section, two books are reviewed. **Radhika Halder** reviews the book *Call for Transnational Jihad* by Arif Jamal. The

book is about globalised terror and discusses infamous names like Al Qaeda, Islamic State, and others. The reviewer makes the point that the author of the book has had a lifelong commitment against Islamic terrorism, involving research on the subject for over two decades. It is a good review, concise, purposeful and very readable. The second Book Review is by **Narender Yadav**. His review of the book *Born to Fly* by Nitin Sathe is heartwarming; the book promises to be much more.

Happy reading

THE "PRIVACY PARADOX" OF THE DIGITAL AGE

ASHISH GUPTA

The unbridled enthusiasm for Information and Communication Technology (ICT) and its proliferation, coupled with the ubiquity of internet access and mobile connectivity has dramatically impacted everyday lives of almost all people across the globe. Information is being collected, collated, analysed and disseminated in almost real time. It has emerged as a strategic resource contributing to capability aggrandisement, competitive dominance, and for identification of potential threats. Information can be garnered through persuasion, inducement, enticement, coercion or can be compromised due to technological inadequacies and human frailties. In the digital realm, the types of personal and social interactions that are played out through the milieu of social media, either wittingly or unwittingly, lead to many privacy breaches and violations. The all-pervasive digital technologies and the changing nature of human interactions, facilitated through digital online tools have affected radical changes in notions, perceptions and expectations of privacy.

The concept of privacy is far more complex, more pervasive and more nuanced than can be encapsulated and explained by a single underlying concept. Privacy is a legitimate expectation, an inalienable right and an indispensable precondition for an inclusive society that ensures human dignity to each and every person. A person's

Gp Capt **Ashish Gupta** is a Senior Fellow at the Centre for Air Power Studies, New Delhi.

fundamental need for privacy is a psychological as well as sociological manifestation of the sense of being human with dignity.[1] Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.[2] The explicit conception of privacy is not easy and has intrigued and vexed generations of philosophers, anthropologists, legal theorists and experts in jurisprudence. However, there is universal acceptance that the concept of privacy is an extremely important determinant of human existence in all its manifestations. It also requires enlightened and balanced elucidation to accommodate critical and aspirational human needs.

Since antiquity, privacy as a cherished and fundamental value has, almost inextricably, been linked with the concept of personal freedom. The Code of Hammurabi protected the home against intrusion, as did ancient Roman law.[3] Privacy, as a term, is open to numerous interpretations and, as a concept, is riddled with ambiguous complexities. Arthur Miller finds privacy "difficult to define because it is exasperatingly vague and evanescent."[4] William Beaney declared that "even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right."[5] According to Robert Post, "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[6] In her book *The Right to Privacy*, Judith Thomson argues that the right to

1. The Social Science Research Network, "Right of Privacy. Constitutional Issues and Judicial Responses in USA and India Particularly in the Cyber Age", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1440665. accessed on April 17, 2017.
2. Daniel J. Solove, "Conceptualizing Privacy", *California Law Review,* vol. 90, issue 4, July 2002, Article 2, p. 1088.
3. Daniel J. Solove, *Nothing to Hide: The False Trade-off between Privacy and Security* (New Haven: Yale University Press, 2011), p. 4.
4. Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: University of Michigan Press,1971), p. 3.
5. William M. Beaney, "The Right to Privacy and American Law", *Law and Contemporary Problems*, vol. 31, no. 2, Spring 1966, p. 253.
6. Robert C. Post, "Three Concepts of Privacy", *Georgetown Law Journal*, vol. 89, August 2001, p. 2087.

privacy is inherently ambiguous as the conceptualisation of privacy encapsulated within a normative set of rules and norms is not possible. She even suggests that all discussion about privacy should be ''reduced" to a discussion of other rights.[7]

The right to privacy is not explicitly mentioned in the Indian Constitution but has been recognised and accepted as being an inalienable part of our constitutional heritage and a natural individual right under Article 21 under the "right to life". As per Article 21 of the Indian Constitution: "No person shall be deprived of his life or personal liberty except according to procedure established by law."[8] In some of the landmark rulings, the Indian courts have vindicated the explicit constitutional human "right to life" and broadened its scope to include the implicit "right to privacy" within Article 21. The 2011 Privacy Bill, aims to provide for the right to privacy to citizens of India and regulate the collection, maintenance, use, and dissemination of their personal information, as also provide for penalisation for violations of such right and for matters connected therewith or incidental / hereto.[9]

IMPACT OF ICT ON PRIVACY

With ICT touching upon various facets of our daily lives, our ability to comprehend, in an objective manner, its implications for, and complications on, privacy is limited. Some of these factors include the volume, magnitude, complexity, and persistence of information; the expanding number of ways to collect information; the number of people affected by the information; and the geographic spread and reach of information technology.[10] These technologies have emerged as a new medium for mediation of most of the private and public communications, social interactions and business transactions. These technologies are the lynchpins of contemporary as well as

7. Julie C. Inness, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press, 1992), p. 28.
8. n.1.
9. N.S. Nappinai, "Our Fundamental Right to Privacy is in Grave Peril", *The Wire*, October 7, 2015, https://thewire.in/12571/our-fundamental-right-to-privacy-is-in-grave-peril/. Accessed on April 17, 2017.
10. James Waldo, Herbert S. Lin, and Lynette I. Millett, *Engaging Privacy and Information Technology in a Digital Age* (Washington, DC: National Academy of Sciences, 2007), p. 27.

quintessential infrastructures and institutions such as banking, health care, defence, education, industry, entertainment, etc.

The burgeoning information technology revolution has created a paradigm challenge to privacy as it facilitates and fosters uninterrupted surveillance, restricts erasure of footprints in cyber space and gives instant visibility to information across the globe. The initial trepidation about the possible misuse of data garnered and stored in large stand-alone computers by the government and other institutions for the mid to the end of the 20th century, has given way to outright desperation and dread due to the possibility of mass surveillance from the range of present-day systems, including the internet; the world wide web; smart mobile phones; biometric surveillance; Global Positioning System (GPS); social networks; big data; cloud computing; mobile computing; database analytics; data mining; and more. Besides, the ubiquitous social media has deeply influenced the way we decide to reveal or conceal personal information. Although many individuals are still sticklers for a certain measure of privacy in their lives, social media has fanned the narcissistic, exhibitionistic and voyeuristic desires of a large section of society and this usually comes at the high cost of losing privacy.

The impact of technological advances varies across social groups and social settings, depending upon the necessity, enthusiasm and naivety with which the technological advancements are perceived and assimilated. The more digitally fluent and affluent members of society are likely to experience the impact of the information revolution in a different way than those who are digitally 'impoverished'. Besides, more digital interaction, engagement and immersion exponentially increase the chances of privacy violation. Information which appears to be implicitly mundane becomes explicitly strategic when it enters the digital realm and unobstructed access to it by all and sundry provokes trepidation and indignation. Even humdrum information of a personal nature becomes a serious concern when digitally exposed to thousands of prying eyes online.

SOCIAL NETWORKS AND PRIVACY

The internet, which was created and nurtured for the primary role of being a system for the upward, downward and lateral sharing of

information, is subtly but surely transforming into a system more frequently being used for communication and social interactions. The notions of "web 2.0", "social media" and "social networking sites" have emerged contextually and have become bywords among netizen communities. Web 2.0/social media platforms are web-based platforms that predominantly support online social networking, online community-building, collaborative information production and sharing, and user-generated content production, diffusion, and consumption.[11] The term "web 2.0" does not necessarily signify the emergence of the internet in a transformative, different version, with functional improvements, rather the emergence of specific social qualities (sharing, online cooperation, etc.) supported by the world wide web.[12] Social media sites enable individuals to enhance and foster online social interactions by seeking and sharing information and ideas, and expressing themselves through opinions, images, photos, music and links to other users. Humans crave *social interaction and affirmation* and the internet has afforded them a platform for visibility and voice, and the worth of being socially relevant.

The internet has created unbridled opportunities for privacy invasion that differ in magnitude, focus, resource requirements and also in their strategic implications, in comparison to methods used some years ago. The old methods of stalking, which required the presence of a perpetrator in close proximity to the victim or interception of physical mail or documents have become archaic and have given way to online methods which are far more effective, invasive and pervasive. The internet is realigning the contours of the 'privacy landscape' through its technical design and pervasive proliferation of technology in almost all social interactions and usages.[13] Through the internet, a massive amount of data can be accessed and synthesised to capture even subtle or hidden information of defamatory or incriminatory nature which one wishes to keep private. Besides, data in cyber space can easily be shared, copied, searched, mined, compiled, compared, matched, combined, or transferred worldwide at the click of a mouse, leading

11. Christian Fuchs et al., *Internet and Surveillance The Challenges of Web 2.0 and Social Media* (New York: Routledge, 2012), p. 3.
12. Ibid., p. 5.
13. Starke-Meyerring, Doreen and Laura Gurak. "Internet" in William G. Staples, ed., *Encyclopaedia of Privacy* (Westport: Greenwood Press, 2007), p. 298.

to a proliferation of personal data and the development of what some privacy researchers have termed a "digital persona"—a collection of an individual's data available in digital form.[14] The internet—the repository with an infallible memory—stores digital contents posted online without any ethical, legal or personal propriety considerations. The internet preserves bad memories, past innuendos, errors of judgement, errors of perception, pervious acts now deemed mistakes, disparaging writings, photos or videos, and makes it difficult to redeem and rehabilitate ourselves by slaying the ghosts of the past.

The privacy issue in the context of the internet takes a range of forms, far more diverse and challenging when compared with the previous challenges of guarding privacy in the era of paper-based data storage and peer-to-peer communication systems. A dramatic burgeoning of data over the past decade, including personal data, either provided consensually or coerced out under false pretences, has exponentially increased the risk of manipulation for a wide degree of uses, entailing varying consequential sufferings for individuals. The pervasiveness of hand-held digital devices and the stupendous popularity of social network sites underpin three issues which impact the way the people, societies and communities view the issue of privacy. In one, the posting of intimate or incriminating information by individuals can lead to a chain of events that can jeopardise interests, social standing, and professional status, and can endanger personal relationships. The second issue which impinges on legitimate privacy interests emerges from the practice of posting information about others with or without their consent or knowledge on social media sites. The cyber landscape is inundated with countless tagged images on social network sites, implicitly or explicitly disclosing details of those having a friendly, casual or no acquaintance with the originators. Social media and Social Networking Sites (SNS) have promoted a culture of exhibitionism and voyeurism that has resulted in public revelation of a great deal of information about others without fully understanding its ramifications and consequences. The third privacy issue stems from the capacity to continuously and incessantly monitor and track individuals online by linking their digital footprints to their names, addresses, orientations, preferences, dispositions, intentions,

14. Ibid., p. 299.

etc. This collected information is then subjected to analytic processes to capture trends, chart patterns and draw inferences.

In the past decade, SNS companies have grown to become extremely profitable, filling the coffers of their owners with power and wealth. Their global ubiquity and multinational character have an important bearing on privacy debates in different contextual frameworks as perceived by different nations. In fact, the outcomes of such debates are meant to be used as reference for seeking technological solutions to the issue of privacy. One of the most popular and possibly the most controversial sites in this regard is Facebook, which has been in the eye of the storm several times in the past for its privacy policy. Since its inception, the company has changed its privacy policy many times, sometimes due to public outrage and concerns expressed, while, at other times, as part of efforts to push the boundaries of acceptable privacy standards.

BALANCING PRIVACY AND NATIONAL SECURITY

The vociferous and ongoing debate between privacy and security and its consequences has led to increasing tension between the principle of 'security' and that of 'privacy'. The threats of internal extremism, global terrorism, radical insurgency, threats from rogue nations and asymmetric threats from non-state actors have resulted in deepening and intensification of security measures across the whole spectrum of political, economic and social, constitutional and security strategies, tactics and approaches. A pressing question recurrently posed, not only by the citizenry but by experts as well, is whether it is possible to strike a balance between security and privacy. In the midst of security imperatives, will it even be plausible to not tread upon fundamental rights and civil liberties. In the present security environment—underpinned by the rationality of a "war on terror" and buttressed by all the possible means, methods and materials—privacy concerns seem trivial compared to overarching security necessities. Security concerns are readily discernable and understandable since the national security, human security and economic security stakes are far higher than the abstract and vague conceptions of privacy rights.

The contemporary compulsions and security imperatives fuelled by the growing public and political fear over the rising scourge of terrorism has, to some extent, pushed the issue of privacy to the sidelines. Since an increasing

number of political, economic and social functions is facilitated, supported and mediated through cyber space, it has given ample opportunities to the law enforcement agencies to garner unprecedented levels of information and unparalleled means to engage in surveillance. In the digital realm, it is nearly impossible to live without generating streams of data about what we read, watch, buy, and who we support, idolise, sympathise and empathise with – and all this data can be accessed remotely. Because of perceptibility, discernibility, much higher stakes and high potential of loss of life, the security concerns are pitched at a higher level of importance than privacy concerns that remain subjective, abstract and contextualised. Given a choice between being secure and being privacy conscious, many will happily trade privacy for a certain level of security. However, protecting the right to privacy of individuals need not be fatally impinging on the efficacy and legitimacy of security measures; it merely demands accountability, oversight and effective regulatory mechanisms.

More ironically, the information revolution has contemporaneously coincided with the evolution of terrorism in its current form, putting digital surveillance on a higher level of importance than other activities of the law enforcement agencies. With the growing threat of terrorism and mounting national security concerns, the law enforcement agencies have also expanded their arsenal of techniques to snoop through the digital packets transiting through the networks, and gather records and data, carry out audio and visual surveillance, and track movements. Despite constitutional provisions and statutory enactments for the protection of privacy, the first casualty of the war on terrorism has been perhaps personal privacy. George Orwell's depiction of a totalitarian society in *Nineteen Eighty-Four* in which the citizenry is subjected to a high degree of control and intrusive surveillance might not be only be a metaphoric construct but closer to present-day realties. As the 'Orwellian metaphor' has underscored, the public and social realms cannot exist without protection of privacy and freedom.[15] Digital surveillance has become far more pervasive and intrusive, and is perceived as a natural manifestation of the problems of modern times, relegating that issue of privacy to obscurity and incongruity.

15. Dionysios Politis, *Socioeconomic and Legal Implications of Electronic Intrusion* (London: IGI Global, 2009), p. 131.

TRADEOFF BETWEEN NATIONAL SECURITY AND PERSONAL PRIVACY: A CASE STUDY

Following the terrorist attack in San Bernardino, California, on December 15, 2015, which killed 14 and seriously injured 22 people, in February 2016, the US Federal Bureau Investigation (FBI) requested Apple Company to assist them in hacking the iPhone, which belonged to Syed Farook, the main perpetrator of the terrorist attack.[16] FBI investigators, in possession of Farook's iPhone, believed that the device contained data which could help them in unravelling Farook's motives. But the data could only be accessed after unlocking the iPhone by using the four-digit passcode. A four-digit passcode has only about 10,000 possible combinations and unlocking a phone by using these might not prove to be that difficult. But modern iPhones have an optional feature that would erase all data on the phone after ten incorrect passcode entries and FBI agents were not willing to take that risk. The request was turned down by Apple.[17] The FBI, armed with an order from a federal magistrate for reasonable technical assistance from Apple to access the data on the device, again approached Apple. Apple challenged the court order, arguing that its encryption technology was necessary to protect its customers' communications, security, and privacy and raised both constitutional and statutory objections to the magistrate's order. A magistrate in the Eastern District of New York ruled in favour of Apple, denying the FBI's request for information on Farook's iPhone by unlocking it.

The debate, once again, has taken centre-stage, this time in Britain. On March 22, 2017, London was rocked by the deadly 'terrorist' attack outside the British Parliament carried out by a 52-year-old Briton Khalid Masood, who drove a car into pedestrians killing three of them, and then fatally stabbed a police officer.[18] The Islamic State (IS) claimed responsibility for the attack, but the precise nature of his

16. Danny Yadron, Spencer Ackerman and Sam Thielman, "Inside the FBI's Encryption Battle with Apple", *The Guardian*, February 18, 2016, at http://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple, accessed on February 22, 2016. Accessed on April 17, 2017.
17. Ibid.
18. Vikram Dodd et al., "Westminster Attack: Police Hunt for Clues after Four Dead in 'Sick and Depraved' Incident", *The Guardian*, March 23, 2017, https://www.theguardian.com/uk-news/2017/mar/22/parliament-attack-police-officer-four-dead-westminster. Accessed on April 17, 2017.

connection with the IS was not yet fully clear at that time. The London police, as part of the investigation, were focussing on Masood's communications and it was widely speculated that Masood was in contact with someone through WhatsApp immediately prior to the attack.[19] In an effort to bolster their fight against terrorism, British government officials scheduled a meeting with representatives of American technology companies seeking help to access to encrypted messages sent through WhatsApp, an instant-messaging service owned by Facebook.[20] Britain is not the only country in Europe seeking a viable and workable solution from Silicon Valley companies to the 'encryption conundrum' which severely contains and retards efforts to identify and prosecute the real perpetrators of terrorist attacks.

The tussle had been simmering in the open for months before the San Bernardino shooting between Washington and Silicon Valley over the privacy of online data and new security technologies. After the San Bernardino shooting, on December 9, 2015, FBI Director James B. Comey, while making a statement before the Senate Judiciary Committee brought out that the IS was increasingly using encrypted private messaging platforms. He said, "This real and growing gap, which the FBI refers to as 'Going Dark'; we believe it must be addressed, since the resulting risks are grave in both traditional criminal matters as well as in national security matters." He further commented that the US government was trying to ensure that the private players who own and operate these platforms—with end-to-end encryption—understand the national security risks emanating from the use of their encrypted products and services by malicious actors.[21] On the other hand, the top tech companies of Silicon Valley, including Apple, have reiterated their commitment to respect the privacy and protection of their customers, and refused to dilute

19. Mark Scott, "In Wake of Attack, U.K. Officials to Push Against Encryption Technology", *The New York Times,* March 27, 2017, https://www.nytimes.com/2017/03/27/technology/whatsapp-rudd-terrorists-uk-attack.html?_r=0. Accessed on April 17, 2017.
20. Ibid.
21. The US Federal Bureau of Investigation, Oversight of the Federal Bureau of Investigation, James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Washington, D.C, December 9, 2015, https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-8. Accessed on April 17, 2017.

their position despite clear national security risks to both the US and elsewhere. In one of his speeches, Tim Cook, the Chief Executive Officer (CEO) of Apple made his stand very clear by saying, "We at Apple reject the idea that our customers should have to make tradeoffs between privacy and security. We can, and we must, provide both in equal measure. We believe that people have a fundamental right to privacy. The American people demand it, the Constitution demands it, and morality demands it."[22]

Melvin Kranzberg once famously commented: "Technology is neither good nor bad; nor is it neutral."[23] The resolution of this raging debate rests on the extent to which national security concerns outweigh the rights of citizen to privacy of their associations, papers and communications[24] — and on the extent to which democratic concepts such as privacy and freedom can be accommodated within a larger security conception and framework. There is no denying the fact that the global scourge of terrorism can be exterminated only through the collaborative and integrated efforts of the global political leadership, military, law-enforcement, intelligence and security agencies, financial institutions and public and private companies— even if it requires transcending parochial, partisan interests and objectively balancing the degree of risk that might be warranted by the potential benefit.

CONCLUSION

The articulation of 'jurisprudence on privacy' in the digital age is still in the evolving stage. In cyber space, the realisation of the technological potential and inclusion of technical innovation has transformed the way information is collected, analysed, synthesised, and disseminated. The exploitation of new technological possibilities and their ingenious application in sustaining the momentum of the information revolution, has greatly changed the methodology, outlook

22. Matthew Panzarino , "Apple's Tim Cook Delivers Blistering Speech on Encryption, Privacy" , *The Techcrunch* , June 2, 2015, http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.oero2hn:kVGu, April 17, 2017.
23. James W. Fraser, *Reading, Writing, and Justice: School Reform as if Democracy Matters* (Albany : State University of New York Press, 1997), p.142.
24. Richard H. Rovere and Gene Brown, *Loyalty and Security in a Democratic State* (New York: Ayer Company Publishers, 1977), p. 354.

and potential dimension of information gathering. The steadily increasing societal dependence on ICT has brought a transformational change in the functioning of social institutions and practices, chiefly characterised by a multitude of demands for personal information. These demands are made, partly, to provide solutions to specific problems by the use of ICT, and partly, for analysis and synthesis of this information for leveraging it as a resource. Even for online interactions or transactions of a trivial nature, furnishing of personal information to institutions and organisations is absolutely essential. Our inexorable dependence on digital technologies for work, for leisure and for everyday life has made us give scant and inadequate attention to the kind of information that is sought, who seeks it and, how it is to be used or exploited. The evolution of a normative framework for privacy in the digital realm is fraught with its own set of challenges and contradictions. Some of these challenges are a result of the gap between the adoption of new technology and the understanding of this technology's implementation on privacy. Many of the challenges have emerged due to the lack of a more flexible and enforceable jurisprudence based on the broad principles of privacy, which needs to balance the established conceptions of privacy, the legitimate expectations of the digital users, and the national security.

AIR GAPPING OF SENSITIVE COMPUTER SYSTEMS: IS IT AN OBSOLETE PRACTICE?

E DILIPRAJ

The evolution process has helped mankind acquire plenty of information and derive enough knowledge from information in all probable fields. The knowledge gained over centuries has, in turn, helped mankind to evolve into a 'technological' being. Yet, it could be stated that "knowledge is free for all, but not all information." The term information means "facts provided or learnt about something or someone"[1] and the term knowledge means "the understanding of someone or something based on the study of facts, descriptions or skills through experience by perceiving, discovering or learning".[2] Therefore, sensitive information such as high-end military technology, business secrets, critical national information, and so on is not to be widely known and, hence, is withheld from circulation.

In the information age, sensitive information is always the target and adversaries are in constant pursuit of such information in order to gain advantage over one another. Also, in the information age, most of the sensitive information is in digital format, stored in secured

---

Mr **E Dilipraj** is an Associate Fellow at the Centre for Air Power Studies, New Delhi.

1. Meaning as explained in the *Oxford Dictionary*, https://en.oxforddictionaries.com/definition/information. Accessed on March 7, 2017.
2. Ibid.

computer systems known as 'air gapped computer systems' which are disconnected from other networks, with very limited access, and with a lot of security. Therefore, these air gapped computer systems have become the primary target in the race for collecting sensitive information, and countries around the world mainly depend on covert practices such as data exfiltration through cyber means to lay their hands on the restricted information available in a secured environment.

With this brief background, this article is a study of a few different methods of data extraction from air gapped computer systems that have come into existence in the recent years as a result of research and development by the security agencies and academic communities of various countries around the world.

AIR GAPPED COMPUTER SYSTEMS AS TARGETS

Air gap, air wall or air gapping is a security measure employed in order to isolate a computer or a network from unsecured networks, such as the public internet or an unsecured local network.[3] Theoretically, an air gapped computer is physically and virtually segregated and, hence, incapable of connecting wirelessly or physically with other computers or network devices. Such security measures are undertaken to secure and protect the sensitive data stored and processed in these isolated computer systems. Air gapped computer systems are used where the system or network requires extra security, such as classified military networks, financial networks that include payment networks that process credit and debit card transactions for retailers, or industrial control systems that operate critical infrastructure such as nuclear power plants, and so on.[4] Considering the sensitivity of the data stored in such infrastructure, in order to prevent unauthorised data extraction through electro-magnetic or electronic exploits, there is often a specified amount of physical space between the air gapped system and the outside walls, and between its wires and the wires for other technical equipment.[5]

3. "Air Gapping", http://whatis.techtarget.com/definition/air-gapping. Accessed on March 7, 2017.
4. Kim Zetter, "Hacker Lexicon: What is an Air Gap", October 12, 2014, https://www.wired.com/2014/12/hacker-lexicon-air-gap/. Accessed on March 7, 2017.
5. n. 3.

However, in the race to achieve global information dominance and also for their national interests, countries around the world target each other's sensitive data vaults which makes these air gapped computer systems natural targets. Although, theoretically, these air gapped computer systems are impregnable, countries have managed to devise mechanisms that can bypass the security shield and bridge the air gap to extract and transfer data to their data processing safe houses, sabotage the infrastructure or even modify/ delete the data.

In order to breach such high sensitive information operations, various security agencies and Research and Development (R&D) institutions of many countries are in the process of developing a number of tools (hardware/software) and technologies that can help them reach their target data vaults. Also, a few countries like the US have already fielded their specially developed tools and techniques to gather data/ information from various sensitive sources around the world for fulfilling their national interest. And it is common knowledge that such tools are implanted on the target air gapped computer systems through covert methods. Therefore, in the endeavour to understand the threats to air gapped computer systems, it is important to study not only the tools and techniques used to extract the data from the high security computer systems but also to identify the methods by which these tools are implanted into the air gapped computers.

IMPLANT METHODS

Since the target computers/ networks are highly secured in terms of physical restriction of access to the location of these computers, the existence of a number of complex firewalls and other security measures like access keys and passwords, and, of course, the disconnect with the external networks, makes it very difficult to target these air gapped computers systems. Therefore, the attacker has to employ covert tactics in order to gain access to these secured systems, and also, the attacker would require vulnerability inside the computer/network in order to extract data. It is for this reason that certain hardware/ software tools have to be implanted into these systems by the attackers, again, with great difficulty. Since, it is not easy for any outsider to physically gain access to the computers/

networks, the attackers use special methods like 'interdiction' and 'insider exploitation' for implanting the tools into the secured systems.

Insider Exploitation: The general definition of an insider threat is: a malicious threat to an organisation that comes from people within the organisation, such as employees, former employees, contractors or business associates, who have inside information concerning the organisation's security practices, data and computer systems.[6] In the case of exploiting secured air gapped computer systems, apart from manipulating the existing insider, even the attacker could become an insider through legitimate means by going through the recruitment process and joining the organisation. Such instances occur when a state is determined to sabotage its adversary's infrastructure and plant its agents deep inside the adversary's clandestine infrastructures. In other cases, the attacker/s convinces an insider to work for it in return for payment in cash or kind, or even deceives them with smart pranks.

Interdiction: Interdiction is the method by which the attacker would intervene during the supply chain process and place the implant on the device before it gets delivered to the intended recipient. In the case of a secured computer system, when a new system is procured by the organisation or whenever a spare part is requested from the manufacturer, to be delivered to the secured infrastructure, the attacker who keeps a tab on every single action by the target organisation, might intervene in the supply chain process, with or without the knowledge of the manufacturer and divert the product to a safe house. The implants are then fitted in the safe house on the target systems/ parts and then the supply chain process continues towards the intended recipient. When the same contaminated parts are utilised in the sensitive computers/ networks, it becomes easy for the attacker to extract information through the implants.

6. "Combating the Insider Threat", National Cybersecurity and Communications Integration Centre, US Department of Homeland Security, May 2, 2014, https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf. Accessed on April 5, 2017.

DATA EXTRACTION TOOLS AND TECHNIQUES

NSA ANT Catalogue: A Sophisticated Cyber Tools Menu

In December 2013, *Der Spiegel,* the German weekly news magazine, carried a report about a sophisticated programme developed by the National Security Agency (NSA) of the US that consisted of a digital toolbox called the "NSA ANT (Advanced/ Access Network Technology) Catalogue". This article, exposing the development of the programme, was co-authored by Jacob Appelbaum, Judith Horchert and Christian Stöcker. The exposed catalogue reveals the magnitude and variety of digital tools being used by the US intelligence agency to spy on its high valued targets. The operations of the ANT division in the Tailored Access Operations (TAO) Department of the NSA, cover a wide range of activities, from penetration of networks, monitoring mobile phones and computers, to diverting, modifying and even deleting data. The web of networks created by the implants of these sophisticated tools is so wide that it has succeeded in establishing a covert network for the NSA that operates parallel to the internet.

The revealed NSA ANT Catalogue is a 50-page document created in 2008. Its list appears like a mail-order catalogue of digital tools, from which the employees of NSA can order technologies from the ANT division for using them against its targets. The ANT division is part of the NSA's TAO Department and they specialise in covert data-mining and data-skimming operations, especially on specific difficult targets. ANT tools are like elite forces which are moved in only when TAO's usual hacking and data-skimming methods are not sufficient to gather the required information from their target systems.[7] While the ANT division develops both hardware and software required for these digital tools, the catalogue of these tools not only defines the operations of the tools but also gives the price for every tool which ranges from free to US$ 250,000.[8]

Every tool that has been developed by the ANT division has its own special purpose and the operating devices cover almost all

7. Jacob Appelbaum, et al. , "Die Klempner aus San Antonio", *Der Spiegel,* January 2014.
8. "Inside TAO: Documents Reveal Top NSA Hacking Unit", *Spiegel Online International,* December 29, 2013, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html. Accessed on April 6, 2014.

peripherals of the computer world from monitors, cables, USBs, routers, servers, mobile phones and chips in both hardware and software formats. Table 1 lists out the various tools revealed:

Table 1: Various Tools of the NSA ANT Catalogue

Operating Device/Area	**Tools**	**Type of Implant**
VGA (Monitor)	• RAGEMASTER	Hardware
Firewalls	• JETPLOW	Software
	• HALLUXWATER	Software
	• FEEDTROUGH	Extraction technique
	• GOURMETTROUGH	Software
	• SOUFFLETROUGH	Software
Mobile Phones	• DROPOUTJEEP	Software
	• GOPHERSET	Software
	• MONKEYCALENDER	Software
	• TOTECHASER	Software
	• TOTEGHOSTLY 2.0	Software
	• PICASSO	Extraction technique
	• CROSSBEAM	Hardware
	• CANDYGRAM	Set-up of several devices, both hardware and software.
	• CYCLONE Hx9	Hardware
	• EBSR	Hardware
	• ENTOURAGE	Software
	• GENESIS	Technology
	• NEBULA	Hardware
	• TYPHON HX	Hardware
	• WATERWITCH	Hardware
Routers	• HEADWATER	Software
	• SCHOOLMONTANA	Software
	• SIERRAMONTANA	Software
	• STUCCOMONTANA	Software

Servers	• DEITYBOUNCE	Software
	• GODSURGE	Software
	• IRONCHEF	Hardware
USB	• COTTONMOUTH I	Hardware
	• COTTONMOUTH II	Hardware
	• COTTONMOUTH III	Hardware
	• FIREWALK	Hardware
W-LAN	• NIGHTSTAND	Hardware
	• SPARROW II	Hardware
For Surveillance and as Radars	• CTX4000	Hardware
	• LOUDAUTO	Hardware
	• NIGHTWATCH	Hardware
	• PHOTOANGLO	Hardware
	• TAWDRYYARD	Hardware
CPUs	• GINSU	Software
	• IRATEMONK	Software
	• SWAP	Software
	• WISTFULTOLL	Software
	• SOMBERKNAVE	Software
	• HOWLERMONKEY	Hardware
	• JUNIORMINT	Hardware
	• MAESTRO-II	Hardware
	• TRINITY	Hardware
Keyboards	• SURLYSPAWN	Hardware

Analysis of NSA ANT Catalogue

A study and understanding of the functions and operational capabilities of the 50 NSA ANT tools helps us to arrive at the following inferences:

- First of all, it is clear beyond doubt that all these tools are specially customised and developed for special operations which are highly covert in nature, for the purpose of gathering information, sabotage, espionage and surveillance mainly from high valued air gapped computers/ networks. Hence, the mere fact that such tools are available, threatens the very practice of air gapping of sensitive computer systems.

- Although, the functionality of the tools can be mainly associated with military operations, it is not necessarily confined to the military only, as a few tools like Cottonmouth can also be used for non-military operations like in the case of nuclear plants and other research and development organisations or even for industrial espionage.
- A few tools belong to a family called ANGRYNEIGHBOR, which gives the impression that there are more families of tools either under operation or development.
- All the documents disclosed related to the NSA ANT catalogue pertained to the year 2007. It is, therefore, likely that these tools have become obsolete and new versions of the tools and models would have replaced them.
- There are passing references to many new technologies, the utilisation of which does not appear in any of the exposed documents. This means that there are several undisclosed tools developed by the ANT Department whose capabilities are not known.
- The fact that the details of these tools were revealed to the world indicates that there would have been a compulsion for the agency to either abandon these tools on the whole or switch to more covert methods of espionage and surveillance.
- If it was a question of abandoning them, the agency would have abandoned several units of these tools which were operational in the field somewhere across the globe. Identification and examination of these, by the technical agencies of other countries which may lay their hands on them, might uncover more precisely the capabilities of these tools.
- In many instances, both hardware and software tools are implanted on devices manufactured by most widely used brands like Samsung, Cisco, Juniper, Dell, etc. As a result of this disclosure, there arises distrust about these brands which, in turn, creates more hassles for the procurement body of any country in terms of rigorous audit during procurement of such devices, especially for national security purposes.
- Countries like India which are mainly dependent on imports for their defence equipment are most vulnerable because of these US cyber tools.

- It is also revealed from the documents that the NSA implants a few of its tools by the method of interdiction, which emphasises the need for enhancing the safety of any supply chain process, especially that of defence and sensitive equipment, irrespective of its size or function. Also rigorous hardware and software security testing should be made mandatory for any peripheral that is bought for critical infrastructures to identify and neutralise any implants before they are connected to the air gapped systems.
- It also emphasises the need to develop indigenous capabilities for the manufacture of hardware in countries like India which, at present, are heavily dependent on imports and cannot afford to become easy targets for such covert cyber tools and sensitive information seepage.

The information and analyses so far dealt with the capabilities of various tools and techniques developed by the NSA, the technical intelligence organisation of the US. The following sections would cover various methods/ technology developed by academia for extracting information from the air gapped computers.

Air Hopper: Technology to Hack Information Using FM Radio Signals

Air Hopper is a keylogger app that is used to find out what is being typed on a computer or a mobile phone. This technology works with the help of an FM radio receiver included in mobile phones. The compromised mobile phone installed with the Air Hopper app captures keystrokes by intercepting certain radio emissions from the monitor or display unit of the isolated/ air gapped computer system. The technology operates with an effective range of 1-7 m, with effective bandwidth of 13-60 bps, effective enough to steal a password or important phrase from an air gapped computer system.[9]

This technology was developed by security researchers at the Cyber Security Labs at Ben Gurion University in Israel. In order to

9. Mordechai Guri, Gabi Kedma, et.al., "AirHopper: Bridging the Air-Gap Between Isolated Networks and Mobile Phones using Radio Frequencies", *Malicious and Unwanted Software – The Americas (Malware)* (2014), pp. 58-67.

escape from Air Hopper, mobile phones and other devices which have FM radio signal receivers have to be banned in the location of the air gapped computer systems with an effective radius of 10 m.

BitWhisper: Hacking Air Gapped Computers Using Heat

The researchers from Ben Gurion University, Israel, the same university where Air Hopper was developed, have developed another technology known as BitWhisper and unveiled it in March 2015. BitWhisper is a technology that allows hackers to stealthily siphon short information such as passwords or security keys from an air gapped system and send the sensitive data to an internet-connected system using the heat dissipated by the computers.[10]

Computers in general are fitted with thermal sensors in order to trigger the internal fans to cool the computer down if threatened by overheating components such as the CPU, GPU and other motherboard components' heat. BitWhisper technology uses these sensors to send and receive commands using heat waves, thereby forming a heat bridge between the computer systems.[11] The different heat patterns generated from the computer are regulated and binary data is modulated into thermal signals. The adjacent computer in close proximity to the air gapped computer uses its in-built thermal sensors to measure the environmental changes. These changes are then sampled, processed and demodulated into binary data in order to exfiltrate data.[12]

Although the communication using this technology can be bi-directional, it has a few serious disadvantages. They are:

- For this technology to work, a malware has to be first installed not only on the attacker's computer but also on the air gapped computer which itself is a difficult task.
- The attack, as described by the technical paper, only allows the transfer of 8 bits of data per hour, which is miniscule compared

10. Swati Khandelwal, "Hacking Air-Gapped Computers Using Heat", *The Hacker News*, March 24, 2015, https://thehackernews.com/2015/03/hacking-air-gapped-computer.html. Accessed on March 20, 2017.
11. Mordechai Guri, Matan Monitz, Yisroel Mirski, et.al, "BitWhisper: Covert Signaling Channel between Air Gapped Computers using Thermal Manipulations", *eprint arXiv:1503.07919*, March 2015, https://arxiv.org/abs/1503.07919. Accessed on March 21, 2017.
12. Khandelwal, n. 10.

to current data standards, yet, the researchers claim that this data transfer speed is enough to siphon a password or a secret key.

- Moreover, the attack, in its current format, works only if the attacker's system/ laptop is in close proximity to the air-gapped computer—approximately within 40 cm/ about 15 inches from one another.

However, the researchers claim that further research would increase the distance between the two systems and would also increase the data transfer speed considerably. Also, it is believed that in the future, Internet of Things (IoT) devices such as the internet connected fax machine or air conditioner would be used instead of an internet connected system/ laptop for this form of heat dependent attack.

GSMem: Hacking Air Gapped Computer Using low-end Mobile Phones

Once again, researchers from Ben Gurion University, Israel, have developed a technique to exfiltrate data from air gapped computers over the Global System for Mobile Communications (GSM) frequencies using a basic low-end mobile phone. This new attack method requires only a low-end mobile phone and the GSM network, and utilises the electromagnetic waves generated by the air gapped computer. For this attack to be successful, a particular kind of malware known as 'GSMem' should be installed in the mobile phone as well as in the target air gapped computer.

Once this is achieved, the attack exploits the natural capabilities of each device to exfiltrate data. Computers, for example, naturally emit electromagnetic radiation during their normal operation, and cell phones by nature are "agile receivers" of such signals. These two factors combined create an "invitation for attackers seeking to exfiltrate data over a covert channel".[13]

Researchers believe that this attack method would be effective for a range of 30 m. This only means that someone with the right hardware can exfiltrate data even from outside a building or even

13. Kim Zetter, "Researchers Hack Air-Gapped Computer with Simple Cell Phone", *Wired*, July 27, 2015, https://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/. Accessed on March 22, 2017.

from an adjacent building. This method of attack could be avoided by banning the use of mobile phones in a radius of 30-35 m around the air gapped computer location. Also, the biggest drawback of this attack method is its need to have the malware pre-installed on the air gapped computer, which is a big challenge by itself.

DiskFiltration: Data Extraction via Covert Hard Drive Noise

The researchers from the same Ben Gurion University who developed the previous three technologies, have developed one more new technology to steal data from air gapped computers, this time using the hard disk's noise. This new method is known as DiskFiltration which uses the acoustic signals (or sound signals) emitted from the Hard Disk Drive (HDD) of the targeted air gapped computer to transfer the data.[14]

The precondition for this technology to be successful is that the targeted air gapped system should be infected with malware in the first place. Once the malware is in place, the attacker can use this malware to manipulate the "actuator"[15] inside the hard drive which moves on the disk plate while accessing specific parts/blocks of the storage. The attacker can transfer the stolen data by manipulating the movements of the actuator and generate acoustic noise (like the Morse code) that could be interpreted into binary data using a smart phone application from six feet away, at a speed of 3 bit per second or 180 bits per minute.[16]

Replacing the Hard Disk Drive (HDD) with the Solid State Drive (SSD), jamming the hard disk noise by generating static noise in the

14. Mohit Kumar, "New Hack Uses Hard Drive's Noise to Transfer Stolen Data from Air-Gapped computer", *The Hacker News*, August 12, 2016, http://thehackernews.com/2016/08/air-gapped-computer-hacking.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1300.wa0ao08cx4.raw. Accessed on March 22, 2017.
15. An actuator is a component of a machine that is responsible for moving or controlling a mechanism or system. An actuator requires a control signal and a source of energy. The control signal requires relatively low energy which may be electric voltage or current, pneumatic or hydraulic pressure, or even human power. The supplied main energy source may be electric current, hydraulic fluid pressure, or pneumatic pressure. When the control signal is received, the actuator responds by converting the energy into mechanical motion.
16. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici, "DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise", Cornell University Library, August 11, 2016, https://arxiv.org/abs/1608.03431. Accessed on March 23, 2017.

background, using the automatic acoustic management feature to regulate the HDD actuator's movement, and banning of smart phones and other types of recording devices near the air gapped computers' location are a few preventive measures available to overcome the threat posed by the DiskFiltration technique.

LED-it-Go: Data Leak from Air Gapped Computers via Hard Drive LED

The researchers from Ben Gurion University have developed another sophisticated method for covertly leaking data from isolated air-gapped computers. This new method utilises the HDD active LED which exists in most of today's desktop PCs, laptops and servers. A pre-installed malware in the air gapped computer system indirectly controls the HDD LED by turning it on and off rapidly (upto 5,800 blinks per second) – a rate that exceeds the visual perception capabilities of humans but could be captured through the lens of a special kind of camera and light sensors. Sensitive information transferred through the blinking LED is received remotely with the help of special cameras or light sensors.[17]

There are several types of equipment that can play the role of a receiver in this method. These are: local hidden camera, high resolution remote camera, drone camera, camera carried by a malicious insider, compromised security camera and optical sensors. This attack method requires an effective range of Line of Sight (LoS) of the camera or the sensor used to receive the data. The least sophisticated counter measure to avoid this method of attack is to disconnect the HDD indication LED or to cover it with black tape. Another interesting solution would be to quarantine the air gapped computer into a separate room without any windows, with surveillance cameras inside, and restrict and regulate human access to the room.

THE WAY AHEAD

The study of the above mentioned tools, techniques and methods to steal data from air gapped computer systems would invariably

17. Mordechai Guri, Boris Zadov, et. al, "LED-it-Go: Leaking (a lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED", Cornell University Library, February 22, 2017, https://arxiv.org/abs/1702.06715. Accessed on March 24, 2017.

invoke the following question: is the practice of air gapping sensitive computer systems for safekeeping of critical data still a relevant practice?

The simple answer to this question is a big 'Yes'. A deeper understanding of the various tools, techniques and methods highlighted in this article and a few others that exist around the world, would reveal that none of these methods has evolved to a stage where it does not need any assistance. For instance, all the methods developed by the academia explained above work only if the target computer is already compromised with a malware. It should be understood that to compromise an air gapped computer with a malware is itself a difficult task. Over and above that, if compromised by some means such as interdiction or with the help of an insider, there are simple measures available to foil attempts of data leak, using various methods, as highlighted above. If an organisation includes these preventive actions in its Standard Operating Procedures (SOPs), that itself could act as a serious deterrent to these data leak tools and methods.

Considering the development achieved in data leak methods, there are, however, a few takeaway points for the cyber security community that could help organisations and institutions safeguard their critical data.

First and foremost is the need to stay updated with the development of various data siphoning technologies around the world. Knowledge of the various developing methods in this sphere could help the cyber security teams to easily device strategies to enhance the security for the air gapped computers in their organisation and also devise strategies to counter the same.

Besides, updated knowledge on the existing methods of exploitation of air gapped computers could help the cyber security teams to conduct regular audits at the right place, on the right peripherals, and with the right tools and techniques.

The study of the various tools and techniques reveals that different methods have different effective operational ranges and operating bandwidths. Table 2 summarises it all:

Table 2: Different Types of Air Gap Covert Channels and Operational Ranges

Method	Example	Max Bandwidth	Effective Range
Electromagnetic	AirHopper GSMem USBee	48 bit/s 1-1000bit/s 4800 bit/s	~5-10 m
Acoustic	Fansmitter Diskfiltration	900 bit/sec 10K bit/h	~15 m
Thermal	BitWhisper	1-8 bit/h	40 cm
Optical	Keyboard LEDs Screen LEDs Implanted Infrared LEDs Hard Drive LED	150 bit/s 20 bit/s 15 bit/s 4000 bit/s	Line of sight

Source: Mordechai Guri, Boris Zadov, et. al, "LED-it-Go: Leaking (a lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED", Cornell University Library, February 22, 2017, https://arxiv.org/abs/1702.06715. Accessed on March 24, 2017.

Therefore, depending on the availability of space and the criticality of the data stored, organisations could introspect about increasing the radius of the quarantine region around the air gapped computer systems. For instance, if a military organisation has 3 to 5 m as the sanitised region around an air gapped computer, it can increase that radius to 8 to 10 m as technologies have been developed to easily compromise the 5 m air gap.

The practice of interdiction by attackers emphasises the need for hardware and software testing of any new product that is shipped from the vendor (especially a foreign vendor) for use in the air gapped computer system/network. Additionally, the use of indigenously developed hardware and software could be made mandatory for air gapped computers used for critical infrastructures.

Finally, it needs to be noted that air gapped computer systems have succeeded in securing the critical data of many organisations and even states for some time now (except in a very few cases like Iran and the Stuxnet episode). This practice will continue in the future too only with enhanced security levels, increased levels of caution, with more emphasis on the use of indigenous technology and also with high levels of suspicion.

PRESIDENT TRUMP'S HUNDRED DAYS: US-IRAN RELATIONS AND THE NUCLEAR DEAL

HINA PANDEY

On April 29, 2017, President Trump completed 100 days of his ascendance to the White House. Within these 100 days, President Trump appointed important National Security Council (NSC) members who are responsible for guiding the American security and foreign policy. Interestingly, a lot has happened on the US domestic and foreign policy front since then. For instance, the US domestic politics witnessed the shortest tenure of the National Security Adviser (NSA) in American history; a number of presidential executive orders were signed—one such resulted in the travel ban on nationals from Iran, Iraq, Libya, Syria, etc.; the US has withdrawn from the Trans-Pacific Partnership (TPP)—it could have been a promising economic arrangement for the region; and the proposal for a Mexican border wall is being debated financially.

Additionally, President Trump has also authorised the first military action of his tenure in Yemen, air strikes in Syria, and, recently approved the 'Mother of All Bombs' (MOAB-ing) in Afghanistan to sanitise the Islamic State (IS) Khorasan in Afghanistan. Moving on to

Ms **Hina Pandey** is an Associate Fellow at the Centre for Air Power Studies, New Delhi.

the nuclear domain, three important issues have received Trump's attention: these are the US-Russia nuclear cooperation, North-Korea's nuclear capability build-up and the much talked about Iran deal. This article examines the last of these issues, the nuclear agreement between Iran and the international community, as seen from the foreign policy prism of President Trump.

The US Administration's position on the Iranian nuclear deal had been clear ever since the possibility of Trump becoming the next US president came to the forefront. The Administration's current position on the Joint Comprehensive Plan of Action (JCPOA) is focussed on its effective implementation through a rigorous oversight. The hardliners are waiting for Iran to commit a mistake in order to justify calling off of the deal. However, it is also true that the current US Administration is occupied by various other significant foreign-security policy issues on which promises are yet to be delivered. Does that imply a silver lining for the JCPOA? Will the distraction help in sidelining of the Iran issue for some time? Or has the Trump Administration's attitude on the Iran deal changed after its successful implementation in the past one year? Will all this add up to a continuity of Obama's policy on Iran? If so, are relations going to be better? What are the issues that will continue to play spoiler in the US-Iran equation? To answer these questions, an assessment of the new Administration's attitude on Iran and, more specifically, the JCPOA, is imperative. In this context, this article will examine the present status of US-Iran interaction in the absence of any formal diplomatic relations between the two countries.

TRUMP'S ATTITUDE TOWARDS IRAN DEAL

With the election of President Donald Trump, a Republican with a fierce stand on Iran, US-Iran relations were expected to become inevitably more vulnerable. In fact, during his presidential campaign, his position on nuclear issues, including the JCPOA, had been viewed by experts as impulsive and unpredictable. He had indicated many times during his campaign speeches that he would dismantle the P-5+1 nuclear agreement with Iran.In his 2016 speech, he said, "My number one priority is to dismantle the disastrous deal with Iran."[1]

1. Sarah Begley, "Donald Trump's Speech to AIPAC", *Time,* available at http://time.com/4267058/donald-trump-aipac-speech-transcript/. Accessed on April 30, 2017.

There were apprehensions since the beginning that under the Trump presidency, Iran's nuclear debate would be renewed by the Congress itself, especially with a Republican majority in both Houses—this would eventually lead to the calling off of the landmark deal.

Despite all that has been said about the deal, recently the US certified that Iran had complied with the 2015 nuclear framework agreement. The inter-agency review of the nuclear deal has been underway for some time. A few days before the completion of 100 days, the US Department of State certified to US House Speaker Paul Ryan on April 18, 2017, that Iran had been compliant to the commitments under the JCPOA.[2] Interestingly, the main content of the declaration statement appeared in a letter with the misleading title: "Iran Continues to Sponsor Terrorism". This is telling of the reluctance within the Trump Administration to accept the successful implementation of the JCPOA. In the same letter, Iran was also identified as a leading state sponsor of terrorism. Clearly, the friction between the US and Iran on the issue has not diffused, despite Iran's compliant behaviour on the nuclear agreement. Additionally, on the certification issue, some American media reports have confirmed that President Trump had expressed disagreement with the State Department and denigrated personally the certification letter, contending that "Iran is not living up to the spirit"[3] of the nuclear deal.

It can be argued that with the State Department's certification, the Administration might be buying time to assess its action on the Iran deal. In any case, the current US approach on Iran appears to

2. Rex Tillerson, Press Statement, US State Department, "Iran Continues To Sponsor Terrorism", Available at https://www.state.gov/secretary/remarks/2017/04/270315.htm. Accessed on April 20, 2017; Zack Beauchamp, "The Trump Administration Just Quietly Admitted That The Iran Deal Is Working" , *Vox,* April 19, 2017, available at https://www.vox.com/world/2017/4/19/15355726/trump-iran-deal-remaining. Accessed on April 24, 2017; and Aleksandr S. Kolbin, "Why the 'Nonproliferation Complex' Should Help Donald Trump," *The Bulletin of Atomic Scientists*, December 9, 2016, available at http://thebulletin.org/why-%E2%80%9Cnonproliferation-complex%E2%80%9D-should-help-donald-trump10273. Accessed on December 15, 2016.
3. Fred Fleitz, "On Iran, Trump Does the Right Thing and Rebukes the State Department 'Swamp'", *Fox News,* available at http://www.foxnews.com/opinion/2017/04/22/on-iran-trump-does-right-thing-and-rebukes-state-department-swamp.html. Accessed on April 27, 2017.

be in confusion as, in the past three months, voices from within the Trump Administration have sent mixed signals on the nuclear deal. For instance, in the immediate transition period, President Trump's team had examined proposals for new non-nuclear sanctions on Iran, focussing on its ballistic missile developments or human right violations.[4] In the subsequent days, new sanctions were imposed on Iran to punish it for its recent ballistic missile tests in February 2017. Additionally, while announcing the sanctions, the Administration also conveyed its resolve to respond with more sanctions in the future, if the provocations recur. Clearly, the intention was also to signal that the era of sanctions is not over yet. [5] Around the same time, Vice President Pence commented in an interview to ABC news that the White House was also deliberating on whether the US would honour the Iran deal.[6]

A tougher tone on the issue was expressed earlier by Secretary of Defence James Mattis, in his confirmation ceremony. He categorically stated that he would have not signed the nuclear deal with Iran, and offered ideas on how to improve the agreement. Furthermore, he declared that after the confirmation of the NSA team, he would ensure collectively that the terms of the deal are changed to make it better.[7] A similar view was also resonated by Rex Tillerson, who too reiterated, during his confirmation ceremony, that additional areas are to be considered in the JCPOA to limit Iran's progress towards ballistic missile development in the future.[8]

On the other hand, some subtle support on the JCPOA is also visible from within the Administration, especially if assessed in the context of the one year of successful implementation. For instance,it

4. "Trump Team Considering New Non-Nuclear Sanctions on Iran*: FT",* available at http://www.reuters.com/article/us-usa-trump-iran-idUSKBN13R1DE. Accessed on December 12, 2016.
5. David Sanger, "US Impose New Sanctions on Iran Over Missile Test", *New York Times,* February 3, 2017.
6. Ben Wolfgang, "Vice President Mike Pence: White House 'Evaluating' President Obama's Iran Nuclear Deal", *Washington Times,* available at http://www.washingtontimes.com/news/2017/feb/5/mike-pence-vice-president-white-house-evaluating-p/. Accessed on May 2, 2017.
7. "James Mattis on Iran", *Iran Primer*, January 17, 2017, available at http://iranprimer.usip.org/blog/2017/jan/17/mattis-iran. Accessed on May 2, 2017.
8. "Rex Tillerson on Iran", *Iran Primer,* January 12, 2017, available at http://iranprimer.usip.org/blog/2017/jan/12/rex-tillerson-iran. Accessed on May 2, 2017.

must be noted that, contrary to its earlier position, the US has not scrapped the deal but has engaged in an inter-agency review. Additionally, the US is aware of the support to the deal from its European allies. Much before the American presidential election, the European leaders had pledged their resolute commitment to the deal, regardless of the outcome. Thus, in the light of the Iranian compliance and the support from US allies, it can be rightly argued that the US would have to abide by the deal. It is indeed in the US' interest to work with the allies and manage US-Iran relations no matter how difficult they become in the future. In fact, one of the most significant opponents of the nuclear deal, Rex Tillerson, noted in a recent press statement that breaking out of the deal is "not a prudent way to be dealing with Iran".[9] Despite being a staunch critic of the deal, Mattis too is of the opinion that "the United States must live up to its obligations and work with its allies" in keeping the deal.[10]

It is important here to recognise that nothing in the JCPOA prevents Iran's ballistic missile tests or its linkages with terror groups. Thus, as long as Iran continues to implement the deal in accordance with the JCPOA, the US cannot potentially harm the deal's execution. However, the continuous imposition of sanctions on Iran might indirectly impact the deal's execution as Iran's patience would be put to continuous test. Interestingly, the idea of maintaining pressure on Iran can be traced back to the overall strategy of the Obama Administration, which consisted of engaging in negotiations towards a comprehensive agreement on containing the nuclear issue and, at the same time, stressing firmly on US interests vis-à-vis Iran.

CONTINUITY FROM THE OBAMA ADMINISTRATION?

On January 16, 2017, the implementation of the JCPOA completed one year; in the next four days, Donald Trump was sworn in as the 45th president of the United States. What followed thereafter on the Iranian nuclear issue, evidently conveys the continuity from the previous Administration. Of course, the Trump Administration's tone on the issue is staunchly Republican, which is likely to prevent

9. Press Release, "Secretary of State Rex Tillerson Press Availability", April, 19, 2017, US Department of State, available at https://www.state.gov/secretary/remarks/2017/04/270341.htm. Accessed on May 2, 2017.
10. Ibid.

further convergence between the mutual interests, however, one cannot ignore the fact that a stern posture towards Iran and the JCPOA had also been taken by the Obama Administration. In fact, it is the continuity in these issues that is likely to continue impacting US-Iran relations in an adverse manner.

For instance, the renewal of the National Emergencies Act last year by Obama continued to define Iran in terms of a national emergency for US security interests. Until the last few days of his presidency, Obama maintained that Iran "*posed an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States*".[11] The Act remains in place, and it is more than likely that the Trump Administration will continue with it.

In the near future, the US Congress will discuss three new Bills relating to new sanctions on Iran. Interestingly these Bills are continuing from the Obama Administration and Obama had promised to veto them. However, in the new Administration, with the tone on sanctions already set, it is likely that action might be taken. The Bills (HR-5119-No. 2H2o, HR-5631 and HR-4992) expand the scope of the sanctions related to civilian nuclear energy, human rights violations by Iran and its ballistic missile activities respectively.

It must be noted that various key Iranian defence entities such as the Ministry of Defence and Armed Forces Logistics (MODAFL), Defence Industries Organisation, Aerospace Industries Organisation and other missile entities are already under the US sanctions outside of the JCPOA agreement.[12] There is every reason to believe that in the future, if Iran conducts more missile tests, the US would enforce further sanctions. This should be viewed in the light of the fact that the US would have anti-Iran allies to answer to. It is for this purpose that the US would most likely move forward with the Iran policy that is coupled with containment by Iran of the nuclear issue, including

11. "Notice - Continuation of the National Emergency with Respect to Iran", White House Press, March 9, 2016, available at https://www.whitehouse.gov/the-press-office/2016/03/09/notice-and-letter-continuation-national-emergency-respect-iran. Accessed on September 8, 2016.
12. Non-Proliferation Designations, US Office of Foreign Assets Control, US Department of Treasury, January 17, 2016, available at https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20160117.aspx. Accessed on September 1, 2016.

ballistic missile development, as the US considers Iran's programme to be a significant threat to regional security. At the moment, it seems highly unlikely that the American debate surrounding it would diminish in the coming years.

TREND IN US-IRAN RELATIONS: "ENGAGEMENT WITH CONTAINMENT"

Unfortunately, on Iran's part, the most irksome issue remains the American sanctions on its ballistic missiles programme. Those who observe US-Iran relations argue that if the pressure from the US continues, it might not impact the deal so much as it is in Iran's interest to comply with the deal, but as indirect retaliation to the US pressure, a reaction in other areas across the Middle East can be expected. As it is, there is an increasing sense within the hardline factions of the Iranian government that the nuclear deal is one part of a larger Western strategy to push Iran off its revolutionary path. Any more pressure might further reinforce these viewpoints among the conservatives in Iran .[13]

More than a year has now passed since the nuclear deal was concluded. However, not much has changed in US-Iran relations despite a newly opened channel of communication. Even today, the Islamic Republic of Iran is considered one of the most hostile nations towards US interests and vice versa. The two countries have witnessed periods of extreme engagement, estrangement, and nuclear standoff with each other. Unfortunately, a new era of rapprochement is yet to begin in the bilateral relations. The two countries remain estranged on many issues. While there is a generic positivity about the successful implementation of the nuclear deal, it has failed to generate any positivity in the mutually hostile perception of each other.

The ambassadorial relations between the two countries are yet to blossom. The US still operates its consulate in Iran through the Swiss Embassy. For the United States, Iran is still classified under "Country of Particular Concern" (CPC), which calls for further restrictions on

13. Payam Mohseni, " Iran and the US Elections: Observations from a Trip to Iran", *The Bulletin of Atomic Scientists,* December 13, 2016, available at http://thebulletin.org/iran-and-us-elections-observations-trip-iran10284?platform=hootsuite. Accessed on December 15, 2016.

certain imports from, and exports to, it.[14] According to the official statement by the US Department of Treasury, entering into financial agreements with Iranian banks is strictly prohibited. The embargo further extends to the import of technology and goods originating in the US from anywhere in the world. The US continues to deny Iran access to these good and services. [15]

The graph of US-Iran relations post the nuclear deal has been fluctuating, to say the least. On the one hand, there is criticism about the implementation of the nuclear deal, an ongoing inter-agency review of the completion of 90 days of the JCPOA—the final outcome of which is yet to be unravelled—and an increased sanctions debate and escalating nuclear weapon rhetoric expected when President Trump meets Benjamin Netanyahu. On the other hand, the US and Iran are cooperating on trading goods post the conclusion of the deal. Fig 1 below shows that imports from Iran to the US that started after a gap of many years, have increased significantly post the implementation of the JCPOA.

Fig 1: US-Iran Trade

Source: http://iranprimer.usip.org/blog/2017/feb/16/recent-trends-us-iran-trade

14. Executive Summary, Iran 2014 International Religious Freedom Report, available at http://www.state.gov/documents/organization/238666.pdf. Accessed on September 16, 2016.
15. Adam Szubin, "US Treasury Official on Nuclear Deal", United States Institute of Peace, August 6, 2015, http://iranprimer.usip.org/blog/2015/aug/06/us-treasury-official-nuclear-deal Accessed on September 1, 2016.

RECENT TRENDS IN US-IRAN TRADE

In fact, with the opening up of the Iranian economy, more lucrative opportunities for American exports, notably in aviation, have also opened up. Last year, Boeing inked an agreement for the purchase by Iran Air of more than six dozen planes; the reported value was $16.6 billion. The list price of a single 777 exceeds the value of all American exports to Iran last year. Iran has ordered 30 of that model, in addition to 50 Boeing 737 MAX 8s, the total value of which would more than double that of all exports to Iran for the past three decades combined. It is important to note that the Trump Administration appears to be comfortable with it, as Boeing has received permission from the US government for negotiation of the deal On April 4, 2017, Boeing signed an agreement with Iran to sell 30 units of the 737 MAX aircraft to Iran Aseman Airlines, which included the right to buy another 30 at a later date. It is reported that this would create approximately 18,000 American jobs in the future.[16]

While this may signal that all is going well in the US-Iran economic engagement, on the military side, the trend is quite the opposite. In the last one year, approximately 35 naval encounters of an unsafe nature occurred between the two countries. These were viewed by the US as "unsafe and unprofessional," according to the Pentagon spokesman Capt. Jeff Davis. The United States and Iran had 250 run-ins in the first half of 2016 alone, according to US 5th Fleet statistics. [17]

It is true that landmark nuclear agreements have the potential to completely re-shape the dynamics of a bilateral relationship. However, the same cannot be expected of the US-Iran bilateral ties for the time being. The recent trend in the US-Iran relations only adds to this observation.

16. "Boeing Signs $3 Billion Deal to sell Planes to Iran Airline", available at https://www.usatoday.com/story/money/business/2017/04/04/boeing-co-says-signed-new-deal-iranian-airline/100013846/. Accessed on May 3, 2017.
17. "Timeline of US-Iran Naval Encounters", available at http://iranprimer.usip.org/blog/2016/aug/29/timeline-us-iran-naval-encounters. Accessed on May 2, 2017.

THAAD DEPLOYMENT IN SOUTH KOREA: WILL THIS MOVE ALTER CHINA-SOUTH KOREA RELATIONS?

DEBALINA GHOSHAL

In March 2017, the US commenced the deployment of the Terminal High Altitude Area Defence (THAAD) system in South Korea at the Osan air base. Parts of the THAAD system has already arrived in South Korea[1] after South Korea's then acting President and Prime Minister, Hwang Kyo-ahn called for urgent deployment of the THAAD system on the grounds that a nuclear armed North Korea would be "appalling" and "beyond imagination."[2] This decision to deploy the THAAD in South Korea was inevitable as US Secretary of Defence James Mattis and South Korean Defence Secretary Han Min-koo, over a telephone discussion, had agreed to hasten the deployment of the system.[3]

Ms **Debalina Ghoshal** was formerly an Associate Fellow at the Centre for Air Power Studies, New Delhi.

1. Paula Hancocks and Joshua Berlinger, "Missile Defense System that China Opposes Arrives in South Korea", *CNN,* March 8, 2017, http://edition.cnn.com/2017/03/06/asia/thaad-arrival-south-korea/Accessed on March 15, 2017.
2. Dagyum Ji, "S. Korean PM Calls for Urgent THAAD Deployment After DPRK Missile Test", *NK News,* March 6, 2017, https://www.nknews.org/2017/03/s-korean-pm-pushes-for-urgent-thaad-deployment-after-dprk-missile-test/ Accessed on April 1, 2017.
3. Hancocks and Berlinger, n. 1.

However, it was a known fact that the deployment of the THAAD system in South Korea would spark criticism from China, which has time and again, opposed it. In fact, the Chinese Foreign Ministry expressed its discontent by announcing that Beijing maintains "firm opposition and strong dissatisfaction" about the defensive system.[4] The THAAD system is believed to be crucial for South Korea to mitigate the missile threats from North Korea. But the decision to deploy the THAAD in South Korea was not an easy one for Seoul, especially amid the burgeoning relations between Beijing and Seoul which Seoul knew would be jeopardised with its deployment.

Moreover, South Korea, which had hoped that China would play a pivotal role in the North Korean nuclear crisis, was disappointed with China's lackadaisical effort to solve the nuclear conundrum. It is against this background that this paper analyses the rationale for South Korea to deploy the THAAD, the Chinese and South Korean reactions on its deployment and what the THAAD deployment holds for South Korea-China relations.

THE RATIONALE FOR THAAD IN SOUTH KOREA

The North Korean Threat: As soon as reports came in that the United States had commenced sending parts of the THAAD system to South Korea, US Pacific Commander, Adm Harry Harris, stated, "Continued provocative actions by North Korea…. only confirm the prudence of our alliance decision last year to deploy THAAD to South Korea."[5] Despite the United Nations Security Council (UNSC) prohibiting North Korea from test firing ballistic missiles, North Korea has continued to defy the UNSC Resolutions over the years. These resolutions include the most recent Resolution 2321, implemented on November 30, 2016, which demanded that North Korea reestablish its pre-existing moratorium on testing of missiles.

North Korea has also conducted five nuclear tests despite the UNSC Resolutions—in 2006, 2009, 2013, and two tests in 2016.

4. Lindsay Maizland, "The Surprising Reason Why China is Blocking South Korean Music Videos and TV", *Vox,* March 7, 2017, http://www.vox.com/latest-news/2017/3/3/14795636/china-south-korea-pop-culture-kpop-attacks-thaad. Accessed on March 10, 2017.
5. James Pearson and Ju Min Park, "US Starts Deploying Anti-Missile in South Korea After Defiant North's Latest Rest", Reuters, March 7, 2017, http://uk.reuters.com/article/uk-northkorea-missiles-idUKKBN16C0ZH. Accessed on March 10, 2017.

All its ballistic missile systems are nuclear capable and that has caused concern in South Korea and in the United States, which has its forward deployed forces stationed in South Korea. In a recent interview in April 2017, a North Korean government official declared that the country would "never stop" its nuclear tests as long as the US continued what North Korea views as "acts of aggression."[6] In fact, the decision to send parts of the THAAD to South Korea came a day after North Korea fired four ballistic missiles into the Sea of Japan.[7] The White House spokesman, Sean Spicer viewed these missile tests as "provocative behaviour" and sought to take defensive actions against the missile threats, including the deployment of the THAAD battery in South Korea.[8] In response to the North Korean ballistic missile tests, a US official had already stated, "[b]eefed-up missile defence is among the economic and military options being weighed in a White House review of policy toward nuclear-armed North Korea, expected to be completed in coming weeks."[9] It was quite obvious that the THAAD was to be deployed at the earliest. Hence, along with the Patriot defence system and Korea's indigenous Korean Air and Missile Defence (KAMD), the THAAD system would strengthen Korea's 'defence by denial' capability vis-à-vis North Korea.

China's Lackadaisical Approach: Despite the looming threat from North Korea, South Korea did not deploy the THAAD system on its territory for a while due to the Chinese concerns and apprehensions regarding the system. South Korea had hoped that China would impose sanctions on North Korea for its nuclear and ballistic missile programmes but was disappointed due to the lack of any stringent action from China's side. In addition, the then South Korean President Park Guen-hye had wished to normalise relations with North Korea, based on cooperation and goodwill, a policy she termed as "trust politik". This policy needed China's support to actively deal with North Korea, and prevent further nuclear and missile tests from

6. Will Ripley, Tim Schwarz, Ben Wescott, "Nuclear Tests Will 'Never Stop', North Korean Government Official Says", *CNN*, April 27, 2017, http://edition.cnn.com/2017/04/26/asia/north-korea-official-nuclear/ Accessed on April 28, 2017.
7. "North Korea Fires Four Missiles Toward Japan, Angering Tokyo and South Korea", *Reuters*, March 6, 2017, http://www.reuters.com/article/us-northkorea-missiles-idUSKBN16C0YU. Accessed on March 7, 2017.
8. Ibid.
9. Ibid.

taking place, but China failed to support South Korea to make the policy of "trust politik" a success. For South Korea, China was crucial to resolving the North Korean nuclear crisis, as it felt that Beijing's close alliance with the Hermit Kingdom would influence the latter to rethink its nuclear and ballistic missile programme. However, Beijing, on the other hand, clarified that despite North Korea being an ally, it had no influence on the latter's nuclear and missile programme.

China is North Korea's biggest trading partner, the source for food, energy and arms, and a key player in the nuclear issue in the Korean peninsula. China's expression of dissatisfaction over the North Korean nuclear issue, at least in the past, has only been a sham. Despite all its commitments to impose sanctions on North Korea, China's trade relations with North Korea have continued. In March 2016, China's Foreign Minister Wang Yi, instead of supporting complete sanctions on trade with North Korea, recommended a "suspension for suspension" policy in which he called on North Korea to suspend its nuclear and missile programme but in exchange, a suspension of the US-South Korea military exercise. [10]

CHINESE REACTIONS TO THE THAAD DEPLOYMENT

China has not perceived the deployment of the THAAD in South Korea in a positive light, as it views this defence system as strategically destabilising. A Chinese spokesperson had raised concerns that the system "will jeopardise security and the strategic interests of regional countries, including China, and undermine the strategic balance in the region."[11] China also fears that the radar (AN/TPY-2) that is a component of the THAAD system would provide the United States greater leverage to track Chinese long range ballistic missiles.[12]Also, according to Beijing, a US missile defence system in the Asia-Pacific region negates China's own nuclear deterrent capability and would

10. "China Proposes US-N. Korea Suspension", *Taipei Times,* March 8, 2017. Accessed on March 15, 2017.
11. Ben Rosen, "Why China is Strongly Objecting to South Korea's THAAD Development," *The Christian Science Monitor,* March 1, 2017, http://www.csmonitor.com/World/Asia Pacific/2017/0301/Why China is strongly objecting to South Korea's THAAD developmentsMarch1, 2017. Accessed on March 31, 2017.
12. Abraham Denmark, "China's Fear of US Missile Defense is Disingenuous", *Chicago Tribune,* March 21, 2017, http://www.chicagotribune.com/news/sns-wp-china-comment-b7e5a026-0e27-11e7-9b0d-d27c98455440-20170321-story.html. Accessed on March 25, 2017.

only strengthen the US' foothold in the region. This concern that the THAAD would undermine China's security has been raised by China's Foreign Minister Wang Yi. Hence, wary of this destabilisation, China's Ministry of Foreign Affairs spokesperson has warned South Korea that it would bear the "potential consequences"for the deployment of the THAAD system. In fact, Wang has alerted South Korea on the probability that the THAAD would make South Korea less secure.[13]

In November 2016, during the implementation session of Resolution 2321, China had urged the global order to resume the Six Party talks, including a peace treaty. It is noteworthy to mention here that North Korea too seeks a peace treaty with the US as post Korean War in the 1950s, there has been only an armistice between the two countries. In March 2013, North Korea, however, declared the armistice of 1953 that ended the Korean War as invalid.[14] In a recent editorial in China's state run daily, *The Global Times*, China warned, "[t]he United States has deployed a missile defence system right in front of China's door, and they must pay for that decision." The editorial further stated, "China must make sure the THAAD deployment is being made in vain, by strengthening its own nuclear deterrent." [15]

INTERNAL CONFLICT

The dissatisfaction over the THAAD deployment in South Korea is not confined to China or North Korea. There is also discontent in South Korea regarding the decision to deploy the THAAD system. Opposition parties like the Democracy Party have expressed dissatisfaction over the decision to deploy the THAAD system without approval from the National Assembly. Though Moon Jae-in of the Democracy Party voices support for the US-South Korea alliance, he has demanded that the decision to deploy the THAAD be postponed until after elections, and, instead, has been in favour of resuming the

13. Ibid.
14. Madison Park, "North Korea Declares 1953 Armistice as Invalid", *CNN,* March 11, 2013, http://edition.cnn.com/2013/03/11/world/asia/north-korea-armistice/ Accessed on April 1, 2017.
15. "China Must Strengthen Nuclear Arsenal in Response to THAAD Deployment: State Media", *RT.com,* March 10, 2017, https://www.rt.com/news/380068-china-nuclear-response-thaad/ Accessed on March 15, 2017.

dialogue and reconciliation with North Korea.[16] Before the elections, Moon-Jae and his party had also thought of conducting a summit with China to discuss with it the crisis over the deployment of the THAAD system.'[17] The impeachment of President Park Guen-hye has resulted in the Opposition party, the Democracy Party coming into the limelight, with a more China- friendly attitude. In fact, as Moon Jae became the president of South Korea in the recent elections, he has promised to resolve the North Korean nuclear crisis, and wishes to rejuvenate the old 'Sunshine Policy' which was neglected over the last decade due to South Korea's attempt to befriend the United States that led to the isolation of North Korea.

THAAD AND CHINA-SOUTH KOREA RELATIONS

Nevertheless, the THAAD deployment may not prove conducive for South Korea-China relations, even though relations between the two countries in the recent past have been improving. That the relations would be soured was expected as far back as in 2014 itself, when the Chinese state owned Xinhua News Agency warned, "South Korea will sacrifice its fast-developing relations with China if it should be seduced into the [THAAD] defence network, ignoring the protests of the largest economy in Asia."[18] In the state run daily, *Global Times*, it was proposed that the "Chinese society should coordinate voluntarily in expanding restrictions on South Korean cultural goods and entertainment exports to China, and block them when necessary."[19] China had already imposed undeclared sanctions on South Korea right after South Korea's decision to deploy the THAAD system in 2016.

In 2016, there had been cancellations and possible bans on South Korean TV series as well as K-pop music videos in China while

16. Brian Padden, "South Korean Impeachment Intensifies Divide Over THAAD", *Voice of America,* March 3, 2017, http://www.voanews.com/a/south-korea-impeachment-thaad/3748027.html. Accessed on March 20, 2017.
17. Christine Kim, "South Korea Opposition to Seek Summit with China if Front Runner Elected", *The Wire,* April 13, 2017, https://thewire.in/123700/south-korea-opposition-seek-summit-with-china-if-frontrunner-elected/ Accessed on April 25, 2017.
18. Quoted in Debalina Ghoshal, "How Will THAAD Affect Seoul-Beijing Relations?," *Strategic Review,* September 7, 2016, http://www.sr-indonesia.com/web-exclusives/view/how-will-thaad-affect-seoul-beijing-relations. Accessed on April 15, 2017.
19. Rosen, n.11 .

there was a call in China for a total boycott of South Korean goods. According to the state-owned Korea Creative Content Agency, "China, including Hong Kong, was the second-biggest importer of South Korean books, comics, music, video games, movies, animation and other content, accounting for 24 per cent of those types of exports at $189.9 million in 2014."[20] This is because South Korean products are very popular amongst the Chinese. South Korea's Lotte Group, a Korean conglomerate that is providing the land for the deployment of the THAAD is already facing the brunt in China where it has established its business. A massive project of the Lotte Group in China's northeastern city of Shenyang was put on hold in December 2016 and recently the conglomerate was also charged 44,000 Chinese yuan for violating Chinese advertising laws.[21] All these incidents happened despite the then South Korean President, Park Guen-hye's attempt to normalise relations, marked by a visit to China in 2015 to attend the Chinese military parade marking the 70th anniversary of end of World War II.[22]

There are reports that China has asked its tour agencies to stop trips for tourists to South Korea. In January 2017, China also banned the import of 19 South Korean beauty products and the Chinese General Administration of Quality Supervision, Inspection and Quarantine refused to approve of some of the South Korean cosmetics, resulting in a decline in the stocks of cosmetics in South Korea.[23] Though Korea's Ministry of Food and Drug Safety claimed that the products had failed to meet China's cosmetics related regulations,[24] it was widely assumed that the reason for the ban was the THAAD issue.

20. Christopher Bodeen and Youkyung Lee, "Pop Stars, Diplomacy Victims of Cooling China S. Korea Ties", *Associated Press,* August 10, 2016, http://bigstory.ap.org/article/a085bd1d4ba549ba8e76b27a219d386a/pop-stars-diplomacy-victims-cooling-china-korea-ties. Accessed on April 10, 2017.
21. Padden, n.16.
22. Scott A. Snyder, "Why South Korea's President Park Attended Xi's Military Rally in Beijing," *Newsweek,* September 4, 2015, http://europe.newsweek.com/why-south-koreas-president-park-attended-xis-military-rally-beijing-332528?rm=eu. Accessed on April 10, 2017.
23. Yoon Ja- Young, "China Bans Imports of 19 Korean Cosmetics", *South China Monitoring Post,* January 11, 2017, http://www.scmp.com/news/asia/east-asia/article/2061152/china-bans-imports-19-korean-cosmetics. Accessed on April 10, 2017.
24. "China's Import Ban on Korean Cosmetic Products", *KBS World Radio,* January 16, 2017, http://world.kbs.co.kr/english/program/program_economyplus_detail.htm?No=5894. Accessed on April 15, 2017.

Though in 2015 South Korea joined the China led Asian Infrastructure Investment Bank (AIIB), in July 2016, reports came in that China had demoted a South Korean vice president of the AIIB to a directorial position on allegations of an accounting scandal. Many analysts felt that this was a direct result of the then decision of South Korea to consider deploying the THAAD in its territory. In January 2017, Korea's Finance Minister, Yoo Il-ho, expressed concern on several suspected cases of non-tariff barriers in bilateral trade since July 2016.[25] China is South Korea's largest trading partner and the THAAD could have negative repercussions on these relations, especially on the Free Trade Agreement (FTA) as well as on the Regional Comprehensive Economic Partnership. What is making matters worse is that South Korea complains that it has no proof against China that these trade restrictions on South Korea are a result of the THAAD deployment since, according to South Korean Finance Minister Yoo ll-ho, China did not directly say it was targeting South Korean firms.[26]

In March 2017, there were reports that the Lotte Group was the victim of a cyber attack by Chinese hackers. Moreover, Chinese protestors were seen organising a rally in protest at Lotte's land swap for the THAAD deployment, holding placards that stated, "Lotte issued a declaration of war against China and Lotte should leave China right now."[27]

Apart from economic and trade related actions, China could also take strategic actions vis-à-vis South Korea. Beijing and Seoul are already entangled in a territorial dispute regarding the Socotro Rock in the East China Sea. In 2015, China reiterated its demands that the island should be named as Suyan Reef as Beijing feels that the territory falls under its own jurisdiction. In 2013, China had declared an Air Defence Identification Zone (ADIZ) in the East China

25. "China Turns Screw on Corporate South Korea Over US Missile Shield", *Financial Times*, January 5, 2017, https://www.ft.com/content/00a51c58-d25d-11e6-9341-7393bb2e1b51. Accessed on April 20, 2017.
26. Jack Kim and Christine Kim, "Top South Korean Presidential Candidate Demands China Stop Retaliation Over THAAD", *Reuters*, March 14, 2017, http://www.reuters.com/article/us-southkorea-china-idUSKBN16L0J7. Accessed on April 20, 2017.
27. "Lotte's Chinese Website Hacked in Protest of US Missile Defense System," *Yonhap News Agency*, March 1, 2017, http://english.yonhapnews.co.kr/business/2017/03/01/28/0503000000AEN20170301005600320F.html. Accessed on April 20, 2017.

Sea. Anti-missile drills are already being conducted by China, with cooperation from Russia. Moreover, Chinese long range missiles are equipped with counter-measures to evade enemy missile defence systems. Recently, in April 2017, there were reports that China had attempted hacking of the THAAD system in South Korea. This is being done to either develop THAAD-specific counter-measures or THAAD-specific mechanisms that would disrupt and jam the system.[28]

THE SILVER LINING IN THE CHINA-SOUTH KOREA RELATIONS

Amid the growing bitterness in the South Korea-China relations, there is still a silver lining: in April 2017, Seoul and Beijing discussed ways to impose tougher sanctions on North Korea.[29] In February 2017, China had also banned coal imports from North Korea as a step to penalise it for continued missile testing, despite the UNSC sanctions.[30] In March 2017, reports came in that South Korea and China would join talks with the member states of the Trans-Pacific Partnership to discuss a broader scope for Asia-Pacific trade integration.[31] In April 2017, there were reports that Chinese traders were not providing those goods to North Korea that were on the UNSC sanctions list, and those that did, were having the goods checked at the Chinese customs. However, for non-sanctioned products, business between the Chinese and North Korean traders is going on as usual.[32]

28. Iain Thomson, "China 'Hacked' South Korea to Wreck Star Wars Missile Shield", *The Register*, April 21, 2017, https://www.theregister.co.uk/2017/04/21/china_accused_south_korea_hack/ Accessed on April 22, 2017.
29. "China, South Korea Discuss More Sanctions on North Korea Amid Talk of Trump Action", *Reuters,* April 10, 2017, http://in.reuters.com/article/northkorea-nuclear-idINKBN17C0A2 Accessed on April 15, 2017.
30. Steven Jian, "China Bans All Coal Imports from North Korea Amid Growing Tensions", *CNN,* February 20, 2017, http://edition.cnn.com/2017/02/19/asia/china-coal-north-korea-ban/ Accessed on April 15, 2017.
31. Nyshka Chandran, "After US Drops TPP, China Joins Member States in Trade Talks", *CNBC,* March 14, 2017, http://www.cnbc.com/2017/03/14/china-south-korea-join-tpp-members-in-trade-talks.html. Accessed on April 1, 2017.
32. Tom Mitchell and Xinning Liu, "China's Trade with North Korea Targeted by Trump", *Financial Times,* April 23, 2017, https://www.ft.com/content/14e6fe4c-27e0-11e7-9ec8-168383da43b7. Accessed on April 25, 2017.

CONCLUSION

South Korea is trying to convince China that the THAAD is a defensive capability meant to counter the North Korean threat and does not pose a threat to China. However, China's apprehensions of increased US influence in the Asia-Pacific region are least likely to make China buy this explanation. China's common practice is to achieve political and foreign policy goals by imposing harsher trade restrictions on the concerned country, and there is little doubt that it would practise the same against South Korea this time. According to a former senior Chinese official, Yang Xiyu, "China can see benefits only for a US regional plan, not for South Korea's national security interest."[33] However, all said and done, the progress of the THAAD deployment in South Korea would depend on the new president of South Korea. China expects the new South Korean government to take the Chinese concerns into consideration and deal with the THAAD issue "appropriately". It is only a matter of time to see how Moon deals with the THAAD issue without upsetting the United States or China and, at the same time, resolves the issues with North Korea.

33. Gerry Mullany and Michael R. Gordon, "US Starts Deploying THAAD Anti-Missile System in South Korea, After North's Tests", *The New York Times,* March 6, 2017, https://www.nytimes.com/2017/03/06/world/asia/north-korea-thaad-missile-defense-us-china.html. Accessed on April 10, 2017.

THE GROWTH OF TEHRIK-E-TALIBAN PAKISTAN

SHREYA TALWAR

INTRODUCTION

The beginning of the year 2017 was marked by an upsurge in terrorist attacks all across Pakistan. Starting with an Improvised Explosive Device (IED) explosion in Parachinar of the tribal region's Kurram Agency on January 20, it continued with a string of suicide bombings in Lahore, Peshawar, Mohmand Agency and Sindh. Seventy-two people were killed and over 200 injured after a suicide bomber struck in the midst of devotees at the shrine of Lal Shahbaz Qalandar in Sehwan town, located in Karachi.[1] It was one of the most lethal attacks in Pakistan by militant groups in the last few years. These attacks were executed by the Tehrike-e-Taliban Pakistan (TTP) and other sectarian groups they are associated with.

After the launch of the military operation 'Zarb-e-Azb' in mid-2014 to clear out the TTP strongholds in the region, the security situation did appear to be better, and saw a downward trend in terrorist attacks. However, despite the fall in the number of terrorist attacks, terrorism is certainly continuing to spread across Pakistan. By

Ms **Shreya Talwar** is a Research Associate at the Centre for Air Power Studies, New Delhi.

1. Z.Ali and Hafiz Tunio, "Bloodbath at Sehwan Shrine," *The Express Tribune*, February 17, 2017, at https://tribune.com.pk/story/1329603/bloodbath-sehwan-shrine. Accessed on March 20, 2017

December 2016, violent activities in the tribal areas had dropped by 14 percent, but overall terrorist incidents had gone up by 4 percent in the urban heartland.[2] Provinces such as Punjab and Sindh which were earlier unused to any Taliban selected activities, are seeing a surge in terrorist attacks.

The military operations led by the Pakistan Army were able to destroy some of the bases and strongholds of the TTP. However, the TTP continues to be a potent threat to Pakistan's national security. According to the annual report of the Lahore-based think-tank, Pakistan Institute for Peace Studies (PIPS), although there has been a decline in militancy in 2016, the TTP managed to carry out 106 attacks and is a major contributor to the instability within Pakistan.[3] The TTP has been a distinct terrorist organisation. There were always groups in Pakistan with anti-state objectives in the past as well, but they decided to bond together for the first time under a single banner—the TTP. The group was able to forge multiple alliances with other groups having different backgrounds, tribal affiliations and motivations, which acted as force multipliers and increased its lethality and operational effectiveness. For the first time, a group like the TTP made inroads into the urban centres of Punjab and attacked the army on its home front as retribution for the military operations in the tribal regions. The TTP has managed to survive and it is intriguing to understand how it has been able to for so long.

The law and order situation in Pakistan is also deteriorating. There has been a phenomenal rise in heinous crimes in all the provinces of the country. Crimes like murder, kidnapping for ransom and bank robberies have increased at an average of 17.86 percent as compared to the figures of 2007, according to the National Crime Data (NCD).[4] Moreover, the dangerous nexus of militants and crime syndicates directly contributes to the high rates of organised crime in both urban and tribal regions.

2. Iftikhar Firdoos, "Terror Returns: We Need To Look Inwards," *Express Tribune*, February 27, 2017, at https://tribune.com.pk/story/1335015/analysis-need-look-inward. Accessed on March 20, 2017.
3. "Pakistan Security Report," *PIPS Research Journal*, vol.9, no.1, 2016, p.5, at http://www.pakpips.com/downloads/325.pdf. Accessed on March 15, 2017.
4. "Crime Report of Five Years Issued," *The News*, March 29, 2013, at https://www.thenews.com.pk/archive/print/629546-crime-report-of-five-years-issued. Accessed on March 20, 2017.

The paper looks into how a local movement has grown to become a deadly insurgency in Pakistan within a few years. It also throws light on how the TTP has been able to become a distinct force due its organisational structure, goals and strategies that have been the driving forces of its growth and survival.

BACKGROUND

The dawn of this century witnessed a shift in the paradigm of terrorism with the rise of well organised terrorist groups and sophisticated extremist infrastructure. The ignorance about the potent nature of terrorism came to an end through a rude awakening in the form of the 9/11 attacks. These attacks set in motion a series of events that shifted the principle operational and ideological source of threat from Afghanistan to Pakistan's tribal areas.[5] The situation in the Federally Administered Tribal Areas (FATA) began to change after the influx of foreign fighters in 2002. Al Qaeda and its associates began to plan attacks against the coalition forces in Afghanistan. It was joined by the Haqqani network and Gulbudin Hekmatyar of the Hizb-e-Islami. Pakistan agreed to be a partner in the "War on Terror" with the Americans in exchange for material and financial support. The Pakistan Army was deployed in the FATA regions to weed out 'foreign terrorists'. The launch of drone strikes to kill Al Qaeda's members and destroy its bases in the tribal regions of Pakistan resulted in heavy civilian casualties. The Pakistani state's support for the drone strikes and military operations against Al Qaeda, led to the formation of an anti-Pakistan coalition in the form of the TTP.

Within a few months of its inception, the TTP was able to consolidate its foothold in South Waziristan and adjacent areas. The tribal areas of FATA steadily fell to the Taliban groups and the "Waziristan Shura" came into being. Military operations proved ineffective initially because the militants rejected any offers of ceasefires. In 2007, the agencies of South and North Wazirisitan were turned into no go areas for Pakistani state representatives and security forces. The TTP demonstrated their fighting skills by capturing 300 Pakistani soldiers in August 2007. The TTP started extending its

5. Rohan Gunaratna and Khurram Iqbal, *Pakistan: Terrorism Ground Zero* (London: Reaktion Books, 2011), p.36.

influence to the adjacent settled areas of Khyber Pakhtunkhwa (KPK) after consolidating its structure in FATA.

Initially restricted to the tribal areas of Pakistan, the TTP proved to be expansionist. The following section analyses the different factors that enabled the TTP to grow into a lethal phenomenon across Pakistan.

ORGANISATIONAL STRUCTURE OF TTP

Unlike other terrorist groups, the TTP is not a centralised and united movement, but a decentralised one composed of different nodes of leadership and local commanders coalesced under a common umbrella, seeking to coordinate their activities. It may be understood as a network of franchises through which the TTP maintains the strength of its 'operational capability'. These regional commanders are self-sufficient and have liaison management mechanisms in place to coordinate with sub-organisations or other terrorist groups.

The structure of the TTP is similar to the model of a 'coming together federation'. In this case, the independent groups come together to form a single entity by pooling their sovereignty while maintaining their identity in order to enhance their overall security. The constituent groups carry out their activities independently according to the goals of the organisation. Similarly, the TTP was organised around a 40-person council, or *shura* (parliament), with representatives from all seven tribal agencies of FATA and from the KPK's settled districts of Swat, Bannu, Tank, Lakki Marwat, Dera Ismail Khan, Kohistan, Buner, and Malakand. It meets very often to plan tactics and discuss strategies and the *amir* (president) holds press conferences and gives statements or speaks through a spokesperson fairly often. Given its umbrella structure, however, it appears that the TTP's participating militias and their field commanders make tactical decisions themselves as opposed to following orders from the *amir* or *shura*.

The TTP is currently headed by its Amir Mullah Fazlullah, and Sheikh Khalid Haqqani is his deputy. Shakeel Ahmed Haqqani is the head of the political *shura* of the TTP, and Qazi Hammad, the *qazi* or chief justice.

The nature of the TTP is not rigid and continuously changes due to various divides and splintering within the organisation. The constituent members of the TTP often separate from the group due to divergent motives and actions but also reunite to fight against a common external threat.

GOALS AND STRATEGIES EMPLOYED BY TTP

The TTP's proclaimed goals are "to enforce *Shariah*, to unite against the NATO forces in Afghanistan and do defensive *jihad* against the Pakistan Army."[6]

The TTP's first major goal is to unite against the North Atlantic Treaty Organisation (NATO) forces in Afghanistan. The military operations and drone strikes conducted in Afghanistan and the FATA region post the 9/11 attacks by the United States in order to hunt down Al Qaeda and other foreign fighters resulted in the anti-US/NATO stance of the TTP. They sought to seek revenge for the interference in their region, and for the heavy civilian casualties from the drone strikes. This further allows the TTP to gain legitimacy in the eyes of the locals and other groups since the fight in Afghanistan is a common grievance and a matter of valour and honour.

The second goal announced by the TTP was "defensive *jihad* against the Pakistan Army." The Pakistan Army was considered apostate and corrupt due its allegiance and support to the US-NATO forces, and its joining the "War on Terror". Moreover, the army's presence in the tribal areas in the form of checkposts and raids was unacceptable to the locals given how the army had never been present in the region earlier, according to an understanding with the state of Pakistan at the time of its formation.

Third, the TTP seeks to enforce the *Shariah* in order to gain social control in Pakistan. Its specific interpretation of the *Shariah*, similar to that of the Quetta Shura Taliban, is austere and manifested in the establishment of parallel *Shariah* courts and in the reformation of the society along the rigid Deobandi lines, as it sees the Pakistani government as being corrupt and apostate.

6. Samir Puri, *Pakistan's War on Terrorism: Strategies for Combating Jihadist Armed Groups Since 9/11* (New York: Routledge, 2012), p.75.

Although, there are several disagreements within the TTP, what binds the group together is a common purpose to establish an Islamic state in Pakistan that is based on *Shariah* law, to resist any attempts to counter this goal and to support efforts to expel the coalition forces in Afghanistan. The TTP's strategies, discussed in the following section, are in pursuit of these goals.

STRATEGIES OF THE TTP

The TTP's strategies can be understood as follows:

First, the TTP carried out a war of attrition against the government by repeated attacks on the Pakistani military infrastructure and civilians. It executed suicide and rockets attacks on numerous military bases in Pakistan, attacked government building and schools. However, this led to a serious backlash from the Pakistan government. A series of military operations was launched in the tribal regions by the Pakistan Army with the objective of destroying the group's bases. It reduced the number of attacks as the bases were destroyed. Thus, the TTP, in order to bear the cost of continuing this war of attrition against the government, *forged links with terrorist groups in Punjab and Karachi*. It allowed them to retain their operational capability and hold out against the military operations against it. As a result, even though the number of attacks went down, the TTP was able to geographically extend itself through its network, and execute attacks in Punjab and Sindh, which had earlier, not seen any sort of Taliban activity.

Second, the TTP included the sectarian agenda as part of its smaller objectives, and strengthened its relationships with sectarian groups such as Sipah-e-Sahaba Pakistan (SSP), Lashkar-e-Jhangvi (LeJ), Harkat-ul-Jihad-al-Islami (HuJI) et al. The TTP has played a major role in some of the worst sectarian attacks, particularly in the Kurram and Khyber Agencies where the Shia population is higher. By exploiting the sectarian differences, the TTP has been able to consolidate its Sunni constituency as well.

Third, terrorist groups intimidate the local people in the region as a strategy to "overthrow the government and gain social control over the population."[7] It is well known that the writ of the government

7. Andrew H. Kydd and Barbara F. Walter, "The Strategies of Terrorism," *International Security*, vol. 31, no. 1, pp. 49-80, see http://www.jstor.org/stable/4137539.

and rule of law in the FATA and KPK are poor. Taking advantage of this, the TTP has used a combination of intimidating the local tribal leaders and targeting the limited administrative infrastructure in the tribal areas. Tribal leaders, '*maliks*', who serve as interlocutors between the political agents and the locals, have been killed by the TTP.[8] The killing of the tribal leaders fulfils two aims of the terrorists. One, they use it as a tool to coerce the local people to obey their orders; and two, they destroy all lines of communication between the Pakistan government and the tribal people in the region. The elimination of *maliks* has destroyed the most likely resistance to the Taliban control.[9] In December 2008, the TTP officially imposed the *Shariah* in Orakzai Agency located in FATA, [10] and the population was forced to submit to the terrorists as a result of the campaign against their tribal leaders.

Fourth, a provocation strategy is an attempt to induce the enemy to respond to terrorism with indiscriminate violence, which radicalises the population and leads them to support the terrorists.[11] The strategy attempts to convince the local population that the attacks on the Pakistani military are justified due to the aggressive military operations carried out by it in the region.

RECRUITMENT STRATEGIES

The basic condition for a terrorist group to sustain itself is a continuous feed of recruits. The TTP has often invoked its objective to fight against the Western forces present in Afghanistan and the US attacks in Pakistan's tribal region to gain legitimacy and the support of the local population; essentially using revenge as a driver of recruitment. Selective employment of the tribal Pashtunwali code accentuates their recruitment objectives. TTP cadres reportedly regularly visit refugee camps and recruit those wanting to avenge the death of family members killed by the Pakistani military or who are frustrated

8. Tayyab Ali Shah, "Pakistan's Challenges in Orakzai Agency," Combating Terrorism Centre, July 3, 2010 at https://www.ctc.usma.edu/posts/pakistan%E2%80%99s-challenges-in-orakzai-agency. Accessed on March 20, 2017.
9. Dexter Filkins "Right at the Edge" *The New York Times Magazine*, September 5, 2008, at http://www.nytimes.com/2008/09/07/magazine/07pakistan-t.html. Accessed on March 20, 2017.
10. Raheel Khan "Militancy and Conflict in Orakzai Agency," New America Foundation, April 19, 2010.
11. David A. Lake, "Rational Extremism: Understanding Terrorism in the Twenty-first Century," *Dialog-IO*, vol. 56, no.2, Spring, 2002, pp.15-29.

and angry with the government for the lack of basic human facilities in these camps.

The TTP's insurgency is a complex conflict featuring not just anti-state conflict, but inter-tribal warfare as well. For instance, the Pakistan Army has often made use of the rivalry between different armed militants of tribes in order to counter the targeted group. However, this aspect of Pakistan's counter-terrorism strategy backfires as it actually empowers the tribal identity and helps the targeted group in its recruitment drive.

The TTP attracts recruits by conferring social prestige and authority upon them, and extending political backing offering clout. The interaction is used to glorify war and martyrdom, while gradually giving the individual a sense of belonging to a peer group and ultimately convincing him to volunteer for *jihad*.

Finally, it also provides financial incentives to the recruits in both direct and indirect ways. It can be deduced from the above section that money plays a central role in retaining existing members and attracting new recruits. Finances are required not only for executing operations but also for sustaining the organisation itself. Thus, the following section outlines the TTP's sources of finance.

SOURCES OF FUNDING

The Tehrik-e-Taliban Pakistan finances its cadres and activities through organised crime such as extortion, smuggling, donations, ransom money from kidnappings, collection of road taxes and transit fees as well as by collecting *zakat* and *ushr* – forcibly or voluntarily.

The use of criminal activities to fill the coffers of the TTP gained currency in 2004. According to a Federal Investigation Agency official, when the military became involved in an armed confrontation with the militants in FATA, the militants started sending groups of men to the urban areas, not only to recruit people but also to raise money through robberies and other crimes.[12] In fact, this phenomenon was essentially a reaction to the events following the 9/11 attacks. After the war on terror was launched, the Pakistani state took a number of steps to dismantle the terrorist

12. Zahir Shah, "Hostage to Jihad," *The Herald* (Karachi), October 2008, p.80.

infrastructure. It involved a clampdown by the authorities on the financial infrastructure of the terrorist organisations. Accounts were frozen, transactions to suspected organisations, especially global and transnational ones, were monitored strictly, and the impunity was checked. All this created considerable financial problems for the terrorist organisations and they began exploring new sources of funding.

It is important to note, however, that criminal activities in the tribal areas had been going on prior to the emergence of the TTP. The illegal economic networks operating in the region have flourished due to the clandestine support, or apathy, of the state officials or the tribal elders. After its formation, the TTP took over the role of the earlier authorities of protecting and, at times, sponsoring illegal businesses.

Illegal activities provided the TTP with a regular source of income as crime provides cash on a rapid and repeatable basis. The diversity and availability of illegal activities means they can take place anywhere and avoid detection by the authorities.

Table 1 gives an overview of how organised crime not only fills the TTP's coffers but enhances the legitimacy of the group, establishes its authority and undermines the legitimacy of the state. When groups engage in extortion and the population does not report the activity to the authorities, the terrorists have achieved at least the passive support of the population. The fact that the TTP is able to extort large sums of money from the people could be an indication of the lack of confidence in the state's ability to resolve the matter. In other words, it shows that even if the terrorists do not have the support of the population, they have been successful in making the state appear to have no control. By engaging in these practices, the terrorists show that the state cannot control its own territory. Additionally, it allows them to maintain more control and become independent of other groups or state sponsorships.

Table 1: TTP and Organised Crime

Crime	Criminal Aim	TTP's Aim
Extortion	Obtain funds; sustain territory for prestige	Funds; undermining state's legitimacy; exerting power
Kidnapping	Obtain funds	Funds; leverage to free imprisoned leaders; making a political statement
Bank robbery	Obtain funds	Obtain funds; divert government security resources
Murder/targeted killing	Enforce criminal order; revenge; cash contract	Obtain funds; exert power; prevent collaboration with the government
Smuggling	Obtain funds	Exerting control over territory; funds

THE TTP NETWORK

When survival becomes paramount, terrorist groups find that collaboration with other groups increases potency and operational effectiveness. The TTP has formed a deep web of alliances with groups in Pakistan and Afghanistan. The point has been made by Michael C. Horowitz and Philip B.K Porter, in their article "Allying to Kill," which explains that alliances between terrorist groups occur frequently and are forged in order to increase lethality.[13]

AL QAEDA'S INFLUENCE ON TTP

Al Qaeda continues to operate in FATA by building a close relationship with the TTP's militant groups. There is evidence to suggest that Al Qaeda's organisational infrastructure is concentrated in Northern Waziristan and it has been training its militants in the

13. Michael C. Horowitz and Philip B.K Potter, "Allying to Kill," *Journal of Conflict Resolution,* vol.58, no.2, November 2011, p.10, at https://www.researchgate.net/publication/228192307_Allying_to_Kill. Accessed on March 20, 2017.

same camps as the TTP.[14] Al Qaeda's most important role in the tribal areas since 2007 has been to provide ideological support for groups such as the TTP that have decided to confront the Pakistani state militarily. Al Qaeda initially championed the argument that the Pakistan Army is essentially a foreign infidel force because of the Pakistan government's collaboration with US and NATO forces in Afghanistan. Accordingly, resisting the army's incursions into the FATA is portrayed as an obligatory "defensive *jihad*," an argument now echoed by TTP propaganda.

Additionally, the use of suicide bombers is attributable to the Al Qaeda's *modus operandi*. It was introduced by Al Qaeda as a new parameter for retribution that the terrorist groups could use to launch lethal attacks on the Pakistani people and government for maximum damage. The TTP included the Tafkiri Doctrine, which allows Muslims deemed apostate as acceptable targets, also akin to Al Qaeda. Strong ideological and operational ties between the two groups create a tough challenge for the Pakistani authorities.

TTP AND THE AFGHAN TALIBAN

After the downfall of the Taliban regime in Afghanistan post 9/11, many Afghan Taliban were given shelter in FATA by the tribes residing there. One of the factors explaining the hospitality afforded to the refugees is the Pashtunwali code. The Pashtunwali code is an unwritten code and traditional lifestyle which the indigenous Pashtun people follow. The Pashtunwali code – principles of hospitality and granting asylum to someone in need were put into use at the time of the militant influx in FATA following the fall of the Taliban and the US military operations in Afghanistan. The TTP and Afghan Taliban share deep ideological affinities and interpersonal relationships which were formed while fighting against the Soviets in Afghanistan. However, the TTP's anti-Pakistan objectives are in direct conflict with the Quetta Shura and the Haqqani group's efforts to accommodate the Pakistani government as they stage attacks inside Afghanistan. Thus, the Afghan Taliban has distanced itself from the TTP and does not

14. Brian Fishman, "The Battle for Pakistan: Militancy and Conflict Across the FATA and NWFP," *New America Foundation*, April 2010, p. 8, at https://brianhowesfishman.files.wordpress.com/2010/04/militancy-and-conflict-across-the-fata.pdf. Accessed on March 20, 2017.

support its goal of defensive *jihad* against the Pakistan government and army.

TTP AND THE PUNJABI TALIBAN

Hassan Abbas explains the Punjabi Taliban as a "loose conglomeration of members of banned militant organisations of Punjabi origin—sectarian as well as those focussed on the conflict in Kashmir—that have developed strong connections with the Tehrik-e-Taliban Pakistan."[15] The organisations that comprise the Punjabi Taliban are Sipah-e-Sahaba Pakistan, Lashkar-e-Jhangvi, Jaish-e-Muhammad as well as their parent organisations Harkat-ul-Jihad-ul-Islami, and Harkat-ul-Mujahideen. These groups which essentially focussed on the Kashmir agenda or on sectarianism, began sharing the TTP's anti-state stance in the light of Pakistan's collaboration with the United States led 'Global War on Terror' and the Red Mosque siege in 2007.

It is important to acknowledge that these links are not new since many personal relationships were formed during the 1980s when the leaders of these groups interacted with each other in Deobandi *madaris* or had the opportunity to wage *jihad* against the Soviets.[16] They have always played an important part in the Afghan *jihad* and have received their training in camps in Afghanistan. In order to make inroads into Punjab and attack the army as revenge for its operations in the FATA, the TTP and Al Qaeda strengthened their links to the Punjabi Taliban. They received logistical assistance from the Punjabi Taliban and were able to spread their tentacles within Punjab. The Punjabi Taliban also gain from allying with the TTP. Subsequently, pockets of these well trained militants began sprouting throughout KPK, particularly in Waziristan, Darra Adam Khel, Swat, Kurram, Mohmand, Bajaur, and Khyber. With the passage of time, they were absorbed into the organisations, with the TTP being a major recipient.[17]

15. Hassan Abbas, "CTC Sentinel: Defining the Punjabi Taliban Network," Council on Foreign Relations, April 2009, at http://www.cfr.org/pakistan/ctc-sentinel-defining-punjabi-taliban-network/p20409. Accessed on March 20, 2017.
16. Dr. Syed Manzar Abbas Zaidi, "The Punjabi Taliban," Centre for International and Strategic Analysis, No.12, 2014, p.6, at http://strategiskanalyse.no/Publikasjoner%202014/2014-02-20_SISA12_The%20Punjabi%20Taliban_MZ.pdf. Accessed on March 20, 2017.
17. Abbas, n.15.

The Punjabi Taliban functioning as a franchise of the TTP, have been involved in carrying out several deadly attacks within Punjab and even engaging in criminal activities to support their missions. They aim not to be a monolithic entity but several smaller and distinct groups in specific geographic areas have intensified their activities in Punjab. This is because the province has been marked out by the TTP as the next target of mobilisation, and in order to do this, it would require recruits who blend into the general population of Punjab.[18] The fact that the number of attacks have increased in Punjab around 2008 and onwards, also strongly indicates the possibility that Punjab has become a target due to the various military actions carried out by the Pakistan Army in the tribal areas.

TTP AND THE ISLAMIC STATE

With the Islamic State of Iraq and Syria (ISIS) losing its stronghold in Iraq and Syria and its fortunes dwindling, it appears to be recalibrating itself towards the Central Asian countries, Afghanistan, and, in particular, Pakistan. It has left some footprints in Pakistan, which is a step towards a dangerous precedent. As far is the ISIS' presence in Pakistan is concerned, Jessica Stern believes the ISIS "has designs on Pakistan, where it would presumably try to exploit the sectarian tensions".[19] This would allow the ISIS to gain currency in Pakistan without appearing on the Pakistani military's radar as a major threat; since sectarian violence is not included in the same category as terrorist violence. She also points out that small groups and individuals (in Pakistan) have been claiming they are killing in the name of the ISIS, which, in turn, appears to be happy to get credit for these attacks.[20]

The TTP is currently the gateway organisation for ISIS through collaborations and alliance formation. In November 2014, six commanders of the organisation announced their allegiance to the Daesh leader Abu Bakar Al-Baghdadi, including the spokesman of the organisation, Shahidullah Shahid, the TTP chief in Orakzai Agency, Saeed Khan, the TTP chief of Kurram Agency, Daulat Khan, the chief

18. Ibid.
19. Sher Ali Khan, Abid Hussain, Umer Farooq and Ghulam Dastageer, "Islamic Republic Versus Islamic State," *The Herald*, vol. 49, no. 3, March 2016, p. 70.
20. Ibid., p. 71.

of Khyber Agency, Fateh Gul Zaman, the TTP chief of Peshawar, Mufti Hassan and the TTP chief of Hangu, Khalid Mansoor.[21] Graffiti supporting Daesh and the flags of the organisation appeared in different cities of Pakistan.[22] Emissaries of Daesh had apparently been sent to Balochistan and had been in contact with Sunni militants from the LeJ, also an affiliate of TTP. Fringe elements of the TTP and other smaller cells, have begun executing attacks in order to attract the ISIS' attention. They were expecting either monetary support and/or an invitation to join the *jihad* in Syria and Iraq, in return, as revealed by security and intelligence officials. The inclusion of the ISIS factor in the current imbroglio and the TTP being its host in Pakistan will probably have a big impact on the terrorist milieu in Pakistan.

CONCLUSION

The alliances of convenience between different terrorist organisations are acting as force multipliers. They are no longer distinguishable on the basis of goals, region or capability. These groups understand the importance of survival, which is next to victory for them; they do so by forming alliances and combining objectives. The TTP's extensive linkages with the Punjabi Taliban, sectarian groups and other transnational groups allow it to expand its tentacles across the country. Thus, even though it may have become operationally weak, terrorism continues to spread in Pakistan, keeping the TTP relevant.

The pre-existing fault lines within Pakistan have provided a thrust to the growth of the TTP. First, Pakistan's use of *jihadi* groups as strategic tools in its foreign policy calculations vis-à-vis India and Pakistan. Such terror groups which serve the interest of Pakistan are yet to be viewed as hazards for Pakistan. The infrastructure of extremists cannot be dismantled if some of the violent groups are glorified simply because they are not anti-Pakistan. The militant groups in Pakistan may differ in background, tribal affiliation and goals but these factors are overridden by personal relationships and a shared history dating back to fighting

21. Kathy Gannon,"Islamic State Group Flourishes and Recruits in Pakistan," *Daily Herald*, November 13, 2016, at http://www.dailyherald.com/article/20161113/news/311139983. Accessed on March 20, 2017.
22. "IS Visits Militants in Balochistan: Jundullah Spokesman," *Dawn*, November 12, 2014, at, http://www.dawn.com/news/1143997. Accessed on February 23, 2017.

the Soviets in Afghanistan. The strong recruitment prowess of the TTP is a testament to this reality.

Second, the TTP's nexus with criminal gangs, as protectors and sometimes also as perpetrators of drug trafficking, gun-running, kidnapping for ransom and even extortion from businesses and households, has allowed it to easily fill its coffers and sustain itself. The fact that the state has not been able to stabilise the law and order situation in the country, points towards lack of political will. The Quetta Commission Report highlights the failures of the federal and provincial governments and the law enforcement apparatus in the proper implementation of the National Action Plan (NAP). Unclear leadership and management arrangements continue to hamper institutional effectiveness. The sense of insecurity that builds among the people, undercuts the legitimacy of the government, providing space for the TTP to grow.

Military force has been able to reduce the physical presence of the TTP from the tribal areas but it is far from defeating terrorism and the ideological drivers of extremism which continue to influence the minds of the people. The TTP has been successful in invoking feelings of anger and revenge against the US invasion of Afghanistan and the US bombing of Pakistan's tribal areas to gain legitimacy in the eyes of the locals and recruit foot soldiers. It enjoys ideological support from larger terrorist organisations such as Al Qaeda, the Afghan Taliban and the Haqqani network which also boosts its legitimacy and gains it tactical and strategic support from smaller groups due to its fluid decentralised nature. The use of force cannot fix these fault lines. Force can kill the terrorist but it does not kill the ideology that has permeated Pakistani society for over three decades. Soft counter-measures are equally important and the Pakistani government's weakness lies therein. This weakness is what groups like the TTP feed off and grow into the monstrosities that they have become.

DETERRENCE THROUGH SPACE: A CASE FOR AN INDIAN ASAT

ANAND RAO

The strategic situation in space is changing. China's Anti-Satellite(ASAT) missile test in 2013 and its previous ASAT test of 2007 have triggered the race for development of ASAT weapons by the world's space powers.[1] Space -based assets are vulnerable to attacks using both hard and soft kill options. The space programmes of some countries indicate research, development and testing of ASAT capabilities. In the current level of technological advancements, satellites orbiting the earth are unprotected, be it from deliberate attacks or collisions due to debris or orbiting objects. Whether or not weapons are actually deployed in space, the era in which satellites could operate without potential threats is over.

Satellites and their associated systems and infrastructure are, by their very nature, highly vulnerable to a wide variety of threats. These threats include permanent or irreversible damage to satellites through direct ascent kinetic energy weapons, Electro-Magnetic Pulse (EMP) weapons or high energy laser weapons. The threats could also include jamming of satellite links or blinding of sensors

Wg Cdr **T H Anand Rao** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

1. Harsh Vasani, "India's Anti-Satellite Weapons", *The Diplomat*, June 14, 2016, http://thediplomat.com/2016/06/indias-anti-satellite-weapons. Accessed on April 25, 2017.

and disrupting the data links. Aerial strikes could also be employed against ground relay stations, launch sites, communication nodes and satellite command and control systems to render space assets inoperative. Attacks on terrestrial installations and systems may be countered by having a redundancy in the support infrastructure and multiple data links. However, a direct attack on a satellite is difficult to counter with the present capability. Besides upsetting the routine lives of citizens, non-availability of a satellite may disrupt the flow of information into the battlefield and adversely affect the war-fighting capabilities.

India's reliance on satellites is for remote sensing, reconnaissance, communication, meteorology and navigation. Currently, there are about 93 operational Indian satellites in orbit.[2] The reliance on these satellites in everyday life and for military applications is unimaginable. Thus, space stability and space control comprise a fundamental national security interests. Potential enemies understand the high degree to which space-based systems enhance conventional war-fighting capabilities, and a growing number of nations are acquiring the ability to degrade or destroy these systems. India should take steps to mitigate the adverse effects of an enemy attack on its satellites.

The Indian Regional Navigation Satellite System (IRNSS) is one such system which amplifies India's future reliance on satellites. The IRNSS is being developed by India to offset the dependence on the American Global Positioning System (GPS) satellites, and is an example of India's future self-reliance in space. It consists of a constellation of seven satellites, all of which have been launched. It is designed to provide accurate positioning information service to users in India as well as the neighbouring regions. Besides its military significance, some other applications of the IRNSS are disaster management, vehicle tracking and fleet management, integration with mobile phones, precise timing, mapping and geodetic data capture, terrestrial navigation aid for hikers and travellers, and visual and voice navigation for drivers.[3] Besides the IRNSS, India relies on 33 communication satellites of the INSAT and GSAT series and 32 Earth Observation (EO) satellites like the CartoSat, OceanSat, RiSat

2. "Indian Spacecraft", http://www.isro.gov.in/spacecraft. Accessed on April 26, 2017.
3. Ibid.

and ResourceSat. There are also experimental satellites, scientific satellites and small satellites in orbit. An attack on our space assets could impact every element of national power: political, diplomatic, economic and military.

Currently, the Indian space programme is directed towards the pursuit of technologies to enhance capabilities for utilisation of space for socio-economic development and scientific study. From the military point of view, space-based assets are being utilised for navigation, communication and reconnaissance, not only by India but all over the world. However, India has no declared military space doctrine. The Indian Air Force Doctrine of 2012, briefly discusses the air and space paradigm of future wars. A 'Joint Doctrine of the Indian Armed Forces' was released by the chairman of the Chiefs of Staff Committee (COSC) on April 25, 2017. The new Joint Doctrine stresses on space, cyber space and special operations in war-fighting. "India needs to systematically prepare for the emerging triad of space, cyber space and special operations in support of military operations, even as it builds an integrated land-air-sea war-fighting machinery, maintains credible nuclear deterrence and guards against unconventional threats". This is the essence of the underlying theme of the Joint Doctrine.[4]

A Space Security Coordination Group (SSCG) was formed in 2010, with the then National Security Adviser, Mr. Shiv Shankar Menon, as the chairman. The SSCG involved representatives of the Defence, Research and Development Organisation (DRDO), Indian Air Force (IAF) and National Technical Research Organisation (NTRO). This organisation was designated to formulate the government's space policy and respond to all issues concerning space in the international fora, including the International Code of Conduct. The SSCG had given its approval for DRDO to develop ASAT capability.[5] In 2012, the then chief of DRDO, Dr VK Saraswat, stated that India had

4. Ranjit Pandit, "New Joint Doctrine Stresses Space, Cyber, Special Ops in War-Fighting", *The Times of India*, April 25, 2017, http://timesofindia.indiatimes.com/india/new-joint-doctrine-stresses-space-cyber-special-ops-in-war-fighting/articleshow/58365512.cms. Accessed on April 26, 2017.
5. Sandeep Unnithan, "India Takes on China: Anti-Satellite Capability can Target Space Satellites and act as Deterrent against India's Powerful Neighbours", *India Today*, April 28, 2012, , http://indiatoday.intoday.in/story/agni-v-launch-india-takes-on-china-drdo-vijay-saraswat/1/186367.html. Accessed on April 25, 2017.

all the building blocks in place to integrate an anti-satellite weapon to neutralise hostile satellites in low earth and polar orbits. Dr Saraswat indicated that India's Anti-Ballistic Missile (ABM) defence programme could be utilised as an ASAT weapon, along with its Agni series of missiles. This was later corroborated by DRDO, which said that the Indian Ballistic Missile Defence (BMD) programme can incorporate anti-satellite weapon development.[6] The building blocks being mentioned are the launch platforms which could be a ballistic missile of the Agni class or a rocket, Polar Satellite Launch Vehicle (PSLV) / Geostationary Satellite Launch Vehicle (GSLV), tracking radars, and the warhead.

After the successful trial of the Agni-V Intermediate Range Ballistic Missile (IRBM) on April 19, 2012, Dr Saraswat stated that DRDO will field a full-fledged ASAT weapon by the end of 2014, based on the Agni-V and AD-2 ballistic missile interceptor without resorting to actual testing. He emphasised on a defensive strategy for India in the space domain by saying, " India will not test this capability through the destruction of a satellite. Such a test risked showering lethal debris in space that could damage existing satellites. Instead, India's ASAT capability would be fine-tuned through simulated electronic tests".[7] He projected the view that space security entailed the creation of a variety of capabilities, without weaponising. These capabilities included the protection of satellites, communications and navigation systems, and denying the enemy access to its own "space systems".[8] India, apparently, possesses the technical expertise over all the components of ASAT capabilities without actually testing an ASAT weapon. However, merely possessing the technological ASAT capability without actually having tested it may not provide any deterrence value.

China is believed to have carried out eight ASAT tests so far.[9] The more prominent of these tests were conducted in 2007 and 2013. These tests are seen as a dissuasive message to the US to undermine its space dominance. The 2007 test was done on a KT-1 rocket that

6. Vasani, n. 1.
7. Unnithan, n. 5.
8. "ASAT Weapons Program with Chinese Characteristics" , November 23, 2015, http://councilforstrategicaffairs.blogspot.in/2015/11/asat-weapons-program-with-chinese_23.html. Accessed on April 27, 2017.
9. Ibid.

successfully destroyed a redundant Chinese Feng Yun 1-C weather satellite in Low Earth Orbit (LEO), 800 km above the earth's surface. This test reportedly left 2,500-3,000 pieces of space debris in LEO. A Russian satellite is believed to have been struck and destroyed by one such piece in May 2013. In 2013, China launched its ASAT missile, the Dong Neng-2 (DN-2), which is a ground launched, High Earth Orbit (HEO) attack missile. This was a test of the rocket component of a new direct ascent ASAT weapons system derived from a road-mobile ballistic missile.[10] China is developing these relatively simple and economical space launch vehicles based on its Inter-Continental Ballistic Missile (ICBM) technologies and Medium Range Ballistic Missiles (MRBMs), which can be launched from mobile launchers. China seems to have developed its anti-satellite capabilities to deter the United States but it may not hesitate in using these against Indian satellites when the need arises. The tests of 2007 and 2013 prove that India's remote-sensing satellites in LEO and the IRNSS in Medium Earth Orbit (MEO) are vulnerable to China's ASAT weapon systems. China is also known to have developed many ground-based jammers which could be used to deny access to some of our own satellites which are within the reach of China. With further development of these capabilities, China would be in a position to threaten Indian satellites in the event of any conflict. These developments in India's immediate neighbourhood are enough to suggest that India needs a rethink on the direction in which the Indian space programme is moving. The asymmetry in the conventional war-fighting potential between India and China could be offset by creating deterrence through building up offensive and defensive space capabilities.

An option would be to equip our satellites and ground-based systems with advanced electronic protection measures as a counter-measure against soft kill options. Defensive manoeuvres and orbital changes of satellites would also be a cost-effective option. However, these measures alone would not be fool-proof. Denying the aggressor the freedom to use his space-based assets would form a vital aspect of space security for any nation. This would act as a deterrent by providing a demonstrated capability to achieve hard kills on an

10. Vasani, n. 1.

enemy's space-based assets. India has already achieved the required progress in this direction to take the ASAT programme further.

ASAT weapons launched into space can be broadly divided into two categories: direct-ascent or co-orbital systems. Direct ascent systems use rockets or missiles to put a warhead or kill vehicle into a trajectory that collides with the target in orbit without the kill vehicle entering the orbit itself. Whereas, co-orbital systems use a Satellite Launch Vehicle (SLV) to place an interceptor into orbit, after which it manoeuvres to either collide with the target satellite or reaches near the target satellite to achieve a soft kill. Other ASAT capabilities consist of cyber-attacks on satellite systems, Electro-Magnetic Pulse (EMP) explosion devices and Directed Energy Weapons (DEWs). These capabilities have been developed to varying extents by the space superpowers. Some of the emerging technologies at the concept stage are pellet cloud attacks on low-orbit satellites, microsatellite technology and particle beam weapons. Amongst these wide ranging technologies, the cyber attacks, EMP attacks and laser attacks (DEWs) are impermanent in nature and their effects have not been tested. Moreover, to use such attacks from ground-based systems would require large power outputs demanding larger infrastructure which could be subject to targeting by ground-based missiles and strike aircraft. Co-orbital weapons are still in the design and development stages by the space superpowers. With the current progress made in the field of missile technology and ASAT capability in India, further development of direct ascent weapons or kinetic energy weapons to a stage which provides minimum deterrent capability would be an option worth considering. Three critical elements are required to destroy satellites: a long range radar for detection, a missile to carry the warhead and the warhead or 'kill vehicle' itself. All these elements have already been developed in the BMD programme. The Agni-V can reach altitudes of 600 km. This is sufficient to reach satellites in LEO, which are mainly the recce or EO satellites. DRDO's long range tracking radar can scan targets up to around 600 km. The kill vehicle or warhead has been developed as part of the BMD programme. Satellites have a predetermined path which can be continuously monitored and predicted unlike a ballistic missile and are, hence,

easier to target, provided the orbital height is within reach of the launch rocket.[11] With the present capabilities, India can endeavour to target satellites in LEO only.

While the development of ASAT capabilities by India seems a reality in the near future, it may be noteworthy that even the space superpowers have not attained assured destruction capability. There are around 4,256 satellites currently in orbit of which 1,419 are operational.[12] The ease of incapacitating or destroying an orbiting satellite is questionable due to the following factors.

Firstly, identifying an enemy satellite which is operational and has not been decommissioned is itself a demanding task. These decommissioned or dead satellites could act as decoys. Secondly, tests have only been carried out on decommissioned or dead satellites. An operational satellite being used for military purposes would be subject to defensive manoeuvres like inclination and orbital elevation changes. This would pose difficulties in tracking and determining the impact point. Thirdly, even if a satellite is successfully attacked, there exists redundancy through other satellites being used for a similar purpose. It is possible to resume services within an acceptable time gap. Fourthly, there is the cost factor. The Global Positioning System (GPS) and communication satellites in Geo-Stationary Orbit (GEO) are at altitudes of around 20,000 km and 36,000 km respectively. While satellites in LEO can be targeted by solid fuel rockets which are used in ICBMs, for satellites at higher altitudes, liquid fuelled rockets will be required, using GSLV technology. This is cost prohibitive. Multiple targeting by using single launch vehicles will offset the cost factor. As a corollary, selecting higher orbital altitudes (above LEO) for satellites, thereby keeping them beyond reach, would be a basic counter-measure in the present scenario.

Developing ASAT capability will have its pros and cons. The main factor against ASATs is the concern for space debris. However, developing and demonstrating the capability, even without using it, would provide a deterrence value for any country, and can be put to use during a conflict. Hence, it is vital to take a middle path

11. Vasani, n. 1.
12. Andy, "Satellites, Orbiting Earth", *Pixalytics*, August 24, 2016, at http://www.pixalytics.com/sats-orbiting-earth-2016/. Accessed on April 27, 2017.

approach wherein India can develop an ASAT and test it without polluting space with debris. This can be achieved by testing the ASAT at lower altitudes where the resulting debris would reenter the earth's atmosphere and burn up. Alternatively, the ASAT launch vehicle could be made to fly up to the target satellite without actually destroying it and the launch vehicle could be made to reenter the atmosphere and burn out.[13]

A possible apprehension would be the likelihood of sanctions being imposed. This could be a setback for the Indian defence industry which is banking on foreign investments and Transfer of Technology (ToT) for indigenisation. This could also put in jeopardy the India-US civil nuclear agreement signed in 2005 which allowed India to carry out nuclear commerce while not being a signatory of the Non-Proliferation Treaty (NPT). India would also lose credibility in the Inter-Agency Space Debris Coordination Committee (IADC), in which it is an active member. The current treaties like the Outer Space Treaty (OST) have put a ban only on placing of weapons of mass destruction in space. Any new treaty like the International Code of Conduct (which is in the pipeline) would restrict India from developing and testing ASATs, while giving a lead to countries which have already made significant progress in ASAT capability. This is reason enough for accelerating the ASAT programme to prevent being left out of the elite club.

The response that India would get from the international community would be different from the subdued response to China's ASAT test. However, India must prevail in declaring an ASAT test as a technology demonstrator, and not for mass production.

CONCLUSION

With the current global developments in space technology, reliance on space-based assets has increased manifold for various applications and socio-economic well-being. The utility of space as a medium of war has grown exponentially. Hence, space stability and space control are fundamental national security interests. Possessing the capability to make an enemy satellite dysfunctional has far-reaching ramifications and can be used as an instrument of aggression and deterrence. The

13. Vasani, n. 1.

deterrence value of the ASAT capability will be known only when it is tested, and publicly acknowledged. Merely possessing the capability to attack a satellite may not be considered as weaponisation of space. Such a measure would certainly upset the global balance of power and may trigger a race for supremacy in offensive space capabilities and development of counter-measures. However, this is inevitable even with India's tilt towards use of space for peaceful purposes. India possesses the basic infrastructure, expertise and technical prowess to take the ASAT programme further to a level where it can be employed. Prioritisation in development of limited offensive and defensive space capabilities will also result in reorienting the Indian space programme, which is presently for peaceful purposes. Development of counter-measures against enemy ASATs is also probably just as important as developing the ASAT capability itself. Research and Development (R&D) on discreet counter-measures and co-orbital systems needs to progress simultaneously so as to keep India away from the spotlight of space weaponisation.

Deterrence through any military means comes with its associated implications. Leaving aside the economic costs and reactions by the international community, India should see the benefits of a credible space deterrence. Possessing the capability would not be adequate for deterrence unless it is communicated through displayed intent. The deterrent capability should also be credible. Credibility depends on military capability and the political resolve to act. Conducting an ASAT test will not only ascertain India's capability, but also give credibility to its space deterrence.

INDIA'S FOREIGN POLICY: EXPLORING THE MARITIME OUTLOOK

STUTI BANERJEE

INTRODUCTION

Indian foreign policy is based on the principle of peaceful coexistence and non-interference in the internal matters of sovereign states. It is seldom static and is evolving to address the challenges in the ever changing world around it. The decade of the 1990s is seen as a watershed which not only ushered India into economic reforms but also brought about marked shifts in its foreign policy. India has had to seek new partners, allies and friends while reinforcing its old relations, in order to deal with the realpolitik of international politics. While negotiating numerous challenges since then, India's foreign policy has had to contend with rising aspirations that epithets like 'emerging power', 'rising power', 'great power' brought with them. Moreover, the existential realities of the region – its location in an insecure South Asian region, being surrounded on all sides by unstable democracies, conflict-ridden countries, militant activity, authoritarian leaders or weak governments –

Dr. **Stuti Banerjee** is a Research Fellow at the Indian Council of World Affairs, New Delhi.
Disclaimer: The views expressed are those of the author and do not reflect the views of the Council.

persuaded India to move forward to imbibe historic changes in its foreign policy.[1]

For India, the need is to focus on the challenges that are presenting themselves in its immediate and extended neighbourhood. "The promotion of a politically stable and economically secure periphery is a paramount foreign policy objective for India. This is essential to deal with the challenges of fostering sustainable growth and to ensure that regional differences cannot be exploited by those who would keep us absorbed in disputes."[2]

To foster this sustainable growth and to contribute substantially to the security architecture of the Indo-Pacific, India has to focus on its maritime borders. India is a peninsular state. It has 15,106.7 km of land borders and a coastline of 7,516.6 km (mainland). It has 1,197 islands with an area of more than 2,094 km of additional coastline.[3] It is a country with a rich maritime tradition spanning over 4,000 years. The word 'navigation' originates from the Sanskrit word '*navagati*', meaning sea travel.[4] The Indian seaboard had always witnessed peaceful maritime activity, with trade as the prime driver. The maritime domain was a link that allowed India to grow as an economically prosperous empire and it was also the route that was used by India's colonisers to reach its shores as traders. It is also the seas that have helped vastly in the exchange of culture and languages. Thus, the seas have always played an important role in India's relations with the rest of the world. India's maritime history, both ancient and recent, provides adequate justification for it to explore the maritime domain in enhancing Indian foreign policy.

1. Aparajita Gangopadhaya, "India's Foreign Policy in the Twenty-First Century: Continuity and Change, "http://www.pan-ol.lublin.pl/wydawnictwa/TPol7/Gangopadhyay.pdf. Accessed on April 26, 2017.
2. Ministry of External Affairs, Government of India, "Remarks by Foreign Secretary at the Launch of IDSA Report: 'India's Neighbourhood: Challenges in the Next Two Decades'," http://www.mea.gov.in/Speeches-Statements.htm?dtl/20120/remarks+by+foreign+secretary+at+the+launch+of+idsa+report++quotindias+neighbourhood+challenges+in+the+next+two+decadesquot. Accessed on September 6, 2016.
3. Figures have been taken from Department of Border Management, Ministry of Home Affairs, Government of India. http://www.mha.nic.in/hindi/sites/upload_files/mhahindi/files/pdf/BM_Intro_E_.pdf. Accessed on September 7, 2016.
4. The Indian Navy, "India's Maritime Doctrine," Ministry of Defence, New Delhi, 2009, p. 1.

EXPLORING THE MARITIME OUTLOOK

The last decade has witnessed India's dependence on its maritime environment expanding substantially as its economic, military and technological strength grows, its global interactions widen and its national security imperatives and political interests develop beyond the Indian Ocean Region (IOR). India wants to build a seamless and holistic approach towards maritime security, in order to provide 'freedom to use the seas' for its national interests and to ensure that the seas remain secure. The 21st century will be the 'Century of the Seas' for India and the seas will remain a key enabler in its global resurgence.[5] The Asian region has witnessed a remarkable growth in the past few decades. India is the biggest power in South Asia, and it is located in the centre of the South Asian subcontinent. India is adjacent to all the other South Asian countries, while all other countries don't share a common boundary with each other. Thus, India has great influence on the rest of the South Asian countries, except Pakistan. India's cooperation is the key factor in the changing security environment of the region.[6] India, in turn, needs the support of its neighbours to build this secure atmosphere.

Today, there is a national outlook towards the seas and the maritime domain, and a clearer recognition of maritime security as being a vital element of national progress and international engagement.[7] Apart from the 'traditional' threats to security emanating from the seas that surround it, India has to address the challenges posed by a number of non-security threats such as piracy on the high seas, smuggling and trafficking, humanitarian assistance and disaster relief, increased ship movements, and ecological degradation. To be able to address these challenges, India needs to build a comprehensive view, through engagement with the nations of the Indo-Pacific region.

The Indo-Pacific region is an emerging geostrategic and geo-economic concept that has been gaining significance in the field of economic and security studies. It is the geographical connotation of the area which covers the eastern coast of Africa, through the Indian

5. The Indian Navy, "Ensuring Secure Seas: Indian Maritime Security Strategy," Ministry of Defence, New Delhi, 2016, p. i.
6. Swaran Singh, "Strategic Scenario in the Indo-Pacific: Indian Perspective", in Gurpreet S. Khurana and Antara Ghosal Singh, eds., *India and China: Constructing a Peaceful Order in the Indo-Pacific* (New Delhi: National Maritime Foundation, 2016), pp. 15-16.
7. Ibid., pp. ii.

Ocean[8] and to the western Pacific coast. This in keeping with the focus that India wants to give to its policies for West Asia, Africa, South Pacific and East Asia. India aspires to be a net security provider in the region and its "central position in the Indian Ocean overlooking the Sea Lanes of Communication, its proximity to the choke points in the IOR, especially the Malacca Straits, Straits of Hormuz and Gulf of Aden accord it the above specified importance."[9]

To achieve the same, India has to build its Maritime Domain Awareness (MDA) while working on cooperative mechanisms with other maritime forces of the region through agreements such as the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP), Contact Group on Piracy off the Coast of Somalia (CGPCS), and the Shared Awareness and Deconfliction (SHADE) mechanism.[10] This would help in shaping a favourable and positive maritime environment, a fact which has been acknowledged in the new Maritime Security Strategy of the Indian Navy. The document states, "The term (MDA)... qualifies a traditional maritime need for situational awareness at sea, and is used in the modern sense as an all-encompassing concept. It involves being cognisant of the position and intentions of all actors, whether own, hostile or neutral, and in all dimensions – on, over and under the seas. MDA in the areas of maritime interest will be developed by the Indian Navy based on both integral efforts and inputs from other agencies."[11] Further, it states, "Maintenance of presence by our own and friendly maritime forces, both independently and under cooperative mechanisms, would help promote maritime stability."[12] The growth in international trade has ensured that security at sea is an important aspect not just of India's defence policy but also its foreign policy.

8. Saroj Bishoyi, "Geostrategic Imperative of the Indo-Pacific Region: Emerging Trends and Regional Responses," p. 55, http://www.idsa.in/system/files/jds/jds_10_1_2015_geostrategic-imperative-of-the-indo-pacific-region.pdf. Accessed on February 21, 2017.
9. Sarabjeet Singh Parmar, "Maritime Security in the Indian Ocean: An Indian Perspective," *Journal of Defence Studies,* vol.8, no.1, January-March 2014, p.55, http://www.idsa.in/system/files/8_1_2014_MaritimeSecurityintheIndianOcean.pdf. Accessed on February 21, 2017.
10. n.5, p.90.
11. Ibid., p.55.
12. Ibid., p. 81.

Nonetheless, India's maritime growth needs to be viewed in context of the reactions or possible responses from its neighbours and the extra-regional powers. The most important of those would be China. "The Chinese presence in the Indian Ocean, coupled with the land border issue is likely to dictate ... (a) a continental outlook that will remain the foremost point in India's security mainly due to the influence of history and geography. Therefore, the long standing Sino-Indian rivalry and the Chinese ingress into the Indian Ocean need to be examined."[13] China is building a powerful navy that would be able to protect its economic and security assets that are far from home. As the Chinese Navy grows, it will challenge the Indian Navy, especially in the IOR. While this would require defence preparedness, it would also need foreign policy acumen to avoid conflict and confrontation.[14]

In 1993, explosives from a neighbouring country arrived on India's west coast via a boat, and were used to trigger serial blasts that created mayhem in Bombay. Fifteen years later, in November 2008, terrorists landed by a fishing trawler in Mumbai to play havoc with the city once more.[15] The two attacks have brought into focus the need to strengthen coastal security networks for India. Pakistan has time and again stated that there are 'red lines' which, if crossed, could lead to a nuclear war between the two countries. One red line for Pakistan is the economic blockage of Pakistan's ports by the Indian Navy as was done during the 1972 War between the two nations. Dialogue processes with Pakistan, to resolve the issues of dispute, have been India's preferred method of resolving differences.

In the recent past, the government has decided to engage with other nations in West Asia and Central Asia. India and Iran have made progress on the plans for the development of Chabahar port in Iran which will provide India access to the markets of Central Asia and allow it to transport products faster. It will also provide sea access to Afghanistan, and facilitate trade ties among the three

13. Parmar, n. 9, p.57.
14. Stuti Banerjee, "India's Neighbourhood Policy: The Maritime Domain",http://www.thedialogue.co/indias-neighbourhood-policy-the-maritime-domain/. Accessed on April 26, 2017.
15. Arun Prakash, "The Rationale and Implications of India's Growing Maritime Power," in Michael Kugelman, ed., *India's Contemporary Security Challenges*, p.79, https://www.wilsoncenter.org/sites/default/files/ASIA_100423_IndiaSecurityFINAL.pdf. Accessed on April 26, 2017. ,

countries. India has decided to invest US $ 20 billion in it. During Prime Minister Narendra Modi's trip to Tokyo (November 2016), his Japanese counterpart, Shinzo Abe, agreed to help India with the Chabahar project. Both leaders directed their aides to hammer out a plan to fast-track the project. India wants Japanese investment and help in building the railway track between the port city and Zahedan. Both India and Japan see strategic convergence in Chabahar.[16] The International North South Transport Corridor (INSTC) is another such project to link India to Central Asia and Russia. The multi-mode network is of strategic interest to India. Apart from providing India an alternative trade route with Russia, Central Asia and Europe, its potential can be enhanced if India is able to link it with its connectivity projects with other South and Southeast Asian nations. Apart from the economic advantages, closer links with the region would also result in enhanced political and security relations.

The 'Look West Policy' to strengthen India's relations with a region that has a large Indian diaspora and an ability to provide future energy and nutritional security, is important. Similarly, the operationalisation of the 'Look East Policy' through the 'Act East Policy' means comprehensive engagement involving political institutions, security cooperation, economic links and social exchanges. The predominance of Indian culture in the form of religion, literature, architecture, and dance forms among countries such as Laos, Vietnam, Cambodia, Thailand, Sri Lanka, etc, is proof of the exchanges between the nations through ancient maritime routes. India launched Project Mausam in 2014, to renew the cultural links and contact among countries in the IOR, in a mutually supportive and cooperative manner.[17]

The attempt of the Indian foreign policy is to strengthen the Indian economy through its traditional maritime neighbourhood and trading partners. Implicit in this policy is the desire for free movement of people, goods, services and investments across the region. It also includes the security of the Sea Lanes of Communication (SLOCs), freedom of navigation, availability of port infrastructure and non-

16. Sanjay Kapoor, "Why India Must Move Fast on the Chabahar Port Project in Iran," https://scroll.in/article/826565/why-india-must-move-fast-on-the-chabahar-port-project-in-iran. Accessed on 26 April 2017.
17. n. 5, p.22.

discriminatory access to markets. In addition, New Delhi sees the preservation and promotion of the Indian footprint in East Asia, through shared culture, arts and religion, as part of its broader interests.[18]

As trade and commerce increase the need for better shipping facilities, including ships, trained crew, ports and port management, it would mean that India and the countries of the IOR have to collaborate with each other. This view has been encapsulated by the government in its Security and Growth for all Regions or SAGAR initiative. The initiative, as stated by Prime Minister Narendra Modi is to "pursue and promote geopolitical, strategic and economic interests on the seas, in particular the Indian Ocean..... (and build) a network of growing political and economic maritime partnerships, and strengthening of regional frameworks...."[19] To realise the same "India must establish both a climate of trust, and of economic intertwining between itself and its neighbours. This can be achieved by investing and assisting in the development of maritime infrastructure in the Indian Ocean Region, and specially in Bangladesh, Myanmar, Sri Lanka Maldives, Oman and Iran."[20]

In pursuit of its foreign policy objectives of a peaceful and interconnected neighbourhood for stable economic development, India, along with Myanmar, as part of the Kandla Multi-Modal Transit Transport Project, is developing the Sittwe port. The port facility is likely to enhance economic ties with other Southeast Asian countries while, at the same time, help India expand its security and political engagement in the region. India wants to expand its engagements with the various multilateral organisations of the region such as the Association of Southeast Asian Nations (ASEAN), East Asia Summit, South Asian Association for Regional Cooperation (SAARC), Asia-Pacific Economic Cooperation (APEC) and Shanghai Cooperation

18. Nitin Pai, "India and the Indo-Pacific Balance," p. 2, http://nsc.anu.edu.au/documents/ipmsc-papers/India%20and%20the%20Indo-Pacific%20balance%20-%20Nitin%20Pai.pdf. Accessed on February 21, 2017.
19. Prime Minister's Office, Government of India, "Text of PM's Address at International Fleet Review 2016," http://www.pmindia.gov.in/en/news_updates/text-of-pms-address-at-international-fleet-review-2016/?comment=disable. Accessed on September 7, 2016.
20. Vice Admiral Anil Chopra, "Sagarmala or SAGAR: A Maritime Dilemma," Gateway House, http://www.gatewayhouse.in/sagarmala-or-sagar-our-maritime-dilemma/. Accessed on September 7, 2016.

Organisation (SCO). This is in addition to continuous bilateral engagement with the countries to ensure stability and security in the region.

The United States remains the main security provider for most nations of the Indo-Pacific region, as also a major partner of the countries of West Asia. However, India's concern is that the United States does not fully appreciate, and share, India's apprehension with respect to China and its role in India's immediate periphery. India is aware of, and understands, the multifaceted relationship between the United States and China. For India, China is a neighbour with its own complex relationship across the land borders and the maritime domain. The need to stress on its East Asia policy is based on India's independent assessments about China's economic growth, military modernisation, and its assertive posturing in the South China Sea. India has been especially concerned with China's increasing interest and visibility in the IOR, especially amongst India's immediate neighbours.[21] India has to maintain a balance between China, which is increasingly seen as a 'development' provider for most nations, and the United States, that has been the main security provider for this region.

To achieve a better understanding of the maritime domain, India has established the Indian Ocean Naval Symposium (IONS). Its 26 members[22] represent the Indo-Pacific region and their common interests are: to maintain greater strategic interdependence, maintain freedom of movement through the SLOCs, provide safety of life at sea and protect the maritime environment. The Indian Ocean Rim Association (IORA) is another organisation that, while focussed on maritime security, trade, tourism, etc, has expanded its reach for better management and governance of the resources of the Indian Ocean.

The past few years have witnessed a reorientation in India's nautical outlook towards Africa. With increasing emphasis on developing maritime relationships with Mozambique, Kenya,

21. Singh, n. 6, p. 15.
22. Australia, Bangladesh, China (Observer), France, India, Indonesia, Iran, Japan (Observer), Madagascar (Observer), Malaysia (Observer), Maldives Mauritius, Mozambique, Myanmar, Oman, Pakistan, Saudi Arabia, Seychelles, Singapore, South Africa, Sri Lanka, Tanzania, Thailand, Timor Leste, United Arab Emirates, and United Kingdom.

Tanzania, Madagascar, Seychelles and Mauritius, India has reached out to the African states through offers of greater military aid, capacity-building and training assistance. With its economic engagement in the African continent growing rapidly, New Delhi has also sought to widen its sphere of influence in the western Indian Ocean. In a display of a more purposeful maritime diplomacy, Indian naval ships have increased their port visits to Africa's east coast and the smaller Indian Ocean island states.[23] Cooperation in this maritime domain has been limited to port calls by the Indian Navy and the conduct of anti-piracy operations. However, as incidents of piracy in the Gulf of Aden decline due to the sustained efforts, India has to look at other aspects of maritime cooperation. Securing coastlines from the threat of piracy, safeguarding ecological systems and hampering illegal fishing activities are some of the key 'Blue Economy' areas that can be the future spheres of cooperation. Greater collaboration in this area between India and the African littoral states would be beneficial for all, and can be tackled effectively only if all participate.[24] The fact that China has developed a military base in Djibouti, in the Horn of Africa is of strategic concern to India. India has to increase its outreach in the continent.

CONCLUSION

According to former Foreign Secretary Smt. Nirupama Rao, "India has a vision of the Indian Ocean Region unshackled from historical divisions and bound together in the collective pursuit of peace and prosperity. As a mature and responsible nation, one of our foreign policy interests is to evolve a regional architecture based on the twin principles of shared security and shared prosperity. India is well poised to play a substantive and formative role in this regard. ... Maritime security is emerging as an important element of our dialogue architecture with various countries, including with the United States.... In addition to bilateral interactions, (India is) actively

23. Abhijit Singh, "Evaluating India-Africa Maritime Relations," *The Diplomat*, http://thediplomat.com/2015/10/evaluating-india-africa-maritime-relations/. Accessed on April 21, 2017.
24. Elizabeth Sidiropoulos, "India-Africa Relations Under Modi: More Geo-economic?," *Brookings*, https://www.brookings.edu/opinions/india-africa-relations-under-modi-more-geo-economic/. Accessed on April 26, 2017.

engaged with almost all regional bodies that are either based in, or border, the Indian Ocean Region."[25] Prime Minister Modi recently highlighted, "We have seen a major shift towards our neighbours captured in our determined 'neighbourhood-first' approach. The people of South Asia are joined by blood, shared history, culture, and aspirations... India has a long history of being a maritime nation. In all directions, (India's) maritime interests are strategic and significant. The arc of influence of the Indian Ocean extends well beyond its littoral limits... (India) know(s) that convergence, cooperation, and collective action will advance economic activity and peace in our maritime region... (India) also believes, that the primary responsibility for peace, prosperity and security in the Indian Ocean rests with those who live in this region... And, (India) aim(s) to bring countries together on the basis of respect for international law."[26]

With the growing convergence between the military and civil establishments, the seas are poised to play an important role, in the growth of India as also in stability in the region. With the government viewing the India Ocean as an area of growing foreign policy importance, there is a need for maritime domain awareness and capacity building for the Indian maritime forces. Also, there is a need to invest in building a technologically advanced navy and coast guard. India needs to strengthen its relations with Maldives, Sri Lanka, etc. while it builds its relations with the Pacific island nations and continues to strengthen relations with ASEAN and other nations of the region.

To be able to lead in the Indian Ocean Region, India's military capability and diplomatic outreach have to match each other.

25. Ministry of External Affairs, "Address by FS on 'Maritime Dimensions of India's Foreign Policy'," http://www.mea.gov.in/Speeches-Statements.htm?dtl/53/Address+by+FS+on+Maritime+Dimensions+of+Indias+Foreign+Policy. Accessed on April 27, 2017.
26. Ministry of External Affairs, "Inaugural Address by Prime Minister at Second Raisina Dialogue, New Delhi, January 17, 2017," http://mea.gov.in/Speeches-Statements.htm?dtl/27948/Inaugural_Address_by_Prime_Minister_at_Second_Raisina_Dialogue_New_Delhi_January_17_2017. Accessed on April 27, 2016.

'MAKE IN INDIA' IN CIVIL AVIATION

RK NARANG

INTRODUCTION

> *The aviation sector in India is filled with opportunities. The lives of the middle class are being transformed and their aspirations are increasing. Given the right chance, they can do wonders.*
>
> Narendra Modi,
> Prime Minister of India,
> April 27, 2017.

The Airport Authority of India (AAI) [1]had published a document on the Regional Connectivity Scheme called "*Ude Desh Ka Aam Naagrik*" (UDAN) in October 2016. This scheme is aimed at enhancing regional connectivity through fiscal support and infrastructure development as stipulated in the National Civil Aviation Policy, which was issued in June 2016.[2] Indian Prime Minister Narendra Modi flagged off the

---

Gp Capt **RK Narang** is a Senior Fellow at the Centre for Air Power Studies, New Delhi.

1. The AAI is the agency of the Ministry of Civil Aviation, which is responsible for the creation and maintenance of the civil aviation infrastructure
2. "Regional Connectivity Scheme-UDAN", October 2016, http://www.aai.aero/public_notices/aaisite_test/Final-Regional-Connectivity-Scheme(RCS)311016.pdf. Accessed on April 26, 2017.

first flight of Alliance Air under the UDAN scheme from Shimla for Delhi on April 27, 2017.[3] India was the ninth largest civil aviation market in the world in 2016, and is likely to become the third largest and the largest aviation market by the 2020 and 2050 respectively.[4] Civil aviation is a significant sector with a huge economic potential which, if properly exploited, could become an engine of growth for the aviation sector. However, answers to the following questions need to be found before the concept, 'Make in India' is deliberated upon.

- Does India have a 'Make in India' programme in the civil aviation sector and are there programmes to develop commercial passenger aircraft for civil aviation users in India?
- Are there programmes to develop radars, navigation systems, airport and approach aids for the civil airports?
- Who formulates the standards and provides certification for innovative and indigenously designed civil aircraft and systems in India?
- Has India leveraged its large orders for the acquisition of commercial aircraft for achieving 'Make in India'?

The article deliberates upon India's endeavours towards 'Make in India' in the civil aviation sector and the need for initiatives to promote indigenous design and development in this sector.

MAKE IN INDIA

'Make in India' and indigenisation are two terms which are sometimes incorrectly interpreted as design and development in India. Indigenisation could involve the development of a product by local vendors and 'Make in India' would involve the local manufacture of products [designed and developed by foreign Original Equipment Manufacturers (OEMs)] with or without the transfer of technology. However, indigenously designed products

3. "How Narendra Modi Government's UDAN Scheme Can Change the Way You Travel", *Financial Express,* April 27, 2017, http://www.financialexpress.com/india-news/what-is-udan-scheme-inaugurated-by-pm-narendra-modi-everything-you-need-to-know/644338/. Accessed on April 28, 2017.
4. "Make in India Aviation", Make in India, http://www.makeinindia.com/article/-/v/make-in-india-aviation. Accessed on April 26, 2017.

are those which are designed by Indian entities. India is acquiring commercial aircraft and developing/ upgrading airports for boosting its regional air connectivity. The 'Make in India' (or indigenous design and development) initiative in the aviation sector has been predominantly focussed on military aviation and is yet to take off in civil aviation despite having enormous potential, with economic and technological benefits. Adequate attention has not been paid to research, design and development of commercial passenger aircraft and ground systems. A closer look at the civil aviation sector would reveal that there is enormous scope also for design and development of support infrastructure and equipment like radars, air navigation systems, airport and approach aids, air traffic systems, etc.

CIVIL AIRCRAFT DESIGN AND DEVELOPMENT

The National Aeronautics Laboratory (NAL),[5] a Public Sector Undertaking (PSU), had initiated the design and development of the 18-20-seat SARAS passenger aircraft in 1999; its first prototype flew in 2004.[6] The crash of its second prototype brought an abrupt end to this project in 2009. The project was revived in 2016.[7] NAL also initiated the development of the CNM-5 five-seat aircraft in collaboration with Mahindra Aerospace in 2016. It had earlier successfully developed the Hansa-3 propeller basic trainer for civil aviation. However, till recently there was no serious attempt to develop large passenger aircraft. A high powered committee for National Civil Aircraft Development (NCAD), set up by the Centre for Scientific and Industrial Research (CSIR) of the Ministry of Science and Technology (Ministry of S&T) had recommended the launching of a civilian aircraft project in May 2010.[8] Another PSU, Hindustan Aeronautics Limited (HAL)[9] issued

5. NAL is a public sector research and development organisation, which is under the Ministry of Science and Technology and has been involved in the design and development of manned and unmanned aircraft for civil and military users.
6. "Maiden Flight of Saras-India", http://www.icast.org.in/news/2004/jun04/jun15cnews.html. Accessed on March 11, 2017.
7. "NAL's Saras to Rise and Fly Again", October 5, 2016, *The Hindu,* http://www.thehindu.com/news/cities/bangalore/NAL%E2%80%99s-Saras-to-rise-and-fly-again/article15427066.ece. Accessed on March 11, 2017.
8. "Plan Panel to Allocate Rs 5,000 Crore to Develop the Civilian Plane", *The Hindu*, January 22, 2012, http://www.thehindu.com/news/national/plan-panel-to-allocate-rs-5000-crore-to-develop-civilian-plane/article2822788.ece. Accessed on September 9, 2016.
9. HAL is under the Ministry of Defence of India.

a Request for Information (RFI) in February 2016 for a joint venture for the manufacture and supply of a 50-80-seat aircraft to connect Tier-II and Tier-III cities in an endeavour to capitalise on the rising demand for aircraft for civil aviation.[10] However, the development of the SARAS and 50-80-seat commercial passenger aircraft is being undertaken by two different agencies, i.e. NAL and HAL, which are placed under the Ministry of S&T and the Ministry of Defence (MoD) respectively.

Ownership and Support: The projects for indigenous design and development of commercial, civil aircraft are initiated by NAL, which is mandated to design and build small and medium-sized civil aircraft in India.[11] However, there is no involvement of the public sector (Air India) and private sector users in the civil passenger aircraft development projects of NAL. The lack of ownership of the users in these projects indicates a lack of commitment to indigenous projects. The absence of assured orders and support from the users makes such projects economically unviable.

AIR TRAFFIC AND GROUND SYSTEMS

India is a huge and densely populated country with varied terrain and has a large network of airports. The Indian government is in the process of operationalising and upgrading airports in the smaller cities to provide air connectivity to regional passengers. Therefore, it needs a large number of air traffic management, navigation and other ground systems and a lot of foreign exchange is likely to be spent on acquiring these. But there has not been adequate emphasis on the design and development of these systems. Bharat Electronics Limited (BEL), a PSU, has been developing primary radars,[12] communication systems, etc. for the armed forces and weather radars for civilian use,

10. "Request For Information (RFI) for Selection of a Partner to Manufacture 50-80 Seater Regional Aircraft in India," http://www.hal-india.com/Common/Uploads/TenderDoc/7078_TenderPDF1_FinalRFIRTA.pdf. Accessed on March 11, 2017.
11. CSIR-NAL, "The Mission and Mandate," http://www.nal.res.in/pages/mandate.htm. Accessed on April 30, 2017.
12. The primary radar illuminates the target with a microwave signal, which is reflected back by the surface of the target to identify the range and bearing of the target. However, it cannot determine the identity of the target. This radar works on a standalone mode and does not require any assistance from the target.

but there is no known programme for developing secondary traffic surveillance radars[13], precision approach radars, and other radio aids for civil airports.[14]

CIVIL AIRCRAFT PROCUREMENT

India's civil aviation companies, in both the public and private sectors, are likely to buy/wet lease about 900 passenger aircraft. These include 155 Boeing 737 Max jet planes by Spice Jet in a $22 billion deal in 2017,[15] 250 aircraft by Air India, 100 aircraft by Vistara,[16] 75 aircraft by Jet Airways,[17] 250 Airbus aircraft by IndiGo (for $27 billion)[18] and 72 aircraft by GoAir.[19] In addition to this, the Indian Air Force (IAF), Central Armed Police Forces (CAPFs), some state governments, cargo operators, and other private entities operate passenger and cargo carrying transport aircraft.

Leveraging Procurements: Indian public and private sector commercial operators are buying a large number of passenger aircraft, which could be leveraged for acquiring civil aviation manufacturing, Maintenance, Repair and Overhaul (MRO) and other technologies. The local manufacture and establishment of

13. A secondary radar transmits a signal which is received by the transponder fitted in the airborne target. The transponder processes the information and replies with information on distance, azimuth as well as the identity of the airborne target. This radar requires the active participation of the airborne transponder.
14. "CivilianRadars",BEL,http://bel-india.com/Products.aspx?MId=14&LId=1&link=83. Accessed on April 27, 2017.
15. Saurabh Sinha, "SpiceJet to Buy up to 205 Boeing Aircraft Worth Rs 1.5 Lakh Crore", *The Times of India*, January 20, 2017, http://timesofindia.indiatimes.com/business/india-business/spicejet-to-buy-up-to-205-boeing-aircraft-worth-rs-1-5-lakh-crore/articleshow/56514144.cms. Accessed on March 25, 2017.
16. PR Sanjai, "Airline Companies Seen Ordering New Aircraft on Sturdy Passenger Traffic Growth: Capa", *Livemint*, June 3, 2016, http://www.livemint.com/Industry/XUpiGZTKnIsbCK6w8zDKAM/Airline-companies-seen-ordering-new-aircraft-on-sturdy-passe.html. Accessed on September 4, 2016.
17. Robert Wall, "Boeing Bags Order for 75 New 737s From India's Jet Airways", *Wall Street Journal*, November 9, 2015, http://www.wsj.com/articles/boeing-bags-order-for-75-new-737s-from-indias-jet-airways-1447054496. Accessed on September 4, 2016.
18. Anurag Kotoky, "IndiGo Confirms $27 Billion Order to Buy 250 Airbus Planes", *Bloomberg*, August 17, 2015, http://www.bloomberg.com/news/articles/2015-08-17/india-s-indigo-confirms-order-to-buy-250-airbus-a320-neo-planes-idfkj8wd. Accessed on September 4, 2016.
19. "Budget Carrier GoAir to Purchase 72 A320neo Aircraft from Airbus", *The Economic Times*, July 13, 2016, http://economictimes.indiatimes.com/industry/transportation/airlines-/-aviation/budget-carrier-goair-to-purchase-72-a320neo-aircraft-from-airbus/articleshow/53183199.cms. Accessed on September 4, 2016.

aircraft, assemblies and sub-assemblies, of MRO facilities, etc. will result in the strengthening of the local aviation industry, and create jobs in the long run.

Indian commercial airline operators comprise a mix of public and private sector entities, with different work cultures and economic models. The lower numbers of acquisitions by individual operators make it difficult to negotiate with the OEMs for local manufacture or shifting of MRO facilities, etc. to India. However, if some means are found to integrate the requirements for acquisition of common platforms by the public and private sector entities, India would be in a much stronger position to negotiate with the OEMs for local manufacture of aircraft and components, shifting of MRO to India, etc. The acquisition of technologies and local production could also result in a marginal increase in the acquisition costs, which will have economic implications for the commercial aviation operators and may not be acceptable to them. Therefore, there is a need to find ways to compensate them in the overall interest of the aviation industry and the people of India. Whether integrating acquisitions works or not, one aspect that is clear is that acquisition of aircraft by commercial aviation operators needs to be leveraged for local manufacture or 'Make in India'.

Technological Gains: India's civil aviation acquisition deals in the past did not result in local production of aircraft, assemblies, sub-assemblies of MRO services or acquisition of establishments for manufacturing machines and equipment. China, on the hand, leveraged the economic potential of its aviation market and succeeded in establishing the Airbus A-320 and A-330 assembly plants at Tianjin in 2008 and 2016 respectively and the Boeing assembly plant in Zhoushan in 2016-17.

Role of R&D Organisations: R&D organisations play an important role in strengthening the aviation manufacturing capability. Indian R&D organisations are normally not involved in the civil, commercial passenger aircraft deals. In contrast, China had sought machinery while procuring 40 MD-90 (160-seat) passenger aircraft from McDonnell Douglas for $1.5 billion. Before the deal, Chinese engineers had visited the MD-90 plant at Columbus, Ohio, in August 1993, and bought computer controlled machines(which were used for making parts for the B-1 bomber and C-17 transport aircraft)

for $5.4 million, which later proved useful for China in developing large bodied aircraft, including commercial passenger aircraft.[20]

FUTURE AIR TRAFFIC MANAGEMENT SYSTEMS

The US Federal Aviation Agency (FAA)[21] and European Aviation Safety Agency (EASA)[22] have been developing technologies to support the International Civil Aviation Organisation (ICAO)[23] in facilitating the integration of civil Unmanned Aerial Vehicles (UAVs) in the non-segregated air space. However, there is no known programme to develop technologies like ground-based collision avoidance, and traffic separation systems, etc. for future air traffic systems to facilitate the integration of civil UAVs in the non-segregated air space in India.

RESEARCH AND DEVELOPMENT (R&D)

R&D is an essential aspect of capability development. The civil aviation authorities of leading countries have R&D directorates or equivalent organisations to undertake R&D programmes.[24] The FAA of the USA has the Airport Technology Research and Development Branch[25], and the EASA also has a research division.[26]However, the key stakeholders in civil aviation in India, i.e. Ministry of Civil Aviation (MoCA) and its two subordinate establishments i.e. Airport Authority of India (AAI) and Directorate General of Civil Aviation (DGCA) have traditionally not been involved in such R&D activity. Also, R&D is not included in the functions of the MoCA.[27] The R&D

20. John Mintz, "Sale of Aircraft Machinery to China Shows Perils of Exporting Technology", *Washington Post*, June 7, 1998, http://www.washingtonpost.com/wp-srv/politics/special/campfin/stories/mcdonnell060798.htm. Accessed on April 28, 2017.
21. "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap, 2013", FAA, https://www.faa.gov/uas/media/uas_roadmap_2013.pdf. Accessed on April 28, 2017.
22. Cordón et. al, "RPAS Integration in Non-Segregated Airspace: The SESAR Approach", November 25-27, 2014, http://www.sesarinnovationdays.eu/sites/default/files/media/SIDs/SID%202014-19.pdf. Accessed on April 28, 2017.
23. "Unmanned Aircraft Systems (UAS)", ICAO, 2011, http://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf. Accessed on April 28, 2017.
24. https://www.faa.gov/nextgen/equipadsb/research/. Accessed on July 14, 2016.
25. "FAA Airport Technology Research and Development Branch", FAA, http://www.airporttech.tc.faa.gov/. Accessed on April 27, 2017.
26. http://www.eurocontrol.int/sesar-research. Accessed on April 27, 2017.
27. "Functions Alloted to the Civil Aviation Ministry", Ministry of Civil Aviation, June 23, 2014, http://civilaviation.gov.in/sites/default/files/6_0.pdf. Accessed on September 7, 2016.

Directorate of the Civil Aviation Department of the DGCA was renamed as the Aircraft Engineering Directorate on November 3, 2009.[28] R&D normally involves the development of new technologies within the country, whereas the Engineering Directorate of the DGCA looks into the certification of aircraft and licensing of operators/ pilots based on prevailing standards. Therefore, non-availability of an R&D organisation in the MoCA and absence of programmes for indigenous development of passenger aircraft and support equipment like airport aids, air traffic systems and other technologies related to the operations of airports in India indicate the absence of the 'Make in India' initiative in the civil aviation sector.

CIVIL AVIATION TESTING AND CERTIFICATION

DGCA is responsible for the testing and certification of civil aircraft and other systems in India. However, its involvement in certification is limited to certification of products that have already been certified by the leading civil aviation agencies of the world e.g. FAA and EASA. DGCA normally does not formulate standards and certify innovative and indigenously designed civil aviation products for which there is no equivalent product in the world. Also, it does not have the infrastructure to test indigenously designed and innovative civil aviation products. The non-availability of a mechanism for the formulation of qualitative requirements, testing and certification, adversely impacts innovations and indigenous design and development in the civil aviation sector. The Centre for Military Airworthiness and Certification (CEMILAC), a DRDO laboratory, has the infrastructure to test and certify military aviation products, which could be upgraded (if required) and utilised for testing and certification of civil aviation products. DGCA could collaborate with CEMILAC to formulate standards, carry out testing of indigenously designed and innovative products, and formulate processes for their certification, which are acceptable and recognised by the leading civil aviation agencies of the world i.e. FAA and EASA, etc. Similarly, some of the laboratories available in the other government departments and the private sector could be authorised to certify civil aviation

28. http://dgca.nic.in/dgca/publicnotice%20Rand D0-AED.pdf. Accessed on September 7, 2016.

products, if they have the necessary testing facilities and expertise. Establishment of a mechanism for assessment and certification of innovative civil aviation products will support the 'Make in India' initiative.

THE WAY AHEAD

The MoCA, Ministry of S&T, MoD, DGCA, HAL, DRDO, industry and academia could all play major roles in developing futuristic civil aviation technologies.[29] Indian R&D agencies are developing manned and unmanned aviation products primarily for the military. The rising demand for air transport services in the civil sector has made India a lucrative market for civil aviation products. The design and development of civil aviation products need to be given greater emphasis in India. The lack of ownership and support to indigenous programmes for the development of commercial passenger aircraft, and the fewer numbers required for the military, adversely impacts the economic viability of indigenous aviation development programmes.

The Technology Development Board of the Ministry of S&T supports technology initiatives in the civil aviation and air transportation sectors. BEL has developed coastal surveillance radars, C-Band and S-Band Polari metric doppler weather radars for civil operators and a wide variety of radars for the Indian armed forces. The expertise of NAL, BEL and other PSUs should be utilised for developing commercial passenger aircraft, radars, communication and other systems for civil airports.[30]

Similarly, there is a need to develop future air traffic surveillance and other systems for providing traffic separation and collision avoidance to the UAV traffic. Futuristic technologies like the Light Detection and Ranging (LIDAR), Automatic Dependent Surveillance-Broadcast (ADS-B), Mid-Air Collision Avoidance System (MIDCAS), airborne radar for collision avoidance, airborne internet protocols, peer-to-peer communication systems, etc. need to be evaluated and developed to facilitate the integration of civil UAVs in the non-

29. "Technology Development Board", http://tdb.gov.in/our-objective/#. Accessed on July 9, 2016.
30. "Civilian Radars", BEL, http://www.bel-india.com/Products.aspx?MId=14and LId=1and link=83. Accessed on September 7, 2016.

segregated air space. The integration of UAVs in the Indian air space also needs to be included in the MoCA's strategic plan.[31]

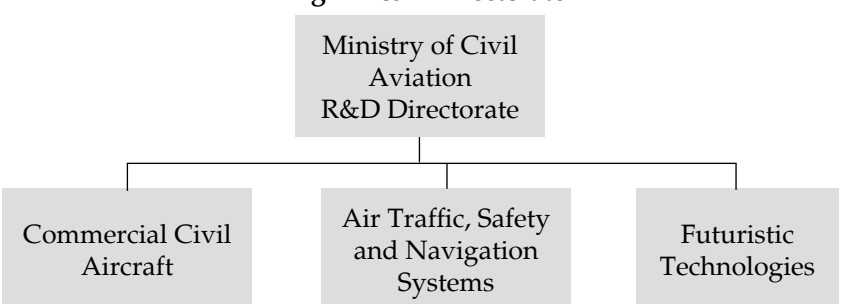
The large-scale procurement of products common to various commercial, civil aviation operators can bring enormous technological dividends if the civil aviation acquisition is leveraged. The civil passenger aircraft and air traffic equipment acquisition deals could be leveraged for setting up of manufacturing units, establishment of MRO facilities and production of assemblies and sub-assemblies of civil aviation aircraft and air traffic equipment in India, which, in turn, would strengthen its aviation industry and provide jobs. The participation of the academia and industry in research and development needs to be enhanced to support the endeavours of the PSUs in developing futuristic civil aviation technologies.

PROPOSED SYSTEM AND FRAMEWORK

There is a need to initiate 'Make in India' in civil aviation manufacturing and support indigenous design and development of air traffic systems, commercial passenger aircraft alongwith formation of standards and certification of indigenously designed manned and unmanned aircraft in India. The following are proposed:

- **R&D Directorate:** Establish an R&D Directorate in MoCA for design and development in three key sectors of civil aviation; firstly, commercial, civil aircraft; secondly, air traffic safety and navigation systems; and thirdly, futuristic technologies (Fig 1)

Fig 1: R&D Directorate



31. Strategic Plan, Ministry of Civil Aviation 2010-2015, http://www.civilaviation.gov.in/sites/default/files/mocaplan_0.pdf. Accessed on July 9, 2016.

- **Civil Aviation R&D and Procurement Council:** Set up a civil-aviation R&D and procurement council comprising NAL, DRDO laboratories, BEL, HAL, PSUs, IAF, academic institutes, private sector entities and engineers from the R&D Directorate of MoCA (Fig 2).

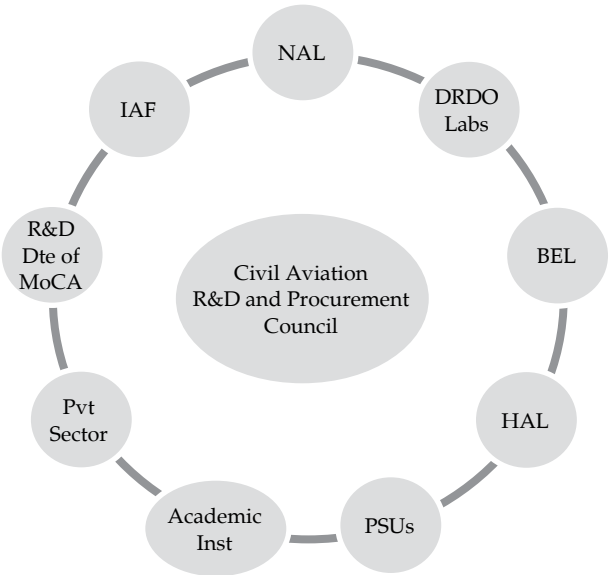
  Research and Development: To design and develop commercial passenger aircraft and support infrastructure like traffic monitoring, traffic separation systems, radars, airport aids, navigation systems, etc.

  The research and development of support infrastructure should start from the areas in which Indian industry has already made some progress e.g. BEL is making radars, communication systems, etc. for the military, which could be suitably customised and developed for civil aviation. As experience and expertise are gained, the scope of design and development should be gradually enhanced, and more products should be brought under the programme for indigenous development.

  A realistic roadmap should be formulated, which covers the entire cycle of the development, production and supply of indigenously designed products to Indian and global customers to make such projects economically viable.

  The participation of the private sector entities should be encouraged to take advantage of their innovations and production efficiencies.

Fig 2: Proposed Civil Aviation R&D and Procurement Council



Leveraging Procurements: The proposed council could leverage large orders of Air India, the IAF and other government entities for seeking transfer of technology, shifting of production lines and MRO services, manufacturing of assemblies and sub-assemblies in India and to get enabling machines and equipment from the OEMs. The council could also explore ways to leverage procurement by private sector civil aviation companies for 'Make in India'.

- **Balancing Technology Gains and Cost Escalations:** 'Make in India' or seeking the transfer of technology, or local production from OEMs could result in some cost escalation for the commercial, civil operators. The Indian government would need to come out with pragmatic solutions to balance out such escalations in the cost of acquisition e.g. by providing tax holidays or other benefits to offset the cost escalations of the concerned commercial airliners.
- **R&D Organisations in Procurement:** Involve DRDO, NAL and HAL in civil aviation procurement deals to negotiate with OEMs for identifying, acquiring, seeking local manufacture of aircraft, assemblies and sub-assemblies, machines, equipment, etc.

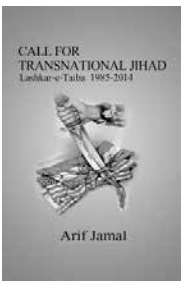
- **Certification of Civil Aviation Products:** Set up an agency within the MoCA to formulate qualitative requirements, testing and certification of innovative and indigenously designed civil aviation products (even if no equivalent products are available anywhere in the world). The proposed agency may coopt CEMILAC and the Directorate General of Aeronautical Quality Assurance (DGAQA) for technical support till the R&D and Certification Agency of the DGCA gains experience and expertise.
- **Ownership:** The three stakeholders of the civil aviation domain i.e. Air India, AAI and DGCA of the MoCA, need to take ownership of design and development of commercial passenger aircraft, air traffic management and civil aviation certification systems respectively.

CONCLUSION

The 'Make in India' initiative of the government has the potential for an energising indigenous civil aviation industry. It could provide impetus for indigenous design, development and manufacture in the civil aviation industry. MoCA would need to take ownership and get involved in R&D of commercial passenger aircraft, airport aids, and navigation systems to develop these technologies as well as future air traffic systems. Similarly, commercial passenger aircraft acquisitions have enormous potential for acquisition of enabling technologies and local manufacture of aircraft, systems and sub-systems from the OEMs. The concept of the off-the-shelf purchases and lifetime product support, etc. may be good for small commercial operators, however, it would not strengthen the aviation eco-system—in fact, such a system ensures continued dependence on the OEMs. The strengthening of the certification system in the MoCA would promote innovations and indigenous development in the civil aviation manufacturing. Civil aviation technology would have technological spinoffs for the military aviation, automobiles and other civil industries. The strengthening of the aircraft manufacturing industry would create jobs, reduce cash outflow from the country and reduce dependence on foreign OEMs.

BOOK REVIEW

CALL FOR TRANSNATIONAL JIHAD:
Lashkar-e-Taiba 1985 – 2014
Author: Arif Jamal
Publisher: Kautilya Books
2017
Rs. 1500



RADHIKA HALDER

Terrorism studies have really come into the limelight in the 21st century, owing to the widespread reach of terrorist organisations and the gruesome acts they have perpetrated in this century. While terrorism, as a phenomenon, was not new to the world, till the 1980s, however, it was seen in limited regions. What we see now is the globalised and transnational nature of terrorism and the shifting targets of terror organisations (to the most powerful nations of the world). Even as terrorism has been spreading across the world as a phenomenon, the roots of global terror can be traced back to Afghanistan and Pakistan. This was mostly after the major terrorist organisation, Al Qaeda, came to the forefront through its activities directed against the West, especially 9/11. This gory event not only shook the United States but made the entire world aware of the grave outreach of terrorism.

Ms **Radhika Haldar** is a Research Associate at the Centre for Air Power Studies, New Delhi.

Al Qaeda's cult leader Osama bin Laden stirred a viral ideological phenomenon which made counter-terror measures immensely difficult to arrive at. The origins of Al Qaeda were traced back to Afghanistan, particularly during the Soviet invasion in 1979, with evidence of funding from Pakistan's Inter-Services Intelligence (ISI) for the Mujahideen movement. Soon, the world started acknowledging Af-Pak as the hub of terrorism, and in 2009, the then Secretary of State Hillary Clinton stated in an interview that the goal of the United States "is to protect the United States, our allies, our friends around the world, from what is the epicentre of terrorism, namely, the Afghanistan-Pakistan border". Not very long after this, in 2011, Osama bin Laden was found to be hiding in Pakistan and was killed in an operation led by the US Navy SEALS, which shed further light on the extent to which Pakistan has supported various terrorist entities.

In the meantime, India faced several attacks as well. One of the prominent ones was the attack on the Indian Parliament in 2001, resulting in the killing of security personnel at Parliament House along with the terrorists. A series of attacks in crowded public areas and high security defence establishments, especially in Jammu and Kashmir, ensued in the years after this, until India faced one of the deadliest terror attacks on November 26, 2008. These attacks were mostly attributed to the terror organisation, Lashkar-e-Taiba (LeT), which has been nurtured by the Pakistani state to conduct covert operations in India. The LeT aims to achieve this by first "liberating Kashmir" followed by the destruction of India. The 26/11 attacks were a direct attack on the country's financial capital and areas that members of the international community reside in, or visit frequently. The LeT is also known to target countries such as the USA and Israel and strives to wage *jihad* against them as well.

Today, Al Qaeda and further, the Islamic State (IS) seem to have garnered most of the global attention. However, in such times, it is pertinent to study organisations such as the LeT that have survived and retained their prominence since 1985. The renowned Pakistani journalist Arif Jamal, in his book *Call for Transnational Jihad: Lashkar-e-Taiba 1985-2014*, has brilliantly managed to recall the entire historical background, origin, ideology, propaganda, tactics and operational

capability of the organisation through his immense research. Not only has he used primary resources for most of his work, he lays down the entire picture, along with the political landscape of the countries involved in the formation of the organisation, making the book a well rounded work on the organisation.

The LeT was the militant wing of the Markaz Dawat wal Irshad (MDI) organisation, which was formed in 1985 but whose historical roots began with the Meccan rebellion and various other events that took place in the year 1979. That is where the book starts from, going in deeply into the sequence and analysis of the events that took place and eventually shaped the formation of the MDI in 1985. While the MDI members were always split into two groups, only one managed to sustain itself and take over the organisation. This was the group of *jihadists* led by Hafiz Saeed and Zafar Iqbal, who not only took over the organisation but in due course of time, renamed it as Jamaat ud Dawa (JuD), and separated the LeT from the JuD, in order to let it function independently. This was done in a bid to help both MDI and LeT survive in the wake of President Bush asking the State Bank of Pakistan to freeze all the accounts of both organisations.

The book mentions how JuD functions more like an institution with several departments pertaining to sectors such as health, education, infrastructure, and relief work for those in need. The JuD is more commonly used as the public face of the LeT which helps it to raise money and garner support not only in Pakistan but in the diasporas across the world. Most of the funding of the LeT, in addition to the ISI, has been attributed to revenue from Saudi Arabia and the Gulf countries, and further, to organised crime. Moreover, almost any country in the world with an aggrieved Muslim population has always seen a degree of involvement of the LeT in its resistance movements. MDI Global, the global face of JuD, is perhaps the most far-reaching and widespread terrorist organisation ever known. In addition to this, it is also observed that a section of the MDI wanted to create a unified MDI Indian Ocean Command, securing all the regions around the Indian Ocean and establishing branches in each. The book contains an elaborate account of each of the countries where the MDI has set up cadres, and sent men for training.

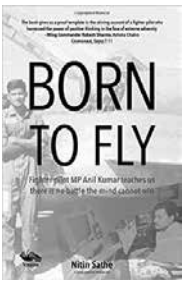
One of the fundamental differences between the LeT and most other terror outfits is the indoctrination and "conditioning of *jihad*", as the author puts it in one of the chapters. The LeT has a full-fledged course of training and programmes that recruits are required to undergo. These programmes are not related to military and physical training until the first mandatory course, *Daura-e-aama*, has been completed. The *Daure-e-aama* is a 21-day course which encourages the recruits to practise the Salafist way of performing rituals as well as imbibe the parts of the *Quran* dealing with *jihad*. This is done to prepare recruits mentally to kill and die in the name of Islam. Further, training in the use of light arms is also given in this programme. The idea is to psychologically condition the recruit towards the use of violence, and desensitise then towards the idea of *jihad*. After this, those who clear this programme and show the best capabilities to become *jihadis* go on to the next course which is the *Daure-e-khaasa*. This programme is aimed to prepare recruits for *jihad* in Indian Kashmir and tests them for obedience to superiors as well as adaptation to inhospitable environments. Heavier arms and ammunition are introduced, and training to facilitate smuggling of narcotics and various other goods is also given. This comprehensive manner of indoctrination at the mental level and training at the physical level are definitely some of the unique features of the LeT, making its ideology and propaganda almost unbeatable. The book contains a detailed study of this very aspect, highlighting the challenge it poses to counter-terror initiatives.

Moreover, the book has made some lesser known revelations regarding the connection between Pakistan's reputed spy agency, the ISI and the LeT, exposing the deep-seated issues and enmity that India faces from its immediate neighbour. Not only has the author managed to gather information from first-hand sources, but has further brought out the lethal nexus between state and non-state actors, with proper evidence and justification, risking his own position as a Pakistani journalist. The LeT definitely has an elaborate agenda for India, and also thorough plans and targets globally which have been highlighted in the book, making the LeT more threatening than Al Qaeda or even the IS, for that matter.

According to the author, the threat from the LeT is not likely to diminish the future—he feels that all the countries under the

radar of this well trained and equipped group, need to undertake effective military and intelligence measures to tackle it. The book contains a large amount of facts and figures and is a detailed study of the organisation's various activities and strategic moves, which is a boon for scholars of terrorism. The author not only uses personal experiences and first-hand narratives but evidently understands the complexities of the militant landscape in Pakistan which only adds to the book. Additionally, a lot of misconceptions regarding *jihad* as a concept and confusion among the various religious and political schools within Islamist organisations are to an extent, put to rest, in the book. At times, the book contains an influx of information too hard to process in one go, making it highly informative and data heavy, but leaving the reader greedy for more analysis. However, that does not diminish the fact that the book is the closest source of information on the LeT and JuD in today's world. All in all, the most commendable part of the book is the author's commitment against Islamist terrorism and his dedication towards personally conducting research in that direction for over two decades. The book is an excellent reflection of the same.

Born to Fly : Fighter Pilot MP Anil Kumar Teaches Us There is No Battle Mind Cannot Win
Author: Nitin Sathe
Publications: Vitasta
2016
Rs 495



NARENDER YADAV

"Touch the Sky with Glory", the motto of the Indian Air Force, is derived from the eleventh chapter of the Gita. It is also reflected in the inspiring biography of an air warrior who became a quadriplegic after an accident in the fledgling stage of his career as a fighter pilot. Despite the handicap, he did not lose hope and turned into a writer, making his life purposeful. The author of the biography, Air Commodore Nitin Sathe, calls him the Indian Stephen Hawking.

In this biography the author chronicles the life and times of Flying Officer MP Anil Kumar, beginning with a village in Kerala, going into the Sainik School, Kazhakootam, and then to the National Defence Academy (NDA) and Air Force Academy (AFA). After passing out, he was posted to two air bases to fly the MiG-21. Unfortunately, in a tragic accident, he suffered a grave spinal injury that left him in a quadriplegic condition for life. After one and half years in bed, he gradually developed the habit of reading, overcoming numerous physical problems. To begin with, someone would read out the newspaper and other material to him, but later, a stand was arranged

Dr Narender Yadav is a PhD in Military History. He is a Deputy Director in the Ministry of Defence, History Division.

to suit his needs. He could now turn the pages himself with the help of a small stick held in his mouth.

Extensive reading encouraged his urge to write. Someone at the Paraplegic Home, Pune, where he had been shifted from the Military Hospital, suggested that he use his mouth for writing. At first, MP thought it would be impossible, but persuasion worked. A small board placed on a stand at the correct height, assisted him. He could now hold a pen in his mouth to write on the paper clipped on the board. Though the task was challenging, MP found it enjoyable and satisfying. Gradually, he started writing articles on various themes. A computer and the internet proved to be a blessing. His intellectual exploration now knew no bounds. His articles were published in leading newspapers and magazines. One of his articles titled "Airborne to Chairborne" greatly impressed the editor of a famous national newspaper. Soon, this article found a place in school text books in Maharashtra and Kerala.

MP had become a hero to many by now. Hordes of visitors, including students, teachers, readers and friends began to visit him to draw inspiration. E-mails and letters arrived daily, appreciating his articles. He generally replied to all the e-mails and letters, and advised his readers about their problems. Despite the limitations imposed by his physical disability, he made life intellectually stimulating and satisfying. True to the motto of the Indian Air Force, Anil touched the sky with glory. In May 2014, he passed away at the age of 50, leaving behind an indelible mark on many hearts and minds.

The book is organised in 24 chapters. It starts with a preface and a brief touching note on "Last Landing". Then there is a flashback of the time when Flying Officer MP Anil Kumar met with an accident while returning on his motorcycle after night flying, and was shifted to the Military Hospital. The next chapter details his family background and his childhood at his village Chirayinkeezhu in Kerala. Subsequent chapters delve into his life at the Sainik School Kazhakootam, NDA, AFA, and the advance training at the Fighter Training Wing, Hakimpet, and passing out as the best cadet in aerobatics. The next two chapters describe his experience of flying the MiG-21 aircraft at two air bases. Another five chapters describe his life at the Military Hospital and Paraplegic Home where he made his life purposeful, despite numerous physical limitations. The last

chapter includes the reminiscences of his friends and followers. Some beautiful photos and mouth written letters at the end add to the value of the book.

This biography of Flying Officer MP Anil Kumar also enlightens us on life at prestigious institutions like the Sainik Schools, NDA and AFA. The author details the objectives and a brief history of these institutions as well as the nuances of training there. The chapter on the Sainik School describes the factors which prompt one to join a particular Service. In MP's case, it was an old Harvard aircraft displayed in front of the academic block at his Sainik School which inspired him to defy gravity by joining the flying branch of the air force. The tough routine at NDA makes cadets learn "when the going gets tough, the tough get going". Further, the training here fostered camaraderie amongst the cadets and helped them adapt to any environment in life. AFA develops an 'air sense' in the cadets. Indeed, it was the training at these institutions which made MP strong enough to bear the agony and extract the best out of the worst situation. There are many such issues which have brilliantly been woven by the author in the biography.

The narrative is lucid and attractive and completely engages the reader. The author first introduces the reader to the system, makes him understand the concept, genesis and a brief history. The humour injected at various intervals makes the book interesting. A page for contents and illustrations at the start of the book could have been convenient for the readers. But this in no way affects the rich material contained in the book. It is a true tribute to MP Anil Kumar by his NDA batchmate, Air Cmde Nitin Sathe, and teaches the lesson that given the chance and the environment, even a bedridden and wheelchair-borne person can become an inspirational being. Surely, the book will inspire many to lead a more purposeful life.

NOTES FOR CONTRIBUTORS

Articles submitted to *Defence and Diplomacy* should be original contributions and should not be under consideration for any other publication at the same time. If another version of the article is under consideration by another publication, or has been, or will be published elsewhere, authors should clearly indicate this at the time of submission.

Each typescript should be submitted in duplicate. Articles should be typewritten on A4/ Letter paper, on one side only, **double-spaced (including the notes)** and with ample margins. All pages (including those containing only diagrams and tables) should be numbered consecutively.

There is no standard length for articles, but 3,000 to 3,500 words (including notes and references) is a useful target. The article should begin with an indented summary of around 100 words, which should describe the main arguments and conclusions of the article.

Details of the author's institutional affiliations, full address and other contact information should be included on a separate cover sheet. Any acknowledgements should be included on the cover sheet as should a note of the exact length of the article.

All diagrams, charts and graphs should be referred to as figure and consecutively numbered. Tables should be kept to a minimum and contain only essential data. Each figure and table must be given an Arabic numeral, followed by a heading, and be referred to in the text.

Articles should be submitted on high-density 3~ inch virus free disks (IBM PC) in rich text format (RTF) together with **an exactly matching double-spaced hard copy** to facilitate typesetting; notes should be placed at the end of each page. Any diagrams or maps should be copied to a separate disk separately in uncompressed TIF or JPG formats in individual files. These should be prepared in black and white. Tints should be avoided, use open patterns instead. If maps and diagrams cannot be prepared electronically, they should be presented on good quality white paper.

Each disk should be labelled with the journal's name, article title, author's name and software used. It is the author's responsibility to ensure that where copyright materials are included within an article, the permission of the copyright holder has been obtained. Confirmation of this should be included on a separate sheet included with the disk.

Copyright in articles published in ***Defence and Diplomacy*** rests with the publisher.

STYLE

Authors are responsible for ensuring that their manuscripts conform to the journal style. The Editors will not undertake retyping of manuscripts before publication. A guide to style and presentation is obtainable from the publisher.

The style should be followed closely. Dates in the form January 1, 2000. Use figures for 11 and above. British spellings are to be used. Authors should provide brief biographical details to include institutional affiliation and recent publications for inclusion in About the Contributors. Sub-headings and sub-sub-headings should be unambiguously marked on the copy.

NOTES

Notes should be **double spaced** and numbered consecutively through the article. **The first line of a note must align with subsequent lines. Each note number should be standard size and have a full point**.

a) References to books should give author's name: title of the book (italics); and the place, publisher and date of publication in brackets.
   e.g. 1. Samuel P. Huntington, *The Common Defense* (NY: Columbia UP, 1961), Ch. 2, pp. 14-18.

b) References to articles in periodicals should give the author's initials and surname, the title of the article in quotation marks, title of the periodical (italics), the number of the volume/issue in Arabic numerals, the date of publication, and the page numbers:
   e.g., Douglas M. Fox, "Congress and the US Military Service Budgets in the Post War Period," *Midwest Journal of Political Science*, vol. 16, no. 2, May 1971, pp. 382-393.