CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

Internal Security Challenges to India in 2020 and Beyond

Brig Narender Kumar, SM, VSM (Retd) is a former Senior Fellow at the Centre for Land Warfare Studies (CLAWS) and presently a Distinguished Fellow at USI, New Delhi.

Abstract

The biggest challenge to a nation state is the "the protection of physical, political and cultural identity of citizens". The internal security threat to the state today is from state and non-state actors and in physical and cognitive domain as well. However, the paradigm of internal security have now grown to include the threat from cyber, political warfare, transnational terror organisations, water scarcity, societal dissension and black swan events such as coronavirus and technology. The focus of internal security is and should be the society. Issues of individual liberty and societal security often appear at odds with each other. However, the key to dealing with internal security is to keep the focus on both the people and the society.[1]

Introduction

It is undeniable that the states are no longer a safe sanctuary. India is a target, starting from terrorists seeking to attack citizens, to malicious cyber activity against citizens, institutions of governance, critical infrastructure or political and moral subversion through psychological and political warfare. Digital connectivity

Key Points

- In the current milieu, the threat to states is more from asymmetric and political warfare rather than from conventional military capabilities.

- Cross-border terrorism in Jammu and Kashmir, insurgency in the north-eastern states and left-wing extremism in certain states, continues to remain national security challenges.

- Radicalisation and transnational terrorism are a major challenge to India's internal security.

- Internal faultlines is a peril of corridor for cyber and political warfare.

- The employment of technology and the whole of government approach, is imperative to deal with the threats to internal security.

Internal Security Challenges ...

is being misused to cause communal, religious and social disharmony, to trigger internal instability. Political and cyber warfare are emerging as potent tools to disrupt economic activities and public life, destruction of public and private properties, attacks against critical defence infrastructure and disruption in services. The threat from public disorder and the disaffection of the people with the state, is more volatile than the threat from the terror organisations. According to the PHD Chamber, north Indian states incurred a loss of Rs 34,000 crore in the economy due to Jat agitation.[2] The loss to the public property and private citizens is in addition to these quoted figures.

The radicalisation in combination with international and transnational terrorism cannot be discounted and is becoming even more pronounced because it is now dishevelled with the secessionist and separatists organisations within the country. Radicals are slipping through benign organisations that have a different face to show to the world but act differently behind closed doors. Such organisations become more dangerous when they develop linkages with political parties in the guise of vote bank. The Islamic Research Foundation (IRF) of Zakir Naik and the Popular Front of India (PFI) are emerging as potential radical organisations that have the potential to trigger instability.

Understanding the Emerging Concept of Internal Security

The concept of internal security is set to change with the changing character of warfare. Till the recent past, national security was restricted to defending borders and preventing the loss of territory, but the paradigm of national security has now assumed, significance due to internal security challenges. The concept of national security as endorsed by Hans Morgenthau's description is the "protection of physical, political and cultural identity of a nation-state".[3] Internal and external securities are overlapping and two cannot be separated. Today, securing economic infrastructure, food supply chain, the protection of the environment, mitigating disasters, the prevention of erosion of the cognitive domain (that could be manipulated by inimical forces and radical organisations) and the security of citizens, assume even greater focus. Security of data and the

misuse of technology is an emerging threat to citizens and institutions of governance. The cyber, information, psychological and political warfare is emerging as a serious threat to internal security. These threats are amorphous in nature and require technology, the whole of government approach and legal frameworks to deal with these security challenges that can create internal fissures in society and states. Thus, the concept of security in the twenty-first century must be broad and dynamic to cover all the areas which concern the security of the state and its citizens.[4] As a developing nation, there are a number of factors that may expose India to a variety of security challenges. Ideally, national security should be viewed as a multidimensional process whose purpose is to safeguard national values. The most fundamental values of any nation are its survival, self-preservation, and self-perpetuation.[5] One of the greatest values of India under threat is 'unity in diversity'. For a developing regional power, the concept of internal security should be to create conditions of peace, stability, harmony and progress.[6]

Internal Security Challenges to India in Emerging Milieu

In the current milieu, the threat to states is more from asymmetric and political warfare rather than from conventional military capabilities. Political instability erodes the economic competitiveness of a nation. Some of the downsides of political instability includes policy paralysis, risk averseness and the collapse of the executive that can lead to slower growth and will directly impact internal and external security. The conventional domestic threats to national security have been categorised by the Ministry of Home Affairs (MHA) in four groups: terrorism in the hinterland of the country, cross-border terrorism in Jammu & Kashmir, militancy in the north-eastern states and left-wing extremism in certain states.[7]

Political Warfare

Political warfare is emerging as a single biggest factor for the collapse of institutions of governance, communal disharmony, the rise of secessionist and separatist movements, radicalisation and societal division across the globe. The political warfare thrives on internal

instability and ethnic, communal and societal fault-lines. In the broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives.[8] In a more precise manner, "political warfare refers to the employment of military, intelligence, diplomatic, financial, and other means—short of conventional war—to achieve national objectives".[9] India will have to guard against such threats that remain disguised and embedded as socio-political and socio-economic fault-lines. In the age of proactive media, the 'innocent-looking' political movement can activate uncontrolled chaos. West Asia and North Africa will not be the same again due to political warfare that pulled down many regimes and stable countries. The Inter-Services Intelligence (ISI) of Pakistan is working overtime to create political dissent by spreading the "India against minority community" rumour. Political parties, students and social organisations should be careful not to fall into the trap of adversarial propaganda and the creation of anti-India narrative because it has the potential to 'spiral' out of control. Political warfare is a vanguard to trigger hybrid and other asymmetric wars. With multiple secessionist and separatist movements going on in many parts of India, political warfare is a real challenge to the internal security of India and the lethal consequences of this warfare should not be ignored.

Kashmir: A National Security Challenge

Jammu & Kashmir continues to be a national security challenge even post abrogation of Article 370. J&K remains a potential platform for adversarial government actors, Jihadists, radicals, politically disaffected sections of the population, criminals, drug traffickers and sponsored irregulars to operate in conjunction with each other. The fusion of multiple actors in one battle space gives options to trigger a lethal hybrid war. The manifestation of hybrid war that is unfolding in J&K is cross-border terrorism, the battle of perception, cyberwar, political war, diplomatic rhetoric and violent extremism. Post abrogation of Article 370 the government should push the development agenda with adequate urgency. If it fails, the state could plunge into irretrievable chaos. Similarly, the formulation of criteria for jobs and the purchase of land requires urgency so that the subjects of the state are not deprived of jobs,

and colonisation by outsiders does not take place. Though investment plans by 43 companies worth Rs 13,700 crore has been announced, it is yet to unfold on the ground.[10] Detention of over-ground workers, separatists, political activists, led to the snapping of the network between over-ground workers, terror groups and source of funding. Pakistan is endeavouring to re-establish the network to give impetus to proxy war if India does not consolidate the advantages accrued out of these defining steps.

Unresolved Secessionist Movements in the North-East

Secessionist movements in north-east India are still simmering. Naga peace accord is still unresolved, a section of the United Liberation Front of Assam (ULFA) under Paresh Barua is operating from outside the country and the National Socialist Council of Nagaland (NSCN) Khango (K) faction continues to operate from Myanmar. Meitei insurgent groups are not even in talks with the state or the centre government. Many small insurgent groups are still waging an insurgency in parts of Assam and Meghalaya. According to rough government estimates, 4,000-5,000 armed cadres belong to all Naga insurgent groups—NSCN (IM), NSCN (KN), NSCN-K group, and NSCN (R).[11] The predicament is how to rehabilitate these unskilled and many of them illiterate cadres? There are reports that Absalom Rockwang Tangkhul, NSCN (IM) Commander has also crossed over across Tirap (in Arunachal Pradesh) to Myanmar along with 100-140 cadres.[12] Shimrang had said that even if a settlement was not reached at that time, the movement would not wear out. "Even if only 30 to 100 people are left, we will start again."[13] These insurgent groups could now become hedging tools in the hands of Chinese intelligence agencies to cause instability in the north-east. Under the covert support of Chinese intelligence agencies, north-east is seeing the emergence of the United Liberation Front of Western South East Asia (UNLFW) comprising nine prominent terrorist organisations, active in India's peripheral north-east region.[14] These nine groups are the National Socialist Council of Nagaland [Khaplang] (NSCN[K]), the United Liberation Front of Assam-Independent (ULFA-I), the Kangleipak Communist Party (KCP), Kanglei Yawol Kunna Lup (KYKL), the People's Revolutionary Party

of Kangleipak (PRPK), the People's Liberation Army (PLA), Manipuri Naga Revolutionary Front (MNRF), the United National Liberation Front (UNLF) and the National Democratic Front of Bodoland (Songbijit) (NDFB[S]). Veteran journalist-writer Bertil Lintner had said, China's role in north-eastern India is not to create instability but "to maintain instability" because it wants to keep India out of Myanmar.[15] Ethnic and communal faultlines are likely to be exploited by China in the north-east. Bodo Peace Accord 2020 has been signed between the Centre, Government of Assam and All Bodo Students' Union and the United Bodo People's Organisation. It is a welcome step and more than 2,000 Bodo insurgents are expected to lay down their arms. The success of the accord lies in the implementation of the accord by the Centre and the State Government. At the same time, upper Assam was rocked by multiple low-intensity blasts within a span of 15 minutes on 71st Republic Day, this indicates that ULAF (I) is gaining momentum post the Citizenship Amendment Act (CAA). There are reports of youth going missing and intelligence agencies suspects that these youths are joining ULFA (I). The people of Assam somehow are not happy with this development and there is a danger of a revival of ULFA in the state.

Transnational Terrorism Threatening Cultural and Physical Frontiers

Islamic State (IS) and Al Qaeda (AQ) are competing to spread their influence in India's neighbourhood including Sri Lanka, Maldives, Bangladesh and even Myanmar. The next 5 years are going to be crucial, whether India will be able to act as a great wall or transnational terror organisations will be able to penetrate the cultural and physical frontiers, needs to be seen. Threat from 'returning' Islamic State of Iraq and Syria (ISIS) cadres is real. Even if they are not Indians their presence in the neighbourhood is equally volatile and if the cadres are allowed to return even to Bangladesh, Sri Lanka and Pakistan, it will have a serious impact on India. In April 2019, Sri Lankan terror strikes that killed more than 300 people on Easter, is a reminder that ISIS has made landfall in South Asia and there is a need to put measures in place to prevent penetration of ISIS in the Indian states. Asim Umar, earlier named as Sana-ul-Haq, was possibly the highest-ranked terrorist

with Indian roots. He was the Chief of Al-Qaeda in the Indian Subcontinent (AQIS), a terror outfit that AQ leader Ayman al-Zawahiri had formed in September 2014, to take jihadi terrorism to India, Bangladesh and Myanmar.[16] One cannot discount the traction of youths from India (though comparatively marginal) to join IS and AQ in Iraq and Syria. Approximately, of the 100 people who joined the IS in its heartlands, at least half of them came from Kerala.[17] While analysts ponder the ideological underpinnings of Keralite Muslims as the propeller of these foreign fighters, it is more likely that geography and upward mobility play a defining role in pushing them forward.[18] The threat from transnational terrorism to India will get impetus if there is political shielding of radical organisations with linkages to terror organisations.

Radicalisation Likely to Lead to Polarisation of State

Over-regulation of the religious sphere in an effort to combat the radicalisation and jihadism could lead to religious contestation of societal space. There are two main planks used by ideologues to radicalise vulnerable youths—first, victimhood and the second, sense of guilt for not doing enough against perceived injustice. Morocco promotes a reformist religious approach that seeks to "balance modernity and tradition".[19] Radicalisation is a threat to democracy that leads to polarisation in society. It creates a narrative where radicalised individuals or groups start believing that there is only one system and one way of life that is correct and the rest must be eradicated by force or even by violence. It breeds intolerance to others' belief and those who do not support their ideology automatically become enemies. Radicalisation ultimately justifies the use of violence against those who oppose their ideology or belief. India is on the radar of AQ and IS. On September 4, 2014, the leader of AQ, Ayman al-Zawahiri, announced the creation of AQ in the Indian Subcontinent (Jamaat Qaidat al-Jihad fi'shibi al-qarrat al Hindiya) or AQIS.[20] The vulnerable section of the population is from J&K, parts of UP, Bihar, Bengal, Assam, Kerala and many other states in the Southern Peninsula. The government must work with religious clerics, social scientists and psychologists to control the joining of people to these organisations. Security forces

should be kept out of this gambit since they are neither structured nor can they effectively handle this aspect.

Societal Dissention and Communal Divide: A Major Intenal Security Challenge

Terrorist attacks could lead to a spike in hostile rhetoric and low- to medium-level communal violence, which in turn reduces the integration of the minority communities and could lead to acceptance and more tolerance of radicalism.[21] Sri Lanka witnessed this phenomenon post-Easter attack in April 2019, on churches by radicalised Muslims. Though the security forces could control the immediate fallout, it has created a divide in the society. With the sharp divide between Hindus and Muslims post-Citizen Amendment Act (CAA) and proposed National Register for Citizens (NRC), any act of terror by non-state actors or state-sponsored non-state actors, could create communal standoff. It needs to be understood that non-state actors find roots and space when there is a societal and communal divide within a state. Today, ISIS and AQIS are competing throughout South Asia to win recruits, conduct terror attacks and foment religious turmoil and both have increasingly fixed their gaze on India.[22] The objective of the violent extremists is to drag the state into a communal or sectarian divide to polarise the society and eliminate the societal space that represents coexistence between different ethnic and religious groups. In India, AQIS and IS, the two Salafi-Jihadist movements, are seeking to exploit Muslim-Hindu communal tensions for their gain.[23] The AQ and IS advocates the philosophy of provoking communal and sectarian conflict to create an imminent danger and perception of annihilating fear to awaken the Muslim community to wage Jihad. There is a need for the society and state to expose this dogma and that the state and the subjects need to be aware of the greater danger that comes with falling into such a conflict trap.

Illegal Immigration: Needs a Lasting Solution

India has been soft for decades, permitting illegal migrants from Bangladesh to settle in and change the demography in Assam and districts bordering Bangladesh and West Bengal.[24] As a result, the demography of Assam stands altered and the threat of Islamic insurgency/terrorism is knocking at the most critical state of India's north-east. In fact, in November 1998, late Lieutenant General SK Sinha, the then Governor of Assam, had written to the Centre: "It (illegal immigration) poses a grave threat both to the identity of the Assamese people and to our national security."[25] Unfortunately, no one paid heed to his warning. The Bangladeshi illegal immigrants now, with a newly acquired identity, will be difficult to be weeded out due to sheer numbers. This is dividing the society and could be exploited for political purposes. The major fallout is an encroachment on the traditional land that belonged to the communities and tribes and pressure on the state to provide free health, education and subsidised food. There is a likelihood of communal clash because of resource crunch and a sense of deprivation among the legal subjects of the states. Change of demography and census reports are an indicator of the presence of large-scale illegal migrants in border districts.[26] The 'half open arms policy' to settle illegal migrants for vote bank is creating a volatile ground situation. South Asia is becoming an unstable plateau and involuntary migration of population due to political, civil unrest, and disasters is very much a possibility.

Cyber, Information and Influence Operations: A Threat to Internal Security

Bruce Schneier, the Adjunct Lecturer at Harvard Kennedy School, has defined information operations as, "the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent."[27] Information and influence operations exploit cracks in the fabric of society, demography, poor economic conditions and ethnic divisions. Cyber and digital media plays an important role and is used as an enabler to target the vulnerable section of the population. The objective is to create disaffection with the state and an atmosphere of distrust with the institutions of governance. Rumours are traded as truth and fiction as facts. Elections are influenced and government laws with regard to law and order, terrorism, radicalisation and uniform law for all citizens, are portrayed as anti-minority people and at times against communities. These operations are undertaken to construct a perception that leads to hostile social manipulation of a disaffected or fractured

society. One must remember that the internet and other technologies have made it easier to weaponise and exploit societal flaws, beguiling more people faster and compellingly than ever before.[28] Artificial Intelligence has made it much easier to manufacture reality to trick vulnerable individuals and groups by provoking, deceiving or otherwise manipulating them cognitively. The desire to influence the public debate by inimical states is nothing new, as disinformation and psychological operations (PsyOps) have long been a tool in the arsenal of adversarial states.[29] Cyberwarfare is a potent tool to manipulate content to deceive, distract, and disinform the public opinion, which eventually disorient and corroborate a sense of doubt among the public or shape the opinion of a specific target audience on a manufactured narrative.[30] Large-scale cyber-attacks can disable services and critical infrastructure, that could cause massive structural and system losses. Data leakage and data fraud can cause massive losses to states and citizens. Cyberwarfare can be used to destroy the core values of the society, especially in an open and democratic state, thereby questioning institutions of governance and opposing every decision of the state that appears to be against the idea of transparency. The cyber and influence operations against Indian state and institutions are likely to intensify in the near future both from non-state actors and China-Pak strategic nexus.

Black Swan Events

Black Swan Events such as Coronavirus and 26/11 or Mumbai serial bomb blasts in 1993 have a profound impact on internal security. Coronavirus pandemic is a reminder that such Black Swan Events can disrupt freedom of society, supply chain, loss of jobs, economic shutdown and industries coming to a grinding halt apart from loss of lives. Even natural disasters, extreme weather conditions and nuclear accidents could also be part of Black Swan Events that can trigger mass migration or relocation of the population that can put life support chain out of gear. Black Swan Events can also be created by cyber in terms of disabling financial systems, services or even massive theft/leakage of data. Therefore, intelligence agencies and risk management protocols must always be ready to handle such unpredictable situations. Therefore, the contingency plans must exist to deal with such events.

Water Security

Water wars have already begun. There will be 40 percent of Indians who will have no access to drinking water by 2030 and nearly 600 million Indians today are facing high-to-extreme water stress.[31] This is one of the most precious resources that will be contested by the states as well as individuals for survival. Water scarcity can cause mass migration and dislocation of the public from its life-sustaining chain. It is not possible for the states to immediately meet the requirement of housing, food and life support system for unexpected mass migration. It can lead to public disorder and uncontrolled chaos. Water management and mapping of resources are essential. The only method to resuscitate the water sources is the preservation of green cover and a campaign to prevent environmental degradation. India is already on the brink of water scarcity since India holds just about 4 percent of global freshwater and 16 percent of its population.[32] Thus, we are racing against time.

Way Forward

Identify Perils of Corridor to Block Them

Threat monitoring and situational awareness rely heavily on intelligence, surveillance and reconnaissance (ISR) operations. The future challenges range from highly capable near-peer competitors to empowered individuals with nefarious intentions.[33] One of the reasons for insurgencies in north-east and Red Corridor is ungoverned territory that gives rise to erosion in institutions of governance. Instability is triggered when threat monitoring and situational awareness is poor. The dynamic and vibrant intelligence network can act as a shield against the perils of the corridor that may be state-sponsored or triggered by non-state actors. Fusion of Artificial Intelligence (AI), technology based platforms and human intelligence is vital for identification, monitoring and blocking perils of corridor. Equally important is intelligence operations for counter-narrative operations and decoding the threat from political/influence operations.

Dealing with Internal Security is a Whole of Government Approach

The internal security is no more the domain of security forces. It requires the whole of government approach to

deal with the threats that are amorphous and diverse in nature. The threat is from cyber, information, psychological, political, economic and state and non-state actors. It can manifest in the form of violent extremism or even in the cognitive domain. Thus, the response could be through intelligence operations, the participation of society elites, psychological operations, legal warfare, as well as the use of cyber and the security forces. More important is that the state must move fast and not at a bureaucratic pace because insurgents and terror organisations are working at internet speed and government agencies are working at a bureaucratic pace. It is the responsibility of the state to ensure that the best way to deal with radicalisation is to put in place counter and anti-radicalisation measures. De-radicalisation though is desirable but it is extremely difficult to reclaim the radicalised youths. To prevent the disaffection of the youths and eliminate dissention with the state, there is a need to deliver governance and ensure transparency in its functioning.

Technology a Major Stakeholder

The nineteenth-century Industrial Revolution showed how technological asymmetry can translate into geopolitical inequality. In the words of Hilaire Belloc's poem, *The Modern Traveller*, spoken by a European about Africa: "Whatever happens, we have got the Maxim Gun, and they have not." (The Maxim Gun was the first recoil-operated machine gun.)[34] Technology is a tool to deny, disrupt, defeat and destroy the threat that may be from radicals, violent extremists and technologically enabled adversaries. Technology can assist intelligence gathering, strengthening of surveillance grid, public awareness and can also improve urban safety. It is not possible to monitor millions of people who are moving at a fast pace from one city to another by human intelligence; thus, it requires Artificial Intelligence (AI) and networked security set up. Digital mapping of population, CCTV monitoring streets, cities, highways, and even the communication centres are becoming imperative. However, it is not only the technology that can assist in making cities and urban areas safe but to run technology-based systems, it requires trained and skilled manpower that can handle technology at a speed faster than adversaries. Digital mapping of the population is vital and so is having streets and highways under constant electronic surveillance.

Robust Intelligence and Analysis System

Coronavirus pandemic has taught the global community a lesson that, every nation must have a resilient intelligence system that can identify, monitor, and forewarn nations to put protocol of precaution in place so that it does not hurt the economy, the security of citizens and the nation as a whole. Intelligence for a pandemic, grey zone threats and other internal and external security threats differ from each other. It requires a completely different set of skills, technology and method of operations. Therefore, India will have to take a hard look at current intelligence organisations to fight future threats.

Conclusion

Safeguarding the idea of the nation necessitates the identification of threats and the genesis of the threat. Mike Maddison, the Head of Security and Privacy Services at Deloitte UK had said, "You can have the best technical systems in place, but they're not effective if people aren't educated about the risks."[35] Stronger integration of different actors in society, including non-governmental organisations, civil society and business organisations is essential to deny exposed flank to the divisive forces. The technology and agile security measures can not only prevent crime but also improve the efficiency of the criminal justice system.[36] The bottom-line is that, internal security is the responsibility of every citizen and organ of the state. The man and machine both have an important role to secure the nation and make urban areas secure.

Notes

1. Hamid Ansari's speech at 5th K Subrahmanyam Memorial Lecture, 'Some Thoughts on the Domestic Dimensions of Security', released by Press Information Bureau Government of India, released on 14 February 2017.
2. PTI, 'Jat Stir: North India May Face Rs 34,000 Crore Loss, Price Rise', *The Economic Times*, 22 February 2016.
3. Hamid Ansari, 'For Internal Security, the State Must Be Accountable and True to Its Principles', *The Wire*, 15 February 2017.
4. 'The National Security Strategy, Sharing a Common Project', Spain 2013, P 6.
5. Ebeh and John Igbogo, 'National Security and National Development: A Critique', *International Journal of Arts and Humanities*, Vol. 4(2), No 14, April 2015.

...to India in 2020 and Beyond

6. Ibid.

7. Ansari, op. cit (3).

8. Danny Pronk, 'The Return of Political Warfare', *Strategic Monitor 2018-2019*.

9. Ibid.

10. Moushumi Das Gupta, '43 Companies With Rs 13,700 Crore Investment Plan Promise J&K a New Beginning', *The Print*, 18 October 2019.

11. Namrata Biji Ahuja, 'There are a Host of Unresolved Issues', *The Week*, 4 January 2020.

12. Bula Devi, 'Former NSCN (IM) Commander-in-Chief and Associates Slip into China', *National Herald*, 23 November 2019.

13. Namrata Biji Ahuja, 'NSCN (IM) Seeks Support From China as India Hardens Stand on Naga Deal', *The Week*, 22 November 2019.

14. Hriday Ch. Sarma, 'United Liberation Front of Western South East Asia–A New Found Alliance of Terror or an Eruption of Indigenous Grievances?', *Trans Conflict*, 22 September 2015.

15. 'China Wants to Maintain Instability in North-East India', IANS, *India Today*, 26 August 2012.

16. Asim Umar, 'al-Qaeda Terrorist From India Who Had no Digital Footprint', *India Today*, 9 October 2019.

17. 'About 100 People FrKerala Joined ISIS Over the Years: Police', *India Today*, 11 November 2017.

18. Mohammed Sinan Siyech, 'The Islamic State in India: Upgrading Capabilities?', Middle East Institute, 5 February 2019.

19. 'How the Islamic State Rose, Fell and Could Rise Again in the Maghreb, Crisis Group', Report 178/Middle East and North Africa, 24 July 2017.

20. Hari Prasad, 'The Salafi-Jihadist Reaction to Hindu Nationalism', Hudson Institute, 11 July 2019.

21. Daniel Byman, 'Terrorism and the Threat to Democracy', The Brookings Institution, February 2019.

22. Prasad, op. cit. (21).

23. Prasad op. cit. (21).

24. Harsha Kakar, 'Refugees: India Should Learn From Europe's Mistakes', Observer Research Foundation, 25 October 2017.

25. Ibid.

26. Ibid.

27. Bruce Schneier, '8 Ways to Stay Ahead of Influence Operations', *Foreign Policy*, 12 August 2019.

28. Christopher Paul and Marek N Posard, 'Artificial Intelligence and the Manufacturing of Reality', *Rand Corporation*, 20 January 2020.

29. Fabio Rugge, 'Mind Hacking: Information Warfare in the Cyber Age', available at https://www.ispionline.it/it/pubblicazione/mind-hacking-information-warfare-cyber-age-19414, accessed on 19 January 2020.

30. Ibid.

31. Bhasker Tripath, '40% of Indians Will Have no Access to Drinking Water by 2030: NITI Aayog', *Business Standard*, 25 June 2018.

32. Ibid.

33. Claudette Roulo, 'Worldwide Threat Scope, Complexity on the Rise', Defence Intelligence Agency, 4 February 2015.

34. Anja Kaspersen, Espen Barth Eide, and Philip Shetler-Jones, '10 Trends for the Future of Warfare', *World Economic Forum*, 3 November 2018.

35. Sally Whittle, 'The Top Five Internal Security Threats', available at https://www.zdnet.com/article/the-top-five-internal-security-threats, accessed on 10 March 2008.

36. Robert Muggah, 'How Smart Tech Helps Cities Fight Terrorism and Crime', *World Economic Forum*, 15 June 2018.