CENTRE FOR SECURITY STUDIES | **ISSUE BRIEF**

AUGUST 2022

ANALYSIS OF 5G AND FUTURE PROSPECTS FOR THE INDIAN ARMED FORCES

Arun Teja Polcumpally and

Bibaswan Bose

Edited By: Divyashree Jha

About the author

Arun Teja Polcumpally is a PhD Candidate at the Jindal School of International Affairs and a Research Associate at the Centre for Security Studies, JSIA.

Bibaswan Bose is a Doctoral fellow at the Centre of Automotive Research and Tribology, Indian Institute of Technology, Delhi.

About the Centre for Security Studies

The Centre for Security Studies (CSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof Dr Pankaj K Jha. Researchers at CSS – through in-depth analysis briefs and events, reports, policy briefs and print publications – explore both regional and thematic topics in the broader field of international security studies. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian and religious conflict; civil wars and state failure; cyber and space warfare; resource-related security issues; the proliferation of weapons of mass destruction; defence economics and also the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Centre for Security Studies attempts to unfold. Please refer to www.cssjsia.com for further details, and follow the Centre's social media platforms for critical news and research updates:


www.linkedin.com/company/jindal-centre-for-security-studies/


www.instagram.com/css_jsia/


https://twitter.com/Css_Jsia

Get in touch with us through email: css@jgu.edu.in

Important disclaimer

IB2208002

Introduction

Atmanirbharta (Self-reliance) has become a non-negotiable goal of the Indian NDA government under Prime Minister Modi's leadership. Modi's government aims to make it a national mission. The government website dedicated to this goal asks the public to submit their stories of developing autonomous technology and models. A website pinning public stories is a good way of marketing this idea and encouraging the public to get involved. However, under atmanirbhar Abhiyan, the government has put all the initiatives, including welfare policies . Such government actions confuse the public regarding the meaning and scope of 'Atmanirbharta.' Without getting into the political debates, the generic understanding of the term espouses that it aims to achieve self-reliance in almost all sectors. One of the primary sectors where Atmanirbharta becomes important is Defence.

To encourage the indigenous defence industry, in the budget designed for the financial year 2023, it has been decided that INR 55000 crores would be allocated to defence development outside Defence Research and Development Organisation (DRDO) [Behera, 2022]. This budget allotment shows that the government is dedicated to opening new research vistas apart from the government research institutions. To encourage new ideas and technological innovations, a scheme with INR 500 crores has been launched to promote Defence start-ups. Not just asking Indians to provide innovative solutions, the government has also undertaken other initiatives to discourage technology imports. The defence establishment gradually increased the list of items that fall into the category of the import ban. The list numbered 101 in 2020 and grew to 351 in 2021 [Saxena, 2022]. These developments represent India's quest to develop defence technologies indigenously.

Indian Defence Review 2021 [Ministry of Defence, 2021] presented some indigenous technological advancements. One example was 'Robotic Lifebuoys' developed by Saif Seas based in Visakhapatnam. This robot is controlled externally by a person at bay. Such technologies are not new; this era requires automation and robots to have some essential intelligence. Attaining new digital technologies like Artificial Intelligence and quantum communications is becoming a zero-sum game. If India does not have these digital

technologies developed indigenously, there is a risk of becoming a technologically inferior power compared tothose who first developed them. Such a situation in hindsight, this article details the focus of Indian defence establishment in 5G technology. It evaluates this technology's use cases and provides prospects.

5G, and its Working

5G communication provides less latency and ultra-fast data transfers using small receivers and senders located across the spaces. It is claimed that 5G would deliver data at less than a millisecond, seven timeshigher than 4G and achieve a peak download speed of 20 Gigabytes per second [Nordum and Clark, 2017]. That means a full HD movie can be downloaded in under a second! 5G technology is not a unique product designed which enhances the speed and bandwidth of data sharing. It is a technique that combines existing technologies and infrastructures, reducing latency and improving the bandwidth securing more connections [Oughton and Frias, 2018]. Five key functional enhancements that 5G provides are.

1. Enhanced mobile broadband
2. Ultra-reliable low latency communication
3. Security
4. Massive machine-type communications
5. Power efficiency

Five techniques can be used to create 5G - Millimeter waves, small cells, Massive MIMO, Beam Forming and Full Duplex [Nordrum and Kristen, 2017]. A simple understanding of the above combination is that.

1. The data from a device is emitted or received in the form of millimetre waves.
2. The receiving and transmitting of those millimetre waves are coordinated using

'Small cells' and 'Massive MIMO.' Small cells are just some kinds of antennae that can be mounted on streetlights and buildings because of their size. These mounted antennae would connect devices simultaneously and send them to the nearest Massive MIMO. Massive MIMO is an augmentation of 100s of large antennae at a single tower. Such extensive collection makes the transfer of large data packets possible. This makes the periphery of the 5G infrastructure.

3. Another technique used would be beam forming. This technique identifies a unique path for a signal to get transmitted efficiently. Similar to that of our google maps. It gives us the best route to the destination. Beamforming is an algorithm that helps identify the most efficient paths for the signals.
4. Last technique is Full Duplex. It makes a user receive and dial a call simultaneously. On a single spectrum, data can simultaneously go in two directions.

All these techniques are used to reduce the latency and increase the speed, which is the core functionality of 5G. The utility of 5G is enormous. It forms a base for all the upcoming revolutions. Driverless cars, AI systems, Internet of Things, Hologram-based virtual meetings, and Virtual reality will seamlessly function (if not be enabled) with 5G. World Economic Forum's paper describes five functional drivers to accelerate the world's digitisation. These functional drivers reshape economies, societies, the military cultures through an unparalleled level of connectivity (Umbach, 2020, p. 5).

Importance of 5G for Indian Military

Considering the growing significance of the data and its allied technologies, 5G technology is regarded as a critical technology [Chikermane, 2019]. Technologically advanced countries like China, the US and Russia are building their 5G infrastructures and trying to divide the rest of the world into allies. Non-allies' groups [Chikermane, 2019] [Jaisal, 2020] show the geopolitical importance of 5G. It is understood from the earlier section that it helps increase the speed and reduce the latency of information flow.

For the military, these aspects will help in realising D2D (Device to Device) and Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2I) communications [Bhardwaj, 2020]. All these mentioned use cases are nothing but efficient use of the Internet of Things (IoT). The IoT concept is realised with the help of 5G networks. Some advanced defence research in India is on hyper-glided vehicles (HGV), swarm drones, and soldier wearables. All these products would require high-speed data transfers enabled by 5G.

For this technology to be realised by the brains of India, the first step is to establish a test bed for the 5G prototypes. India, though a latecomer in this segment, has launched a test bed of eight research institutions led by IIT Madras. The testbed is distributed in six locations. IIT Delhi, Kanpur, Bombay, Madras, Hyderabad, and IISC Bengaluru. This is an essential step toward what the current government calls - Atmanirbharta (Self - Reliance).

This article is not about the importance of 5G but provides a detailed description of the prospects of 5G and the challenges it can face. Accordingly, the following section will detail the political, economic, social and technological aspects of the 5G adoption for the Indian military.

PEST Analysis of the 5G Technology

Political	Economic
1. An outright ban on the Chinese 5G Vendors 2. Absence of Key Technology companies in India	1. As per the union budget 2022, 68 % of the procurement budget is dedicated to domestic industries [India, 2022] 2. 25 % of the defence R&D has been dedicated to Academia, Industry and Startups [India, 2022] 3. High capital cost to set up receivers and

	transmitters within a short distance
Management and Business	**Technological**
1. Absence of 5G technology impact assessment on Defence 2. Only a few 5G technology providers are present worldwide without any Indian company 3. Complex supply chains of 5G will result in security loopholes [Kuehn and Trisha, 2021]	1. Unknown technical vulnerabilities [Kuehn and Trisha, 2021] 2. Spectrum allocation [Polcumpally, 2021] 3. Absence of common 5G standards 4. Increase in the IoT technology

4.1 Current Key Players

The current key players in providing the 5G technology are - Ericsson (Sweden), Huawei (China), Nokia Networks (Finland), Samsung (South Korea), NEC (Japan), Thales Group (France), L3Harris Technologies, Inc. (US), Raytheon Technologies (US), Ligado Networks (US), and Wind River Systems, Inc. (the US) [Marketsandmarkets, 2022].

Challenges to 5G Implementation in the Indian Military

The complex interconnection of the military devices with 5G will force the entire tri-forces to securitise the network. Any hack into the communication network will mean

halting the whole of coordinated operations. Threats to the network are classified into four categories [Bhardwaj, 2020]

1. Eavesdropping and Traffic Analysis
2. Jamming
3. Denial of Service (DoS)
4. Man in the Middle Attack

It is noted that 5G will allow all the wireless access technologies so that various devices can communicate [Bhardwaj, 2020]. If this is the case, all types of attacks are also possible. Further, for practical uses, itis proposed that the network infrastructure would be shared among the service providers [Guha, 2021]. Here, the challenge is data accessibility. Is the data safe if the military uses the infrastructure shared by private companies?

Finally, the capital investment is high for setting up the 5G network equipment [Gill, 2019]. It includes new massive MIMO equipment and new devices that can communicate with the allocated 5G spectrum.

5G Solutions Identified from IEEE

To ensure information security, dependability, and administration, the military communication network can utilise 5G massive bandwidth, low time delay, high reliability, multiple connection network capabilities, and multi-access edge computing [Porambage et al., 2018, Al-Ansi et al., 2021]. A 5G military affairs particular network must be constructed to provide a unique, customised network that can use 5G technology to boost military efficiency and meet a range of military application scenarios [Khan et al., 2020, Kania, 2021]. The military network can be completely isolated from the public network and have lower bandwidth [Liao and Ou, 2020]. This will help to create an exclusive, secure, stable, and cost-effective network [Grønsund et al., 2020]. In 2B(to Business), there are seven 5G private network implementation techniques [Bajracharya et al., 2020]. Varied

deployment methodologies are required for different Business and security isolation demands. The following are the top two techniques which will ensure military data security strategies:

The first scheme (as shown in Figure 1) aims to build a private network utilising an existing public or private network's frequency band while isolating the control and user planes from the public network. The 5G specialised network frequency band is a part of the 5G plane that the industry has allocated. Vertical enterprises may build networks independent of service provider constraints because of 5G's frequency spectrum. Because of the restricted spectrum of resources made available to all service providers by the ministry of industry and information technology (MIIT), the military communication spectrum should be dispersed when commercial network standards become available. This deployment technique ensures security by segregating military application data from the public network. The core and wireless access networks may be placed on combat platforms because of their short data transmission distances and low network latency. The private network will not be jeopardised if the digger cuts and blocks the public optical link. It is appropriate for scenarios that demand- mobility, security, and reliability in battle command and equipment support. Because of the network's independence, there are significant installation and ongoing maintenance expenses.

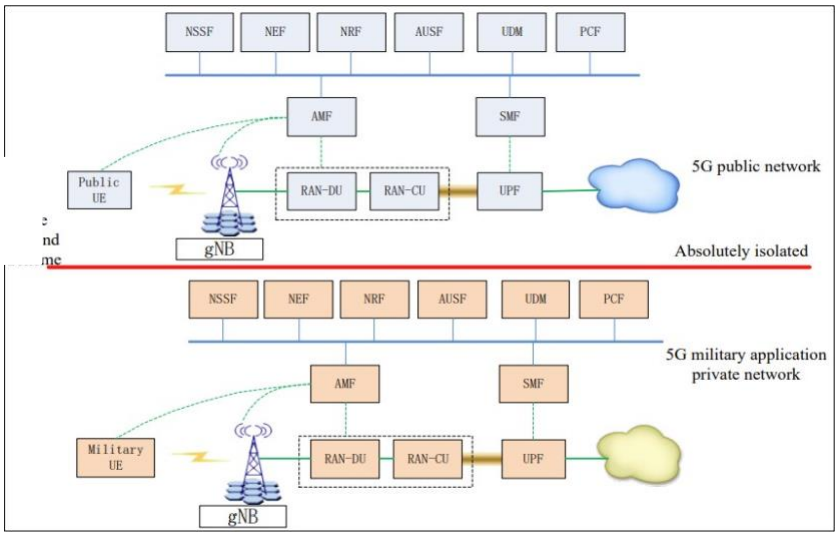

Figure 1: Completely isolated network planes

The second scheme (as shown in Figure 2) aims to use the basic propagation layout of the public network and, at the same time, have a separate control plane. The public network components implement the private and public network control plane functions (authentication, mobility management, etc.). Data may flow inside the private network, but signalling must pass via the control surface of the public network. The second approach may jeopardise data security and privacy. It works well in settings requiring little isolation, such as training exercises and logistical assistance. Meanwhile, network maintenance costs will be reduced.

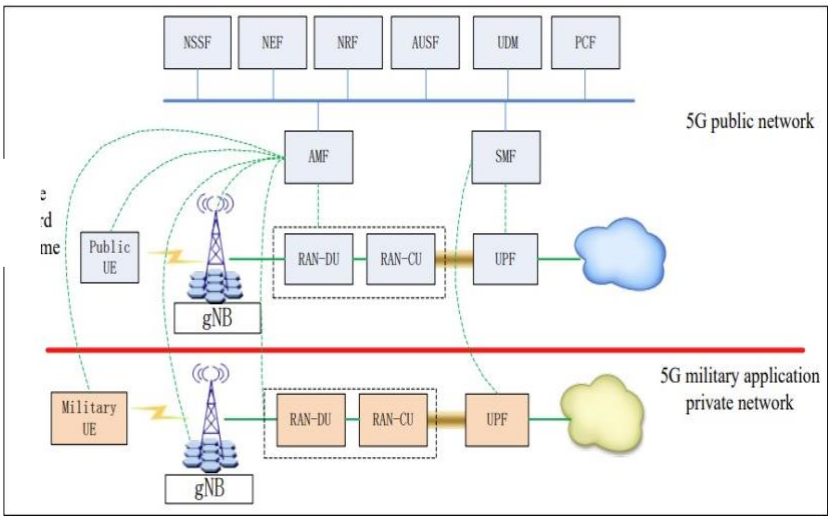

Figure 2: Partially isolated network planes

The TSDSI is developing 5Gi (5G India) standards in India. As part of 5Gi, CEWIT, SAMEER, IISc Bangalore, and five IITs (Madras, Hyderabad, Delhi, Kanpur, and Bombay) are building an end-to-end 5G test bed. In 2018, Rs 2,240 million was invested in the project. The initiative aims to increase academic-industry cooperation on 5Gi standards. Indian Indigenous Test Bed is a native solution. FR1 (3.5 GHz) and FR2 hardware and core networks are being developed (26 GHz). LMLC and MEITY were created effectively to meet rural India's and emerging nations' needs. IMT-2020 releases should include LMLC.

Conclusion

This issue brief has provided a quick understanding of 5G working and the challenges Indian armed forces would face. The PEST analysis from the literature provides the challenges the Indian military would face politically, economically, socially and technologically. PEST analysis is followed by specific challenges faced by the Indian army. The significant challenges identified were economic and technological. Finally, two solutions have been identified from the literature to overcome the technical challenge. The first is to isolate the control planes from the public network using the same commercial bandwidth. The second solution is to have separate control panes for commercial and military communications, but the signal passes through a single control layer.

Now that India has started with the auction of the 5G spectrum, one problem is solved. Action toward the 5G roll-out has been initiated. However, from the argument of Atmanirbharta, India does not have technology companies that have patented 5G technology. Technologically dominating countries like the US and China are leading in the 5G race. Not just 5G., they compete for dominance in all the emerging technologies.

Competing against these technologically advanced countries for dominance in 5G is not suggested for India. India plunged into action when it came to the adoption of 5G. Still, specific recommendations identified from the literature would aid India in tackling technological global politics [Jaisal, 2020].

5. Establish a dedicated and permanent council to deal with emerging technologies and policies.

6. Form a global front apart from the US and China block.

The second recommendation appears like the non-alignment movement, which, even in history, proved futile. The first recommendation is practical. Even the government policymakers would need technology experts to weigh in while making security policies on

emerging technologies. A dedicated department working on them would provide an informed decision-making capacity to the security establishment.

Even in this area, India is actively looking to establish a National Research Foundation along the lines of the US national research funding agency - the National Science Foundation. It would be better if the impact assessment research is also funded significantly. It would help in quick policy making, an area India severely lacks.

Bibliography

[Al-Ansi et al., 2021] Al-Ansi, A., Al-Ansi, A. M., Muthanna, A., Elgendy, I. A., and Koucheryavy, A. (2021). Survey on intelligence edge computing in 6g: Characteristics, challenges, potential use cases, and market drivers. *Future Internet*, 13(5).

[Bajracharya et al., 2020] Bajracharya, R., Shrestha, R., and Jung, H. (2020). Future is unlicensed: Private 5g unlicensed network for connecting industries of the future. *Sensors*, 20(10).

[Behera, 2022] Behera, Kumar, L. (2022). Towards atmanirbharta in defence production.

[Bhardwaj, 2020] Bhardwaj, A. (2020). 5g for military communications. *Procedia Computer Science*, 171:2665– 2674.

[Chikermane, 2019] Chikermane, G. (2019). 5g infrastructure, huawei's techno-economic advantages and India'snational security concerns: An analysis. *ORF Occasional Paper*, (226):62.

[Gill, 2019] Gill, P. (2019). 5 g network - here are the biggest challenges for India as it rolls out its 5g network. https://www.businessinsider.in/tech/news/biggest-challenges-for-indias-5g-network-connectivity- according-to-strategy-expert/articleshow/71609944.cms. (Accessed on 07/31/2022).

[Grønsund et al., 2020] Grønsund, P., Gonzalez, A., Mahmood, K., Homeland, K., Pitter, J., Dimitriadis, A., Berg, T.-K., and Gelardi, S. (2020). 5g service and slice implementation for a military use case. In *2020 IEEE International Conference on Communications Workshops (ICC W orkshops)*, pages 1–6.

[Guha, 2021] Guha, I. (2021). Infra providers eye towersharingpolicy ahead of 5g roll-out — mint. https://www.livemint.com/technology/tech-news/infra-providers-eye-tower-sharing-policy-ahead-of- 5g-rollout-11614014569665.html. (Accessed on 07/31/2022).

[India, and] India, T. (n.d). Reforms.

[India, 2022] India, T. D. I. (2022). Union budget 2022: A roadway to atmanirbhar defence ecosystem. Technical report, Ministry of Finance.

[Jaisal, 2020] Jaisal, E. (2020). The us, china and Huawei debate on 5g telecom technology: Global apprehen- sions and the Indian scenario. *Open Political Science*, 3(1):66–72.

[Kania, 2021] Kania, E. B. (2021). Artificial intelligence in china's revolution in military affairs. *Journal of Strategic Studies*, 44(4):515–542.

[Khan et al., 2020] Khan, R., Kumar, P., Jayakody, D. N. K., and Liyanage, M. (2020). A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys Tutorials*, 22(1):196–248.

[Kuehn and Trisha, 2021] Kuehn, A. and Trisha, R. (2021). This connection is secure: 5g risk and resilience framework for the quad.

[Liao and Ou, 2020] Liao, J. and Ou, X. (2020). 5g military application scenarios and private network ar- chitectures. In *2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, pages 726–732.

[Marketsandmarkets, 2022] Marketsandmarkets (2022). 5g in defense market by communication infrastructure (small cell, macro cell), core network technology, platform (land, naval, airborne), end user, network type, chipset, operational frequency, installation and region (2022-2027).

[Ministry of Defense, 2021] Ministry of Defense (2021). Technical report, Press Information Bureau.

[Nordrum and Kristen, 2017] Nordrum, A. and Kristen, C. (2017). *Everything You Need to Know About 5G*. Accessed: 2022-06-29.

[Nordum and Clark, 2017] Nordum, A. and Clark, K. (2017). Everything you need to know about 5g - IEEE spectrum. https://spectrum.ieee.org/everything-you-need-to-know-about-5g. (Accessed on 07/31/2022).

[Oughton and Frias, 2018] Oughton, E. J. and Frias, Z. (2018). The cost, coverage and

roll-out implications of 5g infrastructure in Britain. *Telecommunications Policy*, 42(8):636–652. The implications of 5G networks: Paving the way for mobile innovation?

[Polcumpally, 2021] Polcumpally, Arun, T. (2021). D10 as an alternative to Huawei 5g.

[Porambage et al., 2018] Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., and Taleb, T. (2018). Survey on multi-access edge computing for internet of things realisation. *IEEE Communications Surveys Tutorials*, 20(4):2961–2991.

[Saxena, 2022] Saxena, V. K. (2022). *Atmanirbharta in Defence: How has been the Journey So Far? Whereare we Headed?*

*****

Arun Teja Polcumpally is a PhD Candidate at the Jindal School of International Affairs and a Research Associate at the Centre for Security Studies, JSIA.

Bibaswan Bose is a Doctoral fellow at the Centre of Automotive Research and Tribology, Indian Institute of Technology, Delhi.