5जी युग में साइबर सुरक्षा की चुनौतियाँ

हम जिस प्रकार से इंटरनेट पर सामग्री का संचार और उपभोग करते हैं उसे देखते हुए 5जी की अति-तीव्र गति से वास्तव में क्रांतिकारी बदलाव हो सकते हैं। भारत में अक्तूबर 2022 में 5जी सेवाएं आरम्भ हुईं थीं और इन दिनों दूरसंचार कम्पनियाँ कुछ चुने हुए शहरों में इसकी सेवाएं दे रही हैं। देश में 2024 के अन्त तक 15 करोड़ से अधिक 5जी उपयोक्ता होने का अनुमान है जो मौजूदा 1 अरब 20 करोड़ मोबाइल फ़ोन उपयोक्ताओं का एक छोटा-सा अंश है। हाल में बढ़े साइबर हमलों और शत्रु देशों तथा ख़तरा पैदा करने वाले अन्य कारकों द्वारा डाटा चोरी या सेंधमारी के पीछे भू-राजनीतिक प्रतिद्वन्द्विता, वाणिज्यिक उद्देश्य और डाटा संचयन जैसे मौलिक कारण हैं। इसलिए यह 5जी नेटवर्क के लिए भी ख़तरा पैदा करेंगे। इनमें महत्वपूर्ण राष्ट्रीय बुनियादी ढाँचे को निशाना बनाने वालों की यह प्रवृत्ति बढ़ी है।

डॉ समीर पाटिल

ऑब्ज़र्वर रीसर्च फाउण्डेशन के विचार मंच में सीनियर फ़ैलो। परस्पर प्रौद्योगिकी और राष्ट्रीय सुरक्षा के लिये कार्यरत।
ई-मेल: sameer.patil@orfonline.org

5जी यानी मोबाइल नेटवर्क की पाँचवीं पीढ़ी, बेतार संचार का नवीनतम वैश्विक मानदंड है। प्रत्येक वर्ष बाद, मोबाइल संचार की एक नई पीढ़ी आती है जो 1जी, 2जी, 3जी, 4जी नेटवर्क इत्यादि के नाम से जानी गई। हर नई पीढ़ी अपने साथ डाटा की मात्रा और गति बढ़ाती रही और प्रेषण अथवा प्राप्ति का समय घटाती गई- यानी डाटा ट्रांसफ़र और डाउनलोड में समय कम होता गया। आशा है कि 5जी से औसत डाटा दर 100 मेगाबिट्स प्रति सेकण्ड होगी और यह बढ़कर 20 गैगाबिट्स प्रति सैकण्ड हो सकती है। इतनी तीव्र गति होने से समय-विलम्बता दर और घटेगी तथा इस प्रकार मोबाइल डाटा संचार में अधिक विश्वसनीयता सुनिश्चित होगी।

हम इंटरनेट पर सामग्री का संचार और उपभोग जिस प्रकार करते हैं उसमें 5जी की अति-तीव्र गति वास्तव में क्रांतिकारी बदलाव ला सकती है। 5जी नेटवर्क शुरू होने का सर्वाधिक ध्यान देने योग्य प्रभाव, उन्नत मोबाइल सेवा में देखने को मिला।[1] इसके बाद तो यह अब धीरे-धीरे शिक्षा प्रौद्योगिकी (एडटेक) स्वायत्त और रोबॉटिक प्रणालियों, टेलीमेडिसिन और सटीक कृषि (प्रिसाइज़ एग्रीकल्चर) को प्रभावित करेगा। यही

नहीं, 5जी इंटरनेट ऑफ़ थिंग्स (आईओटी) प्रौद्योगिकियों और कनेक्टेड उपकरणों के लाभ भी सामने लायेगा। तीव्र गति और अल्प-विलम्बता कनेक्टेड उपकरणों को वास्तविक समय में संवाद करने में सक्षम करेगी, जो बेहतर और अधिक विश्वसनीय कार्यक्षमता होगी। इससे घरेलू उद्देश्यों (जैसे आईओटी-सक्षम स्मार्ट होम) और औद्योगिक क्षेत्र (जैसे-स्मार्ट कारखाने और स्वचालित विनिर्माण) को लाभ होगा। एक अध्ययन के अनुसार 2035 तक 5जी की बदौलत वैश्विक आर्थिक उत्पादन 13 खरब 20 अरब अमरीकी डॉलर हो सकेगा और 22 करोड़ 30 लाख नौकरियों की मदद देगा।[2]

भारत में 5जी सेवा अक्तूबर 2022 में आरम्भ हुई और दूरसंचार कम्पनियों ने दिल्ली, मुम्बई, बेंगलुरु और कोलकाता जैसे चुने हुए शहरों में इसकी सेवा देना शुरू कर दिया। देश में 2024 के अंत तक 15 करोड़ उपयोक्ता होने का अनुमान है जो मोबाइल फोन का इस्तेमाल करने वाली एक अरब बीस करोड़ की आबादी का अंशमात्र है। लेकिन दूसरी और तीसरी श्रेणी के शहरों में एक बार 5जी नेटवर्क आरम्भ होने के बाद, यह संख्या काफ़ी बढ़ सकती है।

> **राष्ट्रीय विकास और आर्थिक विकास में 5जी की सम्भावित भूमिका को देखते हुए इसे निःसंदेह एक महत्वपूर्ण बुनियादी ढाँचा माना जा सकता है। इसलिए 5जी संचार नेटवर्क, तोड़फोड़ सहित साइबर हमलों का एक अहम निशाना होगा।**

5जी की भू-राजनीति

हमारे डिजिटल भविष्य को प्रभावित करने और आर्थिक परिवर्तन लाने की इसकी क्षमता को देखते हुए, कोई आश्चर्य नहीं है कि अग्रणी तकनीकी शक्तियों ने 5जी प्रौद्योगिकी में 'फ़र्स्ट मूवर' लाभ प्राप्त करने का प्रयास किया है। हालाँकि, दुनिया की अग्रणी दूरसंचार कम्पनियों ने 5जी प्रौद्योगिकी विकसित करने का बीड़ा उठाया, लेकिन असली बल चीनी दूरसंचार कम्पनियों ने डाला जो प्रौद्योगिकी का व्यावसायीकरण और इसे अपने प्रतिस्पर्धियों की तुलना में सस्ती दरों पर पेश करके नये बाज़ारों में आक्रामक रूप से प्रवेश कर रही हैं। इससे यह चिन्ता पैदा हो गई कि चीन रणनीतिक रूप से इन कम्पनियों को वैश्विक बाज़ारों पर कब्ज़ा करने के लिए प्रेरित करके जासूसी का एक विशाल तंत्र स्थापित कर सकता है।

ऐसी भी आशंकाएं हैं कि चीन अपनी दूरसंचार कम्पनियों को उपभोक्ताओं की सूचनाएं सरकार के साथ साझा करने को मजबूर करके, 5जी प्रौद्योगिकी को अपना हथियार बना सकता है या कम्पनियों को भू-राजनीतिक उथल-पुथल के समय 5जी नेटवर्क बन्द करने तक के लिए मजबूर कर सकता है।[3] कई देशों में साइबर जासूसी की घटनाओं और आरोपों में कई चीनी दूरसंचार कम्पनियों का नाम आने के बाद से इन चिन्ताओं को बल ही मिला है।[4] उदाहरणार्थ- अगस्त 2020 में ऑस्ट्रेलियाई सरकार और पापुआ न्यू गिनी के राष्ट्रीय साइबर सुरक्षा केन्द्र की एक रिपोर्ट में कहा गया कि एक चीनी दूरसंचार कम्पनी जिसने पापुआ न्यू गिनी का राष्ट्रीय डाटा केन्द्र बनाया था, उसमें साइबर सुरक्षा सम्बन्धी अनेक मुद्दे पाये गये जिसने सरकार का गोपनीय डाटा उजागर कर दिया। इसी तरह 2019 में, इतालवी दूरसंचार नेटवर्क के लिए इसी चीनी कम्पनी के लगाए उपकरणों में कई तरह की कमियाँ पाई गईं। इन उदाहरणों ने चीनी दूरसंचार कम्पनियों के उपकरणों की सुरक्षा, उपलब्धता और विश्वसनीयता पर सन्देह पैदा किया है- कई विशेषज्ञों का मानना है कि ऐसी चिन्ताएँ 5जी डोमेन में और बढ़ेंगी ही।

परिणामवश, पिछले कुछ वर्षों से अमरीका ने 5जी बाज़ार में चीनी दूरसंचार कम्पनियों के प्रभुत्व का मुक़ाबला करने का अभियान शुरू किया है। अमरीकी सरकार ने हुआवेई और ज़ैडटीई को राष्ट्रीय सुरक्षा के लिये ख़तरा बता दिया[5], अमरीकी कम्पनियों को इनके उपकरण ख़रीदने में सरकारी सब्सिडी का उपयोग करने पर प्रतिबंध लगा दिया, और एक विशिष्ट लाइसेंस के बिना हुआवेई कम्पनी को सेमीकंडक्टर चिप्स बेचने पर भी प्रतिबन्ध लगा दिया। हाल में, नवम्बर 2022 में एक और व्यापक कार्रवाई करते हुए अमरीका ने चीन की पाँच कम्पनियों के संचार के नये उपकरण बेचने और उनका आयात करने

पर प्रतिबन्ध लगा दिया। यही नहीं, अमरीका ने अपने सहयोगी देशों को अपने घरेलू 5जी नेटवर्क में चीनी उपकरणों का उपयोग न करने के लिए भी राज़ी कर लिया है।[6]

ज़ाहिर है इन घटनाक्रमों ने न केवल चीन और अमरीका के बीच व्यापार को प्रभावित किया अपितु लोकतांत्रिक देशों और तानाशाही शासनों के बीच व्यापक तकनीकी प्रतिस्पर्धा भी सामने आई है। नतीजतन, चीन और रूस जैसे तानाशाही शासनों से उत्पन्न तकनीकी चुनौती से संयुक्त रूप से निपटने के लिए समान विचारधारा वाले और अग्रणी लोकतांत्रिक देशों को एकजुट करने के प्रयास किये गये हैं।[7] उदाहरण के लिए, ब्रिटेन के पूर्व प्रधानमंत्री बॉरिस जॉनसन ने 5जी और अन्य उभरती प्रौद्योगिकियों की एक वैकल्पिक आपूर्ति शृंखला बनाने के लिए दस लोकतंत्रीय देशों के गठबंधन डी-10 का विचार पेश किया था। चार देशों की सुरक्षा वार्ता यानी क्वाड (भारत, जापान, ऑस्ट्रेलिया और संयुक्त राज्य अमरीका) ने भी अंतर-संचालन-सक्षमता (इंटरऑपरेबिलिटी) और संरक्षा का काम आगे बढ़ाने और 5जी सप्लायर डायवर्सिफ़िकेशन और ओपन रैन (आरएएन) पर काम करने का संकल्प व्यक्त किया है जो सिग्नल-प्रोसेसिंग का कार्य दोहराने के लिए सॉफ्टवेयर का उपयोग करता है।[8] चूंकि तानाशाही शासन 5जी से परे की उभरती प्रौद्योगिकियों के अनुसार कार्य करते हैं इसलिये यह प्रवृत्ति भविष्य में और बढ़ने की उम्मीद है।

5जी और साइबर ख़तरे

5जी के साइबर ख़तरे का परिदृश्य, चीनी दूरसंचार कम्पनियों के दबदबे और हार्डवेयर से पैदा हुए जोखिम से भी परे का है। हाल में बढ़े साइबर हमलों और शत्रु देशों तथा अन्य ख़तरों के पीछे मूल कारण (भू-राजनीतिक प्रतिद्वन्द्विता, वाणिज्यिक उद्देश्य और डाटा संचयन) अब भी

> **तीव्र गति और बढ़ी हुई क्षमता के कारण 5जी को स्थानीय नेटवर्क या उपकरण से इंटरनेट के जुड़ने के स्थान पर अधिक एक्सैस प्वाइंट और नेटवर्क किनारों (एज़िज़) की आवश्यकता होती है। इससे नेटवर्क के अहम कार्य, किनारों की ओर जाकर उपभोक्ता के अधिक क़रीब हो जाते हैं जिससे ज़रूरी सुरक्षा कर पाना और अधिक विश्वसनीय तीसरे पक्ष का वेंडर सुनिश्चित करना चुनौतीपूर्ण हो जाता है। यही परिस्थितियाँ, ख़तरा खड़ा करने वाले कारकों के लिए, हमले की सतह का विस्तार करती हैं। इसके अलावा, मिश्रित प्रकार के नेटवर्क - जैसे 5जी का 4जी जैसी पुरानी प्रणालियों के साथ काम करना भी 5जी नेटवर्क का, पिछली पीढ़ी के नेटवर्क की कमज़ोरियों से सामना करवा देते हैं।**

विद्यमान हैं। इसलिए वे 5जी नेटवर्क के लिए भी ख़तरा पैदा करेंगे और इनमें महत्वपूर्ण राष्ट्रीय बुनियादी ढाँचे को निशाना बनाने की बढ़ती प्रवृत्ति है। राष्ट्रीय विकास और आर्थिक विकास में 5जी की सम्भावित भूमिका को देखते हुए इसे निःसंदेह एक महत्वपूर्ण बुनियादी ढाँचा माना जा सकता है। इसलिए 5जी संचार नेटवर्क, तोड़फोड़ सहित साइबर हमलों का एक अहम निशाना होगा।

ऐसा करते समय, ख़तरा पैदा करने वाले 5जी नेटवर्क और इसके तंत्र (इकोसिस्टम) की कई कमज़ोरियों (वलनरएबिलिटी) फ़ायदा उठाएंगे। प्रौद्योगिकी की जटिलता के कारण 5जी के तंत्र में कई ऐसे गतिशील हिस्से हैं जो इन हिस्सों में से प्रत्येक के लचीलेपन को लेकर अनिश्चितता बढ़ाता है। यही अनिश्चितता, इस ख़तरे का परिदृश्य नाटकीय रूप से बढ़ा देती है। उदाहरण के लिए, यदि नेटवर्क के कुछ सिस्टम्स में पूरी तरह से सुधार नहीं किए गये तो यह साइबर सुरक्षा में सबसे कमज़ोर कड़ी हो सकते हैं। इसलिए 5जी के कनेक्शन, उपकरणों और अनुप्रयोगों (एप्लीकेशंस) की सुरक्षा पर अधिक ध्यान देने की आवश्यकता होगी।[9]

तीव्र गति और बढ़ी हुई क्षमता के कारण 5जी को स्थानीय नेटवर्क या उपकरण से इंटरनेट के जुड़ने के स्थान पर अधिक

एक्सेस प्वाइंट और नेटवर्क किनारों (एज़िज़) की आवश्यकता होती है।[10] इससे नेटवर्क के अहम कार्य, किनारों की ओर जाकर उपयोक्ता के अधिक क़रीब हो जाते हैं जिससे ज़रूरी सुरक्षा कर पाना और अधिक विश्वसनीय तीसरे पक्ष का वेंडर सुनिश्चित करना चुनौतीपूर्ण हो जाता है। यही परिस्थितियाँ, ख़तरा खड़ा करने वाले कारकों के लिए, हमले की सतह का विस्तार करती हैं। इसके अलावा, मिश्रित प्रकार के नेटवर्क - जैसे 5जी का 4जी जैसी पुरानी प्रणालियों के साथ काम करना भी 5जी नेटवर्क का, पिछली पीढ़ी के नेटवर्क की कमज़ोरियों से सामना करवा देते हैं।[11]

इसके अलावा जैसा पहले उल्लेख किया गया है, 5जी नेटवर्क आईओटी-सक्षम उपकरणों का व्यापक प्रसार करेगा। एक अनुमान के अनुसार 2025 तक, लगभग 27 अरब कनेक्टेड आईओटी-उपकरण होंगे। इससे ख़तरा कई गुना बढ़ जाता है क्योंकि इन उपकरणों के साथ नया मालवेयर और बॉटनेट भी होगा। यह अपने साथ डिस्ट्रिब्युटिड डिनायल-ऑफ़-सर्विस या मैन-इन-द-मिडिल जैसे हमलों की अधिक आशंका पैदा करेंगे। ऐसी घटनाएं पहले हो चुकी हैं। जैसे 2016 में, मिराई बॉटनेट ने हज़ारों राउटर, सुरक्षा कैमरों और डिजिटल वीडियो रिकॉर्डर के कामकाज में बाधा डालने के लिए असुरक्षित आईओटी-उपकरणों की कमियों का फ़ायदा उठाया।[13]

5जी के संदर्भ में एक और महत्वपूर्ण आयाम गोपनीयता का जोखिम है। 4जी की तुलना में, 5जी पर चलने वाले नेटवर्क का कवरेज क्षेत्र बहुत छोटा होता है। इसलिए इन्हें कई छोटे एंटिना और बेस-स्टेशनों की ज़रूरत पड़ती है। यह मोबाइल फ़ोन या अन्दर और बाहर इंटरनेट उपयोक्ता की सटीक लोकेशन ट्रैक करवा सकता है जिससे उनकी निजता भंग हो सकती है।[14] यही नहीं, 5जी को पिछली पीढ़ी के प्रोटोकॉल से भेद्यता विरासत में मिली है यानी ख़तरा पैदा करने वाले कारक, अंतरराष्ट्रीय मोबाइल सब्सक्राइबर पहचान (IMSI) अर्थात् मोबाइल नेटवर्क पर ग्राहकों की पहचान करने और प्रमाणित करने में उपयोग होने वाला नम्बर पकड़ सकते हैं। आईएमएसआई को अपने कब्ज़े में करके ख़तरे के कारक, किसी व्यक्तिगत उपयोक्ता की गतिविधि पर नज़र रखने के लिए क्षेत्र विशेष में ट्रैकिंग लोकेशन और कॉल इंटरसेप्ट सहित मोबाइल ट्रैफ़िक रोक सकते हैं।

साइबर सुरक्षा की यह चुनौतियाँ और गोपनीयता जोखिम केवल 5जी तक ही सीमित नहीं रहेंगे। भले ही 5जी नेटवर्क का धीरे-धीरे दुनिया भर में प्रसार हो रहा है लेकिन प्रौद्योगिकी की अग्रणी कम्पनियों ने पहले ही अगली पीढ़ी की प्रौद्योगिकियों पर काम करना शुरू कर दिया है। उदाहरण के लिए, क्वाड देशों ने अंतरिक्ष-आधारित 6जी पर सहयोग की योजना घोषित की है ताकि प्रौद्योगिकी के आकार लेने के साथ ही डिज़ाइन-आधारित सुरक्षा और साइबर सुरक्षा कार्यप्रणालियों को शामिल करना सुनिश्चित किया जा सके।[15] उधर चीन भी 6जी प्रौद्योगिकियों के बारे में उन्नत अनुसंधान और नवाचार की योजना तैयार कर रहा है।[16]

निष्कर्ष

संक्षेप में, 5जी डिजिटलीकरण और विकास के नये अवसर प्रदान करता है, लेकिन प्रौद्योगिकी और नेटवर्क डिज़ाइन सुरक्षित नहीं हैं। इसलिए, भारत जैसे जो देश 5जी अपना रहे हैं उनके पास एक साइबर लचीली योजना पहले से तैयार होना आवश्यक है। बहुत कुछ इकोसिस्टम के विभिन्न तत्वों की साइबर और सूचना-सुरक्षा नीतियों पर निर्भर करता है। 5जी नेटवर्क से जुड़ने वाले संगठनों को उभरते ख़तरों की जानकारी होनी चाहिए और उनके अनुसार सुरक्षा प्रोटोकॉल अपनाने चाहिए, अपने लिये ख़तरे की स्थिति निर्धारित करनी चाहिए, और अपना डिजिटल बुनियादी ढाँचा सुरक्षित करना चाहिए। इसके लिए लगातार अपडेट और अपग्रेड करने की आवश्यकता होगी क्योंकि ख़तरा पैदा करने वाले कारक, उभरती कमज़ोरियों का फ़ायदा उठाना जारी रखते हैं। इस लचीलेपन में, अंतिम उपयोक्ताओं की जागरुकता भी एक महत्वपूर्ण तत्व होगी। उनकी साइबर हाइजीन-साइबर स्पेस की सुरक्षित प्रथाओं की उनकी समझ - उन्हें ख़तरों से बेहतर ढंग से निपटने और अपनी रक्षा करने में मदद कर सकती है। ❑

संदर्भ

1. इंटैल, "Top Use Cases विथ 5जी Technology", https%//www.intel.com/content/www/us/en/wireless&network/5g&use&-cases&applications.html

2. आईएचएस मर्किट, "The 5th Economy," नवम्बर 2019, https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/the_ihs_5g_economy_-_2019.pdf
3. आँद्रेआस कुएह्ल और तृषा राय, "This Connection is Secure% A 5th Risk and Resilience Framework for The QUAD," Observer Research Foundation, December 1, 2021, https://www.orfonline.org/research/a-5g-risk-and-resilience-framework-for-the-quad/
4. समीर पाटिल और किशिका महाजन, "Expanding Chinese cyber&espionage threat against India," Observer Research Foundation, April 18, 2022, https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india/
5. फ़ैडेरल कम्युनिकेशंस कमीशन, "FCC Designates Huawei and ZTE as National Security Threats,' June 30, 2020, https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats
6. ब्यूरो ऑफ़ इन्डस्ट्री एंड सिक्योरिटी, यूएस डिपार्टमेंट ऑफ़ कॉमर्स, 'Supplement No. 4 to Part 744 of the Export Administration Regulations,' https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file
7. समीर पाटिल, 'Tech collaboration between democracies, ऑब्ज़र्वर रीसर्च फाउण्डेशन, सितम्बर 15, 2022, https://www.orfonline.org/expert-speak/tech-collaboration-between-democracies/
8. द व्हाइट हाउस, 'Quad Joint Leaders' Statement', मई 24, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/
9. टॉम व्हीलर और डेविड सिम्पसन, 'Why 5th requires new approaches to cybersecurity', ब्रुकिंग्ज़, सितम्बर 3, 2019, https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/
10. राज शिवराजू, 'Cybersecurity challenges that could potentially arise in the 5th era', फ़ाइनैन्शियल एक्सप्रेस, नवम्बर 26, 2022, https://www.financialexpress.com/education-2/cybersecurity-5g-technology-challenges-of-5g-internet-of-things-education/2892243/
11. कुएह्ल और राय, 'This connection is secure'
12. मोहम्मद हसन, 'State of IoT 2022% Number of connected IoT devices growing 18% to 14.4 billion globally', आईओटी एनालिटिक्स, मई 18, 2022, https://iot-analytics.com/number-connected-iot-devices/
13. जॉश फ्रुह्लिंगर, 'The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet', सीएसओ, मार्च 9, 2018, https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
14. नोकिया, 'Privacy challenges and security solutions for 5th networks', https://www.nokia.com/thought-leadership/articles/privacy-challenges-security-solutions-5g-networks/
15. एशियन न्यूज़ इंटरनेशनल, 'Quad Countries to Focus on Tackling China Threat In Telecom, 6G Technology', एनडीटीवी, फ़रवरी 3, 2023, https://www.ndtv.com/world-news/quad-countries-to-focus-on-tackling-china-threat-in-telecom-6g-technology-3749668
16. ग्लोबल टाइम्स, 'China to formulate 6G industry development plan, seek breakthroughs', ग्लोबल टाइम्स, मार्च 1, 2023, https://www.globaltimes.cn/page/202303/1286460.shtml

प्रकाशन विभाग के विक्रय केंद्र

नई दिल्ली	पुस्तक दीर्घा, सूचना भवन, सीजीओ कॉम्प्लेक्स, लोधी रोड	110003	011-24367260
नवी मुंबई	701, सी- विंग, सातवीं मंज़िल, केंद्रीय सदन, बेलापुर	400614	022-27570686
कोलकाता	8, एस्प्लेंडेड ईस्ट	700069	033-22488030
चेन्नई	'ए' विंग, राजाजी भवन, बसंत नगर	600090	044-24917673
तिरुवनंतपुरम	प्रेस रोड, नयी गवर्नमेंट प्रेस के निकट	695001	0471-2330650
हैदराबाद	कमरा सं. 204, दूसरा तल, सीजीओ टावर, कवाड़ीगुड़ा, सिकंदराबाद	500080	040-27535383
बेंगलुरु	फर्स्ट फ्लोर, 'एफ' विंग, केंद्रीय सदन, कोरामंगला	560034	080-25537244
पटना	बिहार राज्य कोऑपरेटिव बैंक भवन, अशोक राजपथ	800004	0612-2675823
लखनऊ	हॉल सं-1, दूसरा तल, केंद्रीय भवन, क्षेत्र-एच, अलीगंज	226024	0522-2325455
अहमदाबाद	4-सी, नेप्चून टॉवर, चौथी मंज़िल, नेहरू ब्रिज कॉर्नर, आश्रम रोड	380009	079-26588669