The 5G Era: Progress and Data Security Need to Exist Together

(By - Lt. Gen. Dr. S. P. Kochhar, Director General, COAI)

India is at the cusp of a digital revolution that has the potential to radically transform our daily lives. The revolution will be powered by 5G and simply put, would involve the transmission of large amounts of data over high speeds. How would this impact our lives?

Imagine a world where driverless cars are a reality. A post-pandemic world where doctors monitor your health remotely. Imagine AI-enabled drones monitoring agricultural land, construction sites, defense areas, and generating reports in real-time. All this would be enabled through 5G communication.

5G will push us into a world of interconnected networks, devices, and applications where each activity would become a potential attack vector. It will give a strong impetus to new technologies like Internet of Things (IoT), Augmented Reality (AR), Virtual Reality (VR), Artificial Intelligence (AI), etc. These new technologies involve the transfer and exchange of large amounts of data. This could translate into security challenges if data gets intercepted by people with dubious intentions. In short, 5G will escalate our vulnerability to security breaches with its attributes of edge computing, dynamic bandwidth sharing, among others.

Earlier, cyber-hygiene was possible because preceding networks were hub-and-spoke designs in which everything came down to hardware choke points that could inspect possible threats. However, 5G will push this outward to a web of digital routers spread throughout the network. What was possible before via physical appliances will now be virtualized to perform software higher-level network functions. Moreover, the network would also be managed by AI-software that could itself be vulnerable and may give the attacker an unsolicited control over the network.

The dynamic nature of 5G would expand the potential source points for cyber threat. Low-cost, short range, small-cell antennas deployed throughout urban areas will become the new hard targets. These cell sites will use 5G's Dynamic Spectrum Sharing capability in which multiple streams of information share the bandwidth in so-called "slices" with each slice embedding its own varying degree of cyber risk. Such dynamic shift in the functions of the network requires also dynamic cyber protection solutions rather than constant reliance on a uniform lowest common denominator solution.

5G will usher a hyper-connected world by connecting billions of IoT inclusive hackable smart devices. The used cases of IoT can be found everywhere, from public safety to battlefield, from healthcare to transportation – all of which are immensely vulnerable. With so many participants, each dependent on the other, a robust and reliable security infrastructure is a must. Consumers, organizations, and cities across the country seeking to use 5G, at present, are ill-equipped to handle its subsequent potential cyber threats. The present cybersecurity principles lay the burden on each user. Hence, targeted government interventions post extensive review and comparison of current security standards with 5G cyber risk factors is important.

Industry stakeholders must be encouraged to share cyber risks identified internally. This information could be a great asset in developing a strong collective defence. Telecom Service Providers (TSPs) today operate in isolation in an economic environment that goes against investments which do not contribute to profit. Hence, protective actions on cybersecurity undertaken by one TSP could be undermined without the contribution of other TSPs towards the same. Therefore, the sentiment of cyber accountability must be stirred with the combination of proper market-based incentives and apt regulatory oversight.

Customers fail to link their purchasing decision to a potential cyber risk outcome. This is because TSPs and application vendors have failed to publicise meaningful security indicators. We understand that the pace at which deployment is happening is important but without a good targeting solution, it can be disastrous. Hence, companies must now embrace and be held accountable for a new cyber regime. Chronic underinvestment in cyber risk reduction should be reversed, AI and machine learning should be employed towards data protection. A proactive shift to leading indicators of cyber-preparedness should be made. Best of class practices to identify, protect, detect, respond, and recover from cyber threats must be adapted.

Government must establish a new cyber regulatory archetype to reflect the new realities of time. Adversarial relationship between the regulators and the regulated must now be reversed to give way to effective cyber relationships. Companies that embrace their cyber responsibilities should not be penalized by those that fail to step up. Consumer transparency should be promoted. Assessment and certification of connected devices for security should be done.

Moreover, international bodies should be re-engaged. An informed third-party oversight, early in the 5G industry's design and deployment cycle, is vital to prioritize cyber security. In addition to this, there should be no compromise in adhering to the globally harmonized security standards developed by 3GPP standardization body for 5G.

5G is critical for India to take strides into the future and to be competitive in the global arena. However, to make this a reality what is also important is digital literacy and an increased consciousness towards data security. Building a scientific temper and developing an understanding of revolutionary technologies like 5G can truly make our country a global digital powerhouse.