Virtual SIM: RSTV – In Depth

Anchor: Teena Jha

Larger Background:

- The Pulwama terror attack that claimed the lives of 44 CRPF personnel on February 14th, 2019 was coordinated through virtual SIM's or virtual phone numbers.
- Officials investigating the case have revealed that the suicide bomber, Adil Dar, was in constant touch with Jaish-e-Mohammad handlers in Pakistan through a virtual SIM number.
- The user gets a virtual SIM by downloading an application of the service provider on his smartphone. He gets a number from the service provider after getting a verification code.
- Mobile numbers of the virtual SIMs used by terrorists who carried out the Pulwama attack were prefixed by +1, the area code of the United States, which means that the virtual SIM was generated by a service provider in America.
- India will now send a request to the US, seeking details of the service provider of virtual SIMs who perpetrated the February 14th attack.
- In addition, details on who activated the virtual SIM and Internet Protocol addresses will also be sought.
- In this edition of In-Depth, we will understand what a virtual SIM is? How does the technology work? How did terrorists of the JeM get access to virtual SIMs and how it helped them to avoid being tracked.

Analysis:

- The probe into the Pulwama terror attack has revealed that the terrorist used advanced communication technology to stay in touch with each other during the planning as well as the execution of the attack.
- Pulwama bomber Adil Dar and his handlers across the border, communicated with each other using virtual SIM cards.
- India is now seeking details of the service provider from the United States of America so as to ascertain the identity of the terrorists who were involved in the attack.
- The Pulwama attack was one of the deadliest attacks on security forces in Jammu and Kashmir- in which 44 CRPF personnel were martyred, and several injured as an explosive laden SUV, rammed into a convoy.
- The probe has now revealed that the suicide bomber, Adil Dar, and his Pakistani based handlers, belonging to the Jaish-e-Mohammad, were in constant touch with each other, making use of a new technology, called the 'Virtual SIM'. Dar was also in touch with the mastermind of the attack, Mudassir Khan, using the virtual SIM.
- Khan was killed in an encounter in Tral, following the Pulwama attack. The probe has also revealed that the virtual SIM used in the Pulwama attack was generated by a service provider in the United States of America.
- It becomes very difficult for the intelligence agencies in India to stop anything of this nature- because it is being conducted on a virtual SIM. This becomes a security challenge.

A Look at a few Specifics:

- The usage of virtual SIM's are a fairly new approach by the terrorists across the border to stay in touch. With a virtual SIM connection, one does not need a local registered SIM card, to get an active mobile connection.
- In this technology, the computer generates a phone number and the user downloads an application of the service provider on their smartphone. The number is linked to social networking sites like

WhatsApp, Facebook, Telegram or Twitter.

- The verification code generated by these networking sites, is received on the smartphone and the user is all set to use the phone.
- The officials said that the numbers used were pre-fixed with '+1'.
- It is important to note that '+1' is the **Mobile Station International Subscriber Directory Number** (MSISDN), used for the United States of America.
- The Pulwama attack was a very sophisticated attack. It was an attack that required a very high degree of coordination and precision. There were other people also involved in the chain who gave information as far as the movement of the convoy is concerned.
- Thus, there would be more than one virtual SIM card along this entire chain. These people would have been passing on information onto their central control agencies at the Jaish-e-Mohammad headquarters, in Pakistan.
- Security agencies are now tracking as to who would have paid the virtual SIM provider, and who activated it. However, there are chances that the terror groups used forged identities as was done in the 26/11 Mumbai terror strikes, which made use of a similar technology.
- During the Mumbai terror attacks probe, it was found that an amount of 229 USD, was wired to Callphonex via Western Union Money Transfer.
- The money was sent to activate **Voice-over-internet-protocol (VoIP)**, used during the terror strikes. The money was received from 'Madina Trading', located in Brescia in Italy.
- The Italian police concluded that the Brescia based company made several transfers using the identity of innocent, unsuspecting persons whose ID cards or passports, might have been stolen.
- Virtual SIM's offer a variety of conveniences for the user. With the help of service providers, security agencies can also access them to know who made the calls.
- Virtual services came into vogue in the mid 1990's, as a way to combat long-distance phone charges. **The main difference between a virtual SIM and a conventional SIM card is that all features and contents are downloaded directly to the phone into an App, instead of a physical SIM card.**
- In other words, a virtual SIM is the technology that replaces traditional plastic SIM cards, and integrates its operation in the mobile device.
- It is an e-SIM that involves a dummy SIM card that does not have a fixed number.
- The e-SIM is purchased online and a new number is tied to it.
- This new number functions like a regular phone number, operating out of a conventional SIM card, without the need of an internet connection to place calls.
- In the same way, when a number needs to be changed, it can be replaced by attaching a new number, to the same SIM.
- The use of such a service would entail using the mobile network of an e-SIM provider, and using a phone without additional security or encryption.
- This also means that while users might not be able to access someone's encrypted phone records, the service provider will have a database of all calls, messages, and other forms of activity from a virtual SIM.
- This helps security agencies as well. For instance, in order to locate a terrorist, who used a virtual SIM, security agencies need to only approach the service provider, who gave the terrorist the number. The service provider can then dig out from his server, information about the buyers, and the associated IP addresses.

Advantages of a Virtual SIM card:

There are some very obvious advantages of a virtual SIM card. These are:

- They are friendly with the environment, since it does not need plastic.
- It also does not suffer wear or deterioration during use.
- It improves security as thieves can't extract the SIM.
- It also means saving space on the devices, by not having to reserve a space.
- Device manufacturers also do not have to accommodate a SIM card slot in their phones. This gives

them more flexibility in terms of design.
- The virtual SIM card can be embedded into the device’s internal hardware which can lead to thinner phones, and probably more efficient batteries.
- Virtual SIM cards allow instant change of a service provider operator as well. It would be enough to scan a QR code, provided by the operator, and have the virtual SIM configured.
- One needs to simply activate the e-SIM on the desired device and one is ready to go.

A Note on SIM Cards:

- SIM cards are essentially the brain of your phone. It helps keep you in touch with telecom service providers.
- They store information required for user authentication in a mobile device.
- The first SIM card was developed in 1991. The first SIM card was about the size of a credit card. Since then, there have been several updates, making these SIM cards smaller and smaller. However, the purpose of the SIM has not changed by any of the technological evolutions. SIM’s have always been and will always be a way for people to have a secure method of accessing a phone company network.
- A subscriber identity module or a subscriber identification module, widely known as a SIM card, is an integrated circuit that securely stores the International Mobile Subscriber Identity or the IMSI number and its related key. These are used to identify and authenticate subscribers on mobile telephony devices like mobile phones and computers.
- A SIM card contains its Unique Serial Number or ICCID, International Mobile Subscriber Identity Number (IMSI) number, security authentication, a list of the services the user has access to, a Personal Identification Number (PIN), and a Personal Unblocking Code (PUC) for PIN unlocking. It is also possible to store contact information on several SIM cards.
- SIM cards are used on GSM and CDMA phones. They can also be used in satellite phones, smart watches, computers and cameras. SIM cards in the form of full, mini, micro and nano are still prevalent. But, in a world that is increasingly digital and virtual, the use of embedded SIM’s or e-SIM’s and virtual SIM’s are starting to gather pace.

Some More Characteristics of Virtual SIM Cards:

- Virtual SIM cards are not attached to a mobile phone and are created online to help in communication.
- It is a cloud-based number that can be used from any device via an App.
- To use this, customers sign up for a service by installing an App on their mobile phones.
- This App generates a phone number without linking it to a physical SIM and syncs it with an email account or a social network. The App also lets users link multiple numbers with a single account.

e-SIM Cards:

- e-SIM cards are those which are permanently embedded in devices which connects to the internet.
- They are integral to the device which means that they cannot be removed. The information on an e-SIM is rewritable, meaning that the user can decide to change the operator with a simple phone call.
- One of the advantages of the e-SIM technology is that it makes it much easier to switch telecom service providers. e-SIM is a global specification by the GSMA, which enables remote SIM provisioning of any mobile device. Remote provisioning is the ability to remotely change the SIM profile on a deployed SIM, without having to physically change the SIM itself.
- Apple recently introduced the Apple SIM which uses remote provisioning, rather than the traditional SIM card approach.

Soft SIM:

- A soft SIM is a collection of software applications and data that performs all of the functionalities of a SIM card.
- A soft SIM does not reside in any kind of secure data storage.
- The information is held in the memory and processor of the device. Many phone companies are against soft SIM’s, because they are perceived as more exposed to the question of hacking.