Centralised We Secure

With stand alone surveillance systems coming a cropper, India needs centralised monitoring solution to mitigate internal security threats

By Lalit K Chandak

The terrorist attack of 26/11 at Mumbai has exposed the chinks in India's internal security mechanism. It's a fact endorsed even by the Prime Minster Manmohan Singh. While speaking at the Chief Ministers conference on internal security recently he made a candid admission that the defence mechanism to thwart terror threats were inadequate and much more was needed to strengthen our set up for collection of technical signalling and human intelligence.

Communication plays an extremely vital role in national security as it is the first step to check or allow terrorists to plan their activities. In the last ten years, the telecommunications networks have grown hugely, both in wireless as well as data networks. Besides, number of service providers has also increased with opening of these sectors for new operators. However, at the same time, lawful monitoring has become extremely difficult and challenging.

Not a Fool-Proof Mechanism

Under the current Indian regulations, licensed telecom service providers (both wireline, wireless and datacom) are required to provide call content and call related information of a defined target over dedicated E1 links to law enforcing agencies (LEAs) working under various ministries—Prime Minister's Office (PMO), Defence, Home, Finance, and Communications.

In case the target is a data service subscriber or user then the service provider is required to deliver all the target related communication—e-mail, instant messaging, VoIP, FAX, HTTP browsing—in a format which is identical to the way the target sees it.

Of late, anti-national elements are taking advantage of such widely available options to communicate globally. Co-ordinated converged and centralised monitoring of such misuses of communication options is proving to be a technical nightmare for the security agencies.

This has led to dispersed nature of various 'proprietary' lawful monitoring solutions currently deployed on India's multiple communication networks on the edge.

This has created a confusing situation where multiple Indian security agencies do not have coordinated view of any target's full communication activities. For example a VoIP call with egress on one operator's gateway and ingress on another operator's gateway—cannot be heard in sync and use of multiple modes of communication by a specific target (fixed line: TDM; wireless: GSM/CDMA; and IP: chat, email, VoIP) again are not easily co-related and deciphered in real time without involvement of multiple technologies, persons and agencies.

Cost Vs Commitment

Each telecom player has the freedom to procure its lawful monitoring

in compliance with TEC GRs and in turn secure approval of the procured equipment from the LEAs. For telecom or gateway operators, compliance to Lawful Interception and Monitoring Solutions (LIMS) is a cost as it does not generates revenue; though its a mandatory for getting license.

The tendency is to comply with the regulatory requirement at minimum cost. National security is not a driving motivation in such a purchase. Such a practice results in multi-vendor solutions being deployed among operators, some of which are not exacting in their compliance of national security requirements. What this means is that LEAs need to be conversant with each such LIMS offerings.

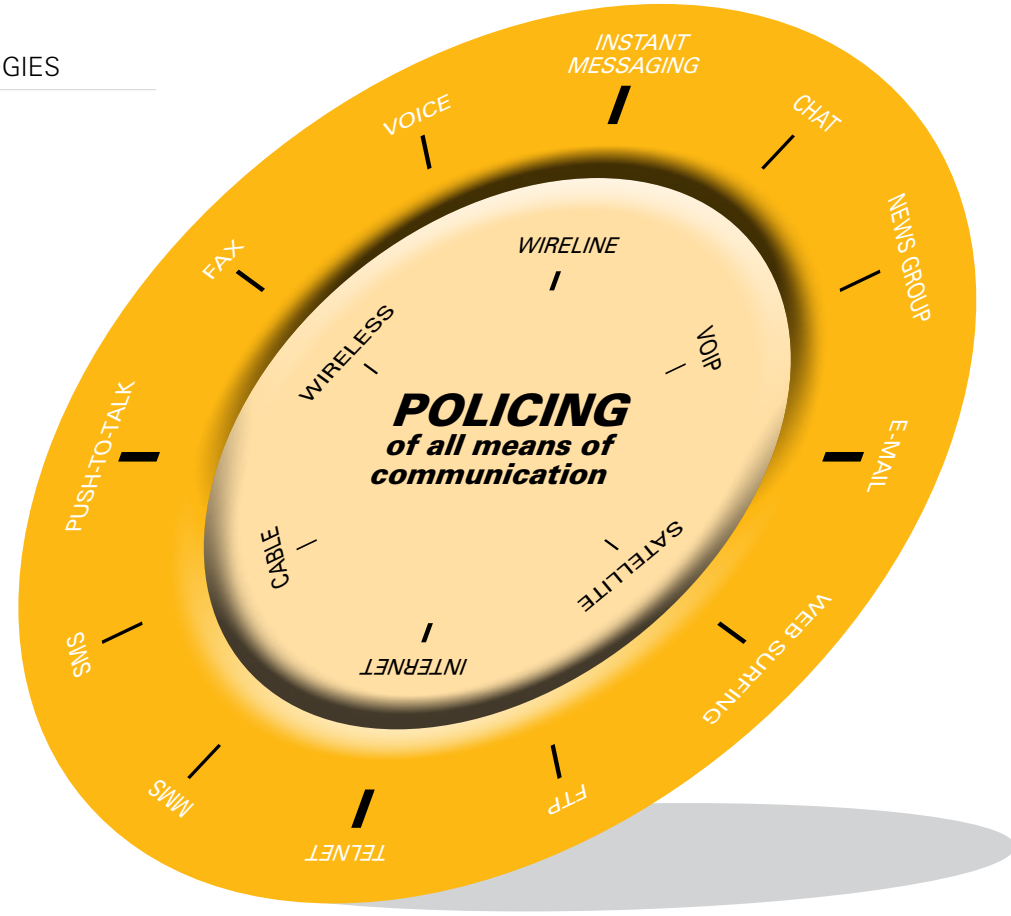
Moreover provisioning of the targets and delivery points of target related content and information is currently housed near the switch itself where the interception is taking place. This approach has two serious drawbacks. One, the concerned agency has to convey the targets to the carrier and two, provisioning of a target needs has to be done manually on each switch.

While the above sea of data is being gathered for lawful monitoring in India, each security agency is individually trying to make sense from all these different inputs flowing to them from various technology platforms.

In addition, under the current procedures, one LEA's targets and inputs collected from it are not known to the other LEAs. This results in lack of coordinated operation and working.

The impact of such a procurement process where multiple technology solutions get deployed in India by new emerging ILD and NLD operators has made the LEA's task of electronic surveillance of warranted targets even more difficult and complicated.

The most widely used medium—Internet remains almost unmonitored in such a situation. In view of large number of licensed ISPs, the lawful monitoring is difficult. Existing deployment of lawful monitoring solutions with ISPs are largely non-functional and where deployed—have become outdated as they have not grown with ever growing traffic requirements.



India needs to procure centralised Lawful Interception and Monitoring Solution, complete with a planned backup system and disaster recovery mechanism for a nation-wide deployment

In case of Internet, DoT has been accepting self-certification from ISPs for compliance to lawful monitoring by directing these operators to buy a C-DoT platform for this task. Unfortunately, the platform has not been tested against TEC GR for compliance to defined lawful monitoring requirements for ISPs.

Even ISPs that have deployed the C-DoT solution have not seen it in operation.

Centralising Lawful Monitoring

Policing of all means of communication (see flow chart) needs to be done at each state level through a centralised deployment of lawful monitoring.

The growing use of Internet Protocol (IP) for communications brings in a new dimension that has made the LEAs task even more complex today. Data from IP based services gets aggregated across "data pipes" of the world's Internet protocol networks and is deployed globally.

Even in India we have over 130 licensed ISPs working through four Indian international gateway operators. Additionally, there are various satellite based operator networks.

Unfortunately, these services, apparently anonymous to the non-technical user, are being increasingly

The Unification Advantage

- Single platform at national level (with redundant back-up) will facilitate the deployment of unified LIMS across multiple networks like wireline, wireless (GSM, CDMA and satellite) and IP networks to cover all means of communications.
- Such a system would provide the LEAs with the following functional advantages:
  - Provisioning and monitoring of targets can be done by each LEA from its own location (independent of the other LEAs) without having to involve the carrier.
  - Each LEA can target the same suspect with its own pre-defined parameters for monitoring of both TDM and IP and view data of both through one interfacing front-end.
  - New front-ends can be set up on an IP network without much difficulty.
- An IP based LIMS, makes it easier to gather and share information across the country with various security agencies with geographical location no longer proving to be a hindrance in such an activity.
- Such a LIMS network helps to effectively control illegal ILD calls across the country.
- It provides the means to fully audit service providers' payment of regulatory dues and thus prevents all kinds of revenue leakage.
- It prevents duplication of resources on multiple technology platforms with each service provider and makes better utilisation of national wealth.

deployed for the perpetration of organised crime including terrorism. For example, a net based voice or chat session being conducted by a terrorist as an Internet user becomes more difficult to reconstruct since his ingress and egress could be on two different gateways or satellite operators.

Fortunately, if targeted surveillance is applied comprehensively across the data or IP links of the world's networks, valuable information can be captured and reconstructed for use by LEAs.

Hence, it has now become necessary for the LEAs to think in terms of identical gigabit probes being placed with all Indian international gateway and satellite operators and such data being read into a centralised location for reconstruction and replay.

IP makes such working possible where geographical location no longer remains relevant. It also enables tapped data to be reconstructed and shared simultaneously with multiple security agencies across the country. In fact, Solutions using IP surviellance like "Directed Analysis" are available for LEAs to target and capture information of identified users.

Additionally, illegal ILD calls and under-reporting by some licensed telecommunication companies is causing a huge recurring loss annually to the country. Traffic running on international gateways, illegal calls and their downstream gateway locations across the country can easily be detected with a centralised converged TDM/IP based LIM solution. Savings on this account alone justifies a centralised deployment of LIM in India.

Setting up of a centralised and converged LIMS is thus the need of the hour largely in view of growing means of communication and in the interest of national security.

It has now become necessary that the responsibility for purchase of technology for LIMS should be moved from the ambit of each telecom and gateway operator to the control of LEAs where such purchase cost could still be met in some way by the licensed service provider.

The Indian government should now consider the procurement of such centralised LIM solution for nation-wide deployment with a planned back up system supported with a disaster recovery site.

Need For a Watch Dog

Since Lawful Monitoring requirements need to be defined for LEAs working under various ministries—PMO, Defence, Home, Finance and Communications—an Inter-Ministerial Group (IMG) needs to be setup to co-ordinate on all aspect of this critical national requirement.

A core technical group, with experts from public and private sectors, needs to be put together under this IMG and tasked with the responsibility of defining a national technical requirement which is implemented within a fixed time-frame with sub-centres at each state level.

Since this is a national security requirement, tender process of purchase should be avoided and instead a technology driven process of purchase should be defined which does not compromise on the technology needs. Funding for such a platform should be done based on fees collected from licensed operators.

As far as possible, Lawful Monitoring solutions currently deployed with various telecom operators should be integrated with the central platform. Sub-centres created at state level should also be integrated with the central platform. G

—The author is President, Span Technologies