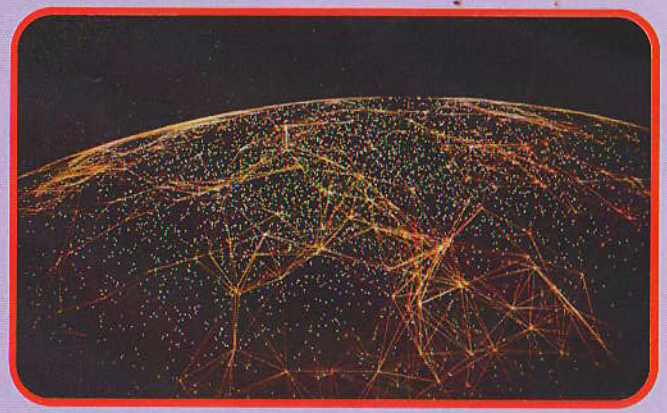

Anand Swaroop, IPS
Director,
Directorate of Coordination
Police Wireless (DCPW),
MHA, Block No.9, CGO Complex,
Lodhi Road, New Delhi – 110003
Ph: 011-24361561 Fax: 011-24369511
director@dcpw.gov.in
@DCPW_official

समन्वय निदेशालय पुलिस बेतार

DIRECTORATE OF COORDINATION POLICE WIRELESS

HEADS' OF PPDR CONFERENCE

20th & 21st January 2020, Vigyan Bhawan, New Delhi

Session on
Security Concerns of Radio, Satellite & Broadband Communication Equipment / Networks
– Hardware, Software, Firmware

1615 – 1745 Hrs, 20th Jan 2020

Organised by:
Directorate of Coordination Police Wireless
Ministry of Home Affairs
Government of India

Objective:-

PPDR (Public Protection & Disaster Relief) Organizations (viz. States / UTs Police, CAPFs, NDRF, SDRF, Fire, Hospitals, Local Administration and many others) need Robust, Reliable, Secure & Resilient Communication Networks for day-to-day effective & efficient Public Protection, Law Enforcement during Emergency situations and Management of Disaster Relief operations.

Security Concerns:-

Currently, most of the Police Communication Equipment like HF, VHF & UHF wireless sets, Satcom Terminals, VoIP Phones, Data Terminal Equipment etc. are imported. All Police Organizations have some concerns about security of Radio Communication Equipment and they have been trying to address them. There is an urgent need to address these security concerns for the benefit of all Central & State Police Organizations.

Even today, a large number of Police Organisations are using Analog Radios based on discrete components without encryption or low end encryption. The Police Forces are now inducting Digital Radios for Voice, Data and GPS Tracking into their communication systems. Most of the Digital Radios are IP based which can have Advanced Encryption Systems. Some information in the Data Packet like IP address etc. are not encrypted which can compromise security of the data passing over the network and makes it vulnerable to attacks.

The software loaded on to the microchips in Police Wireless Sets may contain malware which can breach network security. There is an urgent need to have a mechanism to check the critical components in the equipment for malware / bugs.

Department of Telecom has also expressed security concerns in view of the expansion of Telecom Services in India. DoT has included certain security conditions in all Telecom Licenses issued by them .

The licensees are expected to be completely and totally responsible for security of their Networks. They shall have organizational policy on security and security management of their networks including Network forensics, Network Hardening, Network penetration test, Risk assessment. Actions to fix problems and to prevent such problems from recurring should be part of the policy.

They are also expected to induct only those network elements into its telecom network, which have been got tested as per relevant contemporary Indian or International Security Standards e.g. IT and IT related elements against ISO/IEC 15408 standards, for Information Security Management System against ISO 27000 series Standards, Telecom and Telecom related elements against 3GPP security standards, 3GPP2 security standards etc and audit their network from security point of view once in a year as per applicable standards.

How to address these concerns :-

In order to ensure information security, cyber security, network security and end-to-end security, complete hardware & software details of equipment are required from OEM of the communication equipment. Since most of the OEMs are foreign companies, it becomes very difficult to get complete details from them. Hence, better control over OEMs is needed like US and UK etc. to compel OEMs to share details of the equipment.

STQC has recently setup common criteria testing lab to for evaluating the security functions or mechanisms of the IT products and certifying the same.

National Centre for Communications Security under Department of Telecommunication has setup Security Assurance Standards Facility at Bengaluru for the development of Indian Telecom Security Assurance Requirements (ITSAR) and Test Schedules and Test Procedures (TSTP) for all ICT equipment.

DCPW is also the central distribution authority for cipher documents to all police organizations in India. As per Crypto Policy of Government of India, for secret communication, the communication equipment must be tested and granted Grade 3 by SAG and the algorithms are to be developed by Government Organizations / PSUs only. Scientific Analysis Group (SAG) under DRDO provides security grading for equipment only and are yet to develop capabilities to do security grading of Communication Network.

DCPW has recently been assigned the task of monitoring of HF/VHF/UHF Terrestrial Police Radio Networks to prevent breach of Radio Communication Security and is required to enhance its capabilities in terms of equipment and human resources to fulfill the task.

However, there is no such dedicated facility for testing and certifying police communication equipment. Therefore, a need was felt by Ministry of Home Affairs (MHA) to have a centralized organization to test and certify communication equipment for procurement by police organizations. Testing of equipment may be required after repair also as there is a possibility of adding malware / bug at the time of repair. Accordingly, MHA has identified DCPW as an Inspection Agency for all CAPFs for testing electrical, radio and communication parameters of radio equipment. DCPW is upgrading its infrastructure and capabilities to meet the requirement for testing of equipment.

Challenges remaining:-

The ultimate aim is to achieve fool proof security for communication networks of police organizations towards which a lot of work is to be done.

Way Forward / Expected Outcome:-

Therefore, a session on **Security Concerns of Radio, Satellite & Broadband Communication Equipment / Networks – Hardware, Software, Firmware** is being held as part of the conference where experts from National Security Council, IIT Bombay, SAG, Central & State Police Organisations, STQC, PSUs and Industry will deliberate on the above security concerns that exist in the minds of police organizations.

A major expected outcome of this session is an outline to further promote development of indigenous encryption systems & encryption hardware for incorporation in Police Communication Equipment.