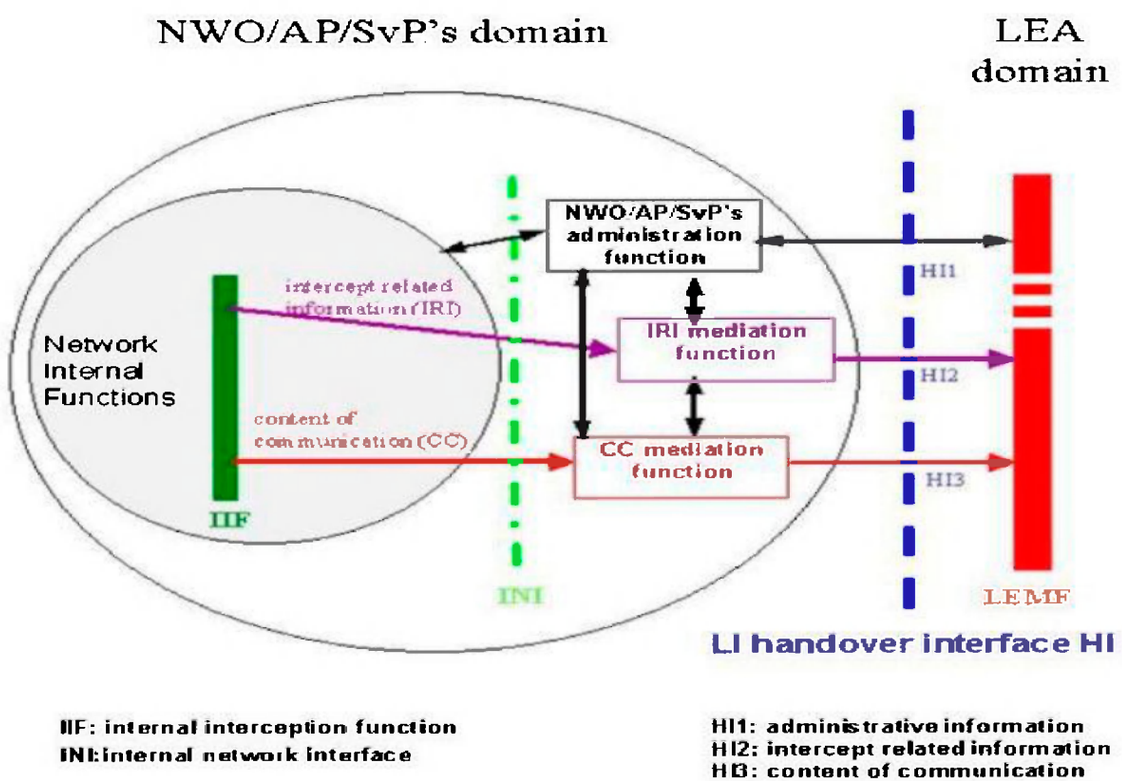
(S//SI//REL) Exploiting Foreign Lawful Intercept (LI) Roundtable

[redacted] S31122

(U) Definition

Lawful Intercept (LI) – obtaining communications network data by legal authority for analysis or evidence



(U) LI Standards

- CALEA (US)
- ETSI (European)
- SORM (Russian)
- Other

(TS//SI//REL) Countries of Interest

- Pakistan
- Afghanistan
- Iran
- Iraq
- Yemen
- Syria
- China
- Egypt
- Algeria
- Mexico
- Indonesia
- UAE
- Saudi Arabia
- Russia

(S//SI//REL) XKS Fingerprints (~60)

- Aqsacom
- ATIS
- Ericsson
- ETSI
- Huawei
- Motorola
- Nokia
- Siemens
- Trovicor
- Utimaco
- ZTE
- GENERIC

(U//FOUO) Access Methods

- FORNSAT
- Microwave (F6)
- Special Source Operations (SSO)
- Tailored Access Operations (TAO)

(S//SI//REL) Taplists

- Developing advanced analytics to determine patterns in numbers being tasked
- Creating database to store LI-related information
- Discovering informal tasking

(S//SI//REL) Mapping Networks

- Telecommunication and Internet Service Providers in a region
- LI vendors/service providers
- IP addresses/ports of usage
- Likely transmission medium

(S//SI//REL) Processing Solution

- KITTYBINGE
- TAO custom solutions
- STARPROC

(S//SI//REL) Types of LI

- Telecommunication
- Internet

- Differentiating between regular voice/Internet traffic from tasked traffic. Protocol indications?

(S//SI//REL) LI Pod

(S//SI//REL) LI Discussion Topics

- Discovery
- Access Methods
- Tapiist Analytics
- Corporate Database
- Corporate Processing Solution
- Other Issues/Roadblocks