ICCRTS – June 2005

Validation method of a telecommunications blackout attack

João Amado, Paulo Nunes

Academia Militar

"Shortly after Locke set the National Guard in motion, his office in Olympia received a call from a furious Secretary of State Madeleine Albright. Albright demanded demanded the governaror immediately to take action to release her from her hotel where she was trapped by the demonstrators". N30 Seatle

[Networks and Netwars, Arquilla]

…and if the Secretary of State couldn't even call ?

- *Could this hapen?*
- *Who could do it ?*
- *With what effort?*
- *Could this happen in Portugal?*

According with the *Gartner Group* and *United States Naval War College*

"…in order to achieve important damages would be necesary a a group with important resources including 200 milions of dolars and would request a planning of 5 years"

1. Scenario Analysis: characterization of the available services and networks in the target area;

2. Logical Target Selection: Identification of potential targets according to the perceived services value;

3. Target Information Upgrade: additional information in order to upgrade the target information;

4. Physical Target Selection: selection of the class of elements more vulnerable in the network;

5. Attack Simulation: use of software tools to model and simulate a network attack;

6. Virtual Attack Success Assessment: takes place after the simulation period and will allow the evaluation of the network attack effectiveness.

1. Scenario Analysis

- Voice over circuit switching network;
- Voice over packet switching network;
- Voice over mobile networks GSM/GPRS, UMTS;
- Data over circuit switching network;
- Data over packet switching network;
- Data over mobile networks GSM/GPRS, UMTS, WiFi, WiMax;
- TV – over microwaves;

2. Logical Target Selection

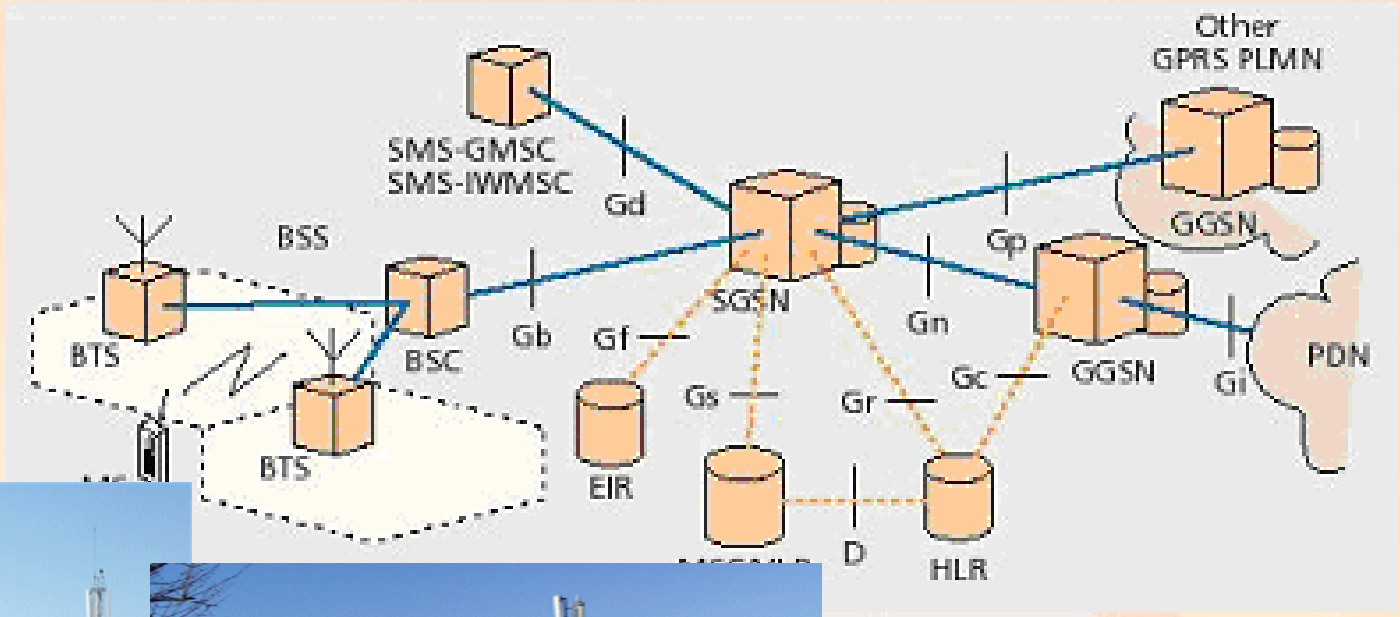
- Target selection based on less cost-benefit logic
- Backup systems awareness

Network	Operator	Service	Usage
GSM/GPRS	Optimus	Voice	Fare
		Data	Poor
	TMN	Voice	High
		Data	Average
	Vodafone	Voice	High
		Data	Fare

Backup for some services !

3. Target Information Upgrade

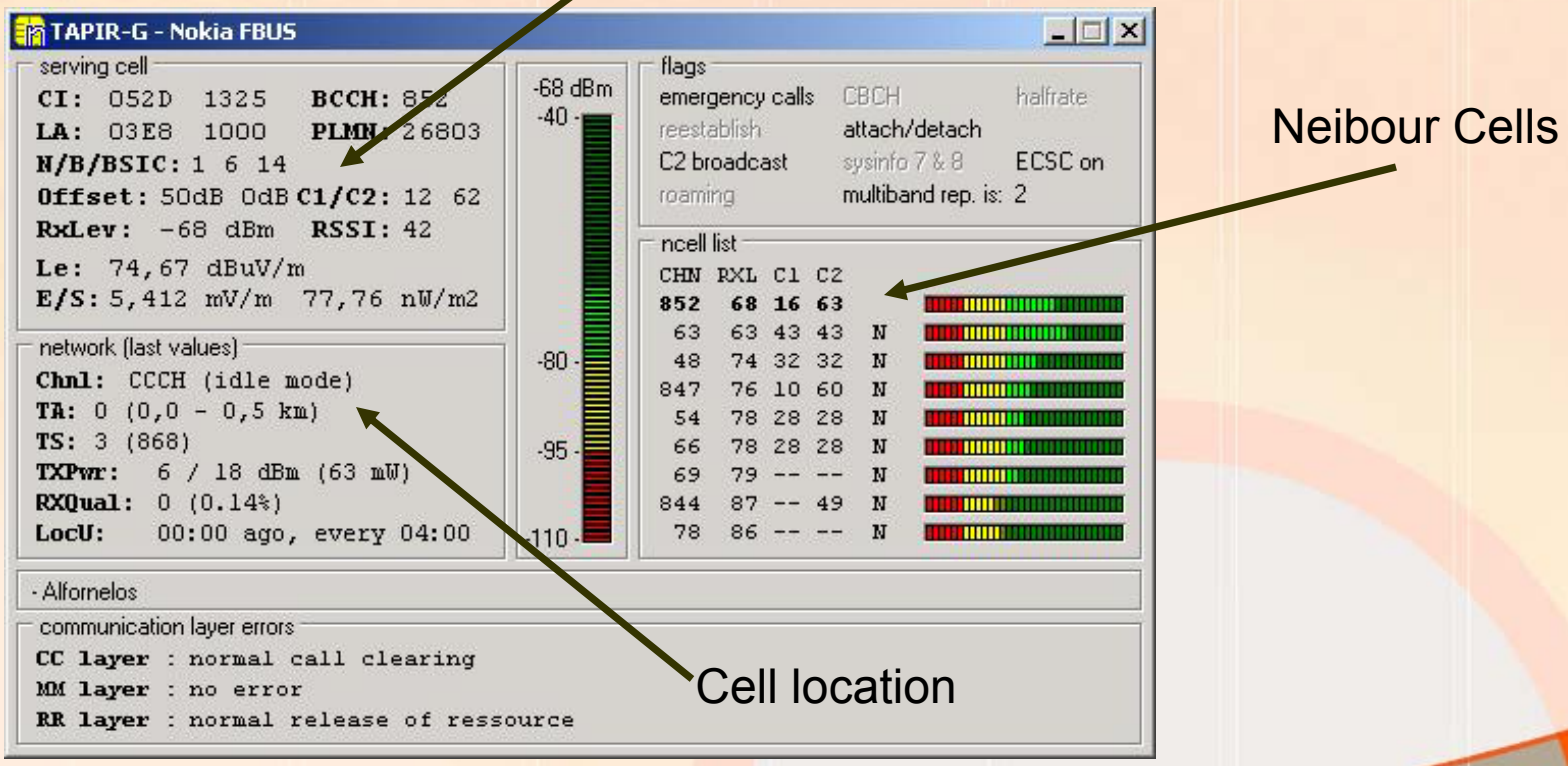
- *Collect aditional information*
- *Example for the GSM/GRPS network*



www.comsoc.org]

4. Physical Target Selection

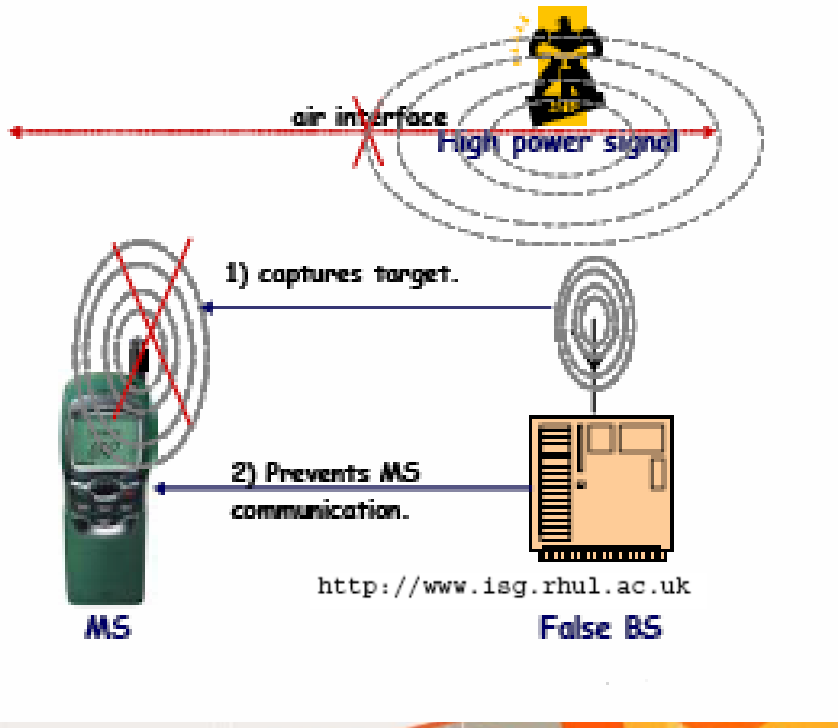
- *Example for the GSM/GPRS network - NetMonitor*



5. Attack Simulation

- Build the attack tools to implement the planend attack

- *Example for the GSM/GRPS network*
  - Deny of service interrupting the connection between Cells and the netwrok.
  - Deny of Service using a fake Base Station.



6. Virtual Attack Assessment of Success Target Information Upgrade

- onclude if it is possible to perform this type of attack;
- valuate the impact of the attack, showing for how many time it would be possible to disrupt the communications, and what would will have to be the necessary effort for the service restoration;
- valuate the amount of effort needed to prepare, coordinate and perform the attack;
- hat skills would be necessary the attacker to have in order to perform this type of attack.

- *What to do with the collected information?*
  - *Centralized Database with the relevant information of the telecomunications infraestructure, including the identifyed wick points, available to operators and security agencies.*
  - *Examples from other countries*
    - *ISAC – Information Sharing and Analysis Center (EUA)*
    - *CIIP – Critical Infraestructure Information Protection (Suécia)*