Panel discussion 24.2.2014

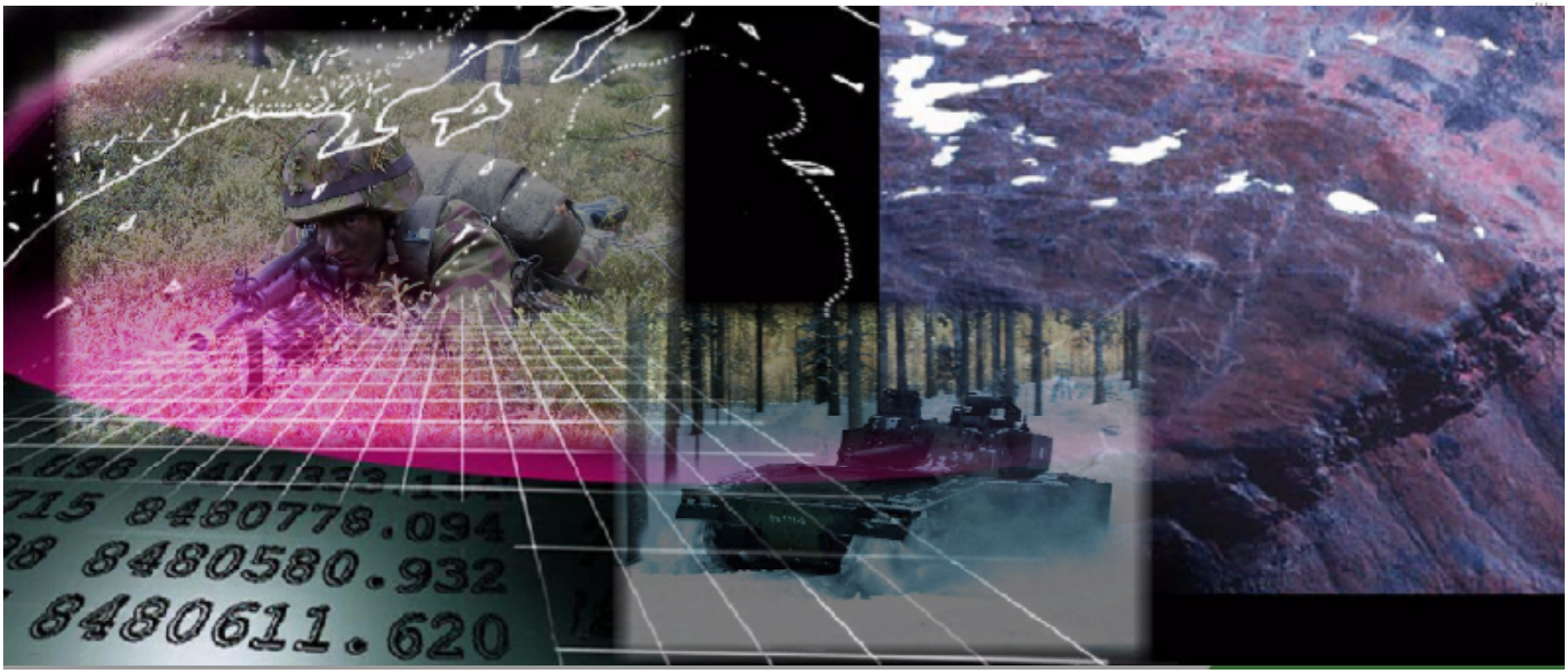
- Topic: **Threats and Challenges in Modern Communications**
- First presentations by panelists in designated order:

1. Julio Vivero, Spain
2. Tatsuya Yamazaki, Japan
3. Daniel Riviello, Italy
4. Tapio Saarelainen, Finland

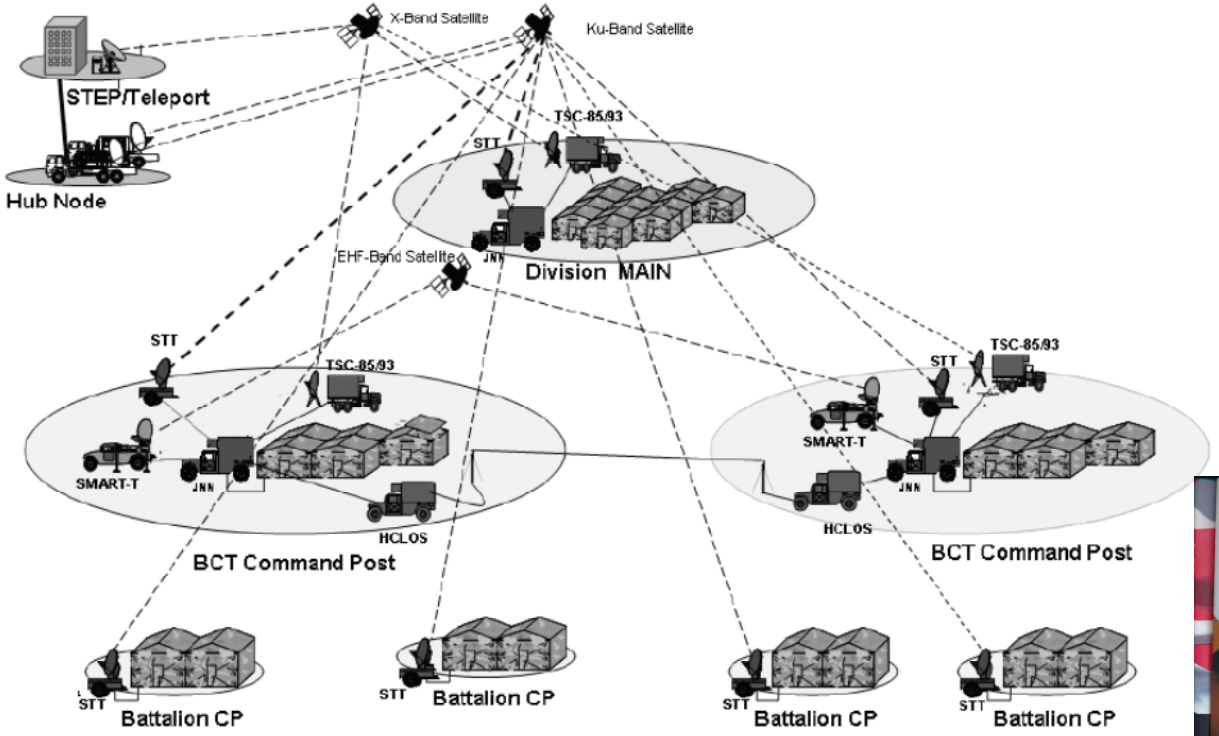
- Discussion
- Comments and questions from audience are warmly welcome

Threats and Challenges in Modern (MILITARY) Communications

Army Academy
Major Tapio Saarelainen, PhD



Communication systems and various networks in hostile battlespace



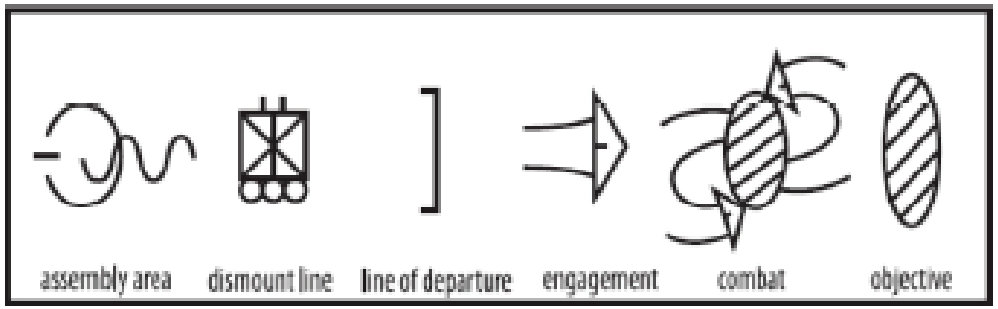
2. tou

Maasotakoulu

PUOLUSTUSVOIMAT | FÖRSVARSMAKTEN | THE FINNISH DEFENCE FORCES

Threats in military communications

1) Lack of energy
2) Lack of connectivity
3) Lack of bandwidth
4) Malicious software (malware)
5) Interruption caused by the enemy
6) Effect of war
    - Physical
    - Electrical
    - Electro-magnetic



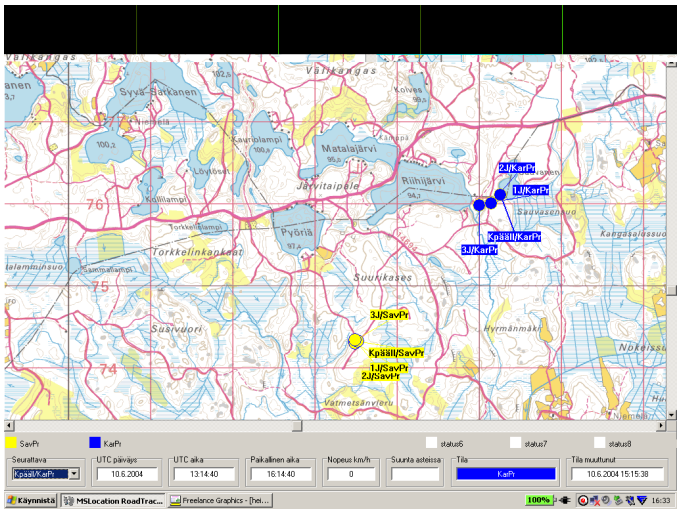
Challenges with wearable and ubiquitous technology

Interference, short-range

PUOLUSTUSVOIMAT | FÖRSVARSMAKTEN | THE FINNISH DEFENCE FORCES

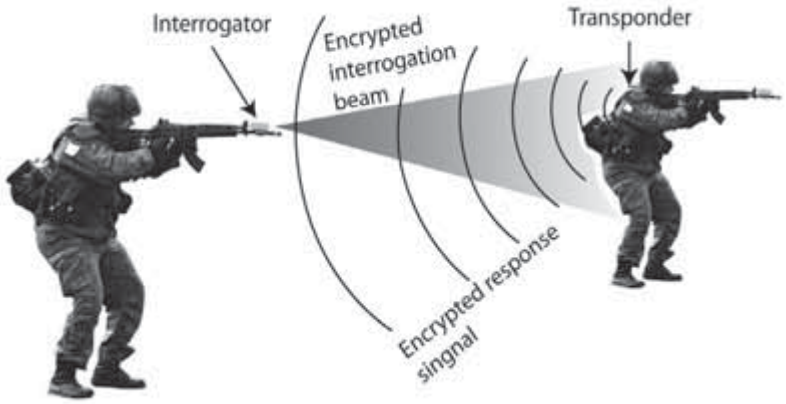
Challenges with modern military communication networks

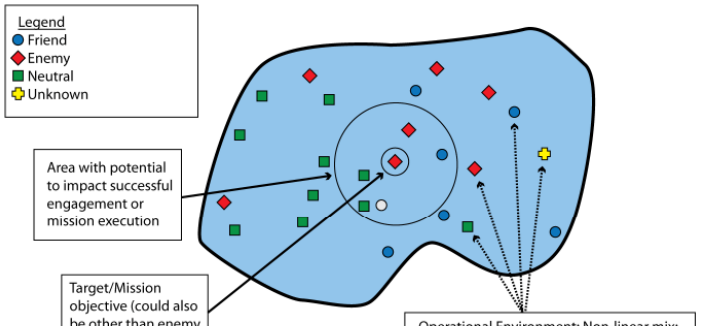
1. To update constantly and forward near real-time information from top to bottom and vice-versa (the other way around)
2. To maintain the ubiquitous networks and withstand enemy military actions and countermeasures



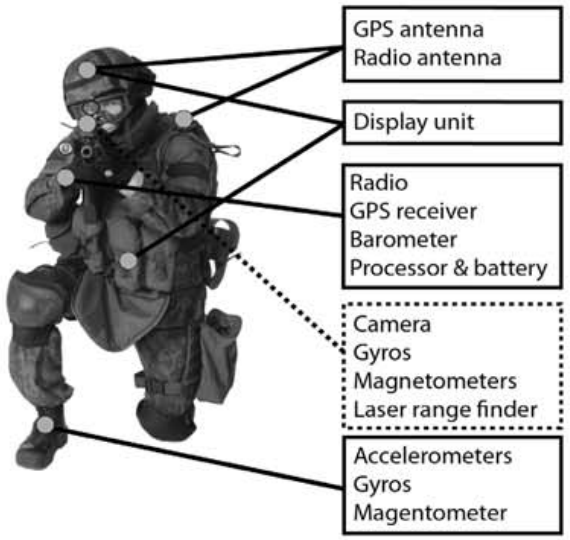
Challenge: Identification of Friend or Foe (IFF)

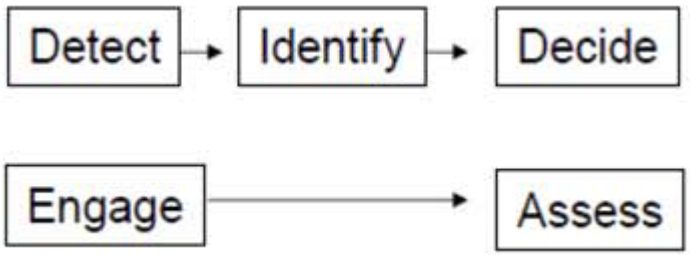
GOAL: To avoid fratricide and collateral damage





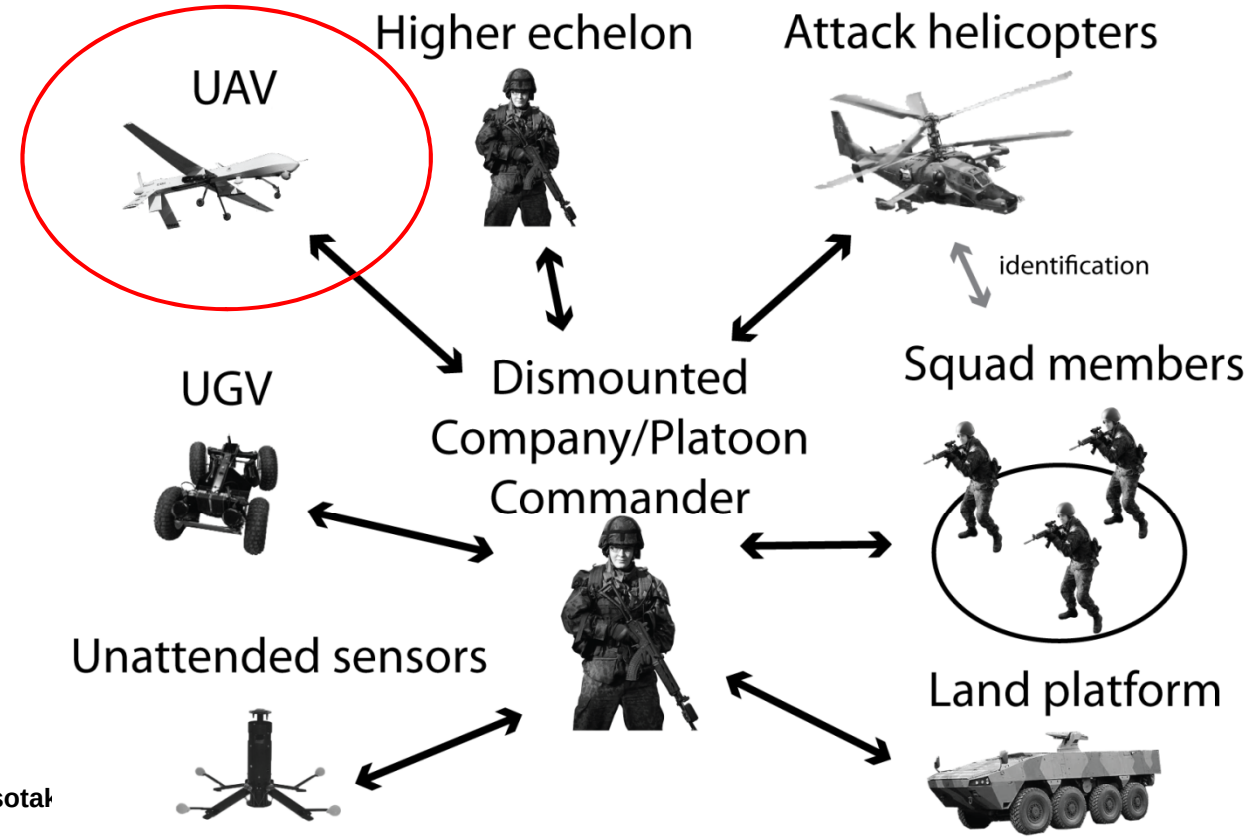
Objective: Maximize combat effectiveness and minimize fratricide/collateral damage. Missions are executed and/or weapons delivered against specific within the context of the other object/entities in the battlespace. This requires both SA and TI.





Challenge: To maintain and control sensor networks

Several types of networks with
various network nodes and freuencies
and topologies




GOAL: Operational performance


KIITOS

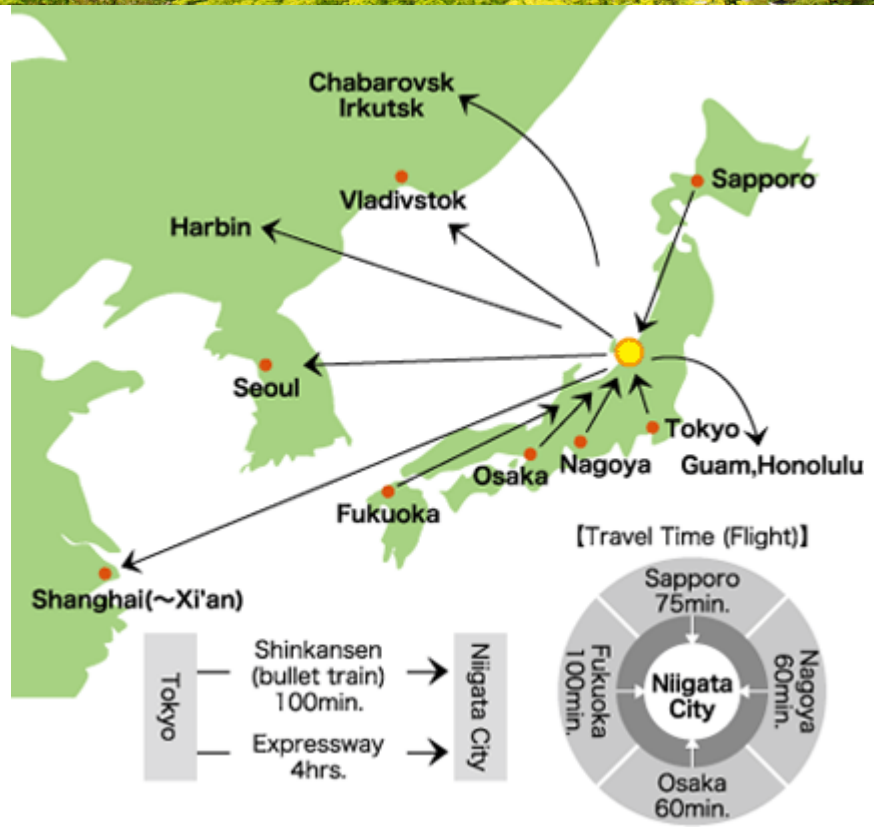
PANEL COMMUNICATIONS

Topic: Threats and Challenges in Modern Communications

Tatsuya Yamazaki, Niigata University, Japan

Self-introduction

Niigata University



National Institute of Information and Communications Technology (NICT)

7 months ago

Retrieved from NICT Web page

Threat by disasters

the Great East Japan earthquake

11 March, 2011

NICT activity for evacuees

NICT provided wireless Internet environment to more than 50 sites of the shelters and support centers damaged by the earthquakes, for supporting their recovery.

Cognitive Wireless Router (CWR) system

Reliable and stable broadband wireless access to Internet

New challenge

- After the earthquake, Japanese government decided to start development of resilient information and communications technology .
- It must contribute to building really robust cities against disaster.
- R&D of optical networks, knowledge processing as well as mobile, wireless and satellite networks are included.

Network Redundancy or Resilience?

- Designing a resilient network is more than just adding redundancy.
- Incorporating the level of redundancy is required to create a resilient network.
- Redundancy needs more cost. Who should meet the cost?
- Designing based on short-term and long-term perspectives is needed.

Threat in IoT

- "A fridge has been discovered sending out spam after a web attack managed to compromise smart gadgets."
- Recently, The news starting with the above sentence was reported.
- In the era of IoT (Internet of Things), it is said everything is connected and communicating.
- Considering the fact of the news, we should discuss *importance of disconnectivity* as well.

- Revenge Porn is a social problem.
- Legislation to punish the persons posting images is proceeding.
- The posted images are copied and scattered unceasingly.
- The idea of *the right to be forgotten* is now discussed.
- How to realize the mechanism to make the posted images forgotten.

SPACOMM2014

THREATS AND CHALLENGES IN MODERN COMMUNICATIONS

CODE: GMV-SPACOMM2014-PRE-002
FECHA: 24/02/2014
VERSIÓN: 1

Secure e-Solutions®
GMV SOLUCIONES GLOBALES INTERNET S.A.U.

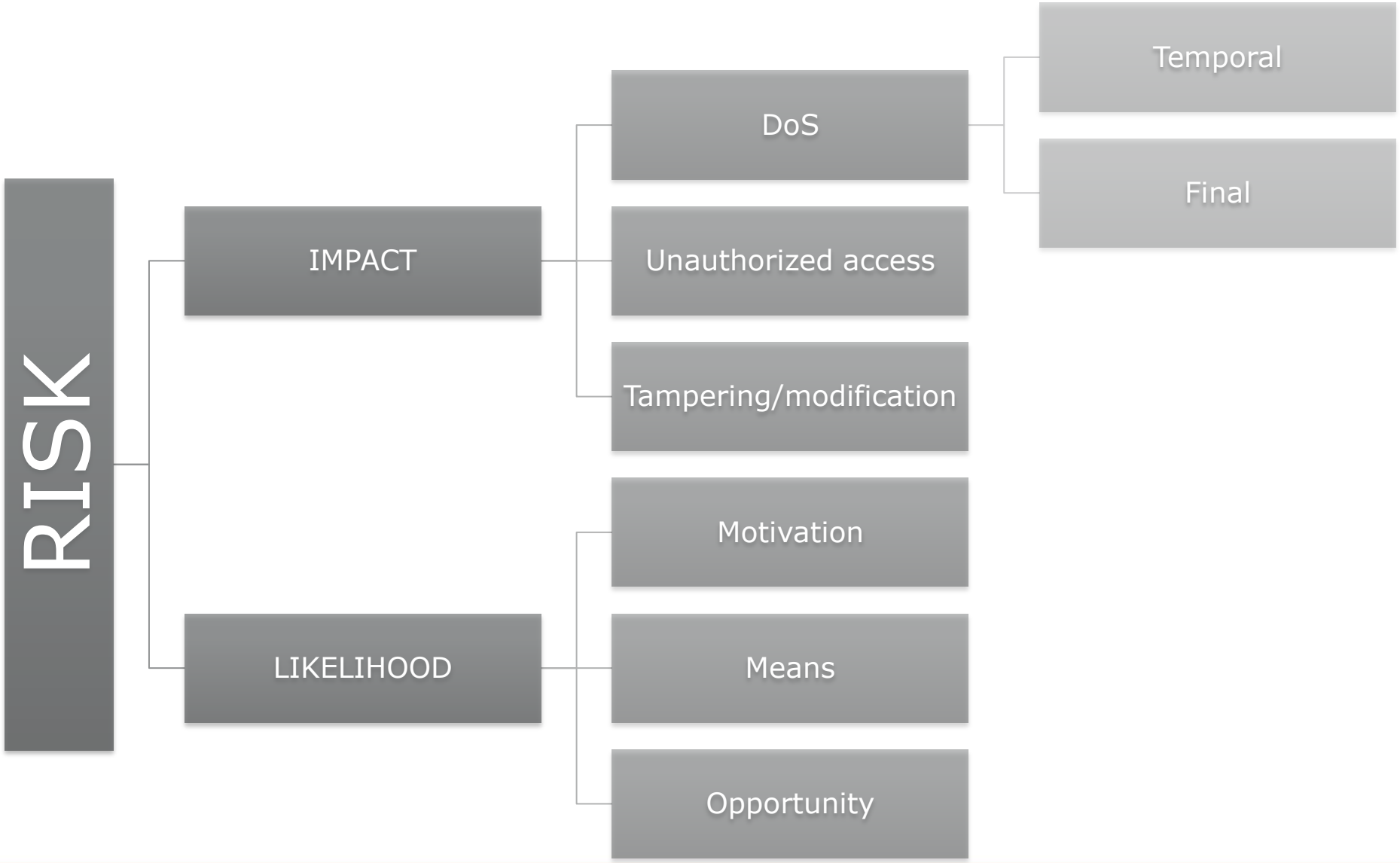
GMV-UNCLASSIFIED

gmv® INNOVATING SOLUTIONS

COMMUNICATION THREATS

- Jamming:
  - Accidental
  - Intentional
- Eavesdropping:
  - Espionage
  - Fraud
- Unauthorised telecommanding:
  - Hijacking
  - Sabotage
  - Denial of Service
  - Grilling
  - Collisioning
  - Fraud (illicitly using satellite capacity)
- Communication Errors:
  - Weather conditions
  - Coverage

RISKS


RISK
IMPACT
LIKELIHOOD
DoS
Unauthorized access
Tampering/modification
Temporal
Final
Motivation
Means
Opportunity

CHALLENGES

High likelihood

- Jamming
- Eavesdropping

Open channel

High Impact

- Unauthorised telecommanding

Cost & Repair limitations

Thank You

Julio Vivero
Head of Consulting Area
Email: jvivero@gmv.com
www.gmv.com

gmv®
INNOVATING SOLUTIONS

Challenges in modern communications: software-defined radio implementation of spectrum-sensing cognitive radios

Daniel Riviello

Politecnico di Torino, Italy CSP - ICT Innovation, Turin, Italy

NexComm 2014 - Panel Communications
Nice, February 23-27, 2014

Cognitive radio standards

Cognitive radio (CR) goal

Opportunistic Spectrum Access (OSA) of spectrum holes in licensed bands, called *White Spaces* (WS).

2 IEEE emerging standards:

- **IEEE 802.11af or White-Fi**: CR engine only based on Geolocation TVWS Database
- **IEEE 802.22 WRAN**: CR based on both Geolocation TVWS Database and Spectrum sensing techniques
  - Energy detection (ED) based.
  - Feature-based detectors.
  - Eigenvalue-based detection (EBD) algorithms.

SDR challenges

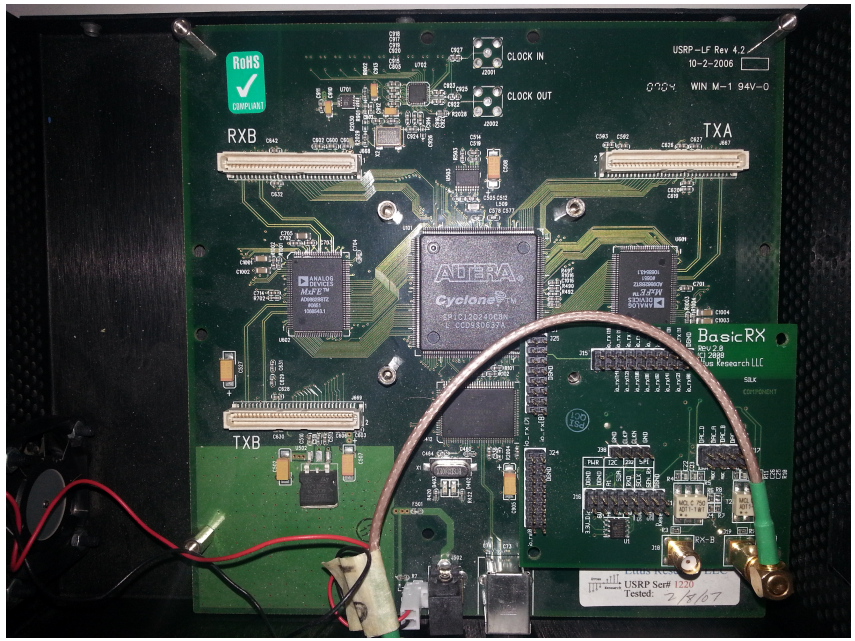
- Ongoing Ofcom White Space Trials in UK, database providers have started the qualification process.
- In other countries (like Italy), no available databases.
- Spectrum sensing needed for database construction, updates and future assistance with GLDB.

Challenges

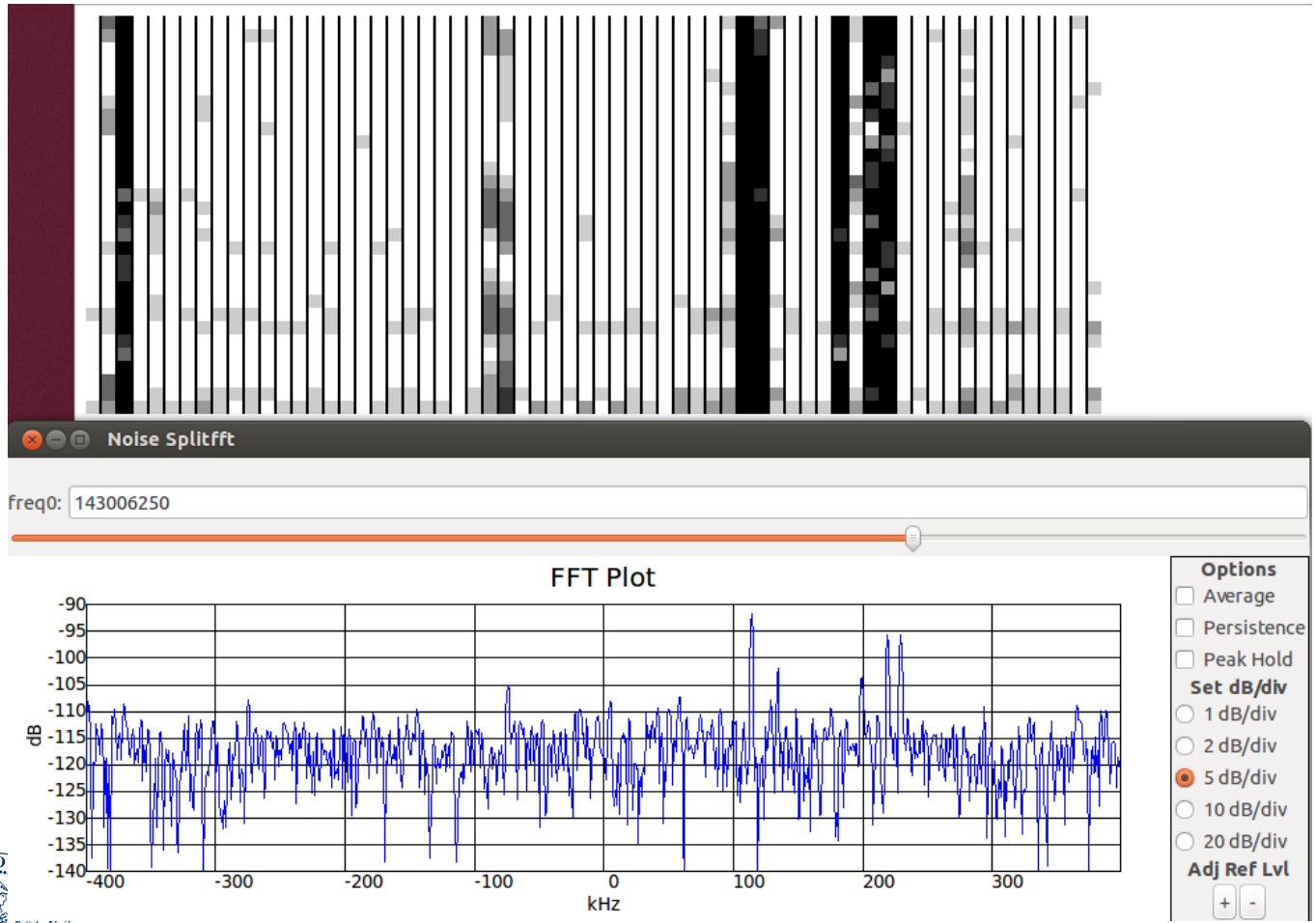
- Can a CR be fully implemented in software-defined radio (SDR)?
- Can spectrum sensing algorithms be implemented in SDR with low budget middle end transceivers?

GNU Radio and USRP front end

- GNU Radio is a free software platform for building software-defined radios
- Universal Software Radio Peripherals (USRPs) are middle end transceivers:
  - FPGA: digital baseband and IF section
  - all signal processing done by the host CPU



Spectrum sensing demo EBU 2014



Multi-band Energy Detection based spectrum sensor designed for DMR channels, presented at RadioHack kickoff session on February 10 at EBU 2014, Geneve