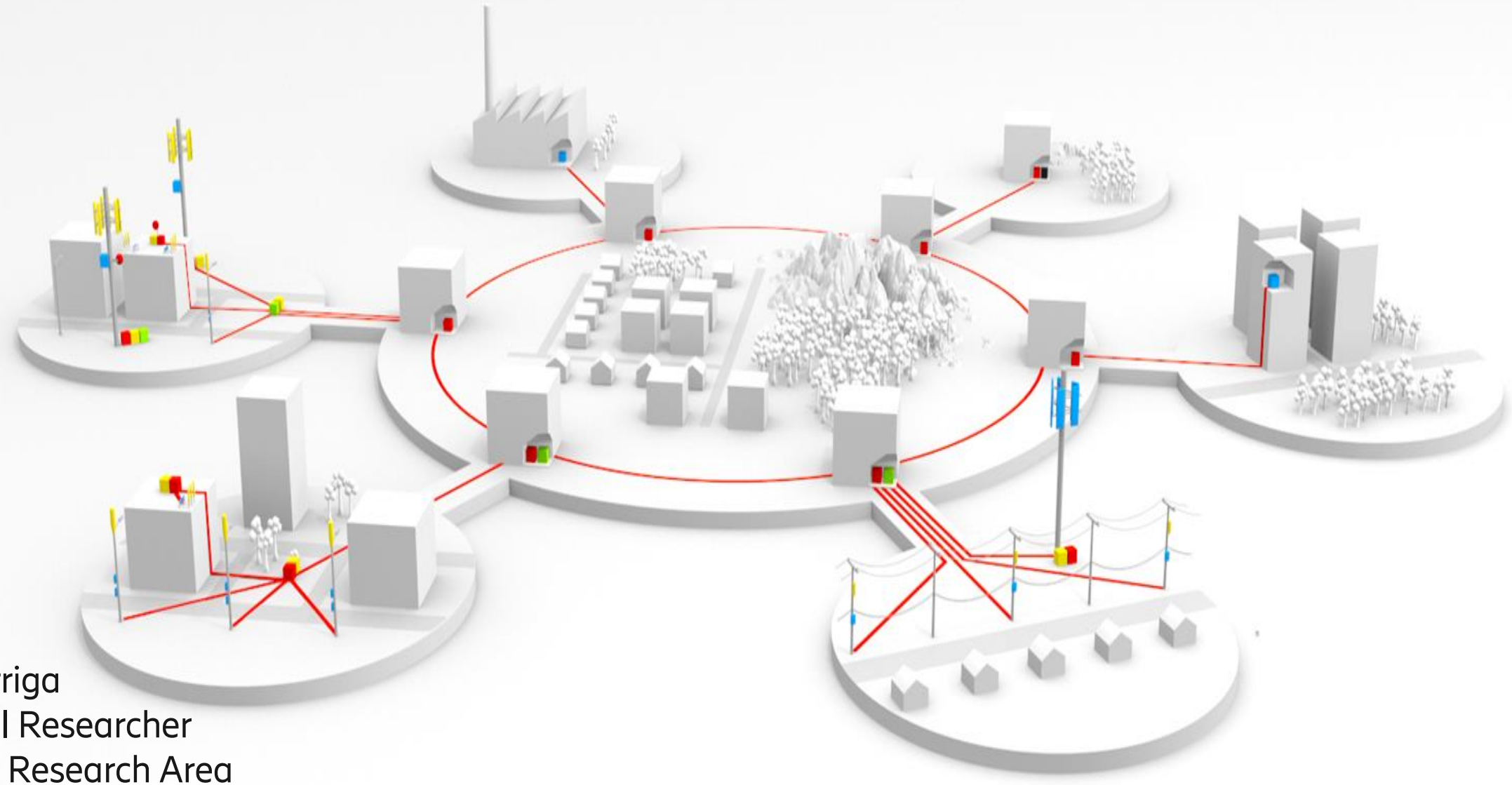
Cybersecurity Challenges in SNS



Luis Barriga
Principal Researcher
Security Research Area
Ericsson

Outline

—What will drive cybersecurity in SNS

—How to create trust in SNS

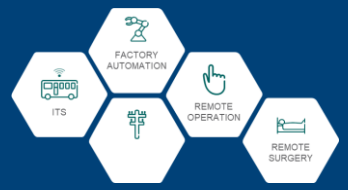
—Cybersecurity Challenges for SNS

What will drive Cybersecurity in SNS

Use Cases

Massive IoT

Critical IoT



Enhanced MBB

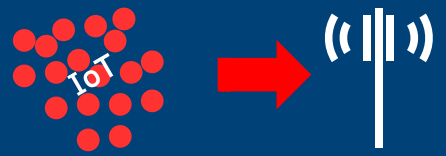
Threat landscape

Legacy Designs

Legacy trust model

Home network — Roaming Nw

New threats



New tech

Containers

Orchestration

HW Enclaves

Adversarial ML

Regulation

GDPR

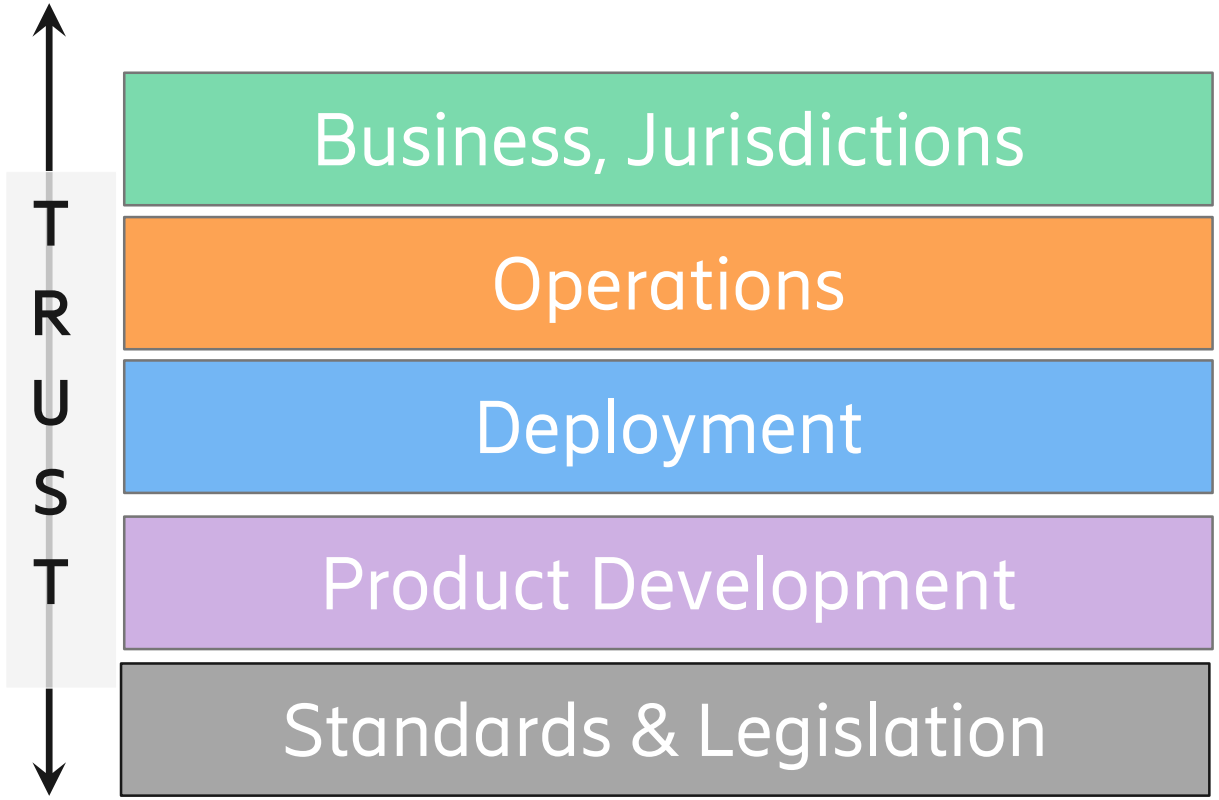
CONGRESS.GOV SBOM

What will drive cybersecurity in SNS
Lessons from 5G Security

- **Use-Case driven**
  - Efficient authentication signaling
  - Authentication agnostic for non-SIM devices
- **Changing threat Landscape**
  - Interworking security at the edge
  - Increased control by home operator upon roaming
  - IoT DDoS attack mitigation
- **New technologies**
  - Containers, Orchestration, Enclaves
- **Regulation**
  - GDPR – SUPI, SUCI, GUTI …

How to create trust in SNS

Security Assurance Frameworks



ATT&CK™

Cybersecurity Challenges for SNS

Security Assurance

- **Continuous integration & delivery** (CI/CD)
  - Assurance occurs b/w integration and delivery
  - Any change in target requires re-assurance
  - Continuous assurance is not feasible today
- **Virtualization, containers…**
  - VNF can run on different HW platforms
  - Unclear boundaries of "security target"
  - Assurance needs to consider HW root of trust
- **Human-based process**
  - Requires domain knowledge, security skills
  - Automation is hard. AI could help.
- **Formal Verification/Proofing Tools**
  - For software security, code analysis
  - For protocol analysis

Risk/Threat Management & Hunting

- **Human-based procedures**
  - Domain knowledge, security skills
  - AI-based automation?
- **Threat Intelligence platforms**
  - Focus on static IoC's & day-1 detection
  - TI for threat prediction & response
  - TI for sharing AI-models
- **Responsible disclosure**
  - Cooperation b/w academia & industry

Cybersecurity Challenges for SNS

AI/MI/ML

- Robustness
  - Model: extraction, inversion, stealing
  - Model evasion (increase false +/-)
- Assurance of AI-solutions or components
- Access to real big data (“data neutrality?”) for data-driven R&I

IoT HW/SW (Jungle)

- Need for IoT security Toolbox
  - IoT Identity management
  - IoT authentication framework
  - IoT assurance / certification
  - IoT Trustworthiness online
  - IoT regulation

Cybersecurity Regulation

- NG GDPR
- Fragmentation across jurisdictions
- Need for harmonization
- Lawyers & Technologists joint effort