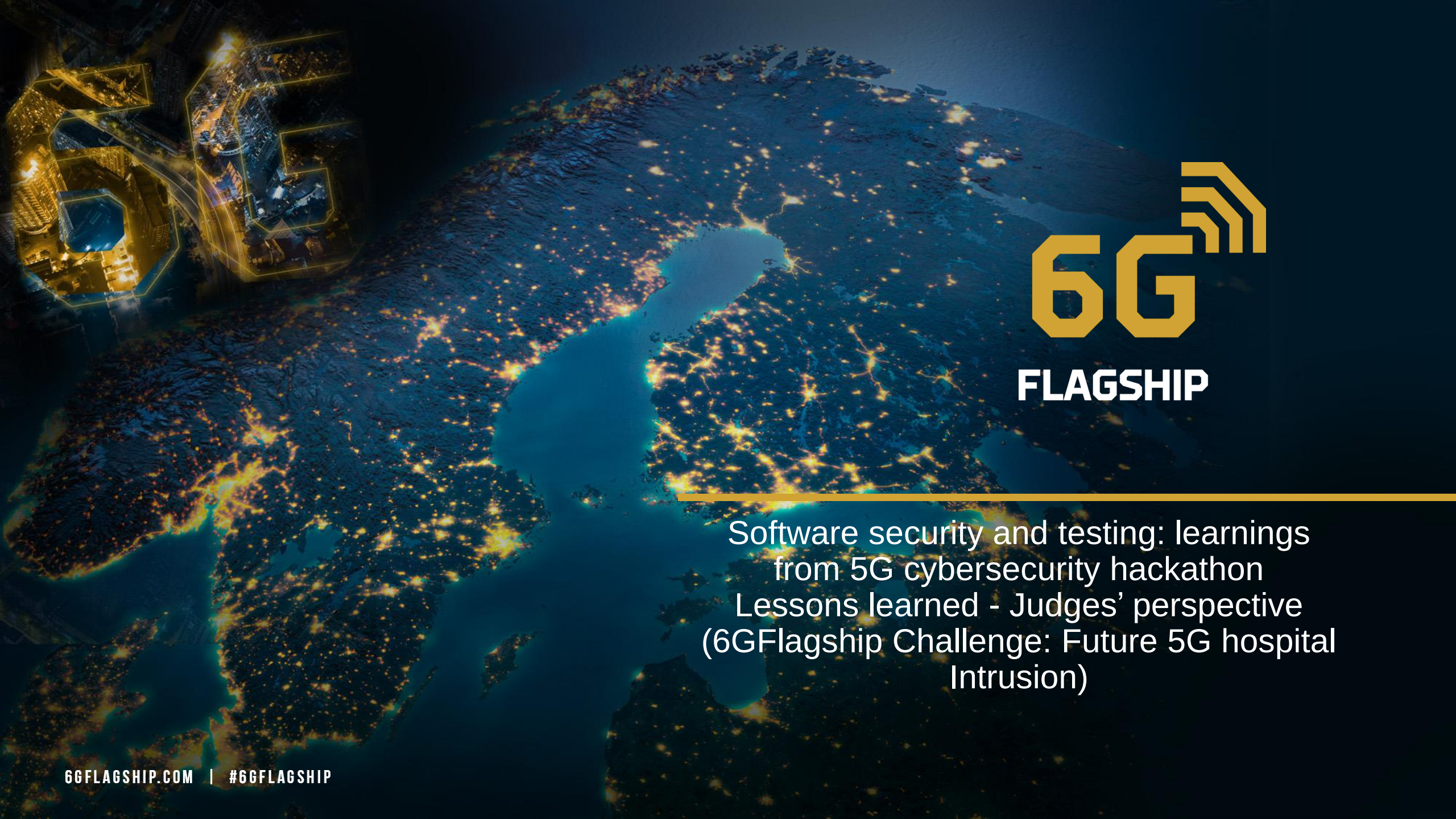
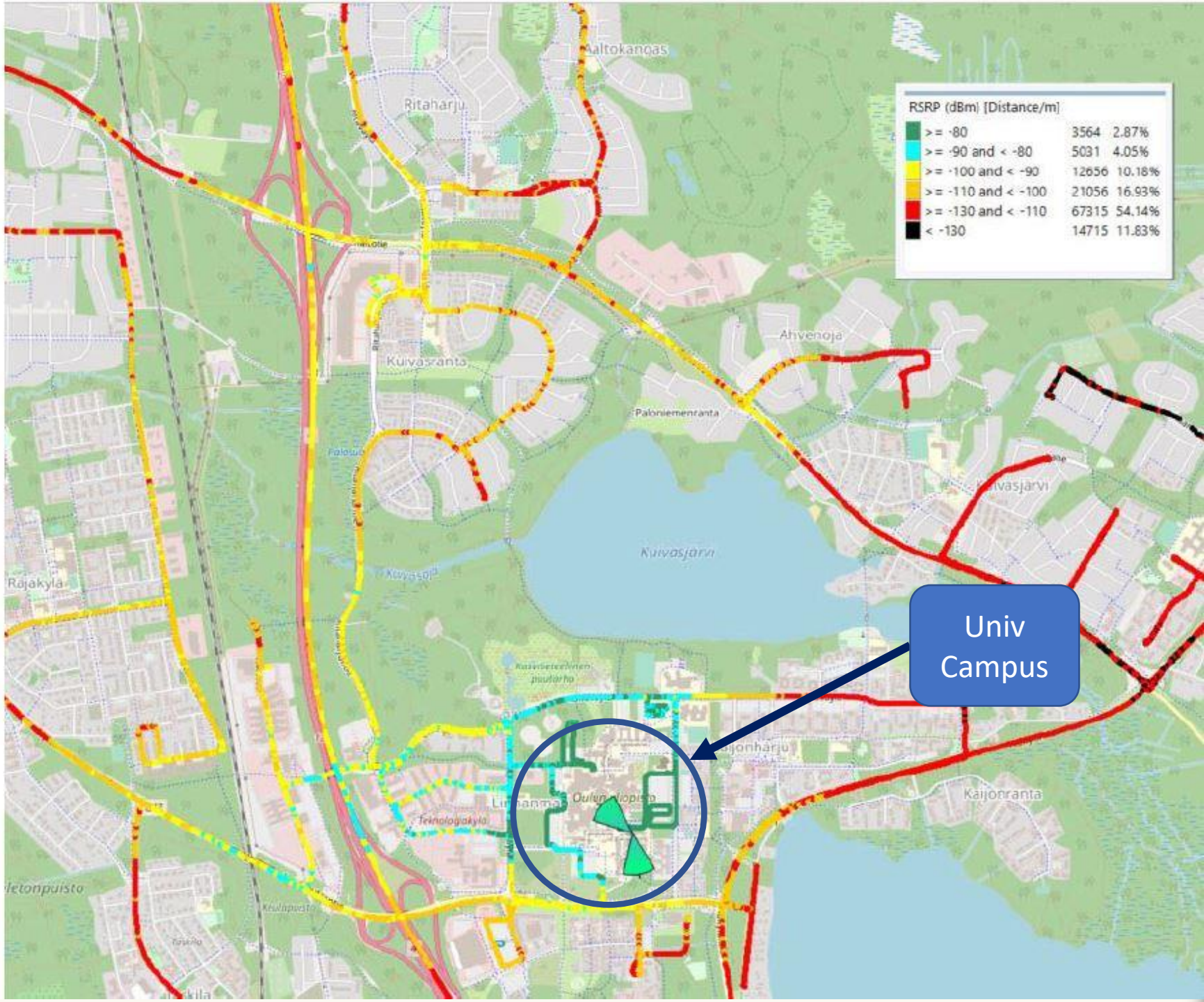


6G FLAGSHIP

Software security and testing: learnings from 5G cybersecurity hackathon Lessons learned - Judges' perspective (6GFlagship Challenge: Future 5G hospital Intrusion)

Where's the 5G ?

Outdoor coverage for used cell. Threshold for Red > -110dbm



Hack our Future Digital Health

In 6GFlagship challenge medical specialist in central hospital is using digital means and wireless communication for providing consultation to a nurse who is visiting a patient at home.

Digital data is collected via 360-video, close-camera view and biosensors. Critical symptoms are shown locally and remotely.

Applications are connected using 5G

Hospital:
Specialist

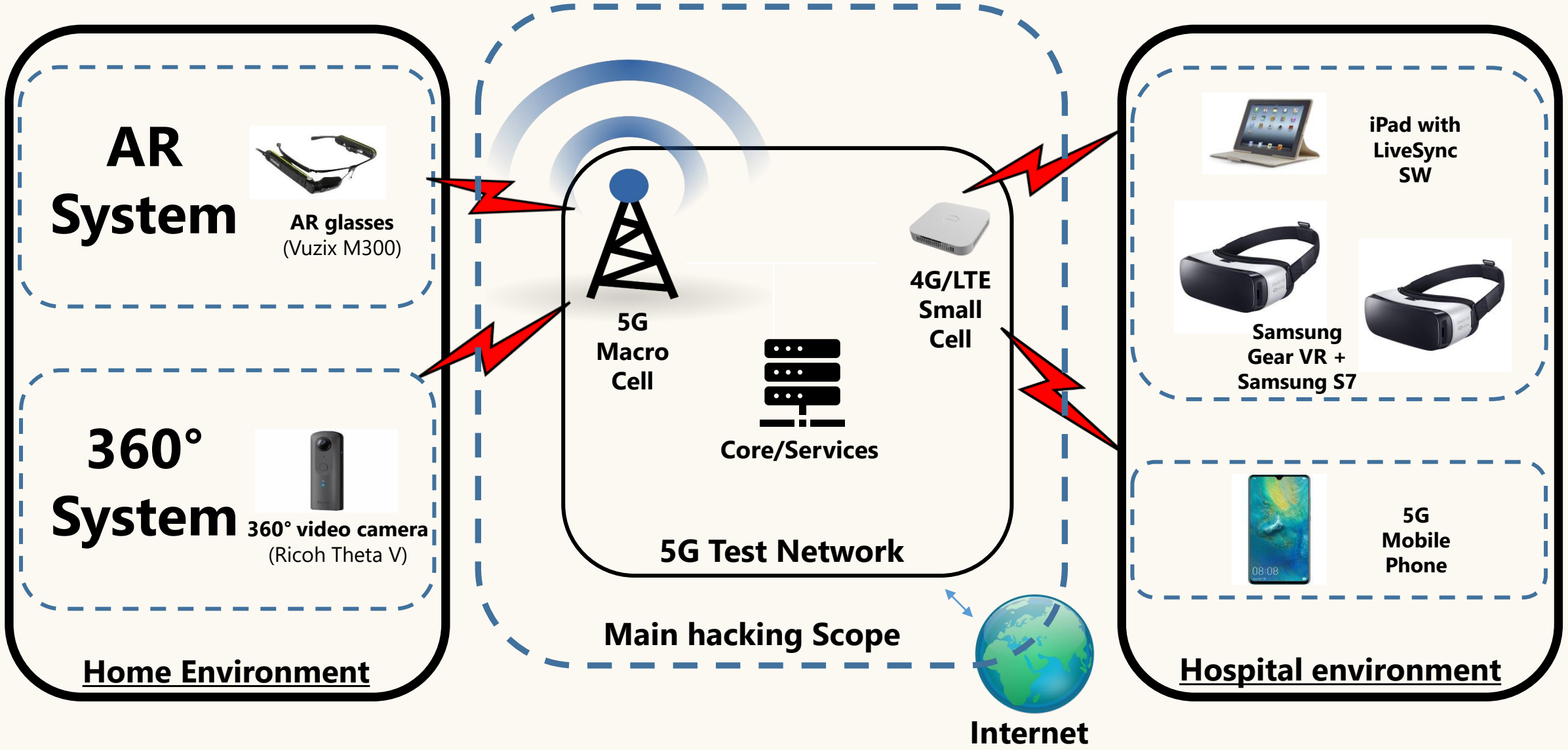
Home:
Nurse &
Patient

5G

AR/ Camera
Biosensors
360 Camera

VR, Tablet:
- 360 view
- Data from biosensors
- Close view from AR

Technical architecture



What did we (judges) and they (teams) do?

1. We were there to evaluate teams and their performance, not 5G itself
2. Seven (+ ½) teams in the “infrastructure & hospital use case” challenge
3. Approaches taken by the teams
   a. Systems approach, go after setup itself, its admins and the admin procedures (1 team)
   b. Traditional IT approach, treat it as generic Internet or Cloud computing (5 teams)
   c. 5G specific approach, go after the 5G aspects and physical setup (1 ½ teams)

→ → →

1. Most pressure on 5G security will come from security generalists
2. All technology consolidates, Internet =~ Cloud =~ 5G =~ CNI =~ ...
3. Good news: this makes building, testing and defending familiar

What did the teams say that they learned?

- Worth it, too complex for the available time, recon first, if you can't break it from inside then try from outside, segregation and ACLs important
- <no comment>
- Not so challenging as expected, learned a ton of stuff, opportunity to apply new techniques, useful 5G knowledge, attack across slices instead of access network, vertical movement useful, abstraction also creates fragility
- Learned, isolate, monitoring and opsec important, got 5G domain knowledge
- <no comment>
- From radio compromise the core and then come back, segmentation
- A lot of targets, segregation and ACLs, abstraction also creates fragility

prize - #pentestersiwouldhireformy5gcore

- The winner - Deep Cuts
- Very professional high quality pentesting report
- Focus on 5G core services
- Down the same rabbit holes + two unique findings

Recommendations from teams (to regulator)

- Promote best practices: ~“system understanding is needed in building and operating complex systems”
- Danger areas: “management interfaces & abstractions”
- Also heed: “operational security important in 5G” and “penetration testing”
- Training: “people that understand both telecom and security needed, also for virtual operators”