A Full Stack Hybrid 5G Testbed for Security Testing

LF ONE Summit

November 15, 2022

Dragoslav Stojadinovic

kryptowire labs

Zane Ma

Georgia Tech School of Electrical and Computer Engineering
College of Engineering

Experimenting in 5G

- Promise of *ubiquitous*, *high-speed*, *low-latency* internet access
- Bulk of research in wireless communications oriented towards 5G
- With 5G being a new technology, security is still in its research infancy

No good way to test 5G attacks / defenses

- All reliable solutions either closed-source, prohibitively expensive or don't work out-of-the-box

Testbed Requirements

FIDELITY

- **Over-the-Air (OTA) transmissions** for real physical layer signals
- **Physical devices**:
  - *Software Defined Radio (SDR) – UE/gNB*
  - *Commercial Off-the-Shelf (COTS phones and 5G modems) – UE*
  - Used to maintain and **verify fidelity**

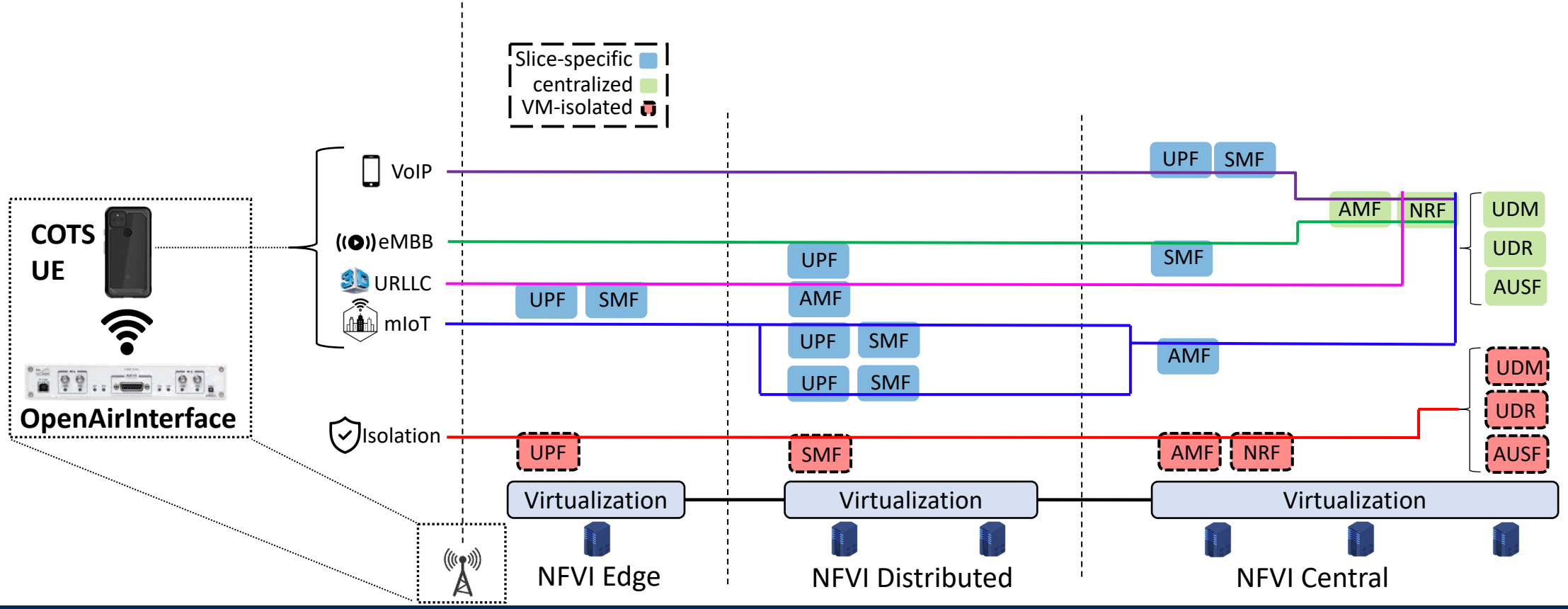
LARGE SCALE

- Emulated components – Docker
- Used for **large scale experimentation**

MATURITY

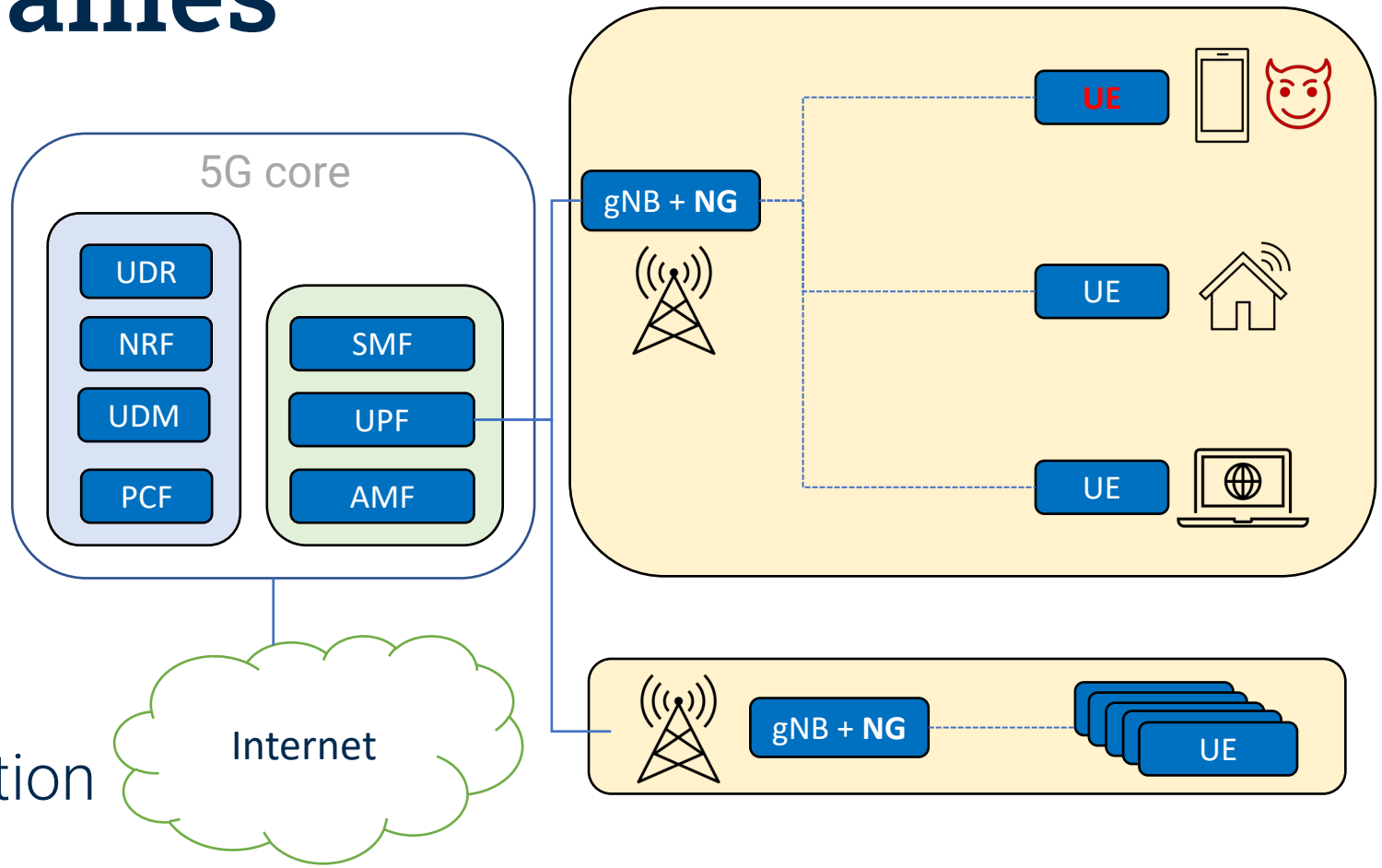
- **OAI –** full-featured 5G implementation in active development

5G Testbed Deployment



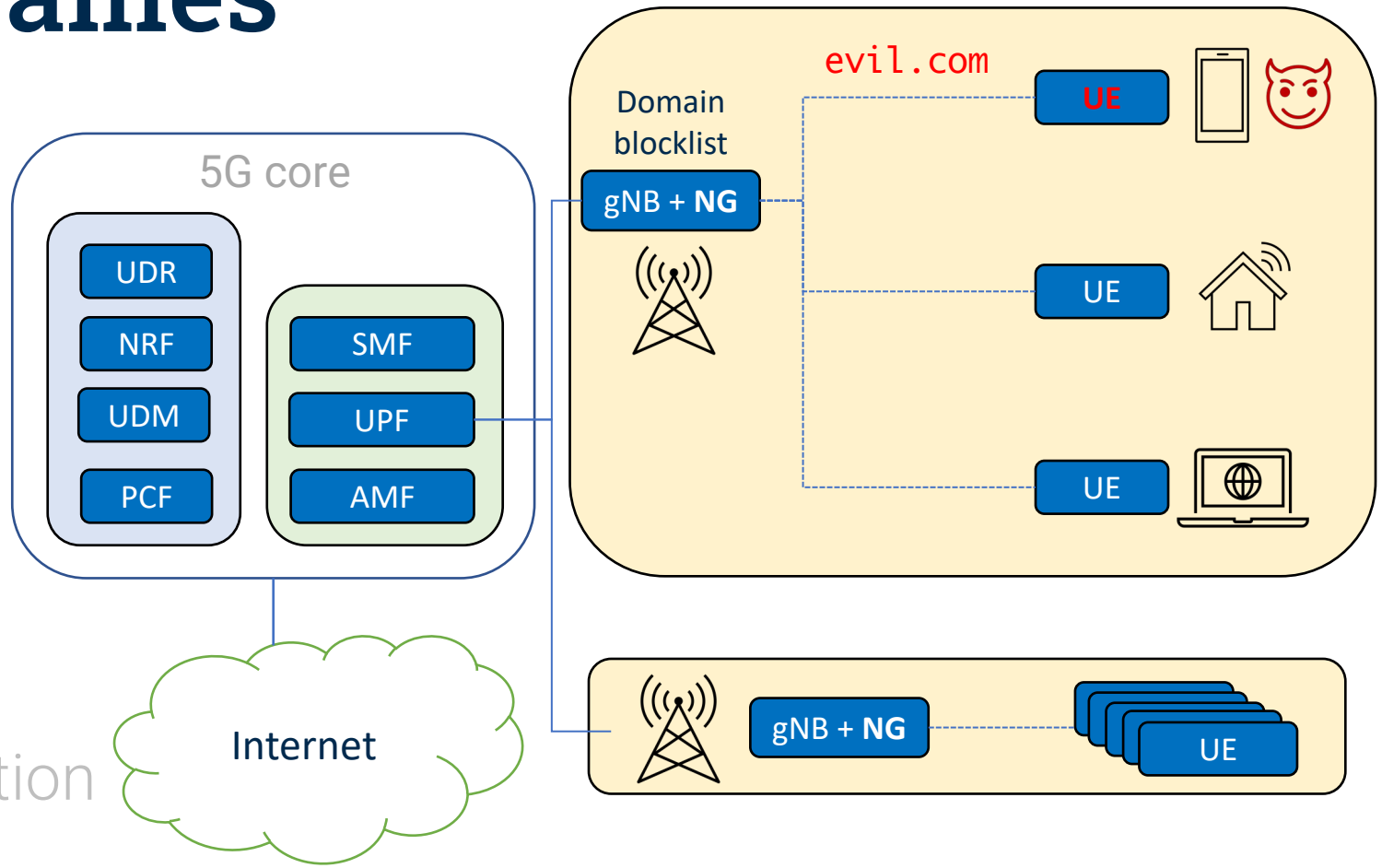
5G Network Games

1. Threat detection
2. Network isolation
3. Interrogation
4. Threat list expansion
5. Stepping stone detection



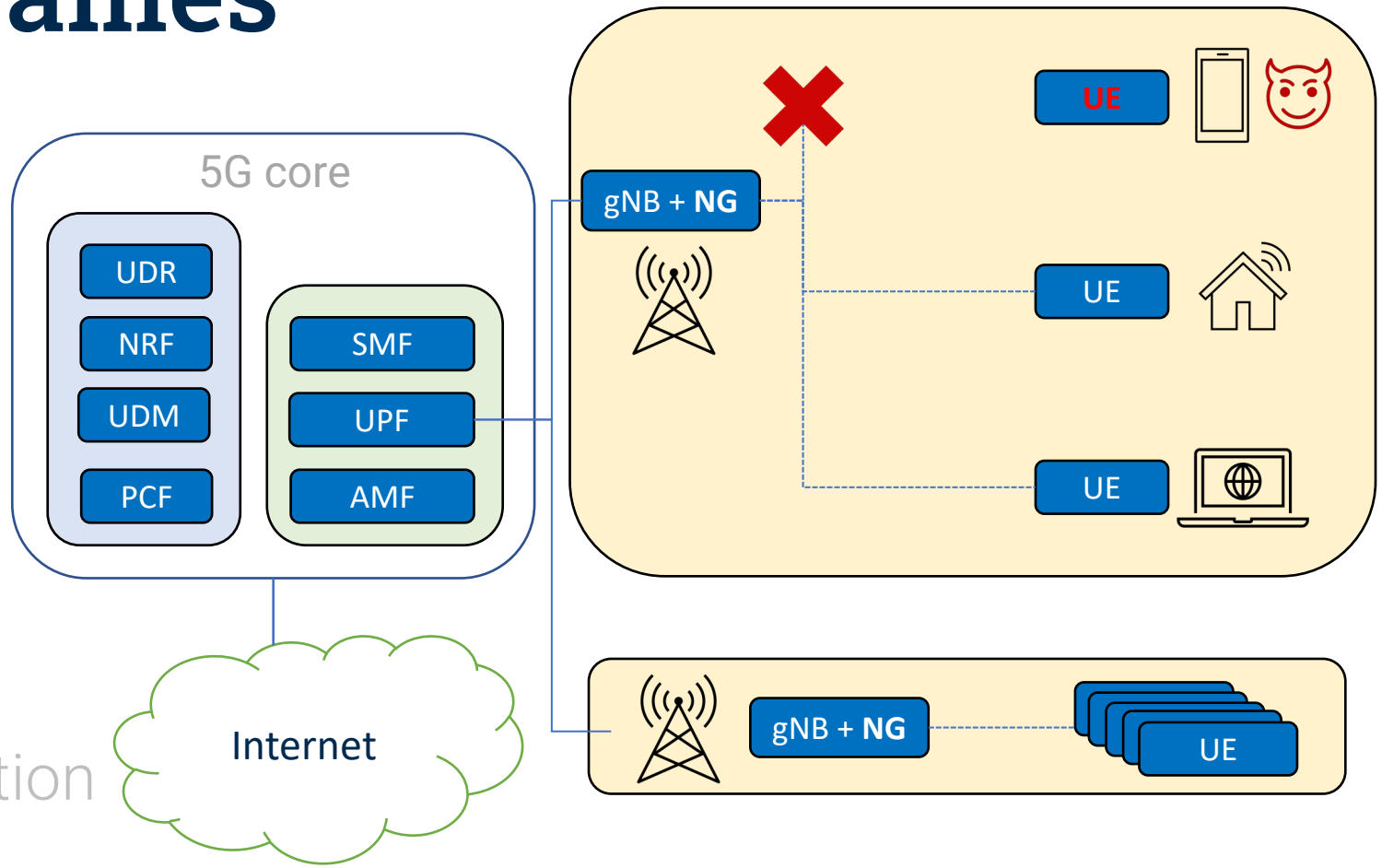
5G Network Games

1. Threat detection
2. Network isolation
3. Interrogation
4. Threat list expansion
5. Stepping stone detection



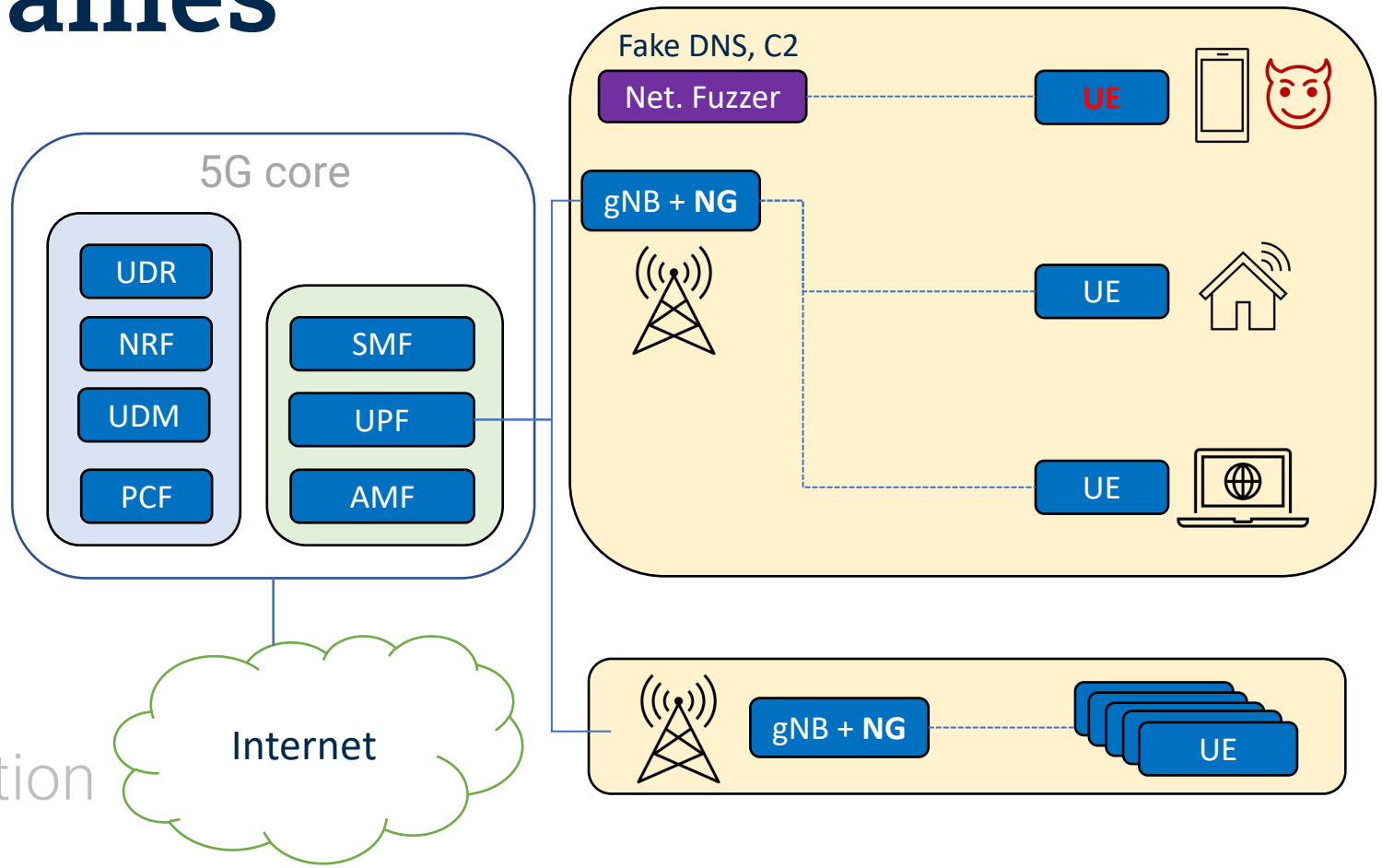
5G Network Games

1. Threat detection
2. Network isolation
3. Interrogation
4. Threat list expansion
5. Stepping stone detection



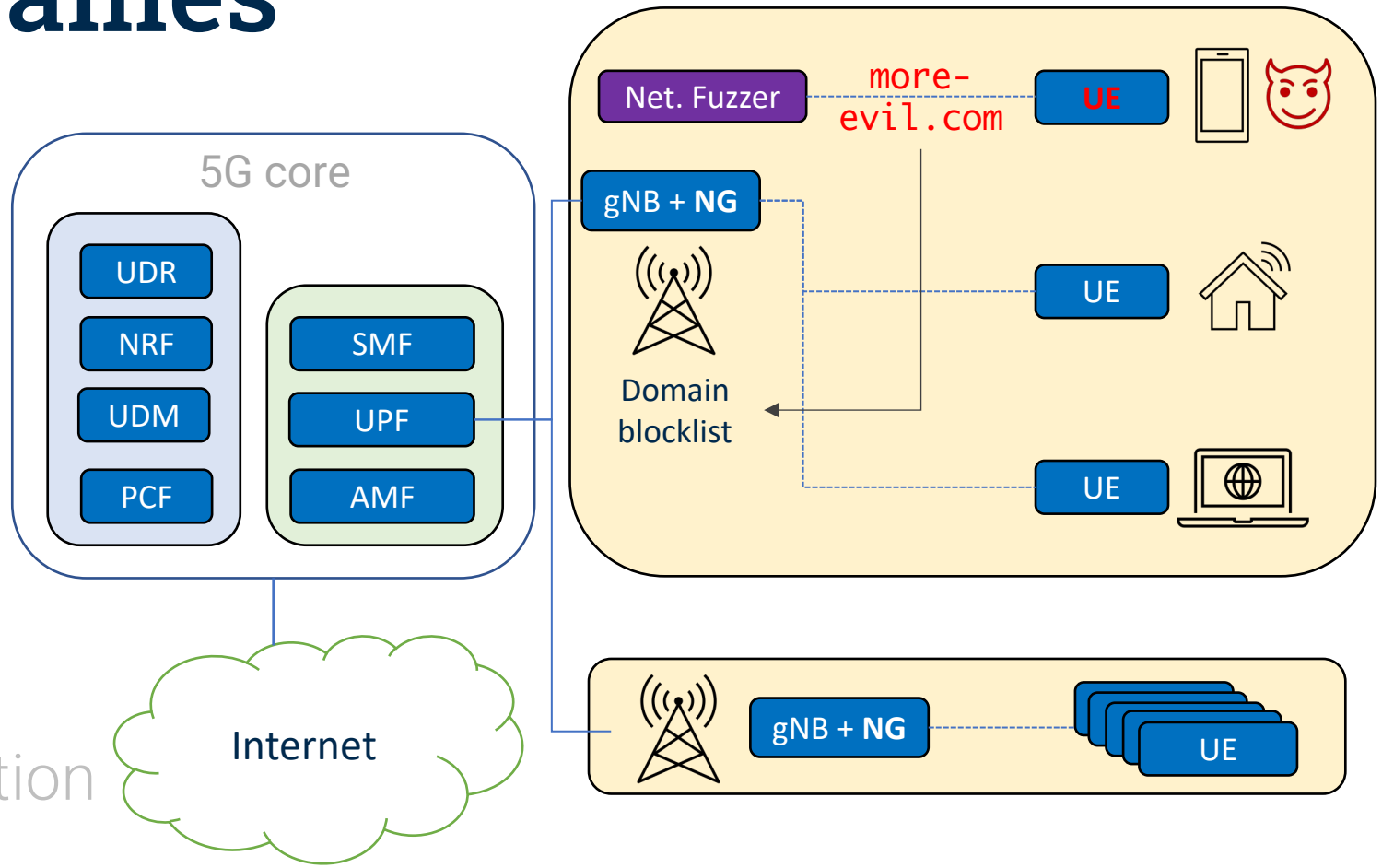
5G Network Games

1. Threat detection
2. Network isolation
3. Interrogation
4. Threat list expansion
5. Stepping stone detection



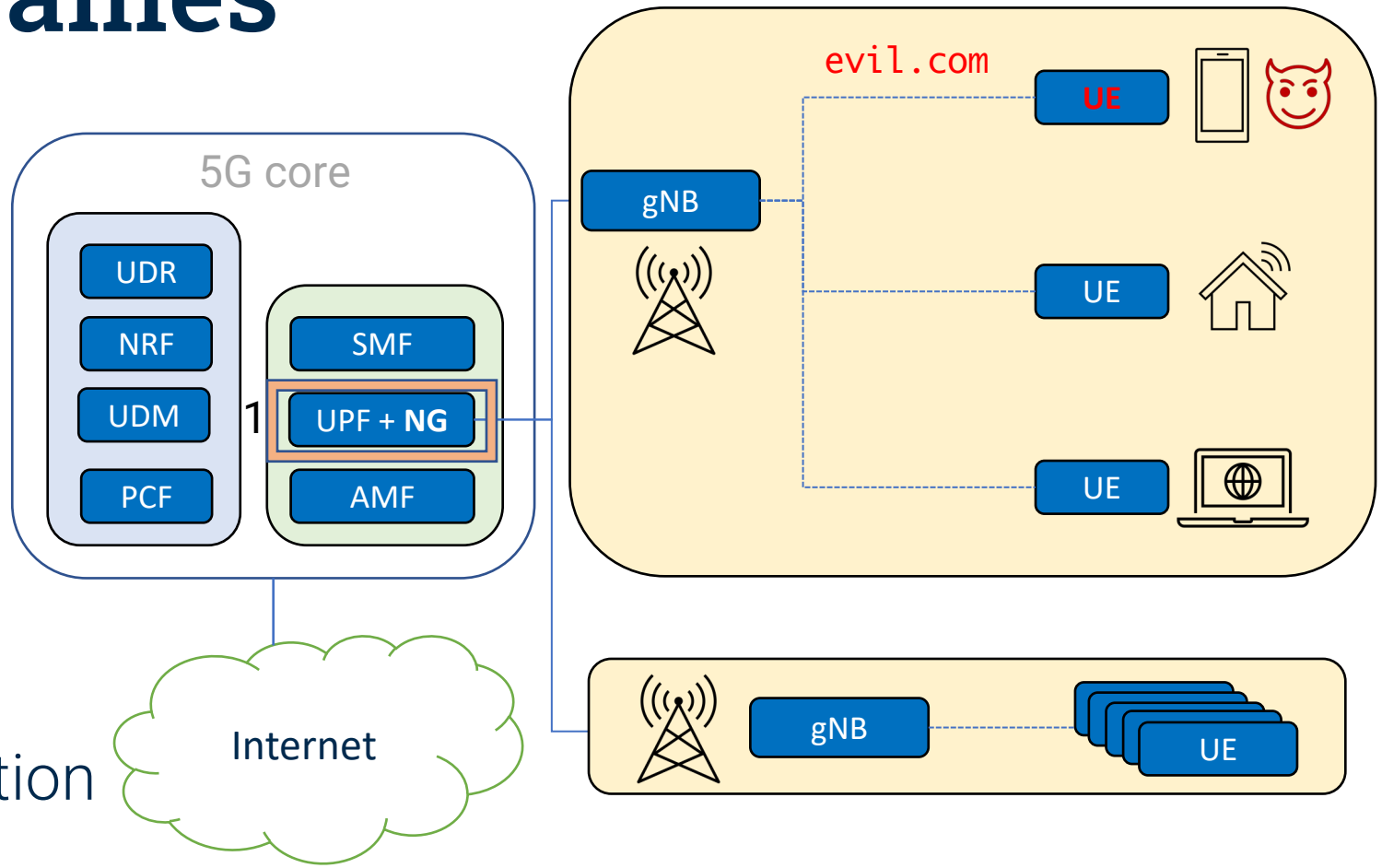
5G Network Games

1. Threat detection
2. Network isolation
3. Interrogation
4. Threat list expansion
5. Stepping stone detection



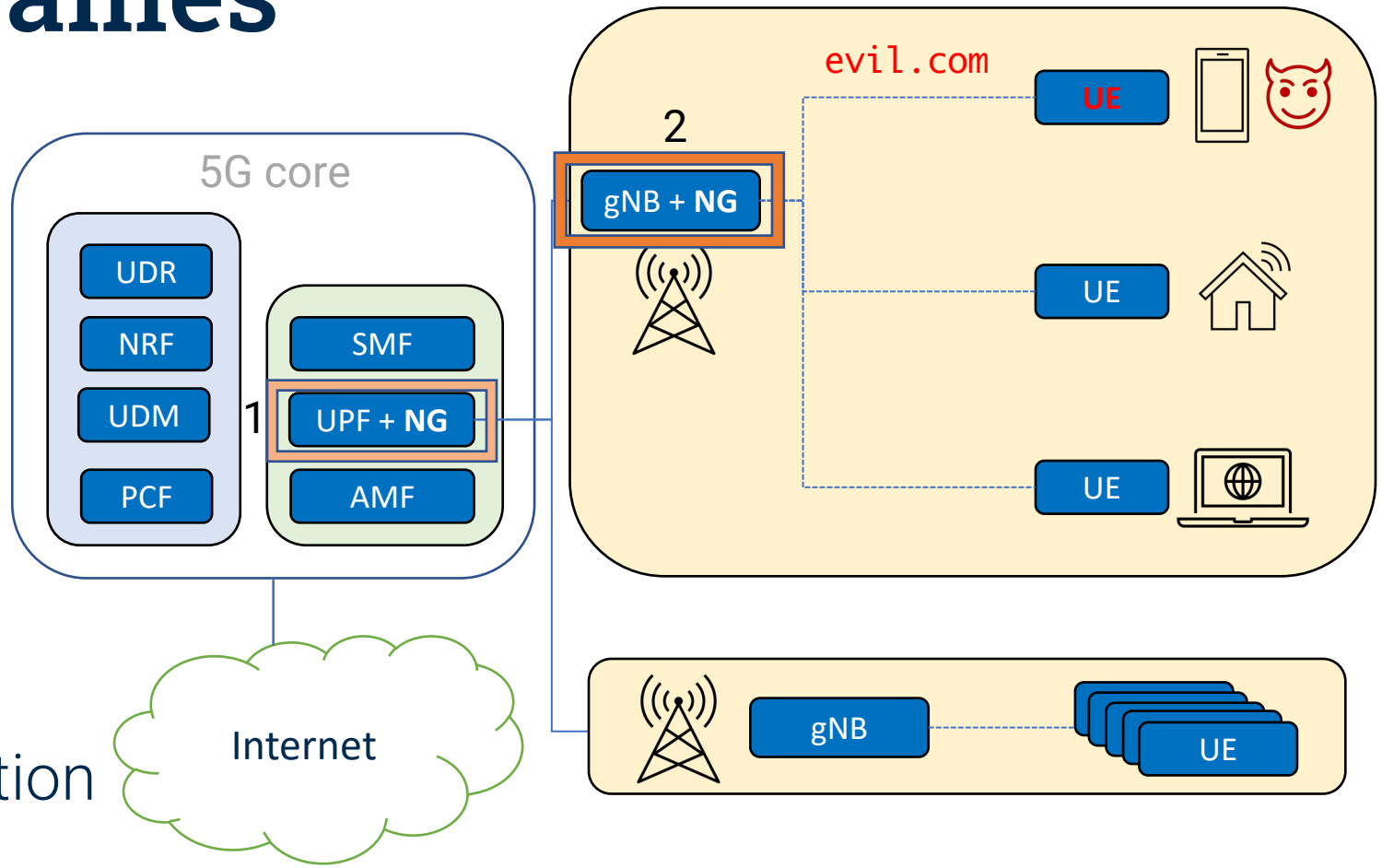
5G Network Games

1. Threat detection
2. Network isolation
3. Interrogation
4. Threat list expansion
5. Stepping stone detection



5G Network Games

1. Threat detection
2. Network isolation
3. Interrogation
4. Threat list expansion
5. Stepping stone detection



Looking Ahead

- Check it out! https://github.com/chateauxvt/oai5gtrafficgen
- Looking for collaborators and feedback
- Actively developing secure framework for composable, dynamic network defense primitives, e.g., firewall, DDoS defense, etc.
- Building more advanced defensive cyber operations that utilize5G-specific methods such as pushback, stepping-stone detection