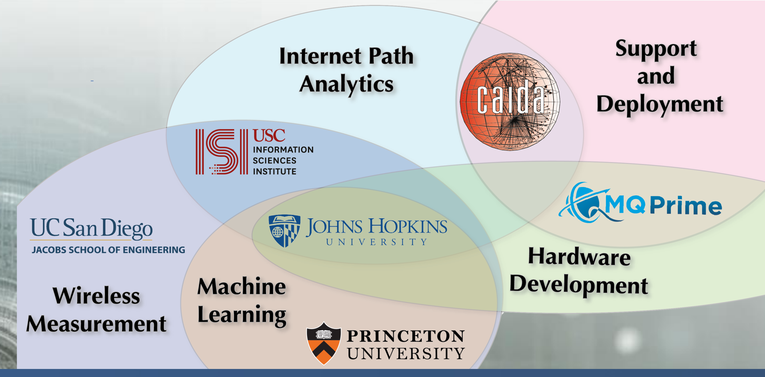
AVOID

Keeping Communications Unobservable



Project Goal

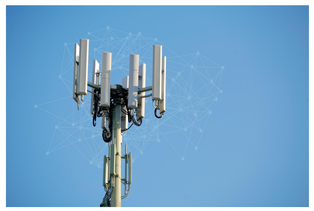
We tackle a fundamental problem for today's military: securing communications over commercial networks by avoiding adversary-controlled infrastructure.

Motivation

The core problem when operating through **unknown** or **non-cooperative commercial 5G infrastructure** is that the unknown infrastructure potentially exposes communications to an adversary.

When communications traverse adversary-controlled infrastructure, it allows DOD's sophisticated adversaries to recognize, disrupt, or extract intelligence from the communications. Even encrypted communications reveal the communicating source and destination IP addresses, which leaves the traffic remain vulnerable to advanced analysis techniques able to extract information directly from the encrypted data portion.

Risks of non-cooperative infrastructure



Obfuscation techniques offer limited protection

A natural response to the powerful threats posed by the unknown communication infrastructure is to disguise traffic in hopes of evading adversary detection. Such disguises create an arms race with ever more sophisticated disguises and advanced network intelligence techniques to detect them. With each new obfuscation attempt, DOD will never know if the disguise fools the adversary or if the adversary is simply lulling them into a false sense of security. Worse still, once an adversary learns DOD's obfuscation approaches, the disguises themselves can unintentionally draw unwanted attention from that adversary.

Fundamentally, **traffic obfuscation cannot provide meaningful security guarantees** when the underlying infrastructure is an unknowable black box.

While our technology is advanced, our goal is simple: to secure DOD communications over commercial networks by avoiding adversary-controlled infrastructure.

Solution

We propose the AVOID system - **Automated Verification Of Internet Data-paths** – that creates an unprecedented capability through two deliverables that tackle two high risk attack vectors for 5G communications.

I. Avoid initiating communications with adversarial base stations

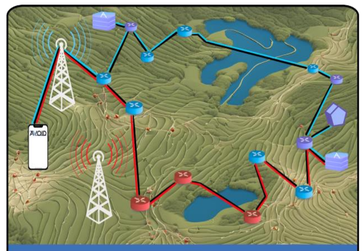
Several governments have reported that Chinese intelligence can control Huawei and ZTE base stations anywhere in the world, which would allow them to observe all traffic passing through those base stations.

Base station vendor classification and selection

AVOID leverages deep learning to **recognize potentially malicious 5G base station vendors** in seconds. AVOID also **provides a mechanism for DOD devices to connect to specific benign base stations.**

II. Avoid untrusted communications infrastructure along entire path

AVOID embeds topologic and geographic awareness into an overlay routing system, providing a mechanism for DOD's communications to avoid adversary-controlled territory across the global Internet and **route communication along benign paths**.



AVOID Routing System

The outcome will be an end-to-end adversary avoidance routing system that does not require modification to existing applications or routers in DOD networks, nor cooperation by any third-party network.

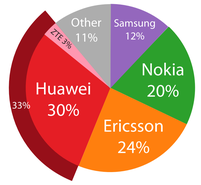
With AVOID, infrastructure is *knowable*.

Solving DOD's biggest communication challenges

- Embed topologic and geographic awareness into the routing system
- Ensure DOD communications avoid adversary-controlled infrastructure
- Provide safe communication network paths to DOD-controlled networks

How Large is the Problem?

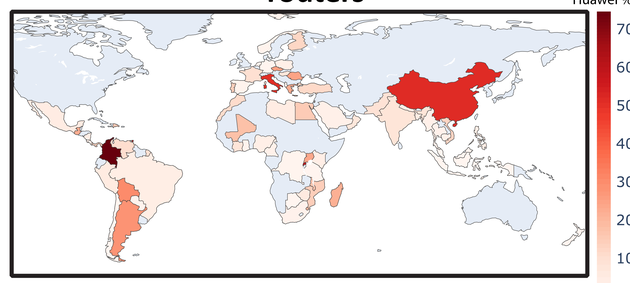
basestations



Huawei and ZTE had over 33% of the global market share of base stations in 2021*.

https://evertiq.com/news/52267

routers



CAIDA inferred Huawei routers in 85 countries in Feb 2024.

Competitive Advantages

Leverages Existing Commercial 4G/5G infrastructure

- Instant & ubiquitous communications
- Cheap commercial equipment (phones)
- No cost to maintain or deploy infrastructure

Allows Soldiers To Use Personal Phones

No other solution addresses this problem

- Other solutions put service members (& DOD) at risk
- AVOID deals with operational reality

Key Takeaways

- AVOID mitigates the problem of threats in the infrastructure
- Shift traffic from risky infrastructure to benign infrastructure

The Automated Verification Of Internet Data-paths for 5G project is funded by the U.S. Office of the Under Secretary of Defense for Research and Engineering, and the U.S. National Science Foundation (NSF) via Convergence Accelerator grants ITE-2226460 and ITE-2326928.