

Whistleblower Disclosure: Evidence of Protocol Violations and Neuroweapon Activation via 4G/LTE Sub-6GHz Infrastructure

Daniel R. Azulay

Monday 6th April, 2026

Disclaimer

This report presents **firsthand evidence, technical analysis, and documented protocol violations** suggesting the **covert integration of directed-energy and neuroweapon capabilities into 4G/LTE sub-6GHz infrastructure**. The claims are grounded in **observed regulatory breaches, unauthorized signal modulations, and classified technology transfers** within protected civilian frequency bands.

The author, acting as a whistleblower, submits this evidence for validation by **independent technical bodies, law enforcement, and international oversight organizations**. The purpose is to expose potential **crimes against humanity, violations of international telecommunications law, and the weaponization of civilian infrastructure**.

Executive Summary

Evidence indicates that **legacy directed-energy and radiofrequency (RF) technologies**, originally developed for military applications, have been **covertly embedded in 4G/LTE sub-6GHz infrastructure** through defense contractor pathways. This integration appears to enable **neurological targeting capabilities**, facilitated by:

- **Protocol violations** in protected civilian frequency bands (e.g., **600 MHz–6 GHz**).
- **Unauthorized signal modulations** consistent with directed-energy weaponry.
- **Defense contractor involvement** in both military RF programs (e.g., TITAN) and 4G/LTE infrastructure development, including **Anduril, Palantir, and BAE Systems**, who hold patents for **sub-6GHz shielding penetration** and directed-energy applications.
- **ATIS (Alliance for Telecommunications Industry Solutions)**, which played a central role in designing **4G/5G protocol security architectures**, and whose board of directors has historically included leadership from **DARPA, BAE Systems, DoD, Navy, and CIA**.

This is not theoretical. The author has compiled **technical data, patent filings, and spectrum analysis** pointing to a **coordinated effort to repurpose civilian 4G/LTE networks** for dual-use applications, including **neurological and behavioral influence**. Notably, **BAE Systems' patents** demonstrate the ability to penetrate shielding using sub-6GHz directed energy, explaining why targets rarely find relief outside a **full Faraday cage**.

1 Background: Key Entities and Technologies

1.1 WaveBand Corporation and Sierra Nevada Corporation (SNC)

- WaveBand specialized in **RF and antenna technologies**, including concepts like **MEDUSA** (a directed-energy system using pulsed microwaves to induce auditory effects via the Frey effect).
- Acquired by SNC in 2005, WaveBand's IP was integrated into SNC's defense portfolio, which includes **electronic warfare, AI-driven targeting, and space systems**.
- Patents and technical documents suggest **MEDUSA-related technologies evolved into advanced neurological targeting systems**, with applications in **sub-6GHz bands**.

1.2 Palantir, Anduril, BAE Systems, and the TITAN Program

- **TITAN (Tactical Intelligence Targeting Access Node)** is a U.S. Army AI-driven system for **multi-domain sensing, data fusion, and autonomous targeting**.
- Prime contractors and partners include:
 - **Northrop Grumman** (directed-energy weapons, high-power RF)
 - **L3Harris** (electronic warfare systems, RF spectrum dominance)
 - **Sierra Nevada Corporation** (legacy WaveBand RF/antenna technologies)
 - **Palantir** (AI-driven data fusion and autonomous targeting)
 - **Anduril** (autonomous weapons systems, AI-driven sensor networks)
 - **BAE Systems** (sub-6GHz shielding penetration, directed-energy applications)
- These firms are simultaneously involved in **4G/LTE military applications**, creating a direct pipeline for **military RF technologies into civilian networks**.

1.3 BAE Systems: Sub-6GHz Shielding Penetration

- BAE Systems holds **multiple patents** for technologies enabling **sub-6GHz directed energy to penetrate shielding**, for example "APPARATUS FOR A DIRECTED ENERGY WEAPON" (EP 3 581875A1).
- These patents demonstrate that **sub-6GHz directed energy can be deployed via drones or 4G/LTE infrastructure**, making it **highly difficult for targets to find relief without a full Faraday cage**.

1.4 ATIS: Military and Intelligence Influence on Telecommunications Standards

- The **Alliance for Telecommunications Industry Solutions (ATIS)** is a key organization responsible for **developing and standardizing protocol security architectures for 4G and 5G networks**.
- ATIS has played a **central role in defining the security and signal modulation standards** that underpin modern telecommunications, including:

- **Protocol security architectures** for 4G/LTE and 5G.
- **Signal modulation and encryption standards.**
- **Network interoperability and authentication frameworks.**
- Historically, ATIS’s **board of directors and leadership** have included high-ranking officials from:
 - **DARPA** (Defense Advanced Research Projects Agency)
 - **Department of Defense (DoD)**
 - **U.S. Navy**
 - **Central Intelligence Agency (CIA)**, including **weapons experts and signals intelligence (SIGINT) specialists.**
- This **military and intelligence influence** over ATIS raises critical questions about the **potential embedding of dual-use or offensive capabilities** within civilian telecommunications standards, including:
 - **Backdoors or vulnerabilities** in protocol security architectures.
 - **Adaptive modulation techniques** that could facilitate directed-energy or neuroweapon applications.
 - **Lack of transparency** in the standardization process, particularly regarding the involvement of defense and intelligence agencies.

1.5 Department of Defense (DoD) and 4G/LTE: Dual-Use Risks

- The DoD has pursued **4G/LTE integration for military applications**, leveraging commercial infrastructure for **command-and-control, sensor networks, and autonomous systems.**
- **Sub-6GHz bands** (e.g., 600 MHz–6 GHz) are used for both **4G/LTE and legacy directed-energy research**, including:
 - Neurological disruption (e.g., microwave auditory effect)
 - Behavioral modification (e.g., pulsed RF influence on cognitive function)
- **Classified DoD research** on RF bioeffects remains undisclosed, despite its relevance to 4G/LTE safety.

1.6 The Directed-Energy–4G/LTE Nexus

- **Sub-6GHz 4G/LTE and directed-energy systems** share reliance on **precise signal modulation and adaptive protocols.**
- **Protocol violations** in 4G/LTE sub-6GHz deployments include:
 - Unauthorized waveform modulations matching directed-energy signatures.
 - Adaptive beamforming algorithms repurposed from electronic warfare (EW) systems.
- Patents linked to SNC, Northrop Grumman, Anduril, and BAE Systems describe **RF modulation techniques capable of influencing neural activity**, including:

- Pulsed microwaves for auditory and cognitive effects.
- Ultra-narrowband signals for peripheral nervous system disruption.
- **Shielding-penetrating sub-6GHz directed energy**, deployable via drones or 4G/LTE infrastructure.

2 Evidence: Protocol Violations and Neuroweapon Activation

2.1 Documented Spectrum Anomalies

Independent analysis reveals:

- **4G/LTE sub-6GHz base stations transmitting unauthorized modulations** in protected civilian bands (e.g., **1.7 GHz, 1.8 GHz, 2.5 GHz**).
- **Signal patterns** consistent with:
 - Pulsed RF modulations used in directed-energy weapons.
 - Ultra-narrowband spikes at frequencies linked to neurological resonance.
 - **Shielding-penetrating waveforms** matching BAE Systems’ patented techniques.
- **Correlation between 4G/LTE rollouts and reported neurological symptoms**, including:
 - Tinnitus and auditory hallucinations (microwave hearing).
 - Cognitive impairment and sleep disturbances.
 - **Persistent exposure even within partially shielded environments**, consistent with BAE Systems’ shielding-penetration patents.

2.2 Patent and Contract Trail

- SNC, Northrop Grumman, Anduril, and BAE Systems hold patents for directed energy weapons and AI driven autonomous weapons.
- DoD contracts awarded to TITAN partners include **Directed Energy “dual-use” development** with no public oversight of RF safety protocols.
- **Revolving-door personnel** between defense contractors, the FCC, and telecom firms have facilitated regulatory bypass.

2.3 Whistleblower Testimony and Technical Data

The author possesses:

- Relevant patents from SNC, BAE Systems, and telecom partners.
- SDR IQ-streams showing **unauthorized modulations in live 4G/LTE sub-6GHz networks**, which must be **shielding-penetrating waveforms** utilizing multipath propagation given they penetrate a well but partially shielded home.

- Repeatable and replicable frequency measurements near human heads that statistically differ from measurements near mobile phones, with a **very tight frequency distribution in three distinct center frequencies** near human heads, both indoors and outdoors, which is a paradoxical finding as one would expect the opposite: wider distribution of frequencies near heads vs phones.
- Spoofed or cloned 4G Uplink signals coming from towers in a downlink fashion, measured with a log-periodic directional antenna.
- Evidence of impossible mobile phone frequency selection, e.g. operators using the wrong frequency allocations vs what is publicly documented and would be expected, leading to the conclusion that cognitive targeting is given priority (mainly in the 2.5GHz band, the uplink portion of channel 7, which overlaps military channel 41) over lawful use of mobile frequencies by mobile devices.
- Evidence of severe technical interference during research of this topic, including but not limited to infection with pegasus-spyware, email interference, device exploits, data falsification, mail theft, and parcel theft.
- Medical evidence clearly pointing to what is publicly known as Havana Syndrome, while a hospital treated it as psychosis and refused to investigate the extensive neurological symptoms the author presented with. This hospitalization occurred exactly 48 hours after the author sent a first article implicating the merger of 5G and AI technologies as a weapon to government officials.
- Evidence of non-response and dismissal from government officials and Dutch intelligence in the matter, even when clear evidence is present.

3 Mechanism: How 4G/LTE Sub-6GHz Enables Neuroweapons

4 Implications: Why Targets Rarely Find Relief

- BAE Systems' patents for **sub-6GHz shielding penetration** demonstrate that **conventional RF shielding (e.g., partial Faraday cages, RF paint, or metal mesh) is ineffective** against these directed-energy systems.
- The use of **adaptive modulation techniques** allows 4G/LTE infrastructure to **bypass traditional shielding**, delivering targeted exposure even in **indoor or partially shielded environments**.
- This explains why affected individuals report **persistent symptoms regardless of location**, with **only full Faraday cages providing reliable relief**.

5 ATIS and the Standardization Process: A Closer Look

5.1 Historical Board Composition

- ATIS's board of directors has included **high-ranking officials** from:
 - **DARPA**: Known for developing **dual-use and offensive technologies**, including directed-energy weapons and neurotechnologies.

Table 1: Convergence of Military and 4G/LTE Sub-6GHz Technologies

| Component | Military Application | 4G/LTE “Civilian” Application | Evidence of Convergence |
|------------------------------|--|---|--|
| Sub-6GHz Antennas | Directed-energy weapons (e.g., MEDUSA, BAE Systems drones) | 4G/LTE base stations | Patents for dual-use phased arrays and shielding penetration |
| Signal Modulation | Neurological disruption (pulsed RF) | “Efficient” data encoding | Unregistered pulse patterns in 4G/LTE |
| Adaptive Protocols | Targeted RF exposure (EW systems) | “Smart” network optimization | Beamforming algorithms matching EW systems |
| Shielding Penetration | BAE Systems’ drone-mounted directed energy | “Enhanced coverage” in urban environments | Patents for sub-6GHz shielding penetration |
| AI-Driven Targeting | Autonomous weapons (e.g., TITAN, Anduril) | Network analytics | Palantir/Anduril’s role in both military and 4G/LTE systems |
| Protocol Standards | ATIS-led security architectures with DARPA/DoD/CIA/BAE input | “Secure” civilian telecommunications | ATIS board membership and standardization influence |

- **Department of Defense (DoD):** Directly involved in **military communications, electronic warfare, and directed-energy research.**
- **U.S. Navy:** Focused on **RF and sonar technologies**, with applications in both warfare and surveillance.
- **Central Intelligence Agency (CIA):** Including **weapons experts and SIGINT specialists**, suggesting a focus on **covert applications of telecommunications technologies.**

5.2 Implications for 4G/LTE Security

- The involvement of **DARPA, DoD, and CIA leadership** in ATIS raises concerns about:
 - **Embedded vulnerabilities** in 4G/LTE protocol security, potentially allowing for **unauthorized access or signal injection.**
 - **Dual-use modulation techniques** that could be repurposed for **directed-energy or neuroweapon applications.**
 - **Lack of independent oversight** in the standardization process, particularly regarding the **influence of defense and intelligence agencies.**

- ATIS’s role in **defining encryption, authentication, and signal modulation standards** for 4G/LTE means that any **embedded backdoors or offensive capabilities** would be **systemically deployed across global telecommunications infrastructure**.

6 Call to Action

6.1 Crimes Against Humanity

The **deliberate exposure of civilians to weaponized RF signals**—without consent—violates the **Nuremberg Code, UN Convention on Biological Weapons, and Geneva Protocol**.

6.2 Regulatory Failure

The **FCC, ITU, and ATIS** have failed to enforce protocol compliance, approving deployments based on **incomplete or manipulated data**.

6.3 Urgent Investigative Steps

- Forensic audits of 4G/LTE base stations for unauthorized modulations and shielding-penetrating waveforms.
- Subpoena of defense contractor records (including BAE Systems, Anduril, and Palantir) related to 4G/LTE dual-use programs.
- Congressional hearings on DoD–telecom collaboration and the role of Palantir, Anduril, BAE Systems, and ATIS.
- International oversight via the UN, WHO, and ICC to assess potential war crimes.
- Independent review of **ATIS-led standardization processes**, particularly the involvement of **DARPA, DoD, and CIA-affiliated board members**.

6.4 Public Right to Know

Citizens in 4G/LTE-deployed regions report symptoms consistent with directed-energy exposure. **Transparency is required to:**

- Halt further deployments until safety is verified.
- Provide medical monitoring for affected individuals.
- Hold accountable those responsible for covert weaponization.
- Inform the public about the **ineffectiveness of partial shielding** and the need for **full Faraday cages** in severe cases.
- Disclose the **full extent of military and intelligence influence** over telecommunications standards via ATIS and other standardization bodies.

7 Conclusion

The evidence demands immediate action from **law enforcement, human rights organizations, and the global scientific community**. The integration of **shielding-penetrating directed-energy technologies** into 4G/LTE infrastructure—if confirmed—represents a **flagrant violation of public trust, human rights, and international law**. The involvement of **ATIS, with its historical ties to DARPA, DoD, and CIA leadership**, further underscores the need for **full transparency and independent oversight** of telecommunications standardization processes.

Next Steps:

- Grant whistleblower protections to those with additional evidence.
- Conduct independent spectrum analysis of 4G/LTE networks, with a focus on **sub-6GHz shielding-penetrating waveforms**.
- Pursue legal action against complicit contractors (including BAE Systems, Anduril, and Palantir) and regulators.
- Launch public awareness campaigns on **risks, rights, and the limitations of conventional RF shielding**.
- Investigate and disclose the **role of ATIS and its board members** in shaping 4G/LTE protocol security architectures.