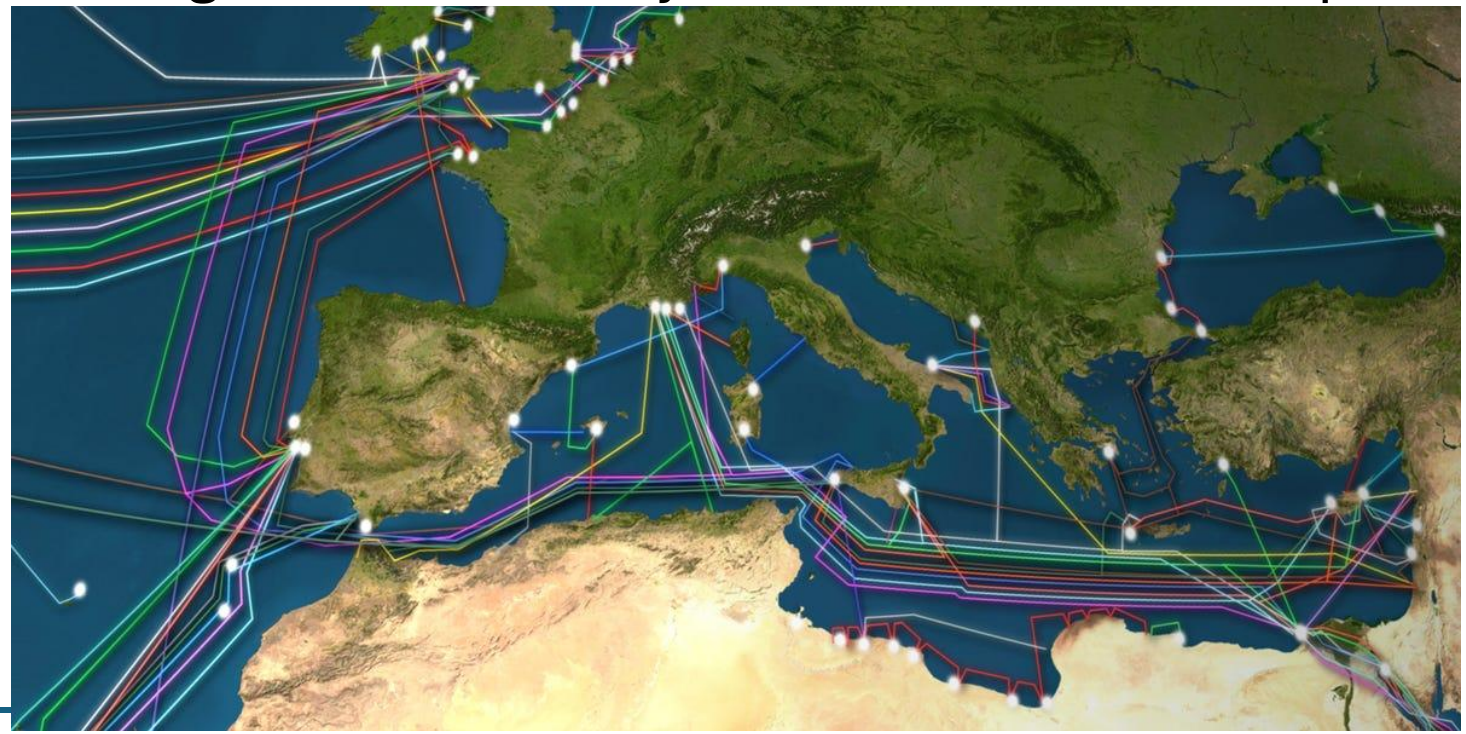
Security challenges in the implementation of national optical networks and modern broadcasting systems

Prof. Dr. Sc. Kire Jakimoski,
Head of Sector of Advanced Technologies,
Institute of Cybersecurity and Digital Forensics,
Military Academy "General Mihailo Apostolski" – Skopje,
University Goce Delcev, Stip, Republic of N. Macedonia

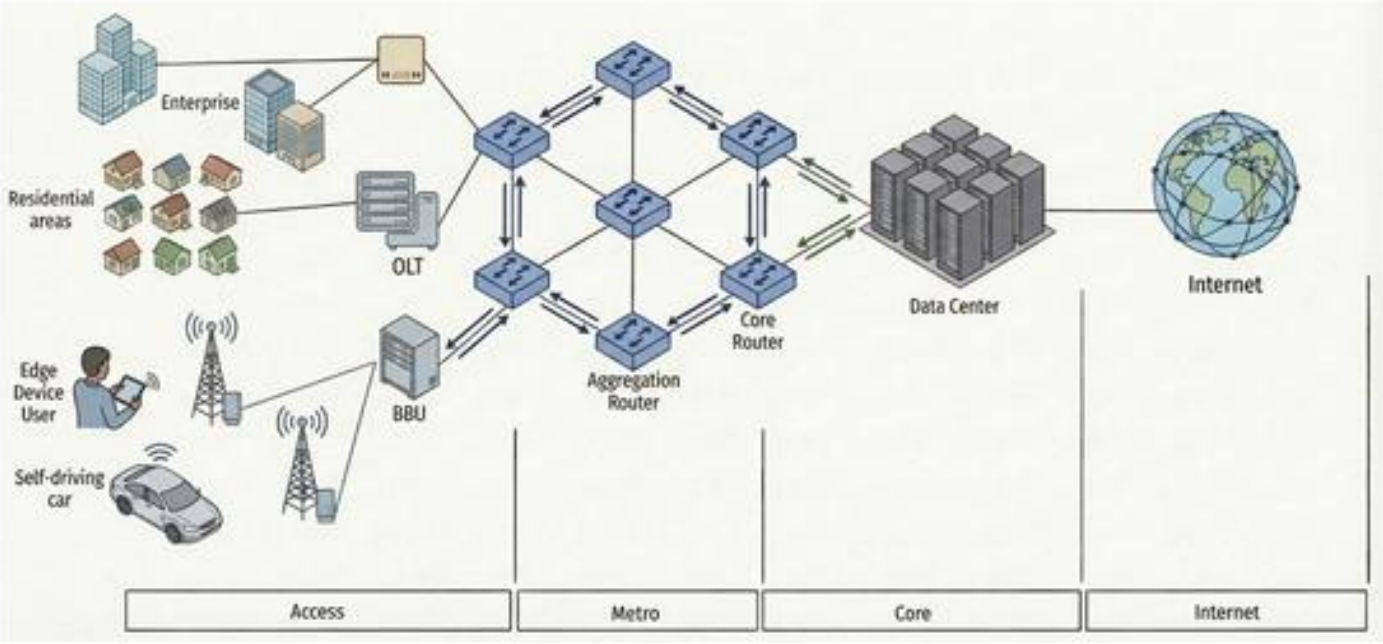
Global Status of Optical Network Security

- Historically, fiber-optic transmission was considered inherently more secure due to its closed nature and the assumption that tapping would cause easily detectable signal attenuation.
- Modern threat intelligence has entirely invalidated this assumption.



Global Status of Optical Network Security

- **Optical network cyber attacks** target the **physical and control layers** of fiber-optic infrastructure.
- While fiber is naturally **immune** to **electromagnetic eavesdropping**, attackers **exploit optical hardware vulnerabilities** through **physical tapping, signal interception,** and **control-plane manipulation** to steal data or severely disrupt critical communications.



High-level optical network architecture illustrating the access, metro, and core domains, along with representative components and interconnections.

Gazani, A., Mantzavinos, A., Tsompanoglou, P., Kantelis, K., Petridou, S., Nicopolitidis, P., & Papadimitriou, G. (2026). Optical Network Security: Threats, Techniques, and Future Directions. *Electronics*, *15*(4), 878.

Global Status of Optical Network Security

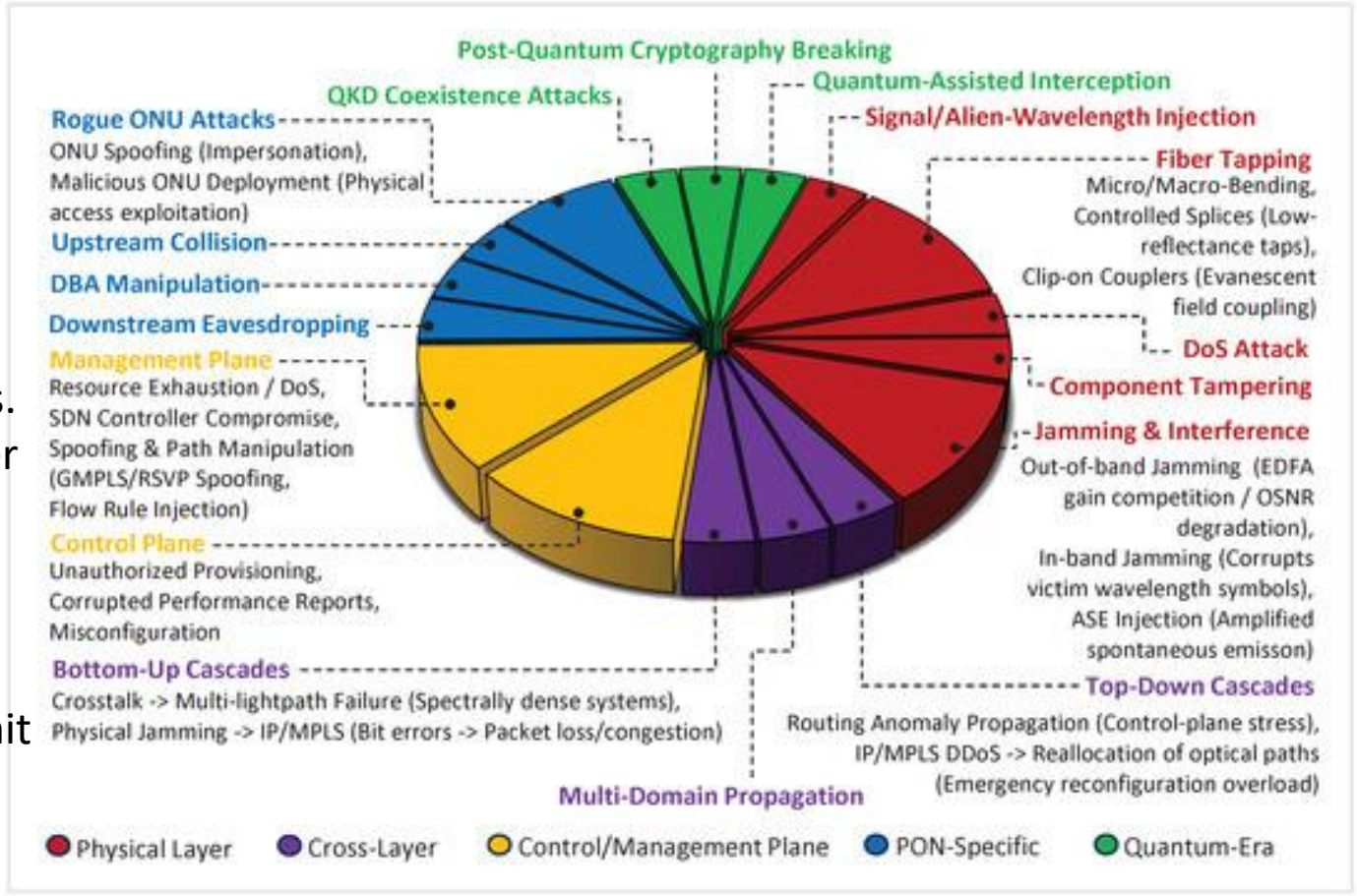
Key Attack Vectors

•**Fiber Tapping (Eavesdropping):** Attackers physically clamp onto a fiber-optic cable to bend the fiber slightly, leaking and capturing a small percentage of the light signal to extract confidential data undetected. [1, 2, 3]

•**Optical Jamming & Spoofing:** Threat actors inject continuous light signals into a fiber line or flood specific wavelengths (crosstalk exploitation) to disrupt, degrade, or completely block legitimate data transmissions (DoS). [1, 2, 3, 4, 5]

•**Control Plane Manipulation:** Modern software-defined networks (SDN) rely on automated management systems. Attackers target this software layer to reroute traffic, alter network topologies, or drop wavelengths. [1, 2]

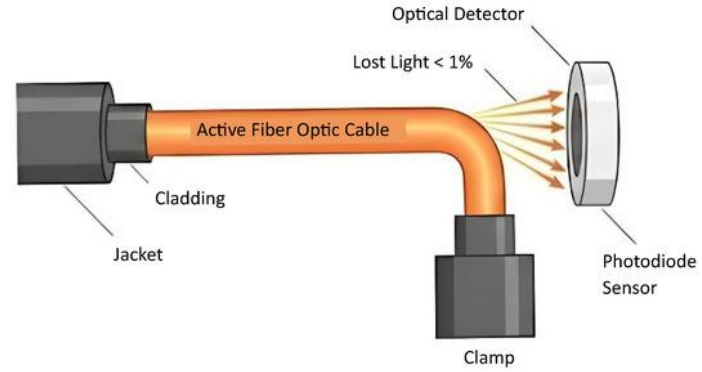
•**Man-in-the-Middle (MitM) Active Devices:** Malicious actors insert active optoelectronic devices between communicating nodes to intercept, modify, and retransmit traffic, compromising data privacy and integrity. [1]



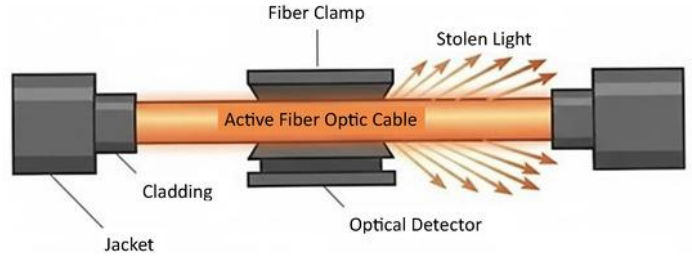
Physical Layer Vulnerabilities and Advanced Tapping

- Global military and intelligence actors have developed highly sophisticated, non-intrusive physical interception methods.
  - **Micro-Bending Exploits:** Modern tapping devices can capture sufficient escaping photons to reconstruct the data stream while introducing a negligible insertion loss of $\alpha \leq 0.1\ dB$.
  - Standard carrier network monitoring algorithms typically classify losses below $0.2\ dB$ as natural fiber aging or environmental temperature fluctuations, leaving the tap entirely undetected.

- ✓ Deploying G.657.A2 bend-insensitive fibers significantly reduces the success of fiber taps. These fibers resist micro-bending and limit light leakage, even in dense, complex urban deployments, preventing attackers from capturing usable signals.
- ✓ Using hardened, bend-insensitive fibers in both backbone and last-mile connections complements encryption efforts, providing a physical layer of security against data interception attempts.



(a) Bending-induced leakage enabling passive power diversion.



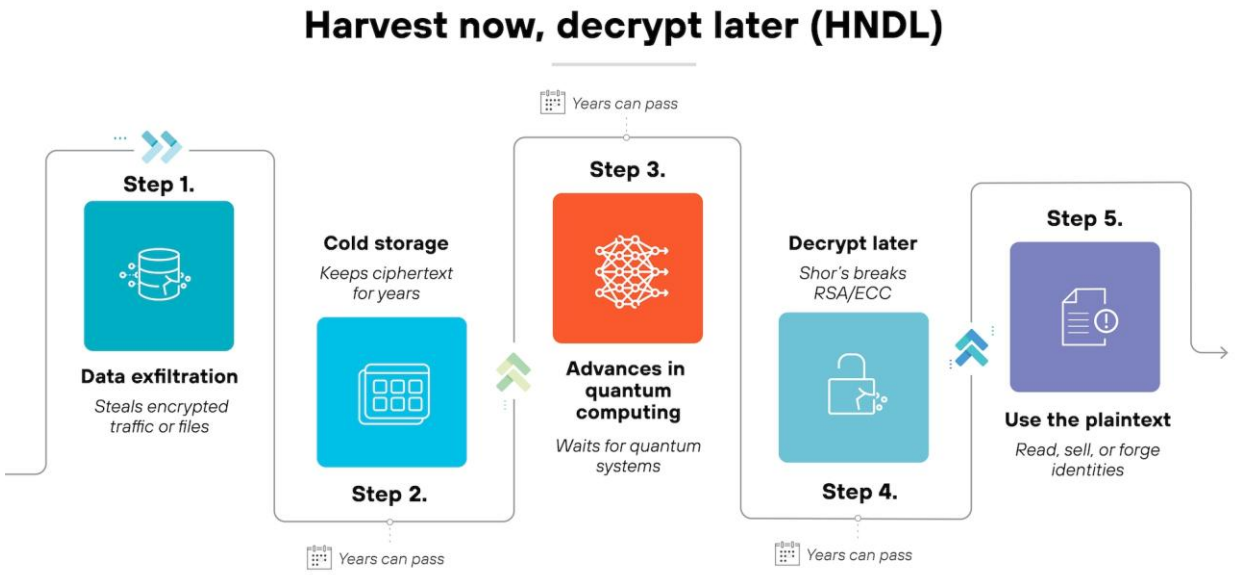
(b) Cladding-based tap using a non-intrusive fiber clamp or coupler.

Representative physical-layer eavesdropping mechanisms in optical fibers: (**a**) controlled micro-/macro-bending causing light leakage and (**b**) cladding-based tapping via external coupling devices

The Cryptographic Crisis: "Store Now, Decrypt Later" (SNDL)

- Adversarial nation-states are executing mass-harvesting operations on global optical transit corridors.
  - **SNDL Attack Vector:** Encrypted fiber-optic traffic is tapped, copied, and archived in massive sovereign data centers. Although current algorithms like AES-256 are mathematically secure against classical computing, the timeline to quantum vulnerability has accelerated.

- **The Quantum Threat:** Shor's Algorithm running on a cryptographically relevant quantum computer (CRQC) will factor prime numbers exponentially faster than classical computers, instantly breaking asymmetric algorithms (RSA, ECDH).



https://www.paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc

The Cryptographic Crisis: "Store Now, Decrypt Later" (SNDL)

- **Global Mitigation Status:** The global community is transitioning to a hybrid defense model:
  - **Post-Quantum Cryptography (PQC):** Standardizing mathematical algorithms (such as NIST's ML-KEM/Kyber and ML-DSA/Dilithium) that are resistant to both classical and quantum computation.
  - **Quantum Key Distribution (QKD):** Utilizing the physical principles of quantum mechanics (such as the Heisenberg Uncertainty Principle) to exchange cryptographic keys. Any attempt to tap or measure a quantum channel perturbs the quantum states:

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

Δx **(Uncertainty in Position):** Represents how precisely the position of a quantum particle (such as a photon or electron) is known.

Δp **(Uncertainty in Momentum):** Represents how precisely the momentum (or velocity) of that same particle is known.

$\hbar$ **(Reduced Planck's Constant):** A fundamental physical constant in quantum mechanics, equal to $h/2\pi$ (where h is Planck's constant). It sets the microscopic scale at which quantum effects become dominant.

  - This perturbation instantly collapses the superposition, altering the polarization state of the transmitted photons, thereby signaling to both endpoints that an interception is taking place.

Global Status of Optical Network Security

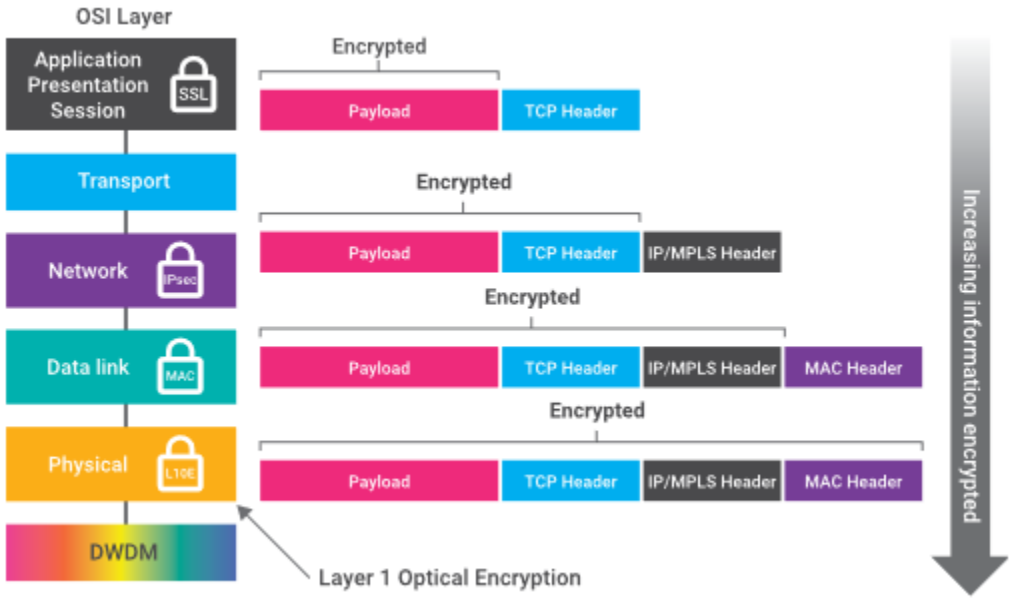
Common Detection & Defense Strategies

•**Optical Time Domain Reflectometry (OTDR):** Network operators use OTDR and inline optical spectrum monitoring to measure light loss, pinpointing the exact physical location of a fiber tap or cable break. [1]

•**Data Encryption:** Encrypting data at Layer 1 (Optical Transport Network) or using hardware-level MACsec ensures that even if a signal is intercepted or tapped, the data remains unreadable. [1, 2, 3]

•**Quantum Key Distribution (QKD):** Systems are increasingly using photonic integrated circuits for QKD, which relies on quantum mechanics to detect eavesdropping instantly when a photon's state is altered. [1, 2, 3]

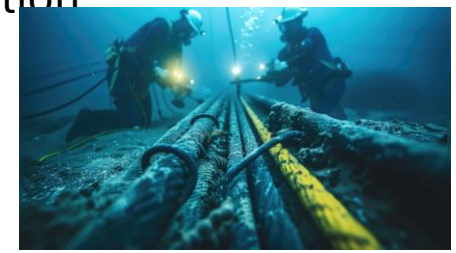
•**Multi-Path Routing (MPR):** Networks deploy instinct-reactive defense mechanisms, such as self-organizing dynamic routing, to reroute traffic away from degraded or compromised links automatically. [1]

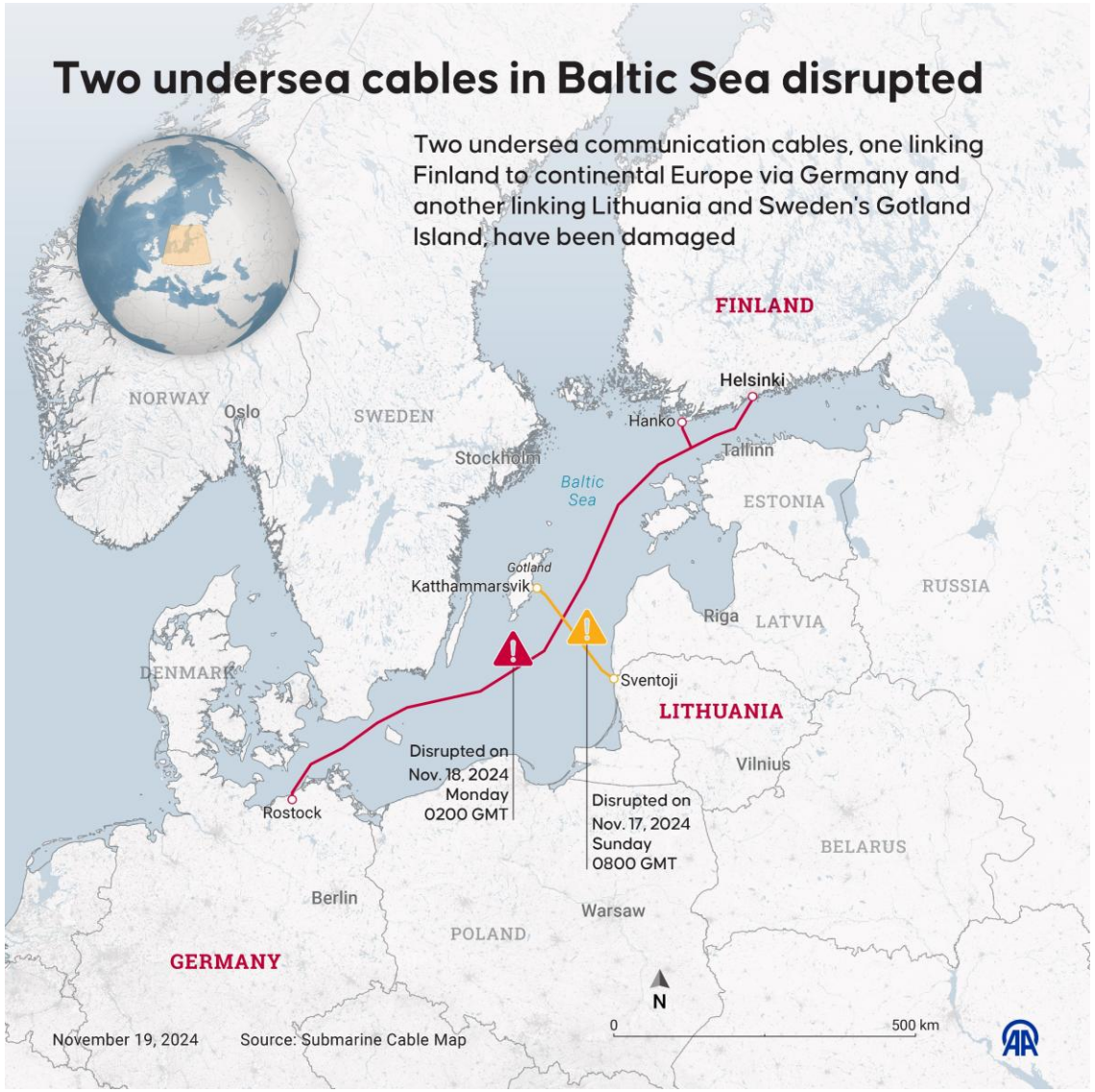


Optical Networks Attacks - Examples

- **Undersea and Ground Corridor Interdiction:** The dependency of global internet routing on tight physical pathways is a major systemic risk.
- Recent events:
  - severed Nord Stream Baltic connectors,
  - the Red Sea subsea cable cuts, and,
  - the July 2024 coordinated attacks on French domestic fiber paths.

They demonstrate that state-sponsored actors are mapping physical fiber junctions for both kinetic sabotage and deep signal interception





Optical Networks Attacks - Examples

- **Undersea and Ground Corridor Interdiction:** The dependency of global internet routing on tight physical pathways is a major systemic risk.
- Recent events:
  - severed Nord Stream Baltic connectors,
  - the Red Sea subsea cable cuts, and,
  - the July 2024 coordinated attacks on French domestic fiber paths.

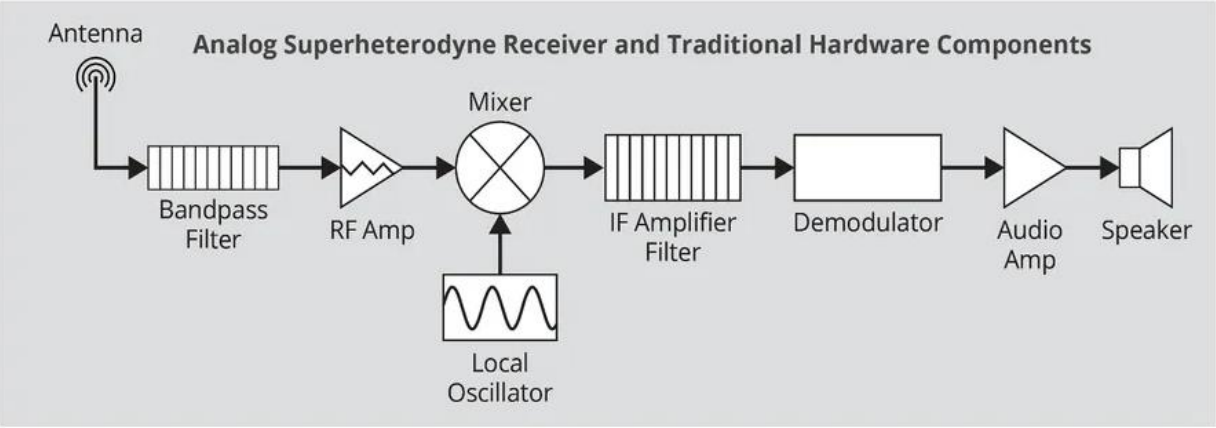
They demonstrate that state-sponsored actors are mapping physical fiber junctions for both kinetic sabotage and deep signal interception.

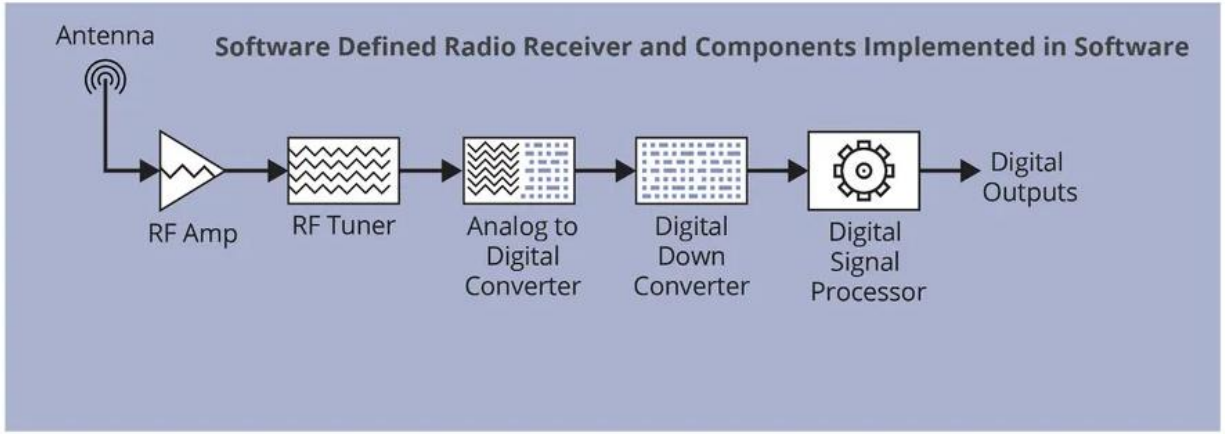
https://w.media/fibre-optic-cables-vandalised-in-france/

Modern Broadcasting Security Status
DAB+

- Traditional broadcasting was unidirectional (simplex), analog, and relied on expensive, highly specialized hardware. Today, modern digital broadcasting systems are **software-defined** and heavily dependent on **IP-based distribution networks**.

- **DAB+ (Digital Audio Broadcasting)** is increasingly **vulnerable** to **radio-frequency** and **network-level cyberattacks**.
- Because DAB+ is a wireless, **one-way broadcast** technology, it **lacks** native **internet return paths**, making **standard internet-based hacking impossible**.
- However, bad actors exploit vulnerabilities in the radio frequency (RF) broadcast chain and the complex software decoders installed inside modern "smart" receivers. [1, 2]





Modern Broadcasting Security Status
DAB+

Primary Attack Vectors

•**GPS/GNSS Spoofing & Jamming:** DAB+ operates on a Single Frequency Network (SFN), which relies heavily on precise timing. Attackers can use malicious signals to disrupt or spoof the synchronization systems, taking down regional broadcasts or inserting false emergency messages. [1]

•**Over-the-Air Data Injection (RF Attacks):** Because radio signals are inherently passive, hackers can transmit malicious data payloads (like crafted traffic or metadata packets) over the air. If a receiver or connected car's head unit has unpatched software vulnerabilities, it can be compromised when parsing these broadcasted files. [1, 2, 3]

•**Backend & Multiplex Infiltration:** Threat actors can gain unauthorized access to the studio-to-transmitter links (STL) or multiplexers. This allows them to hijack the digital stream to broadcast fake audio or manipulate Traffic Message Channel (TMC) and Electronic Program Guide (EPG) data. [1, 2]

Impact on Connected Vehicles

- Many modern vehicles have head units equipped with DAB+ and internet connectivity.
- Hackers can exploit vulnerabilities by sending corrupted DAB+ metadata or radio-frequency-enabled cyberattacks that target the vehicle's internal data buses.
- These attacks act as a “back door,” enabling malicious actors to bypass security systems and gain lateral access to the car's network, putting connected vehicle operations at risk. [1, 2, 3, 4]

Modern Broadcasting Security Status
DAB+

Defense & Mitigation

To combat these evolving radio-frequency threats, industry regulators and network operators implement strict resilience frameworks: [1, 2]

•**Robust Synchronization:** Broadcasters deploy anti-jamming and anti-spoofing GNSS receivers alongside multi-constellation antennas to maintain network reliability. [1]

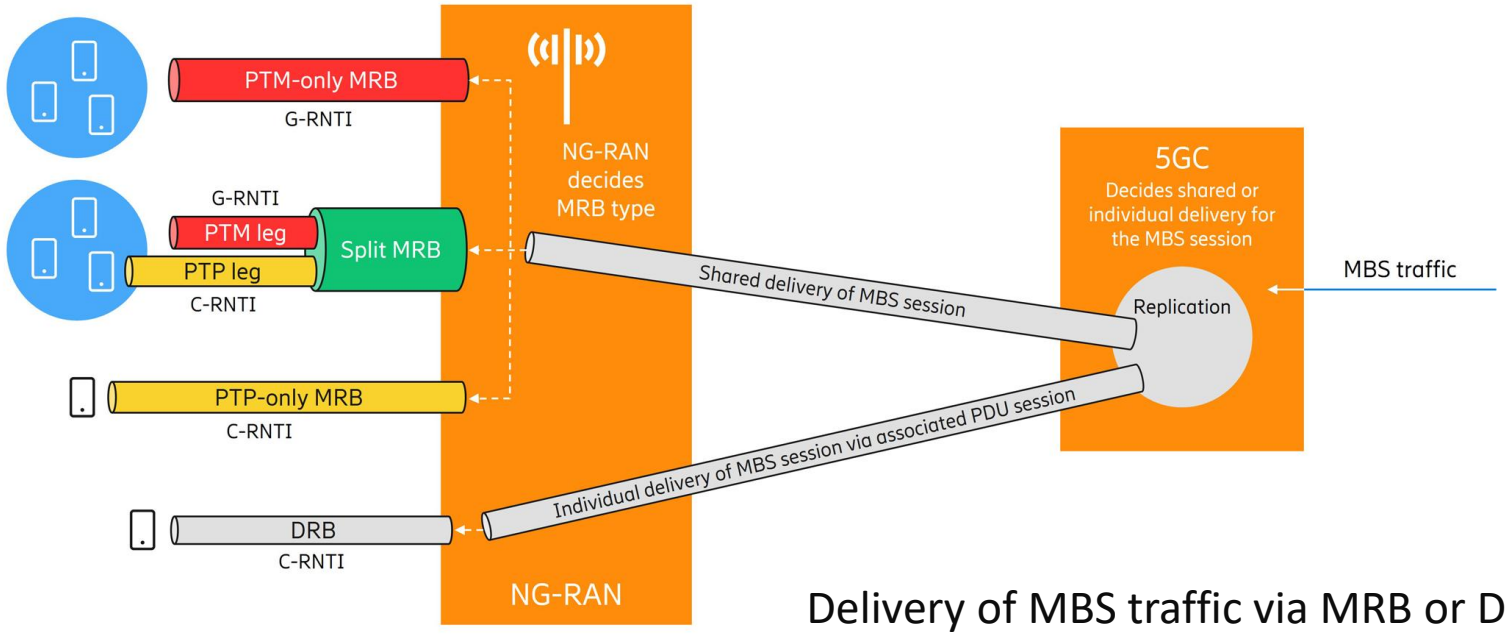
•**Secure Software Lifecycles:** Vehicle manufacturers and radio software developers conduct rigorous security testing to ensure head units do not execute malicious data when receiving standard over-the-air packets. [1, 2]

•**Automotive Sandboxing**: Vehicle manufacturers implement strict network segregation (sandboxing) between the infotainment head unit and the safety-critical CAN bus to isolate any malicious code originating from an RF broadcast.

Modern Broadcasting Security Status
5G Broadcasting

Cyber attacks on 5G broadcasting infrastructure target its unique architectural shifts—such as software-defined networking (SDN), edge computing, and cloud virtualization—expanding the network's attack surface far beyond traditional 4G boundaries.

- Because 5G broadcasting relies heavily on internet protocols (IP) and software-based components rather than dedicated hardware, it faces severe threats ranging from core system manipulation to over-the-air signal disruption. [1, 2, 3]



Delivery of MBS traffic via MRB or DRB radio bearer

https://www.ericsson.com/en/blog/2022/12/multicast-broadcast-group-communication

Modern Broadcasting Security Status

5G Broadcasting

Key Attack Vectors in 5G Broadcasting

The blend of traditional media distribution with cellular technology introduces specific entry points for cybercriminals:

•**Over-the-Air RF Jamming & Spoofing:** Bad actors can employ cheap, illegal RF jammers or construct fake 5G base stations to override legitimate broadcast signals. This can completely deny service or allow attackers to inject malicious data, unauthorized emergency alerts, or propaganda. [1, 2, 3]

•**Content Production Center Infiltration:** Because 5G Broadcast relies entirely on IP-based workflows, standard network reconnaissance and scanning malware can target media production facilities. Attackers can execute Advanced Persistent Threats (APTs) to disrupt real-time media feeds before they reach the transmitter. [1, 2, 3]

•**Control-Plane Exploits:** Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) are foundational to 5G infrastructure. Malicious software loops or configuration errors can be exploited to cause a Denial of Service (DoS) across the broader broadcasting network. [1, 2, 3, 4, 5]

•**GTP-U Tunnel Abuse:** Attackers can compromise edge nodes or physical devices to abuse the GPRS Tunneling Protocol (GTP-U). By injecting rogue packets directly into the tunnel between the base station and the user plane, they can cause network crashes or force user modems to downgrade to vulnerable older networks. [1, 2]

•**Supply Chain Interceptions:** The hardware and software components powering 5G transmitters (antennas, edge routers, and encoders) originate from global vendor ecosystems. Intercepted supply chains can result in hardcoded backdoors or unpatched, hidden system vulnerabilities. [1, 2]

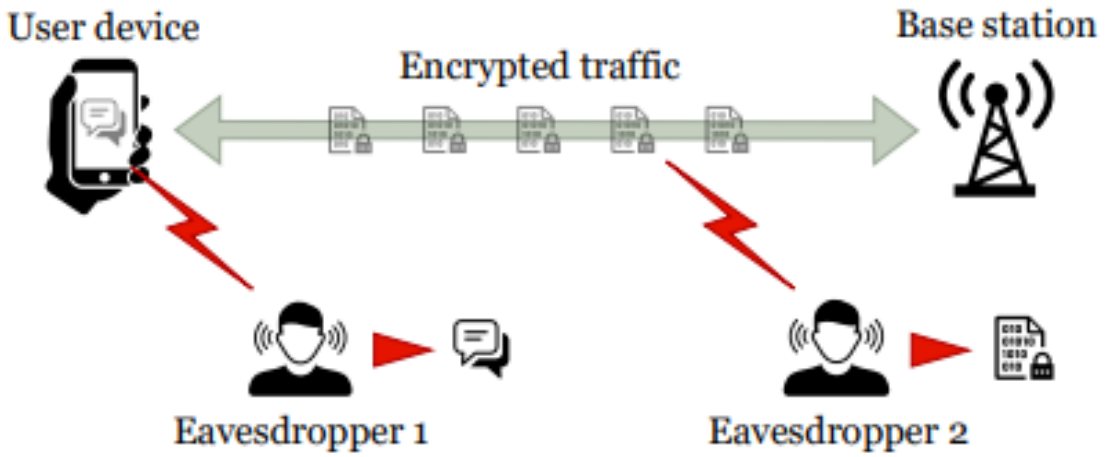
Modern Broadcasting Security Status - 5G Broadcasting

Consequences of Successful Attacks

Widespread Media Blackouts: Distributed Denial of Service (DDoS) attacks amplified by 5G's massive bandwidth can overwhelm edge resources, cutting off entire cities from critical live updates and news. [1, 2, 3]

Data Interception and Fingerprinting: Sophisticated passive network sniffing, while technically difficult due to 5G beamforming, can still allow adversaries to map out user locations and capture unprotected user data or device identifiers. [1]

Manipulation of Public Safety Data: If an attacker successfully compromises the integrity of a broadcast stream, they can broadcast fraudulent public alerts, sparking panic or disrupting regional stability. [1, 2, 3, 4]

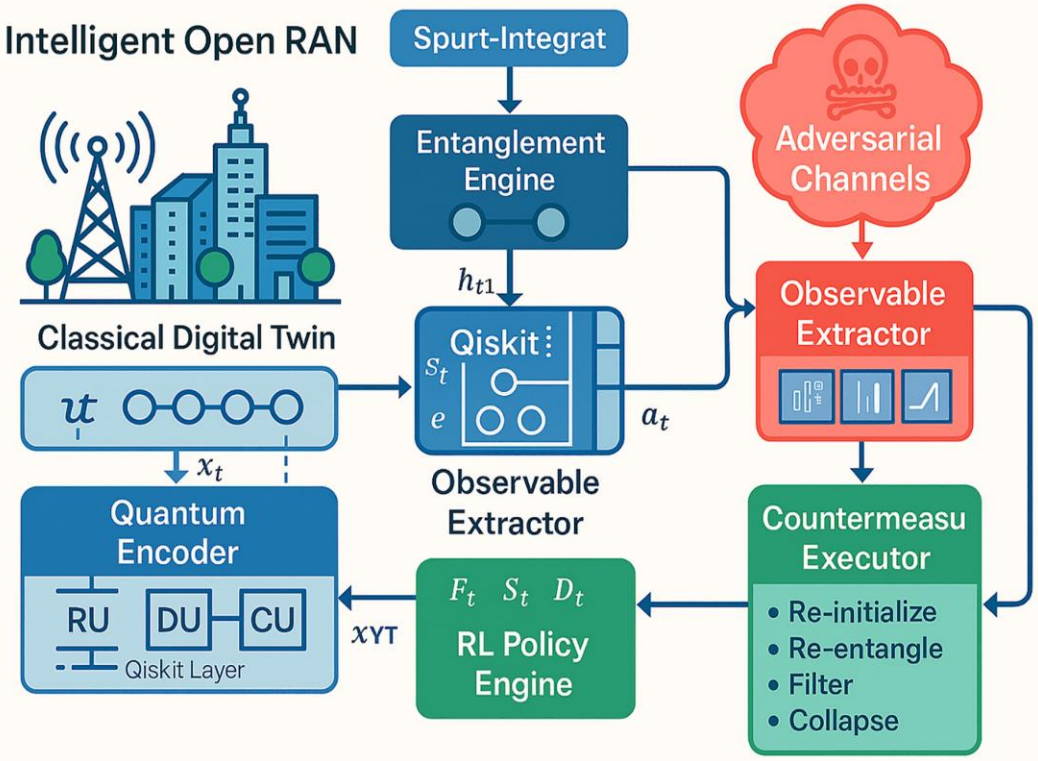


Modern Broadcasting Security Status - 5G Broadcasting

Emerging Security Countermeasures

To combat these threats, standard network security is pivoting toward automated, intelligent mechanisms: [1, 2, 3]:

- **Network Deception Systems (RDS):** Deployed inside production centers, these systems build virtual network topologies to trick and stall automated scanning tools, identifying threats before they hit critical broadcast nodes.
- **AI-Driven Digital Twins:** Advanced frameworks like *TwinGuard* utilize AI and digital network copies to detect and instantly block control-plane attacks in under 100 milliseconds.
- **Zero-Trust & Strict Isolation:** Implementing airtight network slicing ensures that if a general data network segment is compromised, the high-priority broadcasting slice remains entirely insulated. [1, 2, 3, 4]



Cybersecurity Driven Quantum Digital Twin for Proactive Threat Reversal in Open RAN https://doi.org/10.1049/qtc2.70027

The AI Offensive & Cognitive Warfare

The incorporation of Artificial Intelligence (AI) into the threat landscape has transformed localized cyber incidents into highly automated, systemic operations.

Phase	**1. Automated Reconnaissance**	**2. Deepfake Synthesis**	**3. Broadcast Path Breach**
Objective	Target Discovery	Payload Development	Infrastructure Injection
Mechanism	Automated vulnerability mapping of weak 5G Core architecture and open SBA interfaces.	Generative AI models clone a leadership figure's voice using captured open-source audio.	Unauthorized access to the service bus to inject the cloned payload directly into the Cell Broadcast Centre Function (CBCF) or multiplexer (MUX).
Impact	"Exposes vulnerable Service-Based Architecture (SBA) API endpoints.	Creates high-fidelity, weaponized media.	Compromises cell broadcast schedules to distribute fraudulent data.

The AI Offensive & Cognitive Warfare

AI-Driven Infrastructure Reconnaissance

- State-sponsored hacking groups use specialized Machine Learning (ML) algorithms to crawl public records, road construction permits, and network BGP (Border Gateway Protocol) routing tables.
- These AI agents autonomously reconstruct the exact physical layout of a nation's optical backbone, identifying critical choke points (such as shared bridges or minor regional switching hubs) where a physical cut will cause maximum regional disruption with minimal footprint.

AI Deepfake Synthesis and Broadcast Injection

- The primary objective of modern hybrid warfare is **Cognitive Warfare**—influencing the perception and decision-making of a targeted population.
  - **The Cloned Voice Vector:** Generative AI voice cloning requires only a few seconds of clean reference audio (often harvested from public speeches) to generate highly authentic, synthetically cloned audio.
  - **The Ultimate Hijacking Scenario:** In a crisis, an adversary breaches a DAB+ EDI link or a 5G Broadcast control plane, injecting an AI-cloned message of the President or Military Command declaring a false surrender or a fake evacuation order. By bypassing internet social media platforms (which can be blocked or debunked quickly) and utilizing the trusted, high-availability over-the-air broadcast network, adversaries can trigger immediate, systemic public panic.

An example of a sophisticated AI attack

As the Chief Risk Officer (CRO) of a large CRO with an international structure, you manage the consequences of a highly sophisticated security intrusion.
A Treasury officer approved a $10 million wire transfer after a video conference with a person who appeared to be the Regional President.
Post-incident forensics revealed that the video was a high-fidelity synthetic production (deepfake) that bypassed corporate biometric liveness detection and mimicked the executive's specific speech patterns.
At the same time, similar synthetic media was posted on social media to spread misinformation regarding the firm's liquidity, causing a temporary decline in the share price."

Liveness detection is an advanced security technology (commonly based on artificial intelligence and computer vision) used in biometric systems to verify that a biometric sample—such as a face, voice, or fingerprint—comes from a real, living human being, rather than from an artificial reproduction.
Its primary purpose is to prevent so-called spoofing attacks. Without live detection, the most common biometric facial recognition system could be unlocked simply by displaying a user's photo on paper or a video played from another phone.

An example of a sophisticated AI attack

- This scenario is a classic example of **Emerging Threat — artificial intelligence** allows an attack to be carried out on multiple fronts at once, combining **social engineering, cybercrime, and economic sabotage**.

Global Regulatory and Standardization Responses

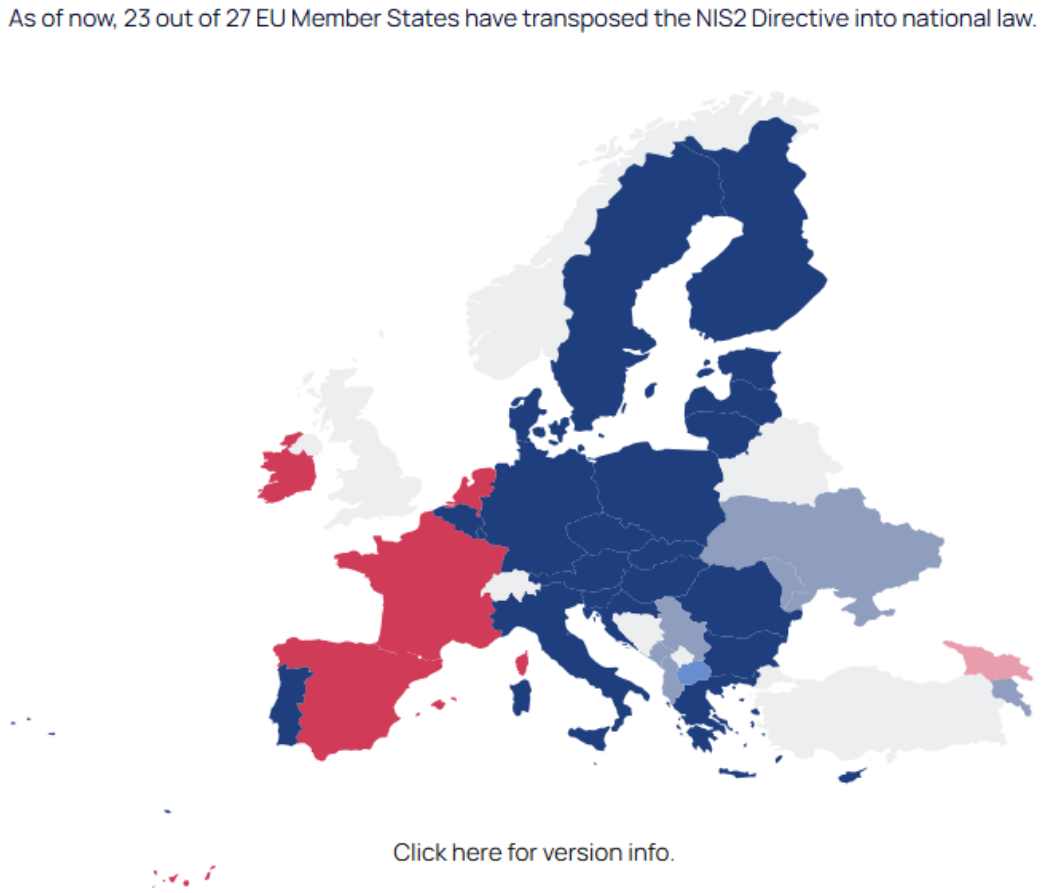
- To defend against these emerging threats, international bodies have updated their regulatory frameworks to enforce strict critical infrastructure security.

The European Union: NIS2 Directive

The **Network and Information Security (NIS2) Directive** dramatically expands security mandates across critical sectors in Europe, including telecommunications and public broadcasting.

- **Sovereign Accountability:** Under NIS2, executive management boards are directly liable for cybersecurity negligence.
- **Incident Reporting:** Critical operators must issue an early warning within **24 hours** of detecting a significant incident, followed by a detailed notification within **72 hours**.

Supply Chain Security: Telecommunications and broadcasting companies must vet their entire vendor list, directly targeting the elimination of high-risk suppliers from critical networks.



Global Regulatory and Standardization Responses

- To defend against these emerging threats, international bodies have updated their regulatory frameworks to enforce strict critical infrastructure security.

ITU-T and 3GPP Standard Protocol

•**ITU-T SG17 (Security):** Actively publishing standards for transport network security, including guidelines for securing DWDM systems against optical-tapping methods.

https://www.itu.int/en/ITU-T/about/groups/2025-2028/Pages/sg17.aspx

3GPP Security Group (SA3): Formulating strict cryptographic validation mechanisms for 5G Broadcast, ensuring that future mobile devices can cryptographically verify the signature of over-the-air cell broadcasts before rendering them to the end-user.
https://www.3gpp.org/3gpp-groups/service-system-aspects-sa/sa-wg3

Global Regulatory and Standardization Responses

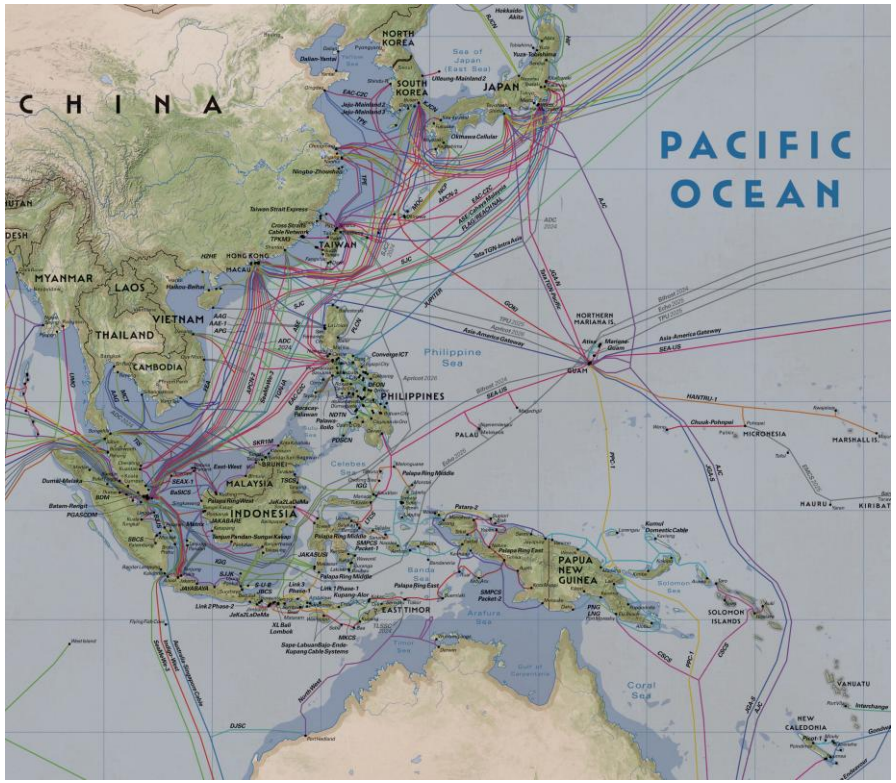
➢ To defend against these emerging threats, international bodies have updated their regulatory frameworks to enforce strict critical infrastructure security.

United States: CISA Guidelines and the National Quantum Strategy

- **CISA** secures subsea and terrestrial fiber-optic backbones by evaluating security risks, mitigating foreign ownership threats, and setting national resilience standards. The **Cybersecurity and Infrastructure Security Agency (CISA)** works alongside the **FCC** and the interagency Committee for the Assessment of Foreign Participation in the United States Telecommunications Services (colloquially known as "Team Telecom") to safeguard global telecommunications infrastructure.

- **The Quantum Computing Cybersecurity Preparedness Act:** Enforces mandatory migration of federal agencies and critical defense contractors to Post-Quantum Cryptography (PQC) standards specified by NIST.

https://www.congress.gov/bill/117th-congress/house-bill/7535/text



Submarine Cable Map 2024/TeleGeography
This regional snapshot of the web of subsea cables in the Indo-Pacific displays at once both the interdependence and vulnerability of these systems

https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

Recommendation for National Defenses

For nations seeking to secure their optical and broadcasting sovereign assets, a three pillars defense strategy is recommended: