Detection, Response and Mitigation of Hybrid Threats to Telecommunications Infrastructures

A Technical Deep Dive for EU Telecom Security

Ioan Constantin
Orange Romania

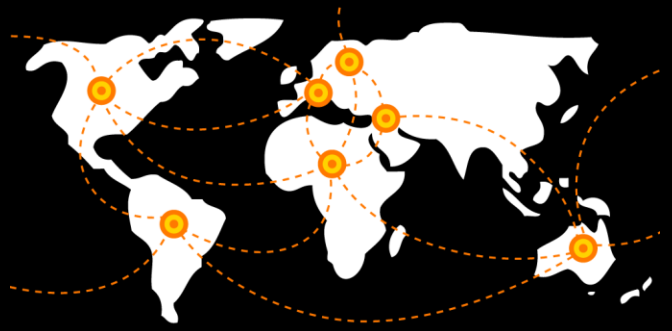


Table of Contents

1. Understanding Hybrid Threats
2. Threat Landscape in the EU
3. Detection Mechanisms
4. Response Strategies
5. Mitigation and Future Directions
6. Conclusion

Part 1

Understanding Hybrid Threats



What are Hybrid Threats?
Definitions, Examples, and Relevance to Telecom

Definition
- Hybrid threats combine cyber, physical, informational, and psychological tactics.
- Aim to disrupt, degrade, or manipulate critical infrastructure.

Examples
- Coordinated DDoS attacks with physical sabotage.
- Disinformation campaigns targeting telecom reliability.

Relevance to Telecom
- Telecom is a backbone for critical services and national security.
- Hybrid threats exploit both digital and physical vulnerabilities.

Key Characteristics of Hybrid Threats

Blending Multiple Attack Vectors



Multi-Vector Attacks

Simultaneous use of cyber, physical, and informational tactics to overwhelm defenses and evade detection.



Stealth and Persistence

Long-term, low-profile operations that exploit weak signals and blend with legitimate activity.



Cross-Border Coordination

Threat actors often operate across jurisdictions, complicating attribution and response.



Disinformation Integration

Use of social engineering and media manipulation to amplify technical attacks.



Supply Chain Exploitation

Targeting vendors and service providers to introduce vulnerabilities into telecom infrastructure.

EU Telecom Infrastructure: Vulnerabilities
Critical Components and Weaknesses

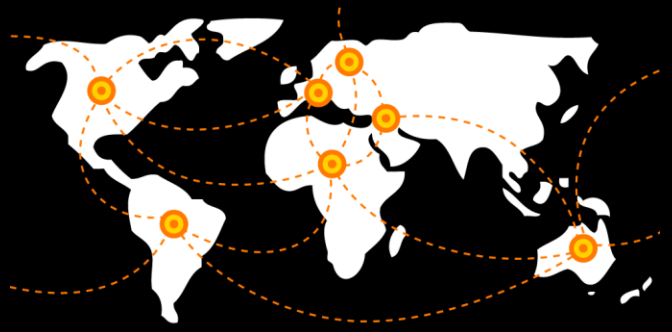
Core Components
- Backbone networks (fiber, microwave, satellite)
- Mobile and fixed access networks
- Data centers and cloud interconnects

Vulnerabilities
- Legacy systems with unpatched software
- Interdependencies with energy and transport
- Exposure to supply chain risks
- Insider threats and privileged access abuse

Impact
- Service disruption, data exfiltration, and loss of trust.

Part 2

Threat Landscape in the EU



Recent Hybrid Attacks on EU Telecom

- 2022: Coordinated DDoS and physical sabotage on fiber lines in Eastern Europe.
- 2023: Disinformation campaigns targeting 5G rollout safety, combined with ransomware attacks on mobile operators.
- 2024: Supply chain compromise via third-party network equipment vendors.

Technical Analysis:

- Attackers used advanced persistent threat (APT) tactics, leveraging zero-days and lateral movement.
- Physical attacks synchronized with peak network loads to maximize disruption.



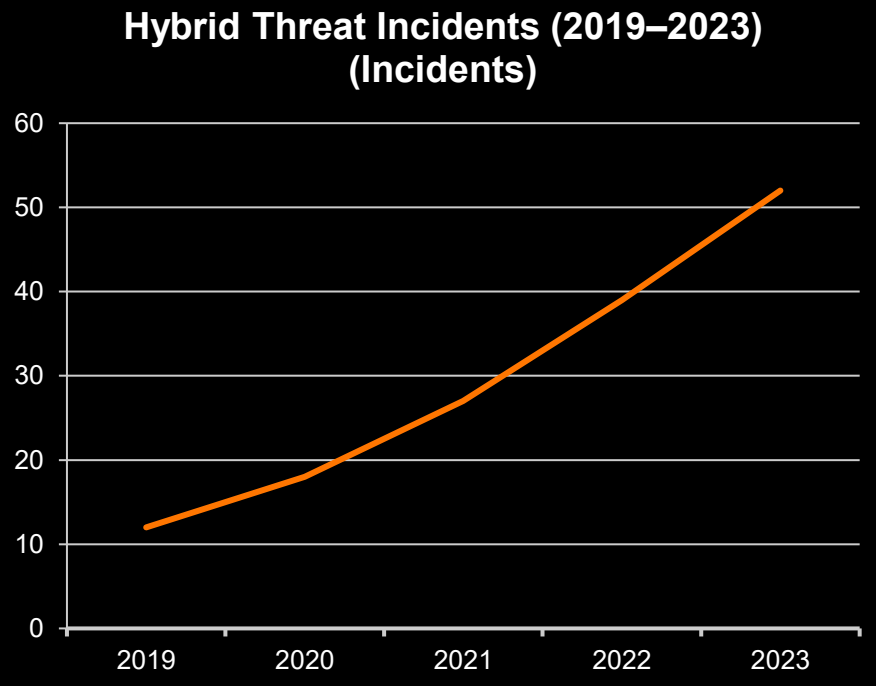
Attack Vectors and Techniques
Mapping Threats to Telecom Layers

Layer	Cyber Techniques	Physical Techniques	Informational Techniques
Core Network	DDoS, BGP hijacking	Cable cutting, arson	Fake outage reports
Access Network	Malware, MITM	Vandalism, theft	Social engineering
Data Center/Cloud	Ransomware, privilege escalation	Power sabotage, intrusion	Phishing, misinformation
Supply Chain	Firmware backdoors	Tampering, theft	Vendor impersonation

Threat Evolution in the Last 5 Years

- Significant increase in hybrid incidents targeting telecom infrastructure since 2019.
- Notable spikes during geopolitical tensions and major events (e.g., elections, pandemics).
- Technical sophistication and automation of attacks have grown.

Graph: Incident counts by year (2019–2023)



Part 3

Detection Mechanisms

Orange restricted

Technical Approaches to Detection
SIEM, Anomaly Detection, Threat Intelligence

SIEM (Security Information and Event Management)
- Aggregates logs and events for real-time analysis.
- Correlates multi-source data to detect hybrid patterns.

Anomaly Detection
- Uses statistical models and machine learning to flag deviations from baseline behavior.
- Effective for detecting stealthy, persistent threats.

Threat Intelligence
- Integrates external feeds (IoCs, TTPs) for proactive defense.
- Enables early warning and contextual analysis.

Key Detection Technologies

Tools and Methods for Telecom Security



IDS/IPS

Intrusion Detection and Prevention Systems monitor network traffic for malicious activity and policy violations.



AI/ML Analytics

Machine learning models identify subtle anomalies and emerging threats in large-scale telecom data.



Network Monitoring

Continuous packet and flow analysis to detect abnormal patterns and lateral movement.



Threat Intelligence Platforms

Centralize and correlate threat data from multiple sources for actionable insights.



Endpoint Detection & Response

Monitors endpoints for suspicious activity, enabling rapid containment and forensics.

Detection Tools Comparison

Open Source vs. Commercial Solutions

Tool/Platform	Type	Features	Pros	Cons
Suricata	Open Source	IDS/IPS, protocol analysis	Flexible, community support	Requires tuning
Splunk	Commercial	SIEM, analytics, dashboards	Scalable, integrations	Cost, complexity
Zeek	Open Source	Network analysis, scripting	Customizable, detailed logs	Steep learning curve
Darktrace	Commercial	AI-driven anomaly detection	Autonomous response	Expensive, opaque models
MISP	Open Source	Threat intelligence sharing	Collaborative, extensible	Needs integration effort

Part 4

Response Strategies



Incident Response Frameworks
NIST, ENISA, and Custom Models

NIST Framework

- Preparation, detection, containment, eradication, recovery, post-incident.

ENISA Guidelines

- EU-specific best practices for telecom resilience and incident reporting.

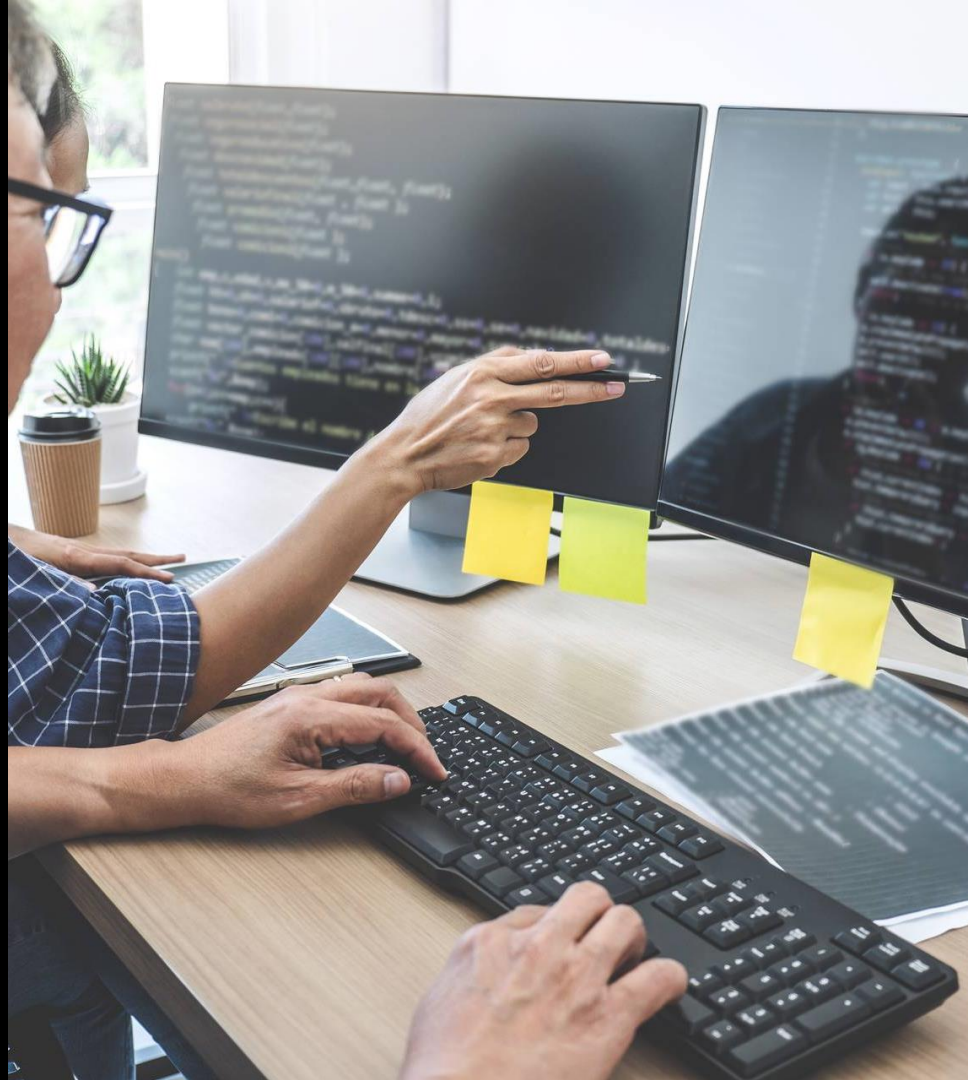
Custom Models

- Telecom-specific playbooks for hybrid threats.
- Integration with national CERTs and sectoral ISACs.

Technical Steps in Incident Response

- Detection & Analysis: Correlate alerts, validate incidents, assess scope.
- Containment: Isolate affected segments, block malicious traffic, disable compromised accounts.
- Eradication: Remove malware, close vulnerabilities, patch systems.
- Recovery: Restore services, validate integrity, monitor for recurrence.
- Post-Incident: Forensics, lessons learned, update playbooks.

Best Practice: Automate containment and recovery where possible.



Real-World Response Metrics

Measuring Effectiveness in Telecom Security



MTTD: 8 min

Mean Time to Detect (MTTD) for advanced hybrid attacks in leading EU telecom operators.

Restreint Orange



MTTR: 42 min

Mean Time to Respond (MTTR) from detection to containment and mitigation.

92%

Incidents contained before major service disruption when automated response is deployed.

Part 5

Mitigation and Future Directions



Advanced Mitigation Techniques
Zero Trust, Segmentation, Supply Chain Security

Zero Trust Architecture
- Enforce least privilege, continuous authentication, micro-segmentation.

Network Segmentation
- Isolate critical assets, limit lateral movement, enforce strict access controls.

Supply Chain Security
- Vet vendors, require SBOMs, monitor for tampering, implement contractual security clauses.

EU Policy Alignment
- NIS2 Directive, GDPR, and sectoral regulations for telecom resilience.

Research & Innovation in Mitigation

Academic and Industry Trends



AI-driven Defense

Adaptive machine learning models for real-time threat prediction and mitigation.



Quantum-safe Cryptography

Research into post-quantum algorithms to secure telecom communications.



Automated Orchestration

SOAR platforms for automated incident response and mitigation workflows.



Collaborative Threat Sharing

Federated platforms for sharing indicators and response strategies across the EU.



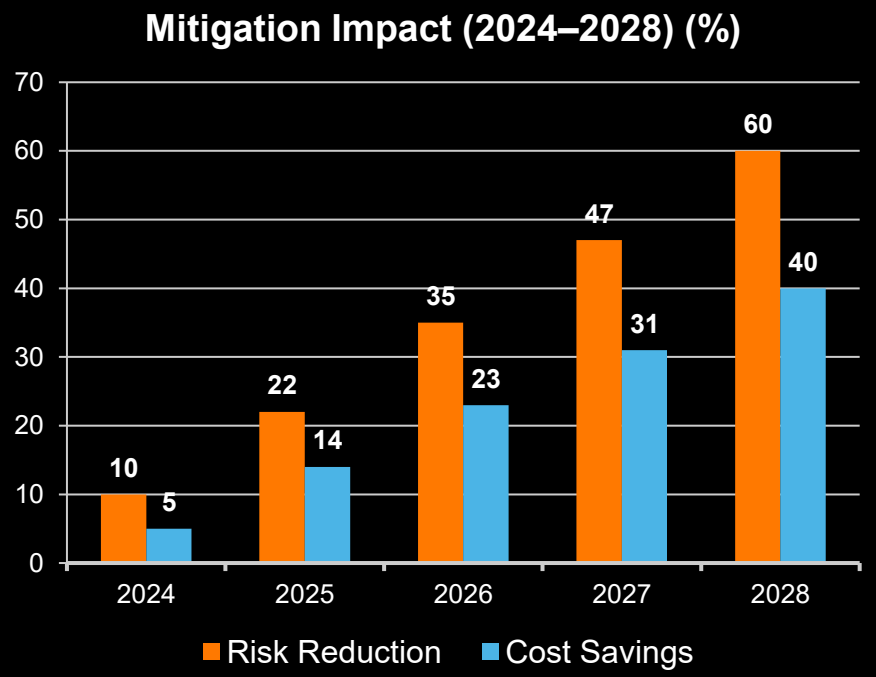
Resilience Engineering

Designing telecom systems for rapid recovery and self-healing under attack.

Projected Impact of Mitigation

- Adoption of advanced mitigation strategies is expected to reduce incident impact and operational costs.
- Quantitative projections based on EU telecom sector studies.

Graph: Risk reduction and cost savings from 2024–2028



Thank you

