Cyber Resilience and PPDR

Reference Document

PSCEurope
Public Safety Communication Europe

fidal field trials beyond 5G

Cyber Resilience and PPDR

Reference Document

PSCEurope
Public Safety Communication Europe

fidal field trials beyond 5G

Contents

Figures

1 Why Cyber Resilience Matters for PPDR

1.1. The PPDR Ecosystem

The PPDR (Public Protection and Disaster Relief) refers to the emergency services, public safety agencies, and communication systems used to protect people and respond to major incidents such as fire, floods, terrorism, accidents, or natural disasters. PPDR intertwines with discussions surrounding cellular networks, broadband communications, and emergency coordination systems that are utilised across Europe.

Figure 1 PPDR Ecosystem Examples

While this document focuses primarily on PPDR communication networks and the underlying ecosystem, the cyber resilience principles discussed are directly applicable to any large-scale, mission-critical communications infrastructure operating under elevated threat conditions. Temporary or event-driven networks, such as the one deployed to support the Paris 2024 Olympics, share many of the defining characteristics of PPDR networks.

1.2. Why PPDR Resilience Matters

Resilience matters in PPDR systems because they must remain operational during major disasters such as flooding, wildfires, terrorist attacks, power outages, storms, or cyberattacks. Ultimately, people's lives depend on the continuous communication these networks offer and networks not being resilient can result in increased response time and increased casualties. In PPDR systems, resilience planning must assume compromise can happen through intentional attacks or unintentional attacks, as shown in Figure .

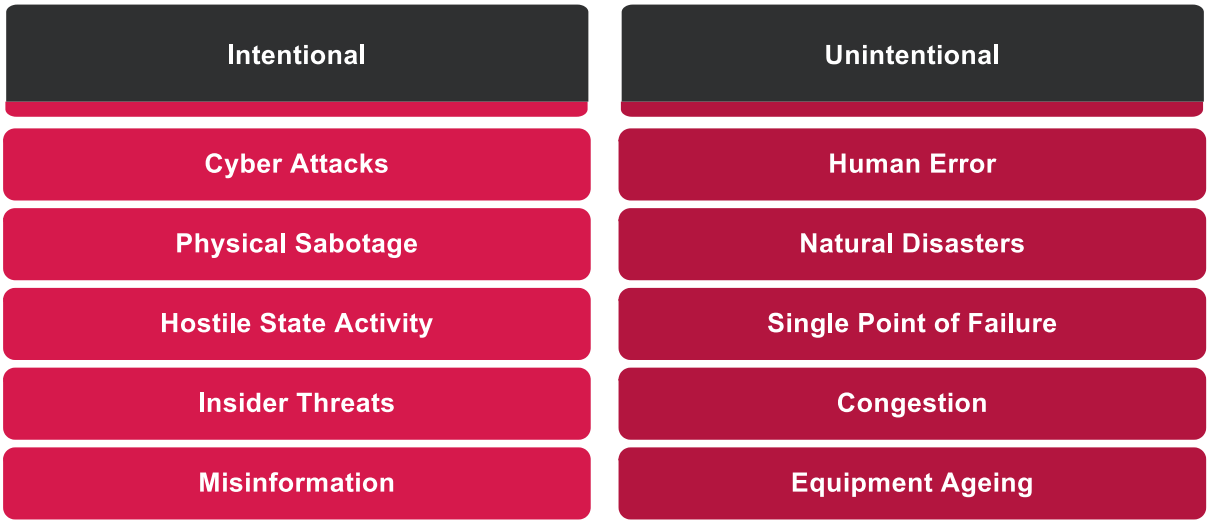

Figure 2 Risk Factors and Attack Types

Cyber Security vs. Cyber Resilience

In the context of PPDR, cybersecurity and cyber resilience are both essential but serve different purposes; cybersecurity focuses on protecting critical communication networks from threats such as hacking, ransomware, unauthorised access, and malware. It aims to prevent or reduce the likelihood of compromise through security measures such as encryption, identity control, monitoring, patching, and secure-by-design principles.

Cyber resilience takes this concept one step further by recognising that some attacks, failures, and disruptions can occur, especially during major emergencies where PPDR systems are under strain. Therefore, cyber resilience focuses on ensuring that emergency services can continue to operate during a cyber incident by implementing redundancy, failover systems, disaster recovery plans, and manual fallback procedures. As shown in Figure 3, cyber resilience consists of four key characteristics.

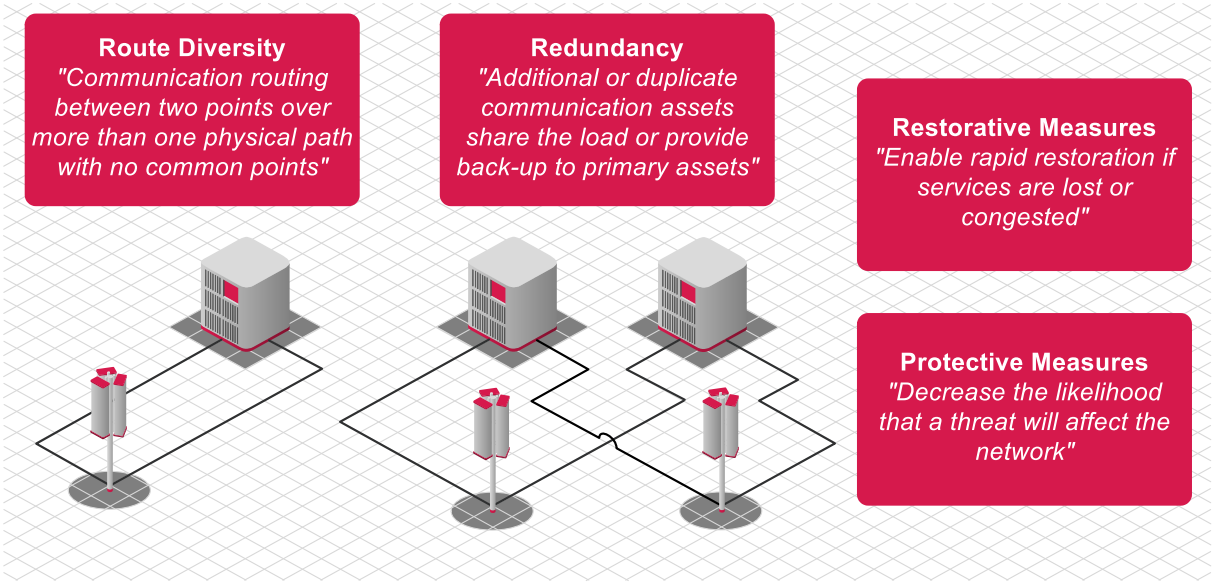

Figure 3 Cyber Resilience Key Characteristics

1.3. Challenges for Availability and Continuity

A familiar reliability benchmark for availability and continuity in public telecommunications networks is the concept of “five nines”, referring to 99.999% availability, which is the equivalent of 5 minutes 16 seconds of downtime per year or 26 seconds per month. 5G networks can take this to even higher levels of reliability, with six nines and even seven nines reliability a requirement in some networks (particularly private industrial settings).

PPDR availability and continuity discussions focus more on maintaining access, as a single site failing at a critical location during a major incident is an unacceptable outcome, regardless of how well every other site performs. Secondly, the timing of any failure matters enormously. Five minutes of downtime spread across a year in a quiet overnight period is categorically different from five minutes of downtime at the peak of a major incident; therefore, we should not be applying commercial SLAs as benchmarks for PPDR networks.

Implications of Cloud and Multi-homing

With the transition away from legacy TETRA (Terrestrial Trunked Radio) and P25 (Project 25) towards 4G/5G-based mission-critical services, PPDR operators are deploying or procuring core network functionality run on cloud-based infrastructure. This shift creates important availability and continuity benefits but also introduces new categories of risk and design complexities. Cloud infrastructure itself relies on power, cooling, and physical connectivity that may fail during the very incident that PPDR is designed to respond to. Moreover, software-defined infrastructure introduces the risk of software-layer failures.

Multi-homing refers to the connection of a device, service, or network node to multiple independent network paths or providers simultaneously, so that traffic can be rerouted if one path fails. At the device level, modern handsets and vehicle-mounted terminals increasingly support simultaneous connectivity across multiple bearers as shown in Figure 4. The 3GPP ATSSS (Access Traffic Steering, Switching, and Splitting) architecture provides a standardised framework for managing this multi-path connectivity, enabling availability and continuity.

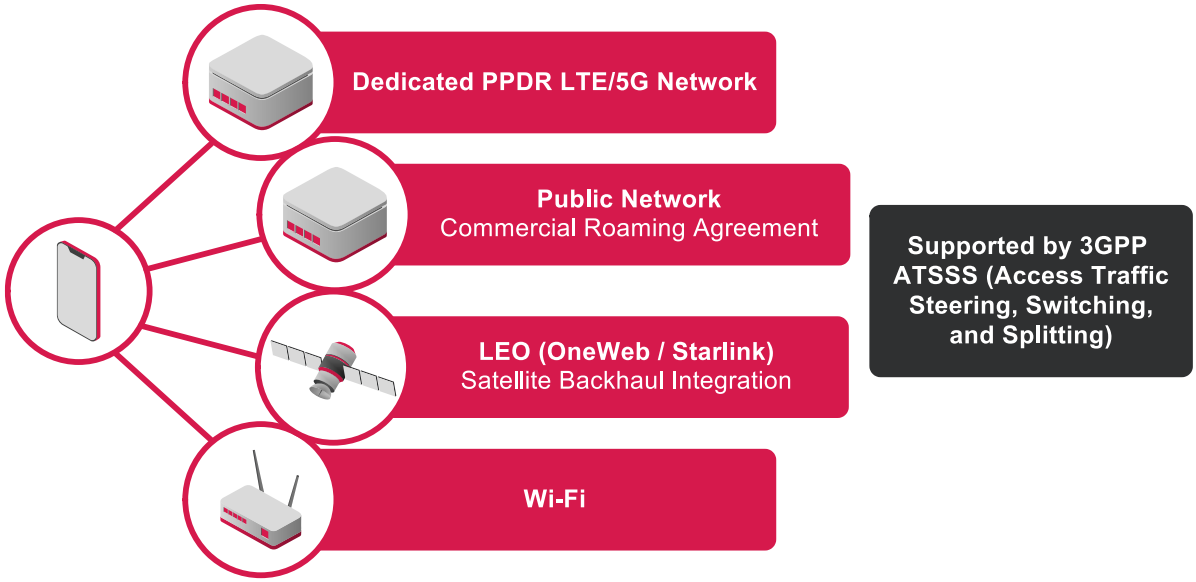

Figure 4 Multi-homing

Sovereignty & Cross-border Issues

PPDR networks are increasingly relying on commercial cloud infrastructure and cross-border interoperability arrangements, leading to a set of governance challenges that are primarily legal and political rather than technical. Most major cloud providers are headquartered in the United States and are subject to legislation such as the CLOUD (Clarifying Lawful Overseas Use of Data Act), which can allow US government agencies to compel access to data held on those CSPs (Cloud Service Providers) infrastructure, regardless of where the data physically resides. For European PPDR operators, this creates a potential conflict with GDPR (General Data Protection Regulation) and with national security frameworks that require strict control over law-enforcement communications data.

Emergencies such as floods and wildfires don't respect national boundaries, creating friction where operational cooperation is required. The EU has done meaningful work to close this gap through regulatory bodies such as EENA (European Emergency Number Association), CEPT (European Conference of Postal and Telecommunications Administrations), and LEWP (Law Enforcement Working Party), which have developed common frameworks for spectrum harmonisation and cross-border protocols. Projects such as BroadWay and ISITEP specifically address cross-border TETRA interoperability, and their findings are being incorporated into 4G/5G-based mission-critical service architectures.

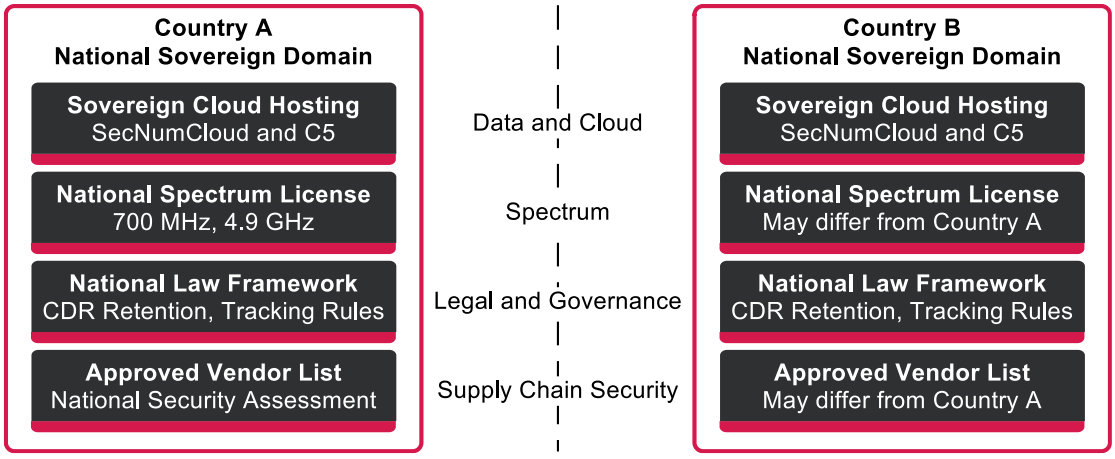

Figure 5 Sovereignty & Cross-border Issues

- Sovereign Cloud Hosting – the response to cloud sovereignty concerns in Europe has been to develop sovereign cloud certification frameworks, such as the SecNumCloud scheme developed by France's ANSSI, requiring that any cloud provider seeking certification must be immune from non-European law. Germany's BSI C5 (Cloud Computing Compliance Criteria Catalogue) takes a somewhat different approach, focusing on security controls rather than the nationality of the operator.
- National Spectrum License – spectrum licenses are nationally governed, meaning PPDR equipment authorised to operate on specific frequencies in one country may be unlicensed and therefore non-compliant or interference-causing the moment it is used in another country.
- National Law Framework – Each country's national legal framework governs critical variables such as how long call data records may be retained, whether foreign personnel can be tracked on shared systems, and who holds security clearance to access PPDR infrastructure, meaning that two countries whose networks are technically capable of interoperability may still be unable to use each other's network due to legal and governance differences.
- Approved Vendor List – when a PPDR operator installs or utilises a base station, router, or core network appliance, they are not just buying a device that performs a function, they are extending a degree of trust to everything within that equipment; the hardware, firmware, software, and supply chain of the vendor. An example of an untrusted vendor is Huawei, with security researchers in several countries identifying vulnerabilities in 5G network equipment, such as undocumented access interfaces, leading to the eventual banning of Huawei equipment in the United States, followed by several European countries. Typically, to be on an approved vendor list, national security agencies will conduct deep technical reviews of their equipment and identify their track record on vulnerability disclosure and remediation.

2 PPDR Network Evolution

2.1. Technology Evolution

PPDR networks have historically relied on purpose-built LMR (Land Mobile Radio) technologies, most notably TETRA (Terrestrial Trunked Radio) in Europe and P25 in North America. While these systems delivered reliable narrowband voice communications, they were not designed for the data-intensive demands of modern emergency response, such as mission-critical broadband services introduced by 4G LTE and 5G.

TETRA and similar narrowband LMR platforms were engineered for reliable, group-oriented voice communications. Over decades of deployment, they have proven highly dependable in difficult RF (Radio Frequency) environments. However, as operational requirements have

grown, their limitations have become a significant constraint for public safety agencies. Figure illustrates some of the key drawbacks of the TETRA system.

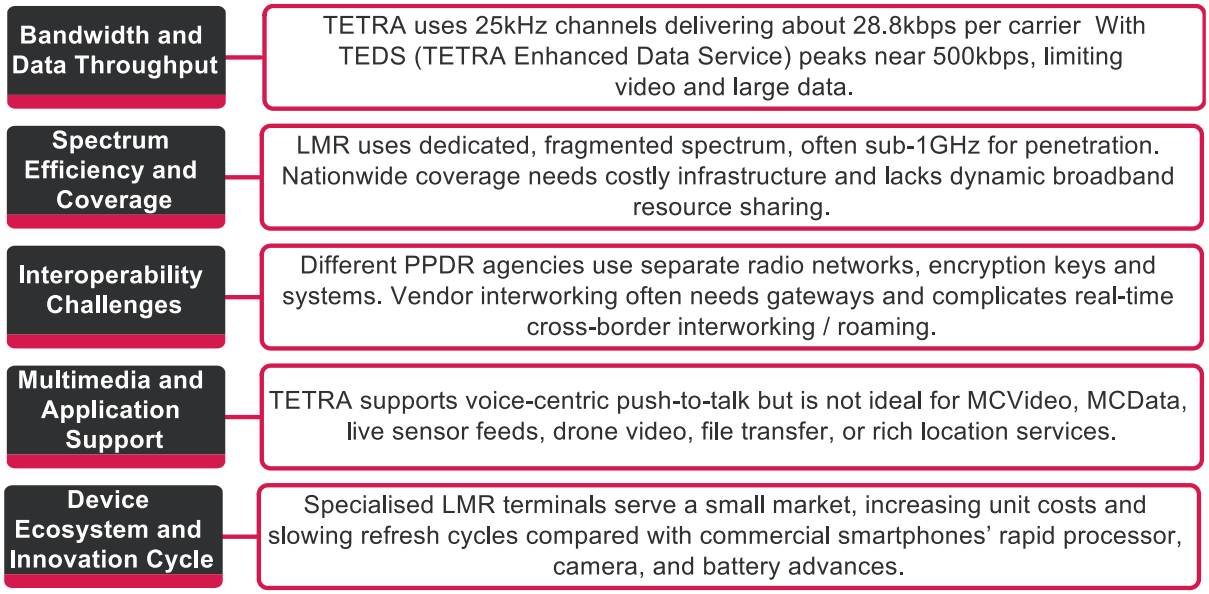

Figure 6 Key Drawbacks of Legacy Technologies

MCX Service Pillars

MC (Mission Critical) services[1] will provide numerous capabilities and functions that can be delivered to groups and users depending on their requirements, this includes PTT (Push To Talk) capability, data exchange and video streaming.

- MCPTT (Mission Critical Push to Talk) - MCPTT is designed to replace the current public safety communication networks. The features provided will deliver the voice functionality currently found within traditional narrow band radio networks.
- MCData (Mission Critical Data) - this focuses on non-voice and non-video traffic. MCData will enable the exchange of data using SDS (Short Data Service), the acquisition and exchange of files, and database queries. MCData will enable computer aided dispatch to be provided and allow for additional features such as event management, robot control, intelligence gathering and dissemination.
- MCVideo (Mission Critical Video) - users will be able to make a video call as a group conference call or direct to another user. There is also the ability to stream video to groups of users from a robot or drone, or a security camera.

Figure 7 identifies a selection of the features supported by the MCPPT, MCData and MCVideo services. In addition, later releases also facilitate various additional enhancements including discrete listening and logging, improved media handling, improved security, etc.

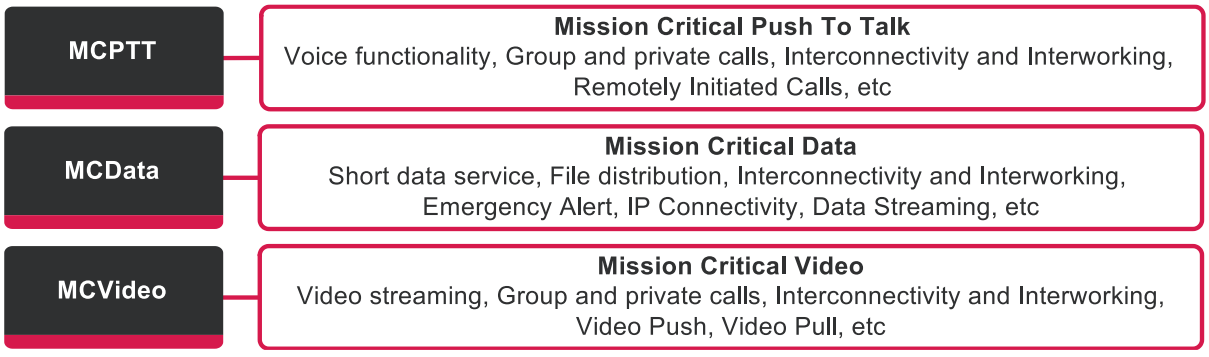

Figure 7 MCX Service Pillars

[1] TS 23.280 Mission Critical Services – Common Architecture

All three services are collectively referred to as MCX (Mission Critical Services) and share a common application-layer security model, group management architecture, and identity framework. They are designed to be access-agnostic. The same MCX clients and servers can operate over 4G LTE, 5G NR (New Radio), Wi-Fi, or even satellite links, providing seamless service continuity as terminals move between access technologies.

Role of the IMS for MCX

The IMS (IP Multimedia Subsystem) forms a foundational layer in the deployment of MCX (Mission Critical Services) over PPDR broadband networks. Standardised by 3GPP, IMS provides the SIP (Session Initiation Protocol) based signalling framework upon which MCPTT, MCVideo, and MCData application servers are built and interconnected. In an MCX architecture, the IMS core, comprising the P-CSCF (Proxy-Call Session Control Function), I-CSCF (Interrogating-CSCF), and S-CSCF (Serving-CSCF), is a critical part of the infrastructure that would demand resilience. These control functions handle the registration, authentication, and session routing of MCX clients, acting as the trusted intermediary between MCX device and the MCX application layer.

IMS also provides the subscriber identity management and service routing policies that allow MCX services to be delivered consistently across heterogeneous access networks, whether the terminal is connected via LTE 5G NR, Wi-Fi, satellite NTN (Non-Terrestrial Network) or a fixed network link. Crucially, IMS enables the interconnection of MCX domains across organisational and national boundaries, supporting the inter-domain group call federation and roaming scenarios that are essential during large-scale cross-agency PPDR incidents. Its integration with the 3GPP security framework, including P-CSCF-enforced IPSec (Internet Protocol Security) associations and IMS-AKA (Authentication and Key Agreement) authentication, ensures that the MCX signalling plane is protected end-to-end, complementing the bearer-level security mechanisms.

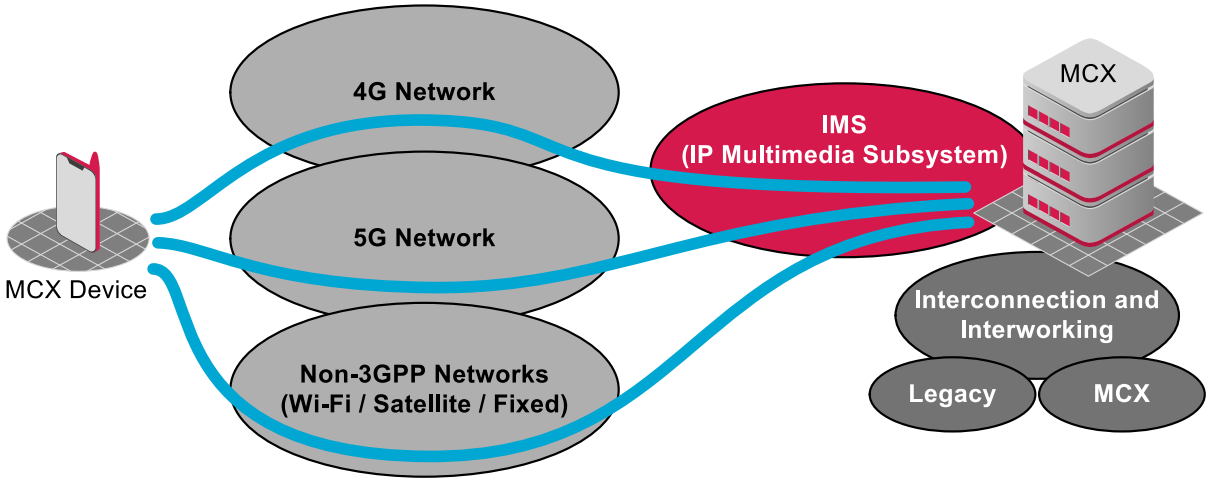

Figure 8 Role of the IMS for MCX Operation

Mission Critical Solutions in 4G LTE and 5G

Recognising that commercial 4G LTE and 5G networks could, with the right enhancements, meet PPDR requirements, 3GPP introduced a comprehensive set of MCS (Mission Critical Service) specification beginning in Release 13. These specifications define three core service pillars, each standardised at the application layer and designed to operate over any 3GPP compliant access network.

Several key LTE features were introduced specifically to support PPDR operations:

- ProSe (Proximity Services) – enable D2D (Device to Device) communications in both network-assisted and out-of-coverage modes. Critical for first responders working in areas where infrastructure has been destroyed or is unavailable, hence the out of network coverage scenario would apply.

- GCSE (Group Communication System Enablers) – provides efficient one-to-many delivery using eMBMS (Evolved Multimedia Broadcast Multicast Service), reducing network load during large scale incidents when many terminals receive the same video or audio stream simultaneously.
- Priority, QoS and Pre-emption – LTE QCIs (Quality Class Identifiers) specifically reserved for MCPTT and MCData ensure that the PPDR traffic receives preferential scheduling and can pre-empt lower-priority commercial traffic on shared networks.
- IOPS (Isolated E-UTRAN Operation for Public Safety) – allows an eNB to continue to provide local MCPTT services even when the backhaul connectivity to the 4G EPC (Evolved Packet Core) is lost, maintaining voice communications during infrastructure failures.

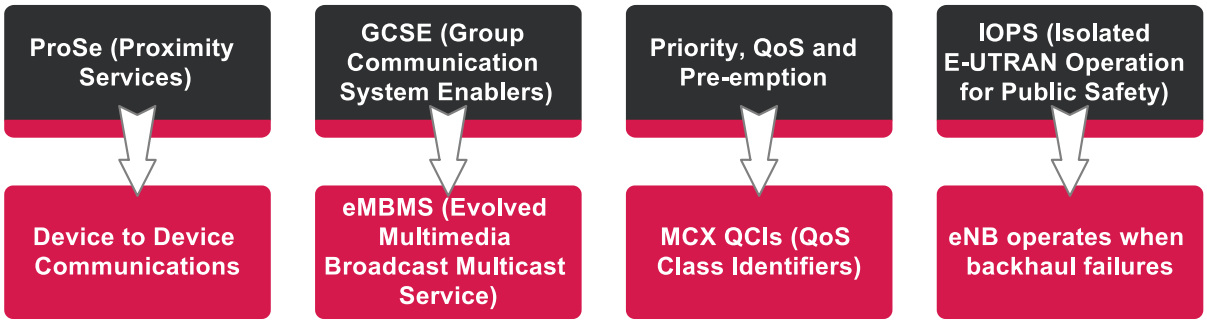

Figure 9 4G Enhancements for Mission Critical Services

5G NR (New Radio) and the 5GC (5G Core) introduce further capabilities that benefit PPDR:

- URLLC (Ultra-Reliable Low-Latency Communication) – this delivers end-to-end latency targets as low as 5ms, enabling time-sensitive applications such as remote-controlled vehicles, real-time augmented reality overlays for first responders, and tactile communications.
- eMBB (Enhanced Mobile Broadband) – providing multi-gigabit peak throughputs which can support high-definition video surveillance, multi-camera command views, and AI-assisted analytics at the edge.
- mMTC (Massive Machine Type Communications) – supports dense deployments of sensors, detectors, and wearable biometric devices which can generate the rich situational data that modern incident command requires.
- Network Slicing – allows a logically isolated resource guaranteed PPDR slice to coexist on shared physical infrastructure.

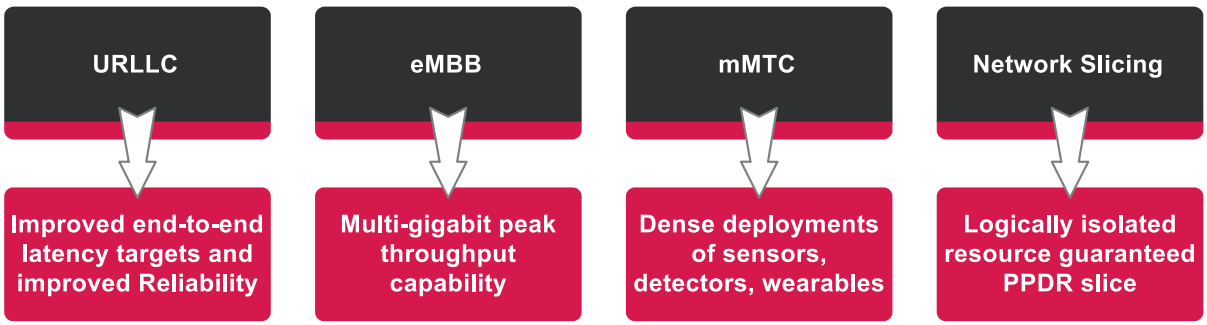

Figure 10 5G Enhancements for Mission Critical Services

LMR/TETRA to MCX Interworking

The transition from LMR / TETRA to MCX over broadband cannot, and should not, happen overnight. Due to their proven reliability and critical role in public safety, LMR networks cannot be replaced immediately. Transitioning from LMR to broadband MCX must follow a phased, carefully managed approach. The technical mechanism that makes this coexistence possible is the IWF (Interworking Function), a standards-defined gateway node that bridges

the narrowband LMR domain and the 3GPP MCX application layer. The IWF enables seamless voice interoperability between LMR and MCX, data service integration, hybrid network support, multimedia feature enhancements for LMR users, standards-based interoperability, and unified control room integration. In practice, a TETRA subscriber and an MCPTT user on a 4G/5G handset can participate in the same talk group simultaneously, with the IWF handling identity mapping, translating between TETRA ISSI (Individual Short Subscriber Identity) / GSSI (Group Short Subscriber Identity) addresses and MCX URIs, as well as floor control arbitration and late-entry support, all transparently to both sets of users.

Two principal architectural approaches exist for IWF deployment. The first is the standardised 3GPP model, in which the IWF connects directly to MCX application servers using defined MC service interfaces, ensuring multi-vendor interoperability and protecting procurement flexibility. The second is a proprietary or hybrid model, where vendor-specific gateways translate between their own LMR infrastructure and an MCX system, which may offer faster initial deployment but risks long-term vendor lock-in.

A hybrid LMR–MCX configuration, particularly for voice communications, represents an effective starting point, with the IWF playing a central role in enabling this step-by-step migration strategy. Over time, as MCX coverage matures and device ecosystems expand, agencies can progressively shift more services, first MCData, then MCVideo, and ultimately MCPTT, onto the broadband network, while retaining LMR as a resilience fallback. The LMR–MCX hybrid model offers a practical, scalable, and future-proof strategy for enhancing mission-critical communications, ensuring operational resilience, user adoption, and ongoing capability enrichment throughout the migration journey. Importantly, this interworking model is not confined to public safety: defence organisations, utilities, critical infrastructure operators, and sectors such as mining, oil and gas, and major event management all share the same requirement for dependable, efficient communications and stand to benefit from the same IWF-enabled transition pathway.

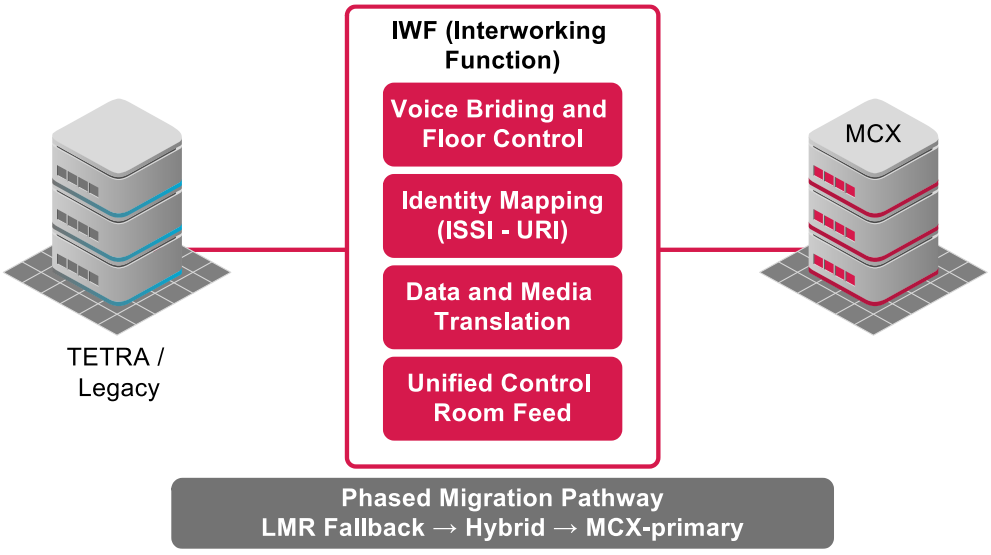

Figure 11 TETRA/Legacy Interworking with MCX

2.2. 5G Network Slicing

Slice Architecture Overview

5G network slicing is one of the most significant architectural innovations for PPDR. It enables a single physical 5G network to be partitioned into multiple logical networks, each called a network slice, each with its own resource allocation, quality-of-service parameters, security policies, and management plane. For PPDR operators, this means that mission-critical services can receive guaranteed resources on a shared commercial network, without being subject to the congestion and interference that affects ordinary mobile broadband users.

In 5G systems, a NSI (Network Slice Instance) is created by combining a set of NSSIs (Network Slice Subnet Instances) spanning the RAN, Transport, and Core domains. Each slice is identified by a S-NSSAI (Single Network Slice Selection Assistance Identifier) value, which consists of an SST (Slice/Service Type) and an optional SD (Slice Differentiator).

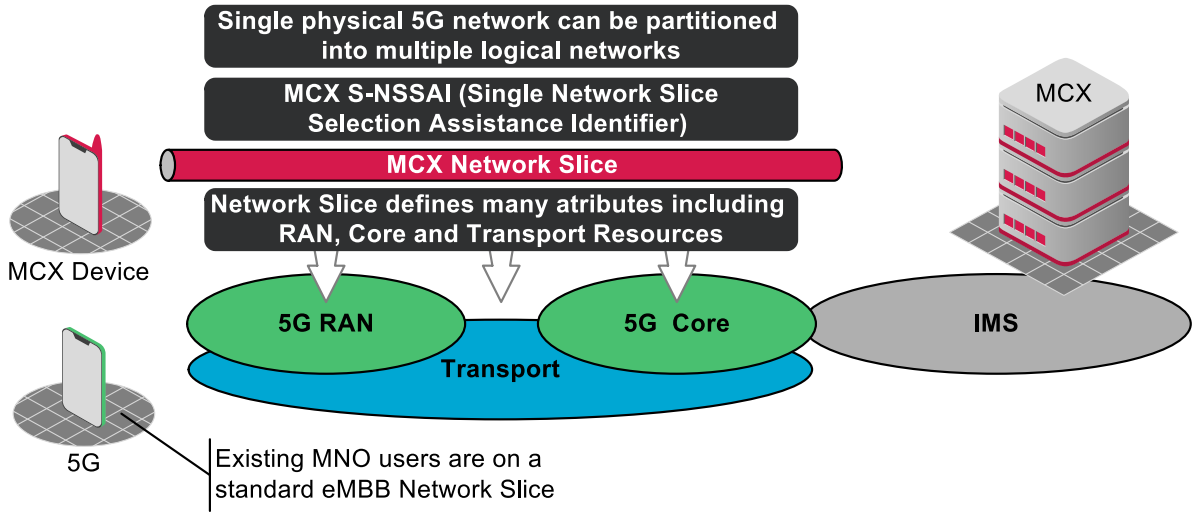

Figure 12 Network Slice Architecture Overview

A single PPDR S-NSSAI deployment may support multiple distinct service types within the slice, i.e. related to MCPTT, MCdata, MCVideo and IoT.

Securing Network Slices

While network slicing provides logical isolation, ensuring that this isolation is robust against both external attacks and inter-slice interference requires deliberate security engineering. 3GPP, NIST, and GSMA have all published guidance on network slice security.

- Isolation and Boundary Enforcement - the most fundamental security requirement for a PPDR slice is that its resources (radio, transport, and core) cannot be accessed, modified, or disrupted by users or functions belonging to other slices. Key mechanisms include:
  - NF (Network Function) isolation - each slice has its own instance of core NFs (e.g., dedicated AMF, SMF, UPF). Shared NFs such as the UDM must implement strict per-slice access controls.
  - VPN and transport segmentation - slice traffic is separated at the transport layer using dedicated VLANs, MPLS labels, or SRv6 segment identifiers. Physical separation of user plane traffic is preferred for high-security PPDR deployments.
  - API gateway enforcement - the SCP (Service Communication Proxy) and SEPP (Security Edge Protection Proxy) enforce authorisation checks on all inter-NF and roaming communications.
- Slice Access Control - only authorised PPDR terminals should be permitted to attach to the PPDR slice. This is enforced through:
  - S-NSSAI-based access control - in the AMF (Access and Mobility Management Function), which validates that the requested slice is permitted for the subscriber's PLMN subscription.
  - NSSAA (Network Slice-Specific Authentication and Authorisation) - introduced in Release 16, which allows an external AAA server, under the control of the PPDR authority, to independently verify that a terminal is authorised to access the PPDR slice, separate from the primary 5G authentication (5G-AKA or EAP-AKA').
  - Device Attestation and Certificate-based authentication - for PPDR terminals, ensuring that only approved, tamper-resistant hardware can access PPDR services.

- Monitoring and Threat Detection - slice security requires continuous monitoring:
  - Per-slice SIEM (Security Information and Event Management) integration - to detect anomalous traffic patterns, signalling floods, or attempted lateral movement between slices.
  - NADF (Network Anomaly Detection Function) capabilities - defined from 3GPP Release 17 for AI/ML-assisted threat detection within the 5G core.
  - Audit logging - all slice management operations, with tamper-evident storage.

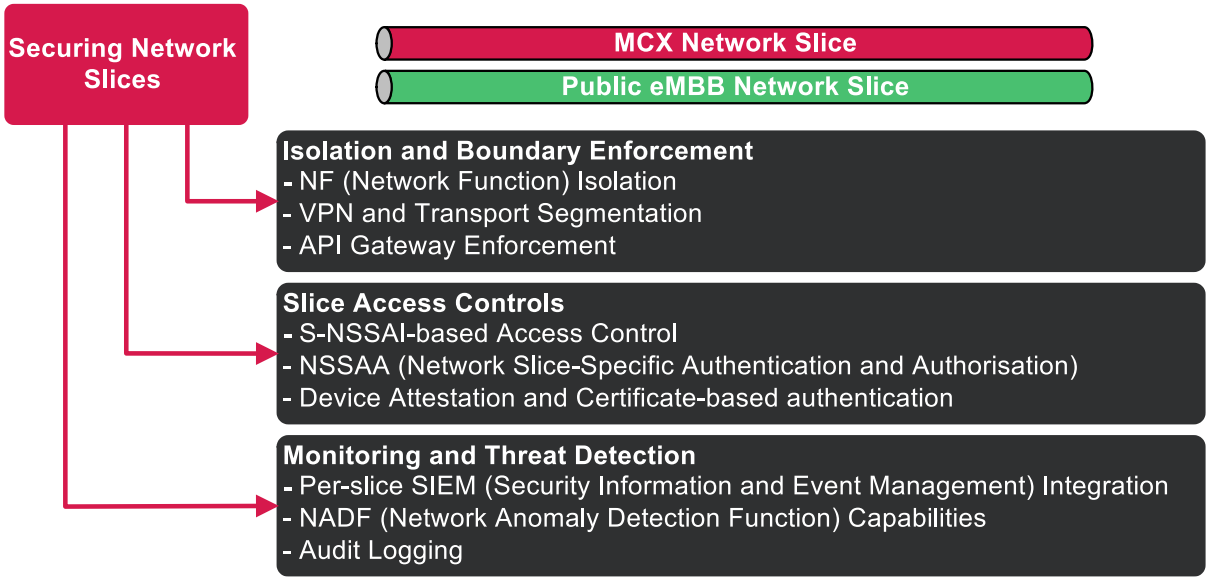

Figure 13 Securing Network Slices

2.3. TN and NTN Convergence

TN (Terrestrial Networks), even the most extensive national 4G/5G deployments, cannot achieve ubiquitous coverage. Rural areas, maritime zones, remote borders, warzones, and disaster-struck regions where infrastructure has been destroyed will include terrestrial coverage gaps for the foreseeable future. NTN (Non-Terrestrial Network), encompassing satellite systems, HAPS (High-Altitude Platform Stations), and airborne relays, offer the complementary coverage needed to extend PPDR connectivity to these areas. The integration of TN and NTN into a unified, seamless system is one of the key themes in 3GPP standards from Release 17 onward.

3GPP NTN Integration Architecture

3GPP Release 17 introduced the first standardised framework for NTN integration with 4G/5G, with further enhancements in Releases 18 and 19. The key architectural options are:

- Transparent Payload Architecture - in this configuration, the satellite acts purely as a bent-pipe repeater, forwarding signals between ground-based base stations and device. The satellite adds propagation delay but does not perform any 3GPP protocol processing. Ground-based gNBs must be enhanced to handle the extended timing advance and Doppler shift introduced by the satellite path. This architecture is simpler to deploy but requires ground station infrastructure near the coverage area.
- Regenerative Payload Architecture - here, the satellite hosts on-board processing capabilities. In the most advanced form, the satellite carries a full 4G/5G base station stack, communicating directly with the 4G/5G Core over inter-satellite links or ground gateways. Regenerative payloads increase on-board complexity and cost but significantly reduce latency and ground station dependency.
- NTN UE Considerations - NTN-capable UEs must address several specific challenges:

- Extended timing advance and HARQ timing - 3GPP defines NTN-specific HARQ process configurations to handle the longer round-trip propagation delay without reducing throughput.
- Doppler pre-compensation - devices in LEO systems must compensate for rapid Doppler shifts caused by satellite motion using GNSS-derived ephemeris data.
- GNSS integration - NTN devices are required to have embedded GNSS receivers to provide location and timing information for network entry procedures.

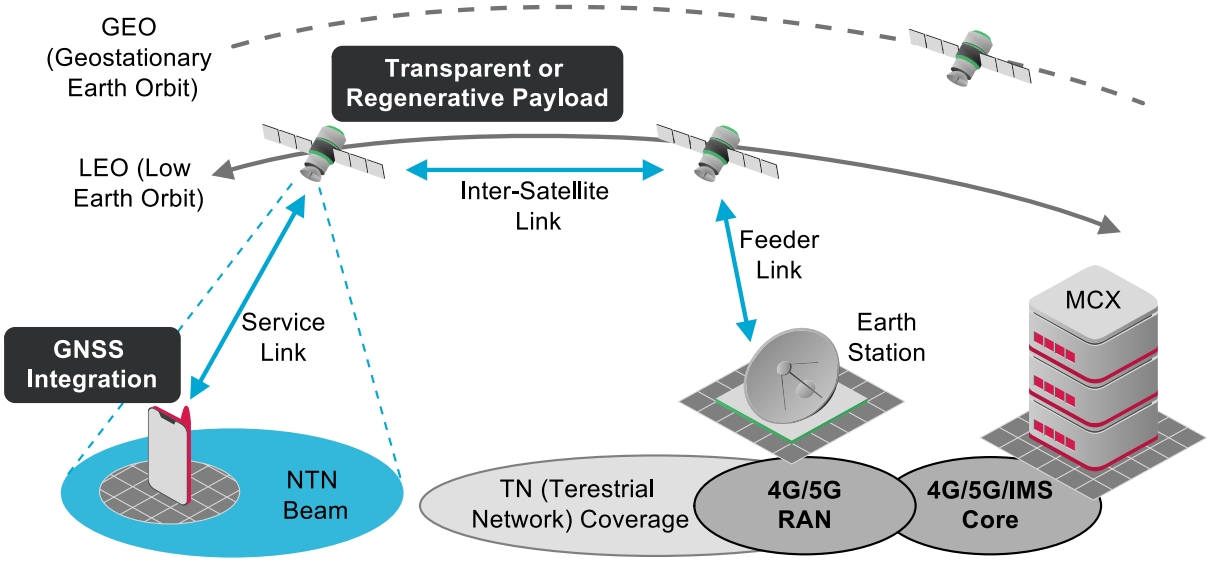

Figure 14 3GPP NTN Integration Architecture

MCX Coverage and Capacity Planning

Coverage and capacity planning are fundamental requirements for PPDR and MCX systems, where network failure is simply not an option. Unlike commercial mobile networks, which are designed primarily around population density and economic return, PPDR networks must guarantee service across a far wider range of environments, including remote rural areas, underground infrastructure, dense urban canyons, and locations that may experience sudden, extreme surges in traffic during major incidents.

Coverage planning must account for in-building penetration, terrain shadowing, and the need to maintain communications for first responders operating in degraded or hostile RF environments. Capacity planning adds a further layer of complexity, a large-scale emergency such as a terrorist incident, natural disaster, or major public event can generate a dramatic and unpredictable spike in voice, video, and data traffic precisely when reliable communications are most critical. This demands that network planners not only design for steady-state usage but also model worst-case concurrent user scenarios, prioritise and pre-empt traffic for authorised users, and ensure backhaul and core network resources can absorb the surge without degradation.

While terrestrial networks, whether purpose-built LTE/5G PPDR networks or commercial networks with dedicated slices, form the backbone of MCX service delivery, they carry an inherent limitation. Even the most extensive ground-based infrastructure has geographic gaps, and it is precisely in the most remote or devastated areas that coverage tends to fail when it is needed most. One extreme is when terrestrial infrastructure is destroyed by flooding, earthquake, wildfires terrorist/war, or simply never existed, NTN provides a resilient, wide-area overlay that can sustain critical voice and data links for incident commanders, field teams, and inter-agency coordination. NTN is therefore not conceived as a replacement for terrestrial PPDR networks but as a complementary tier in a layered architecture, ensuring that coverage obligations can be met even at the edge of the operational envelope.

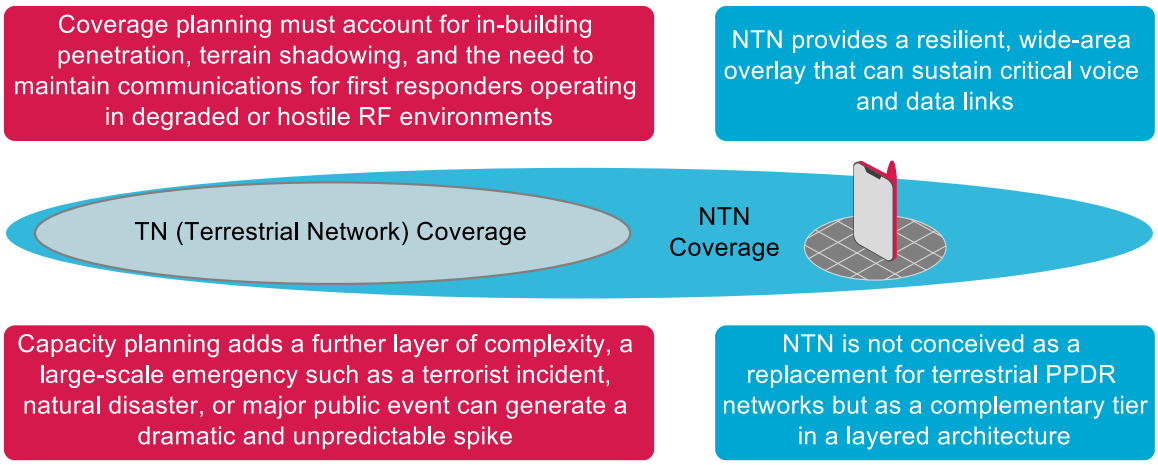

Figure 15 MCX Coverage and Capacity Planning

Solutions for Disaster Coverage

NTN is particularly valuable for PPDR in disaster scenarios, where terrestrial infrastructure may be partially or wholly destroyed. Key solutions include:

- Direct-to-Device Emergency Communications – NTN solutions can provide direct connectivity to standard NTN-capable handsets without requiring ground stations in the affected area. This is critical for:
  - Emergency alerting and evacuation messaging broadcast to all devices within a disaster zone.
  - Two-way voice, data and messaging communications for isolated first responders or survivors with no terrestrial coverage.
- HAPS as an Intermediate Connectivity Layer – HAPS (High-Altitude Platform Stations) are explicitly included within the 3GPP NTN framework alongside satellite systems. Operating at approximately 20 km altitude, HAPS can provide a useful intermediate layer between terrestrial networks and satellites. In PPDR scenarios, HAPS can deliver temporary broadband coverage over unserved, isolated, or disaster-affected areas, supporting emergency teams and recovery operations. Compared with GEO, HAPS offers significantly lower latency; compared with LEO, it can provide longer dwell time over a specific disaster zone, making it well suited for localised emergency coverage.
- Rapid Deployment of PPDR Connectivity – satellite-connected CoW (Cells on Wheels), CoLT (Cells on Light Trucks), or portable PPDR base stations can be deployed into a disaster zone and connected via NTN backhaul to the MCX core network. This can restore local PPDR broadband coverage within hours rather than the days or weeks required to rebuild terrestrial infrastructure. Such deployments can support MCPTT voice, MCVideo, MCData, drone feeds, field sensors, and command applications.
- IOPS via NTN Backhaul – IOPS provides a fallback capability when connectivity to the central core network is lost or intermittent. By using a local EPC or 5G core function co-located with the base station, IOPS allows mission-critical communications to continue between public safety users even when backhaul to the macro core is unavailable. NTN backhaul can restore the 4G S1 or 5G N2 reference connection to the wider core network where possible, while IOPS ensures local PPDR services remain operational if that satellite connection is disrupted.
- Resilience Through Multi-Orbit and Multi-Platform Diversity – a robust PPDR NTN architecture may combine GEO, MEO, LEO, and HAPS assets to reduce dependency on any single platform. GEO can support wide-area broadcast, alerting, and command-and-control messaging where moderate latency is acceptable. LEO can support lower-latency voice, data, and real-time video. HAPS can provide persistent local coverage over a disaster zone. This multi-layer approach improves resilience against single-orbit outages, terrestrial infrastructure failure, congestion, and space-weather-related disruption.

- NTN-Enabled Positioning and Backup PNT (Positioning, Navigation, and Timing) for PPDR – NTN can support positioning, navigation, and timing resilience in GNSS-denied or GNSS-degraded environments, including scenarios involving jamming, spoofing, or loss of terrestrial positioning infrastructure. A dedicated LEO-PNT layer using 3GPP NTN capabilities could provide backup positioning and emergency connectivity, including two-way low-data-rate emergency messaging. This goes beyond simple location reporting from tracking devices and is especially important for PPDR operations where responders require reliable positioning in disrupted, remote, or hostile environments.
- Network Slicing for PPDR Traffic Prioritisation over NTN – network slicing enables isolated virtual networks to be created over shared NTN infrastructure, each tailored to specific service requirements. For PPDR, this allows mission-critical traffic to be prioritised and protected from congestion caused by commercial or public users sharing the same satellite capacity during a disaster. This is essential when a satellite-backhauled CoW must simultaneously carry MCPTT voice, MCVideo drone feeds, MCData command traffic, sensor data, and emergency alerts.
- Integrated Sensing and Communications for Situational Awareness – NTN can support not only communications but also situational awareness through ISAC (Integrated Sensing and Communications). Satellites and HAPS can contribute remote sensing data, environmental monitoring, SAR (Search and Rescue) imagery, fire mapping, flood detection, infrastructure damage assessment, and other operational intelligence. When integrated into PPDR command systems, this data can help create a common operating picture for incident commanders and first responders.
- End-to-End Security for NTN PPDR Links – PPDR NTN architectures must provide strong end-to-end security across satellite, HAPS, terrestrial, and deployable network elements. Satellite links are exposed to cyber and radio-frequency threats, including jamming, spoofing, DDoS attacks, interception, and man-in-the-middle attacks. For PPDR operations, MCX traffic carried over NTN backhaul must be encrypted, NTN-capable devices must be strongly authenticated, and security orchestration must account for the distributed and heterogeneous nature of integrated terrestrial and non-terrestrial networks. Zero-trust principles, secure slicing, and resilient identity management are therefore essential design requirements.

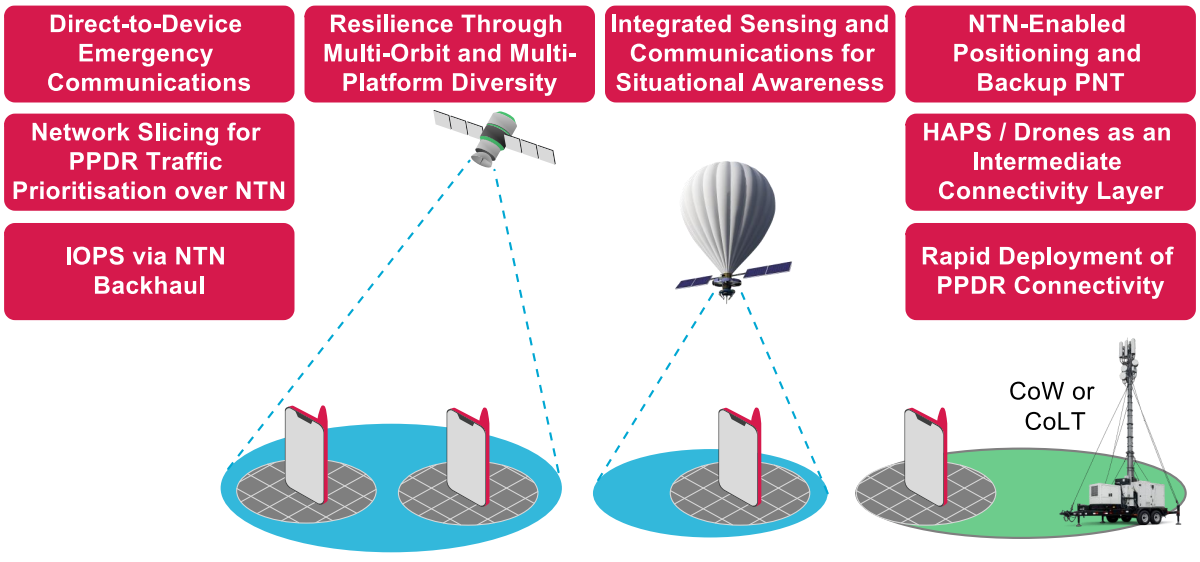

Figure 16 Solutions for Disaster Coverage

2.4. Security Features for PPDR Architecture

Security is a foundational requirement for any PPDR network. Public safety communications carry sensitive operational information, and any compromise, whether through eavesdropping, denial of service, or fraudulent injection of false commands, can have life-threatening consequences. PPDR security must therefore be engineered into every layer of

the architecture. This includes from the radio interface to the core network, from roaming interfaces to end-user applications.

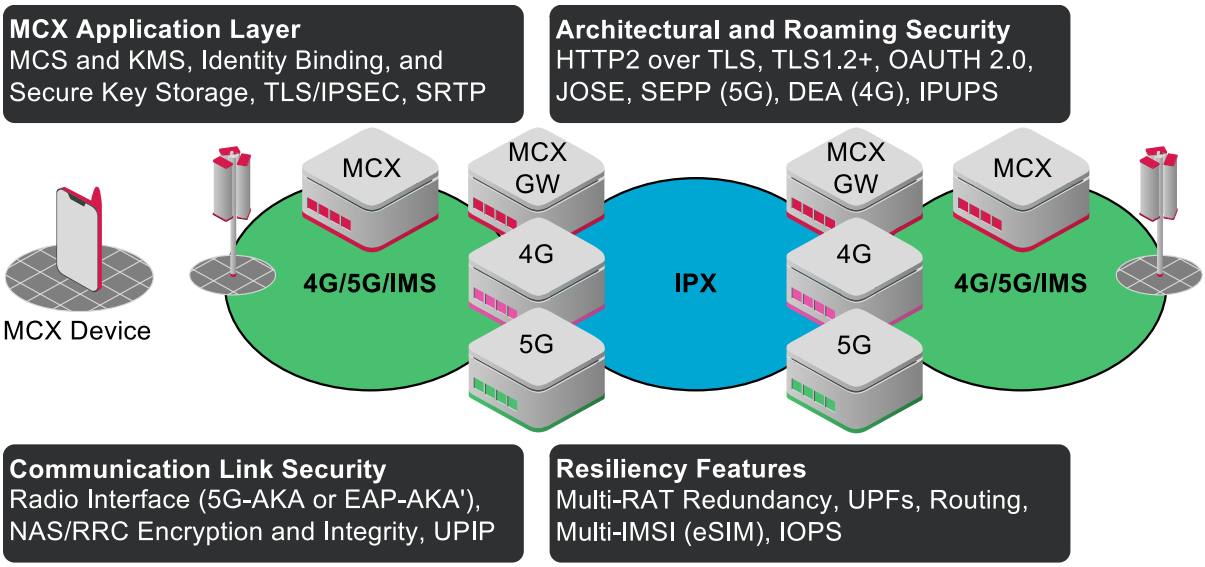

Figure 17 Security Features for PPDR Architecture

Architectural and Roaming Security

In 4G, roaming between PPDR networks (or between a dedicated PPDR network and a commercial host network) relies on the EPC interfaces carried over an IPX (IP Packet Exchange) interconnect, governed by GSMA IR.88. Mobile network operators use the private IPX to communicate with each other and with other service providers for international roaming. In LTE/4G, Diameter-based protocols and the S9 interface are rolled out on the IPX network, used for communicating charging, service control, and QoS control signalling. The principal roaming interfaces are:

- S6a / S6d - subscriber authentication and profile exchange between the visited MME and the home HSS, carried over Diameter.
- S9 - policy and charging rules between the V-PCRF (Visited PCRF) and H-PCRF (Home PCRF), enabling the home network to push QoS policy for PPDR priority bearers to the visited network (note that S9 is often not implemented).
- S8 / Gp - the inter-PLMN user plane tunnel (GTPv1/v2) between the visited S-GW and the home P-GW (home-routed model), or the visited P-GW (local breakout).

At the network edge, a DEA (Diameter Edge Agent) controls ingress and egress of Diameter signalling. The DEA or IPX Diameter Agent provides topology hiding to protect network elements and addresses from being exposed to foreign networks.

GSMA security profiles for LTE cover filtering recommendations for Diameter S6a, S6d, S9, and Gx interfaces, mitigation techniques for mobility and authentication fraud, and threat modelling for GTP-C signalling used to create user plane tunnels.

A critical limitation for PPDR planners is that the IPX is treated as a trusted transit environment, and there is no mandatory message-level encryption on the Diameter interfaces traversing it. This leaves 4G PPDR roaming exposed to the well-documented Diameter signalling attacks, location tracking, call interception, and DoS, which are particularly sensitive threats for law enforcement and emergency services. Signalling firewalls at the DEA are the primary mitigation, but they are not a complete solution.

The 5G Core moves away from point-to-point Diameter towards an SBA (Service-Based Architecture) in which all NFs (Network Functions) communicate over HTTP/2 with a common framework of mutual authentication and authorisation. There are fundamental differences between 4G and 5G core networks. Key mechanisms that can be included are:

- NF mutual authentication via the NRF - every NF must register with the NRF (Network Repository Function) and present a certificate. When one NF wishes to communicate with another, it can obtain an OAuth 2.0 access token from the NRF, scoped to the specific service operation being called. This replaces the implicit, topology-based trust of Diameter with explicit, cryptographically verified authorisation on every API call.
- Mandatory TLS on all SBI (Service-Based Interfaces) - all NF-to-NF communication within the 5GC can be protected by TLS 1.2 or higher. This provides confidentiality and integrity for all control plane messages within the operator's domain, a significant baseline improvement over 4G's largely unencrypted Diameter paths. Note that processing overhead in the virtualised core will increase when TLS is active.
- Certificate-based NF identity - NFs are issued X.509 certificates that encode their NF type, PLMN ID, and NF instance ID. This enables precise filtering, as such an AMF in a roaming PLMN cannot impersonate an SMF or access services outside its authorised scope.

For cross-border PPDR operations, the 5G Core places a SEPP (Security Edge Protection Proxy) at each PLMN's perimeter as the mandatory inter-operator gateway. The N32 interface between SEPPs is split into two sub-protocols: N32-c, which establishes a mutual TLS session and negotiates cipher suites and protection policies before any subscriber data flows; and N32-f, which carries the actual HTTP/2 signalling protected by JOSE (JSON Object Signing and Encryption) at the message level. This means that even where IPX intermediaries are in the path, sensitive attributes remain confidential and tamper-evident end-to-end, a significant advance over 4G's unencrypted Diameter transit. The SEPP also provides topology hiding, replacing internal NF addresses before messages leave the PLMN so that the home network's AMF, UDM, and AUSF are never exposed to the visiting network.

User plane protection across PLMN boundaries is handled separately by the IPUPS (Inter-PLMN User Plane Security) function within the UPFs, controlled by the V-SMF and H-SMF, which enforces valid GTP-U traffic on the N9 reference point and discards anything that fails validation. Together, SEPP/N32 on the control plane and IPUPS on the user plane close the gaps that made 4G roaming security reliant on the trustworthiness of the IPX transit network, a particularly important improvement for PPDR, where roaming agreements may span national boundaries with varying levels of mutual trust.

Finally, the MCX application-layer security operates independently of the underlying bearer, whether 4G, 5G, dedicated, or commercial. Media confidentiality is end-to-end between MCX clients regardless of routing path, whether unicast, multicast, or direct mode, so even the MC gateway server relaying traffic across the MCPTT-10 inter-system reference point cannot decrypt the content. When two PPDR systems interconnect, their KMSs (Key Management Servers) must federate, with each system's home KMS acting as the root of trust for its domain. Cross-domain calls depend on KMS-to-KMS trust relationships to verify identity-based key material across system boundaries. Signalling between MC gateway servers is protected by TLS on the SIP-3 reference point, with IPSec available as an additional option, ensuring both the media and the signalling remain protected across the inter-system boundary.

Communications Link Security

In 5G, security is established from the moment a device first contacts the network and is maintained across every layer of the communication stack. Unlike 4G, where user plane integrity protection was optional and subscriber identity was frequently exposed, 5G mandates a comprehensive set of protections by design. The following mechanisms collectively ensure that a PPDR device's identity, signalling, and data traffic are authenticated, integrity-protected, and confidential from the air interface through to the core network:

- Authentication - 5G-AKA (5G Authentication and Key Agreement) or EAP-AKA' is performed during initial registration, with the SUPI (Subscription Permanent Identifier)

protected during transmission using SUCI (Subscription Concealed Identifier), the SUPI is encrypted using the home network's public key before being transmitted over the air.

- NAS (Non-Access Stratum) security - NAS signalling between the device and the AMF is protected with NAS integrity protection (using NIA algorithms) and optional confidentiality (using NEA algorithms) from the point of initial registration.
- RRC (Radio Resource Control) security - AS (Access Stratum) security between the device and gNB provides integrity protection and ciphering for RRC signalling and user plane data.
- User Plane integrity protection - from Release 15 onward, 5G mandates support for UPIP (User Plane Integrity Protection), which extends integrity protection to the data plane, critical for PPDR to prevent injection of false sensor data or command-and-control messages.

At the application layer, MCX security operates independently of the underlying bearer network, providing a consistent and portable security envelope whether the device is connected over a dedicated PPDR network, a commercial 5G host network, or a direct-mode link. This layer is governed by 3GPP TS 33.180 and ensures that mission-critical communications remain protected end-to-end between users, irrespective of how the media and signalling are routed through the network infrastructure. Key areas include:

- Group communication security - MCX group calls and messages are protected using group keys distributed via the MCS (Mission Critical Security) key management infrastructure. The KMS (Key Management Server) issues group encryption and integrity keys to authorised MCX users.
- Identity binding - MCX user identities are cryptographically bound to their credentials using certificates, preventing identity spoofing within the MCX domain.
- Secure storage of keys - MCX client devices are required to store cryptographic keying material in secure elements or TEEs (Trusted Execution Environments) to resist device compromise.

Integrity & Encryption

In addition to hop-by-hop encryption at the bearer level, MCX provides E2EE (End-to-End Encryption) at the application layer. Bearer-level encryption in both 4G and 5G is governed by algorithm sets: EIA (EPS Integrity Algorithm) and EEA (EPS Encryption Algorithm) in 4G, and NIA (NR Integrity Algorithm) and NEA (NR Encryption Algorithm) in 5G. Each algorithm is identified by a numeric suffix, for example, NIA2/EIA2 uses AES-128-CMAC for integrity, and NEA2/EEA2 uses AES-128-CTR for confidentiality, while a suffix of 0 denotes the null algorithm, meaning no protection is applied. Null algorithms exist for testing and exceptional interoperability cases but must never be permitted in operational PPDR deployments. 4G and 5G networks should be configured to mandate at minimum NIA2/NEA2 and to reject null algorithm negotiation for all PPDR subscribers at the policy level.

Even with strong bearer-layer algorithms in place, hop-by-hop encryption alone does not protect content from the network infrastructure itself. MCX therefore provides E2EE (End to End Encryption) at the application layer using keys derived from group session keys issued by the KMS, ensuring that MCX voice, video, and data content is encrypted from the originating device all the way to the receiving device or devices and is not decryptable by MCX application servers, MC gateway servers, or any intermediate routing element. This means that even where MCX traffic traverses a commercial host network or crosses a system boundary via the MCPTT-10 reference point, the content remains protected against inspection or tampering by any party other than the intended recipients.

Resiliency Features

PPDR networks must continue to function during natural disasters, large-scale attacks and infrastructure failures. Resilience is therefore not an optional enhancement but a core

architectural requirement. The following features collectively provide a multi-layered resilience posture:

- Multi-RAT Redundancy - PPDR terminals may be equipped with multi-RAT capabilities, enabling automatic fallback between access technologies. The MCX client software manages seamless handover between access technologies without dropping active calls or group sessions, using the access-agnostic design of the MCX application layer. Typical priorities will be:
  - Primary - 5G NR (preferred for capacity and latency).
  - Secondary - 4G LTE (widely deployed, mature MCPTT support via IOPS).
  - Tertiary - Wi-Fi (for indoor venue coverage supplementation).
  - Fallback - Satellite NTN (for coverage continuity in destroyed infrastructure scenarios).
  - Emergency - TETRA/LMR (for extreme fallback where all cellular networks are unavailable).
- Redundant User Plane Paths - in the 5G Core, the UPF (User Plane Function) can be deployed in a distributed and redundant configuration:
  - Primary and secondary UPF instances - with active-active or active-standby configurations.
  - Multi-homing of PDU Sessions - across multiple UPFs using redundant transmission, providing seamless failover without session interruption.
  - Edge UPF deployment - close to gNBs, to reduce latency and provide local breakout, limiting the impact of backhaul failures on active PPDR sessions.
- Routing Infrastructure Redundancy - the IP routing infrastructure underpinning the PPDR network should be designed with full redundancy:
  - Dual-homed gNBs and transport nodes - connected to separate physical infrastructure paths.
  - BGP route diversity - ensuring that no single point of failure in the IP backbone can isolate a PPDR site.
  - SDN (Software-Defined Networking) - with centralised path computation enabling rapid re-routing around failed segments.
  - Microwave and satellite backhaul - as secondary transport options for sites where fibre resilience is difficult to achieve.
- Multi-IMSI SIM / eSIM - a Multi-IMSI SIM or eSIM solution provides PPDR terminals with the ability to maintain subscriptions on multiple networks simultaneously:
  - The terminal can switch between operator networks, or between a dedicated PPDR network and a commercial MNO, without a physical SIM swap.
  - In disaster scenarios, if the primary PPDR network operator's coverage is degraded, the terminal automatically activates an IMSI from a secondary MNO, maintaining MCX service continuity.
  - eSIM-based remote provisioning - allows the PPDR authority to remotely update network subscriptions across an entire device fleet, particularly useful during rapidly evolving incidents requiring multi-operator access.
  - Multi-IMSI approaches are being standardised within 3GPP in the context of Disaster Roaming (Release 17), which defines procedures for UEs to access a PLMN during a declared disaster even without a pre-existing roaming agreement.
- IOPS (Isolated E-UTRAN/NR Operation for Public Safety) - allows a base station to continue providing PPDR communications locally even when its connection to the core network is severed:

- A local IOC (Isolated Operation Core) function provides authentication, group call management, and basic MCX services from the base station itself.
- When backhaul is restored, terminals seamlessly re-register with the main core network and synchronise state.

Note that IOPS was defined in 3GPP Release 13 for LTE and extended to 5G NR in subsequent releases.

3 Current Threat Landscape – Cyber & Physical

Historically, PPDR systems operated on purpose-built, isolated radio networks such as TETRA and P25. However, the progressive migration towards IP-based architectures such as LTE (Long-Term Evolution) and 5G has transformed both the capabilities and vulnerabilities of these critical networks as they have inherited the vulnerabilities of the technologies that they rely on. According to the PSTA (Public Safety Threat Alliance), in 2024, attacks on mission-critical PPDR technologies, including public safety radio, CAD (Computer-Aided Dispatch), and PSAPs (Public Safety Answering Points), increased by 60%, with 24 emergency communication systems rendered completely unavailable. The remainder of this section will discuss the current threat landscape in more detail, highlighting both Cyber and Physical elements impacting cyber resilience.

3.1. Attack Vectors

Understanding the precise technical mechanisms by which adversaries gain access to PPDR infrastructure is the foundation of any effective defensive approach. A high-level taxonomy of threat types provides insufficient guidance for security architects and network operators who must implement specific controls against pre-determined attack paths. Figure 18 outlines some key examples of Attack Vectors.

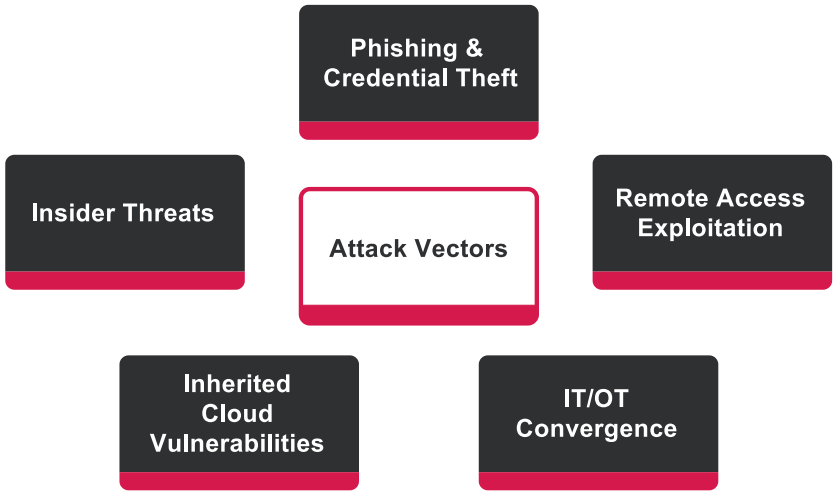

Figure 18 Attack Vectors

- Phishing & Credential Theft - adversaries can use AiTM (Adversary-in-the-Middle) phishing technique, routing victims through a reverse proxy that intercepts session cookies after 2FA is already in place. Platforms such as Tycoon 2FA facilitate this technique at scale as PhaaS (Phishing as a Service).
- Remote Access Exploitation - Internet-facing SSL-VPN gateways and RDP servers are the most directly exploitable entry points into PPDR networks. In 2024, we saw critical pre-authentication vulnerabilities across major gateway appliance vendors such as Ivanti, Palo Alto, Cisco ASA, and Check Point VPN.
- IT/OT Convergence - legacy PPDR systems were engineered when physical isolation was a primary defence. Integration with IP networks for broadband video, cloud CAD, and

real-time mapping has dissolved the air gap between IT/OT systems. In 2024, 83% of successful CAD compromises were traced back to initial access through enterprise IT networks before lateral movement crossed the Purdue Model boundary into mission-critical systems.

- Inherited Cloud Vulnerabilities - the migration to cloud-hosted infrastructure means PPDR agencies inherit a new class of vulnerabilities. Examples include overprivileged IAM (Identity and Access Management) roles, absent MFA, and dormant contractor accounts, which have enabled credential-stuffing campaigns.
- Insider Threats - generally, three types of insiders exist: negligent insiders, malicious insiders, and recruited insiders. Systems such as UEBA (User and Entity Behaviour Analytics) can be implemented to reduce impact and increase resilience.

3.2. Physical Supply Chain

Cyber resilience frameworks often focus on digital attack vectors, yet the physical supply chain represents an equally significant and frequently underestimated attack surface. Modern PPDR systems built on LTE and 5G architectures aggregate hardware from a wide and geographically dispersed supply chain containing chipset foundries, system integrators, national distributors, logistics providers, and local installation contractors. Each hand-off point represents a potential window for adversarial interference. The adversarial model outlined in the MITRE ATT&CK framework encompasses two primary strategies that align with nation-state TTPs (Tactics, Techniques, and Procedures):

- Target Interdiction – intercepting a specific physical supply chain for a known PPDR agency.
- Broad Supply Chain Poisoning – components such as chipsets, firmware images and pre-loaded software libraries are compromised at the manufacturing or distribution tier to create a large victim pool for later exploitation.

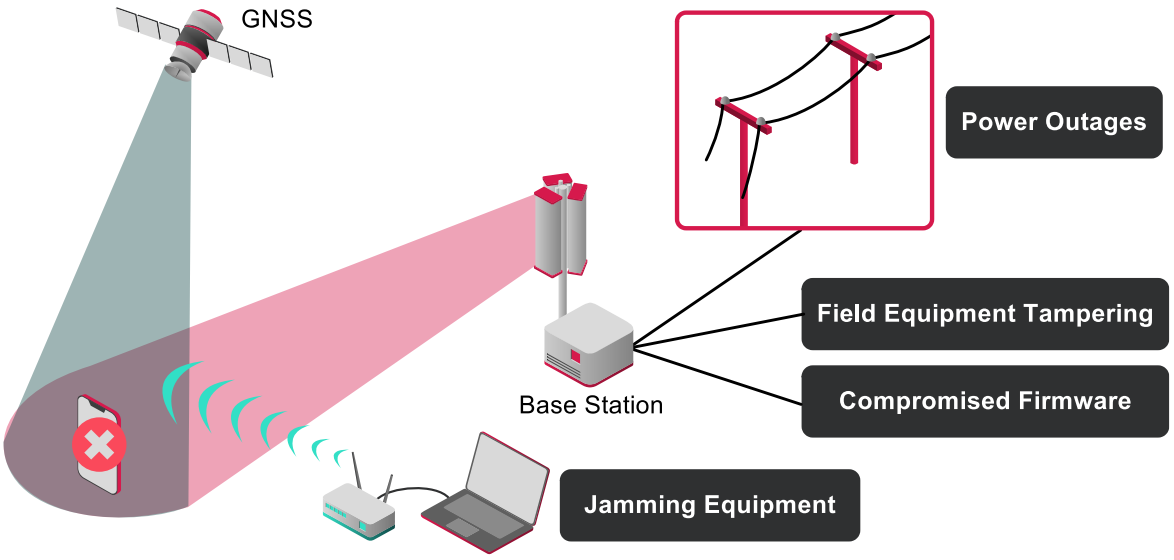

Figure 19 Physical Supply Chain

Tampering with Field Equipment

Hardware tampering encompasses any deliberate physical or logical modification of a device prior to or during its operational life. For PPDR-deployed equipment (eNodeBs, gNodeBs, ruggedised handsets, mounted terminals, etc.), there are three distinct stages of the supply chain that can be impacted:

- Manufacturing – rogue components can be added at the manufacturing stage, introducing secondary communication channels or persistent backdoors that operate below the OS

and hypervisor layer. Such implants are typically invisible to software-based EDR (Endpoint Detection and Response Tools).

- Transport – interdiction attacks are more likely at this stage, with adversaries intercepting shipments and tampering with components. Anti-tampering seals and holographic labels offer weak assurance unless combined with cryptographic hardware attestations. Examples include a TPM (Trusted Platform Module) that generates a measurement of the hardware configuration at first power-on, which can be compared with a vendor-supplied reference value. Where TPM attestation is not available, X.509 certificates can be provisioned at the factory and bound to a HSE (Hardware Security Element) to provide an alternative approach to verification.
- Operation – contractors and vendors access equipment, which represents a recurring exposure window. A technician accessing base stations with supervision can insert hardware implants or rogue network taps. Mitigations here include a TPI (Two-Person Integrity) rule for physical access to critical network nodes, an audit log and a post-maintenance integrity check using trusted hardware fingerprinting tools.

Compromised Firmware

Firmware compromise is architecturally distinct from hardware tampering, as it involves modifying the software executing on embedded processors within the device, rather than introducing rogue physical components. In the base station equipment, this would be the radio controller firmware.

Firmware can be compromised at the factory with pre-loaded malicious images, at the distribution level, or during a maintenance window. MITRE ATT&CK detection strategy identifies the primary indicators of firmware change as:

- UEFI (Unified Extensible Firmware Interface) or BIOS (Basic Input/Output System) version drift versus the vendor-published image.
- Secure boot signature verification failures.
- Unexpected hardware module or drivers enumerated at boot time.

For 5G infrastructure, the 3GPP Security Specifications require cryptographic firmware signing, and the O-RAN alliance specifications mandate mutual authentication between components.

Jamming Equipment

RF Jamming constitutes a denial-of-service attack at the physical layer, degrading or completely denying the radio communication on which the PPDR network depends. The threat landscape encompasses two distinct but complementary attack surfaces: jamming the 4G/5G air interface and jamming the GNSS (Global Navigation Satellite System) signals that underpin positioning and navigation.

Typically, a terrestrial networks site will consist of sectors which include a combination of 4G and 5G cells. Since these are related to different RF (Radio Frequency) bands their coverage will vary. Degradation or Jamming of the signal can be performed on the downlink or uplink channels and could be wideband interference, or specifically targeting key parts of the band, such as the synchronisation signals which are typically in the centre of the band. Alternatively, other more advanced techniques can be deployed with more sophisticated equipment.

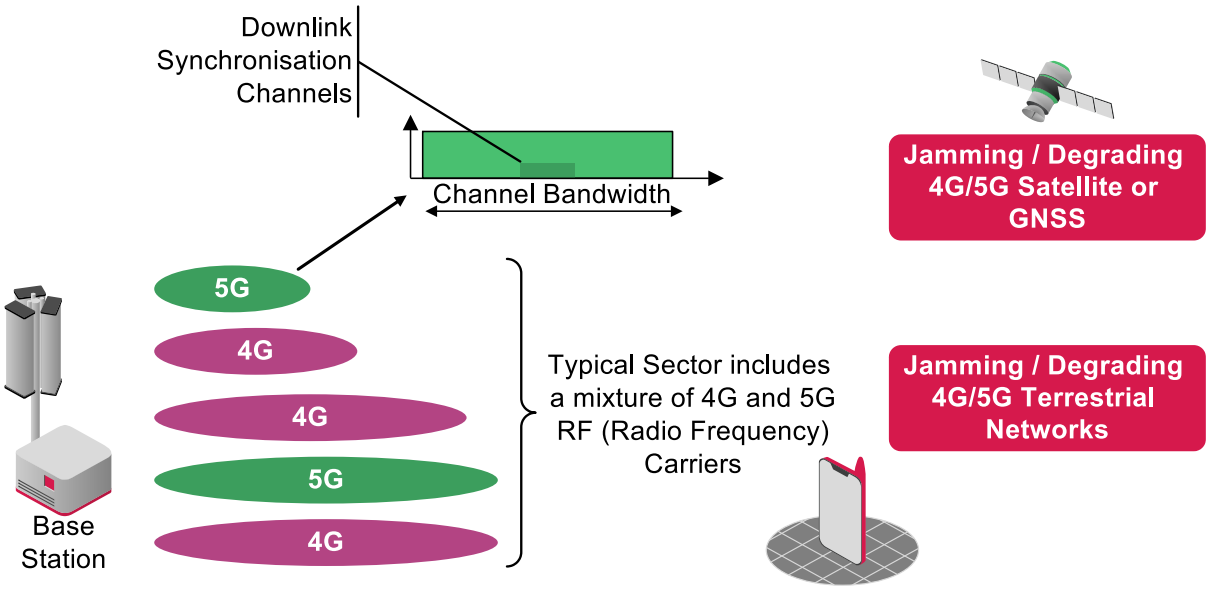

Figure 20 4G/5G and GNSS Vulnerabilities

Power Outages

Power infrastructure underpins every layer of a PPDR communications system. Whether outages are caused by grid failures, deliberate physical attacks, or cascading failures in the wider electrical network, they will ultimately impact a PPDR communication system.

Preventative measures can be implemented by installing UPSs (Uninterruptible Power Supplies) within the RAN, Core Network, and MCX to ensure availability and continuity. Automatic transfer switches can be implemented to transition to generators when the main power supply is lost, with backup generators providing sufficient power to meet high demand. For resilience purposes, an N+1 or N+2 generator capability can be implemented to ensure that power demands are met even if a generator fails. The generators themselves will also require fuel to provide power. Therefore, fuel storage in a secure location must be implemented and maintained. Setting up a supply chain with fuel suppliers can also support rapid stock replenishment when fuel is utilised.

3.3. Human Factors

Technology controls alone cannot secure PPDR systems. The human element (operators, administrators, field personnel, and contractors) remains the most persistent vulnerability across all threat categories.

Figure 21 Human Factors

Countering Misinformation

During major incidents, misinformation spreads across social media faster than official channels can respond, creating two risks for PPDR: the public may self-evacuate in ways that obstruct emergency access or cause secondary incidents; and adversaries may deliberately inject false information into unofficial channels to deceive responders about threat locations or resource needs, which is a documented tactic used within hybrid warfare.

Training and Exercises

Operational resilience must be exercised alongside cyber resilience by implementing tabletop scenarios simulating events such as cellular network failures and MCPTT failures. NCSC guidance recommends that critical national infrastructure operators conduct live-fire cyber exercises at least annually, integrating technical and operational command staff. For PPDR agencies, exercises should also test inter-agency coordination mechanisms for roaming scenarios. National and government-led frameworks, such as the NCSC Exercise in a Box, provide a starting point for tabletop exercises.

Policy and Culture

Even sophisticated security architectures can be undermined by poor access hygiene. Common failure modes include shared credentials, privileged accounts left active after they are no longer required, and unmanaged personal devices introducing malware.

Addressing these requires operationally realistic policies and an effective security culture combining role-based training, clear acceptable use policies, and consequence frameworks that distinguish deliberate violations from unintentional error. Implementing a ZTA (Zero-Trust Architecture) or PAM (Privileged Access Management) tools such as CyberArk or BeyondTrust can provide automated controls over credentials and therefore increase resilience.

3.4. Threat Intelligence, Integration, and Monitoring

Effective cyber resilience requires structured threat intelligence processes that provide continuous, operationally relevant insights into adversary capabilities and intent. Example sources can span both strategic and technical solutions:

- Strategic:
  - NCSC (National Cyber Security Centre).
  - ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information).
  - BSI (Federal Office for Information Security).
- Technical:
  - PSTA (Public Safety Threat Alliance).
  - ENISA (European Union Agency for Cybersecurity).
  - STIX (Structured Threat Information Expression).
  - TAXII (Trusted Automated Exchange of Intelligence Information).

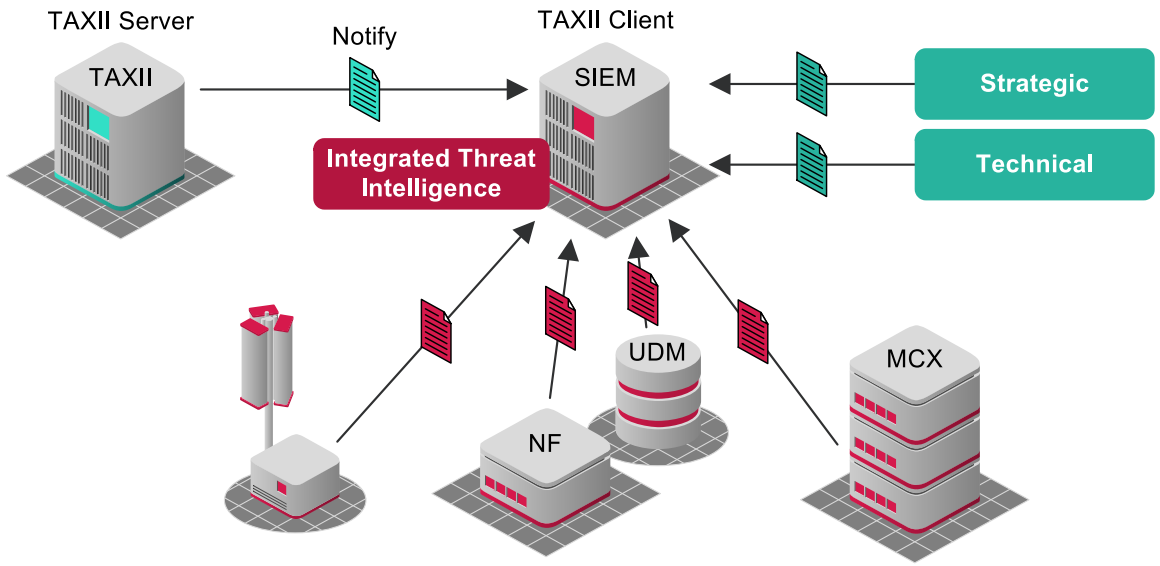

Figure 22 Threat Intelligence Model

From an integration and monitoring perspective, threat intelligence should be integrated with SIEM (Security Information and Event Management) platforms, which aggregate logs from RAN management systems, Core network functions, and the MCX application servers.

Additionally, the SIEM can ingest Threat Intelligence data from external sources such as the aforementioned strategic and technical solutions. Gathered intelligence must be processed and analysed before it has true operational value. Analysis should assess adversary capability, intent, and opportunity. If utilising a Network Slice or components of a public network (RAN Sharing), data gathering may be a responsibility of the MNO (Mobile Network Operator), and it is the job of the PPDR agency to ensure it is being done effectively.

3.5. Incident Response, Restoration, Public Relations, and Trust

When an incident affecting mission-critical infrastructure is detected, the response process must balance technical containment with operational continuity. PPDR deployments cannot simply take a compromised system offline and must therefore adopt a “fight through” posture along the usual implementation of contain, eradicate, and recover sequence that we see applied to traditional infrastructure.

As a working example, a tiered response model aligned to operational impact provides a practical framework:

- Tier 1 – Localised Incident – a single compromised endpoint without service impact.
- Tier 2 – Partial Degradation – manual fallback procedures activate while primary systems are recovered.
- Tier 3 – Catastrophic Failure – full mutual aid and out-of-band communication plans implemented.

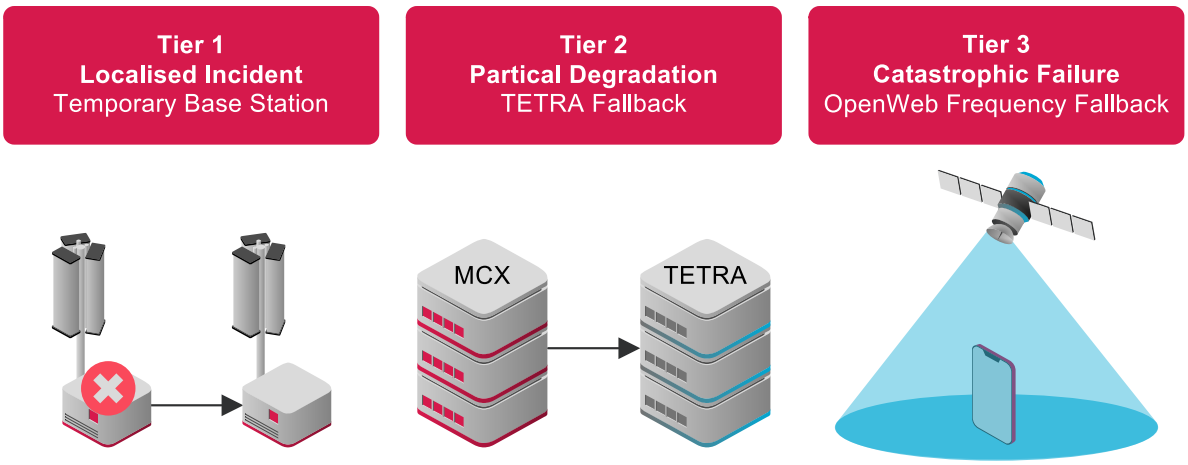

Figure 23 Tiered Response Model

Restoration priorities should be defined by operational criticality, with MCPTT as a priority, as voice coordination remains essential in a degraded network state. If TETRA or P2G fallback infrastructure is available, it should be activated as part of a fallback procedure with the IWF supporting cross-technology talk group continuity throughout the recovery process.

A breach affecting emergency services carries reputational consequences beyond a public network incident, with public confidence impacted by media reporting system failures. Pre-agreed messaging frameworks alongside technical exercises should be implemented to outline the impact of the event without disclosing information that could further impact the network. Long-term recovery will require demonstrable remediation and transparency with oversight bodies such as the ICO (Information Commissioner's Office). It's important to note that the complexity increases when utilising a Network Slice offered by an MNO (Mobile Network Operator), as communication channels can be split, and incident response plans will rely on the MNO to respond accordingly.

The cyber-resilience principles explored in this section find a direct parallel in the way cellular and network infrastructure must be designed and operated to support major public events. Although these events are not PPDR deployments, they still share many of the characteristics required to operate a mission-critical network, such as a zero-tolerance for downtime. Examples include:

- The Paris 2024 Summer Olympics, with a forecasted 3.5 billion (8 times more than observed during Tokyo 2020) cyber-attacks targeting everything from ticketing systems to communication infrastructure.
- For the King of the United Kingdom's Coronation, we saw two different approaches being utilised. The BBC and Neutral Wireless deployed a P5G (Private 5G) network to support network coverage and reduce capacity concerns, whereas Vodafone and Ericsson, working with ITN (Independent Television News), deployed two commercial Network Slices, which were used for live broadcasting of the event.
- The NFL has deployed a mix of private 4G/5G cellular networks across 30 stadiums, with the NFL's CISO describing the approach as explicitly for resilience, noting that cyber and physical security are a single continuum where a compromised system can directly impact the health and safety of the tens of thousands of people within the venue.

Figure 24 Major Public Events

4 AI Threats and Opportunities

The NCSC Assessment on the Impact of AI on cyber threat identifies that skilled cyber actors will highly likely be using AI-enabled automation for elements of the cyber kill chain, supporting scalability and evasive techniques. On the other hand, the growing incorporation of AI models and systems across CNI (Critical National Infrastructure) presents an increased attack surface that adversaries can exploit.

4.1. AI-Powered Attacks

AI presents PPDR agencies with a dual challenge: it is simultaneously a power tool for operational improvement while also expanding the attack surface and barrier to entry for adversaries. Figure 25 outlines a variety of attack mechanisms powered by AI.

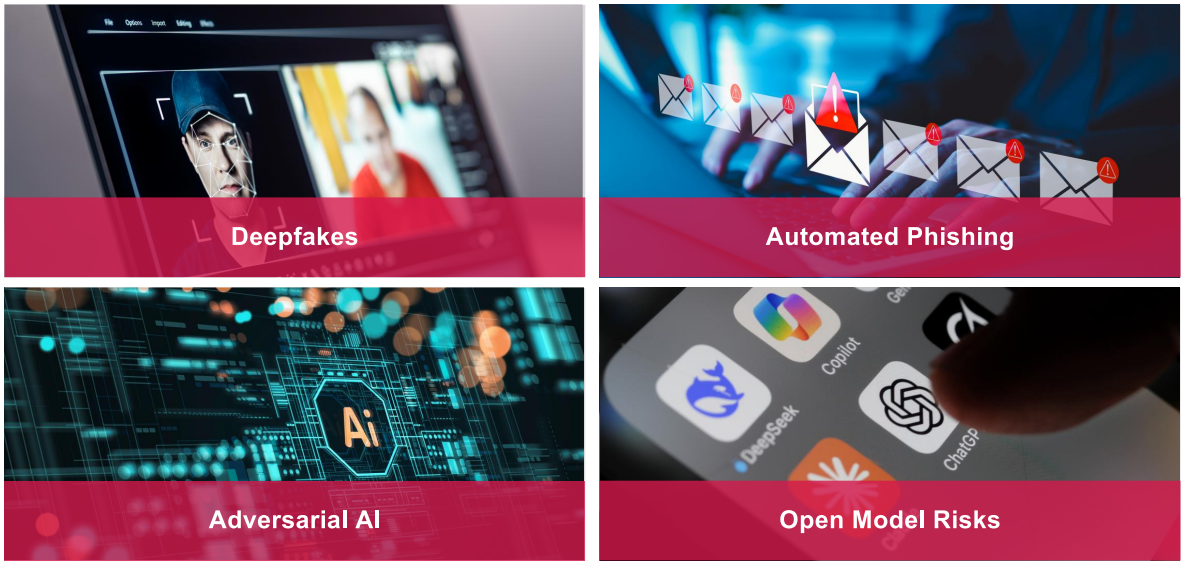

Figure 25 AI Powered Attacks

Deepfakes

AI-generated synthetic audio and video represent a growing threat as primary tools for social engineering and the deliberate spread of misinformation. Commercially available voice-cloning and video synthesis tools can already produce convincing impersonations of senior officers or public officials from minimal source material, leading to spear-phishing campaigns against PPDR staff outside of secure channels. Mitigation focuses on media literacy and verification culture with staff awareness training on synthetic media indicators.

Automated Phishing

Traditional phishing relied on volume to compensate for a low per-target success rate. AI-generated phishing can personalise attacks to each target using publicly available data from

social media and professional directories, producing messages that are contextually plausible and consistent with genuine communications from a known colleague, friend, or supplier.

For PPDR agencies, compromised credentials can expose mission-critical systems. Example mitigation techniques must combine technical controls (email gateway filtering, sandboxed URL analysis, phishing-resistant standards such as FIDO2) with role-specific training tailored to AI-generated threats.

Adversarial AI

Adversarial AI refers to the malicious use of input techniques to deceive, manipulate or sabotage AI-driven systems. Ultimately, adversarial techniques aim to undermine the trust, reliability, and security of AI-driven mission-critical systems. One example is the application of data poisoning attacks, whereby if the model is continuously retrained on incoming network data, adversaries can gradually shift the model's baseline to impact its decision-making outputs.

Open Model Risks

The availability of Large Language Models reduces the barrier to entry for adversaries to develop AI-powered attack tools. Open models can be fine-tuned on PPDR-specific data sets and frameworks to improve the quality and targeted nature of social engineering content. Additionally, open models can also be used to accelerate the understanding of PPDR network architectures for adversaries, reducing the expertise required to perform techniques such as reconnaissance, initial access, and persistence.

An equally important risk is the use of open models within a PPDR agency, which could expose sensitive data, personal information, or network configuration details to open models that lack data governance controls. Agencies are required to mitigate this risk through clear policies and technical controls covering the appropriate use of AI tools. PPDR-ran LLMs can be implemented to deter the use of open models.

4.2. Defensive AI

Beyond its offensive applications, AI plays an equally important role in strengthening the resilience and reliability of mission-critical networks. Defensive AI capabilities span predictive maintenance, resource optimisation, and anomaly detection, each addressing a different layer of operational vulnerability and collectively ensuring that PPDR systems can sustain mission-critical communications under degraded or hostile conditions.

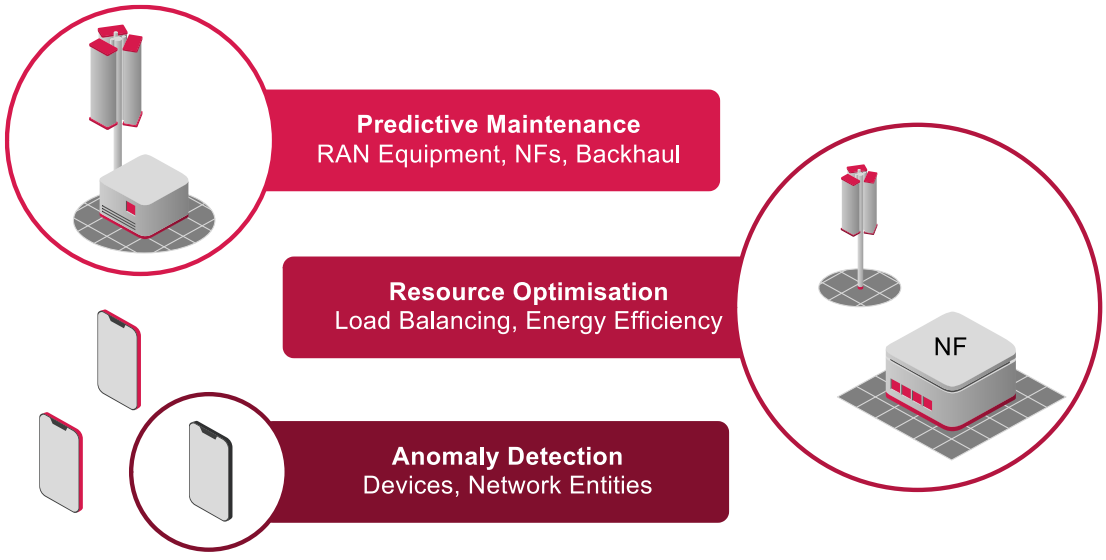

Figure 26 Defensive AI

AI-driven predictive maintenance models continuously analyse key network components, including base station hardware health metrics, power supply status, battery backup capacity, and backhaul link quality, to identify elements at elevated risk of failure before they trigger outages. For PPDR operators, the value of this capability extends beyond simply reducing unplanned downtime; it enables proactive resource positioning that keeps critical communications resilient under pressure.

Complementing this, AI-based RAN resource optimisation models can dynamically adjust cell power, tilt, and antenna beamforming parameters to extend coverage into areas where infrastructure has been lost or degraded. At the core network level, AI-driven load balancing across geographically distributed network functions such as the UPF (User Plane Function) in 5G ensures that the failure or overloading of a single data centre does not create a bottleneck for PPDR session continuity. These capabilities are standardised within the 5G NWDAF (Network Data Analytics Function), which provides a defined interface through which AI-driven optimisation can be applied consistently across the network.

Underpinning both of these functions is the ability to detect anomalies at scale. In a 5G PPDR network, the volume of telemetry generated by network functions far exceeds what any manual review process could handle. Machine learning models trained on baseline network and device behaviour can identify deviations that are both statistically significant and operationally impactful. Importantly, this will require PPDR-specific model training, since commercial mobile network traffic, devices, and network functions behave differently from those in public safety environments.

5 Regulation and Governance

5.1. NIS2

NIS2 is a European Commission directive which targets the security of networking and information systems – hence the NIS (Network and Information Systems) title. In particular, the NIS2 directive introduces a legal framework to which member states must adhere, focusing on 18 critical sectors across the EU. Each member state must define a national cybersecurity strategy, which encompasses cross-border collaboration, with both preventative and reactive measures in place. The key goals for NIS2 are shown in Figure 27.

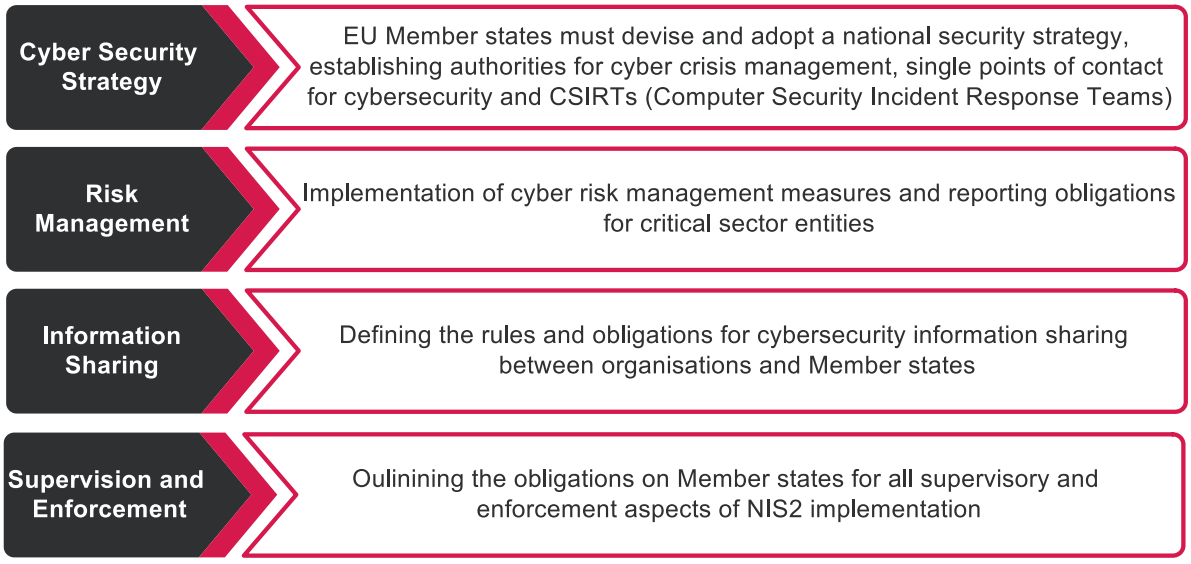

Figure 27 Key Goals for NIS2

Originally, NIS1 covered a smaller number of critical sectors but when NIS1 was reassessed and updated to NIS2, the total number expanded to 18. The latest set of critical sectors is

shown in Figure 28 and applies to both public and private sector organisations that would be classed as medium sized enterprises.

Figure 28 NIS2 Critical Sectors

Although PPDR is not specifically targeted as a sector, it instead serves as an operational use case that can either depend on or support several of these sectors, some with very close ties and others, not so close but still of relevance. For instance, in a PPDR incident, there would be a very heavy reliance on public administration and digital infrastructure; if these sectors were weak in terms of cyber resilience (not adhering to NIS2), it inherently weakens a potential PPDR response. Conversely, a cyber resilience failure in a NIS2 regulated sector such as Chemical Production and Distribution could actually trigger a real world incident that requires a PPDR response.

Figure 29 outlines a selection of key sectors which a PPDR response may need to work with in the event of a natural disaster, terrorist attack, power outage, etc, which highlights why the compliance of these sectors with NIS2 is of paramount importance.

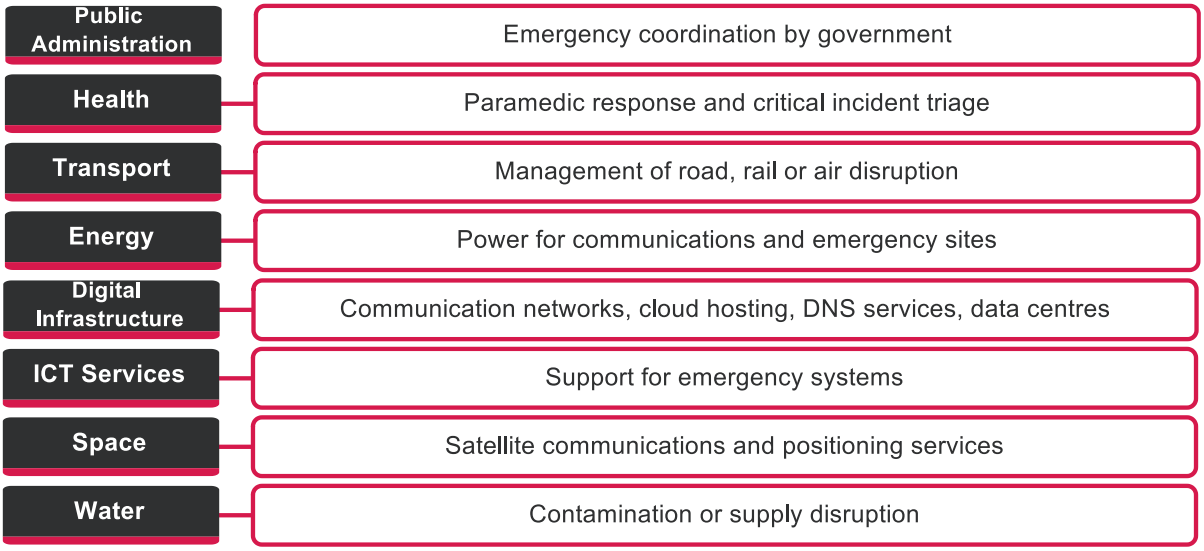

Figure 29 Relationship between PPDR and NIS2 Critical Sectors

5.2. NIST CSF

The NIST CSF (Cybersecurity Framework) 2.0 provides an optional framework for managing cybersecurity risk, and its six core functions: Govern, Identify, Protect, Detect, Respond, and

Recover, map closely to the mandatory obligations introduced by NIS2 surrounding the topic of Risk Management.

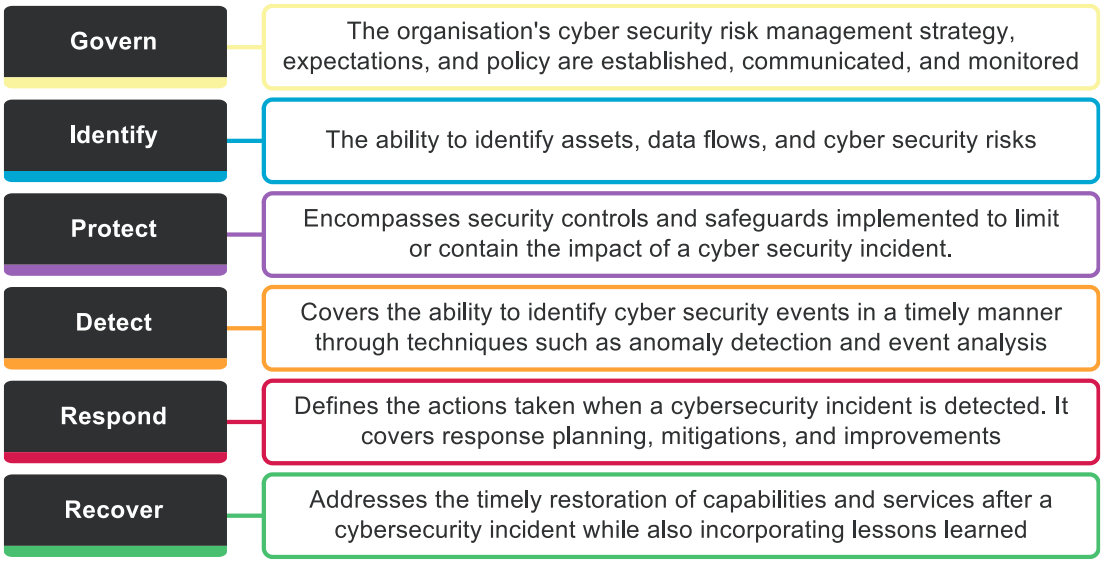

Figure 30 NIST Figure

"Govern" and "Identify" forces PPDR operators to catalogue their most critical assets and direct resources towards protecting what infrastructure matters most. From an asset management perspective, the "Identify" phase outlines hardware inventories, enabling PPDR to track stolen or lost equipment that may have access to MCX services. From a resiliency perspective, "Respond" and "Recover" support PPDR through directly addressing worst-case scenarios, enabling the development of pre-tested response and recovery plans, defining RTO (Recovery Time Objectives), and implementing diverse continuity arrangements.

5.3. EU AI Act

The EU AI Act, which entered into force on 1st August 2024, directly regulates AI systems used in public safety and critical national infrastructure. This is a PPDR-relevant Act as PPDR organisations are potentially deployers of high-risk AI systems. Key PPDR use cases that fall within the AI Act's scope include: predictive threat intelligence, risk assessment tools, AI in the RAN, AI in the Core Network, AI in MCX applications, and anomaly detection.

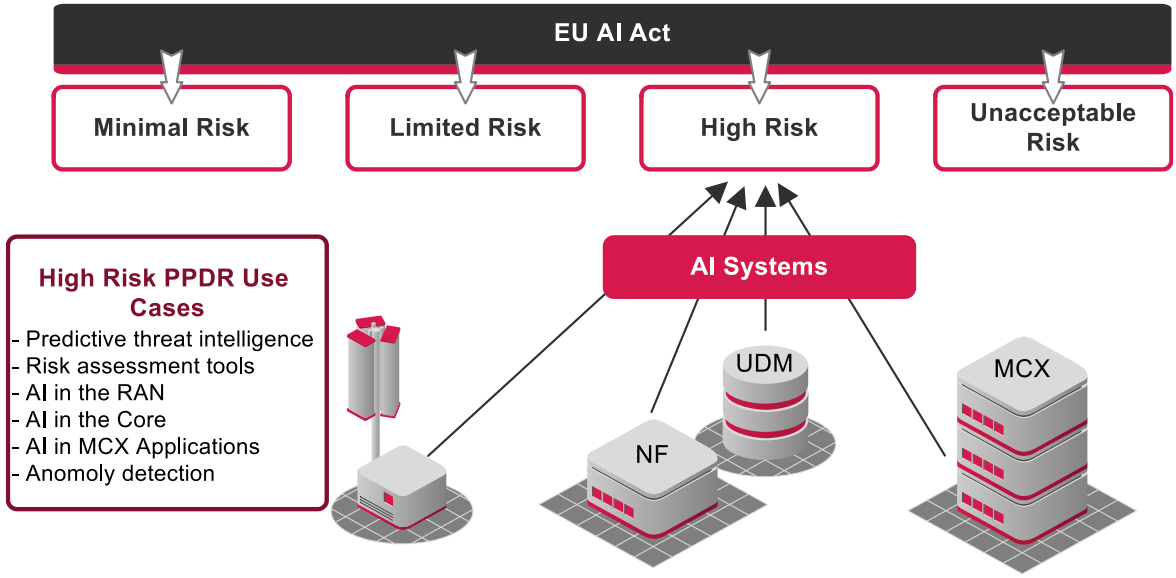

Figure 31 EU AI Act

A cornerstone of the EU AI Act is the requirement for meaningful human oversight of high-risk AI decisions. In PPDR contexts, this means that an AI-assisted system must be reviewable and overridable by human operators. For risk management-related tasks, outputs must be presented as decision-support tools, not determinative outputs. Operators are also required to understand AI system limitations and to detect signs of malfunction and bias.

Deployers of high-risk AI must implement post-market monitoring systems to actively collect and review data on system performance in real-world conditions. Serious incidents defined as system malfunctions causing death, serious harm, fundamental rights violations, or significant property damage must be reported to national authorities. For PPDR organisations, this creates a dual reporting obligation where AI incidents may simultaneously trigger a NIS2 incident report.

Glossary

5G-AKA (5G Authentication and Key Agreement)
AiTM (Adversary-in-the-Middle)
AMF (Access and Mobility Management Function)
ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)
ATSSS (Access Traffic Steering, Switching, and Splitting)
BIOS (Basic Input/Output System)
BSI (Federal Office for Information Security)
C5 (Cloud Computing Compliance Criteria Catalogue)
CAD (Computer-Aided Dispatch)
CEPT (European Conference of Postal and Telecommunications Administrations)
CLOUD (Clarifying Lawful Overseas Use of Data Act)
CNI (Critical National Infrastructure)
CoLT (Cells on Light Trucks)
CoW (Cells on Wheels)
CSF (Cybersecurity Framework)
CSPs (Cloud Service Providers)
DEA (Diameter Edge Agent)
E2EE (End-to-End Encryption)
EDR (Endpoint Detection and Response Tools)
EEA (EPS Encryption Algorithm)
EENA (European Emergency Number Association)
EIA (EPS Integrity Algorithm)
eMBB (Enhanced Mobile Broadband)
eMBMS (Evolved Multimedia Broadcast Multicast Service)
ENISA (European Union Agency for Cybersecurity)
EPC (Evolved Packet Core)
GCSE (Group Communication System Enablers)
GDPR (General Data Protection Regulation)
GNSS (Global Navigation Satellite System)
GSSI (Group Short Subscriber Identity)
HAPS (High-Altitude Platform Stations)
H-PCRF (Home PCRF)
HSE (Hardware Security Element)
IAM (Identity and Access Management)
ICO (Information Commissioner's Office)
I-CSCF (Interrogating-CSCF)
IMS (IP Multimedia Subsystem)
IMS-AKA (Authentication and Key Agreement)
IOC (Isolated Operation Core)
IOPS (Isolated E-UTRAN Operation for Public Safety)
IPSec (Internet Protocol Security)
IPUPS (Inter-PLMN User Plane Security)
ISAC (Integrated Sensing and Communications)
ITN (Independent Television News)
IWF (Interworking Function)
JOSE (JSON Object Signing and Encryption)
KMS (Key Management Server)
LEWP (Law Enforcement Working Party)
LMR (Land Mobile Radio)
LTE (Long-Term Evolution)
MC (Mission Critical)
MCData (Mission Critical Data)
MCPTT (Mission Critical Push to Talk)
MCS (Mission Critical Security)
MCVideo (Mission Critical Video)
MCX (Mission Critical Services)
mMTC (Massive Machine Type Communications)

MNO (Mobile Network Operator)
NADF (Network Anomaly Detection Function)
NAS (Non-Access Stratum)
NCSC (National Cyber Security Centre)
NEA (NR Encryption Algorithm)
NF (Network Function)
NIA (NR Integrity Algorithm)
NIS (Network and Information Systems)
NR (New Radio)
NRF (Network Repository Function)
NSI (Network Slice Instance)
NSSAA (Network Slice-Specific Authentication and Authorisation)
NSSIs (Network Slice Subnet Instances)
NTN (Non-Terrestrial Network)
NWDAF (Network Data Analytics Function)
P5G (Private 5G)
PAM (Privileged Access Management)
P-CSCF (Proxy-Call Session Control Function)
PhaaS (Phishing as a Service)
PNT (Positioning, Navigation, and Timing)
PPDR (Public Protection and Disaster Relief)
ProSe (Proximity Services)
PSAP (Public Safety Answering Point)
PSTA (Public Safety Threat Alliance)
QCIs (Quality Class Identifiers)
RF (Radio Frequency)
RRC (Radio Resource Control)
SAR (Search and Rescue)
SBI (Service-Based Interfaces)
SCP (Service Communication Proxy)
S-CSCF (Serving-CSCF)
SD (Slice Differentiator)
SDS (Short Data Service)
SEPP (Security Edge Protection Proxy)
SIEM (Security Information and Event Management)
SIP (Session Initiation Protocol)
SST (Slice/Service Type)
STIX (Structured Threat Information Expression)
SUPI (Subscription Permanent Identifier)
TAXII (Trusted Automated Exchange of Intelligence Information)
TETRA (Terrestrial Trunked Radio)
TETRA ISSI (TETRA Individual Short Subscriber Identity)
TN (Terrestrial Networks)
TPI (Two-Person Integrity)
TPM (Trusted Platform Module)
TTPs (Tactics, Techniques, and Procedures)
UEBA (User and Entity Behaviour Analytics)
UEFI (Unified Extensible Firmware Interface)
UPF (User Plane Function)
UPIP (User Plane Integrity Protection)
URLLC (Ultra-Reliable Low-Latency Communication)
V-PCRF (Visited PCRF)
ZTA (Zero-Trust Architecture)