# Public Safety Communication as Strategic Infrastructure in European Security Policy

V1.0

Authors: Laurie Ibbs, Rebecca Robinson

Reviewed by: David Lund

12th April 2026

This report is a product of learnings from the Horizon Europe, Smart Networks and Services (SNS) project:

Field Trials beyond 5G (FIDAL).

Project ID: 101096146

PSCE lead the Security work in FIDAL. It was determined that there were many learnings in the context of Public Safety Mobile Communication Infrastructure and Services, which are considered useful to collate in this document. This provides a useful view of the state-of-play regarding security and resilience of Public Safety Mobile Communication Infrastructure and Services.

This document is written primarily for use by the European Commission and European and Schengen Associated Member States, in preparation for the establishment of the European Critical Communication System (EUCCS).



Funded by the European Union

# Contents

Executive Summary: ..... 4
1. Introduction: Reframing PPDR Communications ..... 5
1.1 Purpose and scope of the study ..... 5
1.2 Why PPDR Communications Should Be Treated as Strategic Infrastructure ..... 5
1.3 From Telecommunications Function to Security and Resilience Asset ..... 5
1.4 Core Argument and Structure of the Study ..... 6
2. PPDR Telecommunications as Critical European Infrastructure ..... 7
2.1 Role in Crisis Response and Internal Security ..... 7
2.2 Systemic Interdependence Across the Single Market ..... 7
2.3 Hybrid and Cross-Border Threat Exposure ..... 8
3. The Evolving Threat Landscape for PPDR Communications ..... 10
3.1 Intelligence Exploitation, Metadata Targeting and RF Fingerprinting ..... 10
3.2 Persistent State-Backed Access Campaigns ..... 10
3.3 Space-Based and LEO-Enabled SIGINT as an Emerging Threat Vector ..... 11
3.4 Disruptive Cyber Operations and Signalling Manipulation ..... 11
3.5 Physical-Cyber Convergence and AI-Enabled Threats ..... 11
3.6 The Human Attack Surface: Insider Threat and Social Engineering ..... 12
3.7 Systemic Threat Patterns in PPDR Communications ..... 12
4. Regulatory Frameworks and EU Governance ..... 13
4.1 NIS2, the Cyber Resilience Act, and the 5G Toolbox ..... 13
4.2 High-Risk Vendor Controls and Implementation Gaps ..... 13
4.3 Cross-Border Governance and Regulatory Fragmentation ..... 14
4.4 Compliance, Auditing, and Accountability Mechanisms ..... 14
4.5 Governance Limits and Structural Implications ..... 14
5. Structural and Architectural Vulnerabilities in European Telecommunications Networks ..... 16
5.1 Control, User and Management Plane Exposure ..... 16
5.2 Legacy Signalling and Interconnection Risks ..... 16
5.3 Cloud-Native and 5G Core Dependencies ..... 17
5.4 Open RAN, Software-Defined Radio and Multi-Vendor Risk ..... 17
5.5 Organisational Fragmentation and Collective Cybersecurity Gaps ..... 18
5.6 Structural Vulnerabilities and Systemic Risks in Future PPDR Communications Infrastructure ..... 19
6. Supply Chain and Software Integrity Risk ..... 20
6.1 Vendor Dependency and High-Risk Vendor Controls ..... 20
6.2 Software Assurance, CI/CD Pipelines and Orchestration Security ..... 21
6.3 Hardware Trust, Firmware Integrity and Embedded Risk ..... 22
6.4 Procurement Governance and Whole-of-Lifecycle Assurance ..... 23
6.5 Systemic Risk and Structural Limitations ..... 23
7. Sovereignty, Strategic Autonomy and Industrial Resilience ..... 25
7.1 Sovereignty, Extraterritorial Risk and Cloud Jurisdiction ..... 25
7.2 Sovereign Infrastructure as a PPDR Trust Requirement ..... 25
7.3 EU Telecom Industrial Strategy and Supply Chain Resilience ..... 26
7.4 Security as Strategic Competitive Advantage ..... 26
8. Incident Response and Cross-Border Crisis Coordination ..... 28

8.1 Detection, Escalation and Speed Asymmetry ..... 28
8.2 Restoration Sequencing for PPDR Services ..... 28
8.3 Degraded-Mode and Fallback Communications ..... 29
8.4 EU-Level Coordination (ENISA, CERT-EU, CyCLONe) ..... 29
8.5 Implications for multi-agency response capability ..... 30
9: Building a Secure and Resilient PPDR Telecom Architecture ..... 31
9.1 Zero-Trust and Identity Segmentation in Core Networks ..... 31
9.2 Encryption, Key Management and Secure Signalling ..... 31
9.3 Emissions Security and Transmission Discipline ..... 32
9.4 Network Slicing Integrity and MCX Service Protection ..... 32
9.5 Secure Roaming and Cross-Border Identity Trust ..... 33
9.6 Threat Intelligence Integration, Monitoring and Active Defence ..... 33
10. Investment, Capability and 6G Strategic Positioning ..... 34
10.1 Workforce, Skills and Specialist Capability Development ..... 34
10.2 Strategic Investment Needs and EU Funding Mechanisms ..... 34
10.3 6G Architecture, PPDR Requirements and Standards Leadership ..... 35
10.4 Open RAN, Vendor Diversification and Industrial Opportunity ..... 35
Closing Remarks ..... 36
11 Conclusion ..... 37
Bibliography ..... 39

# Executive Summary

Public Protection and Disaster Relief (PPDR) communications systems should be understood as a strategic component of Europe's security and resilience architecture, rather than solely as a telecommunications capability. They enable coordination, situational awareness, and command during emergencies, and directly underpin the ability of public authorities to act effectively in crisis. When these systems function, emergency response is coherent and authoritative; when they fail, the consequences are immediate, visible, and operationally significant.

Historically, PPDR communications were delivered through dedicated, self-contained networks designed to ensure availability, control, and resilience under adverse conditions. This model provided public authorities with a high degree of assurance over mission-critical communications. However, this position has fundamentally shifted. Modern PPDR capabilities are increasingly dependent on commercial broadband networks, cloud-based services, and complex, software-defined infrastructures. Mission-critical communications are now embedded within a wider and highly interdependent digital and telecommunications ecosystem.

This structural shift alters the risk profile of PPDR communications. Dependence on external operators, vendors, and service layers introduces systemic dependencies over which public authorities often lack direct control. Functions are expressed as software and distributed across networked environments, where the integration of communications infrastructure expands the potential attack surface and complicates assurance. PPDR communications can no longer be considered in isolation as a bounded telecommunications function; they must be understood as part of a broader infrastructure environment in which vulnerabilities, disruptions, or compromises in adjacent systems can directly affect operational capability.

The evolving threat landscape reinforces this change. Telecommunications infrastructure is subject to persistent exploitation by state and non-state actors, including through signalling vulnerabilities, supply chain compromise, and access to management and orchestration layers. These risks are not confined to individual components, but arise from the systemic characteristics of interconnected infrastructure. In this context, the resilience of PPDR communications is inseparable from the resilience of the wider ecosystems on which they depend.

Existing governance and regulatory frameworks have not fully adapted to this reality. While instruments such as NIS2, the Cyber Resilience Act, and the EU 5G Toolbox address important aspects of telecommunications and cybersecurity risk, they are not designed to assure control, availability, and integrity of mission-critical communications under crisis conditions. As a result, there is a growing misalignment between the operational role of PPDR communications and the way in which they are governed, secured, and assured.

# 1. Introduction: Reframing PPDR Communications

## 1.1 Purpose and scope of the study

This study examines Public Protection and Disaster Relief (PPDR) communications within Europe's evolving security and resilience architecture. It focuses on how these systems operate, how they are embedded in wider telecommunications and digital infrastructures, and how this affects reliability during crises.

Aimed at policymakers, regulators, and security professionals, it combines technical, operational, and policy perspectives to assess how PPDR communications function in practice and how they have evolved. The study provides a structured analysis of the systems, dependencies, and governance conditions shaping their resilience, positioning them as components of strategic infrastructure within complex, interdependent environments.

## 1.2 Why PPDR Communications Should Be Treated as Strategic Infrastructure

PPDR communications are often viewed as specialised telecommunications services, but this understates their role in Europe's security architecture. They enable coordination, situational awareness, and command during crises, functions essential to effective state response.

As such, they constitute critical infrastructure: disruptions can cascade into emergency response, public safety, and governance. Their importance is amplified by a structural shift from dedicated networks to integration with commercial telecommunications and digital services, creating dependencies across sectors such as telecoms, cloud, energy, and data infrastructure.

Consequently, resilience depends not only on individual systems but on the wider ecosystems in which they operate. Risks are increasingly systemic and interdependent, extending beyond direct public control. PPDR communications must therefore be understood as strategic infrastructure, both enabling and dependent on broader critical systems.

## 1.3 From Telecommunications Function to Security and Resilience Asset

Historically, PPDR communications relied on dedicated, self-contained networks designed for control and reliability. This model allowed risks to be managed within clearly defined technical and organisational boundaries.

The shift to broadband and data-driven capabilities has integrated these systems into commercial networks, cloud platforms, and software-defined environments. Control is now mediated through external providers, while system behaviour depends on complex software and infrastructure layers.

This transformation makes PPDR communications a distributed capability rather than a bounded system. Risks arise from interactions across infrastructure layers, organisations, and sectors, meaning disruptions in telecoms, cloud, energy, or supply chains can directly affect communications.

PPDR communications are therefore better understood as a security and resilience asset. Their reliability depends on broader infrastructure ecosystems, and their failure impacts crisis response, public safety, and state effectiveness.

## 1.4 Core Argument and Structure of the Study

PPDR communications can no longer be treated as a discrete telecommunications function. Their integration into complex, commercially operated, and software-defined environments makes them a form of strategic infrastructure shaped by system-level dependencies and governance conditions.

Risks emerge from interconnected infrastructure, organisational actors, and cross-border dependencies, placing reliability beyond the sole control of public authorities.

The study progresses from operational roles to systemic risks, examining crisis response functions, threats, governance frameworks, and network architectures. It then analyses supply chains, software dependencies, and issues of sovereignty and jurisdiction, before exploring how incidents are managed across Europe.

Finally, it identifies the conditions for resilient communications and outlines implications for governance, procurement, sovereignty, and system design within Europe’s security and resilience architecture.

# 2. PPDR Telecommunications as Critical European Infrastructure

PPDR communications support state response operations and enable continuity of public authority during crises.

Cyber operations, infrastructure sabotage, and hybrid threat activity increasingly target the critical infrastructure systems that underpin state response capacity. Disruptions affecting communications infrastructure degrade coordination and crisis management functions.

## 2.1 Role in Crisis Response and Internal Security

PPDR communications provide the operational backbone for police services, emergency medical services, fire and rescue authorities, and civil protection organisations. These services operate in time-critical environments where communication failure can have immediate operational consequences. As a result, PPDR systems must meet stringent requirements for reliability, availability, and security that exceed those typically associated with commercial communications services [4], [5].

Reliable communications enable coordination between command centres and field personnel, supporting the dispatch of resources, the management of incidents, and the maintenance of situational awareness during rapidly evolving emergencies. These capabilities increasingly extend beyond mission-critical voice to include the exchange of operational data such as real-time video, geolocation information, and access to incident management systems, reflecting the growing reliance of emergency services on broadband-enabled digital tools [7], [14].

Despite this evolution, mission-critical voice communication remains fundamental to responder safety. In hazardous operational environments, secure two-way communication provides the primary mechanism through which personnel coordinate activity, request support, and maintain contact with command structures. Degradation or loss of these capabilities can rapidly reduce operational effectiveness and increase risk to personnel [5].

The consequences of disruption extend beyond the communications domain. Failures in PPDR systems can delay response, fragment coordination between agencies, and impair rescue or law-enforcement operations. In severe cases, such disruptions may contribute to loss of life and undermine the ability of public authorities to manage major incidents effectively [7], [5].

PPDR communications support operational coordination and the continuity of public authority in crisis conditions [3].

## 2.2 Systemic Interdependence Across the Single Market

European crisis response increasingly operates within an interconnected and cross-border operational environment. Major incidents frequently involve multiple jurisdictions and require coordinated action between authorities across Member States. In this context, PPDR communications form part of a broader “system of systems” linking national emergency services, telecommunications infrastructure, and European crisis-management mechanisms [3].

Cross-border interoperability is a critical requirement within this environment. Emergency services operating near borders, or responding to transnational threats such as organised crime or natural disasters, must be able to communicate across jurisdictions and maintain operational mobility. Fragmentation between national systems or regulatory frameworks can therefore create operational barriers that directly affect the effectiveness and timeliness of coordinated response [4].

Many Member States are adopting hybrid architectures in which public safety communications operate partly on dedicated networks and partly through commercial broadband infrastructure, including virtual operator and shared-network models [1], [2]. While these approaches can improve scalability and access to innovation, they also introduce structural dependencies between mission-critical emergency communications and the wider telecommunications ecosystem.

Failures within commercial telecommunications networks directly affect the availability and performance of emergency communications services via so called "*Spill-over effects"* [12]. These dependencies are further compounded by cross-sector interconnections. Telecommunications networks rely on electricity supply and physical infrastructure, while the restoration of energy systems and other essential services depends on functioning communications networks. Disruptions in one sector can therefore cascade across others, amplifying the operational impact [11], [12].

## 2.3 Hybrid and Cross-Border Threat Exposure

Critical infrastructure systems are exposed to cyber operations, hybrid interference, and state-sponsored disruption [10]. Telecommunications infrastructure has become a particularly attractive target due to its central role in enabling economic activity, government operations, and crisis response [12]. As a result, disruptions affecting communications infrastructure may have immediate and wide-ranging operational consequences across multiple sectors.

PPDR systems are directly exposed to these threat dynamics. Sophisticated threat actors have demonstrated the capability to infiltrate infrastructure networks, maintain persistent access, and position themselves for disruptive activity during periods of crisis [8], [12], [69]. This may result in degraded emergency response capabilities not only via direct attack, but through compromise of the underlying systems on which they depend.

The transition toward broadband PPDR networks based on evolving mobile communications technologies, including LTE and 5G, further expands this exposure. These architectures rely on increasingly complex ecosystems of hardware vendors, software providers, and service operators. As these systems continue to evolve toward more distributed, software-defined, and service-based architectures, they support greater flexibility and capability development, but also increase the potential attack surface and introduce additional vulnerabilities through supply-chain dependencies, software integration, and vendor relationships [7], [9].

Europe's connectivity also depends on global communications infrastructure, particularly submarine fibre-optic cable systems that carry the majority of international data traffic. Disruption to these networks (whether through cyber operations, physical sabotage, or geopolitical conflict) could significantly degrade connectivity across large regions of Europe [13].

For emergency services that increasingly rely on broadband connectivity and digital platforms, such disruptions may have direct operational consequences. Attacks on wider communications infrastructure can impair emergency response capability even when PPDR systems themselves are not directly targeted.

# 3. The Evolving Threat Landscape for PPDR Communications

Modern telecommunications operate within a complex cyber-physical environment spanning digital networks, RF systems, satellites, and global interconnection. This exposes PPDR communications to disruptions beyond their operational boundaries.

They face diverse threats including persistent cyber intrusions, metadata and electromagnetic intelligence exploitation, satellite-enabled SIGINT, signalling manipulation, cyber-physical disruption, and social engineering. These can combine to produce cascading, hard-to-detect failures. As communications underpin coordination and command, they are highly sensitive to disruption.

## 3.1 Intelligence Exploitation, Metadata Targeting and RF Fingerprinting

As PPDR systems integrate with broader infrastructure, communications activity itself becomes an intelligence source. While encryption protects content, it does not prevent analysis of metadata and signal behaviour.

Timing, frequency, and signal characteristics can reveal operational patterns, enabling adversaries to infer deployments and response tempo. Techniques such as radio frequency fingerprinting exploit hardware imperfections to identify individual transmitters independently of content.

Despite some variability, these capabilities enable persistent tracking of devices and operations [17]. The resulting electromagnetic footprint (especially during crisis surges) can expose response structures and activity even when communications are encrypted.

This shifts security requirements beyond confidentiality toward managing behavioural and electromagnetic exposure in contested environments.

## 3.2 Persistent State-Backed Access Campaigns

Telecommunications infrastructure is a priority target for state-backed cyber campaigns seeking persistent access for intelligence collection. Compromised networks can expose call data and sensitive communications, including lawful interception systems [16].

Attackers often use “living-off-the-land” techniques to evade detection, allowing long-term presence within networks. By exploiting routers, authentication systems, and management platforms, they can gain covert, large-scale visibility into communications flows.

As PPDR systems increasingly depend on commercial networks, such compromises can expose emergency communications. This includes operational data on deployments and crisis coordination.

Security models must therefore adopt an “assume compromise” posture, focusing on detection, resilience, and continuity rather than perimeter defence alone [15].

## 3.3 Space-Based and LEO-Enabled SIGINT as an Emerging Threat Vector

The growth of commercial Low Earth Orbit (LEO) satellites has expanded access to signals intelligence. Capabilities once limited to states are now available via commercial platforms that detect and geolocate RF emissions globally.

These systems enable persistent monitoring of radio activity across jurisdictions without terrestrial infrastructure. This “democratisation” of RF intelligence broadens access to electromagnetic surveillance [18].

For PPDR systems, which rely heavily on radio, this creates new exposure. Crisis-driven surges in communications can generate detectable electromagnetic signatures, enabling large-scale observation of response activities.

Current policy frameworks focus on cyber threats but give limited attention to space-based RF monitoring, creating a governance gap. As these capabilities expand, resilience planning must incorporate electromagnetic and space-based exposure.

## 3.4 Disruptive Cyber Operations and Signalling Manipulation

Beyond intelligence gathering, adversaries may disrupt telecommunications by targeting signalling and routing layers. Protocols such as SS7 and Diameter contain structural vulnerabilities due to legacy trust models [19].

Exploitation can enable geolocation, interception, or traffic redirection, often bypassing application-level protections. These attacks are difficult to detect due to their position within core network functions. The associated risks are further amplified by emerging AI-assisted techniques, which lower the barrier to entry for complex signalling attacks and enable more scalable and adaptive exploitation [70].

Similarly, vulnerabilities in inter-domain routing protocols such as BGP can be exploited to redirect or disrupt traffic across networks, including through route hijacks or leaks that may originate from within participating autonomous systems [71]. While secure-by-design alternatives such as SCION have been proposed to mitigate these weaknesses, their deployment remains limited, and BGP continues to dominate global routing infrastructure [72].

For PPDR communications, disruptions threaten operational availability. Failures in signalling or routing can cascade across systems, exposing dependence on external infrastructure beyond public control.

## 3.5 Physical-Cyber Convergence and AI-Enabled Threats

Communications systems now operate across tightly coupled cyber and physical domains. Disruption can propagate between digital networks, RF infrastructure, and physical assets.

Attacks may combine cyber intrusion with electronic warfare techniques such as jamming or spoofing, degrading communications and positioning systems [22].

Artificial intelligence is accelerating these threats by enabling automated reconnaissance, vulnerability discovery, and pattern analysis. This increases the speed and scale of attacks, including rapid identification of operational targets [70] [22].

The result is a multi-vector threat environment where systems may be attacked simultaneously across layers, complicating detection and mitigation, especially where dependencies extend beyond public authority control.

## 3.6 The Human Attack Surface: Insider Threat and Social Engineering

Human factors remain a critical vulnerability. Social engineering attacks can bypass technical controls by targeting personnel for credential access or system manipulation.

Recent incidents demonstrate that attackers can successfully exploit support staff through social engineering to obtain privileged access, including bypassing multi-factor authentication and credential controls. Notable cases include attacks on major enterprises and service providers, where help desk personnel were manipulated into resetting credentials or granting access, ultimately undermining otherwise secure systems [74] [75].

In PPDR contexts, reliance on multiple vendors and service providers distributes access across many actors, increasing exposure and reducing direct oversight. This organisational complexity significantly enlarges the human attack surface.

## 3.7 Systemic Threat Patterns in PPDR Communications

Several structural patterns define the evolving threat landscape.

First, adversaries increasingly target infrastructure and metadata rather than content, reducing the effectiveness of confidentiality-focused security models.

Second, integration with commercial infrastructure introduces systemic dependencies, where external vulnerabilities can directly affect emergency communications.

Third, the operating environment is increasingly contested across cyber, electromagnetic, and space domains, enabling continuous monitoring and potential disruption.

Finally, human vulnerabilities remain significant, particularly in complex, multi-actor environments.

Overall, risks to PPDR communications arise from interconnected cyber, electromagnetic, space-based, and human factors within a highly interdependent ecosystem [21]. Modern systems operate under conditions of persistent access, infrastructure vulnerability, and expanded attack surfaces extending beyond the communications layer.

# 4. Regulatory Frameworks and EU Governance

European telecommunications governance is shifting from sector-specific regulation to a cross-sector resilience model. For PPDR communications, this is significant: systems are now governed within a broader EU framework for cybersecurity, critical infrastructure, and crisis coordination, with control distributed across multiple actors and layers [3], [23], [24].

## 4.1 NIS2, the Cyber Resilience Act, and the 5G Toolbox

At the centre of this framework is the NIS2 Directive, which establishes a harmonised baseline for cybersecurity risk management and incident reporting across critical sectors, including telecommunications [23]. It reframes telecom networks as core components of European resilience rather than purely commercial services.

NIS2 reduces fragmentation but embeds telecoms within a generalised framework not tailored to mission-critical performance. With the removal of sector-specific provisions from the European Electronic Communications Code, it becomes the primary instrument for telecom security, shifting responsibility onto operators to interpret broad requirements. This introduces variability that may not prioritise public safety use cases [23], [25].

The proposed Cyber Resilience Act extends cybersecurity obligations to both hardware and software products, introducing lifecycle security requirements and explicitly addressing supply chain risks [26], [27]. This expands the regulatory scope from network infrastructure to individual components, increasing reliance on the security of third-party products within PPDR systems.

In parallel, the EU 5G Toolbox provides targeted, though non-binding, measures addressing risks from virtualisation, centralisation, and supplier dependencies, including high-risk vendors [9], [28].

Together, these instruments create a layered governance model combining horizontal regulation, product security, and targeted risk mitigation. However, differences in legal status, scope, and timelines introduce practical complexity for operators and complicate compliance and investment decisions.

## 4.2 High-Risk Vendor Controls and Implementation Gaps

High-risk vendor management remains politically and operationally complex. While the 5G Toolbox provides a common framework, implementation is left to Member States, resulting in uneven application. [64]

This reflects limits in EU competence over national security but creates structural weaknesses. EU-level assessments highlight risks from supplier dependency and market concentration [9], yet implementation varies due to national economic and political priorities.

Differences are evident in restrictions on high-risk vendors in critical domains such as the Radio Access Network. Some states apply strict controls, while others adopt partial or delayed measures. This fragmentation weakens collective risk mitigation, as vulnerabilities in one network can affect others across interconnected systems [9], [28].

For PPDR communications, reliance on commercial networks operating under uneven security conditions means resilience depends on decisions beyond public authority control. Market dynamics—cost, speed, and vendor lock-in—often outweigh long-term security considerations unless enforced.

## 4.3 Cross-Border Governance and Regulatory Fragmentation

Effective PPDR communications require seamless cross-border operation, supported by aligned standards and procedures. EU frameworks such as NIS2 and the CER Directive aim to provide common baselines [23], [24], but implementation remains uneven due to national sovereignty.

Flexibility provisions allowing exclusions for national security and law enforcement create uneven application of resilience requirements. This leads to parallel regimes within shared operational environments, complicating coordination during crises.

Divergent national approaches to reporting, certification, and technical standards introduce operational friction. ENISA reporting shows inconsistencies in incident handling and information sharing, limiting situational awareness and delaying coordinated responses [10].

EU coordination mechanisms such as the Cyber Blueprint and EU-CyCLONe improve information exchange [31], but operate within a decentralised system dependent on voluntary cooperation.

As a result, cross-border PPDR operations face reduced reliability and increased uncertainty, where failures in one jurisdiction can impact others.

## 4.4 Compliance, Auditing, and Accountability Mechanisms

A key challenge is the gap between formal compliance and operational security. Although NIS2 strengthens supervisory powers, application remains uneven across Member States.

Limited technical expertise within national authorities constrains effective oversight of complex telecom systems, including virtualised and cloud-based infrastructures. Operators increasingly manage critical trust functions (e.g. certificate authorities), sometimes without full awareness of systemic risks.

This creates latent vulnerabilities that are difficult to detect through compliance-based audits. Many regulators lack the capacity for deep, system-level assessment, leading to a focus on procedural compliance rather than operational resilience [25], [32].

Incident reporting frameworks also show limitations. While operators must report extensively, feedback is often limited [25], reducing the value of reporting for collective security and reinforcing a compliance-driven approach [33], [10]. This weakens shared situational awareness.

## 4.5 Governance Limits and Structural Implications

The EU has developed a comprehensive framework for telecommunications security, reflecting its strategic importance. However, effectiveness depends on implementation, where gaps remain between policy and operational assurance [32]. European measures such as the NIS2 Directive and

Critical Entities Resilience Directive remain primarily focused on terrestrial cyber and physical infrastructure.

As outlined in the previous section, the growing availability of LEO satellite systems is enabling a “democratisation of RF intelligence,” allowing a wider range of actors to observe and analyse radio-frequency activity at scale. This challenges assumptions around control, visibility, and jurisdiction, positioning space-based sensing as an under-addressed frontier in current security frameworks.

Fragmentation, uneven supervisory capacity, and misalignment between market incentives and security objectives constrain resilience. These systemic features of the governance model allow compliance without guaranteeing reliability in complex environments.

PPDR communications depend on high-assurance, cross-border infrastructure, yet operate within systems shaped by heterogeneous regulation, variable enforcement, commercial priorities, and accelerating technological change.

# 5. Structural and Architectural Vulnerabilities in European Telecommunications Networks

Network architecture creates systemic risks beyond individual technologies. Modern telecom networks rely on virtualised software components operating across cloud and interconnected infrastructures.

PPDR communications inherit vulnerabilities that cannot be mitigated through operator action alone. Because they underpin coordination, situational awareness, and emergency response, disruption in underlying networks directly constrains operational effectiveness.

The main vulnerabilities arise from four interrelated trends: exposure between control domains, the persistence of legacy signalling protocols, growing dependence on virtualised and cloud-native core infrastructure, and the complexity of disaggregated multi-vendor architectures. Together, these trends increase both the likelihood of disruption and the difficulty of mitigation.

## 5.1 Control, User and Management Plane Exposure

Modern mobile networks separate control, user, and management planes to isolate functions and improve resilience. In practice, however, software-defined networking and virtualisation have concentrated critical dependencies in the management plane, turning it into a structural point of exposure.

Through NFV and orchestration systems (MANO), the management plane now controls the lifecycle, configuration, and interconnection of core functions. Compromise or disruption at this layer can therefore affect multiple services at once rather than isolated components [34].

This risk is increased by weak segmentation between operational telecom environments and corporate IT domains. Management interfaces are often reachable through shared infrastructure or remote-access pathways, creating routes through which compromise in non-critical systems can reach operational network functions [8].

In virtualised environments, excessive administrative privileges can extend a single breach across orchestration systems, virtualisation layers, and configuration interfaces, turning local compromise into system-wide disruption [34].

For PPDR services on shared commercial networks, this has direct operational consequences. The management plane governs traffic prioritisation, quality of service, and routing policies essential to emergency communications. Compromise here can disable mission-critical capabilities without any physical network failure.

## 5.2 Legacy Signalling and Interconnection Risks

Telecommunications networks also remain exposed through external interconnection. Despite technological change, modern systems still rely on legacy signalling protocols such as SS7 and Diameter for interconnection and roaming, preserving structural dependencies on mechanisms not designed for today’s threat environment.

These protocols were built on assumptions of trust between a limited number of operators. In today's interconnected ecosystem, that assumption no longer holds, exposing networks to threats from a wider range of actors [19]. Access is no longer limited to national operators, but can also be gained through intermediaries, transit providers, or partner networks [35].

SS7 and related vulnerabilities can enable location tracking, interception, call redirection, and denial-of-service attacks. These are systemic weaknesses that can be exploited remotely and at scale [19]. Although newer protocols include added protections, the underlying trust model has changed little, so signalling-based attacks remain feasible in 4G and 5G networks [19].

For PPDR operations, the cross-border implications are significant. Emergency response increasingly depends on roaming, mutual assistance, and shared infrastructure, meaning mission-critical communications are exposed not only to domestic networks but to the cumulative risk of the broader signalling ecosystem.

## 5.3 Cloud-Native and 5G Core Dependencies

The shift to 5G has accelerated the use of cloud-native technologies in telecom infrastructure. Core functions once delivered on specialised hardware are now deployed as software workloads on virtualised platforms and container systems [34]. This transforms telecom networks into distributed computing environments with multiple external dependencies.

Reliability is therefore shaped not only by telecom infrastructure but by the security and performance of virtualisation layers, orchestration platforms, and cloud services. Failures at lower layers can propagate across many network functions at once [34]. Misconfiguration, software flaws, or malicious activity in shared infrastructure can affect multiple operators simultaneously, increasing both systemic risk and the difficulty of containment.

The growing role of large cloud providers extends this dependency further. Telecom workloads are increasingly hosted on infrastructure not owned or directly controlled by operators or public authorities. While this supports flexibility and redundancy, it also concentrates critical functions within a small number of providers, creating strategic dependencies beyond the telecom sector [11].

For PPDR communications, this creates a major exposure. Mission-critical services depend on shared and externally governed infrastructure optimised for commercial efficiency rather than assured availability. Disruption in cloud or virtualisation environments can therefore disable emergency communications without targeting telecom networks directly.

## 5.4 Open RAN, Software-Defined Radio and Multi-Vendor Risk

A further architectural shift is the move toward disaggregated infrastructure, especially Open RAN. Traditional mobile networks were vertically integrated, with clear lines of vendor responsibility. Open RAN separates components to increase flexibility and reduce supplier dependence, but replaces single-vendor reliance with dependence on the successful integration of multiple components.

While this may improve supply-chain diversity and innovation, it also increases network complexity and shifts more responsibility for assurance onto operators and integrators [29]. O-RAN introduces

a disaggregated, multi-vendor architecture with multiple open interfaces (e.g. A1, O1, O2, E2), each requiring dedicated security controls across distributed components [36], [30]. As a result, vulnerabilities may arise not only within individual components, but through interactions between interfaces and architecture elements, reflecting the expanded attack surface and integration complexity inherent in open and interoperable mobile network environments [29].

This complexity is amplified by software-defined radio (SDR), where radio functions are implemented in software rather than fixed hardware. SDR improves flexibility but expands the attack surface to firmware, software updates, and configuration interfaces that shape radio behaviour [17].

For PPDR communications, which depend on reliable radio performance, this introduces additional exposure. Misconfiguration or compromise of radio control functions can affect coverage, availability, and emergency traffic prioritisation, potentially through remote and dynamically propagated changes. Disaggregated architectures improve adaptability but complicate accountability, incident response, and oversight.

## 5.5 Organisational Fragmentation and Collective Cybersecurity Gaps

These architectural shifts are mirrored by growing organisational fragmentation. Modern telecom networks function as ecosystems involving operators, infrastructure providers, vendors, cloud services, software developers, and roaming partners, each controlling different system components.

This model supports innovation but fragments cybersecurity responsibility. Security is typically governed through contracts and service agreements, producing a system of bilateral accountability rather than end-to-end control. No single actor has full visibility over the security of the whole infrastructure [11].

Organisational fragmentation is reinforced by legal and operational barriers. Despite EU-level coordination mechanisms, real-time cross-border data sharing during incidents is constrained by divergent national legal frameworks, liability concerns, and inconsistent interpretations of data protection obligations [73]. These constraints limit the timely exchange of operational intelligence between Member States. More broadly, this reflects a structural coordination problem: differing incentives and priorities between commercial operators and public authorities create “clashing mindsets” that inhibit effective collaboration [35]. In PPDR contexts, where response depends on rapid, cross-border coordination, these frictions materially reduce the effectiveness of otherwise well-defined governance frameworks.

As a result, vulnerabilities can persist between organisational boundaries without clear ownership. Information sharing may also be limited by commercial sensitivities, liability concerns, or regulation, reducing shared situational awareness and allowing threats identified in one organisation to remain unaddressed elsewhere [11].

This fragmentation complicates incident response. In interconnected multi-actor systems, identifying the source of an incident, assigning responsibility, and coordinating remediation becomes much harder, increasing the operational impact of disruptions.

For PPDR communications, this creates a governance gap: emergency services depend on infrastructure that is collectively operated but not collectively governed. Resilience therefore depends on alignment across independent actors with different incentives, priorities, and capabilities. Compliance alone does not ensure resilience in such fragmented environments.

## 5.6 Structural Vulnerabilities and Systemic Risks in Future PPDR Communications Infrastructure

The evolving architecture of telecommunications networks creates systemic risk conditions. Resilience depends on the integrity of complex technical and organisational systems rather than on individual components alone.

Because PPDR communications rely on commercial telecom networks, they inherit structural dependencies on infrastructure not fully designed, controlled, or governed for mission-critical use. Their reliability is shaped by layers of architecture, operational practice, and cross-sector coordination that often lie beyond direct public authority control.

These dependencies also extend into the hardware and software supply chains underpinning telecom infrastructure. As those supply chains become more distributed and globally interconnected, they add further exposure that can affect communications security and resilience at scale.

# 6. Supply Chain and Software Integrity Risk

Emergency response capabilities depend on software supply chains, cloud-native network functions, and globally sourced hardware components. This places critical functions within a multi-layered supply environment.

Failures or compromises within this ecosystem may not manifest as immediate outages. Instead, they can degrade trust, introduce latent vulnerabilities, or enable adversarial access at critical moments [20]. These effects can be difficult to detect, attribute, and contain.

Within the European context, these risks are amplified by Single Market interdependencies, cross-border service provision, and exposure to globalised telecommunications supply ecosystems [3], [11].

While European frameworks introduce important safeguards, they do not resolve these structural conditions. Their effectiveness is constrained by fragmented implementation, limited technical specificity, and an implicit reliance on market actors to manage systemic risk. A gap exists between regulatory compliance and operational resilience [23], [25].

As a result, systemic risks persist at the intersection of vendor dependency, software assurance, and hardware trust. These risks are not isolated or vendor-specific. Increasingly, they are inherent to how modern telecommunications systems are composed, integrated, and continuously modified across distributed and globally sourced supply chains.

## 6.1 Vendor Dependency and High-Risk Vendor Controls

A primary structural vulnerability in European telecommunications infrastructure is the concentration of critical capabilities within a limited number of suppliers, many of which are headquartered outside the European Union, creating a dependency structure in which core network functions rely on a small set of external actors.

From an operational perspective, high levels of vendor dependency constrain resilience by limiting redundancy and reducing the ability to substitute components or services under crisis conditions. In a disruption scenario (whether caused by technical failure, geopolitical tension, or supply chain interruption) PPDR capabilities are exposed to disruption through dependencies embedded deep within commercial network infrastructure [11]. This exposes critical functions to failures that originate beyond the visibility and control of public authorities [8], [6].

From a strategic perspective, vendor concentration raises concerns related to third-country influence, supply continuity, and the potential for systemic vulnerabilities to be introduced across widely deployed technologies [9], [25]. This leads to a risk environment in which a single point of compromise could have cross-network and cross-border consequences.

European policy responses, including the 5G Toolbox, seek to mitigate these risks through vendor risk assessments and the promotion of multi-vendor strategies [9]. However, implementation across Member States remains uneven. This limits the effectiveness of risk mitigation measures at Union level and creates inconsistencies in protection across interconnected infrastructures.

The NIS2 Directive recognises that earlier frameworks allowed significant national discretion, resulting in divergent approaches to high-risk vendor restrictions [23]. This results in an uneven security baseline across the Union, allowing vulnerabilities in one national network to propagate through interconnected systems.

Moreover, current regulatory instruments often lack the enforceability required to drive structural change in vendor diversification. While the EU 5G Toolbox introduced measures to assess and restrict high-risk suppliers, subsequent implementation reviews highlight uneven adoption across Member States and a clear risk of persisting dependency on such suppliers within critical infrastructure [6], [25], [64].

PPDR communications rely on commercial network resilience shaped by these conditions.

## 6.2 Software Assurance, CI/CD Pipelines and Orchestration Security

The increasing reliance on software-defined networking, virtualisation, and cloud-native architectures introduces a new class of risks associated with software integrity and deployment processes. In modern PPDR-relevant networks, core functions are instantiated, updated, and managed through automated Continuous Integration and Continuous Deployment (CI/CD) pipelines, as well as orchestration platforms that control distributed network behaviour [8].

While these approaches enhance flexibility and scalability, they also expand the attack surface, resulting in possible compromise of the software supply chain, via malicious code insertion, dependency poisoning, or credential theft, can introduce vulnerabilities into trusted systems at scale [20].

Recent incidents demonstrate the feasibility of such attacks, including the compromise of widely used software components through long-term infiltration of development ecosystems [20]. Once integrated into deployment pipelines, these compromises may propagate across multiple networks before detection. This increases the potential for simultaneous, cross-operator exposure originating from a single point within the software supply chain.

In parallel, adversaries increasingly employ “living-off-the-land” techniques, leveraging legitimate administrative tools and system functions to conduct operations. This reduces the likelihood of detection, particularly in environments where monitoring lacks sufficient granularity or where baseline behaviours are not well defined [20]. This increases ambiguity around malicious activity, making it indistinguishable from normal system operations.

A further challenge lies in the gap between high-level regulatory guidance and the technical complexity of modern network environments. Industry assessments indicate that existing national guidelines are often insufficiently detailed to support consistent implementation of secure development, integration, and deployment practices [8], [6]. This increases fragmentation in how software assurance is achieved across operators and Member States.

For PPDR communications, the implications are systemic. Software integrity failures may not result in immediate service disruption but can undermine the reliability, predictability, and trustworthiness

of critical network functions. This is particularly critical in high-stress operational scenarios, where rapid updates, scaling, or reconfiguration are required. Software assurance processes are not fully visible, standardised, or controllable by public authorities.

These dynamics are further reinforced by the increasing reliance on external cloud and platform providers to host, manage, and orchestrate network functions. This adds a layer of dependency in which critical control functions are executed within infrastructures that are not owned or directly governed by telecommunications operators or public authorities. [8] This limits visibility into system behaviour, constrains independent verification, and introduces concentration risks associated with a small number of global providers.

## 6.3 Hardware Trust, Firmware Integrity and Embedded Risk

Beneath the software layer, hardware components and firmware represent a foundational but less visible dimension of supply chain risk. Telecommunications infrastructure depends on complex, globalised manufacturing ecosystems, with components sourced, assembled, and integrated across multiple jurisdictions [11]. This adds dependency structure in which the integrity of critical infrastructure is shaped by production processes and supply chains that extend beyond European oversight.

This complexity makes it difficult to establish end-to-end trust in hardware integrity. This exposes infrastructure to the risk that malicious modifications introduced during manufacturing or distribution can persist undetected, particularly at the firmware level where traditional security controls have limited visibility [20].

Firmware-level compromises are of particular concern because they operate below the operating system and can therefore bypass many conventional security mechanisms. As a result, persistent access, data exfiltration, or targeted disruption can be maintained over extended periods, including the ability to degrade or disable network functions at critical moments. Real-world cases demonstrate this capability, including network infrastructure malware such as VPNFilter and Cyclops Blink, as well as firmware-level implants such as MoonBounce [20], [76]-[78].

In parallel, emerging research highlights risks associated with the physical layer of communications systems. Hardware characteristics, such as radio frequency emissions, can be used to uniquely identify devices, but also introduce complexity in maintaining device integrity across firmware changes and hardware variation [17]. This complicates efforts to ensure consistent device authentication and trust in heterogeneous, multi-vendor environments.

For PPDR systems operating in such environments, these factors create a structural limitation in current assurance models. The difficulty of verifying hardware provenance, firmware integrity, and lifecycle integrity at scale limits the ability of operators and public authorities to establish trusted baselines. This exposes critical communications capabilities to embedded risks that may not be fully detectable, mitigated, or remediated through conventional security measures.

## 6.4 Procurement Governance and Whole-of-Lifecycle Assurance

Given the complexity and persistence of supply chain risks, procurement plays a significant role in shaping the structure and composition of telecommunications infrastructure. However, traditional procurement approaches, often focused on upfront cost, compliance, and minimum technical standards, do not fully reflect the lifecycle characteristics of modern telecommunications risk. This causes misalignment between procurement decisions and long-term operational resilience.

European frameworks such as NIS2 and the Cyber Resilience Act introduce requirements related to secure-by-design principles, vulnerability handling, and ongoing risk management responsibilities [23], [26]. When implemented, these measures contribute to improvements in baseline security and influence how vendors and operators address lifecycle risks.

However, a key constraint lies in the fragmentation of responsibility across stakeholders. Operators, vendors, and public authorities often assess risk within organisational boundaries, with limited visibility of upstream and downstream dependencies [6] [25]. This creates systemic blind spots in how interdependencies are identified, assessed, and managed.

Existing sectoral initiatives provide a foundation for addressing these challenges, but remain uneven in adoption and limited in operational integration [8]. This constrains their effectiveness in managing systemic and cross-border risks.

In parallel, current approaches continue to rely heavily on vendor self-assessment and compliance-based assurance models. This limits the ability to independently verify the security and integrity of complex, multi-layered systems.

## 6.5 Systemic Risk and Structural Limitations

Recent incidents affecting both EU institutions and first responder organisations point to a consistent pattern of operational rather than purely technical insecurity. The European Commission breach demonstrates how critical public-facing services, hosted on third-party cloud infrastructure can be compromised without affecting “core” systems, yet still result in significant data exposure and cross-organisational risk, with limited transparency on root cause or impact [80].

In parallel, the phishing-driven breach disclosed by the Dutch National Police highlights how frontline organisations remain vulnerable to basic credential compromise, triggering national-level incident response even when immediate data loss appears contained [81], and reflects a recurring pattern following earlier large-scale breaches of Dutch police personnel data in 2024.

Taken together, these cases suggest that operational security weaknesses emerge at the interfaces between systems, people, and supply chains (*where control, visibility, and responsibility are inherently distributed*) rather than within clearly bounded or individually “secure” systems. This reinforces the view that current European approaches emphasise architectural resilience and regulatory compliance, but insufficiently address the dynamic, cross-boundary conditions under which real-world incidents unfold.

These weaknesses can propagate beyond individual networks and jurisdictions, introducing the potential for large-scale disruption or degradation of critical services such as emergency

communications, even where the originating cause lies outside the immediate operational domain of affected systems.

Such dynamics reflect a broader structural challenge within the telecommunications ecosystem, characterised by fragmented responsibilities, compliance-oriented controls, and partial visibility across increasingly interdependent infrastructures.

As networks become more open, software-driven, and interdependent, evolving toward AI-driven, highly distributed architectures, system complexity and the potential for cascading failure increase, necessitating continuous, end-to-end assurance across a multi-vendor ecosystem, rather than reliance on fragmented, compliance-based controls [29], [8].

Recent large-scale cyber campaigns and infrastructure disruptions further reinforce these dynamics. Incidents affecting multiple jurisdictions simultaneously, including advanced persistent threat activity targeting telecommunications and government systems, demonstrate that highly regulated and security-conscious environments remain exposed to coordinated and systemic risks [20]. While not all such events originate within telecommunications networks, they highlight how interdependency, shared technologies, and governance complexity can enable disruption or compromise to propagate across sectors and borders [20], [11]. For PPDR communications, this is particularly significant, as operational effectiveness depends not only on telecommunications infrastructure itself, but also on the continued availability and integrity of supporting systems including power, financial services, information systems, logistics, and fuel supply chains, all of which underpin the continuity of emergency response operations.

# 7. Sovereignty, Strategic Autonomy and Industrial Resilience

Geopolitical tensions and lessons from COVID-19 have accelerated the EU's focus on "digital sovereignty" and "open strategic autonomy," now framed as essential to security, resilience, and independent crisis response [37].

EU policy links the robustness of telecommunications infrastructure and the European defence technological and industrial base (EDTIB) to operational autonomy [38]. For PPDR communications, this makes jurisdiction, control, and industrial capacity central to telecom policy. Governance is therefore inseparable from sovereignty and strategic resilience.

## 7.1 Sovereignty, Extraterritorial Risk and Cloud Jurisdiction

EU policy increasingly treats legal jurisdiction as a core element of infrastructure security. The CJEU's *Schrems II* ruling found that U.S. surveillance laws (including FISA Section 702 and EO 12333) do not provide protections equivalent to EU law, due to limited safeguards and lack of redress [39]. This highlights a structural issue: EU compliance cannot be guaranteed where data is subject to external jurisdictions.

The extraterritorial reach of laws such as the U.S. CLOUD Act reinforces this risk, allowing authorities to access data regardless of storage location [40], [37]. International analysis identifies government access to data as a structural feature of digital interdependence, affecting sovereignty and trust [41]. The EDPB similarly emphasises that such risks may require additional safeguards or suspension of transfers [42]. Legal exposure is therefore embedded in global cloud architectures.

In response, EU policy promotes data sovereignty through European data spaces and federated cloud infrastructures (e.g. Gaia-X), aiming to reduce reliance on non-EU providers and ensure compliance with EU standards [40], [43], [37].

For PPDR systems, this creates operational constraints. Where adequate safeguards cannot be ensured, data transfers must be restricted or suspended [39], [42], limiting reliance on infrastructure that is not legally compatible with EU requirements.

## 7.2 Sovereign Infrastructure as a PPDR Trust Requirement

Jurisdictional risk extends beyond data to infrastructure control. EU policy increasingly recognises that communications supporting government and security functions require infrastructure under European jurisdiction. Initiatives such as IRIS² aim to provide secure connectivity designed to meet EU security requirements [44].

A distinction is emerging between infrastructure merely located in Europe and infrastructure controlled within it. "Governmental infrastructure," defined by strict ownership and governance controls, reflects recognition that some functions cannot rely on external dependencies without unacceptable risk. Debates around IRIS² participation highlight concerns over non-EU ownership and influence [44].

This aligns with EU and NATO views of digital networks as critical infrastructure and targets for cyber and hybrid threats [45]. Resilience includes not only technical robustness but the ability to absorb and recover from disruption. For PPDR systems, failures in any component (technical, physical, or legal) can cascade across operations, meaning trust must be assessed at system level.

As public authorities increasingly depend on privately operated infrastructure, EU policy emphasises "secure by design" systems and stronger oversight [46]. This supports a layered sovereignty model: core functions anchored in trusted infrastructure, with less critical services relying on commercial providers under defined conditions.

In practice, the level of criticality is not an intrinsic property of the system itself, but of its operational context within PPDR scenarios. A single system may transition between routine and high-criticality use depending on circumstances; therefore, "secure by design" must be complemented by security context-aware operational controls that are embedded in operational procedure.

## 7.3 EU Telecom Industrial Strategy and Supply Chain Resilience

Telecom sovereignty is closely tied to the European industrial base. EU policy identifies dependencies in semiconductors, cloud, and network equipment as strategic vulnerabilities that limit autonomy in crises [47].

The semiconductor sector illustrates this challenge: despite strong research capabilities, Europe remains reliant on external suppliers for advanced chips [48]. Similar dependencies exist across the digital ecosystem, often concentrated in a small number of third countries [49], [43].

The EU has responded with industrial initiatives such as the Chips Act, which aims to expand production, attract investment, and improve supply chain monitoring [48]. Broader strategies seek to identify and reduce dependencies, while sector-specific programmes like IRIS² and the European Defence Industrial Strategy support capacity building in critical areas [38], [44].

However, a gap remains between regulatory ambition and industrial capability. Despite strong frameworks for cybersecurity and data protection, Europe faces challenges in scaling competitive infrastructure, particularly in cloud services dominated by non-EU providers [43]. This limits public-sector control over how critical infrastructure is designed and operated.

For PPDR communications, this creates tension between the need for sovereign, secure systems and the realities of market availability and technological dependence.

## 7.4 Security as Strategic Competitive Advantage

EU policy increasingly frames security and trust as sources of competitive advantage. The EU Cybersecurity Strategy positions secure infrastructure as essential for both resilience and economic growth [46]. Through regulatory frameworks and certification schemes, the EU acts as a global standard-setter, shaping market behaviour and influencing international firms [37].

This extends to promoting "European values" such as transparency and accountability in areas like AI and cybersecurity, positioning trustworthiness as a differentiator in global markets [37]. Industrial initiatives also link "trusted" technologies to long-term competitiveness [48].

Efforts to reduce reliance on non-allied vendors are framed in terms of both security and economic resilience, emphasising “security of supply” [38], [46]. However, implementation remains uneven. Procurement decisions are still driven by cost, availability, and existing market structures, creating a gap between strategic objectives and operational outcomes [38], [43].

For PPDR communications, this gap is critical. Where procurement prioritises efficiency over control and resilience, dependencies persist despite recognised risks.

# 8. Incident Response and Cross-Border Crisis Coordination

PPDR operations depend on timely detection, escalation, and resolution of incidents, which communications systems must support under crisis conditions. Disruptions quickly become system-level events affecting coordination and public safety.

Because infrastructure control is distributed, public authorities have limited ability to prioritise communications or enforce response actions. Incident response depends on telecom operators, cloud providers, and vendors—often outside state authority and jurisdiction.

In the EU, these constraints are amplified by cross-border integration. Networks, cloud platforms, and interconnection systems operate as a transnational system, allowing incidents to propagate faster than coordination mechanisms can respond, while responsibility remains fragmented. EU frameworks support coordination, but operate over infrastructure that is not uniformly controlled or prioritised for PPDR use.

## 8.1 Detection, Escalation and Speed Asymmetry

NIS2 establishes reporting timelines (24-hour early warning, 72-hour notification) [23], but these operate within an environment where threats move at machine speed. Automated and AI-enabled attacks can disrupt systems in real time, while response processes rely on human validation and coordination, creating a structural speed asymmetry [8], [20].

Although EU rules require continuous monitoring and detection [50], escalation remains uneven. Thresholds for incident classification and escalation vary across Member States, reflecting different institutional practices and risk tolerances. This delays collective response and introduces divergence in crisis handling [52], [31].

Fragmentation in reporting and taxonomy further complicates cross-border incidents, where shared infrastructure must be interpreted across jurisdictions with differing procedures [12]. Europe regulates cyber risk, but it does not systematically define cyber harm. Existing taxonomies remain academic and organisation-focused, and are not operationalised for first responder environments, where harm is dynamic, cascading, and context-dependent [79]. This lack of a shared understanding of harm further compounds challenges in detection and interpretation.

Detection is also constrained by reliance on proprietary systems, limiting independent verification and increasing dependence on vendor visibility [53]. Situational awareness is therefore incomplete. Information sharing between operators and authorities is often restricted by commercial and legal concerns, leaving crisis coordinators without full visibility of infrastructure conditions [51], [55].

Overall, incident response is constrained by a mismatch between machine-speed threats and human-mediated, fragmented governance processes, reducing situational awareness and operational effectiveness.

## 8.2 Restoration Sequencing for PPDR Services

Restoration of PPDR services depends on interconnected infrastructures, particularly telecommunications, energy, and digital systems. These dependencies create circular constraints:

telecoms require power, while energy systems depend on communications, delaying recovery and increasing cascading risk [9], [8].

Although PPDR entities are designated as critical [24], restoration priorities are typically determined by operators through business continuity processes, rather than by public authorities. This creates a gap between policy recognition and operational control [50].

In cross-border contexts, differing national priorities further complicate restoration. PPDR services may not be prioritised consistently, especially where infrastructure lies outside the affected jurisdiction [12].

Additional constraints include uneven backup power requirements and limited oversight of critical assets such as submarine cables, creating vulnerabilities and jurisdictional ambiguity in restoration responsibility [55], [11], [13].

Recovery timelines also vary: disruptions may immediately affect operations, while restoration—particularly in cloud-based systems—can be prolonged. This creates a mismatch between the urgency of PPDR needs and infrastructure recovery processes.

## 8.3 Degraded-Mode and Fallback Communications

PPDR communications are shifting from dedicated systems to broadband services over commercial networks, increasing reliance on shared infrastructure and external dependencies [12]. Fallback mechanisms are therefore core, not supplementary, to operations.

Satellite-based systems (e.g. LEO constellations) can provide continuity but introduce scalability limits and new risks, including jamming and signal analysis [53]. Terrestrial fallback (e.g. national roaming) typically supports only basic services, not data-intensive applications required for modern PPDR operations [55].

Virtualised and cloud-based networks further concentrate risk. Failures in shared platforms can affect large segments simultaneously, reducing the effectiveness of traditional fallback models based on isolation [8], [25].

Deployable infrastructure offers additional resilience but is constrained by logistics, spectrum coordination, and lack of harmonised frameworks for cross-border deployment [55].

Fallback systems are also affected by underlying vulnerabilities in signalling and routing protocols, meaning they may remain operational but not secure [19], [11].

Overall, degraded-mode operation represents a redistribution of dependencies rather than an independent resilience layer. No fully sovereign fallback capability exists for PPDR communications.

## 8.4 EU-Level Coordination (ENISA, CERT-EU, CyCLONe)

EU coordination is structured through mechanisms such as EU-CyCLONe, the CSIRTs Network, and CERT-EU, linking technical response with operational and strategic coordination [23], [31]. These frameworks support information exchange and shared situational awareness across Member States.

However, they operate through coordination rather than control. Infrastructure remains under the authority of diverse national and commercial actors, limiting the ability to enforce prioritisation, resource allocation, or restoration decisions.

Alignment between EU and national frameworks remains uneven, with differences in preparedness and incident handling reducing the effectiveness of collective response [52], [31]. Cross-border dependencies, including submarine cables, further constrain coordination due to unclear authority and limited repair capacity [13], [11].

While ENISA mechanisms improve situational awareness, variability in reporting and data quality leads to incomplete or delayed information at Union level [10], [54]. Increasing EU-NATO alignment strengthens coordination across domains but does not resolve fragmented infrastructure control [45].

Overall, EU coordination provides structure but not operational leverage. Its effectiveness is bounded by the infrastructure it does not control, resulting in delays and inconsistencies in cross-border crisis response.

## 8.5 Implications for multi-agency response capability

Incident response frameworks in the EU are well developed in terms of coordination and reporting, but operate within an infrastructure environment characterised by fragmented ownership, distributed control, and cross-border dependency.

PPDR communications rely on commercial networks and global supply chains, yet restoration priorities, fallback capabilities, and coordination mechanisms do not fully reflect these dependencies. This limits the ability to prioritise emergency communications and maintain full situational awareness.

EU coordination mechanisms provide a basis for collective response, but depend on alignment across national systems and timely information sharing. As threats become faster and more complex, gaps between infrastructure dependency and control become more pronounced.

This leads to a key conclusion: the effectiveness of PPDR incident response is determined not only by coordination frameworks, but by the degree of control over the underlying infrastructure. Without such control, resilience remains conditional, and reliable crisis communications cannot be fully ensured.

# 9: Building a Secure and Resilient PPDR Telecom Architecture

PPDR communications are structurally constrained by dependence on complex, interconnected infrastructures not fully controlled by public authorities. These constraints appear in incident response, where limited visibility, prioritisation, and coordination reduce reliability during crises. This creates a need to embed security, resilience, and operational control directly into infrastructure.

Security and resilience must therefore be understood as functions of control over infrastructure, identity, and visibility, rather than properties of individual technologies. Modern PPDR services depend on layered systems (radio, transport, core, cloud, interconnection) operated by multiple actors. Disruptions at any layer can propagate across the system, affecting mission-critical services.

Resilience cannot be achieved through isolated measures alone. It requires integrated architectural principles, technical controls, and continuous monitoring across all layers, including supply chains and externally governed infrastructure. At the same time, virtualised and cloud-based systems introduce both flexibility and new risks, concentrating critical functions in shared environments.

A resilient architecture must therefore ensure segmentation, isolation, and assured fallback while maintaining operational continuity across distributed systems. The objective is to embed resilience by design, rather than relying on coordination across fragmented infrastructures.

## 9.1 Zero-Trust and Identity Segmentation in Core Networks

The shift to broadband and software-defined architectures requires adoption of zero-trust principles, replacing perimeter-based security with continuous verification across network layers [23]. In 5G environments, core functions form a critical control plane, where compromise can have system-wide impact [57].

Mitigation requires identity-centric controls, including least privilege, strong authentication, and continuous validation of interactions between network functions and systems [57]. However, softwarisation (NFV, containerisation, cloud orchestration) weakens traditional boundaries, increasing dependence on correct configuration and isolation enforcement [34].

For highly critical PPDR functions, logical segmentation alone may be insufficient, requiring physical separation or dedicated infrastructure [57]. Implementation is further constrained by skills shortages, limiting the effectiveness of zero-trust models in practice [54].

Zero-trust is therefore necessary but not sufficient; its effectiveness depends on enforceability across complex, multi-actor environments.

## 9.2 Encryption, Key Management and Secure Signalling

Cryptography underpins PPDR communications, but security depends on effective key management rather than encryption alone [23], [58]. This includes protection of subscriber credentials, identifiers, and authentication keys across distributed systems [57].

Cloud-native architectures extend trust boundaries into shared environments, increasing reliance on third-party infrastructure for key protection. This reduces direct control over critical security functions.

Long-term risks such as quantum computing further challenge current cryptographic models, requiring transition planning toward post-quantum approaches [59].

At the same time, legacy signalling systems (SS7, Diameter) remain a structural vulnerability, enabling interception, tracking, and manipulation across networks [19], [20]. These weaknesses persist even where endpoint encryption is strong.

Overall, secure communications depend on control over key management and interconnection integrity, both of which are constrained by external dependencies and jurisdictional limits.

## 9.3 Emissions Security and Transmission Discipline

RF emissions create a parallel layer of exposure where transmission characteristics, not content, reveal operational information. Secure data does not ensure secure operations.

Integration of terrestrial and satellite systems (including LEO constellations) expands exposure, enabling global observation and interference [53]. Adversaries can derive intelligence from signal patterns, metadata, and traffic behaviour without decrypting content.

Distributed architectures (e.g. MEC, dense base stations) increase physical and operational exposure, while metadata remains accessible even where payloads are encrypted [23], [57].

Effective protection therefore requires integrating emissions control, transmission discipline, and physical security alongside cybersecurity. Without this, communications remain observable and disruptable.

## 9.4 Network Slicing Integrity and MCX Service Protection

Network slicing enables mission-critical services (MCX) over shared infrastructure by allocating logically isolated resources [57]. However, this isolation depends on software-defined controls and correct enforcement.

Misconfiguration or compromise of orchestration systems can undermine isolation, exposing PPDR services to interference from commercial environments. ENISA identifies risks where attackers gain control of dedicated slices [57].

Resilience is further constrained during large-scale disruptions, where service continuity depends on operator-led recovery processes. Resource contention and congestion can degrade prioritisation, particularly under stress [51], [57].

Thus, slicing enables PPDR services but does not guarantee isolation or resilience. Effective protection depends on control over orchestration, enforcement of boundaries, and consistent prioritisation across the network.

## 9.5 Secure Roaming and Cross-Border Identity Trust

Cross-border PPDR operations rely on trusted identity and authentication mechanisms across Member States [23]. However, these are distributed across interconnected systems, making trust dependent on the weakest link.

Legacy roaming mechanisms and inconsistent implementation of security controls introduce vulnerabilities, particularly in transitional 5G environments [57]. Differences in national standards and certification create uneven assurance across the Single Market [23].

National measures (e.g. data localisation, access restrictions) may improve security domestically but hinder interoperability and rapid coordination [59]. Trust service providers also represent concentrated dependencies, where disruption can have cross-sector impact [54].

Overall, identity trust is shaped by governance alignment rather than technology alone. Where consistency is lacking, cross-border operations are constrained.

## 9.6 Threat Intelligence Integration, Monitoring and Active Defence

Effective protection requires continuous monitoring and integration of threat intelligence. However, visibility is largely controlled by operators through NOCs and SOCs, creating dependence on externally managed data [57].

Detection of anomalies depends on access to operator-held information, which may be limited or delayed, reducing responsiveness. Variability in reporting and intelligence sharing further constrains situational awareness, particularly in cross-border incidents [20], [60].

Information-sharing mechanisms (e.g. ISACs) improve coordination but rely on voluntary participation, resulting in uneven coverage [23]. Meanwhile, advanced and state-linked threats exploit fragmented defensive arrangements and trusted infrastructure, creating asymmetry between attackers and defenders [60].

This requires a shift toward proactive, intelligence-driven defence, including continuous monitoring and behavioural analysis. However, effectiveness depends on access to timely, comprehensive visibility across infrastructures not fully controlled by public authorities.

# 10. Investment, Capability and 6G Strategic Positioning

PPDR communications are now integral to Europe's wider digital infrastructure, underpinning crisis governance and public authority. As systems evolve from narrowband to broadband and data-intensive platforms, they are increasingly embedded in commercial networks, cloud systems, and cross-border ecosystems. This introduces dependencies beyond national control, requiring reassessment of capability, investment, and governance at both Member State and EU level [56] [62].

The transition to 5G and emerging 6G architectures intensifies this shift, integrating AI, edge computing, and software-defined networking. As a result, PPDR resilience is inseparable from the broader digital infrastructure stack. Workforce capability, investment, architecture, and industrial strategy become interdependent, where weaknesses in one domain affect overall system resilience.

## 10.1 Workforce, Skills and Specialist Capability Development

A persistent shortage of cybersecurity professionals constrains European sovereignty and PPDR resilience, particularly as communications systems become software-defined and interdependent [61]. Emerging 6G ecosystems span telecoms, AI, cloud, and microelectronics, requiring multidisciplinary expertise across domains [62].

This shift introduces operational risks where gaps in expertise affect system integrity and availability. Addressing this requires integrated STEM pathways combining telecom engineering, cybersecurity, and AI/ML, alongside efforts to expand the talent pool and address gender imbalances [62].

NIS2 reflects these governance challenges, requiring Member States to strengthen capacity through cooperation and personnel exchange between authorities and CSIRTs [23]. Cross-border crisis response depends on shared expertise and institutional alignment.

A lack of specialist capability creates systemic risk, as advanced security measures (e.g. post-quantum cryptography, AI-driven management) depend on skilled personnel. Where expertise is insufficient, vulnerabilities propagate across communications systems, directly affecting PPDR reliability [51].

## 10.2 Strategic Investment Needs and EU Funding Mechanisms

Resilient PPDR communications require sustained investment in terrestrial, satellite, and submarine infrastructure [63]. For emergency services, this means ensuring redundancy, secure transport, and continuity across interconnected systems.

The Smart Networks and Services Joint Undertaking (SNS JU) aligns public and private investment, with EUR 900 million allocated for 2021–2027 [64]. Complementary programmes such as Digital Europe and STEP support resilience measures and strategic technologies [65], [66].

Infrastructure design is critical, particularly for submarine cables, which carry most international traffic and represent key dependencies [63]. EU initiatives aim to coordinate investment and reduce risk exposure, including through Cable Projects of European Interest [63].

Cross-border continuity is supported by programmes such as CEF Digital, which funds 5G corridors for seamless operations [63]. At governance level, the CER Directive enables financial support for critical infrastructure, reinforcing that resilience is a public policy objective rather than purely market-driven [24].

## 10.3 6G Architecture, PPDR Requirements and Standards Leadership

6G introduces a new architecture based on AI integration, sensing, and convergence of terrestrial and non-terrestrial networks [62], [67]. These capabilities align with PPDR requirements for real-time situational awareness, precise positioning, and ultra-low latency coordination.

However, increased reliance on software-driven and distributed systems expands the attack surface, linking architectural design directly to systemic risk [68]. This makes security-by-design essential at the level of standards, interfaces, and orchestration.

European participation in standardisation (e.g. 3GPP) is therefore strategically important, ensuring that security, privacy, and lawful access requirements are embedded in future networks [61], [67].

Initiatives such as the EU Critical Communication System (EUCCS) illustrate the move toward a pan-European public safety communications layer [63]. Innovations such as autonomous “In-X subnetworks” and quantum-resilient encryption highlight the need for resilience at both edge and core [62].

Overall, 6G design choices will directly shape the security, resilience, and sovereignty of future PPDR communications.

## 10.4 Open RAN, Vendor Diversification and Industrial Opportunity

Open RAN enables modular, multi-vendor architectures, supporting diversification and reducing supplier dependency [11]. This aligns with EU security policy but increases complexity and introduces new integration risks, where vulnerabilities may arise from the weakest link in multi-vendor systems [11].

The role of system integrators and cloud providers further expands the governance challenge, requiring assessment of a broader set of actors [11]. EU policy recognises high-risk vendors and supports restrictions in critical segments [12], linking procurement to security objectives.

At the same time, Open RAN creates opportunities for European industry, particularly SMEs, to participate in specialised segments of the value chain [11]. However, maintaining resilience requires preserving European control over key technologies, intellectual property, and production capacity [5].

While open architectures enable interoperability and diversification, they must be supported by strong security assurance frameworks to manage increased complexity [2]. Open RAN therefore represents both an opportunity and a governance challenge requiring system-level oversight.

# Closing Remarks

The resilience of PPDR communications depends on aligning workforce capability, sustained investment, secure-by-design architecture, and a governable industrial ecosystem. As systems become more distributed and interconnected, risks from dependency and complexity increase.

Three priorities emerge.

First, regulatory coherence must be strengthened through consistent implementation of security measures across Member States.

Second, Europe must develop sovereign capability to design and operate critical infrastructure within a trusted framework, reducing strategic dependencies.

Third, architectural standards must evolve to reflect modern threats, embedding zero-trust principles, supply chain assurance, and resilience into system design.

Ultimately, communications systems underpin crisis response. If they fail, coordination and operational effectiveness are directly compromised.

# 11 Conclusion

This study has demonstrated that Public Protection and Disaster Relief (PPDR) communications must be understood as a core component of Europe's security and resilience architecture. They underpin the ability of public authorities to coordinate, maintain situational awareness, and exercise command during crises, and therefore directly determine the effectiveness of emergency response and the continuity of public authority under conditions of disruption.

The operational and technological context in which these systems function has undergone a fundamental transformation. PPDR communications are no longer delivered through dedicated, self-contained networks, but are embedded within a complex, interdependent ecosystem of commercial telecommunications networks, cloud infrastructure, software-defined systems, and globally distributed supply chains. While this evolution has significantly enhanced operational capability, it has also introduced systemic dependencies that extend beyond the direct control of public authorities.

As a result, the resilience of PPDR communications is no longer determined solely by the design or performance of individual systems. It is shaped by the security, governance, and reliability of interconnected infrastructure layers across sectors and jurisdictions. Vulnerabilities are systemic rather than localised, and disruptions originating in adjacent systems (including telecommunications, energy, cloud, or supply chains) can directly impair mission-critical communications even where those systems are not the primary target.

The analysis further demonstrates that existing governance and regulatory frameworks have not fully adapted to these conditions. While European initiatives have strengthened the baseline for cybersecurity and infrastructure resilience, they remain primarily oriented toward commercial telecommunications and general risk management. They do not consistently ensure the level of control, prioritisation, and operational assurance required for communications systems that must function reliably under crisis conditions.

This creates a structural misalignment between the critical role of PPDR communications and the conditions under which they are governed, procured, and operated. Emergency response depends on communications systems that must remain reliable under precisely those conditions where dependencies are most exposed, coordination is most complex, and adversarial pressure is most acute. In this context, resilience cannot be equated with compliance; it must be understood as the ability to sustain operational capability under stress.

The central conclusion of this study is therefore that PPDR communications must be governed as strategic infrastructure. Their resilience depends on the extent to which public authorities can exercise effective control, visibility, and prioritisation across the infrastructure ecosystem on which they rely. Where such control is fragmented or externally constrained, resilience remains conditional. Where it is aligned with operational requirements, resilience can be designed, assured, and sustained.

Against this background, the following policy outcomes emerge as necessary conditions for ensuring secure and resilient PPDR communications across the Union:

- **Recognition of PPDR communications as strategic infrastructure within EU and national policy frameworks**
- **Strengthened regulatory coherence and consistent implementation of resilience measures across Member States**
- **Integration of mission-critical requirements into governance, procurement, and lifecycle management**
- **Use of procurement as a strategic mechanism to shape infrastructure design, control, and assurance**
- **Prioritisation of control over critical infrastructure functions rather than reliance on market availability alone**
- **Reduction of strategic dependencies in high-risk segments of the communications and digital infrastructure stack**
- **Development of sovereign and trusted capability for mission-critical communications functions**
- **Alignment of network architecture, technical standards, and resilience requirements for PPDR use cases**
- **Integration of resilience-by-design principles into 5G, 6G, and future network development**
- **Strengthened European influence in international standards-setting processes**
- **Sustained investment in specialist workforce capability across telecommunications, cybersecurity, and software-defined systems**
- **Development of a resilient and competitive European industrial base across critical technology domains**

Taken together, these measures reflect a shift from viewing communications resilience as a function of individual systems to understanding it as a property of the wider infrastructure ecosystem. In an environment characterised by interdependence, automation, and cross-border exposure, the effectiveness of crisis response is determined not only by the availability of communications, but by the degree of control over the systems that enable them, and the quality of the integration between critical systems.

PPDR communications therefore represent a strategic linchpin within Europe's security and resilience framework. Their integrity is not simply a technical or regulatory concern, but a determinant of the Union's ability to act, to coordinate, and to maintain public authority in the face of complex and contested crises.

# Bibliography

[1] J. van de Belt, H. Ahmadi, L. E. Doyle, and O. Sallent, “A Prioritised Traffic Embedding Mechanism enabling a Public Safety Virtual Operator,” Trinity College Dublin, Tech. Rep. 1505.04148v1, 2014.

[2] H. Gierszal et al., “Migration Towards Broadband PPDR Networks,” in Proc. FedCSIS, 2015, pp. 151–158.

[3] European Commission, *EU Security Union Strategy*, COM(2020) 605 final, Jul. 2020.

[4] Electronic Communications Committee (ECC), *Public Protection and Disaster Relief Spectrum Requirements*, ECC Rep. 102, Jan. 2007.

[5] ITU-R, *Radiocommunication objectives and requirements for public protection and disaster relief*, M.2377-2 (09/2023)

[6] European Commission, *Report on the State of Implementation of the EU Toolbox on 5G Cybersecurity*, Brussels, Belgium, Jul. 2020.

[7] ITU-R, *The use of International Mobile Telecommunications (IMT) for broadband Public Protection and Disaster Relief (PPDR) applications*, Report ITU-R M.2291-2, Dec. 2021

[8] GSMA, *Mobile Telecommunications Security Landscape – 2026*, Jan. 2026.

[9] NIS Cooperation Group, *Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures*, Jan. 2020.

[10] ENISA, *Telecom Security Incidents 2024 Annual Report*, 2025.

[11] OECD, *Enhancing the Resilience of Communication Networks*, OECD Digital Economy Papers, 2025.

[12] NIS Cooperation Group, *Cybersecurity and resiliency of Europe’s communications infrastructures and networks*, 2024.

[13] European Commission, *Security and Resilience of EU Submarine Cable Infrastructures*, Oct. 2025.

[14] ETSI, *Additional spectrum requirements for future Public Safety and Security (PSS) wireless communication systems*, ETSI TR 102 628 V1.2.1, Sep. 2014.

[15] A. Kott et al., “Approaches to Enhancing Cyber Resilience: Report of the NATO Workshop IST-153,” U.S. Army Research Laboratory, Rep. ARL-SR-0396, Apr. 2018.

[16] Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA), “Joint Statement on the People’s Republic of China Targeting of Commercial Telecommunications Infrastructure,” Nov. 13, 2024.

[17] M. Irfan, S. Sciancalepore, and G. Oligeri, “On the Reliability of Radio Frequency Fingerprinting,” arXiv:2408.09179, 2024.

[18] RAND Corporation (Cortney Weinbaum, Steven Berner, and Bruce McClintock), SIGINT for Anyone - The Growing Availability of Signals Intelligence in the Public Domain. PE-273-OSD, 2017.

[19] European Union Agency for Cybersecurity (ENISA), “Signalling Security in Telecom (SS7/Diameter/5G),” Mar. 2018.

[20] European Union Agency for Cybersecurity (ENISA), “ENISA Threat Landscape 2024,” Sep. 2024.

[21] European Union Agency for Cybersecurity (ENISA), “Space Threat Landscape,” 2025.

[22] Stephanie Halwa, Lydia Harriss, UK Parliament Post - POSTnote 749 - Electromagnetic (electronic) warfare (10 July 2025).

[23] European Commission, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, Dec. 2022.

[24] European Commission, *Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive)*, Dec. 2022.

[25] European Union Agency for Cybersecurity (ENISA), *Assessment of EU Telecom Security Legislation*, 2021.

[26] European Commission, *Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*, COM(2022) 454 final, 2022.

[27] European Union Agency for Cybersecurity (ENISA), Good Practices for Supply Chain Cybersecurity (June 2023).

[28] European Union Agency for Cybersecurity (ENISA), *Threat Landscape for 5G Networks*, 2019

[29] Ericsson, Securing an Open AI-Driven Mobile Network, 2026. [Online]. Available: https://www.ericsson.com/assets/local/reports-papers/further-insights/doc/2026/securing-an-open-ai-driven-mobile-network.pdf . [Accessed: Apr. 1, 2026].

[30] European Telecommunications Standards Institute (ETSI), "ETSI TS 104 104 V9.1.0 (2022-01): O-RAN Fronthaul Control, User and Synchronization Plane Specification," Jan. 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/104100_104199/104104/09.01.00_60/ts_104104v090100p.pdf

[31] Council of the European Union, *EU Cyber Blueprint*, 2025.

[32] European Court of Auditors, *Special Reports on EU Cybersecurity and Critical Infrastructure Protection*, 2022.

[33] European Union Agency for Cybersecurity (ENISA), *Good Practices for Incident Reporting*, 2019.

[34] European Union Agency for Cybersecurity (ENISA), *NFV Security in 5G: Challenges and Best Practices*, 2021.

[35] K. Nohl, HITB Security Conference Closing Key-note: The Modern Hacker – From Insight to Impact, 2024

[36] O-RAN Alliance WG11, "O-RAN Security Requirements Specification," O-RAN.WG11.Security-Requirements-Specification, O-R003, Version 7.00, 2022.

[37] European Parliament Research Service (EPRS), *Digital Sovereignty for Europe*, 2020.

[38] European Commission, *European Defence Industrial Strategy*, 2024.

[39] Court of Justice of the European Union (CJEU), *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II), Case C-311/18*, Jul. 2020.

[40] European Commission, *A European Strategy for Data*, COM(2020) 66 final, Feb. 2020.

[41] OECD, *Government Access to Data Held by the Private Sector*, 2022.

[42] European Data Protection Board (EDPB), *Recommendations 01/2020 on Measures that Supplement Transfer Tools*, Jun. 2021.

[43] European Commission, *Strategic Dependencies and Capacities*, SWD(2021) 352 final, May 2021.

[44] European Commission, *Secure Connectivity Programme (IRIS²)*, COM(2022) 57 final, Feb. 2022.

[45] NATO, *Resilience of Critical Infrastructure*, 2023.

[46] European Commission, *EU Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 final, Dec. 2020.

[47] European Commission, *Updating the 2020 Industrial Strategy: Building a Stronger Single Market for Europe's Recovery*, COM(2021) 350 final, May 2021.

[48] European Commission, *A Chips Act for Europe*, COM(2022) 46 final, Feb. 2022.

[49] European Commission, *Strategic Dependencies and Capacities – Detailed Analysis*, 2021.

**[50]** European Commission, Commission Implementing Regulation (EU) 2024/2690 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specifications of significant incidents, 2024.

[51] European Union Agency for Cybersecurity (ENISA), *2024 Report on the State of Cybersecurity in the Union*, 2024.

[52] European Union Agency for Cybersecurity (ENISA), Best Practices for Cyber Crisis Management, 2024.

[53] European Union Agency for Cybersecurity (ENISA), *LEO Satcom Cybersecurity Assessment*, 2024.

[54] European Union Agency for Cybersecurity (ENISA), *NIS360 2024*, 2025.

[55] Body of European Regulators for Electronic Communications (BEREC), *Report on Cybersecurity Challenges and Dependencies of Electronic Communications Networks*, 2023.

[56] Radio Spectrum Policy Group (RSPG), *Report on 6G Strategic Vision*, 2025.

[57] European Union Agency for Cybersecurity (ENISA), *5G Cybersecurity – Security Measures under the EECC (5G Supplement)*, 2021.

[58] European Union, *European Electronic Communications Code (EECC) – Security Supervision Framework*, 2018.

[59] Copenhagen Economics, *Resilience and Security of Telecommunications Infrastructure in Europe*, 2025.

[60] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2025*, 2025.

[61] Smart Networks and Services Joint Undertaking, *Strategic Research and Innovation Agenda 2021–2027*, 2nd ed.

[62] European 6G Infrastructure Association, *European Vision for the 6G Network Ecosystem*.

[63] European Commission, *White Paper: How to Master Europe's Digital Infrastructure Needs?*

[64] NIS Cooperation Group, *Second Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*.

[65] European Commission, *Joint Communication: EU Action Plan on Cable Security*.

[66] European Commission, *Digital Europe Work Programme 2025–2027*.

[67] Smart Networks and Services Joint Undertaking, *Research and Innovation Work Programme 2025*.

[68] NIS Cooperation Group, *Cybersecurity of Open Radio Access Networks*.

[69] Joint Cybersecurity Advisory - PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (February 7, 2024)

[70] Kaleem Ullah et al, SS7 Vulnerabilities - A Survey & Implementation of Machine Learning Vs Rule Based Filtering for Detection of SS7 Network Attacks (February 2020)

[71] Kotikalapudi Sriram, Doug Montgomery, NIST Special Publication 800-189 - Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation (December 2019)

[72] Adrian Perrig et al. SCION: A Secure Internet Architecture (August 2017)

[73] European Union Agency for Cybersecurity (ENISA), *Report on CSIRT–Law Enforcement Cooperation*, Nov. 2022.

[74] Netwrix, "An Overview of the MGM Cyber Attack," 2025. [Online]. Available: https://netwrix.com/en/resources/blog/mgm-cyber-attack/. [Accessed: Mar. 31, 2026].

[75] The Independent, "M&S and Co-op hack linked to social engineering of IT workers," 2025. [Online]. Available: https://www.independent.co.uk/news/business/m-s-coop-hack-scattered-spider-it-worker-b2745218.html. [Accessed: Mar. 31, 2026].

[76] Cisco Talos, "VPNFilter update," 2018. [Online]. Available: https://blog.talosintelligence.com/vpnfilter-update/ . [Accessed: Apr. 1, 2026].

[77] UK National Cyber Security Centre (NCSC), Cyclops Blink malware analysis report, 2022. [Online]. Available: https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf

. [Accessed: Apr. 1, 2026].

[78] Kaspersky, "MoonBounce: The dark side of UEFI firmware," 2022. [Online]. Available: https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/

. [Accessed: Apr. 1, 2026].

[79] Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, “A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate,” *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy006, 2018, doi: 10.1093/cybsec/tyy006.

[80] Help Net Security, “European Commission discloses cyberattack on cloud infrastructure website,” https://www.helpnetsecurity.com/2026/03/30/european-commission-cyberattack-cloud-infrastructure-website/ Mar. 30, 2026.

[81] BleepingComputer, “Dutch police discloses security breach after phishing attack,” https://www.bleepingcomputer.com/news/security/dutch-police-discloses-security-breach-after-phishing-attack/ 2026.