COMTEL
Centro Studi

Centro Studi

COM.TEL. S.p.a.

White Paper

Comunicazioni Sicure e Mission-Critical: verso le Mission-Critical Unified Communications nelle Infrastrutture Critiche

Tecnologie, resilienza, applicazioni e regolazione

Centro Studi COM.TEL S.p.a. – ottobre 2026

Comunicazioni sicure e mission-critical: verso le Mission-Critical Unified Communications.

Tecnologie, resilienza, regolazione e applicazioni nelle infrastrutture critiche

Sommario

Executive Summary **4**

1. Quando i secondi contano **7**

2. Cosa sono le infrastrutture critiche **8**

3. Dalle Unified Communications alle comunicazioni critiche e mission-critical **9**

4. Governance operativa in emergenza: chi decide, chi coordina, come si degrada **11**

5. Le tecnologie che ridisegnano il comparto **13**

5.1. Radio professionale e servizi mission-critical del 3GPP 13

5.2. Il 5G Standalone e il network slicing 14

5.3. Il satellite come garanzia di continuità: backhaul e resilienza 15

5.4. Il rischio GNSS: quando il segnale satellitare diventa un bersaglio 15

5.5. I cavi sottomarini: l'altra faccia della connettività 16

5.6. UC, SBC e registrazione: il collante regolamentato 17

5.7. La sicurezza nella voce: dal toll fraud allo spoofing del Caller ID 17

5.8. Operational Technology, IoT e sistemi SCADA: quando la comunicazione incontra l'impianto fisico 18

5.9. Robotica, droni e digital twin: i nuovi endpoint OT 19

5.10. Il digital twin e il rischio dei dati sintetici 19

5.11. Le autostrade digitali dello spazio aereo a bassa quota 20

5.12. Il sensing distribuito in fibra ottica (DFOS) per il monitoraggio strutturale e perimetrale 22

5.13. Smart City: resilienza Urbana, Infrastrutture IoT e Gestione Integrata delle Emergenze 23

5.14. Verso le Mission-Critical Unified Communications (MCUC) 24

5.15. Il rischio quantum computing 27

5.16. Il problema del brownfield: integrare l'esistente 28

6. Perché ora la minaccia cambia scala **28**

7. Il rapporto ENISA NIS360: la mappa del rischio cyber in Europa **30**

8. Un mercato in crescita strutturale **36**

9. La lettura per area geografica **38**

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

10. I driver e gli ostacoli del settore 40
11. L'Agentic AI nelle comunicazioni critiche 42
12. I casi d'uso: scenari operativi 45
12.1. Difesa 45
12.2. Sicurezza pubblica 46
12.3. Protezione civile 46
12.4. Sanità ed emergenza sanitaria 48
12.5. Trasporti: ferrovie, metropolitane, aeroporti, porti 48
12.6. Energia e utility 49
12.7. Acqua e reti idriche 49
12.8. Finanza e servizi bancari 49
12.9. Telecomunicazioni e infrastrutture digitali 50
12.10. Infrastrutture lineari: strade, viadotti e cantieri critici 50
13. L'ultimo miglio della sicurezza: dall'allerta alla decisione delle persone 51
14. L'ecosistema industriale: dai vendor globali agli integratori di territorio 53
15. COM.TEL.: esperienza nelle Comunicazioni sicure 56
16. Il Quadro regolatorio 56
16.1. NIS2 e CER: la resilienza come requisito 56
16.2. Cybersecurity e governance: la responsabilità arriva ai vertici dell'organizzazione 57
16.3. AI Act: quando l'algoritmo entra in control room 57
16.4. La responsabilità penale nell'uso dell'AI per infrastrutture critiche 58
16.5. GDPR: la protezione dei dati non va in pausa in emergenza 59
16.6. DORA: la resilienza operativa digitale nel settore finanziario 59
16.7. Il dibattito italiano sulla biometria 60
16.8. Il procurement pubblico delle infrastrutture mission-critical 60
16.9. Con chi si costruisce un'infrastruttura critica: il Golden Power 61
16.10. Strategie di Supporto all'Innovazione e Semplificazione Normativa 63
17. Le sfide per il futuro delle comunicazioni mission-critical 63
18. Conclusioni 65
Bibliografia e fonti 67
Glossario 70
Nota metodologica sulle fonti di mercato 75

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Executive Summary

Trasporti, energia, acqua, sanità, finanza, pubblica amministrazione, pubblica sicurezza, difesa: da questi settori dipende gran parte della vita quotidiana del Paese, e il loro funzionamento è sempre più legato a un fattore invisibile ma decisivo, le comunicazioni sicure che tengono unite persone, impianti, sensori e sistemi informativi.

Le comunicazioni sicure e mission-critical sono ormai una componente abilitante della continuità operativa delle infrastrutture critiche: dipendono da reti e piattaforme capaci di funzionare anche quando il resto dell'infrastruttura di comunicazione è sotto stress. Le minacce informatiche ad alta intensità e la crescente frequenza di eventi climatici estremi capaci di isolare interi territori rappresentano fattori avversi che le infrastrutture critiche devono affrontare sempre più frequentemente.

La tesi che attraversa questo white paper può essere sintetizzata in una frase: *le comunicazioni mission-critical non sono più un sottosistema ICT accessorio, ma una componente dell'infrastruttura critica stessa,* al pari della rete elettrica o dell'acquedotto che la comunicazione stessa contribuisce a proteggere. Da questa premessa discendono conseguenze dirette su governance, investimenti e procurement che i capitoli seguenti affrontano nel dettaglio.

L'evoluzione tecnologica porta questo dominio oltre le sole reti radio TETRA e LMR, verso architetture ibride che integrano Unified Communications, servizi mission-critical su LTE/5G, connessioni OT/IoT e, sempre più spesso, backhaul satellitare e intelligenza artificiale per l'analisi e l'automazione.

Le principali società di ricerca stimano per questo mercato un valore tra 20 e 25 miliardi di dollari a metà degli anni Venti, con una crescita annua tra il 7% e l'11% e proiezioni tra 30 e 40 miliardi a metà del prossimo decennio.

Tre motori strutturali stanno accelerando questa transizione: il 5G Standalone, con reti private e network slicing; il satellite, come garanzia di continuità quando la rete terrestre cede; e l'Agentic AI, agenti software capaci di supportare le decisioni operative sotto supervisione umana. A questi si affianca un nuovo modello di sicurezza, lo Zero Trust, che non presume fiducia in alcun componente della rete.

La trasformazione digitale delle infrastrutture critiche non riguarda soltanto reti radio o piattaforme di Unified Communications: robotica, droni, sensori IoT e digital twin stanno entrando nella gestione quotidiana di reti di distribuzione, autostrade, linee elettriche, reti idriche e impianti industriali. Questi sistemi sono a tutti gli effetti nuovi endpoint Operational Techology: vanno protetti con la stessa attenzione riservata ai sensori e ai sistemi di controllo tradizionali perché un attacco su un robot, un drone o un digital twin può tradursi direttamente in rischi fisici e operativi.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

In parallelo, il quadro normativo europeo, NIS2, CER, DORA e AI Act, rende la resilienza delle comunicazioni un obbligo di legge e non più solo una buona pratica aziendale, in un contesto in cui la stessa Agenzia dell'Unione Europea per la Cybersicurezza colloca settori chiave come sanità, ferrovie e reti idriche tra quelli più esposti al rischio cyber.

La tavola rotonda del 1° ottobre al Centro Studi Americano ha riportato al centro tre fattori di dipendenza. Il primo è fisico: cavi sottomarini, collegamenti satellitari e data center sono infrastrutture concentrate, difficili da ridondare, e per questo oggetto di crescente attenzione europea, con un hub regionale per la sicurezza dei cavi nel Mediterraneo coordinato dall'Italia. Il secondo riguarda i fornitori: chi controlla una tecnologia, e da chi un'infrastruttura critica dipende, è una scelta di progetto prima di un controllo a valle, come mostra l'esperienza del Golden Power. Il terzo è temporale: il rischio quantistico, con la logica dell'«harvest now, decrypt later», rende urgente pianificare fin da ora la migrazione verso una crittografia post-quantistica, già oggetto di una proposta di modifica della NIS2.

Resta infine una dimensione spesso trascurata: la catena della sicurezza non si chiude nella control room, ma nella persona che riceve un'allerta e deve trasformarla in una decisione. La resilienza della rete è condizione necessaria; la comprensione del rischio da parte delle persone è ciò che la rende sufficiente.

Questo white paper prosegue ed amplia il lavoro dedicato a “Unified Communications 2026”[1] del Centro Studi COM.TEL., estendendo la prospettiva alle comunicazioni per le infrastrutture critiche che tengono in piedi il Paese e alla convergenza verso le Mission-Critical Unified Communications (MCUC).

Il white paper è stato redatto da un team di ricerca guidato dall’Ing. Pietro Parente, Cultore della Materia in “Tecnologie e Processi Innovativi” presso l’Università LUMSA di Roma e Responsabile del Centro Studi COM.TEL S.p.A. Al documento hanno collaborato esperti, imprese e istituzioni appartenenti a diversi settori. I contenuti sono stati ulteriormente arricchiti dagli spunti emersi durante la tavola rotonda tenutasi il 1° ottobre presso il Centro Studi Americani, grazie agli autorevoli interventi dei partecipanti.

Si ringraziano:

Senatore Alessio Butti, Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri, con delega all’innovazione tecnologica
Dott. Maurizio Bellavista - Finance and Innovation TeaTek S.p.a.
Ing. Claudia Belli - Mission Critica Network & Enterprise Ericsson
Avv. Andrea Cartoni Spinelli
Dott. Enrico Cisnetto - Incontra srl
Avv. Mario Costanzo - Of Counsel Solving
Dott. Stefano Di Nono - TIM Sales Medium Centro Sud Medium.

[1] https://www.comtelitalia.it/wp-content/uploads/2026/07/Unified-Communications_-2026-1.pdf

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Avv. Luigi Fimiani - PhD e Research Fellow Scuola Superiore Sant'Anna
Dott. Gianni Ferrari – Country Manager AudioCodes
Dott. Felice Granisso - Amministratore Delegato del gruppo TeaTek S.p.a.
Dott. Renato Loiero - contributo a titolo personale - Consigliere economico della Presidenza del Consiglio dei Ministri e Direttore della funzione Bilancio in Senato
Ing. Nicola Marietti - CEO e co-fondatore di AiviewGroup, Gruppo ENAV
Ing. Roberto Marseglia - Direttore dell'Osservatorio IA UniEticPMI
Ing. Federico Mauri - Direttore generale di A2A Illuminazione Pubblica
Dott. Minniti Gabriele - Whysecurity S.r.l.
Prof. Simone Mulargia - Professore ordinario di "Sociologia dei processi culturali e comunicativi" Università LUMSA e Presidente del Corso di Laurea in AI for Marketing and Communication dell'Università LUMSA
Prof. Carlo Nardello - Cattedra di "Digital Marketing" Sapienza Università di Roma e Presidente di COM.TEL. S.p.a.
Ing. Michele Palermo - Responsabile Industry & Macroeconomic Scenario e co-lead del comitato operativo del Centro Studi TIM
Dott. Emiliano Pisani - Amministratore Delegato NovaNext & Chief Operating Officer COM.TEL. S.p.a.
Dott. Massimo Rosso - Direttore Acquisti RAI
Prof. Mauro Santaniello - Professore associato in Scienza Politica presso il Dipartimento di Scienze Aziendali - Management e Innovation Systems (DISA-MIS) Università degli Studi di Salerno
Ing. Carlo Alberto Scarpato - CEO, Integra Solutions S.r.l.
Ing. Rosario Sorrentino - Regional Manager Centro Sud COM.TEL.
Ing. Giorgio Maria Tosi Beleffi - Head of TLC Sector presso il Gabinetto del Ministro, Ministero delle Imprese e del Made in Italy
Prof. Avv. Vincenzo Valentini - Referendario Corte di giustizia dell'Unione europea - Università degli Studi Guglielmo Marconi

Come supporto alla stesura del documento sono stati usati prompt di IA.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

1. Quando i secondi contano

C'è un momento, in ogni emergenza, in cui la differenza tra un sistema che regge e uno che cede si misura in secondi: il tempo che una control room impiega a capire cosa sta succedendo, a mettere in contatto le persone giuste, a decidere.

Non è una questione di quantità di tecnologia disponibile, ma di come voce, dati, video e allarmi vengono messi a sistema quando la posta in gioco è la sicurezza delle persone o la continuità di un servizio essenziale. Le comunicazioni sicure e mission-critical sono l'infrastruttura invisibile che rende possibile questo momento. Non sono un capitolo a parte delle telecomunicazioni aziendali, ma un dominio con regole proprie: reti che devono funzionare anche quando il resto della rete è sotto stress, piattaforme che devono garantire priorità e tracciabilità, architetture pensate per la crisi prima ancora che per l'operatività quotidiana.

Difesa, sicurezza pubblica, protezione civile, sanità, trasporti ferroviari e aeroportuali, energia, acqua, servizi finanziari sono settori diversi per missione, ma condividono lo stesso bisogno, comunicare senza interruzioni quando interrompersi non è un'opzione. Ed è un bisogno che sta cambiando pelle: la convergenza tra reti radio professionali, 5G privato, satellite e intelligenza artificiale sta dando forma a un nuovo standard, che analisti e operatori indicano come MCUC, Mission-Critical Unified Communications, l'incontro tra la ricchezza funzionale delle piattaforme di collaborazione aziendale e la resilienza delle reti d'emergenza.

Questo white paper prosegue e amplia il lavoro dedicato a Unified Communications 2026[2], spostando l'attenzione dal *digital workplace* aziendale alle comunicazioni per le infrastrutture critiche che tengono in piedi il Paese. Lo fa attraversando cinque piani che si intrecciano sempre più strettamente: le tecnologie che stanno ridisegnando il comparto, dalla radio professionale al 5G Standalone, dal satellite alle nuove architetture MCUC e all'Intelligenza Artificiale; le ragioni per cui la posta in gioco si è alzata, con un rischio cyber che cambia scala; un mercato globale in crescita strutturale; un perimetro normativo europeo, NIS2, CER, AI Act, DORA, che ha reso la resilienza delle comunicazioni un obbligo di legge prima ancora che una buona pratica; e otto ambiti settoriali in cui questi elementi si traducono in scelte operative concrete, spesso poco visibili ma decisive.

> *"Le comunicazioni critiche e mission-critical sono l'infrastruttura invisibile che rende possibile decidere in pochi secondi, quando decidere è tutto ciò che conta."*

[2] Unified Communications 2026: Prospettive, Innovazione Opportunità (https://www.comtelitalia.it/wp-content/uploads/2026/07/Unified-Communications_-2026-1.pdf

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Questa capacità di decidere in pochi secondi non riguarda solo chi lavora in una control room: riguarda anche il cittadino che riceve un'allerta e deve trasformarla in un'azione, spostarsi, restare, aiutare. Il capitolo 13 approfondisce questo ultimo miglio della sicurezza, quello che porta l'informazione dalla sala operativa alla persona.

2. Cosa sono le infrastrutture critiche

Quando si parla di infrastrutture critiche, il riferimento normativo è la direttiva CER (UE 2022/2557), recepita in Italia con il D.Lgs. 134/2024, che definisce critica un'entità la cui interruzione avrebbe un impatto significativo sulla fornitura di un servizio essenziale, sulla sicurezza pubblica o sulla salute della popolazione. La direttiva individua undici settori: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione, spazio e filiera alimentare. Il decreto italiano ha affidato al Nucleo di sicurezza informatico-critica il compito di individuare le singole entità critiche nazionali. Il 26 aprile 2026 il Presidente del Consiglio ha adottato la prima ***Strategia Nazionale per la Resilienza dei soggetti critici***[3], che articola l'azione dello Stato in tre obiettivi: comprendere lo stato attuale di resilienza dei soggetti critici, conseguire e mantenere un livello elevato di resilienza, promuovere la cooperazione tra gli attori coinvolti a livello nazionale, europeo e internazionale.

Tra questi undici settori, le ***infrastrutture digitali*** meritano una precisazione, perché il tema attraversa l'intero white paper: rientrano in questa categoria non solo ***cloud, data center e content delivery network***, ma gli stessi ***operatori di rete telefonica fissa e mobile***, i fornitori di connettività su cui si appoggiano tutte le comunicazioni critiche descritte nei capitoli successivi. In Italia il legislatore lo ha reso esplicito anche fuori dal perimetro NIS2: dal 2019 le reti di comunicazione elettronica a banda larga basate su tecnologia 5G e i servizi cloud sono classificati come attività di rilevanza strategica ai sensi della disciplina *Golden Power*, che attribuisce al Governo poteri speciali di veto su acquisizioni e forniture critiche in questo comparto, sullo stesso piano di difesa, energia e trasporti.

Al di là della definizione giuridica, per chi si occupa di comunicazioni mission-critical le infrastrutture critiche hanno un volto molto concreto e fisico. Sono le strade e le autostrade su cui viaggiano merci e persone, spesso attraversando viadotti e gallerie che richiedono monitoraggio strutturale continuo. Sono gli acquedotti e le reti fognarie che portano acqua potabile e smaltiscono le acque reflue, spesso con impianti e condotte che risalgono a decenni fa. Sono le ferrovie e le linee ad alta velocità, con i loro sistemi di segnalamento e alimentazione elettrica. Sono le linee elettriche di trasmissione e distribuzione che, come ricorda il capitolo sulle tecnologie, sono già oggi sorvegliate con sistemi SCADA e, sempre più spesso, con droni e robot di ispezione. È infine il sistema di protezione civile che, in caso di incendio, alluvione,

[3] https://www.governo.it/sites/governo.it/files/StrategiaNazionaleResilienzaSoggettiCritici.pdf

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

mareggiata o terremoto, deve mettere in comunicazione sensori sul territorio, sale operative regionali e squadre di soccorso nel più breve tempo possibile.

Ognuna di queste infrastrutture ha una propria criticità, una propria maturità nella gestione del rischio e un proprio perimetro normativo, come illustrato nel capitolo dedicato al rapporto ENISA NIS360; ma tutte condividono lo stesso bisogno di fondo che percorre questo white paper: comunicazioni capaci di funzionare quando serve di più, non solo quando tutto va bene.

Parlare di *resilienza* delle comunicazioni critiche richiede di distinguere quattro piani spesso confusi tra loro. La ***resilienza tecnologica*** riguarda la ridondanza di reti, apparati e collegamenti, il piano su cui si concentra oggi la maggior parte degli investimenti. La ***resilienza operativa*** riguarda la capacità di procedure e processi di continuare a funzionare quando la tecnologia sottostante è sotto stress. La ***resilienza organizzativa*** riguarda la capacità delle persone, delle competenze e della catena di comando di reggere un evento prolungato, non solo il picco iniziale. La ***resilienza sistemica***, infine, riguarda la capacità dell'intero ecosistema, fornitori, energia, connettività, supply chain, di continuare a funzionare insieme. I capitoli tecnologici che seguono descrivono soprattutto il primo livello; i capitoli su procurement e fattore umano affrontano gli altri tre.

3. Dalle Unified Communications alle comunicazioni critiche e mission-critical

Le Unified Communications enterprise – centralini IP, strumenti di collaborazione, messaggistica, videoconferenza – sono fondamentali per il digital workplace, e sono oggetto di una trasformazione profonda spinta dall'intelligenza artificiale, come descritto nel white paper Unified Communications 2026 del Centro Studi COM.TEL.

Ma quando l'interlocutore non è un dipendente in smart working, bensì un operatore di una sala operativa 112, un macchinista, un tecnico di una cabina elettrica o un ufficiale in teatro operativo, le regole cambiano. Le UC da sole, infatti, non coprono i requisiti di resilienza, latenza, priorità e sicurezza richiesti da sale operative di trasporti, centrali di protezione civile, control room di energia o centrali 112/118.

Si parla di **comunicazioni critiche** come l'insieme di tecnologie, reti e piattaforme utilizzate in contesti in cui un'interruzione del servizio può avere conseguenze dirette sulla sicurezza delle persone, sulla continuità di servizi essenziali, sull'ordine pubblico o stabilità economica. Si parla invece di **comunicazioni mission-critical** quando la comunicazione è parte integrante di un processo operativo che non ammette rinvii: il comando di un incidente, il dialogo treno-terra, il coordinamento di un soccorso in emergenza.

Per questo, accanto alla UC aziendale che serve il lavoro quotidiano, le organizzazioni che gestiscono infrastrutture critiche stanno costruendo un secondo binario, dedicato

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

e in parte isolato: un **cluster "critico e sicuro"** che integra reti radio professionali, PMR/LMR, TETRA, P25, servizi mission-critical su LTE/5G, con la telefonia e i sistemi UC, garantendo priorità, protezione e ridondanza anche quando parti della rete ordinaria sono compromesse.

Un'evoluzione di questo principio, sempre più rilevante quanto più le infrastrutture si appoggiano a fornitori cloud e data center condivisi, riguarda ***l'indipendenza effettiva della ridondanza***: due collegamenti apparentemente distinti possono comunque appoggiarsi allo stesso data center, alla stessa dorsale fisica, allo stesso hyperscaler o alla stessa alimentazione elettrica, trasformando una ***ridondanza apparente*** in un unico punto di fallimento nascosto (*point of failure*). Verificare che il secondo binario non condivida con il primo lo stesso elemento sottostante è parte integrante, e spesso trascurata, della progettazione di un'architettura realmente resiliente.

Verificare questa indipendenza non può essere un esercizio compiuto una sola volta, in fase di progettazione: fornitori cloud, dorsali fisiche e accordi di fornitura cambiano nel tempo, e una ridondanza indipendente oggi può smettere di esserlo silenziosamente, senza che nessuna modifica esplicita all'architettura lo segnali. Per questo, accanto al principio, andrebbe prevista una pratica: un audit periodico, non solo documentale ma tecnico, che verifichi concretamente se i due canali ridondati condividono ancora, a qualsiasi livello della catena, lo stesso punto di fallimento. Una duplicazione apparente, scoperta durante un'emergenza reale, è più pericolosa di una ridondanza dichiaratamente assente, perché genera un falso senso di sicurezza fino al momento in cui serve davvero.

Nel modello a ***"doppio binario"*** la UC&C enterprise resta dedicata al lavoro quotidiano e alle comunicazioni non operative; il cluster "critico e sicuro" serve invece control room, centrali operative e dispatch, con requisiti di disponibilità e sicurezza molto più elevati. In tempo di pace, questo secondo binario ottimizza flussi di lavoro e monitoraggio; in emergenza, isola i percorsi critici e protegge la capacità operativa delle sale di comando anche quando il resto dell'infrastruttura IT è sotto attacco o fuori uso.

Al centro di questo modello ci sono due componenti tecnologiche che meritano di essere conosciute anche fuori dagli ambienti specialistici.

La **Console di dispatch di nuova generazione** è l'interfaccia che permette agli operatori di gestire in un solo ambiente chiamate, allarmi e flussi provenienti da radio professionali, telefonia, UC e sistemi di allarme, con funzioni di registrazione e instradamento verso i terminali sul campo o verso il videowall della control room.

Il **Session Border Controller (SBC)** è invece il gateway perimetrale che gestisce il routing prioritario, la cifratura, la normalizzazione dei protocolli e l'isolamento logico tra

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

domini di rete diversi, radio, UC, rete telefonica pubblica, reti IP esterne, garantendo continuità operativa anche quando uno di questi domini viene compromesso.

La control room aggrega voce, video e dati OT/IoT in un'unica immagine operativa comune, che consente a operatori e decisori di avere piena consapevolezza situazionale in tempo reale (**situational awarness**): videowall, mappe georeferenziate, telemetria degli impianti, stato delle chiamate, ticket e allarmi convergono in un'unica piattaforma di comando e controllo, sorretta da un'architettura ridondata che comprende connettività, sistemi di autenticazione, applicazioni, registrazione, alimentazione e procedure operative.

Chi intende colpire un'infrastruttura critica non ha necessità di aggredirla materialmente, essendogli sufficiente degradare la capacità di chi la governa di vedere, comprendere e decidere. È un'opzione meno costosa, meno tracciabile e di più difficile attribuzione.

Le comunicazioni *mission-critical* non costituiscono dunque un supporto tecnico delle infrastrutture critiche, ma la condizione del loro funzionamento. Questo aspetto è cruciale ed elegge l'intero dominio delle comunicazioni mission-critical a questione di sicurezza nazionale e non soltanto di continuità operativa.

Se il bersaglio è la decisione, muta anche la natura della difesa. Nella cosiddetta zona grigia – ossia al di sotto della soglia del conflitto armato, con attribuzione incerta – la deterrenza fondata sulla minaccia di rappresaglia opera con difficoltà, non potendosi reagire contro un avversario che non si riesca a identificare con certezza. Resta praticabile la deterrenza per negazione del risultato, che non rende l'attacco costoso ma inutile.

Ne discende che la ***resilienza***, abitualmente presentata come virtù difensiva e passiva, assume in questo contesto una funzione strategica attiva: ove l'avversario sappia che l'interruzione di un nodo non paralizzerà il sistema, perché esistono percorsi alternativi, capacità autonome di funzionamento locale e procedure già esercitate, l'operazione Perché la resilienza dissuada, essa deve essere nota, e la sua comunicazione espone inevitabilmente informazioni sull'architettura che la sorregge. La soluzione ragionevole consiste nel rendere pubblico il livello complessivo di preparazione e non la mappa dei nodi.

4. Governance operativa in emergenza: chi decide, chi coordina, come si degrada

Le tecnologie descritte in questo white paper rispondono alla domanda "come garantire che la comunicazione funzioni". Restano aperte due domande altrettanto decisive, e più organizzative che tecnologiche: chi ha l'autorità di attivare il canale alternativo quando un'infrastruttura entra in modalità emergenziale, chi assegna le priorità tra le comunicazioni in competizione per la stessa banda, e chi coordina IT,

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

OT, sicurezza fisica e control room quando smettono di essere compartimenti separati e diventano, per la durata della crisi, un'unica catena di comando. Nelle organizzazioni più mature queste risposte sono scritte in un piano di continuità operativa e testate con esercitazioni periodiche; in molte altre restano implicite, e si scoprono solo durante l'emergenza reale, quando è troppo tardi per definirle.

Una seconda domanda, complementare, riguarda la ***modalità degradata***: che cosa succede, operativamente, quando parte dell'infrastruttura non è disponibile? Non tutte le funzioni hanno la stessa priorità di sopravvivenza: alcune, come le comunicazioni vocali di comando, devono restare attive per prime; altre, come i servizi dati non urgenti, possono essere temporaneamente sospese senza conseguenze dirette sulla sicurezza. Il passaggio dalla rete primaria a quella alternativa può essere automatico, come nei meccanismi di preemption descritti nel capitolo sulle tecnologie, oppure richiedere un'autorizzazione umana esplicita. La scelta tra le due modalità non è neutra, perché un passaggio automatico riduce il tempo di reazione ma può generare falsi positivi, mentre uno autorizzato è più prudente ma introduce un ritardo che, in alcuni scenari, può essere esso stesso un rischio.

A queste due dimensioni si aggiunge un terzo tema, tanto più rilevante quanto più un'emergenza reale coinvolge soggetti diversi: ***l'interoperabilità*** non è solo tra piattaforme tecnologiche, come descritto nei capitoli precedenti a proposito di gateway multi-vendor e raccordo tra TETRA, 5G, UC e SCADA, ma **tra organizzazioni** con procedure, autorizzazioni e catene di comando differenti, il gestore dell'infrastruttura, l'operatore telco, le forze dell'ordine, la protezione civile, i manutentori, i fornitori ICT. Far dialogare due piattaforme è un problema tecnico che questo white paper affronta; far collaborare in tempo reale organizzazioni che normalmente non condividono una catena di comando è un problema che nessuna tecnologia, da sola, risolve.

Che questo non sia un problema soltanto teorico lo conferma la stessa ***Strategia Nazionale per la Resilienza dei soggetti critici***[4], descritta nel capitolo sul quadro normativo: la valutazione del rischio nazionale condotta dal Punto di Contatto Unico presso la Presidenza del Consiglio ha rilevato che le interdipendenze trasversali tra settori rappresentano una vulnerabilità critica in quasi ogni ambito, non un'eccezione isolata, e la Strategia riconosce esplicitamente che il coinvolgimento del settore privato è una necessità, dato che la maggior parte delle infrastrutture che erogano servizi essenziali in Italia è gestita da operatori privati.

Per rendere misurabile questi aspetti, un insieme di ***indicatori operativi*** potrebbe accompagnare i piani di resilienza delle comunicazioni critiche: la *disponibilità effettiva del servizio*, non teorica ma verificata sul campo; il *tempo di attivazione del canale di fallback*; la *percentuale di chiamate prioritarie completate con successo* durante un evento; la *copertura reale delle aree più critiche*; il *tempo di ripristino dopo un'interruzione*; il *tempo di propagazione di un'allerta* dalla sua origine fino all'ultimo destinatario; e la *tracciabilità completa delle comunicazioni* intercorse, necessaria

[4] https://www.governo.it/it/articolo/strategia-nazionale-la-resilienza-dei-soggetti-critici/32064

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

tanto per la gestione dell'emergenza quanto per l'analisi post-evento richiesta da NIS2 e CER.

Questi indicatori, più che una lista definitiva, sono un punto di partenza: la loro calibrazione settore per settore, trasporti, energia, difesa, sanità, è precisamente il tipo di confronto che un tavolo tra istituzioni, operatori e università può rendere concreto meglio di quanto possa fare un documento.

Un altro aspetto da considerare utile a chi progetta le architetture descritte in questo white paper: la difficoltà nel proteggere sistemi complessi non nasce quasi mai dai singoli componenti, spesso sufficientemente sicuri se considerati isolatamente, ma dal momento in cui questi componenti vengono messi in comunicazione tra loro. La ***complessità***, in altre parole, ***è nemica della sicurezza***. Da qui una proposta di introdurre per le infrastrutture critiche, una forma di revisione periodica della cybersicurezza, sul modello della revisione obbligatoria dei veicoli o della revisione contabile delle società, non un controllo compiuto una sola volta in fase di progettazione, ma una verifica indipendente e ricorrente nel tempo, che consideri insieme processi, persone e tecnologia, e che includa test costruiti per emulare le tecniche di avversari sofisticati, oggi la principale fonte di rischio per chi gestisce infrastrutture critiche.

5. Le tecnologie che ridisegnano il comparto

5.1. Radio professionale e servizi mission-critical del 3GPP

Per decenni le comunicazioni mission-critical sono state sinonimo di radio professionale: reti Land Mobile Radio, TETRA, P25, pensate per polizia, servizi di emergenza, difesa e trasporti, apprezzate per l'affidabilità e per la funzione push-to-talk, che permette di parlare a un intero gruppo con la pressione di un tasto.

Il settore ferroviario ha seguito un percorso analogo con il GSM-R, oggi in fase di migrazione verso il nuovo standard FRMCS, pensato per garantire la stessa affidabilità unita alle capacità dati del 5G.

Il 3GPP, l'organismo che definisce gli standard delle reti mobili, ha portato questa logica dentro LTE e 5G attraverso i servizi MCX (Mission Critical Services). Le specifiche 3GPP definiscono un insieme di servizi mission-critical, tra cui Mission Critical Push-to-Talk, Mission Critical Video e Mission Critical Data. Tali servizi sono progettati per supportare priorità, gestione dei gruppi, continuità del servizio e interoperabilità su reti mobili broadband. Un percorso in continua evoluzione avviato con la Release 13 del 2016 che ha introdotto il Mission Critical Push-to-Talk, la Release 14 che vi ha aggiunto il Mission Critical Video e il Mission Critical Data con le evoluzioni successive fino al 5G-Advanced.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Questi servizi replicano su rete mobile le funzioni di priorità e preemption tipiche della radio professionale: una comunicazione critica può così prendere automaticamente la precedenza su una non critica. Nella pratica, gli operatori non stanno sostituendo la radio con il 5G da un giorno all'altro, la stanno affiancando, costruendo architetture ibride in cui la rete tradizionale (TETRA/LMR) resta un fallback affidabile mentre le nuove funzionalità, video, dati ad alta velocità, applicazioni di control room, arrivano attraverso le reti mobili di ultima generazione. Gli investimenti in infrastrutture Public Safety LTE/5G, secondo alcune stime di settore, sono passati da circa 4,3 miliardi di dollari nel 2023 a una proiezione superiore ai 6 miliardi entro il 2030.

5.2. Il 5G Standalone e il network slicing

Il salto di qualità arriva con il **5G Standalone** (5G SA), la versione della rete mobile che utilizza un core nativamente 5G invece di appoggiarsi all'infrastruttura 4G esistente. È questa architettura a rendere possibile il **network slicing**: la creazione di "fette" di rete logicamente separate, ciascuna dedicata a un servizio specifico, pubblica sicurezza, controllo industriale, trasporto, con risorse radio e di core riservate e parametri di latenza e affidabilità garantiti contrattualmente, non semplicemente auspicati. L'efficacia del network slicing dipende comunque dall'architettura end-to-end, dalla disponibilità di 5G Standalone, dall'orchestrazione, dalla qualità della rete di trasporto e dagli accordi di servizio.

A questo si aggiunge la **comunicazione ultra-affidabile a bassissima latenza** URLLC (Ultra-Reliable Low-Latency Communications), che rende possibile il controllo remoto di impianti e la gestione in tempo reale di veicoli e macchinari connessi.

Inoltre, la connessione di una moltitudine di dispositivi alle reti 5G richiede la gestione intelligente del traffico dati attraverso meccanismi di ***preemption*** (prioritarizzazione), che consentono di declassare il monitoraggio ordinario in caso di emergenza per dare precedenza assoluta alle comunicazioni critiche.

Inoltre, situazioni di pubblica sicurezza o emergenza richiedono soluzioni temporanee e localizzate, come l'attivazione di ***"bolle tattiche 5G"*** per garantire la connettività immediata e sicura in zone colpite da crisi o prive di copertura.

Analisi McKinsey e di altri istituti sottolineano come il 5G Standalone e lo slicing sono abilitanti imprescindibili per casi d'uso industriali e infrastrutturali, dal controllo delle sottostazioni elettriche alla gestione del traffico ferroviario connesso, ma richiedono anche capacità solide di orchestrazione e sicurezza end-to-end, che non tutte le organizzazioni possiedono internamente e che spesso vanno costruite insieme a un partner tecnologico.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

5.3. Il satellite come garanzia di continuità: backhaul e resilienza

Il satellite ha smesso da tempo di essere una soluzione residuale per le zone senza copertura terrestre. Nelle architetture mission-critical più recenti gioca tre ruoli distinti:

- backhaul di continuità quando la rete terrestre, fibra, mobile, ponti radio, si guasta;
- connettività primaria in aree remote come zone montane, piattaforme offshore, tratte ferroviarie o stradali isolate;
- supporto a reti mobili di emergenza temporanee, come celle 5G o LTE montate su mezzi mobili con collegamento satellitare.

L'evoluzione dei satelliti in orbita bassa LEO e la diffusione di offerte di connettività ibrida che combinano rete terrestre e satellitare, stanno rendendo il satellite un elemento di progetto ordinario, non più un'eccezione, per protezione civile, difesa, trasporti e utility, in particolare negli scenari di disastro naturale esteso, dove le infrastrutture terrestri sono le prime a cedere.

5.4. Il rischio GNSS: quando il segnale satellitare diventa un bersaglio

Il satellite, descritto in questo capitolo come garanzia di continuità, porta con sé anche una vulnerabilità specifica che riguarda non solo la connettività ma la localizzazione e la sincronizzazione temporale: il segnale GNSS, Global Navigation Satellite System, su cui si basano GPS e il sistema europeo Galileo, è per sua natura debolissimo quando raggiunge la superficie terrestre, e per questo esposto a due tipi di interferenza. Il jamming disturba o rende indisponibile il segnale; lo spoofing invece lo falsifica, restituendo al ricevitore una posizione o un orario apparentemente validi ma errati. L'Agenzia europea per la sicurezza aerea, EASA, ha aggiornato a luglio 2026 il proprio bollettino di sicurezza sulle interferenze GNSS, introducendo procedure standardizzate di comunicazione tra piloti e controllo del traffico aereo e avviando, insieme a EUROCONTROL, un piano condiviso di monitoraggio degli eventi di interferenza su scala europea.

Il rischio, tuttavia, non riguarda solo l'aviazione: il GNSS è anche il riferimento di sincronizzazione temporale per reti di telecomunicazione, borse valori e reti elettriche, gli stessi settori che il rapporto ENISA NIS360, descritto nel capitolo 7, colloca ora tra i più critici anche a causa della crescente dipendenza dai servizi satellitari. Per le infrastrutture mission-critical descritte in questo white paper, dai droni, ai sistemi di localizzazione delle squadre di soccorso, la raccomandazione è la stessa indicata dalla Commissione Europea nel proprio piano sulla navigazione radio: non affidarsi in modo esclusivo al segnale satellitare, mantenendo sistemi di posizionamento e sincronizzazione complementari come riserva in caso di interferenza.

Un rischio distinto, meno discusso, riguarda la **cifratura dei collegamenti di comando tra i satelliti e le stazioni di terra**: storicamente, per limiti di banda e di

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

latenza, non tutte le trasmissioni satellitari sono state cifrate, inclusi in alcuni casi i comandi stessi inviati al satellite nel momento del passaggio sopra la stazione a terra. Poiché cifrare significa anche autenticare reciprocamente i due soggetti che comunicano, questo resta un punto di attenzione per chi integra connettività satellitare in un'architettura mission-critical, da includere nella stessa valutazione di migrazione crittografica descritta a proposito del rischio quantistico.

5.5. I cavi sottomarini: l'altra faccia della connettività

Nel contesto delle comunicazioni sicure e della protezione delle infrastrutture critiche — ambiti regolati a livello normativo da strumenti quali il Golden Power e il nascente Cybersecurity Act europeo — emerge la centralità strategica delle infrastrutture sottomarine e dei data center, oggi considerati target sensibili negli scenari geopolitici e di guerra.

Se il satellite rappresenta la connettività che non tocca terra, i cavi sottomarini restano la spina dorsale fisica da cui transita la quasi totalità del traffico dati intercontinentale, incluso quello che alimenta le reti terrestri descritte in questo white paper. L'Italia, al centro del Mediterraneo, è un punto di approdo e smistamento particolarmente denso: il solo Sicily Hub di Sparkle collega diciotto cavi sottomarini internazionali.

Il tema è entrato stabilmente nell'agenda di sicurezza europea dopo gli incidenti che negli ultimi anni hanno coinvolto infrastrutture sottomarine nel Mar Baltico. La Commissione Europea ha varato nel febbraio 2025 ***l'Action Plan on Cable Security*** e il 23 giugno 2026 ha annunciato l'istituzione dei primi due ***Regional Cable Hub***, centri di sorveglianza e coordinamento dedicati: uno nel Baltico, l'altro nel Mediterraneo, coordinato dall'Italia insieme a Grecia, Cipro e Malta, con un finanziamento di 3,3 milioni di euro. Lo stesso giorno la Commissione ha aperto un bando da 40 milioni di euro nell'ambito del programma ***Connecting Europe Facility Digital*** per rafforzare la capacità europea di riparazione d'emergenza dei cavi, attraverso moduli rapidamente dispiegabili su navi già operative nel Mediterraneo, nell'Atlantico e in altri bacini.

I cavi sottomarini, infrastrutture "ipercritiche"

L'azione del Ministero delle Imprese e del Made in Italy (MIMIT) si è mossa tempestivamente rispetto alle direttive della Commissione Europea, strutturando un modello d'intervento basato su cooperazione e leadership internazionale. Ha avviato da oltre due anni un Tavolo di Concertazione Pubblico-Privato che unisce 10 amministrazioni pubbliche, 3 associazioni di categoria e 11 grandi operatori privati di rilevanza globale (tra cui Fincantieri, Sparkle, Saipem, Eni, Terna e Prysmian). Questo strumento ha permesso di mappare l'intera filiera e attivare incentivi dedicati alle PMI e ha consentito di porre la centralità strategica dell'Italia che ospita l'approdo di circa 30 cavi sottomarini internazionali. L'Italia si configura come *l'hub naturale* del Mediterraneo e il ponte di connessione verso l'Africa e il Medio Oriente e si è aggiudicata la guida del progetto europeo per la costruzione del primo hub di sorveglianza delle infrastrutture

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

sottomarine nel Mediterraneo (coinvolgendo Grecia, Cipro e Malta) e punta a partecipare al progetto europeo al co-finanziato per la costruzione di moduli per la riparazione dei cavi sottomarini.

In parallelo, il catasto nazionale federato delle infrastrutture (SINFI), gestito da Infratel Italia, si sta estendendo alle infrastrutture subacquee con un modello dati dedicato: i dati relativi alle infrastrutture sottomarine considerate strategiche non saranno accessibili al pubblico, e l'investimento complessivo, che comprende anche lo sviluppo di un digital twin del sottosuolo nazionale, è stimato in 69,9 milioni di euro.

Per le comunicazioni mission-critical descritte in questo white paper, i cavi sottomarini meritano la stessa lettura già proposta per il satellite: un'infrastruttura fisica concentrata, difficile da ridondare con un secondo cavo che condivida la stessa rotta o lo stesso punto di approdo, e per questo da considerare esplicitamente nella mappatura delle dipendenze “ipercritiche”.

5.6. UC, SBC e registrazione: il collante regolamentato

Le piattaforme di Unified Communications e i componenti di sicurezza del perimetro voce-dati restano il punto di raccordo tra il mondo radio/5G e quello enterprise:

- Le UC e i sistemi IP-PBX gestiscono le conferenze di coordinamento e i ponti tra reti radio e telefonia;
- i Session Border Controller assicurano l'interconnessione sicura tra domini diversi, control room, reti esterne, altri enti, con funzioni di cifratura e resilienza;
- i sistemi di registrazione vocale a norma sono obbligatori in molti domini regolamentati, controllo del traffico aereo, ferrovia, mercati finanziari, dove tracciabilità e conservazione a lungo termine delle comunicazioni sono un requisito di legge.

Fornitori globali come Cisco, Nokia, Oracle, con la tecnologia ex Acme Packet, AudioCodes e NEC integrano questi elementi nelle proprie soluzioni, quasi sempre in collaborazione con system integrator locali capaci di adattarle alle normative nazionali e alle esigenze specifiche di ogni settore.

5.7. La sicurezza nella voce: dal toll fraud allo spoofing del Caller ID

Anche quando dati e video assumono un ruolo crescente, la voce resta il canale di coordinamento più immediato nelle infrastrutture critiche, e proprio per questo è un bersaglio. Il perimetro SIP che collega centralini, Session Border Controller, reti degli operatori e piattaforme UCaaS espone a nuove minacce specifiche: toll fraud e l'International Revenue Share Fraud, in cui un interno compromesso genera

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

automaticamente chiamate verso numerazioni internazionali a tariffazione maggiorata; gli attacchi SIP flood/DoS che saturano centralini e SBC; lo spoofing del Caller ID, che induce l'utente a fidarsi di una chiamata che sembra provenire da un numero legittimo; e le campagne di vishing verso cittadini e personale interno.

Le contromisure più efficaci si distribuiscono lungo l'intera "catena della voce" dagli accessi legacy fino alle piattaforme UCaaS – PBX legacy, gateway TDM/SIP, SBC, SIP trunk e piattaforme UCaaS –: hardening dei centralini, segregazione delle reti di gestione, cifratura TLS/SRTP del traffico e limitazione del traffico verso destinazioni ad alto rischio, insieme al monitoraggio dei CDR, i registri dettagliati delle chiamate, per individuare pattern anomali prima che si traducano in perdite economiche. In questo schema gli SBC restano il presidio centrale, affiancati da sistemi di fraud management capaci di isolare rapidamente segmenti di rete o numerazioni sospette. In Italia il tema ha assunto anche una dimensione regolatoria diretta: con la delibera n. 106/25/CONS, AGCOM ha imposto agli operatori il blocco delle chiamate dall'estero che utilizzano numerazioni italiane contraffatte, un intervento entrato in vigore tra agosto e novembre 2025 che, secondo la Relazione annuale AGCOM 2026, ha permesso di bloccare oltre 120 milioni di chiamate illecite nei primi mesi di applicazione. Anche in questo ambito, la voce non è un servizio accessorio ma un asset che richiede lo stesso rigore progettuale e la stessa attenzione regolatoria, NIS2, DORA, GDPR, riservate alle altre componenti mission-critical descritte in questo white paper.

5.8. Operational Technology, IoT e sistemi SCADA: quando la comunicazione incontra l'impianto fisico

Nel mondo delle infrastrutture critiche, reti elettriche, impianti idrici, sistemi ferroviari e siti industriali sono governati da tecnologie operative (Operational Technology, OT) e sistemi SCADA (Supervisory Control and Data Acquisition) che raccolgono dati dal campo e comandano gli impianti attraverso protocolli industriali come Modbus, DNP3, IEC-104 o OPC-UA, sempre più spesso trasportati su reti IP protette.

A questi si aggiungono sensori IoT distribuiti, per il monitoraggio strutturale, ambientale o di processo, e dashboard che restituiscono in tempo reale, attraverso un **digital twin**, lo stato degli asset fisici e i flussi di allarme.

L'integrazione tra OT/IoT e comunicazioni mission-critical è ciò che permette alle sale operative di passare da un modello reattivo, che risponde alle chiamate quando arrivano, a un modello proattivo, guidato dai dati, in cui gli allarmi e le previsioni supportate dall'intelligenza artificiale anticipano il problema prima che diventi un'emergenza conclamata.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

5.9. Robotica, droni e digital twin: i nuovi endpoint OT

Accanto ai sensori e ai controllori tradizionali, un nuovo strato di dispositivi sta entrando nella gestione quotidiana delle infrastrutture critiche: robot di ispezione, droni e gemelli digitali. L'ispezione robotica di gallerie, condutture e cavidotti, i droni per il monitoraggio del traffico, delle linee elettriche e dei cantieri, e i digital twin che replicano in tempo reale lo stato di un asset fisico stanno diventando strumenti ordinari di manutenzione predittiva nei settori energia, trasporti e utility, non più sperimentazioni isolate.

Dal punto di vista della sicurezza, questi sistemi vanno trattati per quello che sono: nuovi endpoint OT, non una categoria a parte esente dalle regole già descritte in questo capitolo. Un drone che trasmette video in tempo reale a una control room, o un robot che accede alla rete di automazione di un impianto per caricare i propri dati di ispezione, espande la superficie di attacco esattamente come farebbe un nuovo sensore SCADA: va autenticato, segmentato dalla rete IT generale e monitorato con gli stessi criteri Zero Trust applicati al resto dell'infrastruttura critica.

La sfida dei prossimi anni, in questo ambito, non è tecnologica ma organizzativa: portare l'automazione fisica, robot, droni, digital twin, dentro lo stesso perimetro di governance e sicurezza di rete già applicato a SCADA e IoT industriale, invece di trattarla come un'iniziativa isolata dei team di manutenzione o di innovazione, scollegata dalla cybersecurity dell'infrastruttura nel suo complesso.

Un aspetto che merita di essere reso esplicito, e non solo implicito nella raccomandazione di trattare questi dispositivi come endpoint OT, è la convergenza tra ***sicurezza informatica e sicurezza fisica***: una compromissione che nasce come evento cyber produce, in questi sistemi, una conseguenza fisica immediata. L'alterazione di un flusso video può nascondere un evento reale all'operatore in control room; la perdita di controllo di un drone, per interferenza o attacco deliberato, può trasformare uno strumento di sorveglianza in un pericolo esso stesso; lo spoofing GNSS descritto nel capitolo sul satellite può indirizzare un dispositivo lontano dal percorso previsto senza che l'operatore se ne accorga in tempo; una telemetria falsificata può indurre una squadra a ritenere sicura un'area che non lo è, o a non attivare un soccorso che sarebbe stato necessario.

Progettare la sicurezza di questi sistemi richiede quindi una competenza che oggi raramente siede nella stessa stanza: chi si occupa di cybersecurity di rete e chi si occupa di sicurezza fisica degli impianti.

5.10. Il digital twin e il rischio dei dati sintetici

Un digital twin, la replica virtuale di un impianto o di un'infrastruttura costruita a partire dai flussi di dati IoT descritti in questo capitolo, è solido quanto affidabili sono i dati che lo alimentano. L'intelligenza artificiale, applicata a questo ambito, gioca un doppio

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

ruolo, non riducibile a un semplice bilancio tra beneficio e rischio. Da un lato permette di analizzare in tempi rapidi la mole di dati generata da sensori distribuiti, utile tanto alla diagnosi del funzionamento degli impianti quanto all'individuazione di comportamenti anomali nella rete che li collega. Dall'altro, la stessa capacità generativa che rende possibile questa analisi può essere usata per produrre dati sintetici credibili: un digital twin può essere indotto a simulare una condizione catastrofica che non esiste, generando un allarme falso che distoglie risorse e attenzione da dove servirebbero davvero, oppure, specularmente, a mascherare una condizione catastrofica reale facendola apparire come normale operatività, ritardando una risposta che sarebbe invece urgente.

Questo rischio riporta l'attenzione su un principio di base della sicurezza informatica che il mondo IoT, concentrato spesso più sul trasportare il dato che sul garantirne l'attendibilità, non sempre rispetta con il dovuto rigore: la tenuta congiunta di confidenzialità, integrità e disponibilità del dato trasmesso. Per un digital twin applicato a un'infrastruttura critica, sapere che un dato non è stato manomesso, e che è disponibile nel momento in cui serve, non è meno importante che tenerlo riservato. È una sfida che, più delle altre descritte in questo capitolo, chiama in causa non solo soluzioni tecniche ma un investimento nella cultura della sicurezza all'interno delle organizzazioni che adottano queste tecnologie, lo stesso tema affrontato, da un'altra prospettiva, nel capitolo sull'ultimo miglio della sicurezza.

5.11. Le autostrade digitali dello spazio aereo a bassa quota

Nel caso dei droni l'evoluzione non riguarda soltanto l'aumento del numero di dispositivi connessi. La diffusione delle operazioni ***UAS (Unmanned Aircraft Systems)*** apre progressivamente alla creazione di una nuova infrastruttura di trasporto a bassa quota, nella quale un numero crescente di aeromobili senza pilota dovrà condividere lo spazio sopra città, strade, ferrovie, porti, aeroporti, reti energetiche e altre infrastrutture critiche.

È il paradigma dello ***U-space***: un insieme di servizi digitali progettati per consentire l'accesso sicuro e scalabile dei droni allo spazio aereo. In termini concettuali, si può immaginare come la costruzione di vere e proprie ***"autostrade digitali del cielo",*** *una nuova infrastruttura critica invisibile* nella quale la separazione e il coordinamento non sono affidati a corsie fisiche, semafori o barriere, ma allo scambio continuo e affidabile di informazioni tra aeromobili, operatori, piattaforme digitali e soggetti responsabili della gestione dello spazio aereo.

In questo scenario, le comunicazioni assumono una funzione direttamente connessa alla sicurezza. Attraverso i servizi U-space vengono infatti gestite informazioni necessarie alla identificazione degli aeromobili, autorizzazione all'accesso allo spazio aereo, conoscenza della posizione e delle operazioni in corso e gestione delle possibili interferenze tra operazioni concorrenti. Il traffico dei droni diventa quindi un sistema

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

cyber-fisico distribuito nel quale la capacità di comunicare in modo affidabile costituisce uno degli elementi abilitanti della sicurezza complessiva.

L'architettura UAS non si esaurisce nella componente hardware del vettore aereo, ma si configura come un ecosistema che connette sensoristica remota e stazioni di controllo centralizzate alle sale traffico operative, eliminando la necessità di presidi antropici *in loco* e garantendo la continuità operativa del business infrastrutturale in condizioni di massima sicurezza. L'impiego di tali tecnologie ottimizza i processi di **manutenzione predittiva (*predictive maintenance*)** attraverso l'acquisizione continua e standardizzata di *big data* diagnostici ed incrementa la **resilienza sistemica** dell'infrastruttura, intesa come capacità di assorbire shock esogeni e ripristinare rapidamente i livelli nominali di servizio.

Questa trasformazione introduce una conseguenza importante per le infrastrutture critiche. Un drone che perde la capacità di essere identificato, autorizzato, localizzato o coordinato non rappresenta soltanto un terminale che ha perso la connessione: diventa un oggetto fisico in movimento all'interno di uno spazio condiviso.

La disponibilità e l'integrità delle comunicazioni diventano quindi requisiti essenziali.

Un'interruzione, un ritardo significativo o un'alterazione delle informazioni può compromettere la capacità di conoscere chi sta utilizzando una determinata porzione di spazio aereo, verificare se un'operazione sia autorizzata o coordinare operazioni simultanee.

Il problema assume una rilevanza ancora maggiore quando queste nuove infrastrutture a bassa quota intersecano infrastrutture critiche terrestri. Autostrade, ferrovie, aeroporti, porti, centrali elettriche, reti energetiche e aree urbane potranno essere contemporaneamente luoghi da monitorare attraverso droni e spazi attraversati da altre operazioni UAS. La sicurezza dell'infrastruttura fisica e quella dello spazio aereo sovrastante diventano così progressivamente interdipendenti.

Per questa ragione, nel futuro ecosistema U-space la comunicazione non può essere considerata un semplice servizio di connettività. Diventa parte della **"traffic infrastructure"** che rende possibile organizzare e governare il traffico aereo a bassa quota. Come una rete stradale non potrebbe funzionare in sicurezza senza identificazione dei veicoli, regole di accesso, segnaletica, gestione delle interferenze e informazioni sul traffico, allo stesso modo una rete ad alta densità di operazioni UAS richiede servizi digitali capaci di costruire una rappresentazione condivisa e affidabile dello spazio aereo.

La conseguenza è particolarmente significativa dal punto di vista delle comunicazioni mission-critical: se i servizi digitali che identificano, autorizzano e coordinano gli oggetti volanti non possiedono adeguati livelli di disponibilità, integrità, autenticazione, resilienza e cybersecurity, gli stessi oggetti che dovrebbero supportare la sicurezza e l'operatività delle infrastrutture possono trasformarsi in un nuovo fattore di rischio per esse.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Questo amplia il concetto stesso di infrastruttura critica. Alla protezione delle reti terrestri e degli endpoint OT si aggiunge progressivamente la necessità di proteggere ***l'infrastruttura digitale che governa lo spazio aereo a bassa quota***, perché da essa dipenderà la possibilità di utilizzare in sicurezza flotte sempre più numerose di sistemi autonomi.

Le autostrade del cielo: una nuova infrastruttura critica invisibile.

Una nuova infrastruttura critica invisibile. I droni aumenteranno di numero per monitorare infrastrutture lineari -l'autostrada - e infrastrutture a sito o ad area. L'America e l'Europa stanno già disegnando le "autostrade del futuro", quelle dedicate ai droni: l'FAA (Federal Aviation Administration) e l'EASA (European Union Aviation Safety Agency stanno definendo le regole per la gestione dello spazio aereo a bassa quota, tra zero e 150 metri di altezza (500 piedi), dove migliaia di droni per il monitoraggio di autostrade, condotte e cantieri potranno presto condividere corsie, priorità e regole di traffico proprio come fanno oggi le automobili. I droni avranno bisogno di comunicazioni sicure non solamente per trasmettere un video o trasmettere un'immagine, ma per essere loro stessi satelliti di comunicazione tra di loro, e per avere i concetti di autorizzazione, di segregazione dello spazio e di *positioning* all'interno dello spazio, in un ambiente distribuito. Come oggi le macchine hanno le corsie di sorpasso e le corsie di marcia, così dovremmo garantire a sistemi e droni differenti, che fanno operazioni differenti, di muoversi in quello spazio aereo

La sfida non è rendere sicuro il singolo drone, ma rendere mission-critical l'infrastruttura di comunicazione che governa il traffico dei droni. Quando migliaia di oggetti autonomi condivideranno lo spazio aereo sopra le infrastrutture critiche, comunicare, identificarsi, essere autorizzati e coordinarsi diventeranno funzioni direttamente connesse alla sicurezza fisica.

5.12. Il sensing distribuito in fibra ottica (DFOS) per il monitoraggio strutturale e perimetrale

Una tecnologia che merita un approfondimento a sé, per la sua applicabilità trasversale a più settori, è il Distributed Fiber Optic Sensing, DFOS già analizzata nel white paper[5] del Centro Stuti COM.TEL. Si tratta di cavi in fibra ottica che, senza bisogno di sensori puntuali alimentati singolarmente, rilevano in continuo, lungo l'intera lunghezza del cavo, vibrazioni, temperature e deformazioni meccaniche, restituendo di fatto un sensore ogni pochi metri per decine o centinaia di chilometri.

Le sue applicazioni intersecano direttamente i capitoli sui casi d'uso di questo documento. Sui ponti e sui viadotti, il DFOS integra il monitoraggio robotico e i digital

[5] "Distributed Fiber Optic Sensing (DFOS): la fibra ottica che ascolta le infrastrutture" https://www.comtelitalia.it/wp-content/uploads/2025/12/Distributed-Fiber-Optics-Sensing_Centro-Studi-Comtel-Innovation.pdf

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

twin, rilevando micro-deformazioni della struttura prima che diventino visibili a un'ispezione tradizionale. Lungo gli acquedotti, la stessa tecnologia individua perdite e variazioni di pressione anomale con una precisione geografica difficile da ottenere con i soli sensori SCADA puntuali. Nel settore energetico, il DFOS è impiegato per la sorveglianza perimetrale di gasdotti e siti industriali sensibili, rilevando scavi non autorizzati o tentativi di manomissione della condotta in tempo reale, un caso d'uso adottato anche a livello internazionale da operatori del comparto oil & gas, lo stesso ambito industriale in cui opera Saipem per il progetto di sicurezza fisica Cepav Due.

Dal punto di vista architetturale, il DFOS condivide con le altre tecnologie la stessa esigenza: il segnale ottico raccolto lungo il cavo deve essere elaborato e trasmesso a una control room attraverso un canale di comunicazione affidabile e, dove la criticità dell'infrastruttura lo richiede, indipendente dalla rete IT/OT dell'impianto sorvegliato, secondo lo stesso principio del doppio binario.

5.13. Smart City: resilienza Urbana, Infrastrutture IoT e Gestione Integrata delle Emergenze

Le infrastrutture di illuminazione pubblica moderna si sono evolute da semplici reti di erogazione a vere e proprie piattaforme capillari per la Smart City che funzionano sostanzialmente sulla base di un sistema di comunicazione. Questo ecosistema urbano distribuito veicola informazioni, sensori e dispositivi tecnologici la cui operatività deve essere garantita non solo in condizioni ordinarie, ma soprattutto durante crisi sistemiche (es. eventi idrogeologici o sismici) che mettono a rischio le dorsali di comunicazione principali.

Per assicurare la tenuta del sistema-città e la continuità di contatto con i centri di comando e controllo (sale operative, sindaci, Protezione Civile), la progettazione della resilienza urbana deve coordinare tre fattori chiave: garantire la comunicazione, garantire l'alimentazione, garantire il dispacciamento e la viabilità per i mezzi che devono intervenire.

Per le comunicazioni le infrastrutture sono ridondate in fibra ottica, un'infrastruttura secondaria in 5G e l'integrazione di sistemi avanzati come i droni o le "bolle tattiche".

Per la resilienza energetica l'alimentazione degli asset critici avviene tramite linee elettriche cittadine primarie supportate da generatori indipendenti e isolati (*best practice* già applicata in grandi eventi internazionali), pronti a intervenire in caso di blackout.

La gestione intelligente della viabilità (Mobilità d'emergenza) consente di utilizzare la rete semaforica smart e la sensoristica di campo per isolare le vie non percorribili, automatizzare la chiusura delle strade e attivare la priorizzazione semaforica per creare corridoi di emergenza dedicati ai mezzi di soccorso e all'evacuazione della popolazione.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

L'efficacia decisionale in scenari complessi richiede l'adozione di sistemi di Intelligenza Artificiale capaci di aggregare flussi di dati eterogenei e talvolta contraddittori dal campo, fornendo ai decisori scenari predittivi e opzioni d'azione rapide.

Tuttavia, la principale barriera all'adozione di queste soluzioni risiede nella frammentazione amministrativa ed economica. In Italia i comuni sono 7.896 e quasi il 70% (69,9%, secondo l'ISTAT[6]) ha meno di 5.000 abitanti: vi risiede il 16,4% della popolazione, ma amministrano, secondo l'ANCI, il 54,9% della superficie nazionale. Per molti di questi enti non esiste un capitolo di spesa integrato che permetta di finanziare in modo coerente comunicazione, alimentazione e sistemi di comando in un'unica progettazione, un vincolo che nessuna tecnologia, da sola, può risolvere.

5.14. Verso le Mission-Critical Unified Communications (MCUC)

Il punto di arrivo di queste tecnologie ha ormai un nome riconosciuto dagli analisti di settore: Mission-Critical Unified Communications, MCUC. Non è un prodotto, ma un'architettura che nasce per risolvere un paradosso della collaborazione moderna: la maggior parte delle implementazioni aziendali di Unified Communications si appoggia oggi su cloud pubblici globali, perfetti per la produttività quotidiana ma poco adatti agli scenari critici, per almeno tre ragioni. Le suite commerciali viaggiano su internet pubblico o su infrastrutture condivise e non possono garantire l'instradamento prioritario dei pacchetti quando la rete è satura in piena crisi; un disservizio del fornitore cloud o un attacco mirato può isolare una control room dalle unità sul territorio; e nei modelli cloud commerciali metadati, registrazioni vocali e coordinate di localizzazione vengono spesso trattati fuori dai confini nazionali ed europei, in tensione con le esigenze di sovranità del dato che la regolazione europea rende sempre più stringenti.

Vale la pena chiarire che la sovranità tecnologica a proposito di MCUC e di localizzazione dei dati, riguarda la capacità di un'organizzazione di mantenere il controllo delle proprie infrastrutture critiche e dei propri dati, non un ripiegamento verso l'autosufficienza a ogni costo. Un'architettura di comunicazione sicura resta, nella grande maggioranza dei casi, il risultato di un ecosistema multi-vendor e internazionale: l'obiettivo è governare le dipendenze critiche con consapevolezza, non eliminarle.

I parametri tecnici di riferimento

Alcuni valori tornano ricorrenti nella progettazione delle reti mission-critical. Il Mission Critical Push-to-Talk, secondo la specifica 3GPP TS 22.179, deve garantire un tempo di accesso al canale e una latenza vocale da bocca a orecchio entrambi inferiori a 300 millisecondi nel 99% dei casi. Le applicazioni di controllo industriale in tempo reale,

[6] ISTAT, Annuario statistico 2025; ANCI, dossier sui piccoli comuni 2026

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

abilitate dallo strato URLLC del 5G, richiedono tipicamente latenze radio inferiori ai 10 millisecondi. Sul piano della cifratura, gli standard più recenti combinano l'algoritmo simmetrico AES-256 con lo scambio di chiavi a curve ellittiche per proteggere voce, video e dati. Il NIST ha già pubblicato gli standard di crittografia post-quantistica ML-KEM (FIPS 203) e ML-DSA (FIPS 204) per la sicurezza con i futuri computer quantistici. Per le infrastrutture critiche è opportuno avviare una valutazione di migrazione, inventariando algoritmi, certificati, dispositivi e protocolli, senza presentare la sostituzione immediata della crittografia esistente come requisito già uniforme per tutti i settori.

Le MCUC affrontano questo nodo con un'architettura spesso descritta come **ibrida cloud-edge**. Le funzioni meno critiche, produttività, collaborazione ordinaria, restano nel cloud centrale, dove beneficiano della scalabilità; le funzioni vitali di comando e controllo vengono invece installate direttamente sul campo o presso le control room locali, in un cosiddetto "**local edge**" che, in caso di interruzione della connessione verso il centro, si isola e continua a garantire comunicazioni radio e coordinamento in modalità autonoma. Per non disperdere gli investimenti già fatti, le piattaforme MCUC includono gateway software che fanno dialogare le reti TETRA e P25 esistenti con i nuovi canali a banda larga, unificando in un'unica interfaccia sale operative che oggi lavorano ancora su sistemi eterogenei.

Un esercizio che le organizzazioni che gestiscono infrastrutture critiche possono utilmente condurre in modo sistematico, e che questo white paper propone come metodo più che come risultato già disponibile, è la ***mappatura delle dipendenze critiche: per ogni servizio essenziale***, da quale rete dipende, da quale fornitore cloud, da quale sistema satellitare, presso quali fornitori si trovano i dati, per quanto tempo il servizio può restare operativo in autonomia, dove si trova il singolo punto di guasto dell'intera catena, e quanto tempo serve per ripristinarlo dopo un'interruzione. Senza questa mappa, anche un'architettura formalmente ridondata può nascondere dipendenze non visibili a un primo esame.

Mappatura delle dipendenze critiche: indicatori di risultato

Un possibile approccio per la mappatura delle dipendenze critiche di ciascuna infrastruttura essenziale, potrebbe essere misurata con due indicatori di risultato: il *tempo di ripristino del servizio* quando opera in condizioni degradate: è il tempo necessario a ripristinare una capacità operativa affidabile in condizioni degradate, non il tempo di ritorno alla normalità, bensì quello occorrente a riprendere le funzioni essenziali mentre l'evento è ancora in corso. Altro aspetto è la *verifica periodica*, non solo progettuale, dell'indipendenza effettiva delle ridondanze dal *point of failure* comune, condotta almeno su quattro dimensioni: alimentazione, vettore fisico, fornitore e gestione delle chiavi

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

crittografiche. La domanda dirimente non è se un'infrastruttura critica subirà un'interruzione, ma se saprà continuare a svolgere la propria funzione essenziale mentre la subisce

Il modello cloud-edge descritto in questo capitolo suggerisce un principio che vale la pena rendere esplicito come criterio di policy, non solo come scelta architetturale: per quanto tempo un'infrastruttura critica deve poter funzionare in piena autonomia quando le reti ordinarie vengono meno? Un ospedale, una rete elettrica, una control room ferroviaria e una struttura di protezione civile non condividono necessariamente la stessa risposta. Questo white paper propone, come contributo alla discussione più che come standard già codificato, un indicatore che chiamiamo ***MAOT, Minimum Autonomous Operating Time***: il numero minimo di ore di capacità operativa autonoma che un'infrastruttura critica è chiamata a garantire in assenza di connettività verso il centro, una soglia che spetta alla regolazione o al procurement, settore per settore, calibrare.

Sul piano della sicurezza, il modello di riferimento non è più il perimetro protetto da firewall e VPN, ma il cosiddetto approccio **Zero Trust**: nessun terminale o utente gode di fiducia automatica solo perché si trova all'interno della rete aziendale, e ogni accesso viene verificato in modo continuo sulla base dell'identità, dello stato del dispositivo e del contesto operativo.

È lo stesso principio che guida l'evoluzione dell'intelligenza artificiale nelle sale operative: si parla sempre più spesso di **Agentic AI**, agenti software capaci di pianificare azioni e supportare in autonomia parte del lavoro di analisi durante una crisi. Perché questo sia compatibile con gli obblighi di supervisione umana e di tracciabilità richiesti dall'AI Act, i modelli devono girare il più possibile in locale, sui server della control room, e ogni raccomandazione generata deve restare tracciata in un registro verificabile.

Anche la **crittografia** guarda già oltre l'orizzonte attuale: gli standard internazionali del NIST spingono verso **algoritmi post-quantistici**, pensati per neutralizzare la minaccia, già oggi concreta, di chi intercetta e archivia traffico cifrato nell'attesa di poterlo decifrare con i futuri computer quantistici ("***harvest now, decrypt later***").

Per le infrastrutture critiche è opportuno avviare fin da ora una valutazione di migrazione, inventariando algoritmi, certificati, dispositivi e protocolli, senza però considerare la sostituzione immediata della crittografia esistente un requisito già uniforme per tutti i settori.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Un benchmark internazionale: FirstNet

Negli Stati Uniti, la rete nazionale a banda larga per la pubblica sicurezza FirstNet, realizzata da AT&T su mandato del FirstNet Authority, è il caso più maturo al mondo di rete mission-critical su scala nazionale. Il programma di investimento decennale avviato nel 2024 vale 8 miliardi di dollari e ha già portato a 1.000 nuovi siti cellulari in 46 Stati, molti in aree rurali, tribali e presso strutture di primo soccorso; nella primavera del 2026 il governo federale e AT&T hanno aggiunto un ulteriore accordo da 2 miliardi di dollari per accelerare il core 5G dedicato. È un termine di paragone utile per l'Europa, che sta muovendo passi analoghi con architetture ibride TETRA più 5G Standalone.

5.15. Il rischio quantum computing

Gran parte delle comunicazioni digitali, incluse quelle mission-critical descritte in questo white paper, si affida a un meccanismo chiamato crittografia a "*chiave asimmetrica*": due soggetti che devono comunicare in modo sicuro si scambiano una chiave segreta attraverso un procedimento matematico che, con i computer tradizionali, richiederebbe tempi talmente lunghi da risultare di fatto inviolabile. È questo il principio alla base della cifratura TLS che protegge la quasi totalità del traffico internet, dei collegamenti satellitari, delle reti private 5G e delle piattaforme UC descritte nei capitoli precedenti.

Per anni, la minaccia rappresentata dal calcolo quantistico a questo sistema è rimasta più un tema di ricerca accademica che un rischio operativo concreto. Un computer quantistico sufficientemente potente sarebbe in grado di risolvere in tempi ragionevoli proprio quel procedimento matematico che oggi rende sicura la cifratura asimmetrica, vanificando la protezione di qualunque comunicazione cifrata con questi metodi. Due fattori hanno reso la minaccia concreta: da un lato i progressi reali, anche se ancora in fase sperimentale, nella potenza di calcolo quantistica disponibile; dall'altro la logica dell'attacco noto come "*harvest now, decrypt later*", già richiamata in questo white paper, per cui un avversario può intercettare e archiviare oggi traffico cifrato con l'intenzione di decifrarlo in futuro, quando computer quantistici adeguati saranno disponibili. Per dati che devono restare riservati per anni, un segreto di Stato, una cartella clinica, un progetto industriale, il rischio è quindi già presente, non rinviabile a quando il computer quantistico sarà maturo.

Il NIST, l'istituto statunitense di standardizzazione, ha pubblicato nell'agosto 2024 i primi tre standard di crittografia post-quantistica, ML-KEM e ML-DSA tra questi, a cui si è aggiunto nel marzo 2025 un quarto algoritmo per lo scambio delle chiavi. Questi standard sono oggi considerati robusti, ma lo stesso processo di standardizzazione lascia aperta una possibilità: non è garantito che restino tali indefinitamente, man mano che la ricerca crittografica e il calcolo quantistico avanzano insieme. Per questo motivo, più che una singola migrazione a un nuovo algoritmo, l'approccio raccomandato è la cosiddetta ***crypto-agilità***, la capacità di un sistema di cambiare algoritmo di cifratura senza dover riprogettare l'intera architettura applicativa.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

L'Unione Europea ha scelto di non lasciare questa transizione alla sola iniziativa dei singoli operatori. Il 20 gennaio 2026 la Commissione ha pubblicato la proposta di direttiva COM(2026) 13, che introduce nella NIS2 un nuovo articolo, il 7, paragrafo 2, lettera k): per la prima volta gli Stati membri saranno tenuti ad adottare, nelle proprie strategie nazionali di cybersicurezza, politiche esplicite per la transizione alla crittografia post-quantistica, non più un obbligo implicito ricavabile per interpretazione. La proposta si innesta su una tabella di marcia già definita dalla Raccomandazione (UE) 2024/1101 e dalla roadmap pubblicata il 23 giugno 2025 dal NIS Cooperation Group, l'organismo tecnico che riunisce le autorità di cybersicurezza nazionali con il supporto di ENISA: tre scadenze progressive, la valutazione del rischio quantistico entro la fine del 2026, il completamento della migrazione dei sistemi più critici entro il 2030, e degli asset restanti entro il 2035.

A conferma della rapidità con cui il tema della crittografia post-quantistica sta uscendo dalla fase puramente teorica, il gruppo TeaTek ha annunciato l'intenzione di dotarsi, in collaborazione con l'Università di Napoli, di un computer quantistico prototipale da 150 qubit, che sarebbe il primo asset quantistico privato italiano messo a disposizione di imprese e ricerca. Si tratta di una macchina ancora a carattere prototipale, ma è un segnale concreto che la transizione verso una crittografia resistente al calcolo quantistico, descritta in questo white paper come priorità di medio periodo, merita di essere pianificata già da ora, non rinviata a quando la capacità di calcolo quantistico sarà pienamente matura.

5.16. Il problema del brownfield: integrare l'esistente

Le tecnologie descritte in questo capitolo vengono spesso presentate come un percorso verso l'architettura futura. Per chi gestisce un'infrastruttura oggi, il problema più immediato è un altro: come integrare 5G, edge computing, cloud e nuovi sistemi di dispatch con impianti esistenti che hanno cicli di vita di decenni, protocolli industriali eterogenei, certificazioni di sicurezza da rinnovare e, spesso, l'impossibilità pratica di essere fermati per una migrazione.

Nei trasporti, nell'energia e nelle utility, dove gli impianti restano in esercizio per trenta o quarant'anni, questo non è un dettaglio implementativo ma probabilmente il vincolo più concreto che si frappone tra l'architettura descritta in questo white paper e la sua adozione reale. Le migrazioni per fasi, i gateway di protocollo che permettono a un sistema legacy di dialogare con l'infrastruttura nuova senza sostituirlo, e la pianificazione di finestre di manutenzione compatibili con la continuità del servizio restano, in questo senso, tanto parte della resilienza quanto la tecnologia più avanzata che le sostituirà.

6. Perché ora la minaccia cambia scala

Le piattaforme di comunicazione non sono più semplici canali di transito: sono archivi dinamici di informazioni sensibili e per questo sono diventate un bersaglio primario. Il

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Cost of a Data Breach Report 2026[7] di IBM, pubblicato a fine luglio, registra un costo medio globale di una violazione di dati pari a 4,99 milioni di dollari, il valore più alto nei ventun anni di storia dello studio, in crescita del 12% sull'anno precedente; il settore sanitario, per il tredicesimo anno consecutivo, resta il più colpito, con un costo medio di 6,6 milioni di dollari per incidente. Una violazione dolosa su quattro, secondo lo stesso rapporto, presenta una componente di intelligenza artificiale nella fase di attacco, e in questi casi il costo medio sale di circa un milione di dollari rispetto alla media.

Con la diffusione dell'intelligenza artificiale sia negli strumenti di attacco sia in quelli di difesa, l'attacco a un'infrastruttura critica tende a smettere di essere un evento isolato per diventare una condizione pressoché continua, in cui sistemi di difesa automatizzati fronteggiano in tempo reale sistemi di attacco altrettanto automatizzati. Il ruolo della supervisione umana resta in questo scenario un presidio e, al tempo stesso, un potenziale punto di fallimento, se non adeguatamente supportato.

Per le comunicazioni mission-critical il rischio non si esaurisce nella perdita di dati: quando un canale di comando viene intercettato o bloccato, l'impatto si trasferisce immediatamente al mondo fisico. Se un flusso video tra un drone e una control room si interrompe durante il coordinamento di un soccorso, o se la telemetria di una sottostazione elettrica viene alterata mentre una squadra sta eseguendo una manovra ad alto rischio, la conseguenza non è un disservizio informatico ma un pericolo diretto per le persone.

È in questo scenario che va letta la portata della direttiva NIS2. In Italia il decreto di recepimento, il D.Lgs. 138/2024, ha ampliato in modo sostanziale la platea dei soggetti vigilati: secondo l'Agenzia per la Cybersicurezza Nazionale, l'elenco dei soggetti NIS individua oltre 20.000 organizzazioni, di cui più di 5.000 classificate come soggetti essenziali; a livello europeo, la Commissione stima che la platea complessiva dei soggetti coperti dalla direttiva superi le 160.000 entità in circa 18 settori essenziali e importanti. Per i soggetti essenziali la norma prevede, tra l'altro, l'obbligo di dotarsi di canali di comunicazione di emergenza alternativi e protetti, capaci di restare operativi anche quando la rete aziendale primaria è compromessa, e introduce una responsabilità diretta, anche personale, degli organi di vertice nella vigilanza sulle misure di cybersicurezza;

Per i soggetti essenziali, la direttiva prevede sanzioni amministrative pecuniarie massime non inferiori a 10 milioni di euro o al 2% del fatturato mondiale annuo, se superiore; per i soggetti importanti, non inferiori a 7 milioni di euro o all'1,4% del fatturato mondiale annuo, se superiore. L'applicazione concreta è disciplinata dagli ordinamenti nazionali e deve rispettare proporzionalità e garanzie procedurali.

Alla domanda su quanto costi rendere resiliente un'infrastruttura di comunicazione andrebbe affiancata quella simmetrica, spesso più efficace nel dialogo con chi decide

[7] https://www.ibm.com/it-it/reports/data-breach

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

gli investimenti: quanto costa non renderla resiliente? Un framework concettuale, che richiederebbe per ogni settore un lavoro di quantificazione ulteriore rispetto a quanto questo white paper può offrire, aiuta a impostare la domanda: il *costo della resilienza andrebbe confrontato con la perdita attesa da un'interruzione*, moltiplicata per la probabilità dell'evento, a cui sommare i costi sistemici indiretti che si propagano ad altri settori dipendenti. Ragionare in questi termini permette di rivolgersi a chi decide il budget, non solo a chi gestisce la rete.

Il ritorno economico della digitalizzazione

Uno studio recente realizzato del Centro Studi TIM[8] - in collaborazione con Intesa Sanpaolo Innovation Center, Osservatori 5G & Connected Digital Industry e Internet of Things del Politecnico di Milano e al Centro Studi COM.TEL., stima per la prima volta i benefici economici della digitalizzazione delle infrastrutture civili italiane. Il patrimonio da gestire è imponente: 240.000 chilometri di strade, circa 60.000 ponti e oltre 2.200 gallerie, affidati a più di 8.000 soggetti diversi, una frammentazione che rende la raccolta e la gestione integrata dei dati una priorità prima ancora che un'opzione. Sulle infrastrutture civili, lo studio stima che una gestione predittiva basata su dati digitali possa ridurre del 27% la probabilità di crolli infrastrutturali e del 31% i costi di manutenzione, con un risparmio cumulato stimato in circa 50 miliardi di euro entro il 2030. Sulla distribuzione elettrica, i benefici stimati includono un risparmio di circa 3,13 TWh l'anno in perdite di rete, pari a oltre 330 milioni di euro, più ulteriori 188 milioni di euro l'anno dalla gestione ottimizzata dei picchi di domanda. Sulle reti idriche, dove le perdite distribuite raggiungono oggi il 42% a fronte del 17% di contatori digitalizzati, lo studio stima un potenziale di riduzione dei costi cumulati di 10 miliardi di euro in quattro anni.

Non significa spendere meno: significa, secondo lo studio, spendere meglio, indirizzando la manutenzione dove serve realmente invece di procedere per cicli uniformi. È un argomento che vale la pena tenere a mente insieme ai capitoli su governance e procurement di questo white paper: la resilienza delle comunicazioni critiche non è solo un costo di conformità, è anche la condizione abilitante per ottenere questi risparmi.

7. Il rapporto ENISA NIS360: la mappa del rischio cyber in Europa

ENISA, l'Agenzia dell'Unione Europea per la Cybersicurezza, pubblica ogni anno il NIS360, uno strumento di valutazione comparativa pensato per autorità nazionali, responsabili politici e operatori dei settori disciplinati dalla direttiva NIS2. Il rapporto non si limita a fotografare lo stato della sicurezza informatica. misura, per ciascuno degli undici settori ad alta criticità individuati nell'Allegato I della NIS2, energia,

[8] Centro Studi TIM – Smart Infrastructure. Le infrastrutture italiane tra sfide e innovazione. 2025

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

trasporti, sanità, acqua, infrastrutture digitali, pubblica amministrazione, spazio e gli altri, due grandezze distinte, la *criticità* del settore per la società e l'economia, e la sua *maturità* nella gestione del rischio cyber, per poi incrociarle in un'unica mappa.

Dimensione	Cosa misura	Perché è rilevante
Maturità	Capacità del settore di prevenire, gestire e recuperare dagli incidenti cyber	Indica quanto il settore è preparato
Criticità	Dipendenza digitale, impatto socioeconomico e rapidità di propagazione di un'interruzione	Indica quanto il settore è importante per società ed economia

La terza edizione del rapporto ENISA NIS360 2026[9], pubblicata il 28 maggio 2026, misura la maturità di un settore osservando quattro dimensioni congiunte: l'efficacia della normativa applicabile, il livello di preparazione delle aziende, la capacità istituzionale delle autorità di vigilanza e la solidità delle strutture dell'ecosistema settoriale. La criticità viene invece valutata sulla base del livello di digitalizzazione del settore, dell'impatto socio-economico di un eventuale incidente e della cosiddetta criticità temporale, cioè la rapidità con cui gli effetti di un'interruzione si propagano al resto dell'economia attraverso le interconnessioni tra settori. Poiché questi fattori evolvono lentamente, i punteggi di criticità restano relativamente stabili di anno in anno, mentre la maturità, che dipende da scelte organizzative e investimenti, può cambiare più rapidamente.

ENISA non sostituisce le autorità nazionali e non svolge un audit sulle singole imprese. I suoi rapporti forniscono analisi, metodologie e orientamenti utili a policy maker, autorità, operatori, università e fornitori. Le conclusioni del NIS360 devono quindi essere interpretate come una valutazione settoriale europea, non come un giudizio automatico su ogni organizzazione.

Il rapporto 2026 NIS360

Il rapporto 2026 NIS360 evidenzia un miglioramento generale della maturità cyber dei settori critici dell'Unione, mentre la criticità resta relativamente stabile. I progressi sono associati all'evoluzione normativa, alla crescente attenzione politica, agli investimenti, alla collaborazione tra operatori e al rafforzamento delle capacità di gestione del rischio. Il miglioramento non è tuttavia uniforme. Persistono differenze tra settori e tra organizzazioni dello stesso settore, dovute a dimensioni, risorse, disponibilità di competenze, sistemi legacy, caratteristiche tecniche delle infrastrutture e capacità delle autorità di supervisione.

[9] https://www.enisa.europa.eu/news/nis360-the-bigger-picture-on-maturity-and-criticality-of-nis-critical-sectors

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

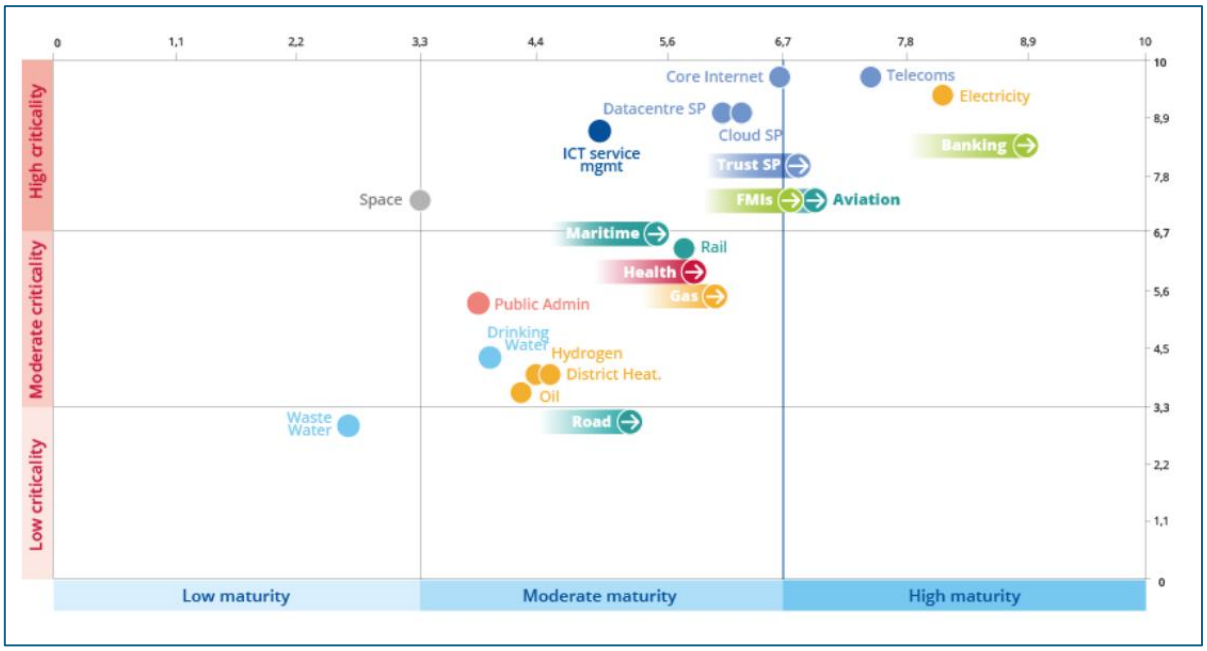


Figura 1: NIS360 miglioramenti della maturità dei settori in un anno

Settore bancario, elettrico e delle telecomunicazioni restano, secondo ENISA, i più maturi e insieme i più critici del panorama europeo. Tre settori sono saliti quest'anno nella fascia di maturità elevata per la prima volta: i servizi fiduciari, l'aviazione e le infrastrutture dei mercati finanziari, queste ultime spinte in modo sostanziale dall'attuazione del regolamento DORA. Altri quattro settori hanno rafforzato la propria posizione all'interno della fascia di maturità moderata: gas, trasporto stradale, trasporto marittimo e sanità.



Figura 2: NIS360 variazione della criticità dei settori rispetto al 2025

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

La zona di rischio: i settori più esposti nel 2026

L'elemento più utile del NIS360, ai fini pratici, è la cosiddetta “zona di rischio”: l'area in cui rientrano i settori la cui criticità supera la maturità con cui gestiscono il rischio cyber, cioè i settori più importanti per la società e insieme meno preparati a difendersi.

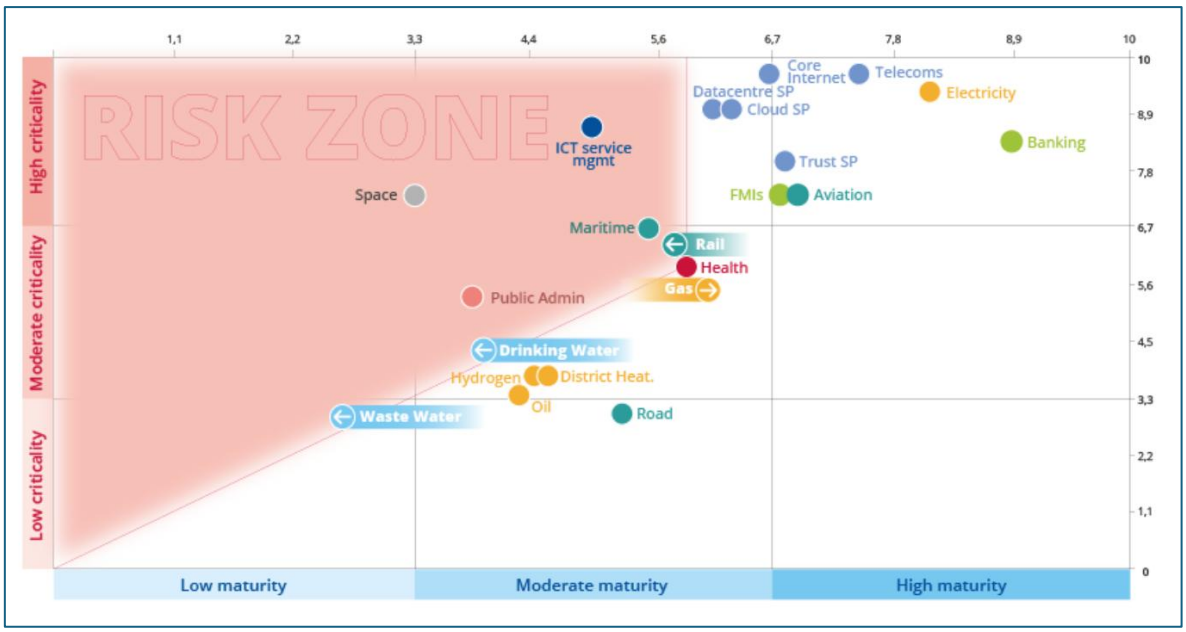


Figura 3: NIS 360: La zona di rischio

Nell’edizione 2026 il NIS360 colloca nella zona di rischio otto settori:

- sanità;
- trasporto ferroviario;
- trasporto marittimo;
- servizi di gestione ICT;
- spazio;
- pubbliche amministrazioni;
- acqua potabile;
- acque reflue.

Tre di questi settori, ferrovie, acqua potabile e acque reflue, sono un caso particolarmente istruttivo: si trovavano l'anno scorso al limite della zona di rischio e vi sono ora pienamente rientrati non perché la loro sicurezza sia peggiorata in assoluto, ma perché altri settori hanno alzato l'asticella della maturità media, spostando così la soglia di riferimento. Un segnale in controtendenza, positivo, riguarda invece il settore del gas, che ha iniziato a uscire dalla zona di rischio grazie a una migliore condivisione delle informazioni tra operatori e a un'attuazione più efficace delle misure di gestione del rischio richieste dalla normativa.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Sanità

La sanità combina elevata dipendenza digitale, forte impatto sociale, dispositivi connessi, sistemi legacy e numerose terze parti. Per le comunicazioni critiche questo significa integrare voce, messaggistica, teleconsulto, allarmi clinici, emergenza, registrazione e coordinamento con protezione civile e sicurezza pubblica.

La priorità è garantire segmentazione, controllo degli accessi, continuità locale e operatività anche quando una parte dell'infrastruttura non è disponibile.

Trasporto ferroviario

Il ferroviario integra sistemi di segnalamento, telecomunicazioni, controllo del traffico, stazioni, manutenzione e servizi ai passeggeri. L'interazione tra IT, OT e sistemi con lunga vita utile rende complessi gli aggiornamenti e la gestione delle vulnerabilità.

ENISA ha rivisto verso l'alto la criticità del settore anche per il ruolo crescente del trasporto ferroviario nella logistica militare e per l'esposizione alle minacce. La comunicazione sicura deve collegare esercizio, manutenzione, sicurezza, emergenza, autorità e infrastruttura.

Trasporto marittimo

Porti, terminal, autorità portuali, navi, compagnie e operatori logistici costituiscono un ecosistema distribuito e interdipendente. La continuità richiede coordinamento tra sala operativa portuale, navi, servizi di emergenza e operatori, con reti terrestri, mobili, costiere e satellitari.

Servizi di gestione ICT

I fornitori ICT e managed services possono diventare punti di propagazione del rischio perché supportano contemporaneamente numerose organizzazioni. La valutazione deve includere cloud, servizi gestiti, sicurezza, autenticazione, certificati, aggiornamenti, subfornitori e piattaforme di comunicazione o dispatch.

Spazio

Il settore spaziale sostiene telecomunicazioni, navigazione, osservazione della Terra, sincronizzazione, sicurezza e difesa. Il suo ruolo crescente aumenta la criticità e le dipendenze da software, reti terrestri, cloud e fornitori specializzati. Il satellite può essere quindi considerato come un livello di resilienza integrato con reti terrestri, radio e mobile, non come sostituto automatico di tutte le altre infrastrutture.

Pubbliche amministrazioni

Le amministrazioni centrali, regionali e locali presentano livelli diversi di risorse, competenze e capacità tecnica. La sicurezza delle comunicazioni di emergenza non può dipendere solo dal singolo ente: sono necessari servizi condivisi, modelli comuni,

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

formazione, accordi interistituzionali e procedure per crisi che superano i confini amministrativi.

Acqua potabile e acque reflue

I due settori comprendono impianti distribuiti, sensori, telecontrollo, automazione e fornitori specializzati. Sistemi legacy, risorse limitate e condivisione delle informazioni non uniforme aumentano il rischio.

L'integrazione tra SCADA e comunicazioni critiche deve consentire di trasformare un allarme in un processo operativo: rilevazione, validazione, classificazione, assegnazione della squadra, comunicazione prioritaria, aggiornamento, chiusura e registrazione dell'evento.

I settori più critici

Sul fronte della criticità, il dato più significativo del 2026 riguarda l'ingresso dello ***spazio*** nel gruppo dei settori più critici in assoluto, insieme a ***settore bancario, elettrico, aviazione e infrastrutture digitali "digital-by-default" come telecomunicazioni, cloud e data center.*** La ragione, spiega ENISA, è la crescente dipendenza di quasi tutti gli altri comparti dai servizi satellitari per posizionamento, navigazione, sincronizzazione temporale e osservazione della Terra. Anche il settore ferroviario ha visto crescere il proprio punteggio di criticità, per il suo ruolo sempre più rilevante nella logistica militare e per la maggiore esposizione a minacce informatiche che questo comporta.

Le dinamiche da monitorare

ENISA individua tre fattori trasversali destinati a influenzare la sicurezza dei settori critici:

- **intelligenza artificiale**: aumenta capacità di analisi e automazione, ma può rendere più efficaci phishing, social engineering, deepfake e attacchi;
- **supply chain**: vulnerabilità di software, hardware, servizi gestiti, aggiornamenti e subfornitori possono propagarsi a più organizzazioni;
- **geopolitica**: tensioni internazionali, sanzioni, dipendenze tecnologiche e disponibilità di ricambi o supporto possono incidere sulla continuità.

Per i sistemi mission-critical ciò richiede supervisione umana, tracciabilità, test, fallback, controllo della filiera, portabilità dei dati, gestione delle chiavi e capacità di operare localmente.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

La voce di ENISA

"I risultati di questo rapporto NIS360 offrono motivi di ottimismo. L'attuazione del quadro normativo completo dell'UE in materia di sicurezza informatica, e in particolare della direttiva NIS2, ha portato a miglioramenti significativi." Juhan Lepassaar, Direttore esecutivo di ENISA.

Perché conta per le comunicazioni mission-critical

Il rapporto NIS360 è la valutazione dell'agenzia tecnica dell'Unione Europea competente in materia di cybersecurity. Per chi si occupa di comunicazioni sicure e mission-critical, il messaggio è diretto: quattro degli otto settori nella zona di rischio, *sanità, ferrovie, acqua (potabile e reflua) e pubblica amministrazione*, coincidono con gli ambiti applicativi al centro di questo white paper. E' la conferma di un pattern strutturale: i settori che dipendono maggiormente da reti di comunicazione critiche e da sistemi di comando e controllo affidabili sono, secondo l'osservatorio europeo, anche quelli che devono investire con più urgenza per colmare il divario tra l'importanza sociale del servizio che erogano e la loro effettiva capacità di difenderlo.

Il rapporto NIS360 fa emergere un altro aspetto non tecnico della sicurezza: la classificazione dei settori più critici, e la crescente attenzione riservata a *spazio, energia e telecomunicazioni*, riflette anche una ***lettura geopolitica del rischio***. In un contesto di crescente competizione e conflittualità ibrida, la capacità di un Paese di mantenere operative le proprie comunicazioni critiche anche sotto attacco è essa stessa una forma di *deterrenza*: un'infrastruttura che si dimostra resiliente scoraggia un tentativo di destabilizzazione. Questa lettura, tuttavia, regge solo se la resilienza dichiarata è verificata nei fatti, non presunta sulla carta, il tema affrontato ***sull'indipendenza effettiva delle ridondanze***.

8. Un mercato in crescita strutturale

Il mercato delle comunicazioni critiche sta entrando in una fase di crescita sostenuta, man mano che governi, agenzie di pubblica sicurezza, aziende di servizi pubblici, operatori dei trasporti, organizzazioni della difesa e imprese modernizzano le proprie infrastrutture di comunicazione per garantire connettività sicura, affidabile e sempre disponibile.

Quanto vale, oggi, il mercato delle comunicazioni critiche? Le principali società di ricerca convergono su un ordine di grandezza, tra i 20 e i 25 miliardi di dollari a livello globale nella seconda metà degli anni Venti, ma le stime puntuali variano a seconda che includano con combinazioni differenti hardware, apparati radio, infrastrutture,

servizi broadband, software MCX, piattaforme di comando e controllo e servizi professionali.

Tabella 1 – Il mercato delle Comunicazioni Critiche

Fonte	Valore 2025 (Mld $)	Valore 2030-35 (Mld $)	CAGR (%)
MarketsandMarkets[10]	19,8	40,2 (2035)	7,3
Mordor Intelligence[11]	20,16	28,02 (2030)	6,81
The Business Research Company[12]	20,91	34,06 (2030)	10,1
Researchandmarkets[13]	17,97 (2026)	29,33 (2032)	8,42

Nota: le differenze fra le stime dipendono principalmente dal perimetro considerato (solo infrastruttura radio, inclusione o meno di servizi professionali, hardware o software)

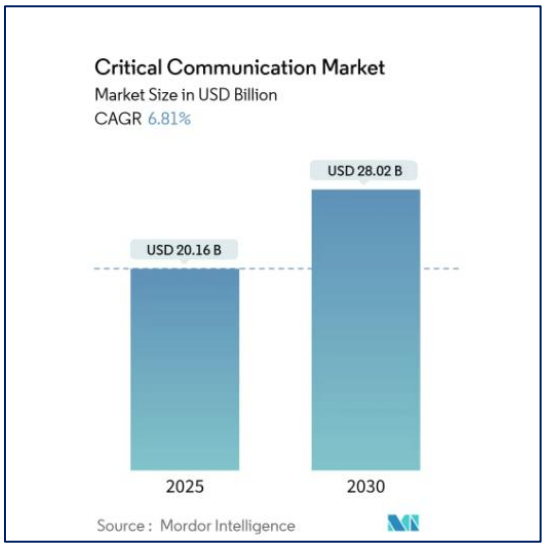


Figura 4: Il mercato delle Comunicazioni Critiche (Mordor Intelligence)

[10] https://www.marketsandmarkets.com/Market-Reports/critical-communication-market-95862445.html
[11] https://www.mordorintelligence.com/industry-reports/critical-communication-market
[12] https://www.thebusinessresearchcompany.com/report/mission-critical-communication-global-market-report
[13] https://www.researchandmarkets.com/report/critical-communication

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

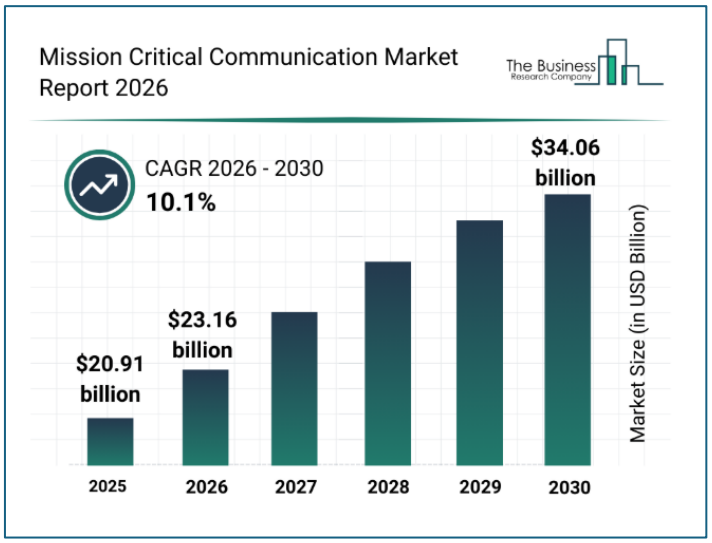


Figura 5: Il mercato delle Comunicazioni Mission-Critical (The Business Research Company)

Le differenze tra le stime dipendono principalmente dal perimetro considerato, solo infrastruttura radio oppure anche servizi professionali, hardware o software. Al di là delle differenze metodologiche, il quadro è coerente: è un mercato in crescita strutturale, non ciclica, sostenuto da digitalizzazione, regolazione europea sempre più stringente sul fronte della resilienza, rischio operativo crescente legato alla cybersecurity, necessità di sostituire infrastrutture legacy e diffusione di 5G e IoT industriale di tipo mission-critical (IIoT). L'intelligenza artificiale, l'edge computing e la risposta automatizzata agli incidenti stanno ulteriormente trasformando i sistemi di comunicazione critica, che da reti tradizionalmente incentrate sulla voce si stanno evolvendo in ecosistemi operativi intelligenti e basati sui dati.

9. La lettura per area geografica

Il **Nord America** resta il mercato più ampio per le comunicazioni mission-critical: secondo Mordor Intelligence deteneva il 34,93% del valore globale nel 2024, sostenuto da investimenti in sicurezza pubblica, servizi di emergenza e difesa, da infrastrutture di telecomunicazione avanzate e dall'adozione precoce di reti LTE e 5G private; tra i fornitori con base statunitense più rilevanti figurano Motorola Solutions e L3Harris Technologies. **L'Asia-Pacifico** è l'area a crescita più rapida, al 7,47% annuo secondo la stessa fonte, trainata dall'urbanizzazione, dallo sviluppo di smart city e dagli investimenti in sicurezza pubblica di **Cina, Giappone, India e Corea del Sud**; Hytera Communications è tra i produttori più attivi nella regione.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

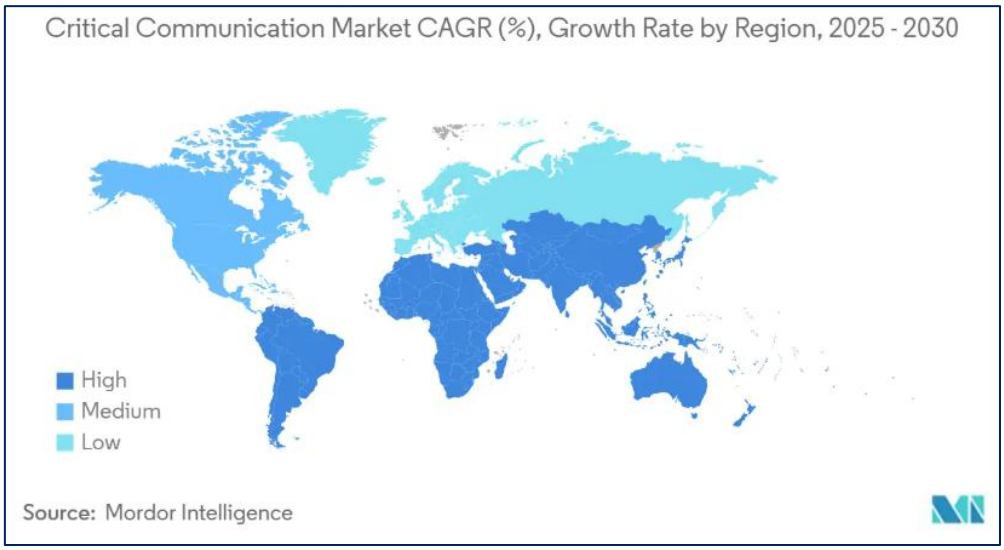


Figura 6: La crescita delle comunicazioni critiche nel mondo (Mordor Intelligence)

L'Europa rappresenta circa un quarto del mercato mondiale e ha una caratteristica che la distingue dalle altre aree geografiche: qui la spinta agli investimenti non arriva solo dalla domanda operativa, ma anche dall'obbligo normativo, NIS2, CER, AI Act, DORA. Grande attenzione è rivolta alla residenza dei dati, alla sovranità digitale e alla gestione del rischio cyber lungo la supply chain. Numerosi Paesi stanno modernizzando le proprie reti TETRA nazionali evolvendole verso architetture ibride con 5G Standalone e network slicing per i servizi di emergenza, i trasporti e le utility, spesso attraverso partnership pubblico-private; tra i Paesi più attivi figurano Regno Unito, Germania e Francia, dove operano fornitori come Thales Group ed Ericsson.

Per **l'Italia** non esiste ancora una cifra unica e consolidata dedicata al solo comparto delle comunicazioni critiche, ma gli indicatori disponibili delineano un quadro coerente con la tendenza europea. Il mercato ICT complessivo supera gli 85 miliardi di euro, con la componente cloud sopra gli 8 miliardi e una crescita a doppia cifra che segnala una domanda forte di servizi gestiti e infrastrutture as-a-service. I programmi legati al PNRR e i piani nazionali su sanità territoriale, cybersecurity e mobilità stanno finanziando interventi su control room, reti di emergenza, sistemi di sorveglianza e telecontrollo; trasporto ferroviario e metropolitano, gestori aeroportuali, operatori energetici e idrici, infrastrutture stradali e portuali hanno avviato gare e progetti per modernizzare le proprie comunicazioni. In quest'ambito accanto ai grandi gruppi internazionali Leonardo ha un ruolo rilevante in Italia e mercati internazionali.

In questo scenario, operatori con base italiana ed europea con competenze consolidate in ambito UC, voce-dati e OT, e con una presenza già radicata nei settori regolamentati, possono giocare un ruolo di orchestratori di soluzioni multi-vendor.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Come si scompone il mercato

Una fotografia più granulare viene da Mordor Intelligence, che colloca il mercato globale a 20,16 miliardi di dollari nel 2025, con una crescita prevista fino a 28,02 miliardi entro il 2030. Per ***tecnologia***, la radio professionale tradizionale, LMR, deteneva ancora il 57,46% del valore nel 2024, mentre i servizi 5G MCX crescono all'8,12% annuo, il segmento più dinamico. Per ***componente***, l'hardware infrastrutturale vale ancora il 44,78% della spesa, ma sono i servizi gestiti e di integrazione a crescere più rapidamente, al 7,36% annuo, segno che le organizzazioni preferiscono sempre più esternalizzare la gestione della rete per garantirsi contrattualmente il livello di disponibilità richiesto. Per ***modello di implementazione***, le reti dedicate private restano maggioritarie, 48,73% del mercato nel 2024, ma sono le architetture ibride a crescere più in fretta, al 7,95% annuo. Per ***settore di utilizzo finale***, la pubblica sicurezza resta l'ambito dominante con il 62,42% del mercato, ma è il comparto energia e utility a mostrare il tasso di crescita più alto, il 7,87% annuo, spinto dall'esigenza di reti a bassissima latenza per la protezione delle reti elettriche intelligenti; la sanità, pur restando un segmento più contenuto in valore assoluto, è quella che secondo gli analisti di settore mostra la crescita percentuale più rapida in prospettiva, sostenuta dai progressi della telemedicina e dall'esigenza di un'assistenza coordinata al paziente.

10. I driver e gli ostacoli del settore

Mordor Intelligence isola alcuni fattori più puntuali che stanno accelerando o frenando la crescita.

Sul fronte dei **driver**, pesano soprattutto le applicazioni di intelligenza artificiale distribuite sull'edge per la “consapevolezza situazionale”, che analizzano flussi video e dati dei sensori direttamente sui siti radio prima di inviarli alla rete centrale, dimezzando latenza e traffico; gli investimenti nazionali per reti LTE/5G dedicate alla sicurezza pubblica; l'obbligo di disponibilità del 99,999% imposto dai regolatori, che spinge verso core ridondati e infrastrutture mobili sul campo; le slice 5G private per irrobustire la cybersecurity delle infrastrutture critiche e la modernizzazione delle comunicazioni marittime di soccorso verso LTE/5G non terrestre.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Tabella 2 - Driver di sviluppo[14]

Driver	Impatto sul CAGR	Rilevanza geografica	Timing
Realizzazione di reti LTE/5G a copertura nazionale per la sicurezza pubblica	+1,2%	Nord America, Europa, Asia Pacifico	Medio termine (2-4 anni)
Migrazione digitale dai sistemi LMR tradizionali a P25/TETRA	+0,8%	Globale, concentrazione in Nord America e Europa	Lungo termine (≥ 4 anni)
Requisito di disponibilità del 99,999% per la rete PSBN (Public Safety Broadband Network)	+1,1%	Nord America, ricaduta in Europa	Breve termine (≤ 2 anni)
Applicazioni di Edge AI per la consapevolezza situazionale per l'adozione di MCX	+1,4%	Globale, adozione precoce in Nord America e Asia-Pacifico	Medio termine (2-4 anni)
Slice 5G private per il rafforzamento della cybersecurity delle infrastrutture critiche	+0,9%	Asia Pacifico, Nord America, Europa	Medio termine (2-4 anni)
Modernizzazione delle Global maritime GMDSS verso LTE/5G NTN	+0,7%	Globale, con enfasi nelle regioni marittime	Lungo termine (≥ 4 anni)

Fonte: Mordor Intelligence

Tabella 3 – Ostacoli per lo sviluppo[15]

Ostacoli	Impatto sul CAGR	Rilevanza geografica	Timing
Scarsità di spettro al di sotto di 1 GHz	-0,6%	Globale, acuto in Nord America ed Europa	Lungo termine (≥ 4 anni)
Elevati investimenti (CAPEX) per l'aggiornamento della rete trunked a copertura nazionale	-0,4%	Globale, con particolare impatto sui mercati emergenti	Medio termine (2-4 anni)
Ritardi nella certificazione di chipset compatibili con MCX	-0,3%	Globale, con variazioni normative a seconda della regione	Breve termine (≤ 2 anni)
Garanzie di QoS limitate sulle reti commerciali 5G SA	-0,2%	Globale, regioni interessate dalla fase iniziale di implementazione del 5G	Medio termine (2-4 anni)

Fonte: Mordor Intelligence

[14] https://www.mordorintelligence.com/industry-reports/critical-communication-market
[15] https://www.mordorintelligence.com/industry-reports/critical-communication-market

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Sul fronte degli **ostacoli**, il più rilevante resta la scarsità di spettro sotto 1 GHz, la porzione di frequenze più efficiente per la copertura ad ampio raggio, conteso tra pubblica sicurezza, broadcasting e operatori commerciali: la strategia nazionale sullo spettro degli Stati Uniti ha riconosciuto apertamente che le assegnazioni attuali non possono sostenere insieme le vecchie reti radio e le nuove esigenze a banda larga, e l'Europa affronta una congestione analoga. Pesano inoltre gli elevati investimenti necessari per rinnovare le reti trunked nazionali, un arretrato nelle certificazioni multi-vendor per i chipset compatibili con lo standard MCX, e le garanzie di qualità del servizio ancora limitate sulle reti 5G Standalone commerciali, non dedicate.

11. L'Agentic AI nelle comunicazioni critiche

Se il 5G Standalone e il satellite sono le infrastrutture che rendono possibile la connettività ovunque e in ogni condizione, il terzo motore che sta accelerando la trasformazione del comparto è l'Agentic Artificial Intelligence, agenti software capaci non solo di analizzare dati ma di pianificare ed eseguire azioni in autonomia.

Nelle comunicazioni critiche l'Intelligenza Artificiale viene introdotta come strumento di supporto all'operatore, con limiti di autonomia definiti, supervisione umana, logging, gestione degli errori e possibilità di funzionamento degradato. Il valore non consiste nell'automatizzare ogni decisione, ma nel ridurre i tempi di analisi e migliorare la qualità delle informazioni disponibili alla control room.

Secondo le previsioni tecnologiche 2026 di **Deloitte**[16], il mercato globale dell'Agentic AI potrebbe raggiungere tra i 35 e i 45 miliardi di dollari entro il 2030, partendo da una base stimata di circa 8,5 miliardi nel 2026; per il solo comparto delle telecomunicazioni, altre stime di settore indicano una crescita da 3,75 miliardi di dollari a quasi 12 miliardi entro il 2030. Il segnale è chiaro: dopo una fase di sperimentazione con assistenti generativi, le organizzazioni stanno iniziando a distribuire agenti autonomi lungo l'intera infrastruttura, dalle reti alla sicurezza, dall'identità digitale ai processi operativi.

Non mancano, tuttavia, segnali di cautela. Il sondaggio 2026 di **McKinsey**[17] sulla fiducia nell'intelligenza artificiale registra un punteggio medio di maturità nella gestione responsabile dell'AI salito a 2,3 nel 2026, da 2,0 nel 2025, ma rileva che solo un terzo delle organizzazioni raggiunge un livello di maturità pari o superiore a tre proprio sul fronte della governance degli agenti, la dimensione più recente e meno matura tra quelle misurate. I settori delle tecnologie, media e telecomunicazioni risultano tra i più avanzati, insieme ai servizi finanziari.

[16] https://www.deloitte.com/it/it/Industries/tmt/perspectives/tmt-predictions-2026.html
[17] https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Deloitte arriva a una conclusione simile nel suo report 2026[18] sullo stato dell'AI in azienda, condotto su oltre 3.200 dirigenti in 24 Paesi: quasi tre aziende su quattro prevedono di utilizzare agenti AI entro il 2027, ma soltanto il 21% dichiara di avere già un modello di governance maturo per gestirli. Per un comparto come quello delle comunicazioni mission-critical, dove un errore dell'algoritmo può tradursi in un rischio fisico immediato, questo scarto tra velocità di adozione e maturità della governance è precisamente il punto su cui si concentra la vigilanza dei regolatori europei, come si vedrà nel capitolo dedicato al perimetro normativo.

Sul fronte industriale, i grandi fornitori di infrastrutture di rete si stanno muovendo di conseguenza. **Cisco** ha presentato nel giugno 2026 **Cisco Cloud Control**[19], una piattaforma unificata pensata per far lavorare insieme operatori umani e agenti AI nella gestione e difesa delle infrastrutture IT critiche, fondamento del modello che l'azienda chiama **AgenticOps**; Cisco stima che gli agenti AI generino fino a 25 volte più traffico di rete rispetto a un semplice chatbot, un dato che aiuta a spiegare perché la capacità di rete e la sicurezza dei protocolli di comunicazione siano tornate al centro degli investimenti. Nello stesso annuncio, Cisco si è impegnata a rendere le comunicazioni sicure rispetto al rischio quantistico sulla maggior parte del proprio portafoglio entro dicembre 2026, richiamando esplicitamente la minaccia “harvest now, decrypt later”. **Ericsson**, dal canto suo, sta sviluppando applicazioni “agentic” per il rilevamento autonomo di anomalie in tempo reale sulle reti di accesso radio, un passo concreto verso reti mobili “auto-riparanti” capaci di individuare e correggere problemi tecnici senza un intervento umano diretto, un'evoluzione che riguarda da vicino anche le reti dedicate ai servizi mission-critical descritte in questo lavoro.

Questo scarto tra velocità di adozione e maturità della governance non è solo un problema interno alle organizzazioni: nel settembre 2026 lo scontro pubblico tra alcuni tra i principali laboratori di intelligenza artificiale, tra chi propone un rallentamento coordinato dello sviluppo e chi ritiene sufficiente la responsabilità individuale di ciascun attore, mostra come il settore stesso non abbia ancora trovato un equilibrio condiviso sul tema. Per le comunicazioni mission-critical, dove un errore dell'algoritmo ha conseguenze fisiche immediate, questa incertezza a monte rende ancora più necessario l'approccio "compliant by design".

Proprio perché si parla di comunicazioni mission-critical, vale la pena rendere più netta una distinzione che finora resta implicita: quali decisioni possono essere affidate all'intelligenza artificiale, e quali devono restare necessariamente umane? Una classificazione utile distingue tre livelli. Nel primo, ***AI advisory***, l'algoritmo analizza

[18] https://www.deloitte.com/it/it/about/press-room/state-of-ai-2026.html
[19] https://news-blogs.cisco.com/emea/it/2026/06/19/cisco-presenta-la-piattaforma-agentica-per-gestire-e-proteggere-le-infrastrutture-it-critiche/

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

segnali e dati senza intervenire sulle decisioni. Nel secondo, ***AI supervised***, il sistema può proporre una priorità operativa, ma l'azione resta condizionata alla conferma di un operatore umano. Nel terzo, ***human-only decision***, le scelte con conseguenze dirette sulla sicurezza delle persone restano di responsabilità umana esplicita e non delegabile. Questa classificazione, più che un vincolo tecnico, è una scelta di governance che ogni organizzazione si trova, prima o poi, a dover affrontare quando distribuisce agenti autonomi nelle proprie control room.

Un rischio complementare a quelli già descritti riguarda lo ***shadow AI***: l'uso, da parte del personale, di strumenti di intelligenza artificiale non censiti né controllati dall'organizzazione, spesso in buona fede e senza consapevolezza del rischio introdotto. Applicato alle comunicazioni vocali e ai Session Border Controller descritti nel white paper, questo significa che un dipendente può esporre inconsapevolmente conversazioni o dati sensibili a un servizio di intelligenza artificiale esterno, non verificato, semplicemente utilizzandolo come supporto al proprio lavoro quotidiano. È un rischio che si aggiunge, più che sostituire, quelli già descritti a proposito della governance degli agenti AI, e che richiede politiche esplicite di censimento degli strumenti di intelligenza artificiale in uso, non solo di quelli formalmente adottati dall'organizzazione.

Restano aperte, in questo schema, due domande operative altrettanto rilevanti*: come si gestisce una raccomandazione dell'agente che si rivela errata*, e che *cosa succede quando l'intelligenza artificiale non è disponibile*. Nel primo caso, la responsabilità della decisione finale resta di chi la conferma, non dell'algoritmo che la propone, motivo per cui il *registro di audit* diventa essenziale anche per l'apprendimento organizzativo, non solo per la conformità normativa. Nel secondo caso, ogni control room dovrebbe poter tornare a una modalità operativa interamente manuale senza che questo comporti l'interruzione del servizio: un'AI che diventa un punto di fallimento unico, anziché un supporto rimovibile, ha invertito la logica con cui dovrebbe essere stata progettata fin dall'inizio.

L'Agentic AI solleva un altro punto critico: oggi gran parte del traffico internet — più del 50% del traffico — non è generato da umani. Alcune valutazioni indicano che sciami di agenti potrebbero compiere il *takeover* di internet nel giro di 48 ore. A livello internazionale presso **l'Internet Engineering Task Force (IETF)** sono in corso discussioni, tra coalizioni diverse di attori industriali per la standardizzazione dell'identità digitale degli agenti di intelligenza artificiale, un livello infrastrutturale di base da cui dipenderanno fiducia e tracciabilità di questi sistemi su scala globale. Tra tutte la coalizione guidata da ICANN (Internet Corporation for Assigned Names and Numbers) e Identity Digital, vorrebbe diventare l'*anchor trust* sul DNS. Altre coalizioni

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

tentano di eleggere le piattaforme stesse, AWS e OpenAI. Huawei sta provando a introdurre altre alternative.

È un tema che travalica il perimetro delle comunicazioni mission-critical trattate, ma che vale la pena segnalare come ambito in cui la partecipazione di soggetti europei e italiani alla standardizzazione tecnica, non solo alla regolazione a valle, può incidere per ottenere risultati significativi.

Infine, con la diffusione dell'Agent AI, in grado di operare con privilegi sempre più ampi e autonomia decisionale, i tradizionali paradigmi di sicurezza puramente software non sono più sufficienti. Diventerà decisivo ancorare all'hardware la sicurezza. Questo passaggio è indispensabile per proteggere l'infrastruttura da una nuova classe di minacce sofisticate: la sicurezza deve basarsi su elementi fisici non alterabili dal software (nemmeno da un'IA con privilegi elevati). l'intera industria dei semiconduttori, guidata da colossi come NVIDIA, Intel, AMD e ARM sta affrontando i nuovi rischi legati ai supercomputer per l'IA.

12. I casi d'uso: scenari operativi

I paragrafi che seguono propongono, per ciascun ambito, uno o più scenari esemplificativi: non la cronaca di un evento specifico, ma una sintesi rappresentativa di come queste tecnologie possono essere messe a sistema dagli operatori del settore, con alcuni riferimenti tecnici agli standard e ai parametri di riferimento.

Casi reali in Italia e in Europa

Nel marzo 2026 il Gruppo FS Italiane ha avviato la sperimentazione di una propria rete 5G lungo circa 60 chilometri della linea alta velocità Torino-Milano, tra Torino e Greggio, realizzata valorizzando le infrastrutture esistenti di RFI e TIM con cinque nuovi siti dedicati, un primo banco di prova concreto per le tecnologie che sosterranno il futuro standard ferroviario FRMCS; a livello europeo, il consorzio internazionale che sviluppa lo standard ha avviato nel corso del 2026 i primi test di laboratorio in tre centri europei. Sul fronte energetico, Terna ha varato un piano da 3,2 miliardi di euro fino al 2028 per la sicurezza del sistema elettrico nazionale, che include, tra circa settanta progetti di innovazione, la sperimentazione di robot per la manutenzione predittiva basata su intelligenza artificiale e visione artificiale; il gruppo multiutility Hera ha inoltre sviluppato, secondo quanto reso noto dall'azienda, una piattaforma che incrocia pattern di consumo, dati meteo e termografie per anticipare i guasti sulla rete fino a 72 ore prima che si verifichino. (Fonti comunicati aziendali)

12.1. Difesa

Le forze armate europee stanno evolvendo verso architetture C4ISR integrate (Command, Control, Communications, Computers, Intelligence, Surveillance and

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Reconnaissance), in cui reti radio tattiche sicure e reti mission-critical su LTE/5G collegano unità, veicoli e sensori in un unico ecosistema informativo. Le sale operative interforze integrano voce sicura, video proveniente da droni e feed da sensori e radar, mentre sistemi di cyber-difesa monitorano in tempo reale la salute delle reti di comunicazione critiche.:

Uno scenario rappresentativo di questa evoluzione è quello di un centro di comando interforze che integra le radio tattiche esistenti con slice 5G dedicati su infrastrutture nazionali e con piattaforme UC sicure per il dialogo con i decisori civili in uno scenario di crisi ibrida, un attacco cyber a un'infrastruttura critica accompagnato da eventi fisici sul territorio. La control room combina in un'unica vista mappe geografiche, feed video, dati di telemetria e comunicazioni vocali, tutte cifrate end-to-end e registrate; il sistema di gestione delle chiavi crittografiche resta interamente sotto il controllo dell'organizzazione, senza che il fornitore della piattaforma o l'operatore di rete abbiano accesso al materiale cifrante, un requisito che nel settore viene spesso descritto come modello a conoscenza zero.

12.2. Sicurezza pubblica

Le forze di polizia europee utilizzano da decenni reti TETRA o equivalenti, oggi in fase di integrazione crescente con LTE e 5G per trasportare video, dati e servizi avanzati oltre alla voce.

Il caso più citato dagli operatori del settore è quello di un grande evento urbano, una manifestazione sportiva, una visita istituzionale, una festività di massa, in cui una control room unificata mette in contatto polizia nazionale, polizia locale, trasporto pubblico e servizi sanitari. Le console di dispatch permettono di coordinare le pattuglie, deviare linee di autobus e metropolitana, gestire i flussi pedonali; sistemi di video analytics basati su intelligenza artificiale analizzano i feed delle telecamere per segnalare sovraffollamenti o comportamenti anomali, generando un allarme per l'operatore umano, che resta l'unico titolato a decidere; tutte le comunicazioni vocali critiche vengono registrate, a garanzia di eventuali indagini successive.

12.3. Protezione civile

Quando un disastro naturale, un'alluvione, un incendio boschivo, un terremoto, colpisce un territorio, le reti di comunicazione commerciali sono spesso le prime a essere compromesse, proprio nel momento in cui servono di più. Per questo le comunicazioni mission-critical in questo ambito devono poter contare su un mix di radio dedicate, 5G e satellite.

In un'emergenza idrogeologica, ad esempio, sensori idrometrici e pluviometrici collegati a sistemi SCADA generano allarmi verso una control room regionale; la piattaforma di comando e controllo avvia conferenze UC che mettono in contatto sindaci, forze dell'ordine e squadre di volontariato; slice 5G dedicati e collegamenti

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

satellitari mantengono la connettività verso le aree colpite anche quando le infrastrutture terrestri sono danneggiate; la registrazione degli eventi supporta l'analisi post-emergenza e la rendicontazione verso le autorità.

Un secondo scenario, sempre più presente nelle esercitazioni di protezione civile, riguarda gli eventi sismici che danneggiano le infrastrutture di rete ordinarie: un terremoto che colpisce un'area urbana densamente popolata può interrompere le dorsali in fibra e saturare in pochi minuti le poche celle radio superstiti, rendendo inutilizzabili le applicazioni di comunicazione commerciali proprio quando servono di più.

In questi casi i mezzi di soccorso possono attivare sul posto una copertura tattica autonoma tramite micro-celle 5G private e nodi di elaborazione locale, il cosiddetto local edge, mentre i droni di ricognizione trasmettono video ad alta definizione al centro di comando mobile secondo lo standard MCVideo; gli agenti sul campo comunicano in modalità MCPTT con meccanismi di priorità sulla cella tattica, garantendo alle chiamate d'emergenza la precedenza assoluta sul traffico dati non urgente.

Un modulo di intelligenza artificiale eseguito localmente sul nodo edge può analizzare lo streaming video dei droni per segnalare in tempo reale anomalie strutturali, mentre la cartografia condivisa viaggia tramite il canale dati MCData, il tutto in piena autonomia rispetto al cloud centrale, non raggiungibile in queste condizioni.

La protezione civile è probabilmente l'ambito in cui le reti di sensori IoT hanno già dimostrato, con casi concreti, la propria capacità di salvare vite. A Genova, dopo le alluvioni del 2011 e del 2014 che avevano causato vittime nella zona del torrente Bisagno, è stata realizzata una rete di sensori pluviometrici e idrometrici collegati via radio che rileva in tempo reale l'innalzamento dei livelli d'acqua e attiva misure preventive, dalla chiusura delle strade all'allerta delle autorità competenti, prima che la piena raggiunga i punti più a rischio.

Per gli incendi boschivi, il sistema europeo di osservazione della Terra Copernicus alimenta l'EFFIS, il sistema europeo di informazione sugli incendi forestali, che integra dati satellitari con le reti di avvistamento a terra per stimare in tempo reale il rischio di propagazione; a livello locale, sensori di temperatura, fumo e umidità distribuiti nelle aree boschive più esposte permettono un preallarme che i soli satelliti, con la loro minore frequenza di passaggio, non potrebbero garantire.

Per i terremoti, la Rete Sismica Nazionale dell'Istituto Nazionale di Geofisica e Vulcanologia, INGV, rileva ogni evento sismico sul territorio italiano e ne comunica tempestivamente epicentro, magnitudo e orario attraverso l'app INGVterremoti: un sistema che non predice il terremoto, va detto con chiarezza, ma che riduce dal minuto al secondo il tempo necessario per distinguere un dato verificato da una notizia non confermata, un vantaggio non banale nelle prime concitate fasi di un evento sismico.

Per le mareggiate e l'erosione costiera, reti di mareografi e stazioni meteomarine, come quella storicamente attiva a Venezia per la previsione delle acque alte, integrano

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

dati di marea, vento e pressione atmosferica per anticipare gli eventi estremi lungo le coste.

In tutti questi casi, il valore aggiunto delle reti IoT non è il singolo sensore, ma l'infrastruttura di comunicazione che porta il dato dal territorio alla sala operativa in tempo utile per agire, esattamente il tema al centro di questo white paper: una rete che deve restare disponibile quando il territorio che sta monitorando è già sotto stress.

12.4. Sanità ed emergenza sanitaria

L'integrazione tra le centrali del 112 e del 118, le reti ospedaliere, la telemedicina e la logistica sanitaria rende le comunicazioni critiche un elemento centrale della resilienza del sistema sanitario, un settore che l'ENISA colloca tra quelli a maturità di sicurezza ancora insufficiente rispetto alla propria criticità. In uno scenario di maxi-emergenza sanitaria, la centrale 112 instrada le chiamate verso la centrale sanitaria specializzata; piattaforme di Computer-Aided Dispatch e sistemi UC collegano ambulanze, pronto soccorso e reparti critici.

Strumenti di intelligenza artificiale possono supportare il triage automatico di messaggi e testi e la definizione delle priorità di chiamata, sempre sotto supervisione umana e, quando la classificazione lo richiede, nel rispetto degli obblighi dell'AI Act per i sistemi ad alto rischio.

12.5. Trasporti: ferrovie, metropolitane, aeroporti, porti

Nel comparto ***ferroviario e metropolitano***, anch'esso segnalato da ENISA tra i settori da rafforzare, molte reti europee stanno migrando verso lo standard FRMCS (*Future Railway Mobile Communication System*), integrando comunicazioni unificate e sistemi SCADA per segnalamento, alimentazione elettrica e informazione ai viaggiatori: una control room integrata gestisce gli allarmi di segnalamento, le comunicazioni treno-terra e gli annunci ai passeggeri, mentre il 5G e il FRMCS abilitano servizi aggiuntivi come il video di bordo e la diagnostica in tempo reale degli impianti.

Negli ***aeroporti***, le comunicazioni critiche collegano la torre di controllo, l'handling, la security, i vigili del fuoco aeroportuali e la dogana, con sistemi di registrazione vocale conformi agli obblighi normativi sui canali di controllo del traffico aereo e operativi, integrati con la gestione bagagli, il controllo accessi e la videosorveglianza.

Nei ***porti***, il coordinamento tra i movimenti nave-banchina, i terminal e la sicurezza perimetrale passa sempre più spesso attraverso reti 5G Standalone private che collegano radio portuali, sistemi UC e tecnologie operative come gru telecomandate e veicoli a guida autonoma, il tutto governato da politiche Zero Trust: ogni gru e ogni veicolo deve superare una verifica crittografica continua del certificato hardware prima di poter ricevere un comando; se un tentativo di attacco informatico cerca di iniettare ordini di movimentazione falsi clonando l'identità di un terminale legittimo, il motore di

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

policy della rete rileva l'anomalia e isola il dispositivo compromesso in tempi molto rapidi, senza dover fermare l'intero terminal.

12.6. Energia e utility

Nel comparto **elettrico**, i sistemi SCADA monitorano e controllano la rete di trasmissione e distribuzione, mentre la control room gestisce gli allarmi e il coordinamento con la protezione civile in caso di guasti estesi.

Un caso spesso citato dagli operatori riguarda la sicurezza delle squadre di intervento in aree remote, dove la copertura commerciale è assente: una utility che dispone di una rete privata dedicata, tipicamente in banda sub-GHz, tra i 410 e i 450 MHz, può dotare i tecnici di dispositivi di protezione individuale con sensori integrati, capaci di rilevare automaticamente una caduta o una perdita di conoscenza, i cosiddetti sistemi “uomo a terra”, e di attivare in automatico una chiamata MCPTT (Mission Critical Push-To-Talk) prioritaria verso la control room centrale, con la posizione esatta del tecnico.

Prima di autorizzare qualsiasi manovra fisica sull'impianto, la stessa piattaforma può interrogare via MCData il sistema SCADA locale attraverspo il nodo edge, verificando che la linea sia effettivamente sezionata prima che il tecnico intervenga.

Un percorso analogo riguarda il **gas** e le altre **utility**, dove il monitoraggio di pressioni, flussi e perdite si accompagna a comunicazioni critiche dedicate alle squadre di pronto intervento, spesso integrate con piattaforme UC e radio, e a sistemi di registrazione e logging necessari per verificare l'efficacia dei piani di emergenza.

12.7. Acqua e reti idriche

Anche le reti idriche compaiono, secondo ENISA, tra i settori la cui maturità di sicurezza non è ancora allineata alla loro criticità. Il caso di una **contaminazione sospetta** su una rete idrica illustra quanto stretta debba essere l'integrazione tra sistemi SCADA, sensori, piattaforme UC e comunicazioni verso enti e cittadini: ogni fase, dalla rilevazione dell'anomalia fino all'allerta della popolazione, va orchestrata in modo sicuro e tracciabile,

12.8. Finanza e servizi bancari

Nel settore finanziario, DORA rende esplicita l’importanza delle comunicazioni e dei sistemi di comando e controllo per la **resilienza operativa digitale**. Gli incidenti sulle infrastrutture ICT, comunicazioni comprese, che impattano funzioni critiche devono essere notificati secondo procedure standardizzate; le control room ICT e i security operations center diventano il punto di raccordo per rispettare i requisiti di monitoraggio, rilevamento, risposta e reporting; le comunicazioni con fornitori terzi critici, cloud in testa, devono essere disciplinate da contratti che rispettino requisiti specifici in materia di audit, uscita dal contratto, livelli di servizio e sicurezza.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Una riflessione analoga si potrebbe estendere ai servizi previdenziali, che pur non essendo oggi un settore autonomo ai sensi di NIS2 o CER, condividono con banche e assicurazioni la stessa natura di infrastruttura di fiducia su cui si regge il rapporto tra Stato e cittadino, e che potrebbero in prospettiva rientrare in un perimetro di resilienza operativa analogo a quello già previsto per il settore finanziario.

12.9. Telecomunicazioni e infrastrutture digitali

Le *reti di telecomunicazione* occupano una posizione paradossale in questo white paper: sono il mezzo attraverso cui passano tutte le comunicazioni critiche descritte nei capitoli precedenti, ma raramente vengono considerate esse stesse un'infrastruttura critica da proteggere. Il rapporto ENISA NIS360 colloca telecomunicazioni, insieme a energia elettrica e settore bancario, nella fascia a maturità e criticità più elevate fin dalla prima edizione del rapporto: non è una new entry, è ***uno dei tre pilastri storici del sistema***. In Italia questa centralità ha anche una traduzione proprietaria, con la disciplina del *Golden Power* che sottopone a controllo statale le operazioni societarie e le forniture critiche sulle reti 5G e sui servizi cloud, e con il servizio pubblico di radiotelevisione, che pur seguendo un quadro normativo distinto da NIS2 e CER, resta un canale di comunicazione istituzionale che nessuna pianificazione di continuità del Paese può permettersi di escludere in uno scenario di crisi.

Per un operatore di rete, la continuità del servizio dipende dagli stessi principi già descritti in questo documento: ridondanza dei nodi di rete e dei collegamenti in dorsale, segmentazione tra rete di gestione e rete di traffico, piani di disaster recovery per i data center che ospitano il core della rete, e capacità di isolare rapidamente un segmento compromesso senza portare offline l'intera infrastruttura. A questo si aggiunge un tema specifico del comparto digitale, i fornitori cloud e i data center della pubblica amministrazione: la migrazione dei servizi pubblici verso infrastrutture cloud rende questi fornitori, anch'essi coperti dalla NIS2 come infrastrutture digitali, un punto di dipendenza critico per il funzionamento quotidiano dello Stato, al pari di una rete elettrica o di un acquedotto, con l'aggravante che un'interruzione qui non blocca un singolo servizio ma può bloccare contemporaneamente decine di amministrazioni che su quell'infrastruttura si appoggiano.

12.10. Infrastrutture lineari: strade, viadotti e cantieri critici

I monitoraggio delle infrastrutture stradali con droni è già una realtà operativa in Italia. Autostrade per l'Italia ha condotto, tra l'agosto 2023 e il luglio 2024, la seconda fase del progetto sperimentale Falco, autorizzato da ENAC per operare in modalità BVLOS (Beyond Visual Line of Sight), oltre la linea visiva del pilota, su cinque siti della rete ligure: 1.407 interventi di droni che hanno monitorato traffico, cantieri, stato della pavimentazione e segnaletica, alimentando in tempo reale il Traffic Control Center e attivando tempestivamente forze dell'ordine e soccorso in caso di incidente.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Autostrade dello Stato ha annunciato per il 2025-2027 un piano da 18,5 milioni di euro per estendere droni, intelligenza artificiale e digital twin al monitoraggio di gallerie, trafori e tratte sensibili della rete statale, dal Monte Bianco al Frejus.

Un caso complementare, sul fronte della sicurezza fisica, riguarda il consorzio Cepav Due, con Saipem capofila, impegnato nella sicurezza dei cantieri della linea alta velocità Brescia Est–Verona: una flotta di droni in modalità BVLOS, la prima di questo tipo in Italia per la security di un cantiere infrastrutturale, sorveglia oltre 40 chilometri di aree sensibili, gallerie, sottostazioni, linee elettriche, giorno e notte e anche a infrarossi. I dati di droni, sensori e telecamere confluiscono in una piattaforma PSIM, Physical Security Information Management, coordinata da una Security Control Room in stretta collaborazione con le forze dell'ordine: secondo quanto riportato dal consorzio, il sistema ha ridotto dell'80% i tempi di intervento delle forze dell'ordine in caso di furti o atti vandalici. Sul fronte strutturale, ponti e viadotti stanno inoltre sperimentando tecnologie di distributed fiber optic sensing, DFOS, cavi in fibra ottica che rilevano in continuo vibrazioni, temperature e deformazioni lungo l'intera opera, già impiegate a livello internazionale anche per la sorveglianza perimetrale di siti industriali e la rilevazione di perdite lungo gasdotti e acquedotti.

Entrambi i casi sollevano una domanda di principio che riguarda, più in generale, ogni piattaforma di sorveglianza aerea o robotica applicata a infrastrutture critiche: il collegamento di comando e il flusso video o telemetrico tra drone e control room dipendono dalla stessa rete IT/OT dell'infrastruttura sorvegliata, o da un canale indipendente? La direttiva NIS2, che classifica le infrastrutture di trasporto tra i settori essenziali, orienta verso la seconda opzione, applicando alle piattaforme di sorveglianza lo stesso principio del doppio binario descritto nel capitolo 3. Le minacce da considerare in fase di progettazione includono le interferenze sui collegamenti radio-comando, il jamming, lo spoofing dei segnali di posizionamento satellitare, e l'intercettazione del flusso video.

> *“Difesa, sanità, trasporti, energia e finanza condividono la stessa architettura di fondo: un doppio binario in cui il lavoro quotidiano e l'emergenza viaggiano su piattaforme diverse ma interoperabili.”*

13. L'ultimo miglio della sicurezza: dall'allerta alla decisione delle persone

Le tecnologie descritte in questo white paper risolvono un problema preciso: far arrivare l'informazione giusta, in tempo, da un sensore a una control room. Ma nei disastri naturali e a causalità mista, dove un evento come un'alluvione può interrompere una sottostazione, isolare ripetitori e contaminare una rete idrica in

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

sequenza, la catena della sicurezza non si esaurisce nell'infrastruttura tecnica: prosegue fino alla persona che riceve l'allerta e deve trasformarla in una decisione, spostarsi, restare, aiutare, senza intralciare i soccorsi.

In questo senso, le comunicazioni sicure verso le infrastrutture critiche e verso i cittadini sono due facce della stessa sfida: rendere possibile agire in pochi secondi quando decidere è tutto ciò che conta.

L'ultimo miglio della sicurezza

Il punto di partenza teorico è considerare una crisi, un disastro, una situazione di emergenza un vero e proprio processo socio-tecnico, in cui la tecnologia deve necessariamente interfacciarsi con le persone. In linea con il sistema della Protezione Civile italiana, riconosciuto *best practice* a livello internazionale, il singolo cittadino deve essere riconosciuto come il **primo attore** della sicurezza. Per mettere concretamente al centro le persone, l'agenda d'intervento deve focalizzarsi su una vera e propria ***Disaster Literacy (Alfabetizzazione all'emergenza)*: ** non è sufficiente possedere strumenti tecnologici; occorre sviluppare competenze basate su quattro fasi chiave: **accesso, comprensione, valutazione e azione**. La comprensione rappresenta l'anello debole tra l'allerta normalmente messa in campo dalle istituzioni o dagli operatori e l'azione del cittadino.

Abbiamo un grosso problema di ***traduzione del linguaggio tecnico e scientifico***. Esiste la necessità stringente di tradurre il linguaggio scientifico e tecnico in termini accessibili. Messaggi non mediati (ad esempio sulla probabilità di un evento sismico) rischiano di generare panico ingiustificato nel pubblico.

Un altro ambito su cui lavorare è su ***Inclusività e approccio multigenerazionale***: a differenza del settore commerciale, la gestione pubblica dell'emergenza non può targettizzare solo alcune fasce di popolazione. È fondamentale adottare una comunicazione multicanale, multigenerazionale e multiculturale che risponda ai bisogni specifici di pubblici diversi (dai giovani agli anziani).

Il ***Protective Action Decision Model***, il modello di riferimento negli studi sui sistemi di allerta pubblica, mostra che la consegna tecnica di un messaggio non equivale a una risposta protettiva: tra la ricezione e l'azione si interpone una sequenza di passaggi cognitivi, attenzione, comprensione, percezione della minaccia, ciascuno dei quali può interrompersi, e ricevere un'allerta non significa aver ricevuto un'istruzione utilizzabile.

La differenza tra ***un'allerta efficace e una inefficace*** dipende spesso dalla qualità del messaggio più che dalla rete che lo trasporta: un contenuto come 80-100 mm di pioggia in 6 ore comunica un dato tecnico corretto ma non traducibile in azione, mentre nelle prossime due ore alcuni sottopassi possono allagarsi rapidamente, evita gli

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

spostamenti, non entrare nei sottopassi risponde alle due domande che contano davvero in emergenza: che cosa significa qui, e che cosa posso fare adesso.

Per le comunicazioni sicure e mission-critical questo significa progettare fin dall'origine non solo l'infrastruttura, ma anche i contenuti: messaggi che riducano l'ambiguità, che rendano evidente "chi deve fare cosa, dove e quando" e che siano compatibili con il tempo disponibile, con il livello di preparazione dei destinatari e con l'evoluzione dell'evento. In questo modo l'energia investita in reti, piattaforme e sale operative si traduce in decisioni praticabili e comportamenti efficaci, allineando la dimensione tecnica della comunicazione con quella umana.

Un ultimo elemento, che le sole tecnologie non risolvono, è la ***multicanalità***: *cell broadcast, app, social media, sirene, radio, televisione e comunicazioni dirette* delle autorità raggiungono la stessa popolazione con canali diversi, spesso in parallelo, e non sempre in modo coerente tra loro. Quando circolano contemporaneamente informazioni ufficiali, rumore di fondo e disinformazione, la vera sfida non è più solo far arrivare il messaggio, ma garantire che tutti i canali dicano, nella sostanza, la stessa cosa nello stesso momento. È un tema di governance dell'informazione più che di infrastruttura di trasporto, ed è probabilmente il punto in cui il confine tra comunicazioni mission-critical e comunicazione pubblica diventa più sottile.

La robustezza delle reti e dei sistemi è una condizione necessaria; la comprensione del rischio da parte delle persone, costruita prima della crisi, è la condizione che la rende sufficiente.

In conclusione, accanto agli investimenti tecnologici e strutturali, è indispensabile progettare e finanziare una vera e propria ***infrastruttura sociale per la sicurezza***.

14. L'ecosistema industriale: dai vendor globali agli integratori di territorio

Attorno a questo comparto si è consolidato un ecosistema a più livelli. Il mercato globale, secondo Mordor Intelligence, è moderatamente concentrato attorno ad alcuni operatori storici, Motorola Solutions, Nokia, Huawei, L3Harris Technologies, Hytera Communications, Ericsson, Thales e Airbus, che fanno leva sulle installazioni radio esistenti, sui portafogli brevettuali e su una profonda conoscenza dei quadri regolatori nazionali per difendere contratti di servizio ad alto margine.

Tabella 4: I principali fornitori di comunicazioni critiche

Fornitore	Paese	Principali tecnologie e soluzioni
Motorola Solutions	Stati Uniti	Radio P25, infrastrutture e dispositivi mission-critical, piattaforme broadband e MCX, software per command centre, video e sicurezza
L3Harris Technologies	Stati Uniti	Comunicazioni tattiche e professionali per difesa, sicurezza pubblica e aviazione: reti e terminali LMR/P25,

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

		sistemi radio tattici, soluzioni dati e video per operazioni mission-critical. Comunicazioni tattiche e partnership con enti governativi
Nokia	Finlandia	Reti private LTE/5G, core di rete, IP/MPLS, reti ottiche, cybersecurity, reti ferroviarie, FRMCS e soluzioni per utilities
Ericsson	Svezia	Reti LTE e 5G, core, mission-critical broadband, network slicing, OSS/BSS e servizi di rete
Airbus Public Safety and Security	Europa	TETRA, Tetrapol, Agnet, MCX su 4G/5G, applicazioni push-to-talk, interoperabilità e collaborazione multimediale
Thales	Francia	TETRA, PMR, LTE/5G mission-critical, crittografia, key management, cybersecurity e soluzioni sovrane
Frequentis	Austria	MissionX MCX, control room, dispatch, gestione incidenti, interoperabilità, registrazione e integrazione voce-video-dati
Hytera	Cina	DMR, TETRA, broadband, dispositivi MCS, body camera, applicazioni dati e soluzioni per sicurezza pubblica
Tait Communications	Nuova Zelanda	P25, DMR, LMR, LTE, satellite, Wi-Fi, dispositivi rugged, sistemi convergenti e servizi gestiti
Sepura	Regno Unito	Terminali TETRA, radio ibride TETRA-LTE/5G, applicazioni broadband, copertura estesa e gestione dispositivi
Streamwide	Francia	Team on Mission, piattaforma MCPTT/MCVideo/MCData su reti 4G/5G, geolocalizzazione, gestione missioni e interoperabilità per comunicazioni mission-critical
CISCO	Stati Uniti	Routing e switching, reti IP/MPLS e WAN private, soluzioni SD-WAN e security, Industrial Ethernet, router e wireless rugged per OT, blueprint di sicurezza per infrastrutture industriali
Leonardo	Italia	TETRA, DMR, broadband, LTE/5G, control room, integrazione di rete e sistemi turnkey per difesa, sicurezza pubblica, trasporti e infrastrutture critiche. Soluzioni in oltre 50 Paesi

La tabella riporta alcuni tra i principali fornitori internazionali di tecnologie per comunicazioni critiche e mission-critical, con focus su sistemi radio professionali, piattaforme MCX, control room e integrazione UC. L'elenco non è esaustivo e non rappresenta una graduatoria, ma una selezione dei principali attori presenti sul mercato globale, europeo e italiano.

Motorola Solutions punta sull'innovazione attraverso soluzioni software avanzate e sistemi di comunicazione integrati; *L3Harris Technologies* privilegia le partnership con enti governativi statunitensi; *Thales Group* persegue attivamente iniziative di trasformazione digitale per mantenere un vantaggio competitivo in un mercato in rapida evoluzione.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Al tempo stesso, fornitori di piattaforme software native per il cloud e specialisti della radio via software stanno erodendo questo vantaggio competitivo, offrendo architetture aperte e servizi basati su API. Le operazioni di acquisizione più recenti riflettono questa transizione: nel 2024 Motorola Solutions ha acquisito Pelco, specialista in visione artificiale, per rafforzare le proprie capacità di analisi video, mentre Nokia ha stretto una collaborazione con Rockwell Automation per integrare il 5G Standalone con l'analisi dei dati nella fabbrica connessa. La differenziazione si sta progressivamente spostando dall'hardware radio al software di orchestrazione capace di garantire prestazioni costanti su reti ibride multi-fornitore.

Alcuni attori meritano una menzione specifica per il ruolo che giocano in Europa e in Italia.

Leonardo, Airbus Public Safety and Security e Frequentis, i tre fornitori europei più rilevanti per il mercato italiano, competono soprattutto sul terreno delle partnership: Airbus ha integrato la propria piattaforma Tactilon Agnet con le infrastrutture 5G private di Ericsson, mentre Frequentis punta sulla continuità fra torri di controllo aereo, sale operative ferroviarie e centri di risposta ai disastri come fattore differenziante rispetto ai concorrenti generalisti.

Altri fornitori specializzati, *Bittium, Sepura, Tait Communications, Streamwide, Cobham, JVCKENWOOD e Rohill Engineering,* presidiano nicchie specifiche, dai terminali tattici militari alle reti TETRA per il settore pubblico.

A garanzia dell'interoperabilità multi-vendor, l'associazione internazionale TCCA certifica la conformità delle piattaforme agli standard 3GPP MCX, evitando che le istituzioni restino vincolate all'hardware di un singolo fornitore.

Sul fronte delle Unified Communications e del networking, attori come *Cisco, Microsoft, Nokia, Oracle, AudioCodes e NEC* forniscono piattaforme UC, SBC e sistemi di registrazione vocale, spesso integrati nelle soluzioni per infrastrutture critiche attraverso partner locali. Nel mondo OT e SCADA, gruppi come *Siemens, Schneider Electric, ABB, GE Digital ed Emerson* restano centrali per energia, acqua e industria.

Tra questi mondi si inserisce un attore spesso poco visibile ma decisivo: il system integrator e operatore regionale, che funge da traduttore tra la tecnologia globale e il contesto locale. Comprendere le normative nazionali, i requisiti settoriali e i vincoli operativi di ogni singola organizzazione non è un compito che un vendor internazionale può svolgere da solo: richiede presenza sul territorio, competenze verticali e capacità di erogare servizi gestiti, manutenzione, supporto continuativo e attività di certificazione.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

15. COM.TEL.: esperienza nelle Comunicazioni sicure

Tra i system integrator, COM.TEL opera come fornitore di soluzioni ICT con esperienza consolidata nell'ambito di Unified Communications, voce, SBC, comunicazioni sicure e registrazione. Ha inoltre una presenza nei trasporti, nella sanità e nella pubblica amministrazione. Il suo ruolo nelle architetture mission-critical consiste nell'integrare tecnologie e domini diversi, infrastrutture 5G o sistemi SCADA per accompagnare verso architetture di comunicazione sicura e mission-critical, sia in ambito nazionale sia in una prospettiva internazionale.

Dopo l'integrazione di NovaNext, COM.TEL. applica alle comunicazioni critiche un modello di AgenticOps basato su tecnologia Cisco, in cui gli agenti AI supportano il centro operativo nel triage degli eventi, nella correlazione delle informazioni e nella preparazione delle azioni correttive, mentre la capacità di governo, il giudizio e la decisione restano affidati alle persone. È un esempio concreto, tra gli altri descritti in questo white paper, di come l'intelligenza artificiale possa affiancare, senza sostituire, l'operatore in control room.

16. Il Quadro regolatorio

Negli ultimi anni l'Unione Europea ha costruito, pezzo dopo pezzo, un perimetro normativo che rende la resilienza delle comunicazioni un obbligo di legge, non più solo una buona pratica aziendale. Conoscerlo è indispensabile per chiunque gestisca infrastrutture critiche o servizi essenziali.

16.1. NIS2 e CER: la resilienza come requisito

La direttiva NIS2 (UE 2022/2555), recepita in Italia con il D.Lgs. 138/2024, ha esteso e irrobustito le regole di cybersecurity per le reti e i sistemi informativi di settori essenziali e importanti, energia, trasporti, sanità, acqua, infrastrutture digitali, pubblica amministrazione, spazio. La direttiva CER (UE 2022/2557), complementare alla prima, ha introdotto il concetto di entità critica e obblighi di resilienza fisica e organizzativa per undici settori chiave: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione, spazio e filiera alimentare. Insieme, i due testi portano dentro il perimetro del risk management e della continuità operativa anche i sistemi di comando, controllo e comunicazione che supportano i servizi essenziali.

Sul piano tecnico-organizzativo, l'articolo 21 della NIS2 elenca un set minimo di misure che i soggetti essenziali e importanti devono adottare in modo proporzionato al rischio: analisi dei rischi e politiche di sicurezza dei sistemi informativi, gestione degli incidenti, piani di continuità operativa e di disaster recovery, sicurezza della catena di approvvigionamento, sicurezza nell'acquisizione e manutenzione dei sistemi, igiene

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

informatica di base e formazione del personale, politiche sull'uso della crittografia, controllo degli accessi e, dove opportuno, autenticazione a più fattori. Per le control room e le reti di comunicazione critiche, questo si traduce in piani di continuità delle comunicazioni, canali di emergenza ridondati e testati periodicamente, e obblighi di logging e di notifica degli incidenti significativi.

L'attuazione italiana della direttiva CER ha compiuto un passo concreto il 26 aprile 2026, con l'adozione, ai sensi dell'articolo 6 del D.Lgs. 134/2024, della prima ***Strategia Nazionale per la Resilienza dei soggetti critici***. Il provvedimento non si limita a enunciare principi: istituisce un Comitato interministeriale per la resilienza, competente a coordinare a livello di governo le misure previste dal decreto, e prevede la creazione di un registro nazionale dei soggetti critici e, ai sensi dell'articolo 16, di un registro nazionale degli incidenti rilevanti. Per le organizzazioni che gestiscono comunicazioni mission-critical, questo significa che l'identificazione formale come soggetto critico, e i conseguenti obblighi di resilienza fisica e organizzativa, non sono più un orizzonte normativo futuro ma un processo amministrativo già in corso.

A questo si aggiunge, come descritto nel capitolo 5 a proposito del rischio quantum computing, l'obbligo in arrivo di dotarsi di politiche esplicite di migrazione verso la crittografia post-quantistica, introdotto dalla proposta di modifica della NIS2 pubblicata dalla Commissione Europea il 20 gennaio 2026.

16.2. Cybersecurity e governance: la responsabilità arriva ai vertici dell'organizzazione

La cybersicurezza non è soltanto un tema tecnico, ma sempre più un tema di governance: ai sensi dell'articolo 23 del D.Lgs. 138/2024, gli obblighi degli organi di amministrazione e direttivi dei soggetti NIS non sono delegabili con effetto liberatorio. È delegabile l'esecuzione operativa delle misure di sicurezza, ma restano in capo al vertice dell'organizzazione l'approvazione delle politiche di gestione del rischio, la vigilanza informata sulla loro attuazione e la verifica della formazione del personale. Per gli amministratori, la tutela non risiede quindi soltanto nella nomina di un responsabile della sicurezza, ma nella capacità di documentare le decisioni assunte, le informazioni ricevute e la formazione effettivamente svolta, elementi che in caso di incidente diventano la prova della diligenza richiesta dalla norma.

16.3. AI Act: quando l'algoritmo entra in control room

Il Regolamento sull'intelligenza artificiale (UE 2024/1689), il primo quadro giuridico al mondo basato sul rischio per questa tecnologia, classifica come ad alto rischio numerose applicazioni utilizzate proprio nelle infrastrutture critiche, in sanità e nella sicurezza pubblica: rientrano in questa categoria, tra gli altri, i sistemi usati come componenti di sicurezza nella gestione di infrastrutture critiche digitali, del traffico

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

stradale e della fornitura di acqua, gas, riscaldamento ed elettricità, oltre ai sistemi impiegati dalle autorità di contrasto e dai servizi di pronto intervento per valutare l'urgenza delle chiamate. Per questi sistemi l'AI Act richiede un sistema di gestione del rischio lungo tutto il ciclo di vita, una governance solida dei dati di addestramento, documentazione tecnica dettagliata, registrazione automatica degli eventi, supervisione umana effettiva, e la registrazione in un database europeo dedicato. Le sanzioni per le violazioni più gravi possono arrivare fino al 3% del fatturato annuo globale, o 15 milioni di euro se superiore.

Un aggiornamento normativo rilevante va segnalato: il Regolamento (UE) 2026/1744, noto come Digital Omnibus on AI, entrato in vigore il 27 luglio 2026, ha posticipato l'entrata in vigore degli obblighi relativi ai sistemi ad alto rischio dell'Allegato III, comprese le applicazioni per infrastrutture critiche, dal 2 agosto 2026 al 2 dicembre 2027, e quella per i sistemi ad alto rischio integrati in prodotti già regolati da normativa di sicurezza settoriale, Allegato I, al 2 agosto 2028. Resta invece invariata al 2 agosto 2026 l'entrata in vigore degli obblighi di trasparenza dell'articolo 50, con la sola eccezione della filigrana sui contenuti generati dall'IA, prorogata al 2 dicembre 2026 per i sistemi già sul mercato.

Il rinvio concede tempo di preparazione, ma non cambia la sostanza: gli algoritmi che oggi analizzano flussi video in una control room, che correlano allarmi provenienti da una rete idrica o che assegnano priorità alle chiamate di un 112, con ogni probabilità rientrano in questo perimetro ad alto rischio e conviene progettarli fin dall'inizio in conformità con l'AI Act, un approccio “compliant by design”, non adattarli a posteriori sotto la pressione della scadenza. È anche per questo che le architetture MCUC più recenti tendono a eseguire i modelli di intelligenza artificiale in locale, sul server della control room, mantenendo un registro di audit firmato e verificabile per ogni raccomandazione.

16.4. La responsabilità penale nell'uso dell'AI per infrastrutture critiche

Oltre al perimetro amministrativo definito dall'AI Act e da NIS2, l'ordinamento italiano ha introdotto un livello ulteriore di responsabilità, questa volta di rilievo penale. La Legge 23 settembre 2025, n. 132, in vigore dal 10 ottobre 2025, ha inserito nel codice penale il reato di illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale, l'articolo 612-quater, punito con la reclusione da uno a cinque anni, oltre a un'aggravante comune per i reati commessi impiegando sistemi di IA come mezzo insidioso. Un successivo decreto legislativo, il 160/2026, ha esteso questo perimetro con un nuovo articolo 437-bis, che punisce l'omissione di misure di sicurezza idonea ad alterare il funzionamento di un sistema di intelligenza artificiale:

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

entrambi i reati sono stati inseriti tra quelli presupposto della responsabilità amministrativa degli enti ai sensi del decreto legislativo 231 del 2001.

Per le organizzazioni che forniscono o gestiscono componenti di intelligenza artificiale all'interno di infrastrutture critiche, la conseguenza pratica è che un'omissione nelle misure di sicurezza non è più soltanto una violazione amministrativa sanzionabile da un'autorità di settore, ma può generare una responsabilità penale individuale e, a cascata, una responsabilità dell'ente stesso. Resta aperta, tuttavia, una criticità che la ricerca sottolinea: in assenza di standard tecnici già consolidati su quali misure di sicurezza siano idonee a prevenire l'alterazione di un sistema di IA, il rischio è che la responsabilità venga accertata ex post, sulla base di quanto accaduto in concreto, anziché sulla base di regole cautelari definite ex ante. È una delle ragioni per cui la ricerca propone lo sviluppo di un dialogo strutturato tra soggetti pubblici e privati e la creazione di ambienti di sperimentazione regolamentata, le cosiddette ***regulatory sandbox***, per consolidare prassi di settore prima che intervenga un contenzioso.

16.5. GDPR: la protezione dei dati non va in pausa in emergenza

Il GDPR resta il quadro di riferimento per la protezione dei dati personali anche in questo dominio: registrazioni vocali, log delle chiamate, metadati di posizione e immagini di videosorveglianza contengono spesso dati personali, talvolta sensibili, come i dati sanitari raccolti durante un soccorso, e richiedono basi giuridiche chiare, insieme a principi di minimizzazione e politiche di conservazione bilanciate con gli obblighi normativi settoriali.

Le architetture Zero Trust, che verificano in modo continuo identità e contesto di ogni accesso, offrono anche un beneficio in termini di protezione dei dati, perché restringono per costruzione la platea di chi può consultare registrazioni e log a chi ne ha effettiva necessità operativa, un principio che il GDPR chiama minimizzazione dell'accesso.

16.6. DORA: la resilienza operativa digitale nel settore finanziario

Un capitolo a parte merita il settore finanziario, dove il Regolamento DORA (UE 2022/2554) ha introdotto un quadro comune di resilienza operativa digitale per oltre 22.000 soggetti, banche, assicurazioni, infrastrutture di mercato, gestori di fondi, fornitori di servizi di pagamento e cripto-asset.

Il regolamento si articola in cinque pilastri:

- la gestione del rischio ICT, un framework integrato per identificare, proteggere, rilevare, rispondere e recuperare da incidenti informatici, con responsabilità diretta dell'organo di amministrazione;

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

- la gestione e notifica degli incidenti, con classificazione degli eventi e notifica iniziale entro quattro ore per gli incidenti maggiori;
- il test di resilienza operativa digitale, con verifiche periodiche fino a test di penetrazione guidati da minacce reali, i cosiddetti TLPT, ogni tre anni per le entità più significative;
- la gestione del rischio derivante da fornitori terzi ICT, cloud compreso, con obblighi contrattuali specifici, un registro delle relazioni di terze parti da tenere aggiornato e la possibilità per le autorità europee di designare come critici alcuni fornitori strategici;
- la condivisione, su base volontaria, di informazioni su minacce e incidenti cyber tra entità finanziarie.

16.7. Il dibattito italiano sulla biometria

Un fronte normativo apertosi nell'estate del 2026, che riguarda da vicino le tecnologie di video analytics e riconoscimento descritte nei capitoli precedenti, è quello del decreto legislativo con cui l'Italia ha adeguato la propria normativa all'AI Act anche per l'uso dell'intelligenza artificiale da parte delle forze dell'ordine. Il testo disciplina il riconoscimento facciale lungo tre direttrici: l'identificazione biometrica in tempo reale per prevenire minacce gravi o ritrovare persone scomparse, l'identificazione dal vivo nel corso di indagini penali già avviate, e il riconoscimento a posteriori su immagini già registrate. Al di là delle diverse posizioni che si sono confrontate sul provvedimento, il caso italiano è utile a chi opera nel settore delle comunicazioni critiche per la domanda di fondo che pone: dove tracciare il confine tra l'efficacia operativa delle tecnologie di riconoscimento, sempre più integrate nelle piattaforme di video analytics per la sicurezza pubblica, e le garanzie di proporzionalità che il diritto europeo richiede quando l'intelligenza artificiale osserva sistematicamente spazi pubblici.

16.8. Il procurement pubblico delle infrastrutture mission-critical

Un tema che la regolazione europea non affronta direttamente, ma che discende naturalmente da essa, riguarda il procurement pubblico: quali criteri, oltre al prezzo, distinguono l'acquisto di una control room o di una rete di emergenza da quello di un bene o servizio ordinario? Nel confronto con gli operatori del settore, alcuni temi ricorrono con una certa frequenza: l'interoperabilità con i sistemi esistenti, la continuità operativa, la portabilità dei dati e la possibilità di cambiare fornitore, la sicurezza fin dalla progettazione, la localizzazione dei dati, una strategia di uscita dal contratto, l'aggiornabilità nel tempo, la sicurezza della catena di fornitura e la capacità di funzionare offline per il tempo minimo richiesto dal servizio.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

16.9. Con chi si costruisce un'infrastruttura critica: il Golden Power

Il quadro regolatorio descritto in questo capitolo, NIS2, CER, AI Act, DORA, disciplina soprattutto come un'organizzazione deve gestire il rischio informatico e operativo delle proprie comunicazioni critiche. Resta aperta una domanda distinta, altrettanto rilevante per chi progetta un'infrastruttura di questo tipo: con chi si può costruirla? Chi è il fornitore, chi lo controlla, e quali dipendenze strategiche crea la scelta di un vendor piuttosto che di un altro?

In Italia la risposta passa attraverso la disciplina del Golden Power, i poteri speciali che il Governo può esercitare su operazioni societarie e forniture ritenute strategiche. La *Relazione annuale sull'attività del Golden Power del 2025*[20] evidenzia che questi poteri sono stati esercitati in 46 casi, ma solo 2 si sono conclusi con un'opposizione vera e propria; negli altri 44 l'intervento si è tradotto in condizioni e prescrizioni imposte all'operazione.

Le notifiche complessive ricevute dalla Presidenza del Consiglio nel 2025 sono state 903, in aumento del 37% sull'anno precedente: un volume che conferma quanto lo strumento sia diventato una tappa ordinaria, non eccezionale, nella pianificazione di un'operazione societaria o di fornitura in un settore strategico. Per le operazioni non ancora irreversibili, la normativa prevede inoltre uno strumento di pre-notifica, che consente di sapere entro 30 giorni se un'operazione rientra nel perimetro del Golden Power prima di renderla definitiva, un passaggio che vale la pena considerare fin dalle prime fasi di un progetto, non a rete già costruita.

Un aspetto spesso sottovalutato riguarda la nozione di soggetto esterno all'Unione Europea rilevante ai fini del controllo: non conta la sede legale dell'azienda fornitrice, ma chi la controlla, anche indirettamente, con un'espressa clausola contro le condotte elusive. Una società stabilita in uno Stato membro ma controllata da un soggetto extra-UE rientra comunque nel perimetro di verifica.

Il quadro è inoltre destinato ad allargarsi: il Regolamento (UE) 2026/1386, entrato in vigore il 16 luglio 2026, imporrà a tutti gli Stati membri, ***a partire dal 17 gennaio 2028***, un meccanismo nazionale di controllo degli investimenti esteri armonizzato a livello europeo, esteso anche alle operazioni formalmente intra-UE realizzate attraverso società controllate da investitori di Paesi terzi.

Il dato più utile per chi progetta un'infrastruttura critica non è quindi il veto, evento raro, ma la capacità dello Stato di incidere concretamente sulle condizioni dell'operazione, un potere di regolatorio e prescrittivo capace di incidere profondamente sulle scelte

[20] Relazione alle Camere sull'attività della Commissione Golden Power, anno 2025 (Presidenza del Consiglio, luglio 2026) https://www.senato.it/service/PDF/PDFServer/DF/448822.pdf

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

industriali che si esercita molto più spesso del potere di blocco. L'intervento si manifesta principalmente attraverso l'imposizione di condizioni stringenti che ridefiniscono l'architettura tecnica e la governance delle operazioni: possono incidere su requisiti di sicurezza, su diversificazione dei fornitori, sul monitoraggio, sul governo delle componenti critiche. Nel procedimento *Golden Power* le condizioni diventano pubbliche e arrivano dall'esterno.

Il settore delle telecomunicazioni offre l'esempio più diretto di come questo si traduca in pratica: gli operatori notificano annualmente al Governo il proprio piano di acquisti per le reti 5G, indicando anche i fornitori potenziali dei componenti più sensibili. Una decisione che nasce come scelta tecnica, quale vendor, quali componenti, quale partner tecnologico, diventa così anche una variabile regolatoria da gestire fin dalla fase di progettazione, non da verificare a operazione già conclusa.

Un secondo aspetto, meno noto ma altrettanto rilevante, riguarda ciò che può essere considerato strategico oltre all'hardware. Il caso ***Manta Aircraft***, la start-up italiana la cui joint venture con un partner cinese è stata bloccata dal Governo nell'ottobre 2024, un veto confermato in appello dal Consiglio di Stato nel marzo 2026, riguardava non un impianto, un componente fisico o un brevetto, ma un patrimonio di conoscenze tecnico-scientifiche ancora in fase di sviluppo; un *"asset strategico"* Per chi integra sistemi complessi di comunicazione critica, la stessa logica si applica al di là del singolo caso: conta non solo che cosa si acquista da un fornitore, ma anche quale conoscenza tecnica si condivide con lui nel corso della collaborazione.

Per chi progetta un'architettura di comunicazione mission-critical, tre domande derivano direttamente da questo quadro: chi controlla effettivamente il fornitore, quanto l'architettura dipende da una singola tecnologia o da un singolo vendor, e quanto sarebbe difficile, in caso di necessità, sostituirlo. Sono domande al tempo stesso di sicurezza, di progettazione tecnica e di procurement, che si aggiungono, più che sostituire, ai criteri già descritti nei paragrafi precedenti. Il principio del "***compliant by design"*** richiamato in questo white paper può essere quindi esteso di un passo ulteriore: non riguarda solo come si costruisce un'infrastruttura critica, ma anche da chi, e da quali dipendenze, la si costruisce.

Il Golden Power come vincolo di progettazione: dall'approccio reattivo al modello "Compliant by Design"

Pianificare la conformità a valle della firma di un accordo commerciale rischia di generare aggravi di costi, ritardi infrastrutturali e modifiche impreviste al progetto. Qual è l'unica indicazione operativa per mitigare questo rischio? Da qualche anno è possibile la pre-notifica preliminare al Governo. Attivabile quando l'operazione è definita ma la scelta

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

industriale non è ancora irreversibile, la procedura si conclude in 30 giorni, non c'è bisogno poi di una notifica formale e quindi l'accordo non subirà effetti negativi.

La formula corretta, «compliant by design», cioè progettare la conformità dall'inizio invece di rincorrerla, include la scelta del fornitore: il momento in cui si chiede allo Stato se quell'operazione rientri nel perimetro, prima che diventi irreversibile, è proprio il quello iniziale, non quello finale. Il Golden Power non è un rischio da gestire alla fine: è un vincolo di progettazione.

16.10. Strategie di Supporto all'Innovazione e Semplificazione Normativa

In questo contesto il MIMIT sta implementando una serie di interventi mirati a sostenere l'ecosistema dell'innovazione e alla semplificazione delle procedure, dedicate in particolare alla tutela e alla crescita di micro, piccole e medie imprese, spin-off universitarie e start-up operanti nel settore deep tech, anche in relazione all'adeguamento alla direttiva NIS2. Nel settore della tecnologia l'ultima iniziativa sugli Accordi per l'Innovazione nel settore TLC e tecnologie ha visto un bando di ca 201 milioni di euro lanciato lo scorso gennaio che ha registrato richieste pari a 302 milioni di euro, confermando l'elevata rispondenza alle esigenze del mercato.

Per quanto riguarda la semplificazione, una delle recenti iniziative relative agli adempimenti previsti dall'articolo 13 del DL 104 per investimenti strategici nazionali superiori al miliardo di euro: l'istituzione di un commissario straordinario e la conferenza unificata semplificata permettono il rilascio dell'autorizzazione unica in due mesi. La semplificazione sta attraendo importanti capitali esteri, con previsioni di investimento nel comparto data center stimate in circa 25 miliardi di euro per i prossimi due anni.

17. Le sfide per il futuro delle comunicazioni mission-critical

I capitoli di questo white paper hanno attraversato tecnologie, mercato, normativa e casi d'uso di settori diversi. Da questo percorso, e dal confronto della tavola rotonda del 1° ottobre, emergono alcuni temi trasversali che il Centro Studi COM.TEL. non ha la pretesa di risolvere in questo lavoro: li propone come agenda di lavoro aperta, un invito al confronto con chi, tra istituzioni, operatori e università, vive ogni giorno la gestione di queste infrastrutture.

1. Quali standard minimi di resilienza, differenziati per settore, potrebbero orientare in modo più uniforme investimenti e regolazione, e quale forma di verifica periodica e indipendente, sul modello di una revisione, potrebbe attestarne il rispetto nel tempo?

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

2. Come si potrebbe avviare, settore per settore, una *mappatura delle dipendenze critiche*, comprese quelle meno visibili, come cavi sottomarini, collegamenti satellitari e catene di fornitura, così da individuare per tempo i singoli *"point of failure"* e pianificare, per la crittografia, la migrazione verso algoritmi resistenti al calcolo quantistico?
3. Un parametro di *autonomia operativa minima* può diventare un riferimento condiviso, calibrato caso per caso da chi regola e da chi progetta?
4. Come si può rafforzare l'*interoperabilità* multi-vendor e, al tempo stesso, governare fin dalla fase di progetto il controllo dei fornitori, anche indiretto, evitando che un'infrastruttura critica resti vincolata a un singolo vendor o a un'unica giurisdizione?
5. Quali *criteri di resilienza*, oltre al prezzo, meriterebbero un posto esplicito nei capitolati di gara pubblici, accanto a quelli già descritti nel capitolo 16?
6. Come si investe, in modo sistematico, in *competenze ed esercitazioni* inter-organizzative, riconoscendo il fattore umano come componente della resilienza al pari della tecnologia, e come si costruisce, prima della crisi, la capacità delle persone di comprendere un'allerta e di tradurla in una decisione?
7. Come si definisce, in ciascuna organizzazione, una *governance dell'intelligenza artificiale* nelle comunicazioni mission-critical, distinguendo le decisioni delegabili da quelle che devono restare umane, e con quali strumenti, come ambienti di sperimentazione regolamentata e dialogo strutturato tra pubblico e privato, si possono consolidare prassi condivise prima che intervenga il contenzioso?

A questi temi se ne affianca uno trasversale, emerso nella tavola rotonda: di fronte alla molteplicità di iniziative pubbliche e private, dal Golden Power ai tavoli settoriali sui cavi sottomarini, dalla sperimentazione con i droni agli investimenti in calcolo quantistico, si sente l'esigenza di un soggetto che faccia da acceleratore, capace di mettere in rete imprese e istituzioni e di ricondurre a una traiettoria comune iniziative oggi parallele, per colmare più rapidamente il divario tecnologico con le principali economie digitali

Questi temi non pretendono di essere esaustivi, né di anticipare risposte che spettano a chi queste infrastrutture le regola, le gestisce o le studia ogni giorno. Possono essere un punto di partenza per il confronto e come agenda aperta per l'evoluzione delle comunicazioni sicure e mission-critical nei prossimi anni, più che come conclusione definitiva.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

18. Conclusioni

Guardando ai prossimi anni, tre movimenti sembrano destinati a consolidarsi. Il primo è una crescita sostenuta almeno fino alla metà del prossimo decennio, con tassi annui che, a seconda del perimetro considerato, oscillano tra il 7% e oltre l'11%. Il secondo è uno spostamento progressivo del valore dall'hardware al software: piattaforme di comando e controllo, strumenti di analisi dei dati, intelligenza artificiale e servizi gestiti pesano sempre di più nel budget delle organizzazioni. Il terzo è un'integrazione sempre più stretta tra mondo AI, mondo OT e comunicazioni, con il 5G Standalone e il satellite nel ruolo di abilitatori di mobilità, copertura e resilienza.

Intelligenza artificiale, 5G Standalone e satellite sono ingredienti strutturali delle comunicazioni critiche dei prossimi anni. L'intelligenza artificiale trasforma dati grezzi, allarmi, video, log, in indicazioni utilizzabili e può automatizzare parti del ciclo che va dalla rilevazione alla decisione fino all'azione, sempre nel rispetto dell'AI Act e sotto supervisione umana. Il 5G Standalone e lo slicing garantiscono che i servizi critici dispongano di risorse dedicate e di parametri di qualità realmente controllati. Il satellite offre la garanzia di continuità e di copertura negli scenari più estremi o remoti.

Un secondo ordine di considerazioni riguarda le dipendenze. Le comunicazioni critiche si reggono su infrastrutture fisiche concentrate, cavi sottomarini, satelliti, data center, e su catene di fornitura che attraversano più giurisdizioni. Governarle significa intendere la sovranità digitale non come chiusura del mercato, ma come capacità di scegliere le tecnologie, sostituire un fornitore e ripristinare rapidamente un servizio. Il principio del «compliant by design» può essere esteso in questa direzione: il momento in cui si verifica con chi si costruisce un'infrastruttura critica, e da chi essa dipende, è l'inizio del progetto, non la sua fine. Lo stesso vale per la crittografia: la logica dell'«harvest now, decrypt later» rende la migrazione verso algoritmi resistenti al calcolo quantistico un adempimento da pianificare oggi, con scadenze già scritte nel calendario regolatorio europeo.

Adottare fin dall'inizio standard di sicurezza, resilienza e tracciabilità allineati a NIS2, CER, AI Act, GDPR e, per il settore finanziario, a DORA, permette di trasformare un obbligo normativo in un vantaggio competitivo anziché in un costo di conformità.

Un'ultima considerazione riguarda il confine tra tecnologia e persone: la resilienza delle reti è una condizione necessaria, ma non sufficiente. Un'allerta tecnicamente perfetta produce effetti solo quando si accompagna alla comprensione del rischio da parte di chi la riceve, e può tradursi in una decisione praticabile. È quella che, nel capitolo 13, viene descritta come infrastruttura sociale per la sicurezza, complementare all'infrastruttura tecnologica.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Investire in competenze organizzative, formazione, simulazioni ed esercitazioni che coinvolgano più enti insieme è forse l'aspetto più rilevante: un sistema mission-critical perfettamente ridondato può comunque fallire se l'operatore in control room non sa utilizzarlo sotto la pressione di una crisi reale, o se il sovraccarico informativo generato da allarmi simultanei ne rallenta la risposta oltre la soglia utile.

La sfida per istituzioni, operatori e integratori nei prossimi anni sarà mettere insieme questi elementi in architetture end-to-end, sicure, resilienti, interoperabili, la cui resilienza sia verificata nel tempo, capaci di reggere un carico operativo crescente, minacce sempre più sofisticate e un'aspettativa di trasparenza e responsabilità che cittadini e mercati non sono più disposti a derogare. Come ha sintetizzato il Sottosegretario Butti, proteggere le comunicazioni significa proteggere la continuità dello Stato, la competitività delle imprese e la vita quotidiana dei cittadini: su questa responsabilità condivisa il Centro Studi COM.TEL. proseguirà il confronto avviato con la tavola rotonda del 1° ottobre.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Bibliografia e fonti

Le note a piè di pagina nel testo rimandano puntualmente alle fonti citate per ciascun dato; l'elenco seguente le raggruppa per argomento, con i riferimenti a testi normativi e standard tecnici non numerati puntualmente nel testo.

Ricerche di mercato

MarketsandMarkets, Critical Communication Market (marketsandmarkets.com/Market-Reports/critical-communication-market-95862445.html).

Mordor Intelligence, Critical Communication Market (mordorintelligence.com/industry-reports/critical-communication-market).

The Business Research Company, Mission Critical Communication Global Market Report (thebusinessresearchcompany.com/report/mission-critical-communication-global-market-report).

ResearchAndMarkets, Critical Communication Market e The Public Safety LTE & 5G Market (researchandmarkets.com).

Deloitte, Technology, Media & Telecommunications Predictions 2026 e The State of AI in the Enterprise 2026 (deloitte.com).

McKinsey, The State of AI in 2026 (mckinsey.com/capabilities/quantumblack/our-insights).

COM.TEL. Centro Studi, Unified Communications 2026: Prospettive, Innovazione Opportunità (https://www.comtelitalia.it/wp-content/uploads/2026/07/Unified-Communications_-2026-1.pdf)

COM.TEL. Centro Studi, Distributed Fiber Optic Sensing (DFOS): la fibra ottica che ascolta le infrastrutture (https://www.comtelitalia.it/wp-content/uploads/2025/12/Distributed-Fiber-Optics-Sensing_Centro-Studi-Comtel-Innovation.pdf)

ISTAT. Annuario statistico 2025

ANCI. Dossier sui piccoli comuni 2026

Sicurezza e normativa tecnica

IBM / Ponemon Institute, Cost of a Data Breach Report 2026 (ibm.com/reports/data-breach).

ENISA, NIS360 2026 (enisa.europa.eu, maggio 2026).

NIST, Special Publication 800-207, Zero Trust Architecture, e Post-Quantum Cryptography Standardization (nist.gov).

3GPP, TS 22.179, TS 22.280 e TS 23.280, Mission Critical Services (3gpp.org).

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Agenzia per la Cybersicurezza Nazionale, elenco dei soggetti NIS e provvedimenti attuativi del D.Lgs. 138/2024 (acn.gov.it).

Testi normativi

Direttiva (UE) 2022/2555, NIS2, e Direttiva (UE) 2022/2557, CER (eur-lex.europa.eu).

Regolamento (UE) 2024/1689, AI Act, e Regolamento (UE) 2026/1744, Digital Omnibus on AI (eur-lex.europa.eu; digital-strategy.ec.europa.eu).

Regolamento (UE) 2022/2554, DORA (eur-lex.europa.eu).

Regolamento (UE) 2016/679, GDPR (eur-lex.europa.eu).

Presidenza del Consiglio dei Ministri, Strategia Nazionale per la Resilienza dei soggetti critici, giugno 2026 (sicurezzanazionale.gov.it) https://www.governo.it/it/articolo/strategia-nazionale-la-resilienza-dei-soggetti-critici/32064

Golden Power (D.L. 21/2012, esteso dal D.L. 22/2019 "decreto Brexit" e dal D.L. 105/2019, rafforzato nel 2022 e ancora nel 2026.

EASA, Safety Information Bulletin su interferenze GNSS, aggiornamento luglio 2026, e piano congiunto EASA-EUROCONTROL (easa.europa.eu)

Commissione Europea, European Radio Navigation Plan, marzo 2024 (transport.ec.europa.eu)

AGCOM, delibera n. 106/25/CONS e Relazione annuale 2026 (agcom.it)

ITU-T, lavori di standardizzazione DFOS per reti telecom (itu.int)

Codice della Protezione Civile (D.Lgs. 1/2018)

Sendai Framework UNDRR, https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030

NIST, Post-Quantum Cryptography Standardization (FIPS 203, 204, 205, agosto 2024; HQC, marzo 2025);

Raccomandazione (UE) 2024/1101; NIS Cooperation Group, sulla transizione alla crittografia post-quantistica, 23 giugno 2025.

Commissione Europea, COM(2026) 13 final, proposta di direttiva che modifica la NIS2, 20 gennaio 2026

Commissione Europea, Action Plan on Cable Security, febbraio 2025

Commissione Europea, comunicato stampa sui Regional Cable Hub, 23 giugno 2026

MIMIT / Infratel Italia, aggiornamento SINFI alle infrastrutture subacquee, decreto ministeriale 28 agosto 2026

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Centro Studi TIM, Smart Infrastructure. Le infrastrutture italiane tra sfide e innovazione, 2025.

Relazione annuale sui poteri speciali (Golden Power) alle Camere, anno 2025

Comunicati aziendali e casi reali

Cisco, comunicati su Cisco Cloud Control e AgenticOps, giugno 2026 (news-blogs.cisco.com).

Ericsson, comunicazioni su applicazioni agentive per il RAN.

Gruppo FS Italiane, comunicato sulla sperimentazione 5G Torino-Milano, marzo 2026.

Terna, piano industriale e comunicati sull'innovazione di rete.

Gruppo Hera, comunicazioni sulla manutenzione predittiva.

Garante per la protezione dei dati personali, pareri e comunicati sullo schema di decreto legislativo in materia di biometria (garanteprivacy.it).

Autostrade per l'Italia, comunicati sul progetto Falco, monitoraggio con droni BVLOS, 2023-2024 (autostrade.it)

Autostrade dello Stato, piano investimenti 2025-2027 (autostradedellostato.it)

Cepav Due / Saipem, comunicati sul progetto di sicurezza dei cantieri Brescia Est–Verona (saipem.com)

Copernicus Emergency Management Service / EFFIS, European Forest Fire Information System (effis.jrc.ec.europa.eu)

INGV, Rete Sismica Nazionale e app INGVterremoti (ingv.it)

Agenda Digitale, "Infrastrutture connesse: l'IoT come strumento di protezione del territorio", caso torrente Bisagno, Genova (agendadigitale.eu)

AP Sensing / Teledyne SP Devices, documentazione tecnica su Distributed Acoustic/Temperature/Strain Sensing (apsensing.com)

ESA, progetti di rilevamento jamming e spoofing GNSS (esa.int)

Protective Action Decision Model di Lindell & Perry (2012, Risk Analysis)

Studi su Impact-base warning: Potter et al. 2018, Weyrich et al. 2018

Segmentazione del pubblico: Bartolucci et al. 2023

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Glossario

3GPP. Organismo internazionale che definisce gli standard delle reti mobili, incluse LTE, 5G e le loro evoluzioni.

AES-256-GCM. Algoritmo di crittografia simmetrica avanzata (Advanced Encryption Standard) con chiave a 256 bit operante in Galois/Counter Mode, che fornisce sia la riservatezza del dato sia l'autenticazione dell'integrità del messaggio.

Agentic AI. Agenti software basati su intelligenza artificiale capaci di pianificare azioni e supportare in autonomia parte delle decisioni operative, sotto supervisione umana.

AI – Artificial Intelligence. Intelligenza Artificiale. Insieme di tecniche computazionali che abilitano sistemi a apprendere, ragionare e prendere decisioni automatizzate o semi-automatizzate.

AI Act. Regolamento europeo sull'intelligenza artificiale (approvato nel 2024, vigore progressivo 2025–2026). Classifica i sistemi AI per livello di rischio (vietati, alto rischio, rischio limitato, rischio minimo) e impone obblighi proporzionati.

BVLOS. Beyond Visual Line of Sight, la modalità di pilotaggio di un drone oltre la linea visiva diretta dell'operatore, soggetta ad autorizzazione ENAC/EASA.

C4ISR. Comando, Controllo, Comunicazioni, Computer, Intelligence, Sorveglianza e Ricognizione: l'insieme integrato di funzioni su cui si basano le architetture di difesa moderne.

CAGR (Compound Annual Growth Rate). Tasso di crescita annuale composto. Misura la crescita media annua di un mercato nel tempo, normalizzando le oscillazioni annuali.

CER. la direttiva europea sulla resilienza delle entità critiche (UE 2022/2557), recepita in Italia con il D.Lgs. 134/2024.

CLI Calling Line Identification". (Identificativo del Chiamante) è il numero di telefono di chi avvia la chiamata.

Cloud Detection and Response (CDR). È una strategia (e classe di strumenti) nativa del cloud focalizzata sul monitoraggio in tempo reale, sul rilevamento delle minacce e sulla risposta automatica all'interno di infrastrutture multi-cloud e ibride. Analizza log di telemetria cloud, API, configurazioni e identità (IAM)

Data Act. Regolamento europeo (UE 2023/2854) che disciplina accesso, portabilità e riuso dei dati generati da prodotti e servizi connessi, inclusi i log delle piattaforme UC.

Data residency. Localizzazione geografica dei dati (dove sono conservati e trattati). Criterio chiave per GDPR, NIS2, Data Act e policy del Polo Strategico Nazionale.

DFOS. Distributed Fiber Optic Sensing, tecnologia che utilizza un cavo in fibra ottica come sensore continuo per rilevare vibrazioni, temperature e deformazioni lungo l'intera sua lunghezza.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Digital Twin – Gemello digitale. Replica virtuale dinamica di un asset fisico (edificio, impianto, infrastruttura), aggiornata in tempo reale con dati da sensori. Integrata con UC per prenotazione spazi, gestione sale e manutenzione predittiva.

DoS (Denial of Service). Un'azione che rende un server o un servizio incapace di funzionare o di rispondere agli utenti reali

ECDH (Elliptic Curve Diffie-Hellman). Protocollo di scambio delle chiavi crittografiche anonimo che consente a due entità di stabilire una chiave segreta condivisa su un canale insicuro, utilizzando le proprietà matematiche delle curve ellittiche.

Edge computing. Elaborazione dei dati in prossimità della fonte, anziché in cloud centralizzato. Riduce la latenza e migliora la reattività per applicazioni critiche come UC mobile e IoT industriale.

EFFIS. European Forest Fire Information System, il sistema europeo, basato su Copernicus, per la stima e il monitoraggio del rischio di incendi boschivi.

FRMCS (Future Railway Mobile Communication System). Lo standard che sostituirà il GSM-R come rete di comunicazione ferroviaria in Europa, basato su tecnologia 5G.

GDPR (General Data Protection Regulation). Regolamento UE 2016/679 sulla protezione dei dati personali. Quadro di riferimento per la privacy in Europa, con applicazione diretta a tutti i trattamenti di dati relativi a persone fisiche nell'UE.

Golden Power. Le reti di comunicazione elettronica a banda larga 5G e il cloud sono esplicitamente classificati come "attività di rilevanza strategica per la sicurezza nazionale", soggette a potere di veto del Governo su acquisizioni e forniture critiche D.L. 21/2012, esteso dal D.L. 22/2019 "decreto Brexit" e dal D.L. 105/2019, rafforzato nel 2022 e nel 2026.

GNSS. Global Navigation Satellite System, la famiglia di sistemi di posizionamento satellitare, tra cui il GPS e il Galileo europeo.

Hosted. Piattaforma UC installata presso data center del provider, in configurazione dedicata (single-tenant).

IoT (Internet of Things). Rete di dispositivi fisici connessi (sensori, attuatori, sistemi industriali) che raccolgono e scambiano dati. Integrazione crescente con piattaforme UC per gestione operativa e sicurezza IIoT (Industrial IoT)

IRSF. International Revenue Share Fraud, la frode telefonica che genera traffico automatico verso numerazioni internazionali a tariffazione maggiorata.

Jamming. L'interferenza intenzionale che disturba o rende indisponibile un segnale radio o satellitare.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

KMS (Key Management System). Sistema software e hardware dedicato alla generazione, distribuzione, archiviazione e revoca delle chiavi crittografiche utilizzate per proteggere i dati.

LMR / PMR (Land Mobile Radio / Professional Mobile Radio). Sistemi di comunicazione radio terrestri bidirezionali, analogici o digitali a banda stretta (es. standard TETRA, P25), storicamente utilizzati dalle forze di polizia, dai soccorritori e dalle utility.

MAOT*, Minimum Autonomous Operating Time*. Il numero minimo di ore di capacità operativa autonoma che un'infrastruttura critica dovrebbe garantire in assenza di connettività verso il centro.

MCPTT (Mission Critical Push-To-Talk). standard di comunicazione professionale definito dal 3GPP che garantisce chiamate vocali istantanee, sicure e con priorità assoluta su reti mobili (LTE e 5G) o Wi-Fi, pensato per le operazioni di emergenza e sicurezza pubblica.

MCUC (Mission-Critical Unified Communications). L'architettura che unisce le funzionalità delle Unified Communications aziendali alla resilienza delle reti mission-critical.

MCX (Mission-Critical Services). L'insieme dei servizi standardizzati dal 3GPP per le comunicazioni critiche a banda larga. Comprende MCPTT (Push-To-Talk vocale), MCVideo (streaming video in tempo reale) e MCData (messaggistica e dati operativi).

Modello ibrido. Architettura che combina componenti on-premise o hosted (per funzioni critiche) con servizi UC/UCaaS in cloud (per scalabilità e innovazione). Il modello prevalente nelle grandi organizzazioni europee.

Network Slicing. Tecnologia nativa delle reti 5G che consente di creare molteplici reti logiche virtuali e isolate sopra una singola infrastruttura fisica di rete, allocando a ciascuna di esse specifici parametri di sicurezza, banda e latenza.

NIS2 – Network and Information Security Directive 2. Direttiva UE 2022/2555, recepita in Italia con D.Lgs. 138/2024. Definisce requisiti minimi di cybersicurezza per circa 160.000 entità essenziali e importanti in 18 settori critici.

On-premise. Modello in cui la piattaforma UC risiede nei data center dell'organizzazione. Massimo controllo, ma richiede investimenti e competenze interne significative.

Operational Technologies (OT). Insieme di hardware e software utilizzati per monitorare e controllare dispositivi fisici, processi e infrastrutture all'interno di settori industriali e produttivi. A differenza dell'Information Technology, che gestisce i dati e i flussi informativi aziendali, l'OT agisce direttamente sul mondo fisico. L'ecosistema OT è composto da dispositivi specializzati che collegano il software ai macchinari:

- **PLC (Programmable Logic Controller):** Computer industriali robusti che ricevono dati dai sensori e comandano gli attuatori (es. avviare un motore).

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

- **SCADA (Supervisory Control and Data Acquisition):** Sistemi software di supervisione che monitorano interi impianti e raccolgono dati in tempo reale.
- **DCS (Distributed Control Systems):** Sistemi di controllo distribuiti utilizzati per gestire processi produttivi continui e complessi (es. raffinerie o impianti chimici).
- **HMI (Human-Machine Interface):** Schermi e cruscotti che permettono agli operatori umani di interagire con i macchinari.
- **Sensori e Attuatori:** I primi misurano grandezze fisiche (temperatura, pressione), i secondi compiono l'azione fisica.

PNT. Positioning, Navigation and Timing, l'insieme dei servizi di posizionamento, navigazione e sincronizzazione temporale forniti dai sistemi GNSS.

PQC (Post-Quantum Cryptography). Algoritmi crittografici progettati per essere sicuri contro gli attacchi informatici condotti sia da computer classici sia da futuri computer quantistici ad alte prestazioni.

PSIM. Physical Security Information Management, la piattaforma software che integra e correla in tempo reale dati da sensori, telecamere e droni per la sicurezza fisica di un sito.

RTP (Real-time Transport Protocol). Il protocollo standard di rete utilizzato per trasportare audio e video in tempo reale su reti IP. Di base non è cifrato.

SBC. Session Border Controller, il gateway che protegge e instrada con priorità le comunicazioni tra domini di rete diversi.

SCADA (Supervisory Control and Data Acquisition). Sistema informatico industriale utilizzato per il monitoraggio in tempo reale e il controllo di impianti fisici e infrastrutture geografiche, quali reti elettriche, gasdotti e acquedotti.

SIEM (Security Information and Event Management). La piattaforma centralizzata del SOC (Security Operations Center) che aggrega, normalizza e correla i log provenienti da qualsiasi fonte aziendale (firewall, server, PC, cloud) per scopi di conformità, investigazione storica e generazione di alert.

SIP – Session Initiation Protocol. Protocollo standard per l'avvio, la gestione e la chiusura di sessioni di comunicazione in tempo reale (voce, video, messaggistica) su reti IP.

SLA – Service Level Agreement. Accordo contrattuale che definisce i livelli di servizio garantiti (disponibilità, tempi di risposta, qualità). Elemento chiave nella valutazione di soluzioni UCaaS managed.

Spoofing (GNSS/CLI). La falsificazione di un segnale, satellitare o telefonico, per fornire a un ricevitore o a un utente un'informazione di posizione, orario o identità apparentemente valida ma alterata.

SRTP (Secure Real-time Transport Protocol). Estensione di RTP che fornisce cifratura, autenticazione dei messaggi, integrità e protezione dai messaggi duplicati (replay attack) per il traffico audio/video.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

TDM (Time Division Multiplexing). Tecnica che divide il tempo di trasmissione in piccoli intervalli per inviare più telefonate contemporaneamente sullo stesso cavo fisico

TLS (Transport Layer Security). Protocollo crittografico operante a livello di trasporto che garantisce privacy, integrità dei dati e autenticazione tra due applicazioni comunicanti (es. un client SIP e un server/PBX). Ha sostituito il vecchio protocollo SSL.

Toll fraud. La frode telefonica in cui un accesso compromesso viene utilizzato per generare traffico non autorizzato a carico della vittima.

UAS (Unmanned Aircraft Systems). Un sistema integrato che comprende il velivolo senza pilota (il drone o UAV), la stazione di controllo a terra (*Ground Control Station*), i link di comunicazione, i carichi utili (*payload*) e il supporto operativo.

UC – Unified Communications. Integrazione di voce, video, messaggistica, presence, conferencing e applicazioni aziendali in un'esperienza coerente.

UC&C – Unified Communications & Collaboration. Estensione della UC che aggiunge strumenti di collaborazione strutturata: workspace digitali, co-authoring, lavagne, gestione progetti.

UCaaS (Unified Communications as a Service). Modello di distribuzione basato su cloud che unifica molteplici canali di comunicazione aziendale (voce, video, chat, web-meeting) in un'unica piattaforma applicativa accessibile via internet.

URLLC (Ultra-Reliable Low-Latency Communications). URLLC è una famiglia di funzionalità 5G progettata per applicazioni che richiedono elevata affidabilità e bassa latenza. I valori effettivi dipendono dallo scenario, dalla configurazione radio, dal trasporto, dal core, dall'edge computing e dal livello di servizio adottato. Progettata per supportare applicazioni industriali e critiche (es. latenza di rete inferiore ai 10 millisecondi ed un'affidabilità di trasmissione prossima al 99,999%).

Vishing. Il phishing condotto tramite chiamata vocale, spesso con spoofing del numero chiamante, per indurre la vittima a fornire informazioni riservate.

VoIP – Voice over IP. Trasmissione della voce su reti IP. Base tecnologica della telefonia IP moderna, dei softphone e delle piattaforme UC.

Zero-Trust. Modello architetturale alla cybersecurity basato sul principio di non concedere mai fiducia implicita a dispositivi o utenti, imponendo la verifica continua dell'identità e del contesto di sicurezza per ogni singola richiesta di accesso alle risorse di rete.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Nota metodologica sulle fonti di mercato

I dati di mercato citati in questo white paper provengono da report pubblici di società di ricerca specializzate e sono riportati con la relativa attribuzione, segnalando le differenze di perimetro e di metodologia tra le fonti; vanno letti come indicatori di direzione e ordine di grandezza, non come previsioni precise. Per ogni fonte è indicata, ove disponibile, la data di pubblicazione; il lettore è invitato a consultare direttamente i report originali per dettagli metodologici e aggiornamenti successivi.

Centro Studi COM.TEL. S.p.a. – Tutti i diritti riservati

Limiti di responsabilità

Le informazioni e i dati contenuti nel presente documento sono forniti in buona fede e COM.TEL. S.p.a. li ritiene accurati alla data della pubblicazione. Gli autori hanno compiuto ogni ragionevole sforzo per garantire l'accuratezza delle informazioni al momento della pubblicazione. In nessun caso COM.TEL. potrà essere ritenuta responsabile per eventuali danni diretti o indiretti derivanti dall'utilizzo delle informazioni qui riportate.

I dati, le analisi, le ricerche, le opinioni o i punti di vista espressi da COM.TEL. S.p.a. non costituiscono evidenze di fatto né garanzie di risultato né costituiscono parere legale. I materiali contenuti in questo documento riflettono le informazioni e le valutazioni disponibili a settembre 2026 e sono soggetti a modifiche senza preavviso.

COM.TEL. S.p.a. non assume alcun obbligo di aggiornare i contenuti della presente pubblicazione, né potrà essere ritenuta responsabile per qualsiasi decisione di investimento, commerciale o di altra natura assunta sulla base delle informazioni qui contenute.

Per ulteriori informazioni:

COM.TEL. S.p.A.

Viale Piero e Alberto Pirelli, 10A

20126 Milano

https://www.comtelitalia.it

Documento redatto dal Centro Studi COM.TEL. – settembre 2026

Tutti i diritti riservati. Riproduzione consentita previa citazione della fonte.