COLPOFER

COLLABORATION DES SERVICES DE **POL**ICE **FER**ROVIAIRE
ET DE SECURITÈ

ANNUAL REPORT 2025

INDEX

In the 2025 COLPOFER Annual Report provides a summary of COLPOFER’s annual meetings, the activities and achievements of its Working Groups, and its involvement in significant international projects.

PREFACE

The year 2025 marked a pivotal moment for COLPOFER and its member organizations, as they continued to strengthen the security and resilience of Europe's railway systems in an ever increasingly complex and dynamic environment. Our efforts were guided by a clear vision: to foster cooperation, build robust public-private partnerships, and promote a strong security culture across all levels of the railway sector.

Throughout the year, COLPOFER served as a trusted forum for dialogue and collaboration among European railway operators, institutional stakeholders, and security institutions. COLPOFER cooperated in initiatives aimed at protecting critical infrastructure, mitigating emerging threats, and ensuring the continuity of safe and reliable rail transport. These actions reflect the organization's commitment to safeguarding railways as a cornerstone of sustainable mobility and economic connectivity.

A key priority in 2025 was the development of public-private partnerships, encouraging cooperation, enabling the integration of resources, expertise, and innovation to address evolving security challenges. Equally important was COLPOFER's focus on fostering a security culture, ensuring that awareness, responsibility, and proactive risk management become embedded practices across organizations and operational environments.

Looking ahead to 2026, COLPOFER will continue to build on these foundations by strengthening collaborative networks, leveraging technological advancements, and promoting harmonized standards across Europe. The objective remains clear: to enhance resilience, anticipate risks, and ensure that railway security evolves in step with the dynamic landscape of global mobility.

COLPOFER extends its sincere appreciation to all members, partners, and stakeholders for their dedication and contributions throughout 2025. Together, COLPOFER will continue to advance its shared mission of creating a secure and resilient railway system for Europe.

OUR MISSION

COLPOFER, established in 1980, is now a Special Group within the International Union of Railways (UIC) focused on enhancing the security and safety of the European railway network. Comprising 26* members from 22 countries, COLPOFER brings together railway police forces and security organizations from various railway companies to collaborate in addressing the growing challenges of criminal activity within the railway environment.

Its primary mission is to safeguard people, premises, trains, and sensitive information, ensuring a secure and reliable transportation environment for all. Through strong cooperation, COLPOFER facilitates the sharing of expertise, best practices, and intelligence among its members, enabling them to effectively combat crimes such as theft, vandalism, terrorism, and human trafficking.

In addition to operational cooperation, COLPOFER plays an instrumental role in the development and implementation of best practices aimed at improving security standards across the sector. These guidelines foster harmonised security approaches and contribute to enhancing the public perception of safety in railway transport. As a proactive community, COLPOFER continues to strengthen the resilience of Europe's railway system and its capacity to respond to evolving risks.

COLPOFER OBJECTIVES

Exchanging information and best practices in the fight against criminality in the railway environment

Defining a common railway security operational strategy and best practices for security solutions

Providing recommendations aimed at enhancing security levels and the perception of security

Fostering Public-Private partnerships to reach extensive and global goals

Footnotes:

* Following the departure of Romania's AGIFER from COLPOFER

COLPOFER MEMBERS

(As of 01/01/2026)

Austria: ÖBB

Belgium: SNCB

Croatia: HZ Infrastruktura

Czech Republic: České Dráhy

Denmark: DSB

Finland: FTIA

France: SNCF **-** Gendarmerie Nationale

Germany: Deutsche Bahn

Hungary: MAV-Start

Italy: FS **-** SNCF SVI **-** Polizia Ferroviaria

Latvia: LDZ SJSC

Luxembourg: CFL

Netherlands: NS N.V. **-** Eurail

Poland: PKP-PLK S.A.

Portugal: CP

Romania: AFER

Serbia: IŽS

Slovenia: SŽ

Spain: Renfe Operadora

Sweden: Trafikverket (Authority)

Switzerland: SBB

United Kingdom: EUROSTAR Ltd. **-** RDG

THE COLPOFER BOARD

President

Salvatore Iannicelli

Secretary General

Maria Cristina Fiorentino

Vice-President

Hendrik Vanderkimpen

Vice-President

Patrick Hennies

Board Member

Włodzimierz Kiełczyński

Board Member

Christophe Bouteille

The Vice-Presidency and Board are central to the organization, providing guidance, and decision-making to ensure the continued advancement of railway security across Europe. Their leadership is key to shaping policies and fostering collaboration among members, ensuring that COLPOFER remains at the forefront of addressing the evolving security challenges within the railway sector.

THE SECRETARIAT TEAM

Secretary General

Maria Cristina Fiorentino

Group Integrated Security FS

Paola Fasano

Group Integrated Security FS

Paolo Cavaliere

Group Integrated Security FS

Alessandro Dell'Oro

The COLPOFER Secretariat provides day-to-day coordination and support for the organisation's activities. It ensures continuity, communication, and effective cooperation among members.

Europe’s Security Posture in 2025:

A Hybridized Threat Landscape

Throughout 2025, Europe operated in a heightened and evolving security environment in which rail networks, as high-throughput, high visibility critical infrastructure, remained exposed to both sabotage and public-order disruptions that can rapidly cascade across national and cross-border corridors.

While 2025 did not generally resemble the earlier era of frequent, coordinated mass-casualty terrorist attacks, the more persistent pattern was cost-asymmetric disruption: low-complexity acts (e.g., fire-setting, cable damage, track interference, station occupations) generating outsized operational and economic impacts, while simultaneously stretching protective security, incident response, and investigative bandwidth.

Across open-source security assessments, this environment was increasingly described as a hybrid threat space, where attribution is difficult, proxies and opportunistic actors can be leveraged, and the strategic objective is often to normalize disruption rather than to maximize casualties. In parallel, terrorism-related risk remained elevated in Europe’s public spaces, with Europol reporting continued terrorism activity and interdictions in the EU context (as captured in the EU TE-SAT 2025[1] reporting cycle), reinforcing that transport hubs and crowded venues remain salient in extremist targeting considerations even when many plots are disrupted upstream.

Rail Networks as Strategic Targets

Rail infrastructure remained one of the most systematically targeted assets in 2025 because it concentrates economic throughput, depends on physically distributed and often accessible technical subsystems, and is difficult to harden uniformly at scale.

A case illustrates how simple methods can scale into national disruption. On 31 July 2025, a fire in a cable duct on the key Düsseldorf–Duisburg[2] rail link triggered widespread disruption, with police investigating suspected sabotage and reporting that accidental causes were ruled out, an ignition device had been placed, underscoring the vulnerability of signaling and communications conduits in high-density corridors.

Crucially, the incident did not remain singular. Within roughly a day, German police reports described a second arson attack on the same strategic corridor, with police indicating the device showed similar characteristics to the first. An escalation pattern consistent with “probing” behavior against known weak points.

A second, distinctly strategic 2025 rail security data point comes from Poland, where reporting described an explosion damaging a railway track on a line leading toward Ukraine, with subsequent Polish statements framing it as sabotage designed to cause catastrophe. In related coverage, the Associated Press[3] broader tracking of suspected Russia-linked disruption in Europe explicitly includes several rail incidents in Poland and more throughout Europe (including explosives detonating on rail lines), illustrating how rail infrastructure sits

Sources:

1. TE-SAT 2025 (Europol);
2. DW and BR24 reporting on the Düsseldorf–Duisburg incidents; Europol; UIC; IISS analysis of sabotage trends (Edwards);
3. AP project on “Russia resource-draining” sabotage campaigns (Burrows); NATO statements on hybrid activity patterns; Security Matters on youth radicalization trends. ENISA’s Threat Landscape 2025

inside a hybrid “grey-zone” contest intended to impose costs and consume security resources.

These rail sabotage examples align with the International Institute for Strategic Studies (IISS) [1] assessment that frames Non-state actor sabotage activity in Europe as an asymmetrical “unconventional war” designed to destabilize European governments, impose socioeconomic costs, and undermine support for Ukraine, often through decentralized activity and the use of proxies recruited online, which complicate attribution and response.

Operationally, the recurring rail-sabotage traits visible in 2025 remain consistent with this pattern: (**i**) interference with signaling, power, and communications subsystems; (**ii**) reliance on simple methods such as arson against accessible infrastructure; and (**iii**) concentration on high-traffic nodes that maximize ripple effects across passenger and freight services.

Politically Motivated Public-Order Disruptions: Rail as a Chokepoint

Beyond covert sabotage, 2025 also demonstrated how rail networks become immediate chokepoints during politically motivated mass mobilization, particularly when protests and strikes converge on stations, track access, and station approaches.

In Italy, pro-Palestinian protest activity repeatedly intersected with rail operations. In September 2025, major demonstrations and a transport-impacting strike produced train delays and reduced urban public transport, with reported clashes at Milano Centrale railway station as demonstrators attempted to enter the main station, and police intervened.

Pro-Pal Protests in Italy in 2025

The same day, Italy’s nationwide protest/strike environment was explicitly described as disrupting trains and transit services across major cities, illustrating that even when the trigger is political (not criminal), the operational effect on rail can resemble a security incident: crowding, access control pressure, cascading delays, and heightened risk of confrontation in station environments. Italy also saw more direct rail stoppage actions; hundreds of pro-Palestinian protesters blocked trains at Pisa railway station, entering the station and occupying a platform, with train traffic halted at the time of reporting.

From a rail-security perspective, this is a high-signal example of “soft target” vulnerability: A relatively low complexity crowd action can suspend service and force rapid decisions on public order policing, passenger safety, and continuity of operations especially during peak commuter flows.

Sources:

1. IISS analysis of sabotage trends (Edwards); NATO statements on hybrid activity patterns; Security Matters on youth radicalization trends.

Cyber-Physical Convergence: Why 2025 Reinforced “Resilience” as the Rail Priority

Although the focus is often placed on physical disruption, Europe’s 2025 security posture is increasingly defined by convergence, where cyber pressure, hacktivism, and physical interference coexist and can compound impacts on transport continuity. ENISA’s Threat Landscape 2025[1] (covering July 2024–June 2025) characterizes Europe’s cyber threat environment as both mature and converging, with transport identified as a repeatedly targeted sector and ideologically motivated activity (including hacktivist-style operations) comprising a significant share of observed incidents.

Meanwhile, IISS’s 2025 assessment[2] emphasizes that Europe’s critical infrastructure remains vulnerable not only because of adversary intent but also because ageing systems, deferred maintenance, and fragmented ownership/governance create single points of failure that can yield cascading cross-border disruption conditions that rail networks exemplify.

In 2025, this convergence was further complicated by the growing security relevance of drones. Drones broaden the threat surface by enabling low-cost hostile reconnaissance (including surveillance of sensitive rail premises and railyards) and potential disruption, adding an aerial layer to traditional perimeter and corridor security challenges. At the EU level, the European Commission has highlighted “hostile overflights,” airspace violations, and disruptions affecting critical infrastructure and transport hubs as part of the evolving drone threat environment, reinforcing that drone incidents increasingly sit within the same resilience agenda as cyber and physical protection.

A central operational constraint in this area is the uneven maturity of response powers and procedures. Within the rail security community, the absence of established procedures is acknowledged, underscoring a lack of standardized playbooks for rapid detection and escalation in the rail domain. In parallel, public reporting on critical-infrastructure protection highlights that only a limited set of law-enforcement bodies typically hold authority to intercept or neutralize drones, while governments debate whether and under what conditions critical-infrastructure operators should be granted powers, because continuous state coverage of all sites is not always realistic. The result is a recurrent gap between the speed of drone-enabled activity and the speed of lawful, coordinated mitigation.

Taken together, the 2025 rail-security lesson is less about isolated events and more about sustained pressure: simultaneous risks from sabotage, protest-driven disruption, and the broader hybrid ecosystem, now including drone-enabled reconnaissance and disruption, where low-cost actions can continuously consume investigative and protective resources, particularly when legal authority and operational procedures for counter-drone action remain unclear or unevenly developed.

Sources:

1. ENISA’s Threat Landscape 2025; 2. IISS analysis of sabotage trends (Edwards)

Conclusions

The year 2025 showed continuity under hybrid pressure: rail networks remained a favored disruption vector, not necessarily because actors sought mass casualties, but because rail offers a uniquely efficient pathway to systemic disruption.

The year's concrete rail examples underline three board level realities:

- **High impact fragility of rail technical subsystems :** low cost, high impact targeted damage to signaling communications infrastructure can paralyze an essential corridor, and repeated attacks can rapidly amplify disruption.

- **Strategic rail relevance in geopolitical contestation :** Associated Press documentation of rail incidents within a wider sabotage campaign highlights rail's role in broader security competition tied to the war in Ukraine.

- **Rail as a political chokepoint** : Pro Palestinian mobilizations demonstrate how stations and platforms can become immediate pressure points for public order, with measurable impacts on train punctuality, station access, and passenger safety management. This creates an environment conducive to vandalism, graffiti, theft, and other forms of criminal activity.

In recent years, DG MOVE and DG HOME projects activities often focused on low probability, high impact threats such as terrorism, and less attention has been paid towards daily petty crimes, for example vandalism, graffiti, aggression, and related phenomena. As stated above, reducing such crimes remains a daily focus for the rail sector and is paramount to the feeling of security and perception of EU citizens. Over time, repeated minor incidents can compound into operational friction and reduced confidence in service continuity.
This balance matters because the same rail system that is exposed to sabotage and public order disruption is also persistently affected by recurrent threats that shape passenger confidence and daily operational stability. In this sense, resilience and continuity must be designed not only for exceptional events but also for sustained, cumulative pressure.

Strategically, this holistic approach means rail security must be organised around endurance and recovery, not just acute response. Resilience becomes the organising principle: hardening critical assets, building redundancy in signalling and power, and developing rapid recovery capabilities that sustain service continuity even under pressure. This requires operational continuity plans that prioritise keeping trains moving (or restoring operations quickly) while maintaining public trust, recognising that disruption itself is increasingly the objective, "better intelligence fusion" should be understood as real time information integration between operators and law enforcement so that emerging patterns (repeat attacks, probing behaviour, or coordinated public order pressure at nodes) can be detected early and mitigated consistently across borders. In this model, intelligence is not only a strategic product; it is an operational input that informs dynamic staffing, access control, protective measures, and recovery sequencing.

Sources:

TE-SAT 2025 (Europol); DW and BR24 reporting on the Düsseldorf–Duisburg incidents; Europol; UIC; IISS analysis of sabotage trends (Edwards); AP project on "Russia resource-draining" sabotage campaigns (Burrows); NATO statements on hybrid activity patterns; Security Matters on youth radicalization trends. ENISA's Threat Landscape 2025

The same approach supports the response to recurrent threats: better understanding the scale of the problems at European level, enhancing cooperation with authorities to address these threats, and seeking technological solutions help mitigate related risks and support the rail community as a whole. This also provides a concrete way to balance the high focus on geopolitical disruption with the continuous work on usual threats such as graffiti, aggressions, and where relevant fraud, without changing the overall strategic framing.

Recurrent threats shape the daily operating environment, absorb resources, and influence how passengers perceive order, safety, and reliability. Graffiti is a clear example of how what is often framed as petty crime can move closer to sabotage dynamics. Repeated intrusions and targeted damage can extend restoration time and create recurring vulnerability points. In periods of heightened social tension, graffiti and aggression may also become more visible and more tightly associated with political movements and protests, reinforcing public order pressure in stations and on trains. Where relevant, fraud adds a further layer of persistent pressure, consuming capacity and affecting trust in systems and processes.

Finally, these requirements are difficult to meet in isolation. Structured collaboration through working groups, communication channels, and formalised partnerships supports interoperability, efficient and effective planning, and scalable response. This structured collaboration remains essential both for high impact disruption and for recurrent threats that continuously affect daily operations and the public perception of security. Collaboration supports earlier detection of patterns, more consistent approaches across borders, and faster circulation of practical countermeasures. It also reinforces alignment between operators and authorities so that prevention, response, and recovery remain joined up across jurisdictions, sustaining resilience not only in crisis moments but across everyday operations where public confidence is built or lost.

Sources:
TE-SAT 2025 (Europol); DW and BR24 reporting on the Düsseldorf–Duisburg incidents; Europol; UIC; IISS analysis of sabotage trends (Edwards); AP project on "Russia resource-draining" sabotage campaigns (Burrows); NATO statements on hybrid activity patterns; Security Matters on youth radicalization trends. ENISA's Threat Landscape 2025

COLPOFER GENERAL ASSEMBLIES

79th COLPOFER GENERAL ASSEMBLY

The 79th General Assembly of COLPOFER was held at the historic Pietrarsa Railway Museum in Naples on June 18–19, 2025, hosted by Ferrovie dello Stato Italiane. The event gathered 47 representatives from 21 organizations across 17 countries, reaffirming COLPOFER's role as a leading platform for collaboration on railway security.

The President, Salvatore Iannicelli, opened the assembly, and a new COLPOFER video was presented, with an invitation for members to contribute media content to create a comprehensive representation of the organization.
The assembly marked significant leadership changes. Patrick Hennies, Chief Security Officer at Deutsche Bahn, was unanimously elected to the COLPOFER Board, succeeding Frank Reitsma following his retirement. Mr. Hennies also accepted the position of Vice President. New chairpersons were appointed for key working groups: Kirsten Verlaan from NS will lead the Terrorist and Extremist Activities group, while Daria Kardel from PKP will chair the Graffiti group.

Group Photo of the participants of the 79th COLPOFER General Assembly in Pietrarsa

The General Assembly agreed to the creation of new working groups focused on Freight and Special Transport, Economic Crime in large-scale projects, and the implementation of the CER Directive.

A key milestone of the assembly was the signing of the Memorandum of Understanding between COLPOFER and UITP, strengthening collaboration on security standards and best practices across public transport networks. Another major topic was the implementation of the EU Critical Entities Resilience Directive.

FS presented Italy's approach, which includes legislative measures, resilience assessments, and the development of a Group Resilience Plan and Business Continuity Framework. European Railways are to be designated as a critical entity of importance due to being essential services to economic and societal functioning, as well as cross-border operations. Members agreed on the need for greater cooperation, data sharing, and the establishment of a dedicated working group to support compliance with the directive.

FS Security, the security provider for the FS Group, presented its operational organization. The company monitored passengers and trains, maintaining strong fraud prevention measures. FS Security is investing in advanced technologies such as video analytics, CCTV, and drones, while expanding training programs and infrastructure to enhance passenger safety.

Working Group presentations provided insights into emerging trends and challenges.

The Terrorist and Extremist Activities Working Group reported an increase in lone-actor attacks and proposed creating a sabotage modus operandi database. The Major Events Working Group suggested relocating coordination centers to host countries and focusing each session on a single topic to improve efficiency. The Ticket Fraud Working Group highlighted the rise of online scams and GPS spoofing in mobile ticketing applications, while the Graffiti Working Group noted stable or declining incidents thanks to security measures, although new trends such as politically motivated graffiti and the use of drones for surveillance were observed.

The UIC Security Platform update emphasized international collaboration on railway security, focusing on crisis management, human factors, and emerging threats such as sabotage and metal theft. Current priorities include protecting vulnerable populations, combating human trafficking, and addressing low-probability, high-impact risks like CBRNe incidents. EU-funded projects such as IMPRESS, ODYSSEUS, CYRUS, SafeTravellers, CBRNe4rail, and BEHOLDER aim to strengthen resilience through advanced technologies, including artificial intelligence and drones. Practical outputs such as training modules, awareness campaigns, and serious games are being developed to enhance preparedness across the rail sector.

The 79th General Assembly reaffirmed COLPOFER's commitment to security, resilience, and innovation. Through strategic partnerships, regulatory compliance, and technological advancement, the organization continues to ensure that the railway sector remains robust against evolving threats while fostering international cooperation.

2nd COLPOFER-RAILPOL SYMPOSIUM

On June 18–19, 2025, the historic Pietrarsa Railway Museum hosted the second COLPOFER Symposium, gathering 47 representatives from 21 organizations across 17 countries. Organized by Ferrovie dello Stato, the event provided a platform for collaboration among railway operators, law enforcement, and institutional stakeholders to address emerging security challenges.

The symposium focused on three critical themes: aggression against railway staff and passengers, sabotage of infrastructure, and public order during major events. Opening remarks by COLPOFER President Salvatore Iannicelli and contributions from leading experts, including Francesca Monaldi, the Head of Italian Railway Police, and Christophe Gradel, President of RAILPOL, emphasized the strategic importance of rail security in today's geopolitical context.

Aggression in the railway environment emerged as a pressing concern, with data showing rising incidents across Europe. Preventive measures such as staff training, public awareness campaigns, and technologies like bodycams and AI-powered CCTV were highlighted as essential tools to protect personnel and passengers.

Similarly, discussions on sabotage underscored the vulnerability of critical infrastructure to low-cost, high-impact attacks. Experts called for stronger intelligence sharing, advanced detection systems, and proactive planning to counter these threats.

Public order during major events was another key topic, with speakers outlining structured approaches combining legal rigor and operational adaptability. Strategies include phased planning, real-time monitoring, and post-event evaluations to ensure resilience while safeguarding civil liberties.

The symposium also addressed broader disaster preparedness, notably Italy's national plan for volcanic risks in the Campi Flegrei and Vesuvio areas, and examined lessons from the April 2025 blackout in Spain and Portugal, which exposed systemic vulnerabilities and reinforced the need for contingency planning and resilient communication networks.

Representatives from the ATLAS network of Police Special Forces showcased a training exercise they participated in, illustrating advanced police tactics, coordinated response procedures and the role of joint exercises in strengthening operational readiness and interoperability among European law-enforcement units operating in the rail environment.

80th COLPOFER GENERAL ASSEMBLY

The 80th General Assembly of COLPOFER was convened in Warsaw from November 26 to 28, 2025, under the strategic theme “Railway Security of the Eastern Flank of the European Union.” This landmark event reaffirmed COLPOFER’s role as a leading platform for collaboration among European railway security stakeholders, addressing emerging challenges and reinforcing the resilience of critical transport infrastructure.

The Assembly commenced with an official welcome by COLPOFER President Salvatore Iannicelli, followed by opening remarks from Piotr Wyborski, President of PKP Polskie Linie Kolejowe S.A., and senior representatives from the Ministry of Infrastructure and Frontex. These interventions underscored the importance of coordinated action to safeguard rail networks against geopolitical risks and operational threats.

Throughout the day, participants engaged in high-level discussions and presentations on priority topics, including border security measures, cooperation with national authorities, and strategies to counter theft, vandalism, and cyber threats. Presentations by representatives from Straż Ochrony Kolei (SOK) and PKP S.A. highlighted operational best practices and innovative initiatives such as the “Safe Level Crossing” campaign. The European Commission provided insights into strengthening the security resilience of the EU railway network, emphasizing the need for harmonized standards and cross-border collaboration.

The afternoon sessions focused on COLPOFER’s specialized working groups, which reported on progress in their respective areas:

The Graffiti Working Group presented a consolidated assessment of evolving vandalism trends affecting European railways, highlighting new operational patterns such as daytime attacks, “SprayCations,” the use of drones and hidden cameras, and acid-based markers. As concrete outputs, the group reported enhancements to countermeasure toolkits, including coordinated police cooperation models, targeted K-9 patrol deployments, and the adoption of advanced detection technologies. The group also reinforced information sharing on offenders’ modus operandi to support preventive strategies.

The Fraud and Ticket Forgery Working Group reported tangible progress in documenting and comparing fraud-prevention measures across members. Key outputs included the consolidation of practices on real-time ticket validation, the use of analytics to detect abnormal purchasing or validation patterns, and the alignment of digital and physical document security approaches. The group emphasized that these outputs are already supporting more proactive fraud detection and cross-border knowledge transfer among operators.

The Terrorism and Extremist Activities Working Group reported on its continuous monitoring of the evolving threat landscape affecting European railways. Outputs presented included updated threat assessments reflecting the persistence of lone-actor radicalisation, ideologically motivated networks, and the increasing convergence of physical and cyber tactics. The group highlighted its analytical contribution in identifying transport infrastructure as a recurring symbolic target, supporting members' situational awareness and preventive planning.

The newly established CER Working Group, chaired by SNCF, reported on its initial outputs aimed at supporting members' implementation of EU Directive 2022/2557. The group delivered a first structured exchange on national transposition challenges, with a particular focus on incident reporting obligations, supply-chain resilience, and the practical implications of prolonged service disruptions. This meeting demonstrated the variety of approach of the current situation regarding business continuity and the steps outlined by each member to comply with a regulation that is still being discussed at state level'

The Freight and Special Transport Working Group and the Economic Crime Working Group are new as of 2025 and are scheduled to start their activities in 2026.

Furthermore, the Brenner Group was presented as a renewed platform for cross-border railway security cooperation along one of Europe's most critical transit corridors. Bringing together railway security services and police authorities from Austria, Germany, Switzerland, Liechtenstein, and Italy, the group is resuming its activities with a focus on enhanced information sharing, structured incident reviews, and the planning of joint operational exercises, reinforcing coordinated responses to shared security challenges.

The 80th COLPOFER General Assembly marked a significant step forward in strengthening the security and resilience of Europe's railway systems. By fostering dialogue, sharing expertise, and promoting coordinated action, COLPOFER continues to support its members in safeguarding rail transport as a vital component of sustainable mobility and economic connectivity.

COLPOFER WORKING GROUPS 2025

COLPOFER Working Groups in 2025

Terrorist and Extremist Activities Working Group

MEMBERS: SNCB, FTA, SNCF, Gendarmerie Nationale, FS Italiane, SNCF Voyages, LDZ SJSC, NS N.V., PKP, CP, RENFE Operadora, Trafikverket, EUROSTAR, and Railpol.

The Terrorist and Extremist Activities Working Group supports COLPOFER by enhancing cooperation on the prevention of terrorism, extremist violence, and sabotage affecting the railway sector, through the comparison of national measures and the development of common approaches.

Meeting held in 2025

- 10 April, hosted by SBB in Bern, Switzerland.
- 12 November, hosted at CP Headquarters, Lisbon, Portugal.

In 2025, the Group focused on the exchange of information on past incidents and attacks, the prevention of sabotage against railway infrastructure, and the assessment of recent threat events across Europe, including suspicious objects and bomb threats. Activities also covered comparisons of national threat levels, the evaluation of new technologies such as portable X-ray solutions for unattended luggage, and the analysis of insider threats.

From top to bottom; Kirsten Verlaan, Chair of Terrorism and Extremist activity, 10th April Group Photo, 12 November working session.

Graffiti Working Group

MEMBERS: SNCB, SNCF, FS Security, NS N.V., PKP, Renfe Operadora, and SBB, DSB, MAV-Start, ÖBB.

The Graffiti Working Group supports COLPOFER by strengthening cooperation among members and promoting the exchange of best practices to reduce graffiti-related damage to rolling stock and railway infrastructure, while ensuring effective network protection. The Group encourages a shared approach to graffiti prevention and response and advocates for the recognition of graffiti not only as an economic and operational issue, but also as a security concern, particularly when linked to organised or cross-border activities.

Meetings held in 2025

- 8 May 2025 in Vienna, Austria. Hosted by ÖBB.
- 26 November 2025 in Warsaw, Poland. Kindly Hosted by PKP.

In 2025, the Working Group focused on the exchange of information regarding international graffiti incidents, including cases involving foreign crews operating in other countries. Activities included the sharing of best practices for graffiti prevention and mitigation, strengthened cooperation with police forces, law enforcement authorities, and institutional partners, and efforts to enhance collaboration among affected stakeholders. Discussions highlighted the importance of prompt graffiti removal as a key deterrent to reduce public visibility, acknowledged that caught-in-the-act cases remain rare in several countries, and addressed data collection, database creation, and emerging graffiti group *modus operandi*.

From top to bottom; Daria Kardel Chair of Graffiti, 26th November Group photos

Fraud & Ticket Forgeries

MEMBERS: ÖBB, SNCB, ČD České dráhy, DSB, SNCF, MAV-Start, FS Security, SNCF Voyages, NS N.V., Eurail Group G.I.E., PKP, ŽSR, SŽ, SBB, EUROSTAR International Limited, and the Rail Delivery Group (RDG)

The Fraud and Ticket Forgery Working Group supports COLPOFER by monitoring trends in ticketing and payment fraud across members and promoting the exchange of countermeasures to limit revenue loss and protect customers. The Group addresses both traditional and emerging fraud schemes linked to digitalisation and evolving ticketing models.

Meeting held in 2025:

- 8 May 2025 held Online
- 6–7 November, kindly hosted by SNCF in Paris

The Working Group focused on real-time information exchange and best practice sharing related to ticket forgeries and credit card fraud. Particular attention was given to the growing use of fake websites and social media pages impersonating official railway operators. The Group also examined fraud affecting pay-as-you-go mobile ticketing systems, including GPS spoofing to avoid fare calculation, as well as risks linked to e-wallet payment fraud and phishing.

Activities further covered the introduction of pay-as-you-go solutions, the implementation of control gates in major stations, and the evaluation of control process efficiency through electronic devices. The Group also advocated for regulatory adaptations, supported the creation of alerts and training materials.

From top to bottom; Carla Zaffiro, Chair of Fraud & Ticket Forgery, 6-7 November Session and Group Photos.

Major Events & Control Room

MEMBERS: SNCB, SNCF, FS Security, SNCF Voyages, and NS N.V.

The Major Events Working Group supports COLPOFER by coordinating communication among members during major international events, with the aim of improving security measures and ensuring timely and effective information exchange. Closely linked to this activity, the Control Room Sub Working Group enhances operational communication between the security control rooms of European railway companies, enabling coordinated responses to incidents during high-impact events.

Meeting held in 2025

- 14 May 2025, held online

In 2025, the Working Groups focused on real-time information sharing related to railway transport requirements for major events at both the national and international levels. Activities included the development of security planning for railway transport during major events, the strengthening of operational communication between railway companies, and the exchange of best practices concerning control room management and technological tools. The Groups also promoted closer cooperation between the Terrorism Working Group and the Control Room community.

From top to bottom; Gaetan Carlens, Chair of Major Events and Control Rooms, DB Control Room, SOK Control Room

Pan-European Corridor X

MEMBERS: ÖBB, ZRS, Hzi HZ Infrastruktura, and SŽ Slovenske železnice.

The Pan-European Corridor X Working Group addresses cross-border security challenges along Corridor X through targeted risk assessment, preventive measures, and case analysis. The Group supports cooperation among railway operators, law enforcement authorities, and other cross-border stakeholders, underpinned by data and information exchange and the sharing of best practices. Its work aims to enhance situational awareness and contribute to greater security harmonisation across the Corridor.

The Working Group does not operate as a permanently scheduled forum. Instead, it is activated on a bilateral, as-needed basis, in response to specific operational requirements raised by participating members and organisations along the Pan-European Corridor X.

The Group's activities focus on the analysis of security threats affecting Corridor X railways, including the monitoring and reporting of illegal migration routes and evolving terrorist threat levels, notably in connection with wider geopolitical developments. Work also includes data and information exchange, best practice sharing, and the analysis of security-related legislation. Bilateral meetings are held with relevant members and organisations to address emerging risks and coordinate preventive measures.

From top to bottom; Dora Mezek-Kukec, Chair of Pan-European Corridor X

New COLPOFER Working Groups in 2025

The **Freight and Special Transport** Working Group focuses on enhancing the security of freight and special transport across the European railway network. Its activities are centred on aligning security policies, operational procedures, and technological requirements along the Trans-European Transport Network (TEN-T), with particular attention to sensitive, high-value, and military transport.

In light of the current geopolitical context, the Group has placed increasing emphasis on military mobility and the resilience of rail freight corridors, recognising the railway system as a critical enabler for defence readiness and strategic mobility. Strengthening the protection, continuity, and reliability of freight rail operations has therefore become a key priority to support both civilian and military transport needs across Europe.

The **Economic Crime** Working Group addresses the rising risks of financial crime across the railway sector, particularly in large-scale, long-term infrastructure and construction projects. Given the complexity and often cross-border nature of supply chains, these projects face heightened exposure to offenses such as corruption, price-fixing, invoice fraud, and both internal and external misconduct. The Working Group fosters collaboration among members to identify vulnerabilities, share best practices, and strengthen preventive and detective controls.

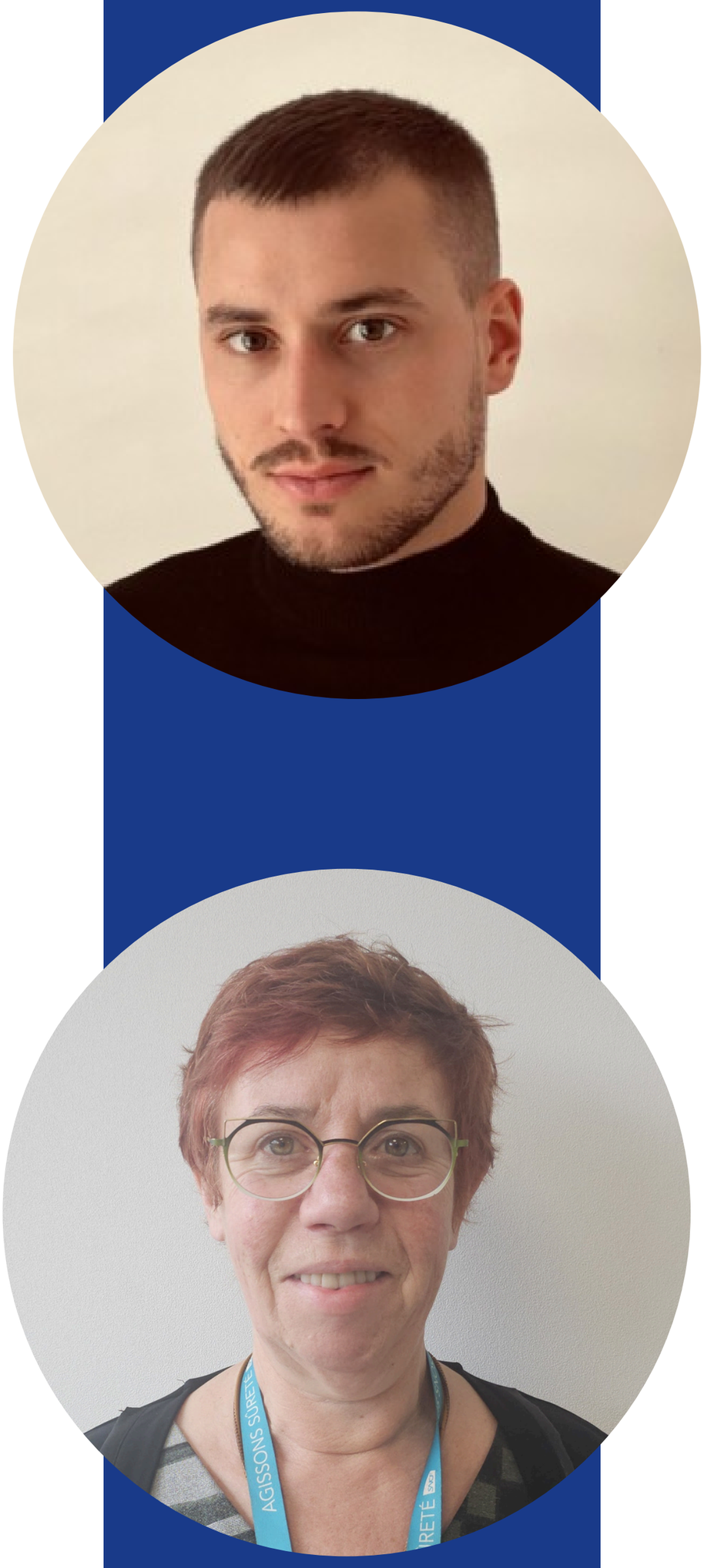
From top to bottom; Galina Bolich Chair of Freight and Special Transport, Tom Woodson, Chair of Economic Crime

New COLPOFER Working Groups in 2025

The **Brenner Group** Working Group strengthens cross-border railway security cooperation along the Brenner corridor, one of Europe's busiest transit routes, by bringing together railway undertakings and competent authorities. Originally established around 1999, the Group is being revitalised within the COLPOFER framework to continue its core mission of practical, operational collaboration.

Priorities include enhanced information sharing, structured reviews of security-critical incidents and lessons learned, and the planning and implementation of joint security operations with rail security units and police forces. The Group supports preparedness for events and major gatherings, most notably preparations for the Milano–Cortina 2026 Winter Olympics.

The **CER** Working Group supports COLPOFER members in addressing the requirements of the EU Critical Entities Resilience Directive (EU) 2022/2557. Through knowledge sharing and coordinated implementation efforts, it assists members in ensuring compliance with the Directive and in reinforcing the ability of railway entities to prevent, withstand, respond to, and recover from disruptive events.



From top to bottom; Hasan Sulic, Chair of the Brenner Group. Anne Nouvel, Chair of CER

COLPOFER EXTERNAL PARTNERS

COLPOFER

UIC

COLPOFER operates as a **Regional Special Group** within UIC to strengthen cooperation and coordination on railway security priorities.

EUROPEAN COMMISSION

COLPOFER engages with the European Commission (including **DG MOVE LANDSEC**) to align on EU transport-security priorities.

UITP

COLPOFER and UITP signed a **Memorandum of Understanding** to strengthen cooperation with the UITP Security Committee.

EUROPOL

COLPOFER is developing a **Working Arrangement** with EUROPOL to establish cooperative relations and reinforce information exchange.

CER

CER is included among COLPOFER's external partnerships as a European **railway-sector stakeholder** for dialogue and coordination.

RAILPOL

COLPOFER partners with RAILPOL under a **cooperation agreement** to enable joint initiatives.

COLPOFER's external partnerships are a cornerstone of its mission to enhance railway security through cooperation and shared responsibility. In line with this approach, COLPOFER endorses partnership agreements and joint projects with European institutions, security associations, and international stakeholders, including UIC Security Platform, the European Commission (LANDSEC, Working Party on Rail Security), the International Working Group on Land Transport Security (IWGLTS), RAILPOL, UITP, CER, and EUROPOL. These relationships help strengthen information sharing and coordination, reinforce synergies, and support practical cooperation frameworks.

COLPOFER

UIC

COLPOFER operates as a **Regional Special Group** within UIC to strengthen cooperation and coordination on railway security priorities.

EUROPEAN COMMISSION

COLPOFER engages with the European Commission (including **DG MOVE LANDSEC**) to align on EU transport-security priorities.

UITP

COLPOFER and UITP signed a **Memorandum of Understanding** to strengthen cooperation with the UITP Security Committee.

EUROPOL

COLPOFER is developing a **Working Arrangement** with EUROPOL to establish cooperative relations and reinforce information exchange.

CER

CER is included among COLPOFER's external partnerships as a European **railway-sector stakeholder** for dialogue and coordination.

RAILPOL

COLPOFER partners with RAILPOL under a **cooperation agreement** to enable joint initiatives.

COLPOFER's external partnerships are a cornerstone of its mission to enhance railway security through cooperation and shared responsibility. In line with this approach, COLPOFER endorses partnership agreements and joint projects with European institutions, security associations, and international stakeholders, including UIC Security Platform, the European Commission (LANDSEC, Working Party on Rail Security), the International Working Group on Land Transport Security (IWGLTS), RAILPOL, UITP, CER, and EUROPOL. These relationships help strengthen information sharing and coordination, reinforce synergies, and support practical cooperation frameworks.

External Partnerships in 2025

UIC Security Platform

COLPOFER strengthened its engagement within the UIC Security Platform's governance by being represented among the Steering Committee members and contributing to alignment on priorities and coordination actions. In parallel, COLPOFER continued to represent region Europe within the UIC Security Platform by clarifying respective scopes and roles, fostering mutual participation in strategic bodies and working groups.

In 2025, COLPOFER participated in the 20th UIC World Security Congress, held in Rabat from 2 to 4 December and jointly organised by UIC and ONCF. The Congress brought together international railway stakeholders to discuss future challenges in railway security under the theme "Tomorrow's Railway Security: Combining People and Technology." COLPOFER's participation supported the exchange of best practices in international cooperation and the strengthening of rail transport security through cooperation. COLPOFER represented a benchmark for cross-border cooperation on the international stage.

European Commission DG-Move

In 2025, COLPOFER actively participated in three meetings of the EU Expert Group on Land Transport Security (LANDSEC) and the Working Party on Rail Security (RAILSEC), held in February, June, and October. This participation focused on key EU transport security priorities, including evolving threat landscapes, cybersecurity risks in the rail sector, voluntary detection performance requirements, and emerging challenges such as counter-drone measures and infrastructure resilience. We also contributed to discussions on EU-funded security projects, crisis preparedness, and lessons learned from recent incidents affecting transport systems. Through these engagements, we supported the exchange of best practices and contributed to coordinated EU efforts to strengthen the security and resilience of land and rail transport across Member States.

RAILPOL

The collaboration between COLPOFER and RAILPOL is formalised in the COLPOFER-RAILPOL MOU, which is built on strengthening public–private partnerships to enhance security across the European railway system, bringing together railway police forces and railway operators' security organisations. Recognised and encouraged at the EU level, this cooperation focuses on improving the protection of people, infrastructure, trains, and information through structured operational and strategic initiatives.

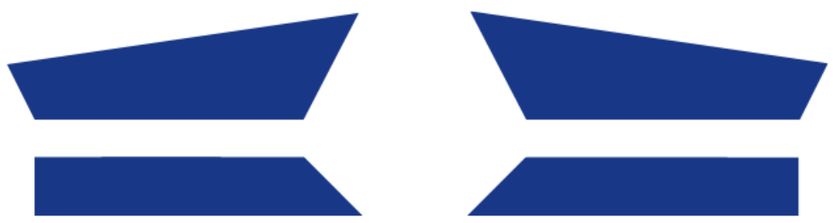
By leveraging RAILPOL's role as a cross-border police platform and COLPOFER's representation of railway operators, the partnership promotes joint training, shared expertise, coordinated operational activities, and continuous information exchange, contributing both to tangible security improvements and to increased passenger confidence in the railway environment.

UITP

Signed during the 79th COLPOFER General Assembly (Pietrarsa, 18 June 2025), the COLPOFER–UITP Memorandum of Understanding formalizes a structured partnership between COLPOFER (including its Working Groups) and the UITP Security Committee, with Salvatore Iannicelli signing on behalf of COLPOFER alongside UITP's Security Committee leadership (Michal Cieslik). In annual-report terms, it extends railway-security cooperation into the broader public transport security ecosystem and turns collaboration into concrete, operational workstreams.

This partnership provides for systemic information exchange on emerging trends (e.g., CCTV evolution, digitalisation, drones), the sharing of analysis on CBRN risks, evolving criminal modus operandi, and cybersecurity, plus joint threat-assessment products. Crucially, it also enables mutual participation in trainings and the joint organization of trainings and tabletop exercises, strengthening common preparedness and security awareness across operators and law-enforcement communities, positioning security as a shared responsibility and supporting safer, more resilient mobility.

In November 2025, COLPOFER participated as a guest in the UITP Security Committee (SECCOM) meeting in Rome (18–20 November 2025), thanks to the COLPOFER-UITP MOU signed earlier in the year. The agenda included a dedicated "COLPOFER Cooperation" session focused on the UITP–COLPOFER MoU and operational cooperation with the Graffiti and Anti-Terrorism working groups, reinforcing coordination between the two networks on shared public transport security priorities.



COLPOFER

www.colpofer.org

colpofer@fsitaliane.it