UNIWERSYTET Andrzeja Frycza Modrzewskiego w Krakowie

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE

e-ISSN 2451-0718
ISSN 1899-6264

2026
Nr 1

https://doi.org/10.31749/2451-0718-btip-2026-1-001
Received: 17.11.2025
Accepted: 5.03.2026

Key barriers to inter-organizational learning in the European security ecosystem

Marta du Vall

PhD, DSc, Associate Professor, Andrzej Frycz Modrzewski Krakow University
https://orcid.org/0000-0003-1245-730X

Introduction

The contemporary security environment of the European Union (EU) is characterized by increasing complexity and the interdependence of threats. These threats, ranging from terrorist networks and international organized crime to advanced cyberattacks, are fundamentally transnational in nature. Their networked nature means that no single Member State, acting in isolation, is able to respond effectively. This leads to an obvious functional necessity for deepened cooperation, information exchange, and, most importantly, collective learning (European Commission, 2025).

In response to this necessity, the European Union has systematically expanded its institutional architecture in the Area of Freedom, Security, and Justice over the last two decades. Specialized agencies have been established, such as Europol (European Union Agency for Law Enforcement Cooperation) (European Union Agency for Law Enforcement Cooperation [Europol], n.d.-a), Frontex (European Border and Coast Guard Agency) (Frontex, n.d.-a), and ENISA (European Union Agency for Cybersecurity) (European Union Agency for Cybersecurity, n.d.-a), whose mandates are directly related to the aggregation, analysis, and dissemination of specialized knowledge.

However, this process of institutionalization encounters a fundamental obstacle: national security, intelligence, and policing remain strictly within the purview of

Member States, constituting the core of their sovereignty (European Commission, 2025). This leads to a phenomenon that can be termed the sovereignty paradigm: Member States create supranational agencies to address problems they cannot solve alone, while simultaneously and deliberately limiting their powers, resources, and access to key intelligence to protect their own decision-making autonomy (Walsh, 2006).

As a result, the European security architecture is torn between the rhetoric of integration and the practice of fragmentation. The central research problem of this article is the discrepancy between the declared need for Inter-Organizational Learning (IOL) and the actual capacity and will of the organizations forming this architecture to implement it. The article posits that inter-organizational learning is a key but underutilized strategic resource of the European Union. Its effectiveness is inhibited not by technological deficits – however significant – but by deep-seated political, cultural, and institutional barriers. Among them, the absolute primacy belongs to a chronic lack of trust (Safjański, James, 2020), which prevents the transformation of distributed data into collective, operational knowledge. The article synthesizes the main barriers and recommends a strategic shift of emphasis from technological platforms to building human and relational capital.

Methodology

This article employs a qualitative approach, combining a targeted literature and document review with an analytical synthesis of selected case studies. The primary methodological objective is to systematically map empirical data regarding the EU security architecture onto two established theoretical frameworks: the 4I organizational learning model and the concept of Absorptive Capacity (ACAP).

The analysis is based on a targeted selection of official EU agency evaluations, policy reports, and peer-reviewed academic literature. Source materials were purposefully selected based on their direct relevance to information-sharing protocols, the institutional mandates of Europol, Frontex, and ENISA, and documented operational challenges within the collaborative governance networks of the EU security sector.

Case studies were chosen using a purposive sampling strategy to illustrate contrasting extremes of IOL effectiveness in practice, allowing for a comparative analysis of learning mechanisms:

1. strategic failure – the Paris (2015) and Brussels (2016) terrorist attacks were selected as a paradigmatic, highly documented example of a catastrophic IOL breakdown. This case serves to illustrate systemic failure at the *integration* stage of the 4I model;
2. operational success – Joint Investigation Teams (JITs) and cross-border Network Operations (e.g., Operation EMMA) were selected as contrasting examples of

functional, bottom-up IOL. These cases were chosen to demonstrate how temporary organizational units can maximize *absorptive capacity* and overcome inherent trust barrier.

The collected empirical data was systematically mapped against the theoretical models to precisely diagnose structural breaking points. The 4I model was used to differentiate between deficits in national-level *interpretation* versus failures in inter-organizational *integration*. Concurrently, the ACAP model was applied to shift the analytical focus from the data senders (EU agencies) to the critical interface and processing capabilities of the receivers (Member States).

Inter-organizational learning (IOL) in the context of security

Organizational Learning (OL) theory largely originates from the analysis of the private sector, where the capacity for adaptation and innovation is a condition for survival and competitive advantage. These elements collectively form an organizational culture conducive to absorbing and utilizing new knowledge. Inter-Organizational Learning (IOL) extends this concept beyond the boundaries of a single firm, describing how knowledge is transferred, assimilated, and co-created between organizations operating within a network.

In the public sector, to which security agencies belong, IOL acquires specific significance. The goals here are not profit or market share, but the improvement of public service efficiency, increased citizen security, or more effective crisis response (Harvey et al., 2010). This collaboration often relies on complex collaborative governance networks rather than simple market mechanisms. Transferring IOL models to the security sector requires accounting for its radical specificity. While private sector cooperation may be based on mutual benefit, the security sector (especially intelligence and police services) operates in a "high stakes, low trust" environment (Boardman, 2006).

Analysis of communication barriers within the intelligence community reveals that the default organizational culture is *not* sharing information (Boardman, 2006). This is perceived as a rational strategy, motivated by the necessity to protect sensitive sources and methods, as well as defending one's own institutional mandates (so-called "turf wars") (Boardman, 2006). This culture is so deeply ingrained that agencies operate in an environment "hostile to intelligence sharing," viewing knowledge as a resource in a "zero-sum game" (Boardman, 2006).

Furthermore, in the complex security ecosystem of the EU, IOL is hampered by a fundamental conflict of mandates. This problem is perfectly visible in the relationships between Computer Security Incident Response Teams (CSIRTs), supported by ENISA, and Law Enforcement (LE), supported by Europol (ENISA, 2020). The mandate of a CSIRT is the mitigation of cyber incident effects and the fastest possible restoration of system functioning (ENISA, 2020). The mandate of law enforcement

is the prosecution of perpetrators, which requires securing and preserving digital evidence (ENISA, 2020). As the ENISA report indicates, CSIRT actions (aimed at rapid repair) can "seriously impede the collection of evidence necessary for criminal investigation, or even destroy it" (ENISA, 2020). Effective IOL in this context does not consist of naive "sharing everything," but on developing complex deconfliction protocols that allow for reconciling conflicting institutional goals.

IOL Models – breaking points

To diagnose where the IOL process breaks down in the security context, the 4I model by Crossan et al. (1999) is useful. This model describes learning as a dynamic, multi-level process of strategic renewal involving four linked processes: intuition – a process at the individual level (subconscious recognition of patterns and possibilities) (Serrat, 2017); interpretation – a process at the individual level (conscious explanation of intuition to oneself and others, making sense of it, and creating cognitive maps) (Lawrence et al., 2005); integration – a process at the group level (developing "shared understanding among individuals and taking coordinated actions") (Lawrence et al., 2005); institutionalization – a process at the organizational level (embedding learning in the organization's systems, structures, procedures, and routines) (Lawrence et al., 2005).

The 4I model allows for a precise diagnosis of where IOL fails in the European security architecture. As empirical analysis will show, the problem is often not a lack of intuition or interpretation at the national level (e.g., an analyst in one Member State identifies a threat). The process notoriously collapses at the integration stage – the inability to transform individual knowledge into "shared understanding" and "coordinated action" at the inter-organizational level. This happens due to trust barriers (Walsh, 2006) and "turf" conflicts (Boardman, 2006), which prevent the flow of knowledge from the individual level to the network level.

The second key analytical model is the concept of Absorptive Capacity (ACAP), defined by Cohen and Levinthal (1990) as an organization's ability to "recognize the value of new information, assimilate it, and apply it" (Cohen & Levinthal, 1990). ACAP is not passive reception; it is an active capability critically dependent on prior related knowledge and existing communication and coordination paths (Farrell & Coburn, 2018). This model, though derived from firm innovation research, is successfully applied to analyze performance improvement in the public sector, including police forces (Harvey et al., 2010). In this context, ACAP is defined as a public organization's ability to access new knowledge, assimilate it, and apply it to improve results (Harvey et al., 2010).

Applying the ACAP model allows for nuanced analysis of IOL failures in the EU. Suboptimal performance of information exchange systems, such as those managed by

Europol (Safjański, James, 2020), does not necessarily result solely from the sender's (Europol) failure. Equally often, it may be the receiver's (national police unit) failure. A Member State may receive high-quality intelligence data but lack the appropriate absorptive capacity – i.e., trained analysts (lack of *prior related knowledge*) or internal procedures (lack of *paths*) – to assimilate and operationally apply this data. This diagnosis shifts the burden of analysis from EU agencies alone to the critical interface between agencies and national bodies.

The architecture of knowledge exchange in the EU

Using the presented theoretical frameworks, it is possible to analyze the key EU security agencies – Europol, Frontex, and ENISA – as central nodes in the IOL network. A synthetic comparison of their mandates, mechanisms, and diagnosed barriers is presented below.

Table 1. Characteristics of key EU security agencies as learning organizations

Agency	Main mandate (related to IOL)	Key IOL platforms/ mechanisms	Identified barriers to IOL (sources)
Europol	Central hub for criminal intelligence and analysis; supporting Member States (MS) investigations.	SIENA (Secure Information Exchange Network Application), EIS (Europol Information System), EPE (Europol Platform for Experts), J-CAT (Joint Cybercrime Action Taskforce).	**Lack of Trust** by MS leading to reluctance to share data (Safjański, James, 2020). **Legal Fragmentation** and data protection limits (European Data Protection Supervisor, EDPS) (Fotiadis et al., 2022). **Bottlenecks** in SIENA architecture (national units) (Statewatch, 2025).
Frontex	Promoting Integrated Border Management (IBM); developing a common professional culture.	Joint trainings (on-the--job, formal), e-learning (EU Learn platform), operations, risk analysis (EUROSUR).	**Culture of Resistance** to negative feedback (e.g., re: fundamental rights). **Low Perception** of value-add by MS (reporting seen as a „burden") (Walsh, 2006). Insufficient transparency of complaint mechanisms.
ENISA (and CSIRT Network)	Building situational awareness; strengthening operational cooperation (CSIRT Network support).	CSIRT Network, common incident taxonomies, threat analysis, joint exercises.	**Conflicting Mandates** (CSIRT: mitigation vs. Law Enforcement (LE): prosecution) (ENISA, 2020). **"Two fronts of trust" dilemma** (CSIRTs must protect constituent trust, limiting data sharing with LE) (ENISA, 2020).

Source: Author's own elaboration.

Europol

Europol's mandate situates the agency as the center of European police cooperation, intended to serve as a criminal information hub (Europol, 2024) and analytical center supporting Member State investigations (Europol, n.d.-a). To this end, Europol manages key IOL platforms: the Europol Information System (EIS), the Platform for Experts (EPE), which hosts, among others, the SIRIUS project facilitating access to electronic evidence from service providers (Europol, n.d.-g), and primarily the Secure Information Exchange Network Application (SIENA) (Europol, n.d.-c).

Analysis of these platforms reveals, however, two fundamental paradoxes limiting Europol's IOL potential. The first is the SIENA Paradox, illustrating the gap between technological optimism and political realism. The official narrative describes SIENA as a "state-of-the-art" platform enabling "rapid and user-friendly exchange" of operational information (Europol, n.d.-f). However, evaluation reports point to a much more problematic picture: SIENA's functioning is often "constrained by limited access" of national bodies, and the multitude of available communication channels (bilateral, multilateral, via Interpol) creates "more difficulties than solutions" for practitioners (Disley et al., 2012). The cause of this dysfunction is not technical but architectural and political. As analyses indicate, the SIENA system was intentionally designed so that data must pass through National Contact Units (Statewatch, 2025). This architecture is a technical reflection of the sovereignty paradigm – Member States, instead of creating a true peer-to-peer knowledge exchange, imposed a "hub-and-spoke" model where national units act as gatekeepers. This intentionally built-in "bottleneck" institutionalizes the lack of trust (Walsh, 2006) in the technology itself, fundamentally limiting the potential for learning.

The second problem is the dilemma of learning vs. legality. For Europol to become a learning organization capable of detecting complex criminal patterns, especially in the era of Big Data and AI, it needs the capacity to analyze vast datasets (Statewatch, 2025). However, the unprecedented decision by the European Data Protection Supervisor (EDPS) in January 2022, ordering Europol to delete its "big data ark" (Fotiadis et al., 2022), demonstrates a fundamental conflict. The EDPS stated that Europol was illegally storing data on persons not directly linked to criminal activity, violating the principle of data minimization (Fotiadis et al., 2022). Europol is thus trapped in an unsolvable conflict: the logic of learning (more data = better patterns and analysis) stands in direct contradiction to the EU's legal logic (data protection and privacy) (Fotiadis et al., 2022). This means Europol, unlike agencies in the style of the American NSA (Fotiadis et al., 2022), is legally restrained from achieving its full data-driven IOL potential, constituting a key, externally imposed barrier.

Frontex

Frontex's mandate focuses on promoting Integrated Border Management (IBM) (Frontex, n.d.-a). A key IOL mechanism in this context is creating a "common European professional culture" for border guards (Frontex, n.d.-c). The agency invests heavily in various forms of knowledge transfer, including on-the-job training, formal courses (e.g., on fundamental rights, languages), and e-learning platforms (like "EU Learn") (Frontex, n.d.-a).

Analysis of Frontex's activity indicates a distinction between performative learning and critical learning. The agency demonstrates high proficiency in performative learning – teaching officers how to perform tasks according to specific procedures (Frontex, n.d.-c). This is "top-down" knowledge transfer. Simultaneously, Frontex exhibits strong resistance to critical learning – absorbing feedback about errors, failures, and systemic problems, particularly in the sensitive area of fundamental rights. Evidence of this dysfunction is clear. The Consultative Forum on Fundamental Rights (CFFR) stated it was "not consulted" on human rights issues, and its comments were "often ignored." Similarly, the Fundamental Rights Officer (FRO) faced allegations of a lack of independence, and complaint mechanisms proved insufficiently transparent and effective. Furthermore, relationships with Member States also indicate value perception problems. Some Member States perceived sharing information with Frontex as an "additional burden" rather than a process bringing "value added" (Walsh, 2006). This points to an organizational culture resistant to negative feedback. From the perspective of OL theory, an organization that systematically ignores feedback mechanisms is not a learning organization; it is an example of institutional unlearning, where the culture actively rejects knowledge contrary to its operational goals.

ENISA

ENISA plays a key role in the EU cybersecurity ecosystem, aiming to raise common situational awareness (ENISA, n.d.-a) and operationally supporting the CSIRT Network (ENISA, n.d.-b). Learning in this network occurs through information exchange on threats and incidents (ENISA, n.d.-a) and creating common frameworks, such as incident taxonomies (ENISA, 2020).

However, as signaled earlier, the main barrier here is the conflict of mandates (ENISA, 2020). This barrier leads to a more complex problem, which can be called the "two fronts of trust" dilemma. CSIRTs, especially national, academic, or sectoral ones, operate largely based on voluntary incident reporting by their constituents, e.g., private sector companies (ENISA, 2020). To maintain this key data flow, CSIRTs must guarantee confidentiality and act in the victim's best interest (e.g., quickly patching the system). At the same time, law enforcement (LE) demands access to the

same data for investigative and prosecutorial purposes (ENISA, 2020). CSIRTs are trapped in a dilemma. If they too willingly and automatically pass data to law enforcement, they risk losing the trust of their constituents.

As research indicates, victims of cybercrime "sometimes refuse to report incidents" to law enforcement for various reasons (ENISA, 2020). In such cases, CSIRTs are "discouraged from sharing information… because they fear losing the trust of their constituent" (ENISA, 2020). CSIRT networks must therefore manage trust on two fronts simultaneously: (1) towards their data providers (private sector) and (2) towards their partners (LE). The interests of these two groups are often contradictory. For this reason, simple technical solutions, such as promoting a "common platform" for data exchange (ENISA, 2019), will not solve the problem. The barrier is fundamentally relational, political, and rooted in the conflicting operational logics of different security ecosystem actors.

Learning from failures and successes

Theoretical and institutional analysis shows that IOL in the EU is a process burdened with structural barriers. This section verifies this thesis through case study analysis, contrasting strategic failure with operational successes.

The Paris (2015) and Brussels (2016) attacks

The coordinated terrorist attacks in Paris (November 2015) and Brussels (March 2016) constitute a tragic and textbook example of a catastrophic failure of inter-organizational learning. Post-mortem analyses revealed that the terrorist network (the so-called Zerkani network) executing the attacks was known to law enforcement and intelligence services in several Member States, including Belgium and France (Andreeva, 2025).

The failure was not a lack of data. It was a systemic inability to integrate distributed fragments of information into a coherent intelligence picture and transform it into "coordinated action," which is the definition of failure at the Integration stage of the 4I model (Lawrence et al., 2005). Law enforcement and intelligence agencies from different states "failed to cooperate adequately," leading to numerous "missed opportunities" to interrupt preparations for the attacks (Andreeva, 2025). This was a direct result of trust barriers (Walsh, 2006), differences in organizational cultures (Boardman, 2006), and the lack of effective intelligence exchange protocols.

However, OL theory also indicates that failure can be a powerful catalyst for learning. The 2015 and 2016 attacks provided a key insight: it was precisely as a result of these failures that a "European counter-terrorism and intelligence cooperation culture" began to develop (Andreeva, 2025). The shock caused by the scale of the attacks and the realization that they were preventable forced national

practitioners to understand that "cooperation is necessary" to meet threats (Andreeva, 2025).

This tragedy acted as a reactive learning mechanism, temporarily overcoming the sovereignty paradigm. The cost of not sharing information (mass casualties) suddenly proved higher than the perceived cost of sharing it. Many subsequent legislative initiatives and the strengthening of agency mandates (including Europol) can be seen as an attempt at institutionalization (the fourth stage of the 4I model) of the lessons learned from this failure.

Studies of success: Joint Investigation Teams (JITs) and Network Operations

In radical contrast to the strategic failures of central data exchange stand the successes of Joint Investigation Teams (JITs). JITs are recognized as "one of the most advanced tools" for international cooperation in criminal matters (European Union Agency for Criminal Justice Cooperation [Eurojust], n.d.). These are ad hoc teams created for a fixed period (usually 12-24 months) and a specific investigative purpose, consisting of prosecutors, judges, and law enforcement officers from two or more states (Eurojust, n.d.). Eurojust plays a key role in the legal, logistical, and financial support of JITs, similar to Europol in operational support (Eurojust, n.d.).

The success of JITs can be explained by analyzing them as incubators of trust and micro-spaces of effective IOL that directly address identified barriers:

1. overcoming the trust barrier: unlike anonymous data exchange via centralized platforms (like SIENA), JITs rely on intensive, daily, face-to-face cooperation (Nuño-Solinís & Urtaran-Laresgoiti, 2018). Trust here is not a prerequisite imposed from above, but a result of shared operational practice focused on solving a concrete, shared problem (e.g., dismantling a specific criminal group) (United Nations Office on Drugs and Crime, n.d.);
2. realizing the "Integration" process (4I): a JIT is by definition an integration mechanism (Lawrence et al., 2005). It forces participants from different legal and organizational systems (Block, 2008) to develop "shared understanding" and take "coordinated actions" in real-time;
3. maximizing Absorptive Capacity (ACAP): a JIT creates a temporary organizational unit with maximum absorptive capacity (Farrell & Coburn, 2018). By gathering experts with the required "prior related knowledge" (police, analysts, prosecutors) in one place, the JIT ensures that newly acquired knowledge (e.g., from a wiretap in Country A) is immediately understood, assimilated, and applied (e.g., to issue an arrest warrant in Country B) (Harvey et al., 2010), without delays resulting from bureaucratic "gatekeepers" (Statewatch, 2025).

The success of JITs proves that effective IOL in the European security sector is largely bottom-up, problem-oriented, and relationship-based, rather than top-down, centralized, and technology-based.

Further evidence of IOL evolution is provided by complex network operations that go beyond traditional state-to-state cooperation. An example is Operation European Money Mule Action (EMMA), which led to the arrest of 178 people in 2016 (Europol, 2016). The key to its success was not only cooperation between 16 states, Europol, Eurojust, and the FBI. It was the engagement of 106 banks and private partners (Europol, 2016).

Similarly, Operation EMMA95, which led to the dismantling of the encrypted communication network EncroChat, was the result of JIT actions (France, Netherlands) supported by Europol and Eurojust (Europol, 2020). This case illustrates that critical infrastructure used by criminals is in private hands.

These cases indicate the most important new trend: the evolution from public-public IOL to public-private IOL. State agencies no longer possess a monopoly on knowledge nor control over infrastructure (financial systems (Europol, 2016), encrypted communication services (Europol, 2020)). Effective crime fighting now requires the ability to learn *from* and *with* the private sector (tech companies, financial institutions).

Europol attempts to institutionalize this new reality through initiatives such as the SIRIUS project (facilitating cooperation with online service providers) (Europol, n.d.-g) or direct cooperation with tech companies (Statewatch, 2025). However, this raises new, complex challenges related to law, ethics, and trust.

Conclusion

The analysis conducted in this article demonstrated that inter-organizational learning (IOL) in the European security sector is a complex, highly politicized process burdened with fundamental contradictions. Its dynamics are defined by the constant tension between the functional necessity of cooperation, forced by the transnational character of threats, and the political and cultural imperative of protecting national sovereignty and secrecy – the sovereignty paradigm.

The main findings of the analysis indicate that the most serious obstacles to effective IOL lie not in the sphere of technology, but in organizational culture and politics. These include, above all, the lack of trust between Member States and agencies (Safjański, James, 2020), a culture of "knowledge hoarding" (need-to-know) rather than "need-to-share" (Boardman, 2006), and deep mandate conflicts (e.g., CSIRT vs. LE) (ENISA, 2020).

A further problem is the dysfunction of centralized models. Top-down, centralized IOL mechanisms based on technological platforms (like SIENA at Europol) are systematically weakened. This happens because their architecture is a political compromise reflecting the sovereignty paradigm (built-in bottlenecks)

(Statewatch, 2025), and their potential is further limited by rigorous European data protection frameworks (the Legality Dilemma) (Fotiadis et al., 2022).

Simultaneously, it is clear that effective IOL – understood as learning leading to behavioral change and improved operational results – occurs primarily in bottom-up, problem-oriented, and trust-based microsystems. Joint Investigation Teams (JITs) are the best example of this, acting as "incubators of trust" and realizing Integration processes (from the 4I model) and maximizing absorptive capacity (ACAP) (Eurojust, n.d.).

Undoubtedly, the current EU security architecture exhibits characteristics of reactive learning, adapting in response to catastrophic failures (Andreeva, 2025). It lacks the mechanisms and organizational culture necessary to implement proactive learning, characteristic of High Reliability Organizations (HRO).

Further progress in building the EU's capacity for collective learning requires a strategic shift in resources and attention. Instead of concentrating solely on investments in further technological platforms, policymakers should equally invest in human platforms – mechanisms such as CEPOL, exchange programs, joint exercises, and facilitating the creation of JITs. Technological platforms can only transmit data; it is human platforms, building social capital, that are capable of generating the rarest and most important resource in the security ecosystem: trust.

The author is aware that a limitation of this analysis is its reliance on publicly available reports and literature. Undoubtedly, further research, particularly ethnographic studies on daily cooperation practices within JITs and deeper analysis of cultural barriers in implementing HRO principles in police forces, is necessary to fully understand the dynamics of learning in this critical sector for Europe.

As noted, the current IOL model in the EU is largely reactive – learning from spectacular failures like the 2015 and 2016 attacks (Andreeva, 2025). This is a costly and inefficient model. An alternative is offered by the concept of High Reliability Organizations (HRO), derived from research on extremely high-risk sectors like aviation, nuclear power, or aircraft carrier operations. HROs are characterized by a proactive approach to learning, based on two key principles: (1) a system perspective, which in case of error focuses on analyzing faulty processes rather than blaming individuals, and (2) *preoccupation with failure*, viewing minor errors and "near misses" as priceless opportunities for learning and system adaptation before they lead to disaster.

Implementing HRO thinking in the European security sector would require a fundamental cultural change. As analyses indicate, security organizations are often dominated by a "culture of punishment" for reporting errors, which prompts employees to hide them. The HRO model requires the opposite: a "culture of reward" or at least a "just culture" (Kanaan & Mayer, 2023) that actively encourages problem reporting. In practice, this would mean that a Frontex officer reporting

a fundamental rights violation or a Europol analyst pointing out a systemic flaw in SIENA data flow (Disley et al., 2012) would not be treated as a problem, but as a key source of learning.

Ultimately, the analysis of IOL barriers leads to the conclusion that the weakest link is not technology, but the human and relational factor (Birdi et al., 2020). Investments in expensive IT platforms (like SIENA) will not yield results if they are not accompanied by equivalent investments in human capital and social networks. The key barrier remains the lack of trust (Walsh, 2006). Trust is not a product of technology; it is built by people through repeated, positive interactions (Birdi et al., 2020). This highlights the key, though often underestimated, role of agencies like CEPOL (European Union Agency for Law Enforcement Training), whose mandate is precisely creating "human platforms" for IOL (European Commission, 2025). Joint trainings, officer exchange programs, and even informal social events (Birdi et al., 2020) build relationships and mutual cultural understanding, which are the foundation of trust. As research indicates, barriers as prosaic as the lack of a common language (Birdi et al., 2020) or misunderstanding of organizational differences (Birdi et al., 2020) are often a greater obstacle to information exchange than the lack of technical compatibility.

References

Andreeva, C. (2025). The Zerkani Network and the 2015 Paris and 2016 Brussels Attacks: An Illustration of Counter-Terrorism Dysfunction in Europe. *Studies in Conflict & Terrorism*, *48*(11), 1313–1341. https://doi.org/10.1080/1057610X.2023.2178078

Birdi, K., Griffiths, K., Turgoose, C., ..., Vonaş, G. (2020). Factors influencing cross-border knowledge sharing by police organisations: An integration of ten European case studies. *Police Practice and Research*, *22*(1), 3–22. https://doi.org/10.1080/15614263.2020.1789462

Block, L. (2008). Combating organized crime in Europe: Practicalities of police cooperation. *Policing: A Journal of Policy and Practice*, *2*(1), 74–81. https://doi.org/10.1093/police/pan009

Boardman, Ch.H. (2006). *Organizational culture challenges to interagency and intelligence community communication and interaction*. Defense Technical Information Center. https://apps.dtic.mil/sti/tr/pdf/ADA451234.pdf [accessed: 30.10.2025].

Cohen, W.M., & Levinthal, D.A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, *35*(1), 128–152. https://doi.org/10.2307/2393553

Crossan, M.M., Lane, H.W., & White, R.E. (1999). An organizational learning framework: From intuition to institution. *Academy of Management Review*, *24*(3), 522–537. https://doi.org/10.5465/amr.1999.2202135

Disley, E., Irving, B., Hughes, W., Patruni, B. (2012). *Evaluation of the implementation of the Europol Council Decision and of Europol's activities*. RAND Europe. https://www.europol.europa.eu/sites/default/files/documents/rand_evaluation_report.pdf [accessed: 30.10.2025].

European Commission. (2025, June 23). Law enforcement cooperation. https://home-affairs.ec.europa.eu/policies/internal-security/law-enforcement-cooperation_en [accessed: 30.10.2025].

European Union Agency for Cybersecurity (ENISA). (n.d.-a). *Cooperation mechanisms*. https://www.enisa.europa.eu/topics/cyber-threats/situational-awareness [accessed: 23.10.2025].

European Union Agency for Cybersecurity (ENISA). (n.d.-b). *CSIRTs Network*. https://csirtsnetwork.eu/ [accessed: 23.10.2025].

European Union Agency for Cybersecurity (ENISA). (2019, July 24). *Sharing is caring: Technical cooperation across CSIRTs, LE and the judiciary*. https://www.enisa.europa.eu/news/enisa-news/sharing-is-caring-technical-cooperation-across-csirts-le-and-the-judiciary [accessed: 23.10.2025].

European Union Agency for Cybersecurity (ENISA). (2020). *ENISA Report on CSIRT-LE Cooperation: A study of the roles and synergies among selected countries*. Publications Office of the European Union. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20on%20CSIRT-LE%20Cooperation%20-%20A%20study%20of%20the%20roles%20and%20synergies%20among%20selected%20countries.pdf [accessed: 29.10.2025].

European Union Agency for Criminal Justice Cooperation (Eurojust). (n.d.). *Joint investigation teams (JITs)*. https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams [accessed: 23.10.2025].

European Union Agency for Law Enforcement Cooperation (Europol). (n.d.-a). *About Europol*. https://www.europol.europa.eu/about-europol [accessed: 23.10.2025].

European Union Agency for Law Enforcement Cooperation (Europol). (n.d.-c). *Information exchange*. https://www.europol.europa.eu/how-we-work/services-support/information-exchange [accessed: 23.10.2025].

European Union Agency for Law Enforcement Cooperation (Europol). (n.d.-f). *Secure Information Exchange Network Application (SIENA)*. https://www.europol.europa.eu/how-we-work/services-support/information-exchange/secure-information-exchange-network-application-siena [accessed: 29.10.2025].

European Union Agency for Law Enforcement Cooperation (Europol). (n.d.-g). *Sirius Project*. https://www.europol.europa.eu/how-we-work/sirius-project [accessed: 24.10.2025].

European Union Agency for Law Enforcement Cooperation (Europol). (2016, November 22). *178 arrests in successful hit against money muling*. https://www.europol.europa.eu/media-press/newsroom/news/178-arrests-in-successful-hit-against-money-muling [accessed: 28.10.2025].

European Union Agency for Law Enforcement Cooperation (Europol). (2020, July 2). *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe [accessed: 28.10.2025].

European Union Agency for Law Enforcement Cooperation (Europol). (2024). *Decoding the EU's most threatening criminal networks. Publications Office of the European Union*. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20report%20on%20Decoding%20the%20EU-s%20most%20threatening%20criminal%20networks.pdf [accessed: 30.10.2025].

Farrell, C.C., & Coburn, C.E. (2017). Absorptive capacity: A conceptual framework for understanding district central office learning. *Journal of Educational Change*, *18*, 135–159. https://doi.org/10.1007/s10833-016-9291-7

Fotiadis, A., Stavinoha, L., Zandonini, G., Howden, D. (2022, January 10). A data black hole: Europol ordered to delate vast store of personal data. *The Guardian*. https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data [accessed 3.11.2025].

Frontex. (n.d.-a). *Career development*. https://www.frontex.europa.eu/careers/what-we-offer/career-development/ [accessed: 23.10.2025].

Frontex. (n.d.-c). *Trainings at Frontex*. https://www.frontex.europa.eu/training/trainings-at-frontex/ [accessed: 23.10.2025].

Harvey, G., Jas, P., Walshe, K., Skelcher, C. (2010). Absorptive capacity: how organisations assimilate and apply knowledge to improve performance. In: K. Walshe, G. Harvey, P. Jas (Eds.), *Connecting Knowledge and Performance in Public Services: From Knowing to Doing* (pp. 226–250). Cambridge University Press.

Kanaan N., & Mayer J.C. (2023). Revealing the spatiality of crises: Lessons from failures of boundary work in a cross-border crisis. *M@n@gement*, *26*(4), 16–34. https://doi.org/10.37725/mgmt.2023.8104

Lawrence, T.B., Mauws, M.K., Dyck, B., & Kleysen, R.F. (2005). The politics of organizational learning: Integrating politics and the 4I framework. *Academy of Management Review*, *30*(1), 180–191. https://doi.org/10.5465/AMR.2005.15281451

Nuño-Solinís, R. & Urtaran-Laresgoiti, M. (2018). Learning from integrated care top performers in Spain. *International Journal of Integrated Care*, 18(S2), Article 4. https://doi.org/10.5334/ijic.s2004

Safjański, T., James, A. (2020). Europol's Crime Analysis System – Practical Determinants of Its Success, *Policing: A Journal of Policy and Practice*, *14*(2), 469–478. https://doi.org/10.1093/police/pay021

Serrat, O. (2017). Knowledge as Culture. In: *Knowledge Solutions: Tools, Methods, and Approaches to Drive Organizational Performance* (pp. 523–557). Springer. https://doi.org/10.1007/978-981-10-0983-9_58

Statewatch. (2025, February 27). *Behind closed doors: Europol's opaque relations with tech companies*. https://www.statewatch.org/analyses/2025/behind-closed-doors-europol-s-opaque-relations-with-tech-companies/ [accessed: 3.11.2025].

United Nations Office on Drugs and Crime (UNODC). (n.d.). *Case studies: Operation "Valter"*. https://www.unodc.org/e4j/en/organized-crime/module-7/exercises/case-studies.html [accessed: 4.11.2025].

Walsh, J. I. (2006). Intelligence-sharing in the European Union: Institutions are not enough. *Journal of Common Market Studies*, *44*(3), 625–643. https://www.jamesigoewalsh.com/jcms.pdf [accessed: 5.11.2025].

Key barriers to inter-organizational learning in the European security ecosystem

Abstract

This article analyzes the mechanisms and barriers to inter-organizational learning (IOL) in the European Union's security sector. The research aims to diagnose why effective IOL remains a systemic challenge despite significant institutional and technological investments. Using a targeted literature review and case study synthesis mapped against the 4I and Absorptive Capacity theoretical frameworks, the study identifies a fundamental tension termed the *sovereignty paradigm*. The analysis of key agencies (Europol, Frontex, ENISA) and specific operations (Paris and Brussels attacks, Joint Investigation Teams) reveals that the main obstacles are not technical. Rather, they are rooted in political and cultural barriers, specifically a chronic lack of trust, conflicting mandates, and cultures resistant to critical feedback. The article concludes that improving IOL requires a strategic shift from investing in centralized technological platforms to building bottom-up, relationship-based human networks capable of generating trust.

Keywords: inter-organizational learning (IOL), European security, European Union, Europol, Frontex, information sharing, trust, absorptive capacity