Proceedings of 5th International Conference CNDGS'2026
ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/10.47459/cndcgs.2026.126**

Digital Evidence in Police Practice and Competency Gaps in Digital Forensics Education

Miloš ZAJÍC[1*], Jan KOLOUCH[1], David KOVÁŘ[1], Dirk PAWLASZCYZK[2], Philipp ENGLER[2] Ronny BODACH[2]

[1] *Department of Security and Law, Ambis University, Lindnerova 575 180 00 Praha, Czech Republic*
[2] *Faculty Applied Computer Sciences & Biosciences, Hochschule Mittweida, University of Applied Sciences. Technikumplatz 17, Mittweida*

Correspondence: [*]milos.zajic@ambis.cz

Abstract
The study aims to analyse the ability of police officers to work with digital evidence in police practice, to identify current systemic and competency-related weaknesses in the field of digital forensics, and to compare their manifestations within the Police of the Czech Republic and the police of the Free State of Saxony within the DiForPol project. A quantitative questionnaire survey was conducted via an online platform in parallel among members of the Police of the Czech Republic and the police of the Free State of Saxony. The data were analysed using descriptive statistics and qualitative content analysis of open-ended responses. The results in both national samples confirm a high level of exposure to digital evidence alongside a limited self-assessed level of professional preparedness, a strong demand for systematic training, and the persistence of technical, organisational, and capacity-related barriers. The findings provide an empirical basis for the development of a harmonised educational framework in digital forensics within law enforcement agencies and for strengthening cross-border cooperation. The study provides systematic comparative empirical data on digital forensics in Czech and Saxon police practice.

Keywords: digital evidence, digital forensics, police practice, police education, professional competence, criminalistics practice, digital crime, forensic data analysis, professional training, Police of the Czech Republic.

Citation: Zajíc, M.; Kolouch, J.; Kovář, D.; Pawlaszcyzk, D.; Engler, P.; Bodach, R. *Digital Evidence in Police Practice and Competency Gaps in Digital Forensics Education.* In: Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959. https://doi.org/10.47459/cndcgs.2026.126

1. Introduction

The current security environment is characterised by the dynamic digitalisation of society, the acceleration of technological development, and the transformation of the nature of security threats. These processes fundamentally affect not only geopolitical relations and the strategic environment of states, but also the everyday functioning of law enforcement agencies in the Czech Republic. Digital technologies have become an integral part of modern society and, at the same time, a significant source of new vulnerabilities that can be exploited by both state and non-state actors [1,2].

In the context of national defence and internal security [3,4], cyberspace has emerged as a distinct domain of security threats in which elements of cyber operations, information influence, criminal activity, and hybrid actions intersect [4]. Digital traces and digital evidence now play a crucial role in identifying perpetrators, reconstructing events, and establishing links between individual incidents. Their significance extends far beyond cybercrime and affects a wide spectrum of criminal activity, including organised crime, terrorism, and activities threatening the fundamental functions of the state [5].

The growing volume, heterogeneity, and technical complexity of digital data impose increasing demands on the ability of law enforcement agencies to properly secure, analyse, and procedurally utilise such data. While technological development progresses rapidly, the adaptation of organisational structures, methodological procedures, and, in particular, systems of professional education often lags [6,7]. This creates a disparity between the actual level of exposure of law

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

enforcement agencies to digital evidence and the level of professional competencies required for its effective use in criminal proceedings.

Within the Police of the Czech Republic, digital evidence represents a routine component of policing activities across various types of units, including uniformed police, the criminal police and investigation service, and specialised departments. However, a systematic empirical analysis focusing on the actual use of digital evidence, the level of professional competencies of police officers in digital forensics, and the identification of organisational, technical, and educational barriers affecting its effective utilisation has so far been lacking. This knowledge gap constitutes a significant issue not only in terms of the efficiency of criminal proceedings but also from the perspective of broader national security interests, as the ability to work with digital evidence represents a key element of the resilience of the internal security system [8,9].

This paper aims to analyse the level of exposure of police officers to digital evidence, to evaluate their self-assessed professional competencies in the field of digital forensics, and to identify key systemic and educational barriers within the Police of the Czech Republic and the police of the Free State of Saxony. At the same time, the paper provides a comparative assessment of whether the identified issues are specific to the national context or represent a broader structural phenomenon across European law enforcement agencies.

The paper also contributes to the professional discourse on how to systematically strengthen the capabilities of law enforcement agencies in the field of digital forensics as part of a comprehensive state response to current and future security threats. Although police forces in the Czech Republic and Germany already cooperate, there is a need to further develop cooperation between regional police units along the Saxon–Czech border. In general, continuous professional education in the field of digital and mobile forensics remains essential for law enforcement agencies.

The findings presented in this paper may serve as an empirical basis for the formulation of educational, organisational, and conceptual measures aimed at strengthening the preparedness of law enforcement agencies in a dynamically evolving security environment. The study addresses the question of whether the identified competency gaps are specific to the national context or represent a broader structural phenomenon.

2. Mathematical Background

The data analysis was conducted on the basis of a questionnaire survey carried out among members of the Police of the Czech Republic and the police of the Free State of Saxony. The overall research sample consisted of two subgroups of respondents, which were analysed both independently and in a comparative context.

The total number of valid respondents was defined as:

$$N = N_{cz} + N_{DE} \tag{1}$$

where:
$N_{(CZ)}$ = 238 represents the number of respondents from the Police of the Czech Republic, and
$N_{(DE)}$ = 248 represents the number of respondents from the police in Germany.

For each observed variable, absolute frequencies of responses were determined:

$$n_{ij} = \textit{the number of respondents in category } i \textit{ within group } j \tag{2}$$

where the index *j* takes the following values:
j = CZ (Czech Republic)
j = DE (Saxony- Germany)

The relative frequency is given by the relation:

$$f_i = \frac{n_{ij}}{N_j} \tag{3}$$

The relative frequencies are further presented as percentages according to the relation:

$$p_i = f_i \,.\, 100 \tag{4}$$

For the purposes of comparative analysis, differences between the proportions of responses across individual categories were examined:

$$\Delta p_i = p_{i\,CZ} - p_{i\,DE} \tag{5}$$

where Δp_i represents the difference in the relative proportion of a given response between the Czech and German samples.

The analysis was descriptive in nature and aimed at identifying trends in relation to the degree of exposure to digital evidence, the level of professional competencies, and perceived barriers associated with handling digital evidentiary tools. Particular emphasis was placed on interpreting differences between the examined groups and identifying systemic factors influencing the observed findings.

Differences between the groups were assessed using differences in relative frequencies, with the analysis remaining predominantly descriptive.

3. Research Methodology

3.1 Study Design

The research was designed as a quantitative empirical study conducted through a questionnaire survey, which was further complemented by a qualitative analysis of open-ended responses. The study was carried out within the framework of the international project DiForPol [2] and involved parallel data collection within the Police of the Czech Republic and the police of the Free State of Saxony (Federal Republic of Germany). The chosen research design corresponds to the exploratory and descriptive nature of the study, the aim of which was to analyse the use of digital evidence in police practice, identify the level of professional competencies of law enforcement officers in the field of digital forensics, and reveal systemic barriers in professional education.

The research was not focused on hypothesis testing or the application of inferential statistical models, but rather on the systematic capture of the current state and structural relationships of the examined phenomenon. This approach corresponds to the nature of the researched issue, the availability of empirical data, and the applied focus of the research within the law enforcement environment [11].

3.2 Questionnaire Design

The questionnaire was designed as an original research instrument, the construction of which was based on an analysis of relevant scholarly literature focusing on digital forensics, police education, and the management of security organisations, as well as on international strategic and methodological documents and consultations with experts from police and forensic practice [5, 6, 12].

In constructing the questionnaire, emphasis was placed on terminological accuracy, clarity of wording, and the practical relevance of individual items for the target group of respondents. Before the main data collection, the questionnaire was pilot-tested on a limited sample of officers from the Police of the Czech Republic. Based on the feedback obtained, minor revisions were made to the wording in order to minimise interpretative ambiguity and enhance the validity of the instrument.

3.3 Structure of the questionnaire items

The questionnaire items were structured into thematic blocks reflecting the individual dimensions of the examined phenomenon.

Specifically, the following areas were covered:

- basic characteristics of respondents and their service positions,
- frequency and nature of work with digital evidence,
- self-assessment of professional competencies in the field of digital forensics,
- availability of technical resources and expert support,
- previous experience with training in this area, and
- perceived barriers to further professional development.

The questionnaire combined closed-ended items using nominal and ordinal scales with open-ended questions, which allowed respondents to qualitatively elaborate on their experiences and identify issues that cannot be fully captured through standardised responses.

3.4 Data Collection

Data collection was conducted via an online survey platform, which enabled efficient distribution of the questionnaire and anonymous collection of responses. This method was selected with regard to the geographical dispersion of respondents and the organisational structure of the Police of the Czech Republic and the Bundespolizei, as well as the need to minimise the administrative burden on research participants.

The questionnaire was distributed electronically, and participation was entirely voluntary. Respondent anonymity was ensured through a combination of technical and organisational measures, thereby reducing the risk of socially desirable responses and potential bias in the collected data.

Data collection was conducted in parallel in the Czech Republic and the Federal Republic of Germany within the framework of the DiForPol project. The questionnaire was methodologically harmonised and linguistically adapted for both environments to ensure the comparability of results while respecting the institutional specifics of the respective police organisations.

3.5 Sampling of Respondents

The selection of respondents was purposively aligned with the focus and objectives of the research project. The survey primarily included officers of the Police of the Czech Republic serving within regional police directorates in the Karlovy Vary, Ústí nad Labem, and Liberec regions, which were selected as relevant research environments with regard to the project focus, regional crime structure, and organisational variability of police practice. Although data collection was primarily concentrated in these regions, representatives from other regional directorates of the Police of the Czech Republic, as well as units with nationwide competence, were also included, allowing for a broader reflection of applied practice across the Czech Republic.

At the same time, the research was conducted in parallel within the police of the Free State of Saxony (Federal Republic of Germany), where officers from various types of units corresponding to the organisational structure of German policing practice were included. The selection of respondents in both countries was designed analogously in order to ensure the comparability of the collected data.

The research sample consisted of police officers assigned to different types of units, particularly public order police, criminal police, and investigation units, and other specialised departments, who may encounter digital evidence in the course of their duties. A purposive (non-probability) sampling strategy was applied to ensure that the collected data reflect the real-world experience of police officers in handling digital traces and correspond to the practical needs of the analysed issue.

The chosen approach was not aimed at achieving statistical representativeness in relation to the entire Police of the Czech Republic or the police of the Free State of Saxony, but rather at providing a descriptive and exploratory analysis within a defined institutional and project framework. The total number of fully completed questionnaires was 238 in the Czech Republic and 248 in the Federal Republic of Germany.

4. Results

The results of the quantitative survey confirm that digital evidence constitutes an integral and routine component of contemporary policing practice. The Czech research sample consisted of 238 officers of the Police of the Czech Republic, primarily serving within the regional police directorates of the Karlovy Vary, Ústí nad Labem, and Liberec regions. The structure of respondents was characterised by a predominance of operational units, particularly criminal police and investigation services (n = 115) and public order police (n = 68), while units with nationwide competence (n = 34), the Police Presidium and its departments (n = 19), and other units (n = 2) were less represented. The German sample included 248 respondents, where operational units also dominated, particularly criminal police (61.29%) and public order police (22.58%), while traffic police (3.63%), cybercrime units (2.82%), and other assignments (9.68%) were marginally represented. Both samples thus correspond to the applied level of policing practice in which digital evidence is routinely utilised.

The Czech sample consisted predominantly of rank-and-file officers in pay grades 8–9 (n = 78), grade 7 (n = 72), and grade 6 and below (n = 68), while senior management was represented by 20 respondents. The German sample was notably experienced, with 45.16% of respondents reporting more than 20 years of service and an additional 27.02% reporting between 11 and 20 years. In the Czech sample, the corresponding figures were n = 26 for more than 20 years of service and n = 66 for 11–20 years.

In response to this structure, the DiForPol project proposes a differentiated training programme reflecting the needs of both rank-and-file officers and more experienced personnel, enabling modular competence development according to professional roles and experience. At the same time, cross-border cooperation is strengthened through joint educational activities involving Czech and German participants, promoting knowledge sharing and harmonisation of procedures across law enforcement agencies.

In terms of the frequency of contact with digital traces, both samples confirmed their high presence in everyday policing activities. In the Czech sample, frequent contact was reported by 77 respondents (32.35%) and occasional contact by 116 respondents (48.74%), meaning that 81.09% of respondents encounter digital evidence repeatedly. Rare contact was reported by 32 respondents (13.45%), and no contact by 13 respondents (5.46%). In the German sample, frequent contact was reported by 42.74% and occasional contact by 28.23% of respondents, totalling 70.97%. Although repeated

contact was slightly higher in the Czech sample, both studies confirm that working with digital evidence is no longer a specialised activity but a routine component of police practice.

This finding is further supported by the frequency of working with digital evidence over the past twelve months. In the Czech sample, 81 respondents (34.03%) reported regular engagement (6–20 cases per year), 97 respondents (40.76%) occasional engagement (1–5 cases), 29 respondents (12.18%) more than 20 cases, and 31 respondents (13.03%) no experience in the given period. In the German sample, the corresponding values were 22.98% (6–20 cases), 36.69% (1–5 cases), 25.40% (more than 20 cases), and 14.92% (no experience).

Both samples demonstrate that digital evidence forms part of routine policing activities across different units and is not limited to isolated cases. Accordingly, the DiForPol project emphasises the integration of fundamental principles of handling digital evidence into a broader spectrum of training activities rather than restricting them to specialised courses.

Regarding the types of digital evidence, both samples show a predominance of traditional categories, particularly computers, storage media, and mobile devices. In the Czech sample, respondents most frequently reported storage media such as USB drives and hard disks (n = 175; 73.53%), computers and laptops (n = 174; 73.11%), and smartphones (n = 111; 46.64%). Cloud data were reported by 64 respondents (26.89%), network or internet data by 48 respondents (20.17%), Internet of Things devices by 20 respondents (8.40%), and in-vehicle IT systems by 6 respondents (2.52%). In the German sample, smartphones and tablets (92.34%), storage media (68.15%), and computers or laptops (64.52%) were most frequently reported, while cloud data (27.42%), network data (29.84%), vehicle IT systems (5.65%), and IoT devices (0.81%) were less frequent.

Despite the high level of exposure to digital evidence, both samples reveal a significant competence gap in digital forensics. In the Czech sample, 20.59% of respondents reported no experience, 47.48% basic knowledge, 27.31% advanced knowledge, and 4.62% expert knowledge. In the German sample, the corresponding figures were 29.84%, 39.11%, 28.23%, and 2.82%. Overall, respondents with no or only basic knowledge accounted for 68.07% in the Czech sample and 68.95% in the German sample. This nearly identical distribution represents one of the most significant findings of the study, indicating that the discrepancy between exposure to digital evidence and professional preparedness is not limited to a single national context.

These findings confirm that a substantial proportion of police officers perform tasks involving digital evidence without adequate formal training. In response, the DiForPol project develops a structured and modular training programme covering both basic and advanced levels of digital forensics, enabling systematic professional development.

Further findings relate to the organisational context of digital evidence handling. Both samples indicate that working with digital evidence extends beyond specialised roles and significantly affects routine investigative and operational functions. Accordingly, the DiForPol project extends training activities to non-specialised roles, particularly investigators and operational officers, while also strengthening access to expert support and knowledge sharing across units.

Important differences were also identified in technical and expert support. While a portion of respondents in the Czech sample had access to specialised forensic equipment, the German sample showed a stronger reliance on standard computing resources. Both samples, however, confirm that technical infrastructure is not uniformly available and varies significantly.

The results also demonstrate a strong demand for further training in digital forensics. In both samples, respondents expressed a high need for education, particularly in areas such as mobile forensics, evidence acquisition, and legal aspects. Give practitioners the necessary training to effectively use forensic software tools and follow a standardized procedure. Training is a serious problem facing organizations that deliver forensic services [13]. There is a lack of complex, realistic training data, which means that most classes are taught with simplistic artificial data. This, in turn influences the quality of education.

In terms of training formats, respondents in both countries clearly prefer practically oriented approaches, including in-person training, workshops, and scenario-based exercises. These preferences are reflected in the project's emphasis on simulation-based learning and practical training modules.

Finally, major barriers to further training were identified, particularly organisational and capacity-related factors, including lack of personnel, time constraints, budget limitations, insufficient technical equipment, and organisational obstacles. These findings indicate that the main limitations are not only individual but also systemic and institutional in nature.

The structured relationship between societal digitalisation, exposure to digital evidence, identified competence gaps, and the educational response within the DiForPol project is summarised in Figure 1.

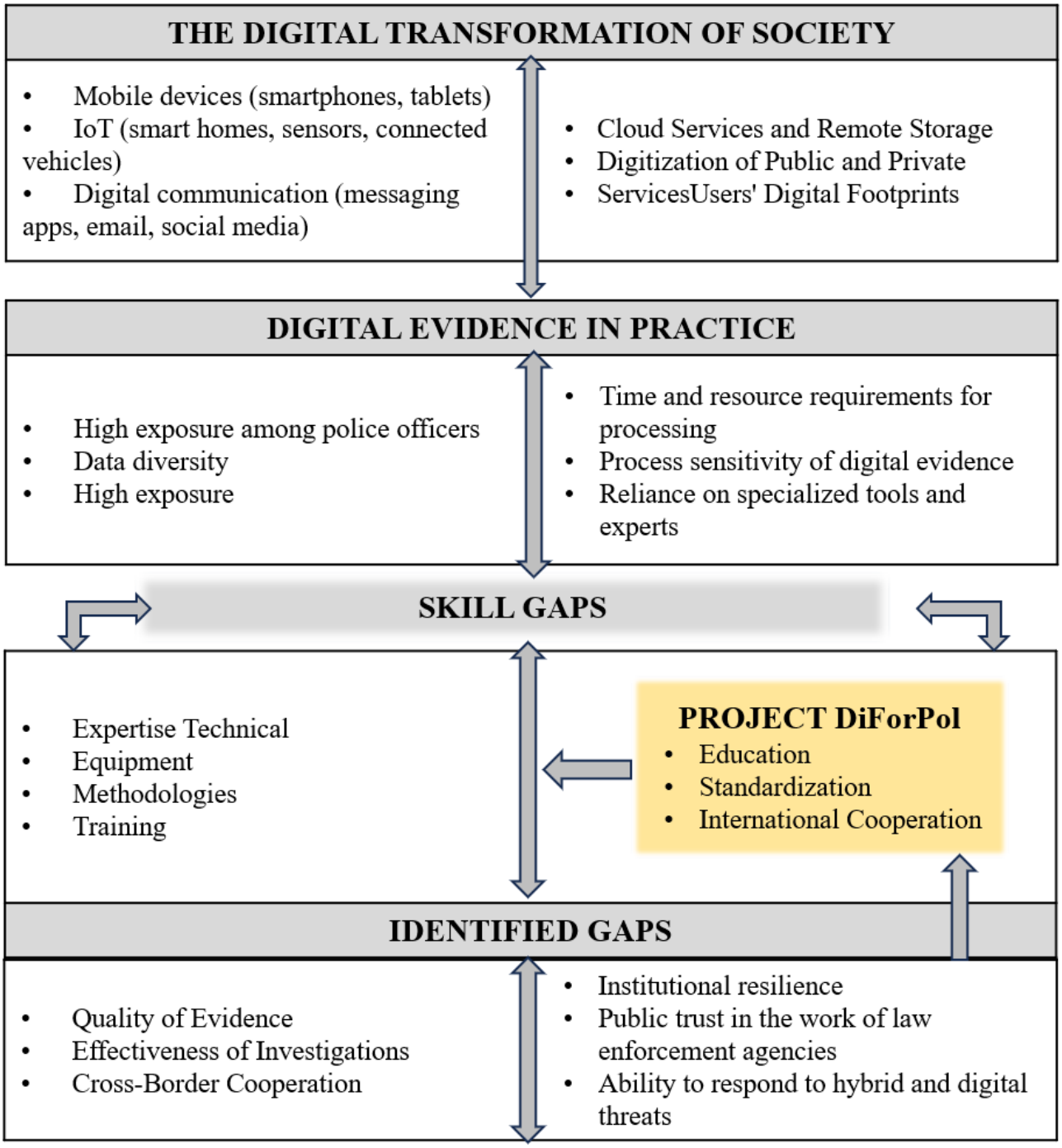

Fig. 1 Conceptual framework of the relationships between societal digitalisation, digital evidence, and competence gaps in policing practice, source: own elaboration.

5. Discussion

The results of the present study clearly confirm that digital evidence has become a structural component of internal security and an integral part of everyday policing practice. A high level of exposure of police officers to digital traces was identified both within the Police of the Czech Republic and the police of the Free State of Saxony. This trend indicates that working with digital evidence is no longer an exclusively specialised activity limited to a narrow group of forensic experts, but rather constitutes a standard competency requirement across operational units of law enforcement agencies. This shift fundamentally transforms the nature of policing and increases the demands placed on the professional preparedness of officers in the context of contemporary security threats [2,9].

The comparative analysis of the Czech and Saxon samples reveals a remarkable degree of consistency across key indicators. In both environments, a high frequency of contact with digital evidence was confirmed, alongside the dominant role of mobile devices, computers, and storage media, as well as a significant prevalence of basic or no professional competencies in digital forensics. The finding that approximately 68% of respondents in both samples fall into the

categories of no or only basic knowledge represents one of the most significant outcomes of the study. This result suggests that the identified mismatch between exposure to digital evidence and professional preparedness is not specific to a single national context but constitutes a structural feature of contemporary policing practice within a broader European framework.

This structural mismatch has critical implications for the institutional resilience of law enforcement agencies. The ability to properly secure, analyse, and procedurally utilise digital evidence represents a fundamental prerequisite for effectively combating modern forms of crime, including organised crime, hybrid threats, and cross-border criminal activities. Insufficient levels of professional competence in this area may therefore lead not only to a reduction in the quality of evidence handling but also to broader systemic risks in the field of internal security [8,1].

The results further demonstrate that work with digital evidence is not confined to specialised forensic units but significantly affects routine investigative and operational activities. The relatively low proportion of specialised forensic personnel in the German sample, combined with the high proportion of respondents using digital evidence in operational practice, confirms that digital forensics is becoming a cross-cutting competency across police organisations. A similar trend is evident in the Czech sample, where a substantial proportion of respondents reported regular or occasional engagement in tasks involving elements of digital forensics. This shift necessitates a redefinition of educational models, which must reflect the need for fundamental forensic competencies even among non-specialised officers.

The identified competence gaps should not be interpreted as individual shortcomings of officers but rather as a consequence of a structural deficit within the system of professional education. Results from both samples consistently point to fragmentation of the training provision, limited access to accredited courses, and significant organisational barriers to participation. At the same time, the high and thematically specific demand for education—particularly in mobile forensics, evidence acquisition, and the handling of data from end devices—confirms that officers are aware of their competence limitations and are motivated to overcome them. The issue, therefore, lies not in motivation but in the absence of a systematic, standardised, and institutionally supported training framework.

An important role in this context is also played by technical and organisational conditions. The comparison of both samples shows that access to specialised forensic equipment is not uniformly ensured and varies significantly across units. While in the Czech environment, some respondents reported access to more specialised tools, the German sample shows a stronger reliance on standard computing resources. In both cases, however, technical infrastructure remains uneven, which may lead to differences in the quality of securing and analysing digital evidence and to potential procedural risks. This aspect further reinforces the need for standardisation of both technical and methodological procedures.

The structured relationship between environmental digitalisation, exposure to digital evidence, identified competence gaps, and the need for a systematic educational response is conceptualised in Figure 1. The model illustrates that increasing societal digitalisation leads to a growing importance of digital evidence, which in turn creates pressure on the professional competencies of police officers. If this pressure is not adequately reflected in training systems and institutional support, a structural competence deficit emerges, potentially affecting the effectiveness of policing. In this context, the DiForPol project can be understood as a targeted systemic response to the identified mismatch.

The DiForPol project represents an intervention framework aimed at strengthening police competencies in digital forensics through standardised and practice-oriented training. Its focus corresponds to the empirical findings of the study, particularly regarding the dominance of mobile devices and electronic communication as key sources of digital evidence. The emphasis on scenario-based training, simulated cases, and the use of realistic datasets reflects the preference structure of respondents in both samples and aligns with current trends in professional training of security forces.

The international dimension of the project is of particular importance, as it responds to the need for strengthening cross-border cooperation between the Czech and Saxon police forces. Comparative results indicate that both systems face similar challenges, creating opportunities for harmonisation of training standards, sharing of know-how, and strengthening interoperability. A joint educational platform based on compatible methodological approaches may significantly contribute to improving the effectiveness of cross-border investigations and to enhancing responses to increasingly transnational crime.

From a long-term internal security perspective, the DiForPol project can be understood as an investment in the human capital of law enforcement agencies. Strengthening competencies in digital forensics has the potential to generate secondary effects, including improved quality of evidence, reduction of procedural errors, shorter investigation times, and overall enhancement of operational readiness. In this sense, digital forensics represents not only a technical discipline but also a key element of modern security infrastructure.

It is, however, necessary to acknowledge the limitations of the study. The research is based on self-assessment by respondents, which may be influenced by subjective perceptions of their own competencies. The purposive sampling strategy also does not allow for full statistical representativeness in relation to entire police organisations in both countries. Nevertheless, these limitations do not diminish the value of the study as applied research, as the parallel data collection in two national contexts and the consistency of identified trends provide a robust basis for further research and policy-making.

Despite the high level of consistency between the Czech and Saxon samples, it is necessary to consider potential sources of variability and limitations in interpretation. Identified differences between the two environments, particularly in the availability of technical equipment and the structure of digital evidence used, may reflect institutional specifics of individual police organisations, differences in competency frameworks, organisational structures, and levels of centralisation of specialised units. At the same time, the use of self-reported data introduces the possibility of bias in

assessing competence levels. While these limitations cannot be fully eliminated, the parallel implementation of the study in two national contexts and the strong consistency of findings significantly enhance the explanatory value of the results and their interpretation within a broader European context.

Overall, the study confirms the existence of a structural mismatch between the dynamics of digitalisation in the security environment and the level of professional preparedness of law enforcement agencies. This mismatch represents a significant challenge for the present and future functioning of police institutions. At the same time, it creates space for targeted interventions, among which the DiForPol project represents a concrete and empirically grounded step towards strengthening the professional, technological, and institutional preparedness of law enforcement agencies in a digitally evolving security environment.

6. Conclusion

Digital evidence has become one of the key pillars of internal security in the contemporary security environment and a fundamental tool of everyday policing practice. Digital evidence has significant characteristics that distinguish it from traditional traces, as it is typically very large (in terms of data volume), dynamic, and can be located anywhere in cyberspace. The lifespan of such a trace can be very short, and any delays—both in the pre-prosecution process and during the investigation—inevitably lead to its loss. This is one of the reasons why the clearance rate for cybercrime is low [14].

The results of this study, based on a comparative analysis of data from the Police of the Czech Republic and the police of the Free State of Saxony, clearly confirm that law enforcement officers encounter digital traces across a wide spectrum of activities, regardless of the national context.

At the same time, both analysed samples revealed a pronounced tension between the high level of exposure to digital evidence and the limited level of professional competencies in digital forensics. The fact that approximately two-thirds of respondents in both countries possess only basic or no knowledge indicates that this issue cannot be considered a specific feature of a single institutional environment, but rather a broader structural phenomenon affecting European law enforcement agencies.

The comparative perspective further demonstrates that both systems face similar challenges in terms of technical infrastructure, availability of specialised tools, and organisation of training. Although certain differences can be identified, for example, in the structure of utilised technologies or equipment availability, the overall picture remains consistent: digital forensics is becoming a cross-cutting competency that extends beyond specialised units and increasingly permeates routine investigative and operational practice.

The empirical findings of this study thus confirm the need for a systemic and coordinated response in the areas of professional education, standardisation of procedures, and strengthening of technological preparedness within law enforcement agencies. In this context, the DiForPol project can be interpreted as a concrete example of such a response, grounded in the identified needs of practice while also reflecting the international dimension of security threats.

From the perspective of strategic internal security management, the ability to effectively work with digital evidence represents not only a professional skill but also a significant factor of institutional resilience. The systematic development of competencies in digital forensics, their standardisation, and their integration with international cooperation therefore constitute key prerequisites for the adaptation of law enforcement agencies to the conditions of digitalised crime and a dynamically evolving security environment.

The primary objective of the DiForPol project is to interconnect continuing education within Saxon and Czech police forces, thereby enhancing the competencies of investigative authorities in the field of mobile and digital forensics and improving cross-border cooperation in the Saxon–Czech border region. This is intended to facilitate the more efficient exchange of information obtained through police work between neighbouring law enforcement agencies. At the same time, the project may serve as a proof of concept for expanding bilateral or multilateral cooperation among law enforcement agencies across the European Union.

References

1. ENISA. *Threat Landscape 2023. Heraklion: European Union Agency for Cybersecurity*, 2023. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. [cit. 31.1.2026].
2. NATO. *Resilience and Civil Preparedness*. Brussels: NATO Headquarters, 2023. Available at: https://www.act.nato.int/article/resilience-and-civil-preparedness-in-nato/. [cit. 28.1.2026].
3. JÁNSKÝ, Jiří., TUŠER, Irena. Security Management—Quantitative Determination of Crime Risk in a Selected Region: Case Study. In: Tušer, I., Hošková-Mayerová, Š. (eds) *Trends and Future Directions in Security and Emergency Management. Lecture Notes in Networks and Systems*, vol 257, 2022, Springer, Cham. https://doi.org/10.1007/978-3-030-88907-4_12
4. TUŠER, Irena, POTŮČEK, Radovan, HOŠKOVÁ-MAYEROVÁ, Šárka. *Risks of the Effects of Restrictive Measures on the Democratic Foundations of a State*, Challenges to national defence in contemporary geopolitical situation; 2022, no. 1, 219-226, DOI 10.47459/cndcgs.2022.28

5. EUROPOL. EU *Serious and Organised Crime Threat Assessment (SOCTA*). The Hague: Europol, 2023. Available at: https://www.europol.europa.eu/publications-events/main-reports/socta-report. [cit. 29.1.2026].
6. CASEY, Eoghan. *Digital Evidence and Computer Crime*. 3rd ed. London: Academic Press, 2011. ISBN 978-0123742681.
7. NIST. *Guide to Integrating Forensic Techniques into Incident Response* (SP 800-86). Gaithersburg: NIST, 2022. Available at: SP 800-86, Guide to Integrating Forensic Techniques into Incident Response | CSRC. [cit. 28.1.2026].
8. OECD. *Strengthening Critical Infrastructure Resilience*. Paris: OECD Publishing, 2019. Available at: https://infrastructure-toolkit.oecd.org/governance/strengthen-critical-infrastructure-resilience/. [cit. 28.1.2026].
9. EUROPEAN COMMISSION. *EU Security Union Strategy*. Brussels: European Commission, 2020. Available at: https://ec.europa.eu/newsroom/pps/items/686851/#:~:text=On%20the%2024%20July%202020%2C%20the%20European%20Commission,fostering%20security%20for%20all%20those%20living%20in%20Europe. [cit. 29.1.2026].
10. CRESWELL, John W. Research *Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4th ed. Thousand Oaks: SAGE, 2014. ISBN 978-1452226101.
11. CEPOL. Law Enforcement Training Needs Assessment. Budapest: CEPOL, 2022. Available at: https://www.cepol.europa.eu/documents/european-union-strategic-training-needs-assessment-2022-2025. [cit. 31.1.2026].
12. CEPOL. Law Enforcement Training Needs Assessment. Budapest: CEPOL, 2022. Available at: https://www.cepol.europa.eu/documents/european-union-strategic-training-needs-assessment-2022-2025. [cit. 31.1.2026].
13. PAWLASZCZYK, Dirk. *Mobile Forensics – The End of a Golden Age?* J Forensic Sci & Criminal Inves, 2022, 15(4), 555917. DOI: 10.19080/JFSCI.2022.15.555917.
14. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC. p. 403. ISBN 978-80-88168-15-7