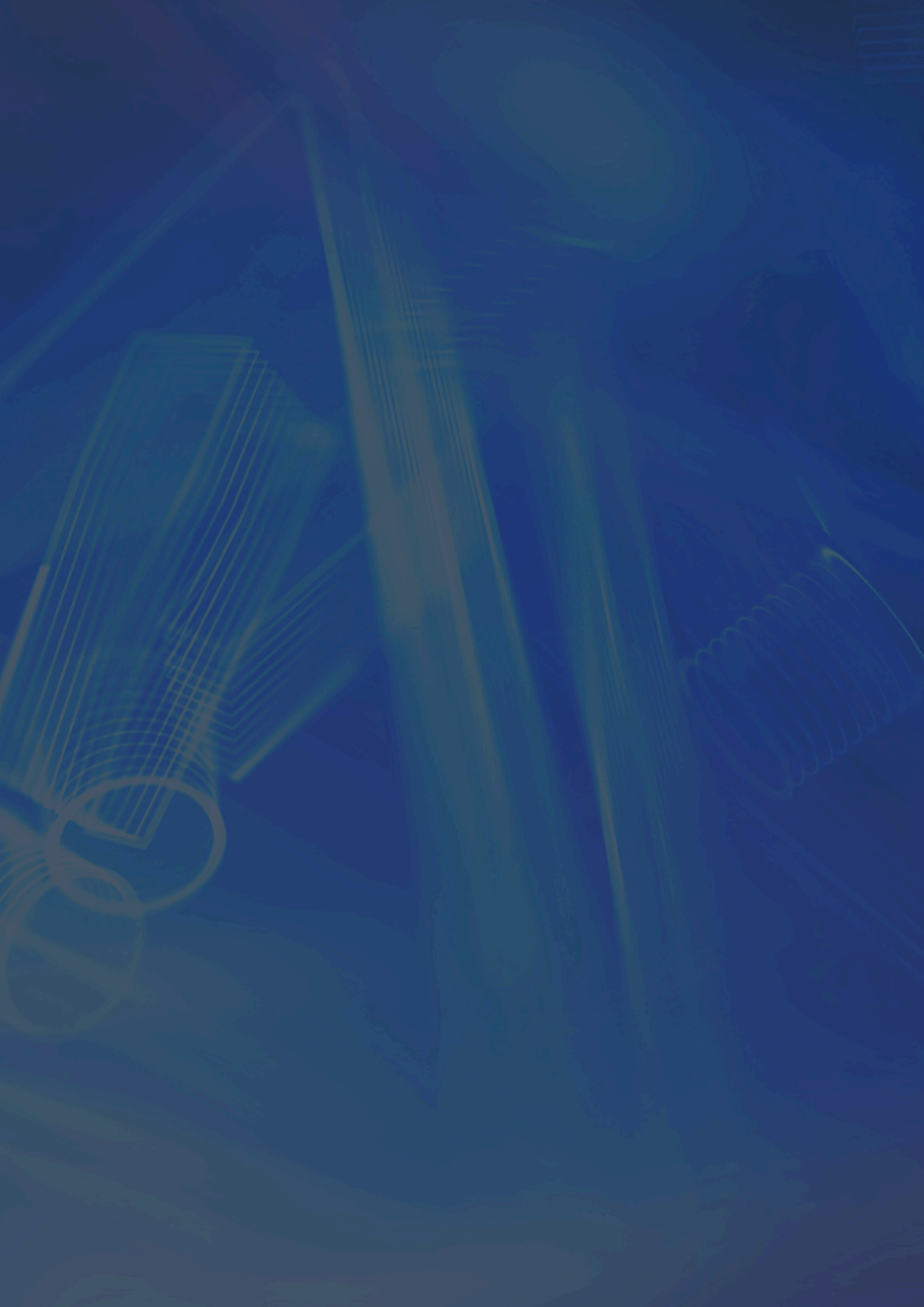
FLASH REPORT 08

DIGITAL TOOLS FOR ONLINE CRIME MONITORING: INVESTIGATIVE TECHNOLOGIES SUPPORTING LAW ENFORCEMENT AGENCIES

Main Authors
Andreas Kosmatopoulos (CERTH)

December 2025

ENACT.
European Network Against Crime and Terrorism



03

About ENACT

ENACT is a knowledge network focused on the fight against crime and terrorism (FCT). The network is funded under the Horizon Europe Framework Programme in Cluster 3 – Civil Security for Society. The project addresses the call topic HORIZON-CL3-2022-SSRI-01-02 'Knowledge Networks for Security Research & Innovation', aiming to collect, aggregate, process, disseminate and make the most of the existing knowledge in the FCT area.

The project aims to satisfy two major ambitions,

- Provide evidence-based support to the decision-makers in the EU research and innovation (R&I) ecosystem in the FCT domain, targeted explicitly at enabling more effective and efficient programming of EU-funded R&I for the fight against crime and terrorism.

- Act as a catalyst for the uptake of innovation by enhancing the visibility and reliability of innovative FCT security solutions.

Report Feedback

We're collecting feedback on this report through the EU Survey Platform, if you'd like to share your thoughts anonymously please click on the link below.

https://ec.europa.eu/eusurvey/runner/FR8-DigitalToolsOnlineCrime

Funded by
the European Union

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Copyright

Acknowledgement

This report was requested by AHEAD (Toward Sustainable Foresight Capabilities for Increased Civil Security). We are grateful for the request, engagement and feedback throughout the development of the report. AHEAD brings together 10 LEAs and seeks to establish and implement a sustainable, capability-based civil security foresight framework. This framework is designed to address the specific needs of civil security practitioners and decision-makers by generating comprehensive capability roadmaps for European civil security.
https://he-ahead-project.eu/

Acronyms

AI	Artificial Intelligence
CSAM	Child Sexual Abuse Materil
EDPS	European Data Protection Supervisor
ELS	Ethical, Legal, Societal
EU	European Union
FCT	Fight against Crime and Terrorism
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IoT	Internet of Things
ISP	Internet Service Provider
IT	Information Technology
LEAs	Law Enforcement Agencies
LLMs	Large Language Models
ML	Machine Learning
NLP	Natural Language Processing
OSINT	Open Source Intelligence
RL	Reinforcement Learning
SIEM	Security Information and Event Management
SKB	Structured Knowledge Base
TTPs	Tactics, Techniques and Procedures
URL	Uniform Resource Locator
VR	Virtual Reality
WWW	World Wide Web

05

Introduction

The World Wide Web (WWW) has been a prominent information system since its initial inception, offering a wide variety of services and functionalities, especially over the years following its holistic integration within modern applications and frameworks. A commonly used categorisation of the different portions of the Web based on their accessibility as well as their search engine indexability is the distinction between **Surface, Deep, and Dark Web**.

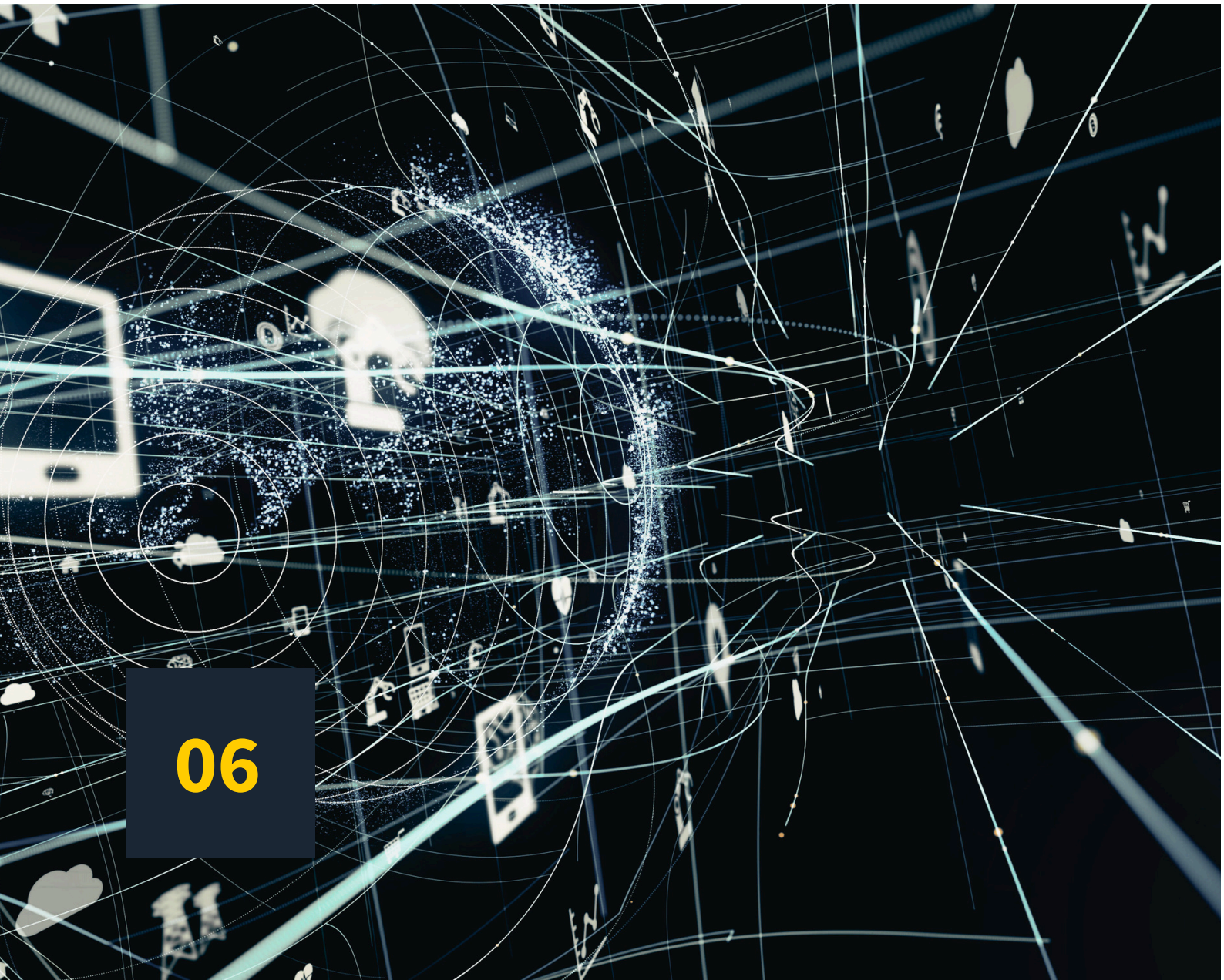
Surface Web refers to the parts of the WWW that can be searched or indexed by search engines and can be directly accessed by the general public. Conversely, the **Deep Web** encompasses all content that is not be indexed by search engines and resides behind login forms (e.g., banking or e-mail services), paywalls (e.g., academic journals or news sites) as well as dynamically generated pages (e.g., e-commerce product filters or flight search results). Finally, **Dark Web** comprises deliberately concealed websites and networks (e.g., I2P, Tor) that require the use of special software to access and navigate. The Dark Web is often associated with activities and services that are illicit in nature, such as crime, drug, and stolen data marketplaces, hacking services, human trafficking, and others. It is estimated that ~4-10% of the Web content corresponds to the Surface Web category, ~90-95% to the Deep Web layer and ~0.1%-1% to the Dark Web portion of the WWW.

Accessing and organising information across these web layers relies heavily on a process known as **web crawling**, which involves systematically browsing and indexing content (or gathering data in the form of targeted web scraping). While manual crawling can benefit from the nuance and context interpretation that experts and investigators can employ, it is prohibitively labour-intensive and unable to scale to the vast size of (a fraction of) the deep or dark web. On the other hand, automated web crawlers are able to index a vast amount of web pages exhibiting significant breadth and speed in their operational functionally. Typically, an **automated web crawler** is provided with a list of site URLs, fetches the content of those pages, extracts the hyperlinks and continues recursively. Automated web crawlers excel in open environments such as the surface web due to their inherent scalability over manual crawling performed by humans.

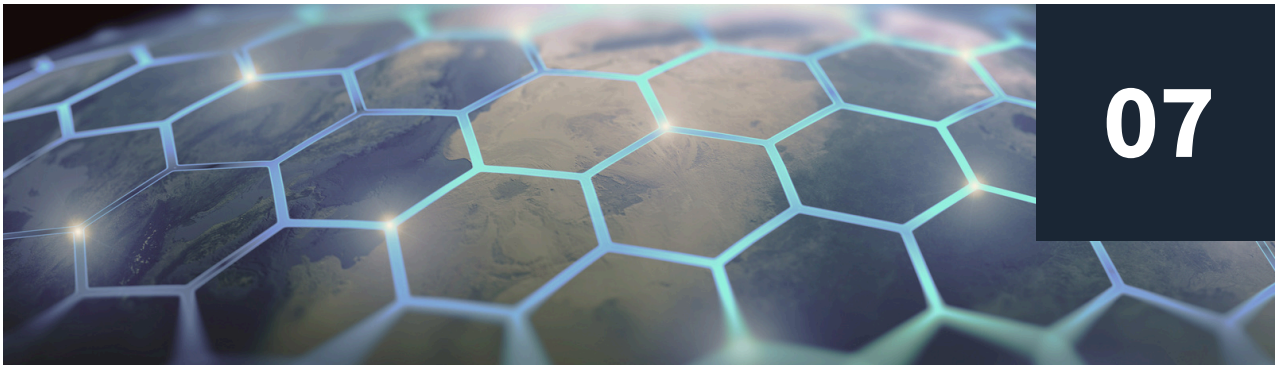
[1] Checkpoint (2025) Deep Web vs Dark Web. *Checkpoint.* https://www.checkpoint.com/cyber-hub/cyber-security/what-is-the-dark-web/deep-web-vs-dark-web/
[2] Bergman, M. (2001) White Paper: The Deep Web: Surfacing Hidden Value. *The Journal of Electronic Publishing.* 7(1). https://doi.org/10.3998/3336451.0007.104
[3] *Barring any anti-bot measures or policies in place.*

Building on the intuition behind web crawlers, web patrolling bots represent a specialised type of (semi-)automated crawler with the design purpose of detecting, monitoring and potentially alerting or responding to specific types of illegal or suspicious activity online. They usually feature real-time surveillance or threat detection, often include AI/ML models for identifying the respective potentially harmful content and are intended to operate as part of a comprehensive LEA workflow. In tandem with web patrolling bots, the concept of **digital twins** offers law enforcement agents a unique approach in potentially supporting their work and activities. More specifically, a digital twin consists of a physical entity (such as an object, model, or person), their virtual representation, and the bidirectional flow of data that connects them. In the context of policing and investigation, digital twins could support investigators by enabling advanced training and analysis capabilities in virtual environments while also augmenting operational intelligence through the use of virtual police assistants.

The report first outlines relevant material from ENACT's Structured Knowledge Base (SKB), followed by an in-depth examination of the policy frameworks, technological landscape and ethical, legal, and societal (ELS) considerations associated with web crawling, digital twin and patrolling technologies in support of law enforcement activities.



06



07

Statistical analysis of ENACT's structured knowledge base

In alignment with ENACT's mission to consolidate and make use of existing knowledge in support of the fight against crime and terrorism (FCT), a comprehensive data collection and characterisation process was undertaken, guided by the EU Civil Security (EUCS) Taxonomy as established by the European Commission in the 2021 EU Security Market Study. This analysis identified a cluster of observations of high relevance to the domain of digital investigative technologies, which have been systematically catalogued in ENACT's structured knowledge base (SKB). Furthermore, several projects, digital tools and initiatives were considered and catalogued in Appendix A.1 to enhance the overall scope and depth of the report.

Figure 1 illustrates that, as expected, the vast majority of observations related to the topic have been classified under cybercrime, reflecting the centrality of online criminal activity in content around web crawlers, patrolling bots, and digital twins. The remaining three categories show only marginal differences in their proportions, suggesting a relatively balanced representation across secondary areas of interest.

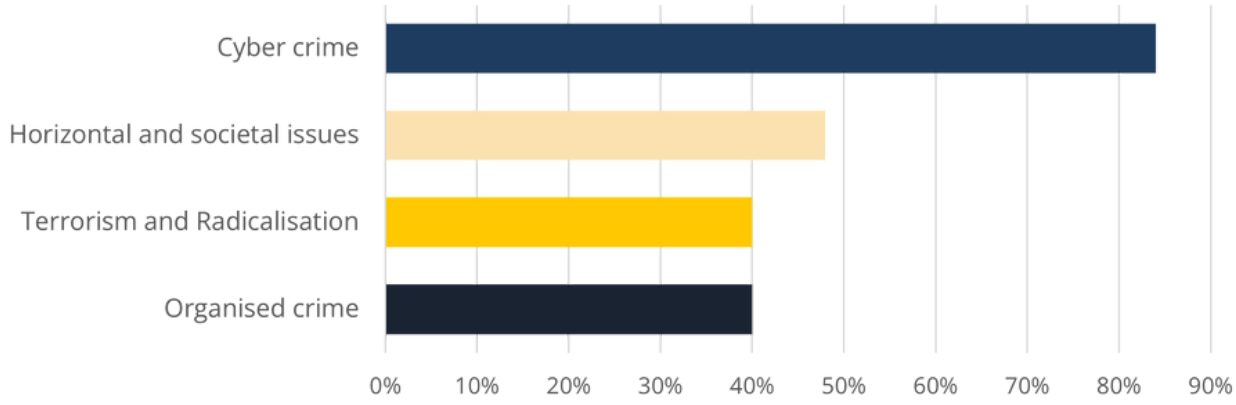


Figure 1 - Classification of observations related to Investigative Web Technologies for LEAs.

Figure 2 showcases the classification of observations according to the EUCS Level 3 (L3) subcategories under the broader EUCS Level 2 (L2) categories defined in the SKB [4]. The vast majority of observations are associated with "CC: Dark net (illegal markets / cryptocurrencies), indicating its strong relevance within the knowledge base. Other frequently occurring subcategories include "CC: Online identity theft" and "CC: Digital Forensics", further illustrating the thematic areas most linked to the relevant content.

[4] *For reasons of clarity and readability, Figure 2 only shows the subcategories with more than 10% participation in the relevant observations of the SKB.*

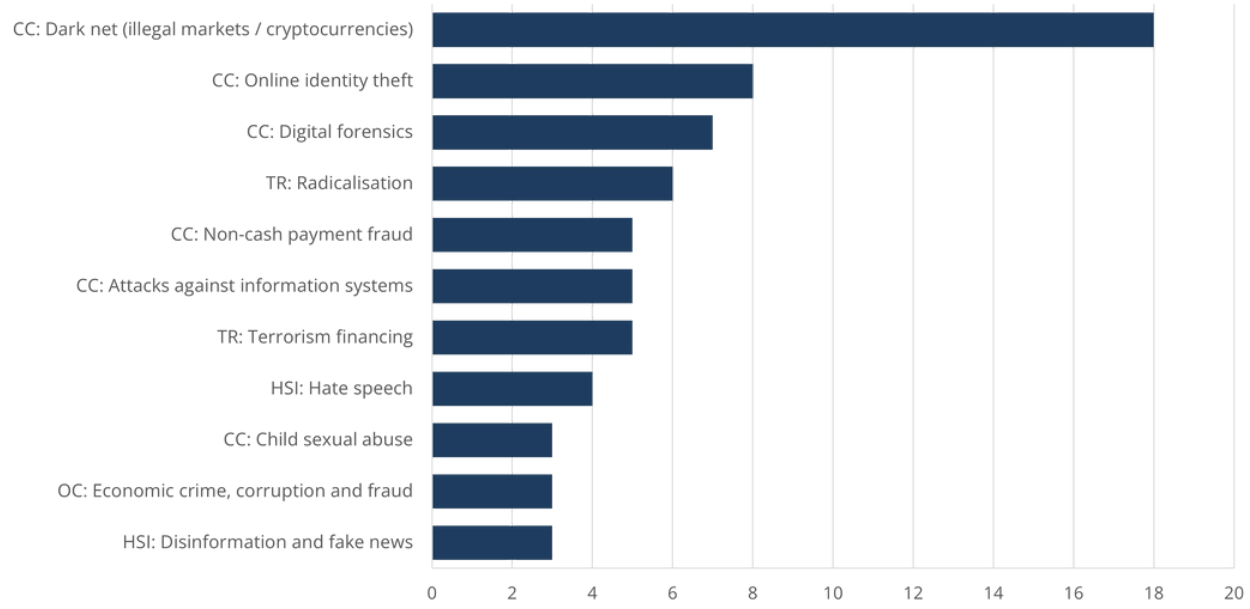


Figure 2 - Classification of observations related to Investigative Web Technologies for LEAs (EUCS L3 / >10%)

Figure 3 illustrates how observations in the SKB relevant to web crawlers, patrolling bots, and digital twins are distributed across the EUCS Taxonomy Functions. The most prominent functions are associated with "Data, information & intelligence gathering management, and exploitation", followed by notable associations with "Investigation and forensics", "Security of information systems, networks and hardware", and "Monitoring and surveillance of environments and activities".

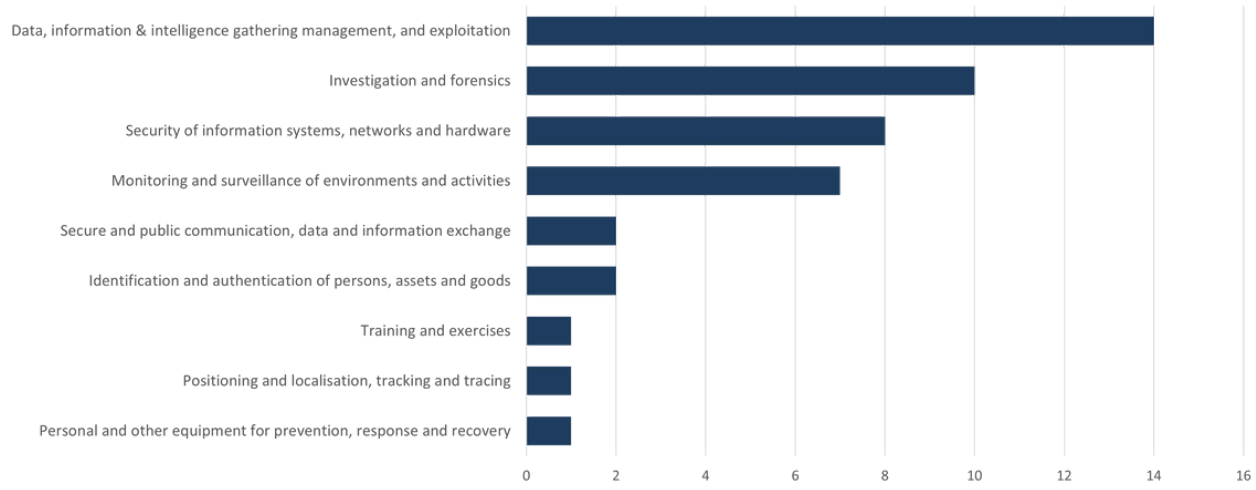


Figure 3 -Mapping of the SKB's observations according to the EUCS Taxonomy Functions)

Finally, Figure 4 presents a similar analysis, this time focusing on the relevance of observations in relation to the EUCS Taxonomy Technologies. As expected, "Internet-based investigation" shows a strong alignment with the topic of the report, with "Data analytics", and "Digital forensics" also appearing frequently among the associated technologies.

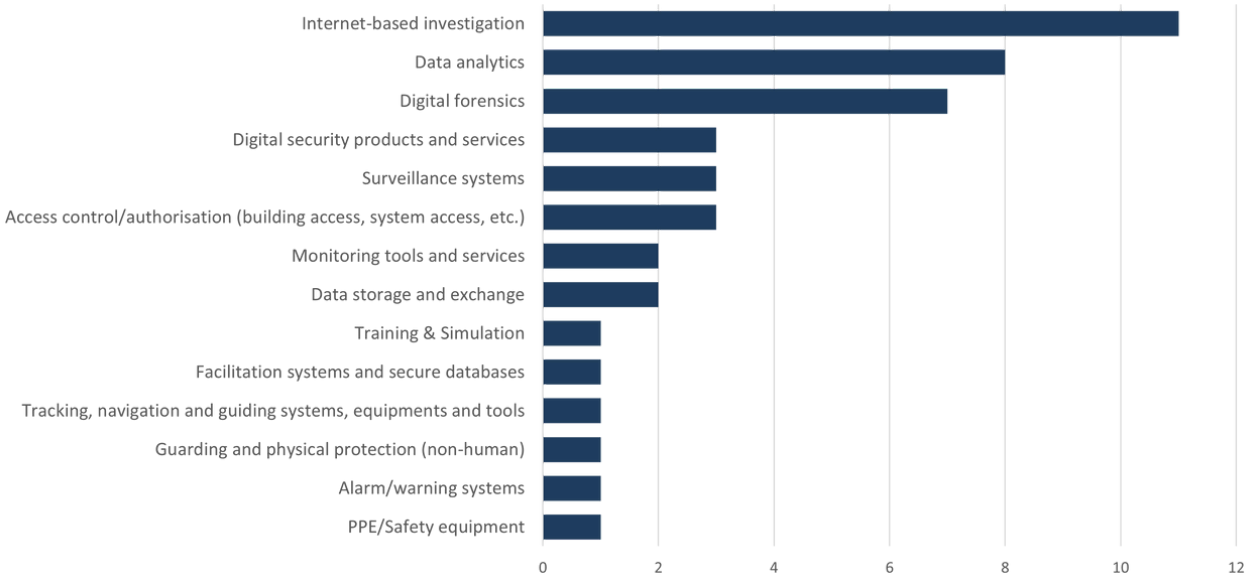
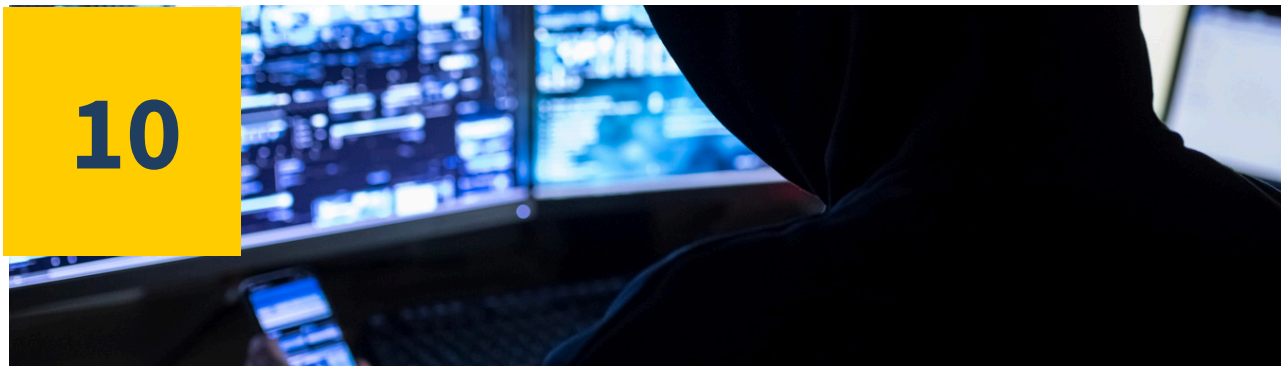


Figure 4 -Mapping of the SKB's observations according to the EUCS Taxonomy Functions)

09



Technology view

The first practical application of web crawlers originated in the early 1990s. As the web transitioned into an expanded network that featured numerous websites of different organizations and topics, it became apparent that there was a need for automated crawlers that could reliably surpass human-curated lists and directories [5]. At its core, an automated web crawler featured a crawl frontier (i.e., a queue of URLs to fetch), an HTTP client that would function as a mechanism to retrieve page content, a parser designed to extract links from retrieved pages and "push" them in the crawl frontier, and mechanisms that dictated the order of URL visits [6] (scheduler) or prevented the web crawler from revisiting the same URLs in an infinite loop fashion.

Early crawlers such as the World Wide Web Wanderer [7], WebCrawler [8], and Lycos [9] established principles that are still followed today, such as the use of robots.txt to provide a website's crawler instructions or politeness delays between requests to avoid overloading sites. Given its prevalence, the primary target of these early attempts was the surface web, and each crawler would perform this procedure using a seed set of known websites as a starting point. Later approaches by Google capitalised on the use of preference ranking among webpages (pioneered by Lycos) to augment automatic indexing using link analysis in the form of the PageRank [10] algorithm. Building on these foundational principles, the following sub-sections explore how modern web crawling technologies - and, subsequently, autonomous patrolling agents and digital twins- have evolved to address the scale, complexity, and specificity of contemporary investigative contexts.

[5] Dean, K. (2025) The History of Search Engines. *SystemTek.* https://www.systemtek.co.uk/2025/03/the-history-of-search-engines/

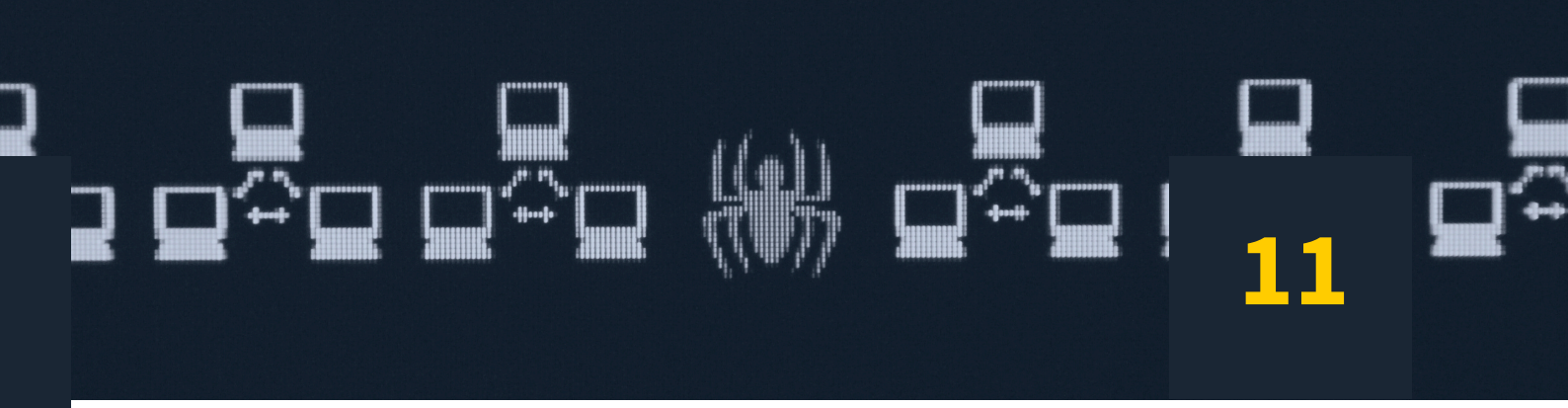
[6] *Two noteworthy examples are breadth-first crawling where a new URL link is placed at the end of the crawl frontier, and depth-first crawling where a new URL is placed at the start of the crawl frontier.*

[7] Gray, M. (1996) Internet Statistics - Growth and Usage of the Web and the Internet. https://www.mit.edu/people/mkgray/net/

[8] https://www.webcrawler.com/

[9] https://www.lycos.com/

[10] Page, L., Brin, S., Motwani, R., & Winograd, T. (1999). The PageRank citation ranking: Bringing order to the web. *Stanford infolab.*



Web crawlers

While the core principles behind a contemporary automated web crawler (i.e., crawl frontier, scheduler, link parser) have remained mostly the same to early web crawlers, several things regarding their applicability and operating conditions have changed considerably. Modern crawlers are designed to operate on a targeted fashion around specific goals or domains (compared to the indiscriminate exploration pattern of early crawlers) and operate on a significantly larger scale across distributed and cloud-based infrastructures while complexities revolving around the nature of online content have risen. Specifically, dynamic content and content rendered client-side via JavaScript characterise the majority of modern web pages, thus requiring more sophisticated tools to access. Additionally, anti-crawling techniques (such as CAPTCHAs and IP throttling) have forced modern crawlers to simulate human behaviour and rotate IP addresses in an attempt to operate and remain effective. These issues are further exacerbated when crawling the credential-protected deep web or the anonymised dark web, and bring forth the need for specialised approaches to access and extract data.

In order to enhance their capabilities, modern crawlers employ Machine Learning (ML) and semantic techniques to improve precision and efficiency. Focused crawling uses either rule-based or ML-enhanced classifiers to only crawl pages that are relevant to a specific topic [11] while predictive strategies discern noteworthy pages by estimating which links are likely to lead to valuable content based on contextual cues and historical data [12]. Finally, semantic crawling revolves around the use of Natural Language Processing (NLP) to prioritise pages based on their meaning instead of simply the existing link structure [13].

A variety of general-purpose modern frameworks support a selection of these techniques either natively, through plugins or through custom logic provided by manual configuration. Tools such as **Scrapy** [14] and **Apache Nutch** [15] offer topic-focused or metadata-aware crawling, with Nutch supporting link filtering, custom scoring, and integration with semantic processing plugins. **StormCrawler** [16] provides scalable infrastructure for web crawling and can prioritise URLs based on context or past crawling performance. Finally, **Crawlee** [17] is able to perform dynamic content crawling while also supporting focused crawling and semantic prioritisation. Despite having a general design, these platforms serve as the technical foundation for more specialised investigative systems, which are covered in the section that follows.

[11] Chakrabarti, S., Van den Berg, M., & Dom, B. (1999). Focused crawling: a new approach to topic-specific Web resource discovery. *Computer networks*, 31(11-16), 1623-1640.
[12] Dang, T. K. N., Bucur, D., Atil, B., Pitel, G., Ruis, F., Kadkhodaei, H., & Litvak, N. (2023). Look back, look around: A systematic analysis of effective predictors for new outlinks in focused Web crawling. *Knowledge-based systems*, 260, 110126.
[13] Dong, H., & Hussain, F. K. (2013). SOF: a semi-supervised ontology-learning-based focused crawler. *Concurrency and Computation: Practice and Experience*, 25(12), 1755-1770.
[14] https://scrapy.org/
[15] https://nutch.apache.org/
[16] https://stormcrawler.apache.org/
[17] https://crawlee.dev/

Web Crawling in the Law Enforcement Context

General-purpose crawlers aim for breadth or domain-specific crawling while investigative-focused crawlers are tailored for targeted data collection, operating across a range of environments. Based on the task at hand, investigative-focused crawling may focus from surface web forums and social platforms to credential-protected deep web pages and dark web marketplaces.

Various projects funded under the Horizon 2020 programme have attempted to integrate web crawling in the law enforcement context. The **DANTE** platform [18] employed multilingual crawling featuring analytics model with the goal of identifying propaganda, financial links across surface and dark web domains, and recruitment material. Similarly, in the **TENSOR** [19] project, an integrated platform was implemented to detect terrorist-generated content on the surface, deep, and dark web- using crawling, NLP technologies, and multidimensional analysis. The **TITANIUM** project [20] enabled LEAs to trace illicit transactions across darknet markets by correlating web data with blockchain analysis while the commercial platform Cerberus [21]provides deep and dark web search capabilities through an indexed, queryable interface without requiring direct access to anonymised networks.

Several crawlers employed by LEAs offer features beyond raw data collection, such as cross-referencing with threat intelligence databases or web content aggregation. Specifically, **Web-IQ Voyager** [22] aggregates surface and dark web content into dashboards suitable for use by investigators and includes modules for child protection, extremism, and fraud monitoring. The **Internet-Forum-Profile-Text-Analyser (IFPTA)** tool, offered as part of the **ASGARD** platform [23], uses crawled forum data to support the early identification of suspect narratives or users. The **ARTE-Fact tool**, developed within the **PREVISION** platform [24], focuses on using targeted crawl-and-detect approaches to automate the discovery of stolen cultural heritage objects that exist across online marketplaces. As these tools continue to evolve, they offer LEAs more refined and purposeful access to the online spaces most relevant to their investigations across a wide range of digital contexts.

[18] DANTE - Detecting and ANalysing TErrorist-related online contents and financing activities. https://cordis.europa.eu/project/id/700367
[19] TENSOR - Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition. https://cordis.europa.eu/project/id/700024
[20] TITANIUM - ools for the Investigation of Transactions in Underground Markets. https://cordis.europa.eu/project/id/740558
[21] Searchlight Cyber (2025) Cereberus. https://slcyber.io/dark-web-security-products/cerberus/
[22] Web-IQ (2025) Voyager. https://www.web-iq.com/voyager
[23] ASGARD - Analysis System for Gathered Raw Data. https://cordis.europa.eu/project/id/700381
[24] PREVISION - Prediction and Visual Intelligence for Security Information. https://cordis.europa.eu/project/id/833115

Adaptive Monitoring in Web Intelligence

Typically, web crawlers operate in a scheduled fashion by systematically traversing and indexing large volumes of content with little to no awareness of context or temporal urgency. Patrolling (or autonomous) agents are designed in a different way that permits them to be selective, persistent, and often event-driven. Specifically, patrolling agents continuously monitor a specific set of sources such as forums, news feeds, or social media, and based on new or modified content perform a predefined set of actions.

Their key characteristic is the ability to perform (near) real-time detection and usually feature a selection of semantic filtering or behavioural pattern recognition capabilities that aid them in their indented functionalities. They are designed with a long-running focus on reactivity for fast-changing and volatile environments such as political discussions, disinformation campaigns, hate speech incidents or online harassment networks and, unlike crawlers that passively revisit pages on a schedule, can respond dynamically to relevant content by flagging changes, issuing alerts or triggering follow-up actions.

Several general-use case platforms operate under these principles. **Google's real-time indexing mechanisms** [25] permit the (near) real-time indexing for high authority or priority websites (such as news outlets, job posting, or livestream video pages) while **Twitter's internal compliance bots** [26] use AI-driven content classification to flag posts that violate community standards, with the ability to trigger automated or human review. Until its deprecation, **CrowdTangle** [27] focused on tracking viral content across Facebook and Instagram. Similarly, a wide variety of social media and consumer intelligence is gathered through tools such as **Brandwatch** [28], **Talkwalker** [29] and **Meltwater** [30] that continuously monitor millions of sources for emerging trends, sentiment shifts, and entity mentions. The widespread use of these tools in commercial and civic contexts underscores their maturity and potential, suggesting that similarly valuable insights could be achieved in specialised domains such as investigative and law enforcement operations.

[25] Google (n.d.) Indexing API Quickstart. https://developers.google.com/search/apis/indexing-api/v3/quickstart
[26] X (2021) An update to the Twitter Transparency Center. https://blog.x.com/en_us/topics/company/2021/an-update-to-the-twitter-transparency-center
[27] Meta (2024) CrowdTangle. https://transparency.meta.com/researchtools/other-data-catalogue/crowdtangle/
[28] https://www.brandwatch.com
[29] https://www.talkwalker.com/
[30] https://www.meltwater.com

Adaptive Monitoring in Web Intelligence

Recent years have seen the extension of legal enforcement agencies' capabilities related to surveillance, early warning, and threat detection, through the integration of patrolling bots and autonomous agents into their operational workflow. Unlike traditional techniques that focus on retrospective data analysis, autonomous agents and patrolling bots offer (near) real-time scrutiny of online behaviours, making them particularly valuable in critical contexts such as the detection of child exploitation material, cybercrime, and radicalisation monitoring.

Research and development efforts under EU-funded projects have contributed to the expanding capabilities of autonomous agents in the law enforcement context. The **RED-Alert** platform [31] monitored online communication channels for radicalisation cues by combining social media scraping, real-time NLP-based content analysis, and social network mapping. The **INSIKT** project [32] focused on developing multilingual and deep learning-based monitoring tools to detect radical content and covert online radicalisation in (near) real-time. Similarly, **CyberSANE** [33] deployed real-time threat-detection monitoring tools that continuously patrolled IT infrastructures and web sources to identify indicators of compromise or early signs of cyberattacks.

Other projects have been developed to address more specialised investigative domains. **Project Arachnid** [34], led by the Canadian Centre for Child Protection, scans millions of websites daily (including the dark web) for child sexual abuse material (CSAM), automatically flagging and classifying harmful content for removal or investigation. Likewise, **Tangles** [35], developed by Cobwebs Technologies (now part of PenLink), provides real-time monitoring of the surface, deep, and dark web, focusing on organised crime, trafficking, and extremist networks. The platform supports automated data collection, link analysis, and alerting capabilities, enabling investigators to identify connections between individuals, events, or online identities across multiple platforms.

Data Representation through Digital Twins

The term digital twin describes the virtual representation of real-world entities or systems that are data-driven. While the term originated in industrial engineering, it has since been applied across numerous domains, including healthcare [36], urban planning [37], and more recently, public safety and criminal investigations [38]. Specifically in the context of investigative modelling, digital twins offer interactive environments that, unlike static dashboards, evolve in real time and allow investigators to simulate scenarios, replay events, and test decisions before acting. Digital twins enable a shift from reactive analysis to proactive decision-making and paired with crawlers and autonomous patrolling agents, they can function as advanced decision-support systems for complex, high-stakes environments.

[31] RED-Alert - Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing. https://cordis.europa.eu/project/id/740688
[32] INSIKT - Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization. https://cordis.europa.eu/project/id/767542
[33] CyberSANE - Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures. https://cordis.europa.eu/project/id/833683
[34] Project Arachnid. https://www.projectarachnid.ca
[35] PenLink (2025) Open-Source Intelligence, Simplified. https://www.penlink.com/platform/open-source-intelligence/
[36] Papachristou, K., Katsakiori, P. F., Papadimitroulas, P., Strigari, L., & Kagadis, G. C. (2024). Digital twins' advancements and applications in healthcare, towards precision medicine. *Journal of Personalized Medicine*, 14(11), 1101.
[37] Huzzat, A., Anpalagan, A., Khwaja, A. S., Woungang, I., Alnoman, A. A., & Pillai, A. S. (2025). A comprehensive review of digital twin technologies in smart cities. *Digital Engineering*, 100040.
[38] Asadi, A. R., Akinremi, T. P., Appiah, J. K., Jayathilake, H. M., Ibitoye, O., & Said, H. (2025). Bits, Bytes, and Bars: Towards a Digital Twin of the US Criminal Justice System. *International Journal of Human–Computer Interaction*, 1-22.

Digital Twins in the Law Enforcement Context

Over the recent years, the operational planning of law enforcement agencies has steadily increased the incorporation of digital twin technologies to enable the real-time integration and simulation of complex environments leading to effective proactive and reactive response.

The **INFINITY** project [39] employs digital twin technology with AI and virtual reality (VR) to support collaborative investigations, allowing LEAs to explore and analyse multimodal case data in immersive environments. **LAW-GAME** [40] applies similar principles in a training context, enabling officers to practice procedures and tactical decisions in realistic, AI-driven simulations. **TESTUDO** [41] extends the concept into critical infrastructure protection, combining autonomous robotic patrols with a real-time digital twin of critical sites to detect intrusions and coordinate responses.

In broader safety and urban management domains, **PANTHEON** [42] supports disaster resilience by modelling cities through ”Internet of Things” (IoT) and drone data, offering LEAs tools for simulating incidents and optimising emergency coordination. The **Crowd Safety Manager** [43] provides a localised 3D digital twin of urban areas to track crowd density and movement during large events so as to support crowd management at both the planning and operation phases **Frontex** has also launched a contest [44] to develop digital twin solutions for border surveillance, enabling simulation of terrain, movement, and system performance in challenging environments. Lastly, **SHIELD4CROWD** [45] advocated for research, incorporation, and funding of projects related to digital twins, recognising their potential to enhance situational awareness and coordination during security incidents in public spaces.

AI-based Honeypots for the Detection of Individuals Engaging in Criminal Activities

Honeypots are decoy systems designed to attract adversaries into controlled environments where their actions can be observed without risking production assets. They provide actionable intelligence on attacker tactics, techniques, and procedures (TTPs) and have become integral to modern defensive strategies [46][47]. Additionally, honeypots are utilised in conjunction with other security components (e.g., Intrusion Detection (IDS) and Security Information and Event Management (SIEM) systems) in order to improve and enhance their detection performance.

[39] INFINITY - IMMERSE. INTERACT. INVESTIGATE. https://cordis.europa.eu/project/id/883293
[40] LAW GAME - An Interactive, Collaborative Digital Gamification Approach to Effective Experiential Training and Prediction of Criminal Actions. https://cordis.europa.eu/project/id/101021714
[41] TESTUDO - Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention. https://cordis.europa.eu/project/id/101121258
[42] PANTHEON - Community-Based Smart City Digital Twin Platform for Optimised DRM operations and Enhanced Community Disaster Resilience. https://cordis.europa.eu/project/id/101074008
[43] Krishnakumari, P., Hoogendoorn-Lanser, S., Steenbakkers, J., & Hoogendoorn, S. (2023). Crowd Safety Manager: Towards Data-Driven Active Decision Support for Planning and Control of Crowd Events. *arXiv preprint* arXiv:2308.00076.
[44] Frontex (2025) Winners of the Prize Contest AWARDED - Congratulations!. https://www.frontex.europa.eu/innovation/research-and-innovation/prize-contests/prize-award-contest-on-copernicus-border-surveillance-service-evolution-CczoJ8
[45] SHIELD4CROWD - Setting baseline for a PCP Heightening Innovation Procurements in the European security ecosystem and Leveraging synergies through Dissemination activities for CROWD management. https://cordis.europa.eu/project/id/101121171

Nevertheless, despite their value, conventional honeypots are constrained by limited realism and static behaviour. In particular, low-interaction designs are easily fingerprinted by attackers and quickly bypassed, whereas high-interaction counterparts provide greater realism but entail substantial resource demands and produce voluminous data that can be challenging to manage [48][49][50]. Furthermore, conventional honeypots introduce additional limitations including scalability (i.e., honeypots are typically deployed in limited numbers, leaving much of the attack surface uncovered), data overload (i.e., large quantities of noisy logs drowning valuable insights), inadequate detection of advanced or evolving attack methods due to static configurations, and adversarial awareness, where attackers actively fingerprint honeypots and feed misleading information. Collectively, these weaknesses restrict the ability of honeypots to sustain interaction with the attackers and deliver accurate quality intelligence. Consequently, these challenges highlight the need for systems that can adapt dynamically and maintain credibility over extended interactions.

Artificial Intelligence offers a pathway to address these shortcomings. Machine learning enables honeypots to adapt responses in real time, improving believability and reducing analyst workload. For example, supervised learning approaches such as Random Forests have achieved detection accuracies of up to 98% when classifying honeypot-directed traffic [48]. Reinforcement Learning (RL) allows honeypots to model attacker–defender interactions as sequential decision processes and optimise responses to maximise engagement [50]. Generative AI, particularly Large Language Models (LLMs), enables dynamic simulation of system outputs, ranging from shell commands to API responses, making honeypots significantly harder to distinguish from real targets [51][52][53].

Several concrete implementations in the literature demonstrate technological feasibility. **HoneyIoT** [50] uses RL and Markov decision processes to learn device-specific responses; deployed on the Internet, it deceived adversaries during reconnaissance and captured real IoT malware samples. **shellLM** [52] leverages LLMs to generate Linux shell outputs, achieving a 90% true-negative rate when tested by security experts, who were unable to distinguish it from genuine environments. **DecoyPot** [53] employs retrieval-augmented LLMs to create dynamic API outputs, reaching a similarity score of 0.978 compared with real services. In addition, **ChatGPT**-based honeypots have been shown to engage attackers in natural-language conversations, eliciting behavioural insights and prolonging interaction [51]. These approaches collectively extend attacker dwell time, strengthen deception realism, and provide defenders with higher-quality intelligence artefacts.

[46] Sezgin, A., Özkan, G., & Boyacı, A. (2025, April). Advancements and Challenges in AI-Powered Honeypots: A Comparative Study of Detection, Engagement and Ethical Implications. *In 2025 13th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.
[47] Aradi, Z., & Bánáti, A. (2025, January). The Role of Honeypots in Modern Cybersecurity Strategies. *In 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)* (pp. 000189-000196). IEEE.
[48] Alosaimi, R., & Alatawi, A. (2025, April). Leveraging Artificial Intelligence for Enhancing Real-Time Honeypot Security. *In 2025 4th International Conference on Computing and Information Technology (ICCIT)* (pp. 717-722). IEEE.
[49] Scanlan, J., Watters, P. A., Prichard, J., Hunn, C., Spiranovic, C., & Wortley, R. (2022). *Creating honeypots to prevent online child exploitation. Future Internet*, 14(4), 121.
[50] Guan, C., Liu, H., Cao, G., Zhu, S., & La Porta, T. (2023, May). HoneyIoT: Adaptive high-interaction honeypot for iot devices through reinforcement learning. *In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 49-59).
[51] Raut, U., Nagarkar, A., Talnikar, C., Mokashi, M., & Sharma, R. (2023, August). Engaging attackers with a highly interactive honeypot system using chatgpt. *In 2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA)* (pp. 1-5). IEEE.
[52] Sladić, M., Valeros, V., Catania, C., & Garcia, S. (2024, July). Llm in the shell: Generative honeypots. I*n 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 430-435). IEEE.
[53] Sezgin, A., & Boyacı, A. (2025). DecoyPot: A large language model-driven web API honeypot for realistic attacker engagement. *Computers & Security*, 154, 104458.

Policy view

Technology and its capabilities are very important for online patrols. Over the past 20 years, the development has taken major steps, and crime has moved online in many ways. For law enforcement authorities, this constitutes continuous development measures from the perspective of both technology and legislation. The sooner the new legislation can respond to new criminal phenomena, the smaller the time gap and the proceeds of crime in general will be. As the Internet is international, investigative methods and legislation related to patrols must also be international.

In this section, we will focus on the EU and Global level policy expressions, including the Dark Web and ending the section with European Commission FCT policies.

European Union Policies

Europol's Framework for Ethical Technology in Law Enforcement

Europol has published a framework to guide the ethical use of technology in law enforcement, ensuring that implementations respect fundamental rights and freedoms. Established in 2019, the **Europol Innovation Lab** fosters innovation to support EU law enforcement through collaborative, technology-driven solutions aligned with Europol's Strategy 2020+. The **European Clearing Board** (EuCB), created in 2020, connects innovation leads from EU and Schengen countries to coordinate tools and methods for operations and investigations. Under EuCB, the **Strategic Group on Technology and Ethics**, formed in 2021, developed guidelines to assess the ethical use of emerging technologies in law enforcement. These guidelines offer a structured, seven-step method grounded in shared values, aiming to support transparent, context-specific, and ethically defensible decisions—especially in areas where law and ethics intersect or legal clarity is lacking. Use cases illustrate practical application but are not legal endorsements [54].

[54] Europol (2025), Assessing Technologies in Law enforcement. A method for ethical decision making, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/publications-events/publications/assessing-technologies-in-law-enforcement-method-for-ethical-decision-making

EU Directive on Network and Information Security (NIS2 Directive)

The NIS2 Directive (Directive 2022/2555) [55] sets a unified EU cybersecurity framework, expanding on NIS1 to cover 18 critical sectors with stricter rules, broader scope, and stronger oversight. It mandates Member States to adopt national strategies, enhance capabilities, and ensure risk management and incident reporting by medium and large entities. The directive also encourages law enforcement access to network data for investigative purposes, promotes cross-border cooperation via Computer Security Incident Response Teams (CSIRTs) and the European cyber crisis liaison organization network (EU-CyCLONe) for crisis response, while introducing board-level accountability. The NIS Cooperation Group supports implementation through strategic guidance and information sharing.

ePrivacy Directive & GDPR

The 2002 ePrivacy Directive [56] safeguards digital communication privacy and regulates tracking and monitoring. With the rise of new technologies and the GDPR's entry into force, the EU proposed an update in 2017 to address emerging issues like IoT communication and privacy on public networks.

Global/International Policies & Frameworks

Budapest Convention on Cybercrime (2001)

The Budapest Convention [57] is not just a legal instrument but a platform for international cooperation, enabling practitioners to share experiences and collaborate beyond its formal provisions—even in emergencies. Any country can use it as a guideline or model law, with additional benefits available to Parties. Widely adopted in Europe and beyond, it is he first international treaty addressing internet and computer crime by harmonising national laws and improving investigative techniques and encourages international cooperation for cybercrime investigations.

Tallinn Manual (NATO)

The Tallin Manual [58] is a non-binding academic study on how international law applies to cyber operations and conflict. It influences military and intelligence policies on web-based investigations and digital warfare. The Tallinn Manual, developed by the CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence), is a leading academic resource on how international law applies to cyber operations. The original 2013 edition focused on cyber activities amounting to use of force or occurring during armed conflict, while Tallinn Manual 2.0 (2017) expanded coverage to day-to-day cyber incidents below those thresholds. In response to evolving state practice, the Tallinn Manual 3.0 Project was launched in 2021 as a five-year initiative to revise and expand the Manual. It remains a non-binding, expert-led guide aiming for legal objectivity, engaging global legal scholars and states to reflect diverse perspectives on international cyber law.

[55] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)
[56] European Data Protection Supervisor (2025) ePrivacy Directive. https://www.edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en
[57] The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. https://www.coe.int/en/web/cybercrime/the-budapest-convention
[58] NATO (2017) The Tallinn Manual. *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/research/tallinn-manual/

United Kingdom

Investigatory Powers Act (2016)

The Investigatory Powers Act 2016 [59] provides a clear legal framework for UK law enforcement and intelligence agencies to access communications data. It consolidates existing powers, introduces stronger oversight with a judicial approval process (“double-lock”), and modernises capabilities for the digital age (such as requiring internet connection records to support investigations). From June 2018, interception warrants must be authorised by the Secretary of State and approved by an independent Judicial Commissioner, under strict conditions related to national security, economic well-being, or serious crime, with safeguards to protect privacy. It allows GCHQ (the UK's intelligence, security and cyber agency) and law enforcement to perform "bulk interception" of internet traffic and requires Internet Service Providers (ISPs) to retain metadata (e.g., browsing history) for up to 12 months.

India

Information Technology Act (2000), Rules amended in 2021

The Information Technology Act, 2000 (India) [60] grants legal recognition to electronic commerce and digital records, enabling electronic transactions and communication in place of paper-based methods. It also facilitates e-filing with government agencies and amends key laws to support digital processes, aligning with the UN Model Law on Electronic Commerce to promote legal uniformity and efficient e-governance. Additionally, it grants law enforcement agencies access to decrypted content and traffic logs from digital platforms.

China

Cybersecurity Law (2017) & Data Security Law (2021)

China's Cybersecurity Law (2017) [61] establishes a legal framework to safeguard national cybersecurity, protect individual rights, and promote responsible internet use. It applies to all network-related activities within mainland China and emphasizes sovereignty, data protection, and critical infrastructure security. The law mandates cybersecurity measures for network operators, promotes national values online, and supports international cooperation. It also outlines state oversight, encourages public reporting of cyber threats, and includes protections for minors and informants.

[59] Investigatory Powers Act 2016. c. 25. https://www.legislation.gov.uk/ukpga/2016/25/contents
[60] The Information Technology Act, 2000. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
[61] Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017). https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

United States Policies

Patriot Act (2001, amended)

The USA PATRIOT Act (2001) [62] expanded government surveillance capabilities post-9/11 and enhanced U.S. law enforcement's ability to prevent and investigate terrorism by expanding tools already used in organized crime and drug cases. It allowed broader surveillance of terror-related crimes, enabled "roving wiretaps" for mobile suspects, allowed federal agencies to track internet activity related to national security or terrorism under Foreign Intelligence Surveillance Act (FISA) warrants and permitted delayed search notifications to avoid tipping off suspects. The Act also authorized access to business records in national security cases and improved inter-agency information sharing. It modernized laws to address new technologies, increased penalties for terrorism-related offenses, and streamlined processes for investigations across jurisdictions. These reforms aimed to better equip authorities to detect and disrupt terrorist threats.

CLOUD Act (2018)

The CLOUD Act (2018) [63] enables U.S. authorities and trusted foreign partners to access electronic data held by U.S.-based providers for serious criminal investigations, including terrorism and cybercrime. It addresses delays caused by traditional legal channels and allows bilateral agreements with countries that uphold strong privacy protections, creating a faster, rights-respecting framework for cross-border data access.

FBI & ICE Internet Investigative Units

ICE special agents investigate [64] transnational crime and violations of U.S. immigration and customs laws, targeting the illegal movement of people, goods, money, and technology. They make use of open-source intelligence (OSINT), AI, and web crawling for counterterrorism, child exploitation, and drug trafficking. Their work spans from individual offenders to global criminal networks, with a strong focus on crimes like human trafficking, child exploitation, and financial fraud.

[62] Department of Justice (2001). The USA Patriot Act: Preserving Life and Liberty. https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf
[63] Department of Justice (2023) CLOUD Act Resources. *Criminal Division.* https://www.justice.gov/criminal/cloud-act-resources
[64] U.S. Immigation and Customs Enforcement (n.d.) What We Investigate. *Homeland Security Investigations.* https://www.ice.gov/about-ice/hsi/investigate

Dark Web Policies

United States: Dark Web Interdiction Act

This act emphasizes the importance of specialized equipment, forensic capacity, and systematic information sharing to effectively combat dark web crimes. The Dark Web Interdiction Act (H.R. 3587, 118th Congress) [65] proposes the establishment of a specialized task force within the FBI. Key provisions include: Developing multijurisdictional and multiagency responses to dark web activities, providing guidance and training to law enforcement on techniques to recognize and investigate dark web-related crimes, enhancing collaboration with international partners to disrupt illicit marketplaces.

United Kingdom: Joint Operations Cell

The UK's Joint Operations Cell [66], a collaboration between GCHQ and the National Crime Agency (NCA), was established to tackle crimes on the dark web, with an initial focus on child sexual exploitation. Its intelligence methods include analysis of data gathered through mass surveillance, aiming to address various illicit activities such as international sex trafficking and the sale of drugs and weapons on darknet markets.

[65] S.1728 - Dark Web Interdiction Act of 2023. 118th Congress (2023-2024). https://www.congress.gov/bill/118th-congress/senate-bill/1728
[66] GCHQ (2015) GCHQ and NCA join forces to ensure no hiding place online for criminals. https://www.gchq.gov.uk/news/gchq-and-nca-join-forces-ensure-no-hiding-place-online-criminals

European Commission FCT Policies

Commission reports on the effective implementation of the Terrorist Content Online Regulation

The EU's Regulation on terrorist content online [67], in force since June 2022, requires online platforms to remove terrorist content within one hour of receiving an official order. A February 2024 Commission report confirms its effectiveness, with 23 Member States appointing authorities and around 350 removal orders issued to date.

EU Directive on the Protection of the Union's Financial Interests

The Directive aims to harmonize criminal law across EU Member States to better protect the EU's financial interests from fraud, corruption, VAT-related offenses, and misappropriation [68]. It defines relevant criminal offenses, sets minimum penalties (including imprisonment for serious cases), and ensures both natural and legal persons can be held liable. It strengthens cross-border cooperation, data protection, and enforcement, while respecting fundamental rights and the principle of proportionality. The Directive replaces the 1995 Convention and enhances safeguards for managing and recovering EU funds.

EU Action Against Drug Trafficking and Organized Crime

Organized drug trafficking poses a growing security threat to Europe, with record cocaine seizures and increasing violence, including the deaths of children. Synthetic drug production in Europe is also on the rise. Criminal networks fuel this trade through violence, corruption, and money laundering, infiltrating the legal economy and undermining trust in public institutions. In response, the EU has launched a roadmap [69] with 17 actions for 2024–2025, focusing on strengthening port security, dismantling criminal networks, boosting prevention, and enhancing international cooperation. Ongoing strategies from 2021–2025 guide these efforts, backed by new legislation, reinforced law enforcement tools, and a soon-to-be-operational EU Drugs Agency. Operations like EMPACT and MAOC-N have already led to major arrests and seizures.

[67] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2024%3A64%3AFIN

[68] Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L1371

[69] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the EU roadmap to fight drug trafficking and organised crime. COM/2023/641 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0641

Ethical, Legal, Societal view

Use of web crawling, digital twins and patrolling technologies to support law enforcement activities face different ELS considerations, since there are risks in automating such actions. Illegal exploration of content protected by intellectual property, unlawful processing of personal data, and exploring the evidence derived from these technologies [70] in criminal procedures and courts are some of the challenges involving these technologies. In particular, honeypots raise a number of legal and ethical considerations regarding their deployment. Specifically, honeypots are generally regarded as compatible with European data protection law, which permits the processing of personal data for the purpose of ensuring network and information security. However, several risks remain, including the inadvertent collection of personal data, the absence of informed consent, and actions that may be interpreted as provoking illegal behaviour, particularly in law enforcement contexts.

Nonetheless, not leveraging from innovative solutions would bring too many obstacles to LEAs combating cybercriminals. While actors involved in illegal activities try to explore the full potential of technologies to succeed in their actions without punishments, LEAs must observe the limits brought by the legal framework, exactly to ensure the respect for civil rights and liberties. Balance and proportionality are key to this discussion and must consider the different stakeholders who might be affected by it, such as journalists, civilian advocates, minors [71], among others. Thus, it is of utmost importance to ensure and debate an ethical and legal use of these technologies by LEAs, aiming at mitigating harmful effects to society, while responding to criminal activities leveraging from digitalisation and technologies.

[70] Henseler, H. (2023) Unraveling Digital Mysteries: How AI Copilots can Revolutionize Digital Forensic Investigations. *Digital Forensics Research Workshop (DFRWS).* https://dfrws.org/unraveling-digital-mysteries-how-ai-copilots-can-revolutionize-digital-forensic-investigations/
[71] Teunissen C., Cahill M., Napier S., Cubitt T., Boxall H. & Brown R. (2024) Sexual exploitation of children on dating platforms and experiences of revictimisation as an adult. *Trends & issues in crime and criminal justice no. 697*. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti77482

EU and MS legal framework

Different norms compose the relevant legal framework applicable for issues involving the law enforcement use of surveillance technologies and digital twins in the EU. Legislative initiatives on related topics continue to emerge and bring novel regulations to the relevant framework. As an example of this broad framework one can mention the LED Directive [72]. Another example is the Regulation on Markets in Crypto-assets [73], adopted after a dedicated EDPS' Opinion [74], focusing on forms to secure the use of new technologies in the financial sector. This regulation establishes certain measures to combat illegal actions, such as money laundry, including means to protect criminal investigations.

The Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence [75] is another important norm adopted by different EU countries. While the Protocol "aims to improve the traditional co-operation channels and includes provisions to enhance direct co-operation between law enforcement authorities and service providers in a cross-border context", it does not have any provision on direct access to data by LEAs, what was positively welcomed by the EDPS [76].

Legal gaps and uncertainties, nevertheless, still exist. New uses, technologies, cybercrimes, and international standards and guidelines are some aspects that influence the need for more specific regulation. Ethical [77] and legal hacking still operate in an unregulated scenario, which brings several challenges to these hackers. Similarly, there is still no consensus on how to tackle the issue of the deep web, with some mentioning de-anonymisation for access while others defend shutting it down. In the same sense, the implementation of policing techniques still remains a challenge. New and more specific regulations, combined with international co-operation, may be a solution. However, the respect for fundamental rights and freedoms must be a part of all these discussions [78].

[72] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

[73] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

[74] EDPS (2021) Opinion 9/2021 on the Proposal for a Regulation on Markets and Crypto-assets, and amending Directive (EU) 2019/1937. *European Data Protection Supervisor.* https://www.edps.europa.eu/system/files/2021-06/21-06-24_edps_opinion_mica_en.pdf

[75] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Council of Europe. https://rm.coe.int/1680a49dab

[76] EDPS (2022) Opinion 1/2022 on the two Proposals for Council Decisions authorising Member States to sign and ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. European Data Protection Supervisor. https://www.edps.europa.eu/system/files/2022-04/22_01_20_opinion_en.pdf

[77] Jaloyan, G. A. (2023). Hacker éthique: une espèce en voie d'extinction? 1. *Les Notes du CREOGN*, 89. https://cel.hal.science/CREOGN/hal-04295397v1

[78] Warner, C. (2023). Law Enforcement and Digital Policing of the Dark Web: An Assessment of the Technical, Ethical and Legal Issues. *Applications for Artificial Intelligence and Digital Forensics in National Security*, 105-115.

Highlights

Recent developments underscore the growing integration of autonomous agents, patrolling bots, and digital twin technology in law enforcement:

- In Shanghai, authorities have implemented a real-time digital twin of the city, which enables police officers to virtually and accurately explore streets and buildings. The system overlays live surveillance with other data to facilitate crime prevention and emergency response operations [79].

- The upcoming European Police Congress 2025 [80] , scheduled for May 20-21 in Berlin, will focus on critical issues such as cybercrime, the use of AI and drones in law enforcement, combating international threats, and strategies for proactive policing and digital forensics.

- On May 15, the ENTSO-E and EU DSO Entity hosted a webinar titled "TSO-DSO Challenges & Opportunities for Digital Twins" [81], discussing the implementation challenges and opportunities of digital twins in energy systems. The insights of the webinar are applicable to law enforcement agencies interested in adopting similar systems for critical infrastructure monitoring and emergency response.

[79] Singh, R. (2025) Real-life GTA? Shanghai's 3D twin helps police prep for every mission. *Business Standard.* https://www.business-standard.com/world-news/china-shanghai-gta-city-3d-twin-mapping-virtual-patrols-data-access-125040700812_1.html
[80] The European Police Congress. https://www.european-police.eu/
[81] ENTSO-E (2025) TSO-DSO Challenges & Opportunities for Digital Twins webinar with DSO Entity. *European Network of Transmission System Operators for Electricity.* https://www.entsoe.eu/events/2025/05/15/tso-dso-challenges-opportunities-for-digital-twins-webinar-with-dso-entity/

A.1 Projects, Tools, and Initiatives Overview

Project	Purpose and Focus	Funding / Origin	Category
DANTE	Multilingual web/dark web crawling for detecting terrorist content	Horizon 2020	Web Crawling
TENSOR	Targeted crawling and NLP for identifying online radicalization	Horizon 2020	Web Crawling
TITANIUM	Illicit activity tracking through blockchain and dark web data	Horizon 2020	Web Crawling / Data Fusion
Cereberus	Dark web indexing and search platform	COmmercial	Web Crawling
Web IQ Voyager	Aggregates surface/dark web content into LEA dashboards	Commercia	Web Crawling / Investigation Support
ASGARD / IFPTA	Forum post analysis from crawled content for suspect profiling	Horizon 2020	Web Crawling / Behavioural Analysis
ARTE-Fact (PREVISION)	Crawling and detecting stolen cultural assets online	Horizon 2020	Web Crawling / Asset Tracking
RED-Alert	Real-time social media monitoring for radicalization detection	Horizon 2020	Web Patrolling Bot
INSIKT	AI-driven agents detecting radicalization and recruitment patterns	Horizon 2020	Web Patrolling Bot / Social Media Monitoring
CyberSANE	Threat detection via autonomous agents in IT and public networks	Horizon 2020	Web Patrolling Bot / Cybersecurity
Project Arachnid	Automated CSAM detection across the surface and dark web	Canada (Intl. cooperation)	Web Patrolling Bot / Harmful Content Detection
Tangles (Cobwebs)	Real-time monitoring of illicit activity across online layers	Commercial	Web Patrolling Bot / Intelligence Platform
INFINTY	Immersive investigation support via AI and VR-enhanced digital twins	Horizon 2020	Digital Twin / investigation Visualization
LAW-GAME	Real-time monitoring of illicit activity across online layers	Horizon 2020	Digital Twin / LEA TRaining
TESTUDO	City-scale twin integrating IoT, drones, and simulation for disasters	Horizon Europe	Digital Twin / Autonomous Patrol / Critical Infrastructure
PANTHEON	Robotic infrastructure protection with AI-driven situational digital twins	Horizon Europe	Digital Twin / Urban Resilience
Crowd Safety Manager	3D crowd monitoring and prediction system for event policing	Dutch Smart City	Digital Twin / Crowd Management
Frontex Copernicus Prize Contest	Proposed digital twins for border surveillance using satellite and drone data	Frontext / Copernicus	Digital Twin / Border Security
SHIELD4CROWD	Digital twin integration roadmap for future LEA crowd threat response	EU PCP / Horizon Europe	Digital Twin / Public Space Security Planning

ENACT.

European Network Against Crime and Terrorism

@enact-network

enact-eu.net

Scan the QR code to visit ENACT online and read this report in digital format.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.