STARLIGHT

STARLIGHT - Sustainable Autonomy and Resilience for LEAs using AI against High Priority Threats

Jorge García[1], Roxana Pelin[2], Peter Van De Crommert[3], Nizar Touleimat[4]

1. Vicomtech Foundation, Basque Research and Technology Alliance (BRTA)
2. Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC)
3. Dutch Institute for Safe & Secure Spaces (DISSS), representing Netherlands Police
4. LIST Institute, CEA Paris-Saclay Nano-INNOV

Law enforcement agencies (LEAs) now have access to vast amounts of data, which was previously unprecedented. This has been viewed as a great opportunity for LEAs to solve and predict crime, but despite the big-data revolution, they have been unable to make the most of this data. Artificial intelligence (AI) is seen as a solution to many of society’s challenges, such as increasing productivity and efficiency, identifying patterns, and making decisions quickly and accurately. In order to maximise the benefits of AI, LEAs need to adopt a human-centric and inclusive approach alongside a coherent data strategy to ensure the safety and security of society.

Data is vital for AI solutions. Technologies have made it easier to create, store, and distribute data. Social media, smartphones, and IoT devices track our daily interactions and store them on cloud services worldwide. LEAs also have interlinked datasets through investigations, historical cases, and databases. These datasets contain structured and unstructured text, multimedia, and relationship information in multiple languages, which poses a challenge but also an opportunity for AI adoption. LEAs, security practitioners, and others face these challenges daily. New operational capabilities powered by AI are needed to fight against (cyber)crime and terrorism. Solutions must be developed to address threats such as the spread of terrorist and sexually explicit content, trafficking, cybercrime, and attacks on public spaces.

Law enforcement agencies must be supported in their efforts to gather, analyse, and act upon evidence quickly and effectively. Proactive operations that enhance situational awareness, detect patterns, and enable investigative hypotheses are also crucial. As LEAs incorporate AI into their investigations, developed tools must enhance operational capacity, promote interoperability, and foster cooperation. Tools should be easy to integrate, solve problems instead of creating them, and facilitate information sharing and best practices. A sustainable community should work to build better AI solutions for LEAs across Europe through collaboration.

AI used in law enforcement poses legal and ethical challenges. It must be transparent and able to explain decision-making processes. Though AI is used in many LEA environments, its accuracy and specificity are often insufficient. The best-in-class AI solutions are dominated by organisations, who have unrestricted access to vast quantities of high-quality, structured, and labelled data. Europe must address the lack of legislation and coordination to advance research and operational AI, including regulatory, legislative, ethical, and security concerns. Access to data would drive investments and funding opportunities for EU research. Criminals can use AI technology to amplify existing threats and introduce new ones, requiring LEAs to be equipped to respond to these changes. Advanced technology requires enhanced cybersecurity operations, including the use of AI to detect cyber threats. However, all AI systems must be protected to maintain trust, as attackers can exploit their complexity through adversarial AI. A nucleus of AI stakeholders, researchers, and industry professionals should be brought together to promote a strategic and synchronised vision of AI for LEAs at the EU level. Collaboration with civil society and policymakers is also necessary to understand the societal implications of AI adoption and build trust. A dedicated hub is needed to unify AI knowledge, resources, and data for LEAs across Europe and promote long-term AI innovation, adoption, and uptake.

STARLIGHT aims to play a leading role in the effective use of AI for security in Europe. To better prevent, detect, and control crime, LEAs should use AI technologies to protect citizens and public spaces and increase resilience. STARLIGHT supports innovation and awareness of AI’s potential benefits and risks for security and aims to create a European approach to AI for LEAs. By providing LEAs with automated, operational, and cyber-resilient capabilities, STARLIGHT will help tackle traditional and emergent criminal activities, terrorism, cybercrime, and cyberattacks in Europe. To achieve this, STARLIGHT aims to establish a strong EU AI-based security industry with interoperable AI solutions that uphold ethical and societal values to tackle high-priority threats for all LEAs across Europe. Cooperation between researchers and security practitioners will ensure fast and effective uptake and adoption while aligning with legal and ethical provisions, legislative frameworks, and fundamental rights. STARLIGHT will ensure that European LEAs are at the forefront of AI innovation, autonomy, and resilience, prioritising the safety and security of Europe for all through the following strategic goals:

(i) To improve LEAs' knowledge of how AI can enhance their operational and cybersecurity capabilities at both EU and national levels.

(ii) To enhance LEAs' AI capabilities for predicting, preventing, detecting, and investigating criminality, terrorism, and border security while protecting digital infrastructures from cyber threats.

(iii) To develop a cybersecurity strategy and measures to protect AI LEA solutions proactively against cyberthreats (including trustworthy AI).

(iv) To enhance LEA's ability to investigate, combat, and prevent the criminal use of AI, including terrorism.

To transfer knowledge between LEAs, researchers, industry, SMEs, and policymakers, a strong ecosystem is required. It should facilitate an open exchange of the challenges LEAs face with their workflows, duties, and system requirements, as well as ideas on how AI can address these challenges. STARLIGHT's central goal is to build a strong, long-lasting ecosystem that facilitates trustworthy exchange and productive AI technology transfer. The ecosystem will be built around an AI framework that enables the participation of all stakeholders. Informed by end users' requirements and AI Community of Expertise stakeholders, the STARLIGHT framework will include cutting-edge AI/ML and data-driven technologies for (i) creating excellent multilingual and multimodal training and testing data in compliance with legal and ethical regulations at both national and European levels; (ii) using advanced and resilient AI/ML methods and tools to understand both physical (sensors and data-gathering devices for robotics and IoT systems) and cyber worlds (online sources from Surface/Deep Web, Darknets) and generate knowledge and intelligence in an explainable, transparent, and accountable way, by handling large volumes of multimodal data through fusion, correlation, and analysis. (iii) enabling LEAs to analyse, predict, detect, and mitigate cyberthreats and attacks, including adversarial AI.

STARLIGHT will deliver the following main results:

(i) A sustainable European AI Community, bringing together relevant stakeholders from the security and AI domains to foster adoption of AI technologies in the daily operational activities of LEAs.

(ii) A strategy for creating high-quality European training and testing datasets. This will include novel technological solutions for creating and annotating datasets, privacy-preserving measures for training and testing AI tools, and legal and ethical considerations for easier data creation and sharing.

(iii) A STARLIGHT Framework for trustworthy, accountable, responsible, and transparent LEA AI solutions. This will cover all technological needs of LEAs in AI, including machine learning, machine reasoning, natural language processing, robotics, and IoT. It will allow analysis of a wide range of (hybrid) threats and incidents.

(iv) AI-based cybersecurity and protection of LEA AI solutions, to improve cybersecurity operations and protect AI solutions against adversarial attacks.

(v) Detailed pilot scenarios tailored to real operational needs. The project is extendable to address additional areas and challenges posed by the LEAs and Europol.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021797. This article reflects only the authors' views and the Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains.