Warsaw, 17/03/2021
Reg. No 1810
CBD/RIU/BSO/1810/2020

Artificial Intelligence-based capabilities for the European Border and Coast Guard

Executive Summary

This study explores the opportunities for and pathways to adoption of AI-based capabilities in European border security

Artificial Intelligence (AI) is an area of increasing interest that may help address Europe's evolving border security challenges. AI offers several opportunities to the European Border and Coast Guard (EBCG), including increased efficiency and improving the ability of border security agencies to adapt to a fast-paced geopolitical and security environment.[1] However, various technological and non-technological barriers might influence how AI materialises in the performance of border security functions.[2]

In this context, RAND Europe was commissioned by Frontex to undertake a study examining the evolving landscape of AI-based capabilities and characterise the requirements for adopting AI-based systems in border security. This study explored four overarching research questions (RQs):

- **RQ1**: What is the current landscape in the application of AI to border security?
- **RQ2**: Which new and emerging AI-based systems could be applied to border security?
- **RQ3**: In which areas of border security might new and emerging AI-based systems be applied?
- **RQ4**: What steps are required to integrate AI-based systems into border security?

A mixed-methods research approach was used to address these RQs through two work packages (WPs):

- **WP1 – Review of AI-based technologies and their application in border security** involved identifying AI-based technologies of current or potential future use in border security through scoping interviews with Frontex experts, desk research, horizon scanning of emerging science and technology (S&T) trends, and initial analysis of nine selected technology areas – which were selected in consultation with Frontex – through case study analysis and a STREAM expert workshop.[3]

- **WP2 – Roadmapping of AI-based technologies for application in border security** focused on the development of technology adoption roadmaps to highlight possible adoption pathways for the nine technology areas identified in WP1. The roadmaps were developed using data gathered through desk research and interviews with technology and border security experts.

[1] *Accenture (2017).*

[2] *IBM Research (2020), Craglia et al. (2018), Tiempo Development (2019).*

[3] *Systematic Technology Reconnaissance, Evaluation & Adoption Method (STREAM). More details about STREAM can be found in Annex A of the main report.*

AI encompasses systems that can perform tasks with a degree of autonomy, and could be used for various tasks in a border security context

While there is no universally accepted definition of AI, the term may be broadly understood as the application of computer systems that analyse their environment and take action with some degree of autonomy.[4] Box ES-1 provides a definition of AI and discusses three chief types of tasks for which AI can be used.

Box ES-1 Definition of AI and description of key tasks performed by AI-based technologies

AI can be defined as 'Systems (including hardware and software) that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information derived from this data and deciding the best action(s) to take to achieve the given goal'.[5] AI technologies can be categorised in relation to various criteria, including levels of sophistication and the types of tasks an AI-based system can perform. In relation to the latter, AI-based systems are commonly used to support:

- **Automation** of digital or physical tasks (e.g. in the context of administration and information management through the use of Natural Language Processing (NLP) to automate document processing).
- **Cognitive insight** based on the ability of AI-based systems to process and analyse large quantities of data (often referred to as advanced and predictive analytics).
- **Cognitive engagement** where AI-powered intelligent agents can engage or interact with their environment. Though cognitive engagement technologies are, to date, relatively immature and often require human intervention, current examples include intelligent agents used to answer questions and address inquiries or provide product and service recommendations.

Source: RAND Europe analysis.

As discussed in further detail in **Chapter 2** of the main study report, current and potential future uses of AI cut across several border security functions, including[6]:

- **Situation awareness and assessment**: The use of technological systems to collect, fuse and analyse disparate forms of real-time and historical data to facilitate decision-making and performance in complex environments. It includes capabilities used for wide and small area surveillance of people, vehicles and objects, such as shipping containers, and includes systems such as AI-enabled surveillance installations (surveillance towers), autonomous systems (e.g. drones and networked heterogeneous robotic systems), and capabilities for cross-analysis and information correlation of surveillance databases.
- **Information management:** The management of data and information – including through AI-enabled data mining and fusion techniques, NLP, image/pattern recognition, information exchange, predictive analytics and capabilities – to automate information management (e.g. automated machine learning). Information management capabilities can support a wide range of analysis, including in relation to automating administrative processes (e.g. recruitment).
- **Communication:** Communication and information sharing capabilities, including authentication technologies, and AI- and NLP-enabled end-to-end communications capabilities (e.g. chatbots).

[4] *European Commission (2019).*

[5] *European Commission (2019).*

[6] *The study uses a taxonomy of border security functions developed in ESRAB (2006).*

- **Detection, identification and authentication**: Capabilities that are used to detect and identify potential threats and authenticate people and objects. This includes AI-enabled automated border control, biometric scanning, facial recognition and document authentication, as well as threat-detection capabilities (e.g. object recognition), and cognitive robotics (e.g. robotic border patrol agents).
- **Training and exercise**: Capabilities for improving staff readiness and expertise through training and exercise (e.g. AI-enabled synthetic environments and simulation).

AI systems currently used or in development for border security purposes, therefore, include both **'front-end' capabilities**, which end users would directly utilise (e.g. security gates and surveillance systems), and **'back-end' capabilities**, which would have an enabling impact on border security functions (e.g. automated machine learning).

Opportunities, requirements and barriers for adoption were explored for nine AI technology areas

Despite the significant and increasing variety in the border security tasks and functions for which AI might be utilised by end users, not all capabilities may be of equal interest and utility for the EBCG. Summarised in Table ES-1, nine technology areas – illustrating a mix of enabling and front-end technology areas with different levels of maturity – were selected in consultation with Frontex to provide a more in-depth understanding of the opportunities and challenges associated with AI-based capabilities for the ECBG.

As further discussed in **Chapter 3** of the main study report, initial assessment of nine technology areas at the STREAM expert workshop indicated that all AI technology areas were generally considered to bring at least a moderate improvement of the ability of end users to perform border security functions. Additionally, none of the technology areas were perceived to face overwhelming barriers to adoption that could not be overcome, though workshop discussions highlighted that end users should consider their specific needs and requirements in relation to the functions and contexts for which AI-based systems will be used. Table ES-1 illustrates the three highest scored technology areas in relation to the expected impact, feasibility of implementation, and combination thereof.[7]

Table ES-1 Top 3 technology areas according to impact, implementation and combined assessment

Top 3 combined	Top 3 impact	Top 3 implementation
1. Maritime domain awareness	1. Heterogeneous robotic systems	1. Predictive asset maintenance
2. Object recognition	2. Maritime domain awareness	2. Maritime domain awareness
3. Automated border control	3. Object recognition	3. Object recognition

Source: RAND Europe analysis.

[7] *Chapter 4 and Annex D of the main report present the nine technology area roadmaps in more detail, and discuss opportunities and pathways for their adoption in a border security context.*

Table ES-2 Description of examined AI technology areas

#	Technology area	Description
	Automated border control	Integrated systems of electronic border gate (e-gate) hardware, document scanning and verification, and biometric verification facilitating the processing of travellers on border crossings with enhanced security.[8]
	Maritime domain awareness	Capabilities aimed at establishing 'the effective understanding of anything associated with the global maritime domain that could impact [a country's] security, safety, economy or environment', including integrated analysis of various data streams such as Automatic Identification Systems (AIS), coastal and vessel-mounted sensors and other contextual information.[9]
	Machine learning (ML) optimisation	Use of AI to automate the selection, testing and optimising of ML models. This includes the automation of all steps of ML algorithm development from problem identification, data collection and clean-up, model development, training and evaluation.[10]
	Surveillance towers	Unmanned surveillance capabilities in the form of autonomous surveillance towers fielded in border regions, integrating software and hardware surveillance capabilities to, for example, detect illegal border crossings.[11]
	Heterogeneous robotic systems	Networked systems integrating various maritime, land and aerial unmanned assets applied to functions such as border surveillance, environmental monitoring and counterterrorism.[12]
	sUAS	Small autonomous unmanned aerial systems (UAS) with integrated AI-enabled object recognition, classification and tracking capabilities that can be used to perform functions such as border surveillance, environmental monitoring and disaster relief.[13]
	Predictive asset maintenance	Predictive analytics to enable optimal operations and maintenance of technical systems, enabling end users to identify vulnerabilities, sub-optimal performance or potential technical failures in complex technical systems, such as multi-vehicle UAS networks.[14]
	Object recognition	Algorithmic recognition and classification of objects through annotation, training and analysis of complex data – e.g. 3D imagery – utilised to perform functions including detection of suspicious packages, vehicles and cargo.
	Geospatial data analytics	Use of AI to analyse geospatial data, including labelling and classification of satellite imagery. Geospatial data analytics could support operational awareness and threat detection.[15]

Source: RAND Europe.

[8] *European Commission (2020d).*

Future adoption of AI-based systems could be enabled or constrained by various technological and non-technological enablers and barriers

As discussed in further detail in **Chapter 5** of the main study report, several technological and non-technological factors could act as potential barriers or enablers to the adoption of AI-based capabilities in a border security context. While no single barrier is likely to constitute an overwhelming constraint that could not be overcome, various **barriers** – summarised in Box ES-2 – could pose significant challenges to end users and efforts to integrate AI-based systems in support of border security functions.

Box ES-2 Cross-cutting barriers for future adoption of AI-based capabilities

- **Technological barriers.** Technological barriers to adoption may include algorithmic biases, cybersecurity vulnerabilities and other challenges frequently underpinned by insufficient quantity or quality of data used for the development and training of AI models.
- **Cost and commercial barriers.** Despite the decreasing costs of AI and adjacent technologies, perceptions of high direct and indirect financial costs, as well as wider commercial barriers, may constrain end users from investing in AI technologies.
- **Understanding and awareness of AI:** Insufficient understanding of AI and lack of awareness concerning its potential in border security challenge end users' ability to identify opportunities associated with AI. This is frequently linked to wider organisational barriers including organisational structural and cultural inefficiencies which may not allow for innovation and adaptation in response to technological advances.
- **Skills and expertise:** Although many AI-based systems do not require technical expertise from end users who may directly interact with a capability (e.g. operators of surveillance capabilities), skills shortages and lack of expertise may also limit the ability of end users to identify where and how AI may be best applied and address any requirements for adoption.
- **Access to relevant technologies:** End users may face constraints in relation to access to relevant technologies and lack of European strategic autonomy in AI and related technologies (e.g. robotics and unmanned systems). The dominance of non-EU technology suppliers poses challenges for end users as well as developers in relation to information security and data protection.
- **Ethics, human rights and regulatory barriers:** The proliferation of AI technologies and performance of AI algorithms may have ethical implications and carry risks for the safeguarding of human rights, such as individual privacy. Though an evolving legal and regulatory landscape may help address such challenges, regulatory barriers for adoption also include regulatory uncertainty for technology developers and prevailing gaps in regulatory safeguards, including for data protection.

Further to these barriers, the study identifies several overarching technological and non-technological factors that are likely to serve as key **enablers** for the adoption of AI-based technologies in border security, as summarised in **Box ES-3**.

[9] *DHS (2005), Zhao et al. (2010).*

[10] *DataRobot (2020).*

[11] *Feldstein (2019), Anduril.com (2020).*

[12] *Miskovic et al. (2014).*

[13] *Fussell (2019), Planck Aerosystems (2019).*

[14] *SparkCognition (2018), WP1-INT12.*

[15] *Lockheed Martin (2019).*

Box ES-3 Cross-cutting enablers for future adoption of AI-based capabilities

- **Technological enablers and iterative development**: Future adoption of AI-based capabilities could be enabled by advances in AI methods (e.g. through advanced sensory computing and neural networks) and in 'adjacent' technologies (e.g. cognitive robotics and blockchain integration). Such improvements are likely to rely on iterative development and innovative approaches to acquisition and testing of AI-based capabilities.
- **Improvements in usability**: While AI-based systems might be becoming more technologically complex, the simplification of interfaces (e.g. in biometric scanning tools or surveillance technologies) is improving usability of AI-based capabilities and could incentivise adoption by end users.
- **Democratisation of AI**: Commercialisation and democratisation of AI will likely further contribute to decreasing costs of AI-based capabilities, improving the economic viability of AI adoption for end users.
- **EU initiatives on AI**: Ongoing EU-wide initiatives on AI are likely to produce a number of enabling factors, e.g. incentivising further research into the uses of AI, including in the public sector, advancing AI governance and the development of ethical and human rights protection standards in relation to AI, and the strengthening of European strategic autonomy.
- **Public awareness and acceptance**: Increasing use of AI in providing services that benefit individuals and society at large could strengthen the value proposition of AI vis-à-vis the public, and lead to increased public awareness and acceptance of AI-based technologies.

There are various opportunities and options for defining Frontex' role in future AI uptake in border security

The outputs of this study and the nine technology adoption roadmaps seek to provide a high-level overview of the main opportunities, challenges and requirements for the adoption of AI-based capabilities in European border security. Frontex could feasibly support this adoption in several ways, but this might require further consideration of what role Frontex as an agency could play in shaping the future landscape of AI-based capabilities in European border security. As discussed in more detail in **Chapter 6** of the main study report, Frontex could consider:

- **Working to address three overarching baseline gaps** constituting barriers for the adoption of AI-based capabilities in border security, namely: knowledge gaps between stakeholder groups (including technology developers, end users and policy- and decision-makers); organisational, structural and cultural barriers, as well as gaps in organisational skills and expertise; and gaps in the evidence base regarding the impacts of AI in border security.
- **Defining what role Frontex as an agency could play** in shaping the future landscape of AI-based capabilities in European border security. The study outlines five possible roles for Frontex in this context, including facilitating information and knowledge exchange, acting as an 'honest broker' between relevant stakeholder groups, and facilitating access to funding for strengthening the knowledge- and evidence-base on AI and its impacts in border security.
- **Identifying options for addressing key organisational structural and cultural barriers** – including procedural and behavioural inefficiencies – and further assessing organisational gaps in skills and expertise, as well as human and financial resource constraints.