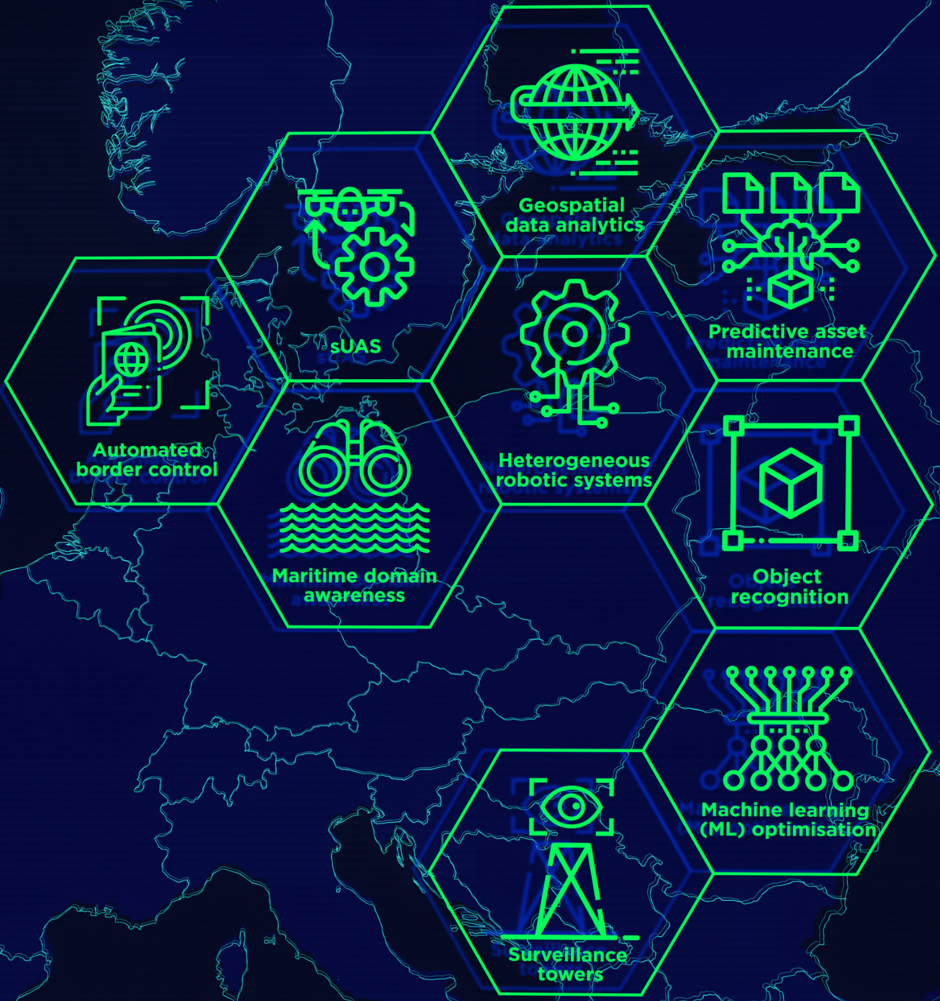
FRONTEX

Warsaw, 17/03/2021


Geospatial data analytics
sUAS
Predictive asset maintenance
Automated border control
Heterogeneous robotic systems
Maritime domain awareness
Object recognition
Machine learning (ML) optimisation
Surveillance towers

ARTIFICIAL INTELLIGENCE -BASED CAPABILITIES FOR THE EUROPEAN BORDER AND COAST GUARD

FINAL REPORT

EUROPEAN BORDER AND COAST GUARD AGENCY

www.frontex.europa.eu | Pl. Europejski 6, 00-844 Warsaw, Poland | Tel. +48 22 205 95 00 | Fax +48 22 205 95 01

Legal notice

This research study has been produced under a contract with the European Border and Coast Guard Agency (Frontex). The information and views set out in this research study are those of the authors and do not necessarily reflect the official opinion of Frontex. Frontex does not guarantee the accuracy of the data included in this study.

Neither Frontex nor any person acting on behalf of Frontex (including the authors) may be held responsible for the use which may be made of the information contained therein. In particular, the information in this research study is provided "as is", authors give no guarantee or warranty that the information is fit for any particular purpose other than the performance of the contract with Frontex. The referenced contractor shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

FRONTEX

Frontex – European Border and Coast Guard Agency
Plac Europejski 6
00-844 Warsaw, Poland

T +48 22 205 95 00
F +48 22 205 95 01
frontex@frontex.europa.eu
www.frontex.europa.eu

Warsaw, March 2021
Research and Innovation Unit

Preface

This document is the final report of a study commissioned by the European Border and Coast Guard Agency (Frontex) in November 2019 to examine Artificial Intelligence (AI)-based capabilities for border and coast guard applications. This report presents the main findings of the study, including:

- A characterisation of the evolving landscape of AI-based capabilities in border security and mapping of the technology, capability areas and border security functions to which AI may be applied;
- Mapping of the current and desired capability levels for nine selected technology areas, as well as pathways to their adoption;
- Discussion of cross-cutting enablers and barriers for adoption of AI-based capabilities in border security; and
- Reflections on the implications for Frontex.

We envisage that the findings of this report might be of interest to border security authorities, industry, innovators and academia, but also more broadly to those interested in the application of AI-based capabilities to novel areas.

This study was commissioned to RAND Europe which is an independent not-for-profit policy research organisation that aims to improve policy and decision-making, for the public benefit, through evidence-based research and analysis. RAND Europe's clients include national ministries of defence, UK government's departments, the European Commission, NGOs and other organisations with a need for an objective interdisciplinary analysis.

For more information about this study, please contact:

Research and Innovation: Border Security Research Observatory
Capacity Building Division
Frontex – European Border and Coast Guard Agency
Plac Europejski 6, 00-844 Warsaw, Poland
Tel. +48 22 205 9500
frontex@frontex.europa.eu
research@frontex.europa.eu

Table of contents

Figures

Tables

Boxes

Abbreviations

ABC	Automated Border Control
AI	Artificial Intelligence
AI HLEG	Independent High-Level Expert Group on Artificial Intelligence
AIS	Automatic Identification Systems
API	Advanced Passenger Information
BCI	Brain-Computer Interface
BCP	Border Crossing Point
C2	Command and Control
CBP	Customs & Border Protection
CNN	Convolutional Neural Network
C-UAS	Counter-Unmanned Aerial System
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DoD	Department of Defense
EBCG	European Border and Coast Guard
EMSA	European Maritime Safety Agency
EU	European Union
EUNAVFOR MED	European Union Naval Force Mediterranean
GATR	Global Automated Target Recognition
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GTAS	Global Travel Assessment System
HMT	Human-Machine Teaming
IARPA	Intelligence Advanced Research Projects Agency

ISR	Intelligence, Surveillance and Reconnaissance
MDA	Maritime Domain Awareness
ML	Machine Learning
NATO	North Atlantic Treaty Organization
NLP	Natural Language Processing
PNR	Passenger Name Record
R&D	Research & Development
RQ	Research Question
S-AIS	Satellite Automatic Identification System
S&T	Science & Technology
STREAM	Systematic Technology Reconnaissance, Evaluation and Adoption Method
sUAS	Small Autonomous Unmanned Aerial System
TNA	Training Needs Analysis
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
WP	Work Package

Acknowledgements

The report was prepared by RAND Europe by the following team members: Erik Silfversten, Luke Huxtable, Linda Slapakova, Pauline Paille, and Kevin Martin. We are thankful for their tireless efforts to produce the highest quality research study with effective and successful collaborative works.

We would also like to express our gratitude to all the experts in Frontex who participated in the consultations, both as part of the interviews and workshops, and who graciously had devoted their time and knowledge to this study.

Furthermore, we would like to send our thanks to the EU and International experts from the following entities: Directorate-General Joint Research Centre (JRC), European Defence Agency (EDA), European Satellite Centre (EU SatCen), European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), NATO Centre for Maritime Research and Experimentation (CMRE), and US Customs and Border Patrol (CBP).

We would like to also acknowledge the support from the academia as well as the research and technology organisations such as Kozminski University, Information Technology Institute, Fraunhofer Gesselschaft, Rey Juan Carlos University, Tel Aviv University, and Centre for Research and Technology Hellas (CERTH).

Additionally, this study would not have been possible without the shared experience and knowledge of multiple industry entities. A list of all the contributors can be found in Annex A.

Nevertheless, any errors or omissions in the analysis presented within this report remain the sole responsibility of the authors.

About Frontex

Frontex, the European Border and Coast Guard Agency, promotes, coordinates and develops European border management in line with the EU fundamental rights charter and the concept of Integrated Border Management. The Agency also plays a key role in analysing and defining the capability needs in border control and in supporting the Member States in the development of these capacities. Furthermore, it provides qualified expertise to support the EU policy development process in the area of border control.

The Border Security Research Observatory (BSO), within Frontex Research and Innovation Unit, is responsible for leading and conducting transformational, need-driven research with academia, EU agencies, international organisations and industry partners to stimulate and support innovation. The ultimate goal is to consistently enhance the capabilities of the European Border and Coast Guard in line with the Capabilities Development Plan (CDP), which includes those of the Member States and of the Agency itself.

1. Introduction

This introductory chapter provides a short overview of the background and context of the study, the research objectives and the approach undertaken to deliver the research. The chapter concludes with an overview of the structure and content of the remainder of the report.

1.1. EU external border management might face various challenges in the coming years, which the use of AI could help alleviate

The European Union (EU) has long been an attractive place to live and work for European and non-European citizens, leading to considerable migratory flows both within and to the EU. External border control and management of migration into the EU has become increasingly challenging in recent years, partly as a result of a significant increase in the number of migrants and refugees reaching the EU's external borders by air, land and sea. 2015 saw an unprecedented 1.83 million irregular border crossings recorded on the EU's external borders, a six-fold increase from 2014, and a seventeen-fold increase from 2013.[1] This was predominantly driven by political and social unrest in the Middle East, Africa and South Asia. Irregular migration into the EU has remained high from 2016–2018, though 2019 saw the number of irregular border crossings reach the lowest level since 2013.[2]

Despite the recent downward trend in irregular migratory flows, future EU external border management and control is likely to be confronted by various challenges, including increasing levels of displacement due to the effects of climate change or trends related to human trafficking and cross-border organised crime. To strengthen its capacity to address and mitigate such challenges, the EU has taken several steps to strengthen European border security cooperation. These include initiatives in the area of external border management and exploring how emerging technologies such as AI might assist in those efforts, such as:

- Regulation (EU) 2016/1624 on the European Border and Coast Guard (EBCG), which put forward general principles for European integrated border management and Regulation (EU) 2019/1896, strengthening the mandate of the European Border and Coast Guard Agency (Frontex).[3]

[1] Frontex (2016), Orav (2016).

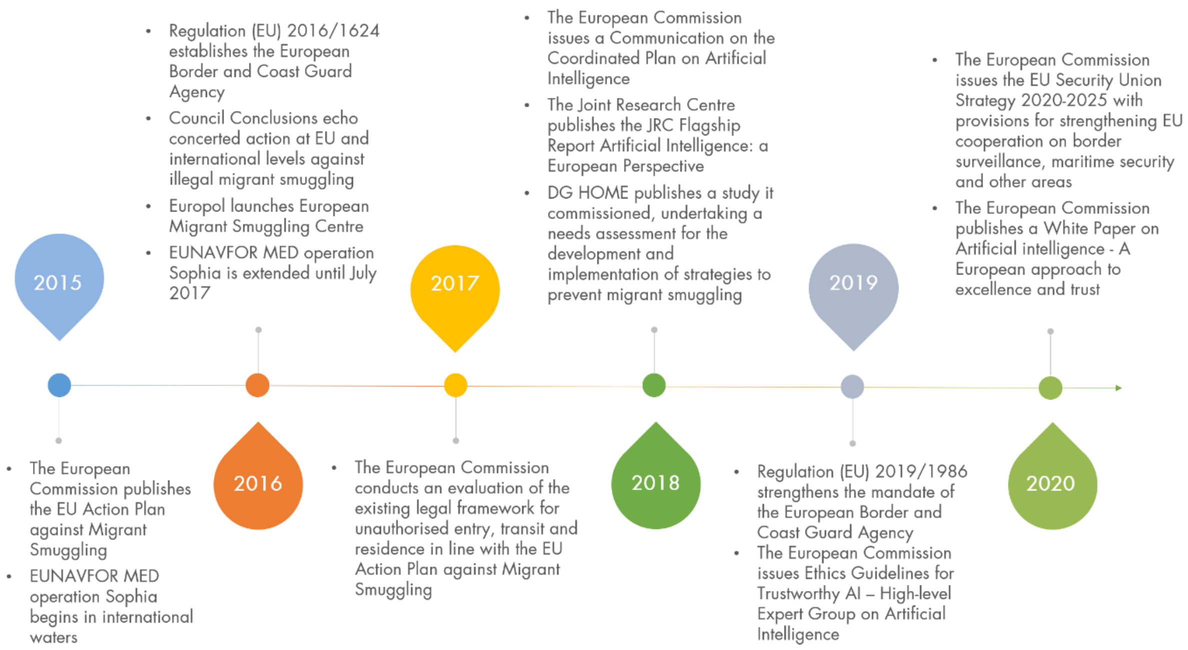
[2] Frontex (2020a).

[3] The European Parliament and the Council of the European Union (2016).

- The European Commission's 2018 European Strategy and Coordinated Plan on AI, which characterised a European perspective on the technological, ethical, legal and socio-economic aspects of AI and principles for its uses in the public as well as private sectors.[4]
- The EU Security Union Strategy 2020, which outlines the EU's priorities for improving internal security, including strengthening the provision of data services for border surveillance and maritime security.[5]
- The European Commission's February 2020 White Paper on Artificial Intelligence, which builds on the 2018 Strategy and Coordinated Plan on AI and outlines principles for a European approach on AI, including addressing its ethical and human implications.[6]

Figure 1.1 provides an overview of these and other recent initiatives from the European Commission and other bodies.

Figure 1.1 Overview of recent EU initiatives to strengthen border security


2015
• The European Commission publishes the EU Action Plan against Migrant Smuggling
• EUNAVFOR MED operation Sophia begins in international waters
2016
• Regulation (EU) 2016/1624 establishes the European Border and Coast Guard Agency
• Council Conclusions echo concerted action at EU and international levels against illegal migrant smuggling
• Europol launches European Migrant Smuggling Centre
• EUNAVFOR MED operation Sophia is extended until July 2017
2017
• The European Commission conducts an evaluation of the existing legal framework for unauthorised entry, transit and residence in line with the EU Action Plan against Migrant Smuggling
2018
• The European Commission issues a Communication on the Coordinated Plan on Artificial Intelligence
• The Joint Research Centre publishes the JRC Flagship Report Artificial Intelligence: a European Perspective
• DG HOME publishes a study it commissioned, undertaking a needs assessment for the development and implementation of strategies to prevent migrant smuggling
2019
• Regulation (EU) 2019/1986 strengthens the mandate of the European Border and Coast Guard Agency
• The European Commission issues Ethics Guidelines for Trustworthy AI – High-level Expert Group on Artificial Intelligence
2020
• The European Commission issues the EU Security Union Strategy 2020-2025 with provisions for strengthening EU cooperation on border surveillance, maritime security and other areas
• The European Commission publishes a White Paper on Artificial intelligence - A European approach to excellence and trust

Source: RAND Europe.

In the context of these initiatives, Frontex became a fully fledged border and coast-guard agency in 2016, with a reinforced mandate in 2019 to support the EU Member States in ensuring safe and well-functioning external borders in Europe through three strategic objectives[7]:

[4] European Commission (2018a), European Commission (2018b).

[5] European Commission (2020a).

[6] European Commission (2020b).

[7] European Commission (2016a), Frontex (2020b).

- Reducing the vulnerability of the EU's external borders (e.g. through comprehensive situational awareness).
- Guaranteeing 'safe, secure and well-functioning EU borders' (e.g. through the deployment of EBCG teams of border and coast guard officers provided by Member States).
- Planning and maintaining EBCG capabilities.[8]

In support of these objectives, part of Frontex's mandate is to monitor and contribute to developments in research and innovation relevant to its area of operations, so as to bridge the gap between technological and research advancements and the needs of the European border authorities. Artificial Intelligence (AI) is one area that has attracted increasing interest from law enforcement and border security agencies in relation to enhancing existing capabilities to address border security challenges.

To date, AI-based capabilities have been explored in relation to various border and migration management tasks, including border surveillance, processing of travellers at border crossings, providing situational awareness and threat detection. In conjunction with an unprecedented rate of innovation and development in AI technologies, AI could offer opportunities to improve the existing way of performing border security functions, including in relation to performing resource-intensive, repetitive or highly complex analytical tasks with increased efficiency, accuracy and quality of results. AI could also, more broadly, improve the ability of border security agencies to adapt to a fast-paced geopolitical and security environment.[9] However, various technical, organisational, ethical, legal and regulatory barriers might influence how AI materialises in the performance of border security functions.[10]

1.2. This study aims to characterise the opportunities, requirements and challenges for AI-based capabilities in border security

The overarching aim of this study is to explore the ways in which the EBCG can maximise the opportunities provided by AI-based capabilities in support of border security functions. To achieve this objective, the study aims to answer four research questions (RQs), outlined in Box 1.

[8] Frontex (2019b).

[9] Accenture (2017).

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

Box 1 Overarching study 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?

Source: RAND Europe.

To address these RQs, the study was divided into two technical work packages (WPs), with a continuous supporting work package (WP0) comprising project management and coordination of project deliverables:

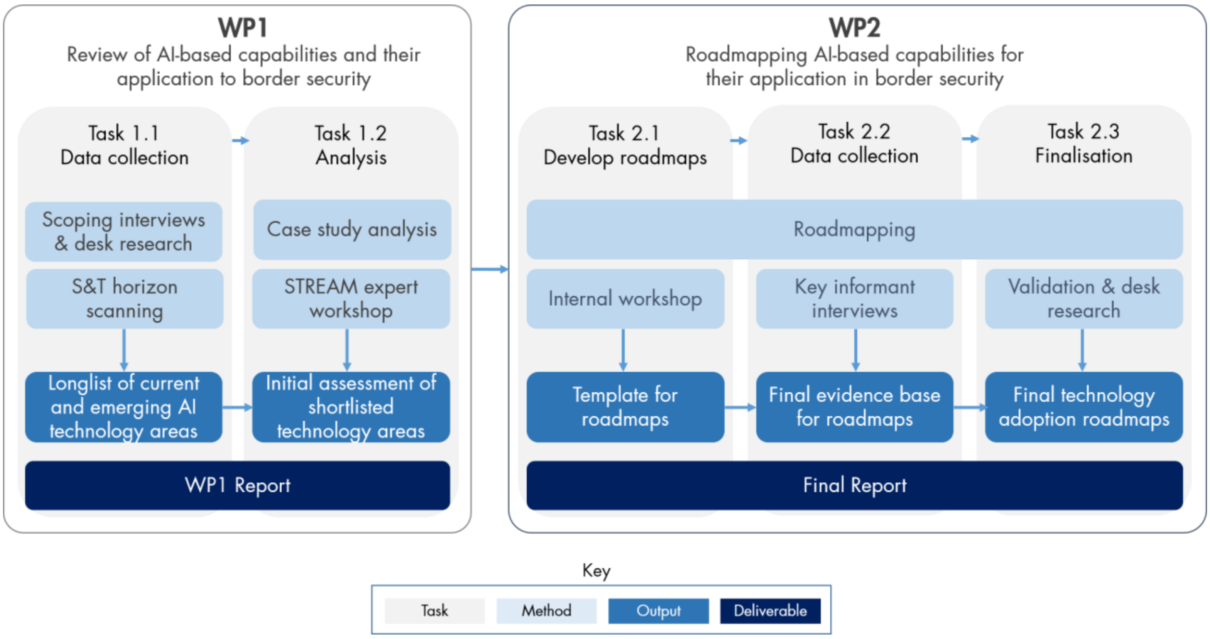
- **WP1 – Review of AI-based technologies and their application in border security** aimed to characterise the current landscape of AI-based applications in border security as well as trends in new and emerging AI-based systems of potential use in border security. This resulted in the identification of nine areas of border security functions in which AI-based technologies are being or might be utilised in the future.
- **WP2 – Roadmapping of AI-based technologies for application in border security** aimed to build on the evidence base provided in WP1 through the development of nine technology adoption roadmaps for the selected areas of border security functions. These served to elaborate on the possible pathway from current to desirable future capability levels, relevant requirements and barriers for adoption, and mapping of relevant technology use cases.

This report provides a summary of all research activities carried out by RAND Europe in answering the RQs outlined above.

1.3. The research team adopted a mixed-methods research approach to meet the study objectives

To meet the objectives of this study, the RAND Europe research team adopted a structured approach that used a range of research methods for data collection, synthesis and analysis. Figure 1.2 provides an overview of the study research approach, which was structured in two WPs. Annex A presents an in-depth explanation of the study methodology.

Figure 1.2 Study research approach


WP1
Review of AI-based capabilities and their application to border security
Task 1.1
Data collection
Task 1.2
Analysis
Scoping interviews & desk research
Case study analysis
S&T horizon scanning
STREAM expert workshop
Longlist of current and emerging AI technology areas
Initial assessment of shortlisted technology areas
WP1 Report
WP2
Roadmapping AI-based capabilities for their application in border security
Task 2.1
Develop roadmaps
Task 2.2
Data collection
Task 2.3
Finalisation
Roadmapping
Internal workshop
Key informant interviews
Validation & desk research
Template for roadmaps
Final evidence base for roadmaps
Final technology adoption roadmaps
Final Report
Key
Task
Method
Output
Deliverable

Source: RAND Europe.

In the first phase of the research, the study team investigated the first three RQs:

1. What is the current landscape in the application of AI to border security?
2. Which new and emerging AI-based systems could be applied to border security?
3. In which areas of border security might new and emerging AI-based systems be applied?

This was achieved through a two-fold data collection process:

- **Scoping interviews** with Frontex experts and **desk research** to identify known AI capabilities or R&D programmes in the military, border security and public safety sectors, as well as possible use cases for AI-based technologies within a border security context.
- **Horizon scanning** for emerging AI-related science and technology (S&T) developments, using RAND Europe's Centre for Futures and Foresight (CFFS)'s horizon-scanning database, in order to understand current and future AI trends that could be relevant to the border security context.

The output of the initial data-collection stage was an overview of AI technologies currently used in relation to border security or of potential utility to border security, characterising the current and future landscape of AI-based capabilities in border security. A summary of this overview is featured in **Chapter 3** of this report. In consultation with Frontex, nine AI technology areas were prioritised for further in-depth review through case study and workshop analysis in the second stage of WP1.

The nine technology case studies were developed through **review of open source literature** and **key informant interviews** with AI technology developers and suppliers. The case studies featured information on the purpose of each technology area (i.e. their use and applicability to the border security context), the status of development (i.e. technological maturity), and potential enablers and barriers for further adoption of the technology. An **expert workshop** was then held, comprising both Frontex and other experts, to provide further depth and nuance to the opportunities for, potential impact of and barriers to the adoption of these technologies in a border security context. This assessment workshop was delivered using the RAND-developed Systematic Technology Reconnaissance, Evaluation and Adoption Method (STREAM) approach, which is further explained in Annex A. The full list of experts who participated in the workshop is included in Annex A, with the output of the workshop summarised in Annex B of this report.

The second phase of the study (WP2) expanded on the findings from WP1 and sought to answer the fourth research question of the study:

4. What steps are required to integrate AI-based systems into border security?

This entailed a further exploration of each of the nine technology areas, including:

- Existing and desired capability levels in relation to each technology area;
- Specific requirements and potential barriers to achieving the desired capability levels; and
- Mapping of relevant illustrative use cases, including commercial products and R&D projects.

The research team employed a **roadmapping approach** that drew on data collected through WP1, additional key informant interviews with technology experts and border security end-users, and internal workshops and additional desk-based research to synthesise, validate and triangulate data and address outstanding data gaps. The output of WP2 is summarised in **Chapter 4** – which presents an overview of the nine technology area roadmaps – **Chapter 5** – which provides additional insights on cross-cutting enablers, challenges and barriers to implementation – and lastly, **Chapter 6** – which offers the study team's conclusion and recommendations on how Frontex can seek to maximise the opportunities provided by AI-based capabilities in the future.

1.4. This report is structured in six chapters

In addition to this introductory chapter, the report features five additional chapters:

- **CHAPTER 2 – AI technologies and their applicability in border security**, which provides the context and conceptual background for the study in relation to the nature of AI technology and its utility in border security.
- **CHAPTER 3 – Current landscape of AI-based capabilities in border security**, which discusses a taxonomy of current and potential future applications of AI technologies in border security and provides an initial assessment of nine selected AI technology areas, based on their likely impact and feasibility of implementation.
- **CHAPTER 4 – Characterising pathways to AI adoption in border security**, which presents nine technology adoption roadmaps, providing a more in-depth characterisation of current and desirable future capability levels, as well as the pathway to adoption of the nine selected AI technology areas.

- **CHAPTER 5 – Cross-cutting barriers and enablers for future AI adoption**, which discusses cross-cutting technological and non-technological barriers and enablers for future adoption of AI-based technologies by the EBCG.
- **CHAPTER 6 – Conclusions and implications for Frontex**, which discusses the key study findings and implications for Frontex and EU external border management.

The core report is accompanied by a full bibliography and four technical annexes:

- **ANNEX A – Methodology**, which provides a description of the study methodology.
- **ANNEX B – Summary of quantitative findings from the STREAM workshop**, which describes quantitative findings from the external workshop that assessed potential impact and feasibility of implementation of the nine selected technology areas.
- **ANNEX C – Catalogue of AI technology use cases**, which includes a longlist of technologies identified in the research.
- **ANNEX D – Technology adoption roadmaps**, which provides an in-depth description of the technology adoption roadmaps for the nine selected technology areas.

2. AI technologies and their applicability in border security

This chapter provides a definitional and conceptual framing to act as background for the analysis that follows in the rest of this report of the opportunities and challenges associated with the adoption of AI-based capabilities by the EBCG. It provides a definition of AI as well as a description of key components and types of AI technologies, and discusses which tasks AI technologies could be used for in the context of border security.

2.1. AI encompasses technological systems that can perform tasks with a degree of autonomy

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.[11] As such, AI systems might seek to perform functions or problem-solving behaviour in relation to searching for problems or solutions, recognising patterns, learning and generalising from past solutions for future problem-solving, planning and organisation of resources, and adapting and transferring learned behaviour.[12] In this context, AI systems can operate exclusively in the virtual world – such as in image analysis software, search engines and speech recognition systems – or be embedded in real-world hardware devices, such as AI software within advanced robots, autonomous cars or drones.[13]

In the context of this study, we refer to AI using the definition developed by the Independent High-Level Expert Group on Artificial Intelligence (AI HLEG) set up by the European Commission, captured in Box 2.

[11] European Commission (2019).

[12] Wong et al. (2020), Minsky (1961).

[13] European Commission (2019).

Box 2 Definition of AI

‘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. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions’.

Source: European Commission (2019).

As captured in Figure 2.1 below, there are four key components to any AI system[14]:

- **Sensors (physical or digital):** The role of sensors (physical or digital) is the acquisition of data. Data underpins the performance of AI systems, and may be acquired in a number of different means, including through the use of physical sensors (such as cameras and microphones), input devices (such as keyboards or mouse clicks) and through the collection and processing of pre-existing data sets, such as text available on websites or in published literature.

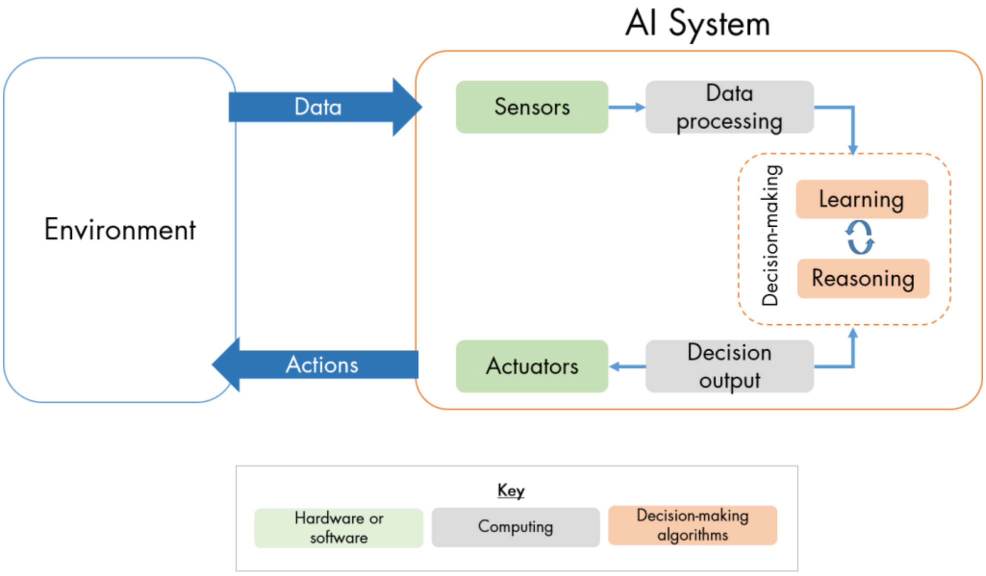
- **Data processing:** Data captured by sensors must be processed before it can be understood and used by the decision-making component of an AI system. As such, data processing refers specifically to the interpretation and simplification of complex data sets into more succinct forms of information, such as the identification of a face within a digital image, or the identification of a specific theme within text stored as a series of zeros and ones.

- **Decision-making algorithms:** Information captured through data processing forms the input for the decision-making algorithms of an AI system, which uses mathematical models to determine an optimum action or output for the system. This action is implemented either in the real or physical world through relevant actuators.

- **Actuators:** Determined by its decision-making, the AI system may perform an action through physical or digital means to engage with the environment or human user. An autonomous vehicle, for example, may decide to change direction based on its interpretation of the road ahead, whereas an AI-driven chat bot may produce a segment of original text based on its interpretation of the preceding text input by a human user.

[14] European Commission (2019).

Figure 2.1 Components of an AI system



Source: RAND Europe adapted from European Commission (2019).

Though AI systems share these common elements, there are various differences between AI systems, including in levels of autonomy and sophistication. A common classification of AI based on its sophistication features the following categories:

- **Artificial Narrow Intelligence (ANI)**: encompasses AI systems that are only able to perform specific tasks autonomously with human-like capabilities, when programmed to do so. ANI systems have a relatively narrow range of competencies, though currently these represent the most advanced AI systems in the present state of AI development.[15]
- **Artificial General Intelligence (AGI)**: refers to AI systems able to replicate human intelligence in its entirety – i.e. learn, perceive, understand and function as a human. AGI systems would include the ability of a system to perform fully autonomous learning of multi-functional capabilities.[16]
- **Artificial Superintelligence (ASI)**: builds on AGI capabilities by exceeding human comprehension. Achieving ASI is likely to lead to a process whereby further advances in AI derive from 'super-intelligent AI designing improvements to itself'.[17]

Further to varying levels of AI sophistication, AI systems may be categorised by their learning ability (e.g. Symbolic AI compared to Machine Learning – ML[18]) or the various techniques associated with AI, including computer vision and natural language processing (NLP), which have different attributes and capabilities to provide for the end user. Table 2.1 provides an introduction of some of these concepts, which are used throughout this report.

[15] Joshi (2019).
[16] Joshi (2019).
[17] Wong et al. (2020).
[18] See Table 2.1 for a definition of Symbolic AI and Machine Learning.

Table 2.1 Summary of key techniques and sub-sets of AI

Category	Technology area	Description
Methods	Artificial Neural Networks	As a technique of AI, Artificial Neural Networks can be described as 'processing devices that are loosely modelled after the neural structure of a brain'.[19] They include Deep Neural Networks – systems that perform deep learning.[20]
	Machine Learning	Machine Learning is commonly understood as a sub-set of AI and a basis of most AI systems, referring to the ability of computers to learn independently through exposure to training data.[21] Machine Learning encompasses 'supervised' and 'unsupervised' Machine Learning (Deep Learning), with the latter able to process unlabelled data by extracting features and patterns autonomously.[22]
	Deep Learning	Deep Learning encompasses unsupervised Machine Learning, describing systems carrying out unsupervised learning methods, i.e. representational learning that is not based on historic data. Deep Neural Networks are able to 'make predictions when presented with unfamiliar data'.[23]
	Symbolic AI	In contrast to Machine Learning, which focuses on the development of algorithms to enable autonomous problem-solving abilities in computers, symbolic AI encompasses the 'explicit embedding of human knowledge and behaviour rules into computer programs'.[24]
Applications	Computer Vision	Computer Vision describes the use of AI to 'train computers to interpret and understand the visual world'.[25] This is frequently applied to the processing of imagery from cameras and videos, e.g. for object recognition and identification.[26]
	Edge AI	Edge AI computing features networks of 'hardware and software platforms connected with IoT [Internet of Things] technologies', performing computations at the 'edge' of a network rather than on a remote server, as is the case with cloud computing.[27] This enables more efficient bandwidth use as well as lower latency, higher privacy and more network robustness.[28]
	Natural Language Processing	Natural Language Processing encompasses AI in relation to language – including speed recognition and language generation – and can thus be defined as 'the automatic (or semi-automatic) processing of human language.[29]

Source: RAND Europe analysis.

[19] Deloitte (2018).

[20] Babuta et al. (2018).

[21] Deloitte (2018).

[22] Salian (2018).

[23] Babuta et al. (2018).

[24] InBenta (2020).

[25] SAS (2020).

[26] SAS (2020).

2.2. Recent years have seen increasing interest in AI and rapid growth of AI applications in various sectors

Recent years have witnessed rapid development of advanced AI techniques, as well as increasing breadth of applications of AI, and a growing interest in the use of AI among private and public sector end users, including border security and law enforcement agencies. Several trends can be identified that have incentivised this growing interest in the uses of AI within border security contexts:

- **The need to process an increasing amount of data**: The growth of data collection (e.g. through social media, increasing number of sensors, the Internet of Things, etc.) is driving a requirement for end users to process increasing amounts of data – often to an extent that is overwhelming for human operators. As such, AI is perceived to have particular utility for tasks and functions that require the processing and analysis of large quantities of heterogeneous data (Big Data).[30]
- **Cost- and resource-efficiency**: Border and Coast Guard authorities might be motivated to use AI in order to address shortages and high cost in relation to human resources. In the European context, the shortage of certain border and coast guard profiles is contributing to interest in a broader uptake of AI in the context of tasks that could be automated, thus enabling better utilisation of human resources and cost-saving.[31]
- **Decreasing costs of data storage and processing power**: Key enabling capabilities and processes, such as data storage and processing power, are increasing in availability and capacity and decreasing in price, which increases the perceived economic viability of AI adoption.[32]
- **Democratisation of AI**: Democratisation of technology, including AI, refers to processes by which technology becomes rapidly accessible to a wide range of people and organisations. In relation to AI, this encompasses the proliferation of open-source, low-cost technological solutions, enabling easier access for a greater number and variety of stakeholders, including border security agencies – which may face greater cost barriers to adopt advanced technologies in contrast to, e.g., stakeholders within defence.[33]
- **EU initiatives on AI**: As discussed in Chapter 1, recent initiatives from the European Commission – including the 2020 White Paper, the 2018 European strategy and the

[27] Eurotech (2020).
[28] Lee et al (2018).
[29] Copstake (2004).
[30] S-INT01.
[31] S-INT02.
[32] Deloitte (2019a), McKinsey Global Institute (2017).
[33] Deloitte (2019b).

2018 Coordinated Plan – have incentivised the development and adoption of AI, in particular human-centric AI, through encouraging investment and cooperation as well as augmenting the EU's global competitiveness in the AI market.[34]

As a backdrop to these trends that provide an impetus for AI adoption, AI provides a number of cross-cutting opportunities and benefits for end users within the public sector. Firstly, AI-enabled systems may be used to perform resource-intensive, repetitive or highly complex analytical tasks to enable more efficient allocation of human and financial resources. Particularly in areas involving vast quantities of data, AI could also enable better data processing and analysis, including the production of more accurate, robust and comprehensive insights (e.g. in the context of threat detection and risk analysis). More broadly, AI could also provide opportunities for strengthening organisational innovativeness and adaptability, i.e. improving the ability of organisations and public sector agencies to adapt to a fast-paced socio-economic, geo-political and security environment through harnessing the benefits of innovative technologies.[35]

There are various tasks that an AI can be used for to harness these opportunities. These tasks are commonly categorised as:

- **Automation**: AI technologies can be employed for the automation of digital or physical tasks, including e.g. in the context of administration and information management. Technologies utilised for task automation encompass cognitive robotics and autonomous systems, and may employ various AI techniques (e.g. NLP to automate the processing of documents).
- **Cognitive insight**: Based on the ability of AI-based systems to process and analyse large quantities of data, AI technologies are used for cognitive insight, i.e. the analysis of data through ML-enabled advanced and predictive analytics. ML-enabled cognitive insight generally encompasses larger quantities of data and greater detail and quality of insights provided by the model (e.g. accuracy of predictions) in contrast to traditional analytics.
- **Cognitive engagement**: AI techniques – such as NLP and ML – are integrated in intelligent virtual agents that can engage or interact with their environment. Though cognitive engagement technologies are, to date, relatively immature and often require human intervention, intelligent agents are employed in the public and private sector to answer questions and address inquiries or provide product and service recommendations.

While this categorisation is applicable to a wider range of sectors, existing and emerging AI technologies can also be mapped in relation to functions and end-user needs that are specific to border security contexts. As such, the following chapter discusses the specific functions that AI technologies are currently being employed for in border security and provides an initial view of the potential impact and barriers to implementation of selected AI technology areas.

[34] European Commission (2018a), European Commission (2018b).

[35] Accenture (2017).

3. Current landscape of AI-based capabilities in border security

This chapter discusses the research findings in relation to RQs 1–3 of the study:

- **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?

In so doing, it presents an analytical taxonomy of AI-based capabilities in border security, and introduces nine AI technology areas that were explored in more detail through the roadmapping exercise (**Chapter 4**).

3.1. AI could be used in relation to various border security functions in relation to various capability and technology areas

The current and potential future landscape of AI-based capabilities in border security is characterised by significant diversity in terms of the tasks, functions and purposes an AI system serves or performs. To provide a clear and coherent framework for characterising this landscape, Table 3.1 provides a summary overview of the different uses of AI that we identified, in relation to a taxonomy of border security functions as well as to the corresponding capability and technology areas. The taxonomy classifies use cases identified through the data collection methods described in Section 1.3 in relation to:

- **Border security functions**: Refers to the broad components of responsibility of the European Border Security and Coast Guard within European Integrated Border Management, as outlined in the EU Regulation 2019/1896. The RAND Europe research team used a classification of border security functions developed by the European Security Research Advisory Board (ESRAB).[36]
- **Capability areas**: Refers to selected capabilities used to carry out the corresponding border security function. While the performance of the listed border security functions may include a wider range of capability areas, Table 3.1 focuses on the key areas within which AI is or could be utilised.
- **Technology areas**: Different technologies can constitute a capability area. The taxonomy includes a selection of illustrative technology areas corresponding to the various

[36] ESRAB (2006).

current use cases of AI-based systems, and emerging S&T trends that indicate potential future uses of AI in border security. A longlist of use cases and S&T items identified is included in Annex C.

Table 3.1 Taxonomy of current and potential uses of AI in border security

Border security function	Description	Illustrative capability areas	Illustrative AI technology areas
Situation awareness & assessment	Collection, fusion and analysis of disparate forms of real-time and historical data to facilitate decision-making and operational response in complex environments. It includes capabilities used for wide and small area surveillance of people, vehicles and objects in the proximity of external borders, at Border Crossing Points (BCPs) and between BCPs.	Surveillance (installations and autonomous systems)	AI-enabled surveillance towers, sUAS, heterogeneous robotic autonomous systems
		Surveillance database cross-analysis and information correlation	Person re-identification, maritime domain awareness
Information management	The ability to manage data and information, including through data mining and fusion techniques, natural language processing, image/pattern recognition, information exchange and capabilities to ensure security and interoperability of systems.	Information management automation	Automated ML, automated data generation, geospatial data analytics
		Data fusion	Maritime and geospatial data analytics
		Predictive analytics	Predictive asset maintenance, AI-assisted analytics of migration flows and cross-border crime trends
Communication	Communication and information sharing capabilities, including secure end-to-end communication, authentication technologies and technologies for secured communications, such as wireless broadband data links.	End-to-end communication	Chatbots and virtual agents, agent-to-system communication links
Detection, identification & authentication	Capabilities used to detect and identify potential threats and authenticate people and objects, such as tracing and tracking technologies, access control, and early warning technologies.	Access control, identification and verification of people and vehicles	Automated border control, biometric scanning, facial recognition, document authentication
		Threat detection	Object recognition; airspace threat detection systems (C-UAS)
		Cognitive robotics	Robotic border patrol agents
Training and exercise	Capabilities for improving staff readiness and expertise through training and exercise.	Training, education and simulation capabilities	AI-enabled synthetic environments and simulation

Source: RAND Europe analysis based on ESRAB (2006).

The taxonomy-based mapping of technology and capability areas demonstrated the breadth of current applications and potential opportunities for end users in the border security context associated with AI. The mapping highlighted several high-level findings with regard to the nature of both the current and potential future landscape of AI-based capabilities in border security:

- The taxonomy covers applications of AI in all three categories of tasks, i.e. automation (e.g. automated border control), cognitive insight (e.g. predictive analytics) and cognitive engagement (e.g. chatbots and robotic border patrols). As such, there are opportunities for border security end users to harness the full spectrum of AI technologies, corresponding advances in the sophistication of AI-based systems and the breadth of their applications.
- Within the spectrum of border security functions, AI appears most frequently utilised for information management purposes, followed by the provision of support in situation awareness and assessment, and detection, identification and authentication. While AI technologies may be utilised as a standalone information management capability (e.g. in the form of solutions for predictive analytics), AI-based information management, in particularly data fusion, is also frequently integrated within wider technological systems (e.g. surveillance capabilities).
- The research team identified few use cases in relation to communication and information sharing capabilities, and training and exercise capabilities. Rather than indicating that AI could be of limited utility in relation to these border security functions, it is likely that relevant use cases can be identified or are being developed in other sectors, such as law enforcement and defence.
- While the taxonomy does not differentiate between the various operational settings in which border security functions are performed, it is recognised that the utilisation of AI-based capabilities and technologies might vary according to the given operational context. End users operate in the context of different border types, which might generate different requirements in relation to the technological solutions or the functions performed by an AI-based system.

3.2. The research team examined nine technology case studies to explore potential impact and implementation factors for AI adoption in border security

Despite the significant and increasing variety in the border security tasks and functions for which AI might be used, not all capabilities are of equal interest and utility for the EBCG. EBCG end users might have different requirements based on operational context and organisational capacity, and thus have different priorities guiding investment decisions in relation to AI-based capabilities. The presence of various barriers to implementation represents an additional factor for investment considerations.

To provide a more in-depth understanding of the opportunities and challenges associated with AI-based capabilities, nine technology areas that could improve existing ways of performing border security functions by the EBCG were selected in consultation with Frontex. These nine technology areas are listed in Table 3.2 below and are further explored in **Chapter 4**.

Table 3.2 Selected technology areas

#	Technology area	Description	Capability area	Border security function
1	Automated border control	Integrated systems of e-gate hardware, document scanning and verification, facial recognition and other biometric verification, which are used to facilitate the processing of travellers on border crossings while enhancing security through the integration of various AI-enabled tools.[37]	Access control, authentication of people and vehicles	Detection, identification and authentication
2	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 contextual information concerning the weather, commercial activities, environmental conditions, military exercises and maritime incidents.[38]	Data fusion, surveillance database cross-analysis and information correlation	Information management, situation awareness & assessment
3	Machine learning optimisation	Use of AI to automate the selection, testing and optimising of Machine Learning models, a solution known as automated machine learning (AutoML). This includes the automation of all steps of ML algorithm development, from identifying the problem/process to be improved, data collection and clean-up, model development, training and evaluation.[39]	Information management automation	Information management
4	Surveillance towers	Unmanned surveillance capabilities in the form of autonomous surveillance towers fielded in border regions, integrating software and hardware surveillance capabilities, e.g. to detect illegal border crossings.[40]	Surveillance (installations)	Situation awareness & assessment

[37] European Commission (2020d).

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

[39] DataRobot (2020).

[40] Feldstein (2019), Anduril.com (2020).

#	Technology area	Description	Capability area	Border security function
5	Heterogeneous robotic systems	A capability that integrates various unmanned systems, including vehicles of 'different sizes and abilities for maritime, land and air environments'.[41] Networked heterogeneous robotic systems may be applied to various functions, including environmental monitoring, border control and counter-terrorism.	Surveillance (autonomous systems)	Situation awareness & assessment
6	sUAS	Small autonomous unmanned aerial systems (sUAS) that may be used to perform functions such as border surveillance, environmental monitoring and disaster relief. sUAS often include integrated AI-enabled object recognition, classification and tracking capabilities.[42]	Surveillance (autonomous systems)	Situation awareness & assessment
7	Predictive asset maintenance	Predictive analytics enabling optimal operations and maintenance of technical systems.[43] This may enable end users to identify vulnerabilities, sub-optimal performance or potential technical failures in complex technical systems such as multi-vehicle UAS networks that are used for ground surveillance or strengthening airspace awareness.[44]	Predictive analytics	Information management
8	Object recognition	Algorithmic recognition and classification of objects through annotation, training and analysis of complex data, e.g. 3D imagery. Object detection and recognition systems are extensively utilised to perform functions including detection of suspicious packages, vehicles and cargo.	Threat detection, information management automation	Detection, identification and authentication, information management
9	Geospatial data analytics	Use of AI to analyse geospatial data, including labelling and classification of satellite imagery. Geospatial data analytics may support operational awareness and threat detection.[45]	Information management automation	Information management

Source: RAND Europe analysis.

[41] Miskovic et al. (2014).

[42] Fussell (2019), Planck Aerosystems (2019).

[43] SparkCognition (2018).

[44] WP1-INT12.

[45] Lockheed Martin (2019).

The nine technology areas represent a variety of capabilities illustrating the range of functions that AI may perform, and the operational contexts in which it may be used. This selection of technology areas also captures the variety in terms of a system's status of development and level of engagement by the end user. Figure 3.1 provides an overview of the nine technology areas distinguished by maturity (i.e. capabilities that are in use, or still in development) and by level of engagement by the end user (i.e. capabilities that represent more underlying technologies, which the end user may not directly interact with, or front-end technologies).

Figure 3.1 Categorisation of selected AI capabilities by maturity and level of end user engagement

	Underlying technology	Front-end technology
In use	• Machine learning optimisation	• Surveillance towers • Maritime domain awareness • sUAS
In development	• Object recognition • Predictive asset maintenance	• Automated border control • Heterogeneous robotic systems • Geospatial data analytics

Source: RAND Europe analysis.

3.3. AI-based capabilities might have different impact and implementation pathways to be considered by the EBCG

To identify the areas of border security in which new and emerging AI-based systems might most likely be applied by the EBCG, the study team carried out an initial assessment of the nine selected technology areas in the form of an external expert and stakeholder workshop. The workshop consisted of a scoring exercise, gathering expert and stakeholder perspectives on the potential impact of and barriers to the implementation of the nine technology areas.[46] Box 3 provides a summary of the criteria against which the technology areas were assessed, with further details provided in **Annex A.**

[46] The workshop methodology is described in further detail in Annex A.1.2.

Box 3 Summary of the technology impact and implementation criteria

Two sets of factors underpin decision-making in relation to the adoption of new or emerging technologies in a given organisational context:

- **Impact**: potential impact of individual technologies on functions and desired outcomes in specified capability areas.
- **Feasibility of implementation**: potential technical, organisational, commercial, regulatory and other barriers to implementation that could impact the feasibility of adoption of individual technologies.

The study team identified the following criteria capturing the scope and nature of potential impact of AI-based technologies on the performance of border security functions:

- **Speed and efficiency**: ability to perform border security functions more efficiently, e.g. faster or with less resources.
- **Accuracy and quality of results**: ability to perform border security functions more effectively, e.g. with higher quality and accuracy of results.
- **Innovativeness**: ability to carry out a border security function through novel approaches using AI technology.

While AI-based technologies could have a significant positive impact in these regards, end users might face various barriers to their implementation. The study team identified six such barriers against which the nine selected technology areas were scored during the expert workshop:

- **Unfamiliarity with technology and uncertainty concerning its performance.**
- **Financial cost to implement, operate and maintain the required technology infrastructure.**
- **Additional infrastructure requirements** (e.g. connectivity, computational power, systems, networks, etc.).
- **Data protection and regulatory barriers.**
- **Limits on access to relevant technologies** (e.g. due to export control restrictions, lack of European suppliers, etc.).
- **Insufficient political or public acceptance** (e.g. due to ethical and human rights concerns).

Annex A provides a more in-depth description of these impact and implementation criteria. Chapter 5 provides additional discussion on the cross-cutting barriers for further adoption of AI in border security.

Source: RAND Europe.

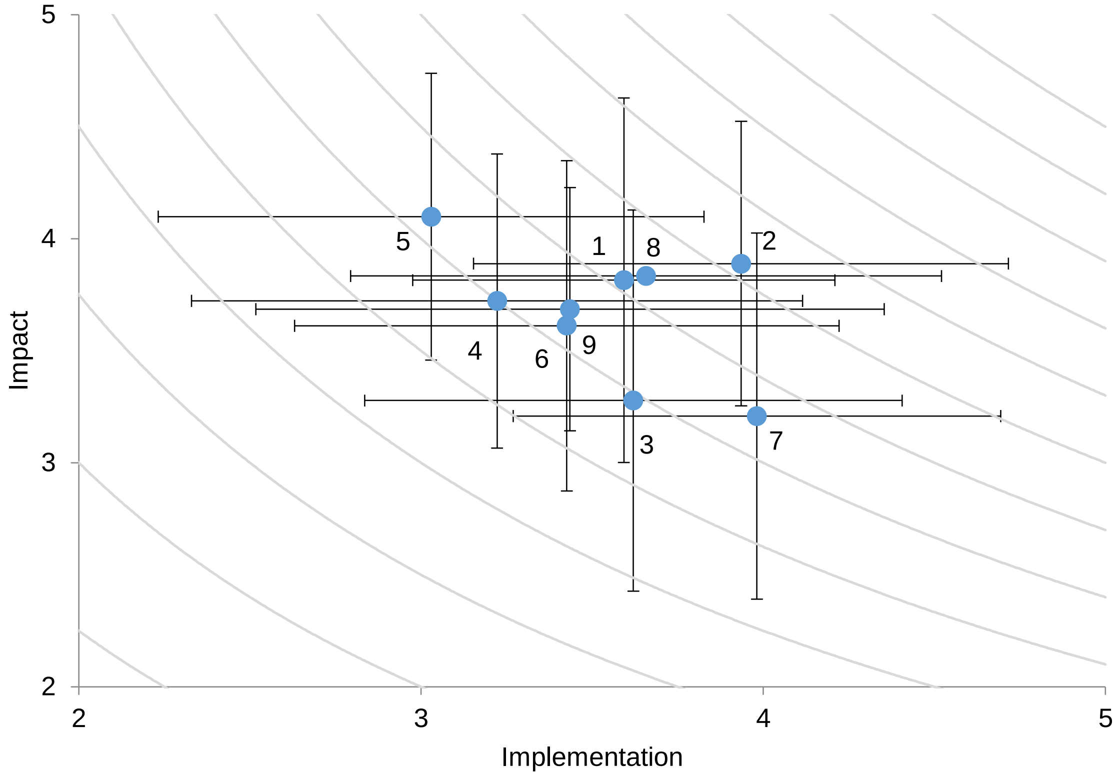
As described in Box 3, the initial analysis of the nine technology areas considered a range of impact and implementation criteria to illicit initial views of stakeholders on how AI-based systems might best be utilised by the EBCG. Figure 3.2 provides a summary of the assessments of the nine technologies against the specified criteria.[47]

[47] Annex B provides a more in-depth discussion of the underpinning quantitative analysis.

Table 3.3 Figure key – numbered technology area labels

#	Case Study	#	Case Study
1	Automated border control (ABC4EU)	6	sUAS (Planck Aerosystems sUAS)
2	Maritime domain awareness (Marint)	7	Predictive asset maintenance (SparkPredict)
3	Machine learning optimisation (AutoML)	8	Object recognition (Synthetik object recognition)
4	Surveillance towers (Sentry Towers)	9	Geospatial data analytics (GATR)
5	Heterogeneous robotic systems control (Roborder)		

Figure 3.2 Aggregated scores for all nine technology areas with error bars (+- standard deviation)



Source: RAND Europe analysis.

The scoring results revealed a number of high-level findings concerning the perceived differences in impact and feasibility of implementation of the nine technology areas:

- On average, AI-based capabilities are expected to have the greatest impact on the speed and efficiency with which border security functions can be carried out. As such, there is more confidence in the positive contribution of AI to make border security functions more efficient by saving financial and human resources, rather than the ability of AI to qualitatively improve the results of processes underpinning such functions (e.g. in their accuracy).
- Maritime domain awareness received the highest combined score for both impact and feasibility of implementation, reflecting expectations for the technology to have a

relatively high impact on the performance of border security functions with relatively low barriers to implementation. This indicates significant potential benefit of AI-enabled information management capabilities for end users.

- While AI-enabled border surveillance systems are seen as having high impact on border security functions, particularly in terms of speed and efficiency with which these are performed, there are a number of important barriers to implementation, in particular financial costs and regulatory barriers – including data protection requirements. The presence of these barriers might indicate that on average AI-based surveillance systems represent potentially high-reward, but also high-risk opportunities for border security authorities.

Table 3.4 Top 3 technology areas according to impact, implementation and combined assessments

Top 3 combined	Top 3 impact	Top 3 implementation
1. Maritime domain awareness	1. Heterogeneous robotic systems control	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.

The technology assessments overall revealed that although the perceived impact and potential barriers of implementation of AI-based capabilities may vary, all selected technologies were generally believed to have at least a moderate positive impact on the ability of end users to perform border security functions. Additionally, none of the technology case studies 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.

These findings indicated that all nine technology areas were of potential interest to end users within the EBCG, and warranted further exploration in relation to the necessary steps to adopt the technologies. The following chapter provides a summary of the technology adoption roadmaps that were developed to address this requirement.

4. Characterising pathways to adoption of AI-based capabilities

Building on the overview of the evolving landscape of AI-based capabilities in border security, this chapter presents research findings in relation to **RQ4** – 'What steps are required to integrate AI-based systems into border security?'. To that end, the chapter further characterises the nine selected technology areas by providing an overview of the findings from the technology adoption roadmaps. These address three core questions:

1. What is the current state of capability?
2. What is the desired future state of capability?
3. What is the pathway to adoption, including requirements for and risks to implementation?

The technology roadmaps draw on data gathered through the case study analysis and expert workshop in WP1, as well as interviews with technology and border security experts and desk research conducted in WP2. The research team structured each technology adoption roadmap to discuss a series of implementation factors, outlined in Box 4.

Box 4 Structure of the technology adoption roadmaps

In this study, technology adoption roadmaps aim to provide a structured description of the potential capabilities that could be implemented in border security and their potential pathways to adoption. Each roadmap is structured as follows:

- Summary of **current and desired capability** levels and the **pathway to adoption**.
- Summary of **key requirements and potential barriers to adoption** in relation to those requirements, including a discussion of seven categories of elements of adoption:
    1. Personnel & training
    2. Infrastructure, equipment & logistics
    3. Information
    4. Organisation
    5. Regulatory, legal & ethical
    6. Technology performance
    7. Other requirements/barriers to adoption
- List of **illustrative use cases** including commercial products and R&D projects currently in use or in development, which could address defined capability needs. This includes a short description of each use case including identified potential benefits and challenges associated with the technology.

Source: RAND Europe.

Rather than providing a detailed implementation plan for any given AI technology or capability, each roadmap provides a **high-level assessment** concerning the adoption requirements for the selected AI technology areas, and presents key factors for consideration by end users. The roadmaps also serve to identify key interdependencies among AI-based capabilities in relation to cross-cutting enablers and barriers to adoption, which are discussed in **Chapter 5**. This serves to identify any gaps in the current understanding of how different technologies might be adopted into European border security and thus inform current and future debate concerning the uses of AI in this context.

The rest of this chapter provides a summary of the findings of the roadmap research, with **Annex C** including full roadmaps for each of the technology areas.

4.1. Automated border control

The use of AI in the context of border control could entail a range of applications including biometric scanning, facial recognition and document authenticity validation. Frequently, these applications are linked into an integrated Automated Border Control (ABC) system consisting of gates and/or other forms of verification hardware. AI in this context could be utilised to improve ABC systems as a capability to detect potential threats, such as face presentation and morphing attacks.[48]

ABC gates can be defined as 'an automated immigration control system that conventionally integrates e-gate hardware, document scanning and verification, facial recognition and other biometric verification to facilitate faster processing of travellers on border crossings, while enhancing security through the integration of various AI-enabled tools. These serve to support the system in 'establishing that the passenger is the rightful holder of the document, examine border control records and automatically determine eligibility of border crossing according to pre-defined rules'.[49] Table 4.1 describes the current and desired capability for this technology area.

[48] Face presentation attacks are adversarial techniques in which a person attempts to be misclassified or misidentified by a biometric recognition system through the presentation of a falsified image (e.g. passport photo). Face morphing attacks, similarly, are digital manipulation techniques by which a person attempts to be misclassified by morphing two images (e.g. passport photos). Source: S-INT1.

[49] European Commission (2020d).

Table 4.1 Automated border control – current and desired capability

Current Capability

Currently, the EBCG employs border controls that rely heavily on border guards. Whilst border guards are supported by some new technologies that automate specific aspects of border control, the level of automation remains relatively low and typically requires human-in-the-loop operators. However, many of the governments across Europe and globally (especially the US) have begun to test the use of border gate technology that will enable more autonomy for processing the passage of goods and people through BCPs.

Desired Capability

As developments in AI and supporting hardware enable greater accuracy, ABC gates are expected to become more prominent. It is expected that ABC will provide 'an automated immigration control system that conventionally integrates e-gate hardware, document scanning and verification, facial recognition and other biometric verification to facilitate faster processing of travellers on border crossing while enhancing security through the integration of various AI-enabled tools'. [50] These functions will be integrated as part of automated controls that will support border guards in establishing whether the passenger is the rightful owner of relevant documents, to automatically determine whether someone can pass through a border according to pre-defined rules.[51] The system will be able to alert border guards to any potential issues or non-compliance with these pre-defined rules.

Source: RAND Europe analysis.

ABC gates require limited amounts of technical knowledge to operate, so are expected to involve few requirements in relation to training of personnel. Some training might be required to ensure a level of organisational knowledge-base in relation to the nature, benefits and potential challenges associated with ABC systems, as well as addressing cultural barriers (e.g. lack of trust in the automation of tasks conventionally carried out by human operators).

Current requirements for achieving desired capability in automated border control are centred on the large amounts of computational power needed and associated cost barriers, as well as current deficiencies in integrated facial recognition and biometric scanning technologies. Although AI has already contributed to enhanced efficiency in facial recognition and biometric scanning processes, current systems do not perform with sufficient accuracy.[52] Technological advances in relevant sensor technologies and extraction algorithms are anticipated to improve these performance shortfalls.[53]

For further information on this technology area, see **Annex D.1.**

4.2. Maritime domain awareness

Maritime domain awareness encompasses capabilities aimed at establishing 'the effective understanding of anything associated with the global maritime domain that could impact [a

[50] European Commission (2020d).

[51] European Commission (2020d).

[52] WP1-INT05.

[53] WP1-INT05.

country's] security, safety, economy or environment'.[54] This relies on integrated analysis of various data streams including Automatic Identification Systems (AIS), coastal and vessel-mounted sensors, and contextual information concerning the weather, commercial activities, environmental conditions, military exercises and maritime incidents.[55] Though new satellite technologies have enabled greater amounts of data to be utilised in maritime domain awareness, extending the scope of information that can be considered – in the absence of effective analytics tools – creates greater complexity rather than clarity for end users, including border security agencies.[56] Table 4.2 captures the current and desired capability levels in relation to this requirement.

Table 4.2 Maritime domain awareness – current and desired capability

Current Capability
Existing capabilities for maritime domain awareness focus on intelligence gathering and threat detection to ultimately support decision-making. They can be described through manifold processes, including data collection via Automatic Identification Systems (AIS) from multiple databases (e.g. satellite imagery, available commercial sources). Once collected data fusion is undertaken using AI-based infrastructures, mistakes, irrelevances and corruption are filtered and eliminated, and the system generates analysis to support activity-detection of maritime vessels. For example, previous activities from a vessel might be flagged to operators and incorporated into semantic categories that facilitate subsequent analysis.[57]

Desired Capability
The next 5–10 years are likely to see greater use of AI-enabled solutions for enhancing situational awareness and threat detection through automated data processing and analysis.[58] Future capability should provide the ability to rapidly fuse maritime data from various sources, including shipping industry data and the Satellite Automatic Identification System (S-AIS), using AI to enable real-time maritime data analytics and improved detection and management of emerging threats. The operational profiling that results from the data about any maritime assets can provide analysts with relevant, rich insights to inform risk assessments. For example, the process will allow a user to know how many times a vessel visited a port at night-time, create a comparative assessment with other vessels, and assess whether an anomaly exists.[59] AI will also develop profiles of vessel behaviour, which could be used to, for example, learn the features of those involved in illicit activity and provide predictions on the most likely ships to engage in unlawful operations.[60]

Source: RAND Europe analysis.

The automation of data fusion and analysis processes presents few additional requirements or barriers related to personnel and skills for end users. Requirements in relation to infrastructure, equipment, logistics and organisation are also limited, indicating limited direct cost associated with AI-enabled maritime domain awareness capabilities.

[54] DHS (2005).

[55] Zhao et al. (2010).

[56] Peled (2020).

[57] WP1-INT07.

[58] Peled (2020).

[59] WP1-INT07.

[60] WP1-INT07.

Given the central role of data in the capability, however, there are several requirements and potential barriers related to the quantity and quality of data that define the pathway to adoption. As data for maritime domain awareness may be sourced from multiple vendors, relevant resources (e.g. databases) might include redundancies, noise and mistakes in the data. As such, improved data cleaning and data fusion capabilities might be needed to ensure accuracy and effectiveness of the model. Improvements in this area could also lead to the advancement of AI techniques to generate entirely new kinds of insights from the same data, with greater efficiency.

For further information on this technology area, see Annex D.2.

4.3. Machine learning optimisation

As machine learning (ML) is applied increasingly across different sectors and disciplines, end users are faced with a process for selecting, testing and optimising a given ML model for their requirements and in the context of different operations. This process conventionally requires several steps[61]:

a) identifying and specifying the business problem and expected value;
b) collecting and cleaning-up data into a standardised format;
c) labelling of data to enable the machine learning process;
d) extraction of features from raw data;
e) manual division of datasets into training, validation and holdout data;
f) selecting and specifying model evaluation criteria and accuracy metrics;
g) (iterative) training of the model based on training data;
h) evaluation of the model's performance; and
i) application of model outcomes into business processes.

To facilitate this process, interest has grown in the use of AI to automate the selection, testing and application of ML models through automated ML optimisation or automated machine learning (AutoML) technologies.

[61] DataRobot (2020).

Table 4.3 Machine learning optimisation – current and desired capability

Current Capability
Machine learning is already being used in border security across the globe. In particular, it is focused on assisting border security agencies and organisations to operate more efficiently in the gathering and processing of vast quantities of data. Whilst already in operation in a number of countries, including in Europe, the capability is still under development and has yet to become fully optimised. One challenge for current capability is the ability to optimise ML models that are in use for data processing. There are a number of AI-based technologies in development that are seeking to automate the selection, testing and optimising of ML models, which currently relies heavily on the use of human operators. There is a lack of standardisation amongst machine learning models, which currently limits the extent to which AI can be used to optimise ML model selection.

Desired Capability
In future, there are a number of areas that are likely to emerge for optimising ML models. To begin with, ML model outputs will become more standardised and models will employ common standards in their interfaces to reduce the requirements for human experts who can select an optimal model. The technology that is already in development – and should be operational in the near future – will allow users to more easily select from an ML-ranked list of machine learning models. This will enable users to make more informed choices based on their individual needs, which will maximise the efficiency of the ML chosen for each task.[62] As an example, the identification of human trafficking networks could benefit greatly from the use of facial recognition in conjunction with clustering, which employs ML models. By optimising the ML models used, law enforcement organisations will be able to more rapidly develop an understanding of different grouping and behaviours for traffickers.[63]

Source: RAND Europe analysis.

Algorithmic tools and models oriented towards the optimisation of other ML models are unlikely to entail any infrastructure-related requirements. However, while the optimisation of ML models is likely to provide increasing utility for end users given the wider uses of ML in other capability areas (e.g. predictive analytics), its adoption is by its nature contingent on wider adoption of ML in an organisation. As such, wider organisational and cultural shift towards innovation and the use of ML is an important requirement for adoption of this technology area. Considering the various performance risks and challenges with the ethics of AI (see Section 4.1.1.), enhancing transparency of ML and addressing the 'black box' challenge of AI represents another key requirement. Enhancing the transparency of ML models would serve to address end-user uncertainties in relation to technology performance, as well as potential algorithmic biases.

For further information on this technology area, see **Annex D.3**.

[62] DataRobot (2020).

[63] WP2-INT10.

4.4. Surveillance towers

In the context of border security, AI-enabled surveillance capabilities could take several forms, including static autonomous surveillance towers fielded in border regions. Surveillance towers represent an example of AI-based capabilities that are already utilised by end users.

Existing research suggests that an increasing number of actors are making use of AI-based capabilities for the purposes of surveillance in various environments, including land and maritime border regions.[64] Surveillance towers have, for example, been procured for installation along the US-Mexico border to enable the automatic detection of irregular border crossings. According to developers these systems provide a static surveillance capability that continues to be developed; furthermore, the current installation and testing of these is contributing to faster improvement of the capability through iterative development and continual testing and adaptation to end user needs and different operational contexts. [65]

Despite the existing adoptions, developers perceive that there continues to be significant reluctance among end users to commit to early fielding of AI-based capabilities, due to insufficient recognition of the readiness levels of the existing technology.[66]

Table 4.4 Surveillance towers – current and desired capability

Current Capability
AI-based surveillance towers currently have limited use in border security. The underlying technologies have been developed but remain relatively untested (although their testing and use is already expanding). The current capability in this area typically involves a static tower equipped with sensor and networking technologies that can be placed in the vicinity of a border. They can be deployed or moved relatively quickly and can include physical and virtual hardening to protect the system and technology components. Whilst relatively untested, the capability that exists includes onboard collection and fusion of data, as well as object detection that employs AI to reduce the amount of information and intelligence that human operators are required to handle and process.

Desired Capability
Whilst the overarching concept already exists, over the next few years the focus is likely to be on the broader testing and iterative development of the surveillance towers to improve efficiency and effectiveness. It is also expected that development will continue in the area of automated object detection and surveillance of large areas, to reduce the burden on human operators. It is expected that surveillance towers will provide near real-time analysis of larger areas through fused sensor data from the systems on board. It is also expected that as the capability develops, the surveillance towers will be seamlessly integrated with sensors from other platforms, such as UAS, to provide comprehensive and fully autonomous situational awareness.

Source: RAND Europe analysis.

There are challenges of limited public acceptance of AI-based surveillance capabilities and extensive polarisation in public discourses concerning the border control policies for which surveillance towers are utilised. The use cases indicate that ethical challenges and limited

[64] Feldstein (2019).

[65] WP1-INT04.

[66] WP1-INT04.

public acceptance, rather than limited technology readiness levels, could represent the key barriers to implementation for end users.

For further information on this technology area, see **Annex D.4.**

4.5. Heterogeneous robotic systems

Heterogeneous robotic systems represent a capability of networked robotic systems that integrate various unmanned systems, including vehicles of 'different sizes and abilities for maritime, land and air environments'.[67] Such networked systems have been of interest in various application areas, including environmental monitoring, border control and counter-terrorism.[68]

Table 4.5 Heterogeneous robotic systems – current and desired capability

Current Capability
Whilst a number of robotic systems are already being used in border security operations, there is no fully functional autonomous border surveillance system in place that employs unmanned and robotic aerial, water-based and ground vehicles as part of an interoperable network. Current capabilities are limited to individual systems and limited integration of platform and sensor data. Their unmanned systems require significant human resources to operate.

Desired Capability
In the next few years, various developers and border security authorities plan to implement a heterogeneous robotic system, which provides a semi-autonomous border surveillance solution with integrated swarms of aerial, water surface, underwater and ground vehicles incorporated directly into the network. Some developers believe that beyond this, there is the opportunity for enhancement with detection capabilities for early identification of land and maritime cross-border crime, including marine pollution.

Source: RAND Europe analysis.

As was noted during the external workshop, the development of heterogeneous robotic capabilities is likely to reduce the number and variety of technical systems being employed by national border security and law enforcement authorities. This indicates the presence of few infrastructure or logistics-related requirements, though organisations might need to conduct a comprehensive assessment of the operational and technical requirements associated with replacing old systems with new capabilities, and advanced cybersecurity solutions may be needed.[69]

Ongoing military R&D efforts on heterogeneous multi-vehicle systems indicate that significant technical challenges still exist with regard to the command and control (C2) of autonomous systems involving multiple vehicles with one human operator. However, the cost-effectiveness of heterogeneous capabilities relies on the ability of one operator to control multiple vehicles

[67] Roborder.eu (2020). Heterogeneity in this context refers to the presence of different types of systems (e.g. aerial and ground vehicles).

[68] Miskovic et al. (2014).

[69] WP1-INT10.

for various tasks or missions.[70] Regulatory barriers – including flight authorisations and data protection requirements (e.g. with regard to imagery and video capture) – were also identified as additional requirements and potential barriers to adoption, particularly in relation to the heterogeneity of the EU regulatory environment and 'strictness' of the GDPR.[71]

For further information on this technology area, see **Annex D.5**.

4.6. Small autonomous UAS (sUAS)

UAS technologies have been adopted in various civilian and military contexts, performing and supporting functions including surveillance, environmental monitoring and disaster relief. Law enforcement and immigration authorities have, for example, utilised drone-based surveillance programmes to detect illegal border crossings and coordinate border-guard patrols in the field.[72] The use of AI in the context of augmenting existing UAS capabilities has included object detection and classification and tracking capabilities, as well as improving the ability of UAS to operate in various operational environments. The current and desired levels of capability in relation to this area are summarised in Table 4.6.

Table 4.6 sUAS – current and desired capability

Current Capability
A range of sUAS are already employed by border security authorities around the world, including the use of AI to augment the ability of drones to identify and track targets. A number of countries are working with contractors to develop and test various AI-based technologies that can improve the use of drones, particularly target identification and tracking, and autonomous flight in challenging environments without the need for human operators to be involved. These technologies are still being developed, but in a number of cases they are already being tested.

Desired Capability
In the next 5–10 years, significant advances are likely in the integration of a range of AI technologies that will improve drone capabilities and provide real-time situational awareness to border guards, including 'full-motion video, automatic target detection and geolocation'.[73] Improvements are also likely in the ability of sUAS to operate fully autonomously through AI-enabled and computer-vision-based precision landing capability, which enables a sUAS to launch from and land on static as well as moving platforms, such as ground vehicles.[74] Finally, sUAS will be equipped with real-time onboard processing of imagery and video, as well as a drone neural network for object detection and classification.

Source: RAND Europe analysis.

Future efforts to develop an increased level of sUAS capability are likely to be constrained by various factors. Interviews with technology developers identified a particular challenge related

[70] Smith & Biggs (2018), Smith & Biggs (2019).

[71] WP1-INT03.

[72] Fussell (2019).

[73] Planck Aerosystems (2019).

[74] Planck Aerosystems (2020).

to the dominance of non-EU technology suppliers (e.g. cheap, off-the-shelf technologies from China) on the global market. This presents European end users with information-security and data-protection vulnerabilities.[75]

Several requirements and barriers for adoption are shared across heterogeneous and homogeneous sUAS capabilities. These include the lack of algorithmic transparency and limited ability to maintain insight into the training of an autonomous system, which often relies on Deep Learning. An additional constraint for current capability is limited scalability and lack of integration into common C2 platforms and related infrastructure. As such, future capability in sUAS technologies is likely to advance through the development of scalable solutions for multi-vehicle platforms and advanced infrastructure shared by multiple or all platforms in use by an end user.[76]

For further information on this technology area, see **Annex D.6.**

4.7. Predictive asset maintenance

As border security operations expand to include new technological systems, the complexity of such systems increases, as does the task of ensuring optimal operations and maintenance of the system. This applies, for example, to the maintenance of multi-vehicle UAS networks that are used for ground surveillance or for strengthening airspace awareness.[77] To facilitate this requirement, industry as well as public sector agencies are leveraging AI for predictive analytics solutions in relation to the maintenance of assets and technical systems, e.g. through identifying vulnerabilities, sub-optimal performance or potential technical failures.[78] Table 4.7 describes the current and desired levels of capability in relation to predictive asset maintenance.

[75] WP2-INT11.

[76] WP2-INT11.

[77] WP1-INT12

[78] WP1-INT12.

Table 4.7 Predictive asset maintenance – current and desired capability

Current Capability
AI that can predict patterns in logistics resupply and asset maintenance is already available, and is particularly prevalent within the logistics industry. The challenge at present is how this capability can be used within the context of border security. A number of relevant AI-based technologies and software systems are available to support it, but they require testing and adapting to the specific requirements of the EBCG.

Desired Capability
Border security authorities can expect that in the future, software will be available with AI and ML algorithms that can analyse data from various sensors and notify users about possible sub-optimal factors in border security operations and logistics workflows, such as factors that could lead to potential damage or failures. These technologies will be able to notify a human operator of potential risks, and decide whether to investigate or take action. From a logistics perspective, AI is likely to enable greater autonomy in predicting and automating the resupply and maintenance of border security assets, with limited human intervention or supervision (although this may still be required for safety or policy reasons).

Source: RAND Europe analysis.

Discussions at the external workshop identified predictive asset maintenance as one of the backend, enabling capabilities for border security end users. As end users are likely to have only limited direct engagement with the platform, there are limited personnel and training requirements associated with the platform. However, the availability of technical experts was identified as key for the initial stages of fielding and adapting the solution to suit the end user's requirements and the nature of the systems to be monitored, as well as ensuring access to historical, technical and sensor data. Access to such data might be constrained by organisational barriers (e.g. through legal constraints, as organisations might need access to data from sub-contractors), as well as lack of fit-for-purpose organisational procedures, financial and contractual models.[79]

For further information on this technology area, see **Annex D.7**.

4.8. Object recognition

Object detection and recognition systems are extensively utilised to perform functions including detection of suspicious packages, vehicles and cargo. While object detection and recognition systems are increasingly able to automatically detect and recognise objects through screening, algorithmic models that these systems use frequently rely on training, which often requires manual annotation of training data. This represents a highly time- and resource-intensive process,[80] exacerbated by the increasing reliance on 3D imaging. As such, AI technologies provide an opportunity to automate the data generation process as well as improve the accuracy of current object recognition systems. Table 4.8 describes the current and desired capability levels for AI-enabled object recognition.

[79] WP1-INT11.

[80] See e.g. Nowruzi et al. (2019).

Table 4.8 Object recognition – current and desired capability

Current Capability
Currently, several object detection and recognition systems are being used as part of border security operations. These systems are already able to detect and identify objects automatically as they pass through border security screening processes and sensors. However, these systems require a substantial amount of resource and time to train the models behind such systems before they can be reliably employed in border operations, including at BCPs. There is ongoing development to address the current challenges through the use of AI.

Desired Capability
In the near term, AI technologies will enable the automation of the data-generation process from which models can be trained, substantially reducing the currently resource-intensive process of training object identification models. AI is also expected to continue to improve the accuracy of existing object recognition systems, which will reduce the reliance on human intervention. Initially, it is expected that these developments will happen in visual and thermal object recognition, followed by radar object detection.[81] The creation of radar signatures is likely to increase object recognition accuracy and speed, when compared to cameras. The optimal desired capability is likely to arrive in the form of an integrated system that draws on multiple sensors.[82]

Source: RAND Europe analysis.

Detection and classification rates are the main indicators for evaluating the ability of a trained algorithm to accurately detect a signal at different distance ranges and recognise an object, e.g. a weapon, a UAS or a specific type of vehicle.[83] To further improve the algorithm's performance, some technology developers have built their own databases rather than using existing ones, tailoring the type of images that will be most useful to detect and classify objects.[84]

As discussed in Table 4.8, however, the pathway to future capability is likely to focus on the automation of synthetic data-generation for object recognition models through AI-enabled synthetic data generators.[85] As object recognition systems increasingly rely on 3D volumetric data, however, such capabilities could continue to rely on the ability of technology developers to access diverse and consistent data, which is frequently limited by information security restrictions, particularly in the security, defence and law enforcement contexts.[86] The performance of object recognition systems, even those based on advanced deep learning techniques, also remains limited in cluttered environments (e.g. environments with a wider variety of different objects).[87]

For further information on this technology area, see **Annex D.8.**

[81] WP2-INT01.

[82] WP2-INT01.

[83] WP2-INT01, WP2-INT02, WP2-INT03, WP2-INT04, WP2-INT10, WP2-INT11.

[84] WP2-INT01, WP2-INT10.

[85] Hjermitslev (2020), Baimukashev et al. (2019), WP1-INT01.

[86] WP1-INT01.

[87] Baimukashev et al. (2019).

4.9. Geospatial data analytics

While satellite imagery represents a valuable data source for strengthening operational awareness and threat detection capabilities, analysing satellite imagery has conventionally been a time-consuming task carried out by human analysts. The use of AI-based models offers the potential to automate the analysis of satellite imagery for object detection and recognition, which will reduce the cognitive burden of imagery analysts and speed up the process of analysing satellite imagery data. This could improve planning, logistics and intelligence-gathering in border security. Current and desired capability levels for this technology area are described in Table 4.9.

Table 4.9 Geospatial data analytics - current and desired capability

Current Capability
Currently, the process of analysing satellite imagery is a resource-intensive activity that relies heavily on human imagery analysts. These analysts require substantial training and experience built up over several years. Some developers are already using AI to advance the satellite imagery process, with ML tools rapidly emerging as the standard for analysing geospatial data.[88] Currently, there is some limited use of this capability in various functions, such as disaster relief and military operations. However, these developments have yet to achieve full automation and currently occur merely in support of the human analyst.
Desired Capability
This is an area where AI is expected to continue its rapid development over the next few years. In the near term, there is likely to be a transition period as AI models are employed more broadly for automated labelling and classification of geospatial data. Human analysts will increasingly be supported by AI and over time, the intent is that these models will be able to operate autonomously in the analysis of satellite imagery for automated target detection and object recognition. As well as this, Deep Learning methods will reduce the need for extensive algorithm training, which will speed up automated object recognition as AI models become capable of teaching themselves to identify characteristics of an object area or target.[89] The longer term aim for this type of AI is to enable the development of an integrated real-time tracking and threat identification system that can improve planning and logistics in border security, as well as other domains. Such systems will provide an integrated decision-support solution that provides real-time analysis of geospatial data streams to gain understanding of threats and decrease response times.[90]

Source: RAND Europe analysis.

Similar to other cognitive insight technologies, geospatial data analytics relies on the availability of large quantities of high-quality data of sufficient diversity and coherence. As such, barriers related to data access – including data protection and regulatory compliance concerns – represent the biggest potential barriers for adoption.[91] In terms of technological advances, the pathway to adoption of the desired capability levels in AI-enabled geospatial

[88] Wegner et al. (2018).

[89] Aerospace Technology (2019).

[90] European Commission (2020e).

[91] WP1-INT08.

data analytics is likely to focus on further improvements in the automation of data labelling and the generation of algorithmic training data. Given the ongoing advances with ML tools and techniques for the analysis of geospatial data, such improvements might be enabled by wider access to data and source code for relevant models, the design and maintenance of comprehensive benchmarking, and quantitative evaluation of tools and models on open-source data of sufficient size and variance.[92]

For further information on this technology area, see Annex D.9.

[92] Wegner et al. (2018).

5. Cross-cutting barriers and enablers for future AI adoption

While the pathway to adoption might differ for individual capabilities, there are a number of common cross-cutting barriers and enablers to adoption among the technology areas discussed in Chapter 4. Drawing on a synthesis of data captured throughout the first and second phases of the research, this chapter provides further insights into the steps required to integrate AI-based systems into border security (RQ4) by characterising these enablers and barriers.

5.1. Future adoption of AI-based systems could be constrained by various technological and non-technological barriers

The research team identified various technological and non-technological factors that cut across many of the identified AI technology areas as potential barriers of adoption. While no single barrier is likely to constitute an overwhelming constraint that could not be overcome, when taken together the various factors could pose significant challenges for end users and efforts to integrate AI-based systems in support of border security functions. This section outlines such barriers, summarised in Table 5.1.

Table 5.1 Summary of cross-cutting barriers for adoption

Category	Description	Section
Technological barriers	Technological barriers for future adoption could include algorithmic biases and other challenges caused by insufficient quantity or quality of data used for the development and training of AI models. This category also includes cybersecurity vulnerabilities and other technological barriers.	5.1.1
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, might discourage investment or limit end users' ability to support the development of AI-based systems.	5.1.2
Understanding and awareness of AI	Insufficient understanding of AI and lack of awareness concerning its potential in border security could challenge end users' ability to identify opportunities associated with AI.	5.1.3

Category	Description	Section
Organisational barriers	A lack of understanding and awareness of AI might be linked to wider organisational barriers, including organisational structures and cultures that might not allow for innovation and adaptation in response to technological advances, including in AI-based systems.	5.1.4
Skills and expertise	Skills shortages and lack of expertise could also limit the ability of end users to identify where and how AI might be best applied and address any requirements for adoption.	5.1.5
Access to relevant technologies	End users might face constraints in relation to access to relevant technologies and lack of European strategic autonomy in AI and other technologies.	5.1.6
Ethics and human rights	The proliferation of AI technologies and performance of AI algorithms might have ethical implications and carry risks for the safeguarding of human rights, such as individual privacy.	5.1.7
Data protection and regulatory barriers	Legal and regulatory barriers for adoption include regulatory uncertainty for technology developers and gaps in regulatory safeguards, such as data protection.	5.1.8

Source: RAND Europe analysis.

5.1.1. Algorithmic biases, cybersecurity and insufficient quantity and quality of data could form technical challenges for future adoption

While technological progress and advances in the efficiency and effectiveness of AI, as well as the increasing scope of the tasks that AI-based systems can perform, represent a key enabler for future adoption, there are several technological factors that are perceived as potential barriers. Algorithmic biases are one such concern, and are a key challenge for the future development of AI-based capabilities.[93] The challenges and risks associated with algorithmic biases arise from AI systems importing and amplifying biases in historical data that end users might be unaware of.[94] Such biases could result, for example, in facial recognition systems misidentifying people with darker skin tones at significantly higher rates than people with light skin tones, increasing the risk of profiling and discrimination.[95] These challenges are further amplified by the nature of AI and ML algorithms as 'black boxes' – i.e. the issue that decision-making processes of an AI or ML algorithm are often impossible to interpret and comprehend, even for programmers and developers of the technology, posing challenges of accountability, liability and end user trust in AI technologies.[96] This is particularly the case in relation to full AI-based systems that already include an AI embedded in hardware.[97]

Technical challenges associated with AI are often derive from insufficient quantity or quality of data being used for the development and training of an AI algorithm. Poor quality of data is

[93] WP 2-INT05, WP2-INT14.

[94] Wirtz et al. (2019), Misuraca & Noordt (2020).

[95] Simonite (2019), WP2-INT14.

[96] Bathee (2018), Craglia et al. (2018), Misuraca & Noordt (2020).

[97] WP2-INT 09.

likely to be directly reflected in the performance of an AI-based system and the outputs produced by an algorithm.[98] Although increasing quantities of data are gathered through advanced data collection tools and proliferating technologies such as IoT devices, data could be insufficiently diverse and lacking in certain aspects (e.g. lack of data on ethnic minorities and persons with darker skin in the case of facial recognition algorithms).[99] Data labelling represents a further challenge for the availability of data for AI development, particularly with regards to data labelling processes that still rely on the time- and human-resource-intensive manual work of technology companies.[100] Lastly, the high data requirements associated with AI development could present hidden costs for end users due to the need to establish and maintain relevant data storage and infrastructure for access and sharing.[101]

5.1.2. Perceptions of high direct and indirect financial costs and other commercial barriers could constrain end users from investing in AI technologies

Despite the falling costs of data storage and processing power, and the increasing economic viability of AI as a result of democratisation of AI technologies, cost-related and commercial barriers continue to represent a key concern for end users. Quantitative analysis of the nine technology case studies through the STREAM workshop – visualised in Figure 5.1 – corroborated this view, with the financial cost of AI-based systems being perceived on average as the greatest potential barrier to implementation. This includes both high direct costs associated with the implementation, operation and maintenance of AI-based systems, as well as indirect costs, such as providing financial incentives to technical experts due to the need to retain technical expertise.[102] Surveillance technologies such as heterogeneous robotic systems and fielded surveillance towers were perceived as facing the greatest cost-related barriers for adoption.

[98] WP2-INT15, WP2-INT14.

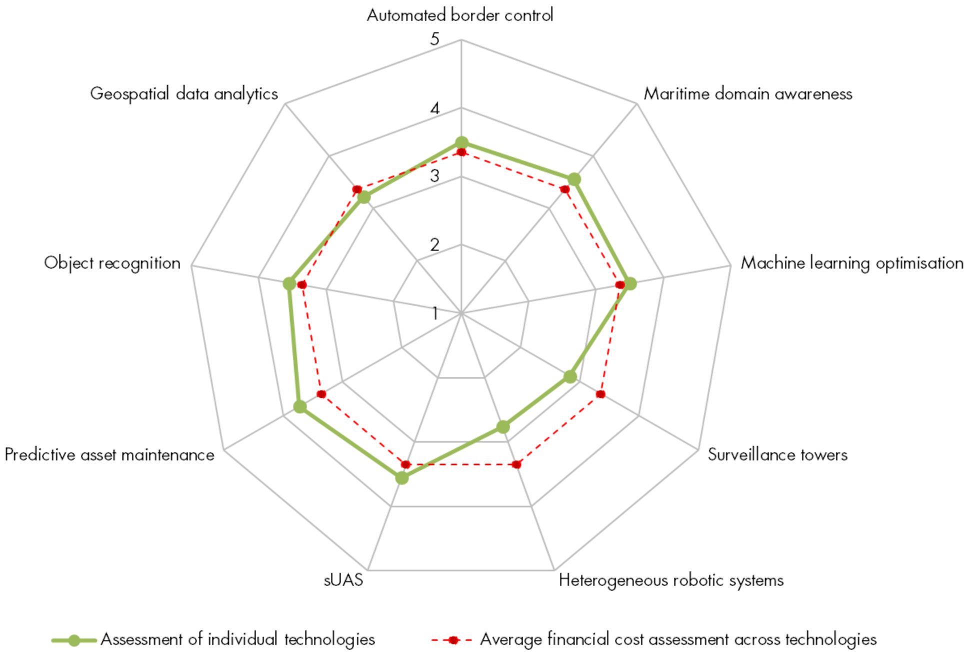
[99] WP2-INT14.

[100] WP2-INT07, WP2-INT09.

[101] WP2-INT14.

[102] S-INT2.

Figure 5.1 Assessment of selected AI technologies based on perceived financial costs[103]



Source: RAND Europe analysis of expert input.

Barriers for adoption related to the perceptions of cost might be further exacerbated by the nature of the AI technology market, which is considered to be more limited for border security end users than other technology markets, e.g. defence. The perception that the market for AI-based border security or law enforcement capabilities is limited could disincentivise investment from relevant stakeholders into further development of innovative border security technologies.[104] Furthermore, investment decisions by stakeholders such as border security and law enforcement authorities sometimes lack comprehensive assessments of investment opportunities, e.g. through cost-benefit and feasibility/market analyses, further impeding the interest or ability to invest in the development and adoption of AI-based systems that are relevant for the end user.[105]

The impact of COVID-19 on the AI market might further exacerbate these barriers, as technology adopters as well as developers might reduce spending on AI systems development or adopt more risk-averse perspectives on technology investment.[106] At the same time, the adoption of AI-based technologies in the context of the pandemic response could contribute to alleviating public uncertainties concerning the uses of AI in public policy, and thus incentivise broader adoption in the public sector.

[103] The figure scale ranges from 1 (insurmountable barriers – barriers could not be overcome) to 5 (negligible or no concern about barrier – barrier could be overcome with very minor or no change or disruption). As such, the higher a technology scored, the more feasible it was considered for adoption in light of the perceived financial costs. See Annex A for full description of the STREAM scores and criteria.

[104] WP2-INT09.

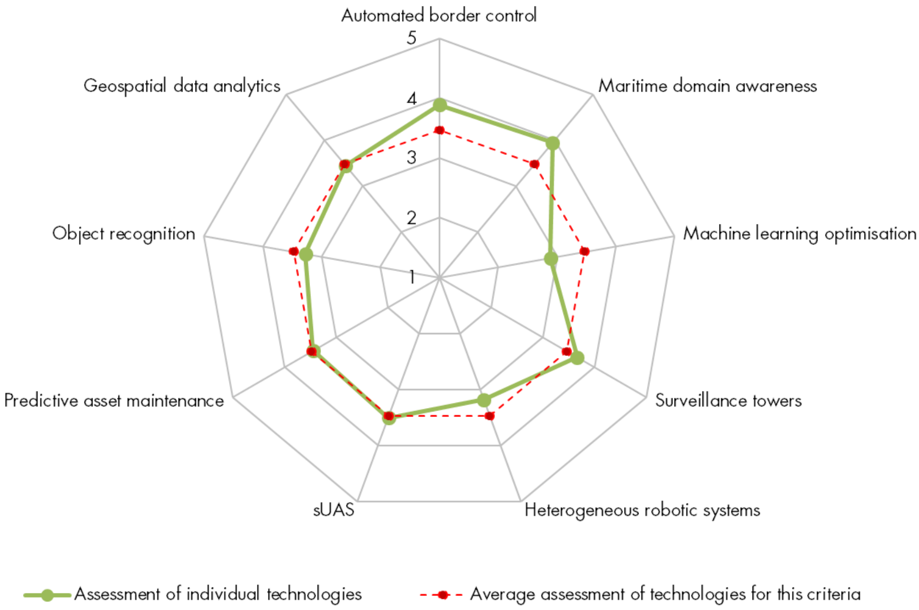
[105] WP2-INT09.

[106] Vernon et al (2020).

5.1.3. Insufficient understanding of AI and lack of awareness concerning its potential in border security could challenge end users' ability to identify opportunities associated with AI

Although there is a growing interest in the potential of AI in border security as well as the public sector more broadly, the adoption and use of AI seems to face barriers related to uncertainties, lack of understanding or awareness concerning AI as a technology and its potential benefits. Though there seems to be a high level of confidence among technology developers in the technology readiness of AI-based systems, the STREAM workshop analysis illustrated that uncertainties concerning the performance of AI technologies are still a relevant constraint for future adoption. Figure 5.2 provides an overview of expert assessments from the STREAM workshop in relation to the degree to which unfamiliarity with technology and uncertainty of performance represents a barrier for adoption for the nine selected technology areas.

Figure 5.2 Assessment of selected AI technologies based on unfamiliarity with technology and uncertainty of performance[107]



Source: RAND Europe analysis of expert input.

Interviews conducted by the research team highlighted that technology advances made in AI-based solutions are often overlooked due to overwhelming uncertainties or a lack of understanding concerning the nature of the technology.[108] This indicates a gap in understanding of the nature of advances in AI as well as its potential for public-sector end

[107] The figure scale ranges from 1 (insurmountable barriers – barriers could not be overcome) to 5 (negligible or no concern about barrier – barrier could be overcome with very minor or no change or disruption). As such, the higher a technology scored, the more feasible it was considered for adoption despite lack of familiarity with the technology and uncertainty regarding its performance. See Annex A for full description of the STREAM scores and criteria.

[108] WP1-INT03, WP1-INT04, WP1-INT07.

users, such as the border security community, between technology developers and end users. These insights corroborate findings of existing research, indicating an 'imbalance between the transformative potential and the effective adoption and use of AI solutions in government [...] in part due to the limited attention given to research on AI use in the public sector'.[109] Uncertainties regarding the performance of AI might be exacerbated by the general lack of sound empirical evidence that AI in fact achieves the desired results in public sector contexts.[110] Knowledge gaps between technology developers and end users could be related to wider structural constraints associated with organisational culture and lack of technical expertise. These issues are discussed in the following two sections.

5.1.4. Adoption of AI technologies in the public sector, including border security, could be constrained by organisational and bureaucratic barriers

Innovation in public sector organisations, including agencies dealing with security and defence, generally revolves around several key drivers:

- **External drivers**: this includes structural factors such as changes in the context in which organisations operate (e.g. fluctuations in migratory flows), the opportunities and challenges associated with technological change, and bureaucratic or political challenges posed by similar organisations.
- **Internal (organisational) drivers**: this includes both organisational culture – which encompasses the preferred practices and approaches that frame the organisation's strategic objectives – and the ability of organisational units to adapt to the tactical or operational challenges they encounter through practices such as training.

Public sector organisations have generally been found to struggle to keep up with the pace of AI adoption in the private sector, despite increasing interest in AI technologies and ongoing efforts to test AI applications and engage with technology developers.[111] Interviews conducted by the research team largely corroborated this view, linking the challenges for AI adoption in the public sector, including in relation to border security, to organisational factors. These factors include cultural resistance to technological innovation, bureaucratic inertia, the presence of governance 'gate keepers' and the nature of the organisational and operational structures of border security authorities, which are not sufficiently suited to effectively engage with technology developers and keep pace with the rate of technological innovation.[112]

While there might be myriad opportunities for Frontex to assume a leadership role in relation to adopting and piloting innovative technologies such as AI, challenges posed by organisational structure and culture were consistently identified by interviewees as a key barrier for this to come to fruition.[113] This includes a reduced number of organisational resources for adopting innovative technologies for automating or digitalising certain border

[109] Misuraca & Noordt (2020).

[110] Misuraca & Noordt (2020).

[111] Wirtz et al (2019).

[112] WP1-INT09.

[113] WP2-INT06, WP2-INT12.

security functions, as well as organisational structures that are perceived as ill-suited to allow the agency to adapt at sufficient pace with technological innovation.[114]

5.1.5. Skills shortages and lack of expertise could limit the ability of end users to determine where and how AI might be best applied, and identify the requirements for adoption of AI solutions

Interviews with technology developers indicated that in many cases the use of AI-based systems does not require extensive technical training, given the simplification of interfaces and enhanced usability. However, skills shortages and lack of technical expertise could present significant difficulties for end users in relation to the potential adoption of AI-based capabilities. Perspectives from stakeholders interviewed for this study corroborated existing research findings related to AI skills shortages and skills gaps between public sector agencies and technology developers, including industry and academia.[115]

Skills gaps or shortages can constrain end users in a number of ways. End users might lack relevant expertise to identify where AI based systems could be most useful in relation to existing processes and functions carried out by the organisation. For example, the use of AI for predictive analytics in the context of risk assessment and producing analyses of migration flows would necessitate staff with expertise in advanced statistics and data science to assess how and for which purposes AI should be utilised.[116]

Assessments of which technologies end users should invest in and which risks may be associated with any given system might also require the presence of a certain level of technical expertise within each organisation. As noted in Section 4.1.2, the need to attract and retain technical expertise in the public sector, including border security and law enforcement agencies, represents potential hidden costs for end users in the form of financial incentives for technical experts. End users should, however be able to identify and articulate potential shortages in skills and expertise within the organisation as well as human resource management.[117]

Lack of technical expertise presents a potential challenge for adoption not only within end user organisations, but also among policy-makers. Insufficient understanding of the technical nature of AI technologies and AI-based systems might be reflected in regulatory frameworks that are not fit for purpose, and constrain technology developers and end users equally. [118] Section 5.1.8 further discusses the challenges associated with legal and regulatory barriers.

5.1.6. End users could face constraints in relation to access to relevant technologies and lack of European strategic autonomy in AI and other technologies

AI-based systems might include a variety of software and hardware elements, the availability of which is not guaranteed for European suppliers. Interviews with technology experts as well as end users indicated that the adoption of AI-based capabilities by European stakeholders in

[114] WP2-INT06.

[115] See e.g. Mikhaylov et al. (2019), Misuraca & Noordt (2020).

[116] WP1-INT09.

[117] WP2-INT09.

[118] WP2-INT14.

border security and law enforcement could face significant constraints due to the dominance of foreign technological suppliers. Such challenges are already materialising, for example with US restrictions on the exportation of AI-based systems and the constraints this imposes on the ability of companies to supply full systems rather than individual components.[119] According to technology developers, the entry of cheaper, off-the-shelf hardware from Chinese developers also present challenges for European technology developers who cannot compete with the price of technological products originating from China.[120]

The above-described challenges relate closely to the wider notion of European strategic autonomy, particularly in relation to digital technologies, such as AI. The concept of strategic autonomy broadly refers to 'the capacity of a political entity to pursue its own course in international relations'.[121] Several key elements in ensuring strategic autonomy in relation to the uptake of emerging technologies – such as AI – among European businesses and the public sector include the strengthening of the European industrial and technological base and its ability to fulfil the end users' technology needs; ensuring resilience of critical infrastructure and ICT systems; and safeguarding the capacity for independent decision- and policy-making, including through the development of a homogenous policy approach and wider promotion of EU ethical standards.[122] Recent EU policy initiatives, including the European Digital Strategy, have increasingly acknowledged the need to foster European strategic autonomy or 'technological sovereignty' in these various aspects.[123]

The use of non-EU AI-based systems could also pose risks in terms of information and cybersecurity for European end users.[124] Some AI-based systems rely on components and hardware systems developed outside the EU, for example in China, causing concern among European technology developers about data being shared with foreign authorities when using non-EU-developed AI-based capabilities. This is prompting increasing adoption of cybersecurity tools – such as virtual private networks (VPNs) and firewalls – to strengthen data protection.[125] The United States, also at the forefront of AI-based technologies, has been willing to develop partnerships with western Balkan states, prompting similar data-sharing concerns.[126]

5.1.7. The proliferation of AI technologies and performance of AI algorithms might have negative implications for ethics and protection of human rights

As noted in Section 4.1.1, faults in AI systems – such as algorithmic biases – present a number of ethical challenges for end users. The research team identified the following challenges related to the ethics of AI and human rights protection:

[119] WP1-INT08.

[120] WP1-INT08.

[121] EPSC (2019).

[122] EPSC (2019), EOS (2019).

[123] Lippert et al. (2019), European Commission (2020c).

[124] WP2-INT11.

[125] WP2-INT11.

[126] WP2-INT15.

- Algorithmic bias could pose a risk to **guarantees of non-discrimination**, e.g. through racial profiling in the context of border control. Uses of emerging technologies with potential algorithmic biases could also pose risks to the safeguarding of neutrality as a core humanitarian principle, e.g. in the context of refugee and migrant registration processes.[127]
- The proliferation of AI technologies could challenge **data protections and the right to privacy**, particularly in relation to AI-enabled biometric scanning, facial recognition and surveillance technologies.[128]
- The reliance of border security staff on algorithmic decision-making could result in **violations of human dignity**, e.g. through undetected errors leading to the deprivation of persons of their liberty.[129]
- Faults in the performance of AI algorithms might, conversely, also lead to the **entry of dangerous persons, placing others at risk.**[130]

With increasing recognition of the need to ensure comprehensive governance of AI, existing research identifies a number of potential steps to address implications of AI for ethics and human rights protections.[131] This includes strong data protection safeguards, incentivising transparency and comprehensive privacy regulation, and emphasising human rights protections within AI governance through mechanisms such as public procurement and standardisation.[132] Through public procurement, end users and public authorities could help to ensure compliance of technology developers with human rights safeguards in the process of designing, developing and deploying AI technologies. Similarly, common technical standards and protocols – as witnessed, e.g. in the case of Internet protocol-based standardisation – could be introduced.[133]

The ethical challenges and potential implications of increasing uses of AI for human rights protection are at the core of concerns related to public perception and acceptance of AI. Public acceptance of the uses of AI in border security and law enforcement might increase as AI technologies proliferate and their benefits are more clearly demonstrated for individual citizens. However, further engagement from end users and public authorities with the general public – through public messaging and transparent communication of the purposes of AI – would be beneficial in addressing potential challenges with public acceptance. Such messaging might aid transparency regarding the purposes of AI usage by emphasising compliance with key data protection frameworks (e.g. the GDPR) and other human rights safeguards.[134]

[127] Jacobsen (2015).

[128] WP2-INT14.

[129] WP2-INT09.

[130] Beduschi (2020).

[131] WP2-INT06.

[132] Beduschi (2020), WP2-INT07, WP2-INT09.

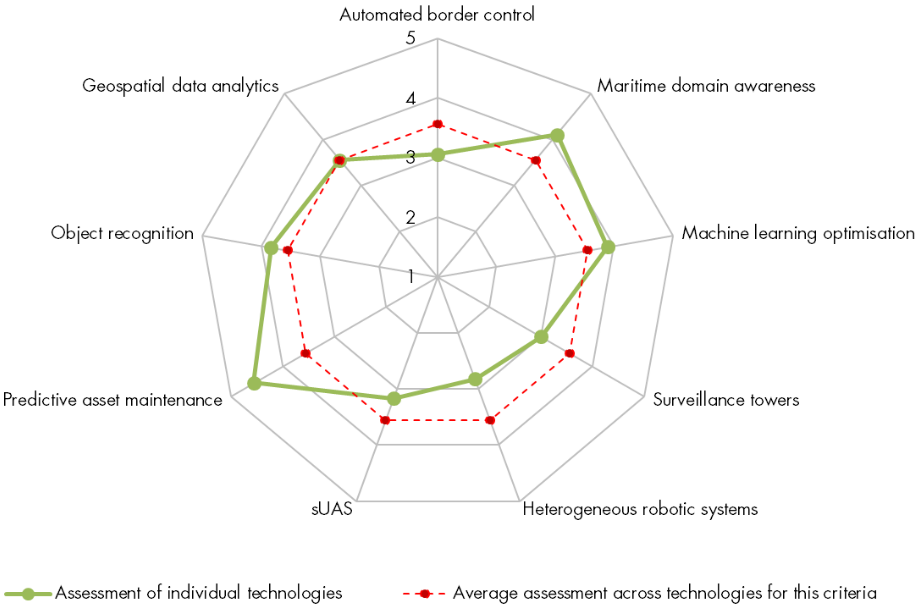
[133] Beduschi (2020).

[134] WP2-INT05, WP2-INT15.

5.1.8. Legal and regulatory barriers for adoption include regulatory uncertainty for technology developers and gaps in regulatory safeguards, such as data protection

In light of the ethical challenges and potential risks for human rights protections associated with AI, technology developers might be required to comply with strict data protection frameworks and other regulations. The EU context could represent a particularly challenging regulatory context for the operation of AI-based capabilities, for example in facial recognition and AI-enabled checkpoint operations, as general data regulations strictly prohibit profiling of individuals.[135] Regulatory barriers and data protection requirements are thus perceived as a potential challenge by developers and end users alike – Figure 5.3 captures the assessments made by external experts in relation to the nine technology areas discussed in **Chapters 3** and **4.**

Figure 5.3 Assessment of selected AI technologies based on data protection requirements and regulatory barriers[136]



Source: RAND Europe analysis of expert input.

Discussions at the STREAM workshop noted that the extent to which data protection represents a barrier to implementation for AI-based capabilities should be evaluated in the context of the type of data captured. This is particularly relevant to considering the barriers to implementation of AI-based border surveillance capabilities. For example, systems

[135] S-INT1.

[136] The figure scale ranges from 1 (insurmountable barriers – barriers could not be overcome) to 5 (negligible or no concern about barrier – barrier could be overcome with very minor or no change or disruption). As such, the higher a technology scored, the more feasible it was considered for adoption in light of relevant data protection requirements and other regulatory barriers. See Annex A for full description of the STREAM scores and criteria.

performing object detection might have different data protection requirements from systems performing facial recognition, a capability which requires more personal data to be processed.

From the perspective of technology developers, regulatory uncertainty and heterogeneity of the European regulatory context also represent significant constraints. It is also recognised by end users that regulations are slower to develop and mature than technology developments, therefore it is likely that mismatches will arise between the AI-based capabilities developed and the regulations by which they will need to abide.[137] Legislations and regulations appear to be the barriers that technology developers will need to overcome to ensure the use of their AI-based solution.[138]

5.2. Technological advances and various non-technological factors could also serve as enablers for future adoption of AI-based capabilities

The research team identified 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. These are summarised in Table 5.2 and described in further detail below.

Table 5.2 Summary of cross-cutting enablers for future adoption

Category	Description	Section
Technological enablers	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).	5.2.1
Iterative development	Improvements in the performance of AI-based systems are likely to rely on iterative development and innovative approaches to acquisition and testing of AI-based capabilities.	5.2.2
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) and improving usability of AI-based capabilities could incentivise adoption by end users.	5.2.3
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.	5.2.4
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, and strengthening European strategic autonomy in AI.	5.2.5

[137] WP2-INT12.

[138] WP2-INT10.

Public awareness and acceptance	Increasing use of AI in the provision of key services could contribute to the value proposition of AI vis-à-vis the public, and thus increase public acceptance and awareness of the benefits of AI technology.	5.2.6

Source: RAND Europe analysis.

5.2.1. Future adoption of AI-based capabilities could be enabled by technological advances in AI as well as in 'adjacent' technologies

Technological advances are a crucial enabler for further adoption of AI by border security end users and the future landscape of AI-based capabilities in border security. This includes both advances in AI technologies (e.g. different AI techniques) as well as 'adjacent' technologies:

- **Autonomous systems**: Improvements in propulsion, vision and navigation capabilities through lower cost advanced sensors, radars and vision systems could contribute to advances in AI-enabled autonomous systems, such as sUAS. Developments in the ability of sUAS to navigate, take off and land in narrow and enclosed spaces might contribute to surveillance as well as search and rescue operations.[139]
- **Blockchain**: Integration of advanced blockchain technologies into unmanned and autonomous systems could contribute to auditability and control of AI-based capabilities such as sUAS, i.e. improving the end users' ability to develop a complete picture of all the unmanned capabilities being used and their location.[140]
- **Biometric data capture**: future tools for facial recognition and person identification might include the integration of thermal imaging and AI technology to enable facial recognition in the dark,[141] feature extraction models using convolutional neural networks (CNN) for facial recognition from partial images (e.g. when only half a face is visible),[142] and transforming infra-red imagery into a form that is closer to visible light images, improving the accuracy of facial recognition in surveillance capabilities.[143]
- **Cognitive robotics**: Emerging S&T trends indicate possible advancements in the use of AI-enabled robotics, including autonomous open-ended learning capabilities that would enable robots to link multiple senses,[144] learn from their experiences and adapt to new tasks with little manual programming input,[145] or autonomously interact and cooperate with other robots through an intrinsic 'social drive' capability.[146]

Future advances in AI are expected to increase the range of tasks an AI-based system can perform, as well as the accuracy and speed at which it can perform such tasks. While interviews with technology experts in many cases indicated that there is already a significant degree of confidence in the performance of current AI-based systems, further advances in the

[139] See e.g. Ackerman (2019), University of Zurich & EPFL (2018).

[140] WP1-INT12.

[141] Ernst (2018).

[142] University of Bradford (2019).

[143] WP2-INT10.

[144] Etherington (2019).

[145] Goal-robots.eu (2020).

[146] Jacques et al. (2019).

effectiveness and efficiency of AI are likely to enable improvements in capabilities – such as biometric scanning and facial recognition – in which experts have clearly identified potential improvements.[147] Data collection through S&T horizon scanning identified a number of emerging trends that might contribute to such improvements:

- Development of **advanced sensory computing**, which could enable memory-like capabilities in robotic systems.[148]
- Development of **novel types of neural networks**, which could enhance the speed and efficiency of neural network-based applications for facial and voice recognition.[149]
- Wider integration of AI into physical hardware, which could create more advanced solutions such as **intelligent sensor networks** and **data storage solutions**.

Though interviews with technology developers confirmed that increasing the abilities of AI-based systems, including autonomous systems, was desirable and a key enabler, it was also emphasised that technological advances and innovation should be cognisant and aligned with desired ethical standards of AI. Further advances in the abilities and sophistication of AI-based systems is thus not expected to categorically lead to the development of fully autonomous capabilities that do not involve some level of human supervision. As such, future advances in AI technology and emergence of key future technological enablers are likely to take place within the bounds of determined ethical standards.

5.2.2. Improvements in the performance of AI-based systems are likely to rely on iterative development and innovative approaches to acquisition and testing

Iterative development of AI systems encompasses early fielding and continual testing and improvement of an AI-based capability based on the end user's requirements and the given operational context. Despite the prevailing uncertainties among end users with regard to the technology readiness of AI-based systems, iterative development has been emphasised as a key enabler to allow end users to fully utilise AI technologies.[150]

Though iterative development and other procurement approaches that permit flexibility within the adoption process might be preferred by technology developers, there is equal recognition of two potential risks or challenges for end users. Firstly, end users could face strong organisational constraints due to the requirement to adapt to traditional procurement approaches. As discussed in Section 5.1.4, these organisational, structural and cultural barriers might result in risk aversion and resistance to wider organisational change, or the inability to adapt processes such as procurement models to technological change. Incentivising inter-stakeholder dialogue between border security authorities and technology developers could alleviate such constraints as concerns from end users are better communicated vis-à-vis industry and vice versa.

[147] WP2-INT10.

[148] Oak Ridge National Laboratory (2018).

[149] Hecht (2019).

[150] WP1-INT04.

Secondly, end users might need to consider the potential harmful impacts of experimental deployment of new and emerging technologies to humanitarian subjects. Existing research documents various risks associated with experimental uses of new technologies in humanitarian settings, including the exposure of already vulnerable subjects to potential technology failures.[151] In border security and management contexts, this could present additional risks to migrant and refugee safety, or compromise the ability of authorities to safeguard the humanitarian principle of neutrality in refugee registration processes.[152]

5.2.3. Simplification of interfaces and increasing usability of AI-based capabilities could incentivise adoption by end users

As AI-based capabilities for current or potential future use in border security are becoming technologically advanced, improvements are also being made in their usability to enable end users to utilise capabilities without extensive levels of technical knowledge or expertise. Interviews with technology developers highlighted that while a lack of technical expertise within public sector organisations might impede the adoption of AI due to misunderstanding of its potential contributions, the use of AI-based capabilities themselves does not require extensive technical knowledge of the systems' features.[153]

The development of highly portable and user-friendly systems currently represents one of the main focuses for technology developers. Small tablets are, for example, used in connection with radar systems to enable users to enter data into a system automatically rather than typing it in manually.[154] This and other advances in designing and developing **human-machine teaming (HMT)** technologies are likely to constitute core enablers for future uses of AI in various operational contexts, such as extensive engagement between border patrol and autonomous vehicles.[155] In such contexts, HMT may improve not only the usability of AI-based capabilities but also provide safeguards against technology failures or accidents involving autonomous systems.

5.2.4. Commercialisation and democratisation of AI will likely further contribute to decreasing costs of AI-based capabilities, increasing the economic viability of AI adoption for end users

As already noted in **Chapter 2**, the democratisation of AI presents a significant driver and enabler for AI adoption by an increasing number and variety of end users, including in the public sector and areas such as border security and law enforcement. This trend includes a large number of AI development efforts taking place as open-source projects, facilitating 'rapid

[151] Jacobsen (2015).

[152] Jacobsen (2015).

[153] WP2-INT04, WP2-INT10.

[154] WP2-INT02.

[155] Recent advances include the improvement of brain-computer interfaces (BCIs) in the amount and quality of data being processed and transferred between the human and the machine. Improvements in BCIs have allowed for significant advances in HMT applications in security and defence, including systems with one operator remotely controlling a drone swarm. Source: Binnedijk et al. (2020), Tucker (2018).

diffusion and adoption by academia and organisation at all scales'.[156] The proliferation of open-source, cutting-edge technologies facilitates the emergence of an ecosystem of 'free or affordable, easy to use, plug and play services built on top of these open source frameworks which can be used by organisations that lack the resources and skill sets to develop in-house solutions'.[157]

The increasing number of commercial actors, including technology start-ups, presents benefits for stakeholders through increasing competitiveness and economic viability of AI-based systems. As noted by one interviewee, commercial products, including AI technologies, are generally believed to bring significant cost-efficiency to end users within the public sector.[158]

5.2.5. EU initiatives could further incentivise research into the uses of AI and strengthen European strategic autonomy

Interest in the uses of AI in border security has increased in parallel to wider EU efforts to incentivise responsible innovation and development of AI – including human-centric AI technologies – for the EU and its Member States. The European Digital Strategy and the corresponding Digital Europe Programme are the most recent examples of these efforts, which focus on incentivising investment and wider deployment of digital technologies, including AI, in European society and the economy.[159] The emerging European interest in AI presents a number of opportunities for the future adoption of AI technologies by end users in the border security realm:

- EU initiatives might provide incentives for further development of human-security-centric technologies and solutions that address the risks and challenges associated with humanitarian technologies.[160] This could be accompanied by corresponding efforts to **develop or strengthen relevant ethical standards and principles for AI governance**, including human rights protections. This could include the development of procurement and standardization frameworks discussed in Section 5.1.8.
- Increasing interest in the use of AI for security and defence applications could incentivise efforts to develop **European strategic autonomy** in AI-based capabilities for security applications. As discussed in Section 5.1.6, efforts to strengthen European strategic autonomy might include various elements, including increasing the resilience of EU technology supply chains and strengthening Europe's position in the global market on AI.[161]
- EU-funded research and development programmes could receive more funding, thus **strengthening the evidence base surrounding the potential uses of AI for border security as well as the impacts of AI in various contexts and operational environments**. This might

[156] Dasgupta & Wendler (2019).

[157] Dasgupta & Wendler (2019).

[158] WP1-INT09.

[159] European Commission (2020c).

[160] Jacobsen (2015).

[161] EOS (2019). Section 5.1.6 discusses the challenges associated with the dominance of non-EU technology suppliers for end users.

assist in addressing prevailing knowledge gaps and associated uncertainties among end users concerning the risks and challenges associated with the use of AI technologies.

- Strengthening the EU legal and regulatory framework on AI could address regulatory uncertainties among technology developers as well as enable access for industry to wider markets rather than individual Member States.

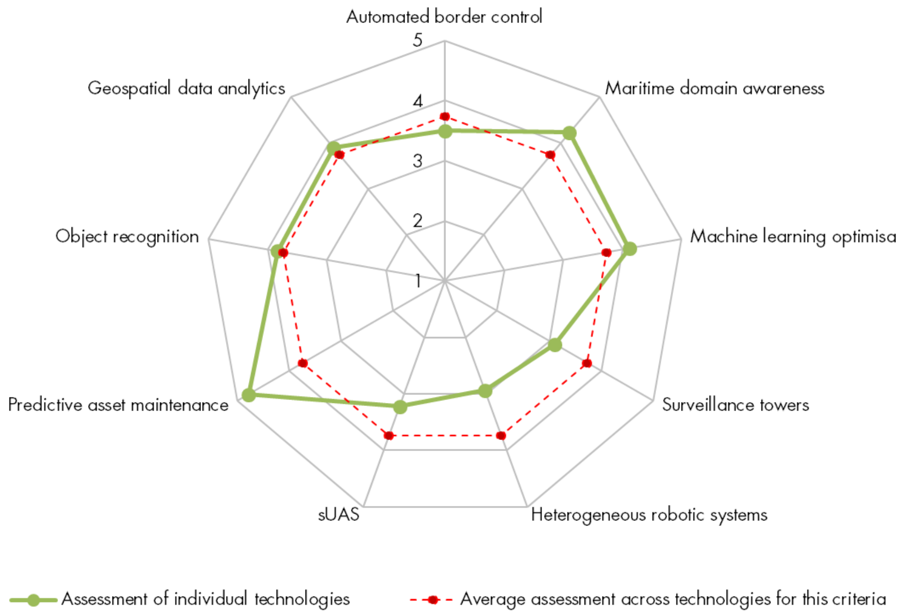
5.2.6. Increasing use of AI to provide services of demonstrable benefit to the general public could improve public awareness and acceptance of AI

Though public awareness of AI technology seems to be increasing, knowledge concerning its purposes, nature and limitations generally remains limited.[162] Levels of public and political acceptance of the uses of AI technologies in border security and law enforcement frequently define the context in which end users make decisions about the adoption of AI-based capabilities. Assessments at the external workshop, shown in Figure 5.4, indicated that public and political acceptance of AI could represent a potential barrier of adoption particularly for surveillance capabilities or systems that citizens might be expected to directly interact with, e.g. ABC gates. This corroborates existing research showing that public concerns regarding the privacy implications of facial recognition technology, lack of trust in the private sector's use of such technology, as well as normalisation of AI-enabled surveillance continue to define public debate concerning the uses of AI.[163]

[162] Ada Lovelace Institute (2019).

[163] Ada Lovelace Institute (2019).

Figure 5.4 Assessment of selected AI technologies based on insufficient public or political acceptance[164]



Source: RAND Europe analysis of expert input.

As AI-based capabilities become more widely used, however, workshop participants also estimated that challenges associated with public or political acceptance are likely to decrease. This might be due to growing familiarity with the technology among the public as well as increasing awareness concerning its benefits, for example reduced waiting times at BCPs. Overall, increasing uses of AI in areas of demonstrable public benefit are thus likely to enable improved value proposition of AI technologies vis-à-vis the general public. Such value proposition should go hand in hand with incentivising informed public debate concerning the impacts of increased uses of AI to further address public concerns and lack of trust in AI and its applications in border security and law enforcement.

[164] The figure scale ranges from 1 (insurmountable barriers – barriers could not be overcome) to 5 (negligible or no concern about barrier – barrier could be overcome with very minor or no change or disruption.). As such, the higher a technology scored, the more feasible it was considered for adoption in light of levels of public or political acceptance. See Annex A for full description of the STREAM scores and criteria.

6. Conclusions and implications for Frontex

This concluding chapter summarises the findings presented in this report and offers key insights and conclusions concerning the current and future landscape of AI-based capabilities in border security, as well as implications for the EBCG. On the basis of these insights, this chapter also includes a set of possible recommendations for Frontex as it considers the risks and opportunities associated with AI technologies in border security.

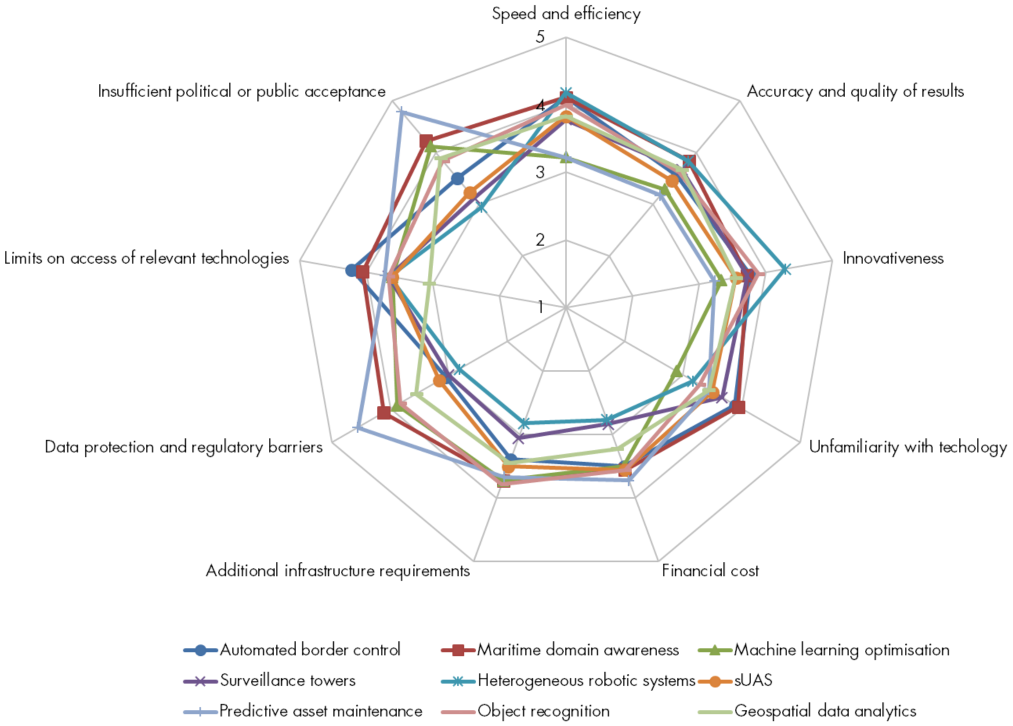
6.1. The evolving landscape of AI-based capabilities in border security provides various risks and benefits for end users to consider

This study has sought to capture the scope and nature of the landscape of AI-based capabilities in border security, including current uses of AI by border security authorities and other relevant stakeholder groups (e.g. defence and law enforcement), as well as emerging trends that could lead to new areas of AI applicability. The study identified a wide range of current and potential future uses of AI in relation to five key border security functions, namely: i) situation awareness & assessment; ii) information management; iii) communication; iv) detection, identification & authentication; and v) training and exercise. For each function, the research team identified different technology areas and capability areas within which AI might be utilised. In consultation with Frontex, nine technology areas were selected for further examination of the potential contributions of, challenges to and requirements for their adoption in European border security.

The evolving landscape of AI-based border security capabilities spans not only the various border security functions and capability areas, but also includes the various types of AI-based systems (i.e. automation, cognitive insight and cognitive engagement technologies) and AI tools and methods (e.g. NLP and ML). This indicates an increasing diversity in the types of AI tools and methods that border security end users could utilise to enhance existing ways of performing border security functions.

The assessment of nine technology areas through the external workshop indicated that AI is generally believed to bring at least an incremental improvement to the existing ways in which border security functions are conducted. This includes 'front-end' capabilities that end users directly utilise (e.g. ABC gates and surveillance systems), as well as 'back-end' capabilities that enable border security functions (e.g. automated machine learning). Figure 6.1 captures the results of initial expert workshop-based assessments of the performance of the selected technology areas against a range of impact and implementation criteria.

Figure 6.1 Summary assessment of selected AI technology areas[165]



Source: RAND Europe analysis of expert input.

Despite the potential positive impact associated with AI-based capabilities, particularly on the efficiency with which border security functions are carried out, end users need to consider a range of barriers to adoption, including technological and non-technological challenges and barriers. Decisions to invest in the development or adoption of a given AI-based capability thus necessarily revolve around the trade-off between the expected benefit and the investments needed to address potential barriers and adoption requirements. Table 6.1 illustrates the three highest scored technology areas in relation to the expected impact, feasibility of implementation, and combination thereof, as assessed by experts and stakeholders during the external workshop.

[165] The higher a technology is scored on the criteria, the more positive its assessment was in relation to potential impact and feasibility of implementation. For impact criteria (speed and efficiency, accuracy and quality of results, and innovativeness), the scale ranges from 1 (negative impact – reduction in capability compared to current practices) to 5 (ground-breaking impact – paradigm shift in capability compared to current practices). For feasibility of implementation criteria, the scale ranges from 1 (insurmountable barriers – barriers could not be overcome) to 5 (negligible or no concern about barrier – barrier could be overcome with very minor or no change or disruption). See Annex A for full description of the STREAM scores and criteria.

Table 6.1 Top 3 technology areas according to impact, implementation and combined assessments

Top 3 combined	Top 3 impact	Top 3 implementation
1. Maritime domain awareness	1. Heterogeneous robotic systems control	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.

6.2. Addressing key baseline gaps could facilitate wider uptake of AI technologies within the EBCG

As discussed in **Chapter 5** in conducting risk and benefit analyses to inform investment decisions, end users might need to consider a range of technological and non-technological factors that could enable or constrain the pathway to adoption. Three factors emerge as baseline gaps, posing wide-ranging constraints on the uptake of AI-based capabilities in border security that merit more in-depth consideration:

- **Knowledge gaps between stakeholder groups**: There remains significant uncertainty among end users. In contrast, technology developers are generally confident in the technology readiness of existing capabilities and the performance of AI at its current levels of sophistication. Perspectives gathered from end users and technology developers indicate a significant knowledge gap concerning the potential utility of AI technologies, its readiness as well as potential risks and challenges for end users.
- **Organisational, structural and cultural barriers, and gaps in skills and expertise**: The public sector in general and border security authorities specifically might face constraints due to the lack of sufficient technical expertise and gaps in skills relevant to innovation and adoption of emerging technologies. Such constraints interact with broader organisational constraints embedded in organisational structure and culture, shaping preferences and practices that might not be fit for purpose in relation to the adoption of rapidly developing technologies, such as AI.
- **Gaps in the evidence base**: The current evidence base regarding the impacts of AI includes predominantly technical assessments of the performance of AI algorithms in controlled environments, rather than real operational contexts. As such, conclusive evidence concerning the impacts of the uses of AI in the provision of public services, including border security and law enforcement, remains limited.[166]

The enablers and barriers identified in **Chapter 5** are cross-cutting not only in relation to individual capabilities and technology areas, but also in relation to the stakeholder groups. This highlights that the nature of the evolving landscape of AI-based capabilities in border security revolves around a **broader innovation ecosystem**, rather than a linear technology developer–technology end user dynamic. Beyond industry (technology developers) and the

[166] Misuraca & Noordt (2020).

EBCG (end users), this ecosystem includes: EU agencies and EU policy- and decision-making bodies, which could define the regulatory context and provide incentives for technology development (e.g. through fostering ethical and trust-worthy AI); academia, which plays a crucial role in providing the knowledge and evidence base for AI development as well as adoption; and civil society, which formulates concerns regarding the ethics of AI and impacts of expanded uses of AI on individual privacy.

6.3. The study findings could incentivise further consideration of Frontex' role in future AI uptake in border security

Frontex' mandate to support research and innovation and contribute to the development of the EU's Integrated Border Management should incentivise further consideration of what role Frontex as an agency could play in shaping the future landscape of AI-based capabilities in European border security. Previous RAND Europe research identified a number of potential roles for organisations in the context of innovation and adoption of emerging technologies for a wider range of stakeholder groups.[167] Frontex should consider these roles as an initial step towards facilitating the uptake of AI-based capabilities among the EBCG. Table 6.2 provides an overview of these roles and their possible actualisation in relation to the future adoption of AI in border security.

Table 6.2 Opportunities for Frontex' role in future adoption of AI in border security

Role	Relation to AI-based capabilities in border security
Identifying future requirements and opportunities for the use of AI in border security	The pace of innovation and technological advances indicates the value of coordinated and holistic mapping of future requirements and opportunities associated with AI and AI-based systems in border security, e.g. in the form of an in-house or commissioned horizon-scanning capability.
Strengthening the knowledge and evidence base and providing thought leadership	The lack of comprehensive evaluations of the impacts of AI in the public sector is a significant constraint for future adoption efforts. Contributions in this context might include commissioning further research on the opportunities, risks and challenges associated with AI-based capabilities in border security or synthesising existing research from across the EU Member States and beyond, providing input for ongoing policy and regulation development at the national and EU levels. This could include research in relation to the ethics and human rights implications of AI to inform the development of pan-European standards for AI governance and human rights safeguards.

[167] Cox et al. (2017).

Facilitating information and knowledge exchange	Further to direct contributions to the knowledge and evidence base in relation to AI in border security, Frontex could incentivise information provision and knowledge exchange concerning the opportunities, risks and challenges associated with AI-based capabilities in border security. This could take the form of gathering and sharing lessons learned or developing training and education materials/programmes for end users within Member States. As such, Frontex could take a role in developing or facilitating public awareness campaigns or educating policy- and decision-makers concerning the benefits and risks associated with AI in the context of border security and similar contexts (e.g. policing and law enforcement).
Facilitating coordination between different stakeholder groups	The above-described presence of knowledge gaps, including among end users and industry as well as policymakers and industry, may incentivise Frontex to consider taking the role of an 'honest broker' between different stakeholder groups, including end users from EU Member States, the European Commission, industry, academia and other stakeholders.
Incentivising innovation	Frontex could support the development of national capabilities or multi-national/EU projects through sponsoring or hosting technology demonstrators, e.g. of AI-based systems of potential use in border security. This might serve to strengthen awareness among end users concerning the potential uses of AI in border security, as well as facilitate iterative improvement of AI-based systems.
Facilitating access to funding	More indirectly, initiatives to strengthen the knowledge and evidence base concerning the impacts of AI could also take the form of direct R&D funding, facilitating access to relevant funding instruments that are relevant for border security research and innovation.

Source: RAND Europe analysis.

Insights gathered from Frontex-based interviewees throughout this study indicated that various organisational limitations and capacity gaps might constrain Frontex' ability to take a more active role in defining the evolving AI-based capabilities landscape. As such, operationalising the opportunities for Frontex' role described in Table 6.2 could rely on several enabling factors that might require further change:

- **Organisational structure and culture**: organisational and cultural change was consistently highlighted by interviewees as a key barrier for future uses of AI in border security. This indicates that identifying and addressing specific key procedural and behavioural limitations could provide a significant improvement to existing levels of capacity within Frontex.
- **Skills and expertise**: enhancing familiarity with emerging technologies was identified as a key element in strengthening organisational capacity to identify current and emerging opportunities, as well as risks associated with emerging technologies such as AI. The development of relevant education and training initiatives and tools could address such gaps and constraints imposed on organisational capacity.
- **Human and financial resources**: in connection with the lack of certain types of expertise, particularly technical expertise, innovation pursued by public sector organisations is likely to be constrained by limited human and financial resources. Identifying a

selected number of strategic priority areas and defining a clear vision of Frontex' role in shaping the evolving landscape of AI-based border security capabilities could enable wider impact to be achieved – despite the presence of resource constraints – by avoiding duplication and orientating resources towards a coherent set of strategic goals.

These high-level recommendations are somewhat limited by the data available to the study team, i.e. they draw on open-source data and insights provided by a limited number of stakeholders and Frontex experts. However, Frontex should consider a more comprehensive and in-depth assessment of the opportunities regarding its role in facilitating or enabling the adoption pathways outlined in **Chapter 4** and **Annex D**, and identify resources and capacities that could be used or further strengthened. There are several options available to Frontex for addressing each of these three areas, with Table 6.3 outlining potential corresponding actions.

Table 6.3 Potential actions for addressing the key challenges to the wider adoption of AI-based capabilities in European border security

Category	Potential Actions
Organisational structure and culture	Conduct a survey of border security staff to better understand the cultural barriers to adopting AI-based technologies.
	Implement a thorough review of current procedures for adopting new technology and use this to inform in-depth revisions of appropriate procedures where possible.
	Undertake basic awareness-training for staff targeted at improving their understanding of the awareness of AI-based technologies and the role and benefits they could have within border security.
	Encourage broader involvement from border security guards in the trialling and testing of AI-based technologies, and widely publicise the results to demonstrate transparency in the way AI technology is being developed and might benefit border security.
	Establish transparent systems to review and develop organisational structures in light of the potential adoption of AI-based technology.
Skills and expertise	Undertake a Training Needs Analysis (TNA) of European border guards to understand the current skillset and what training and development might be required.
	Understand the most cost-effective balance between training current border security guards and recruiting personnel with additional specialist skills in relevant aspects of AI and related technologies.
	Develop a training plan based on the TNA that addresses short-, medium- and long-term training needs across Europe, and provides a cost-effective solution to delivering training to all who require it through a collective programme.

	Where possible, conduct a targeted recruitment campaign to 'buy-in' appropriate skills and expertise where it is more effective to do so than training existing personnel.
Human and financial resources	Identify strategic priority areas for investment in AI-based technology across Europe to understand the options for combining limited resources.
	Develop collaborative plans for developing the desired capabilities in each of these strategic priority areas, focusing on making effective use of collective resources and avoiding duplication of effort wherever possible.

Source: RAND Europe analysis.

6.4. Opportunities for further research

In addition to the considerations given to Frontex in the previous section, the research team also identified a number of opportunities for further research oriented towards prevailing data gaps concerning the opportunities and challenges associated with AI-based systems in border security, including:

- Longitudinal evaluations of case studies of AI-based capabilities in border security currently in use by end users would be beneficial to strengthen the evidence base concerning the long-term impact of AI capabilities in border security.
- Survey- or interview-based research focused on mapping perspectives from end users (in the EBCG) to develop more granular insights on the areas of most utility for EU border security, as well as the relevant national barriers for adoptions.
- More extensive empirical analysis of successful and failed deployments of AI-based capabilities or similar new and emerging technologies by the EBCG in different operational contexts. This could be carried out through comparative case-study analysis or qualitative evaluations to identify lessons learned and any potential unintended consequences of the use of emerging technologies in different operational contexts.
- Collection of lessons learned regarding the adaptation of procurement models and the use of iterative development approaches in acquiring new capabilities in areas such as policing and law enforcement.
- Comprehensive mapping of AI technology suppliers to identify the extent to which end users might face constraints with regards to the access of AI technologies.

Annex A. Methodology

A.1. WP1 – Review of AI-based technologies and their application in border security

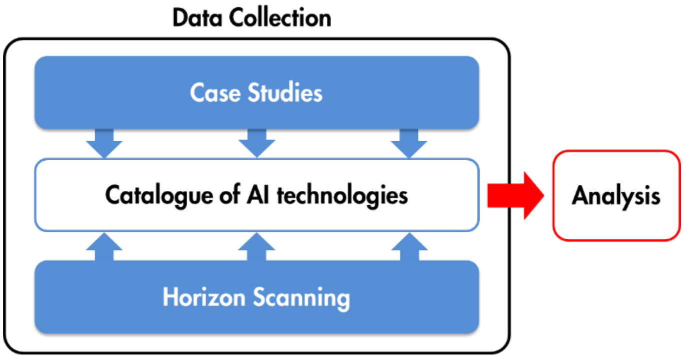
This section outlines the research approach applied for WP1, which consisted of two tasks:

- **Task 1.1: Data collection** through case study analysis and horizon scanning, and
- **Task 1.2: Analysis** in the form of initial assessment and shortlisting of technologies, and in-depth analysis through a STREAM workshop.

A.1.1. Task 1.1 – Data Collection

The research approach for WP1 included a combination of top-down and bottom-up data collection, as visualised in Figure 6.1 Summary of WP1 data collection approach

Figure 6.1 Summary of WP1 data collection approach



Source: RAND Europe

Desk research and scoping interviews

The study team carried out case study analysis as the top-down, application-driven component of the data-collection strategy. The case study analysis aimed at identifying relevant existing AI-based technologies with direct or potential application in border security through an analysis of existing R&D programmes or commercial products in the military, border security and public safety sectors.

The research team adopted a two-pronged approach to identify an initial longlist of AI technologies, consisting of desk research and initial scoping interviews with research and innovation experts at Frontex. The desk research was carried out through online searches using key-word Google searches and targeted online searches on EU funded research or R&D

programmes funded by national governments in the EU and the US. In parallel, the research team conducted six scoping interviews with Frontex experts.[168] Findings from the desk research and the scoping interviews were combined into a longlist of potential case studies that included 43 technologies. These were catalogued in the form of a short description of the technology, its application to border security, geographic location and an assessment of the availability of information.[169]

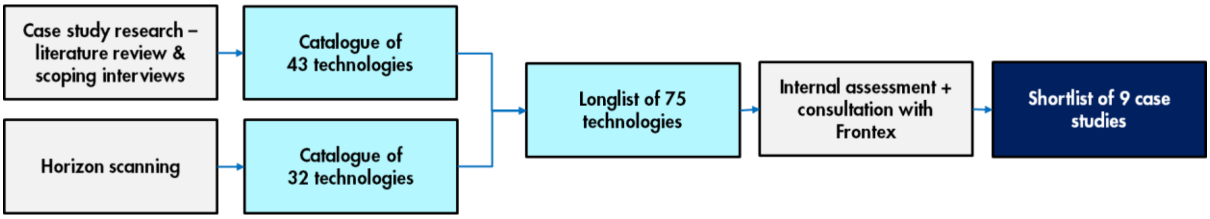
Horizon scanning

To complement the case study research, the research team carried out horizon scanning to collect data through a bottom-up technology-driven approach. This aimed to complement the case study research by identifying relevant technologies that represent emerging areas of interest for border security that have not yet been applied in the context of border security. The horizon scanning consisted of targeted key-word searches of the RAND Europe Horizon Scanning database. The research team identified 32 relevant items, which were catalogued similarly to the technologies identified through case study research, including a short description of the item and its potential application to border security.[170]

Shortlisting of technologies and additional case study data collection

The research team consulted with the Frontex project team to select a shortlist of AI technologies to be examined through case study analysis. From the longlist of 43 technologies identified through case study research and 32 S&T items identified through horizon scanning, nine technology case studies were selected – in consultation with the Frontex project team – for more in-depth review on the basis of their potential impact and availability of information. The selection also sought to ensure the inclusion of case studies that could impact different border security functions. Figure 6. summarises the shortlisting approach.

Figure 6.2 Summary of the technology shortlist approach


Case study research – literature review & scoping interviews
Horizon scanning
Catalogue of 43 technologies
Catalogue of 32 technologies
Longlist of 75 technologies
Internal assessment + consultation with Frontex
Shortlist of 9 case studies

Source: RAND Europe

The research team carried out further data collection for the nine shortlisted case studies through a targeted document review and up to three key informant interviews per case study. The targeted document review focused on reviewing open source information about the technology, including information provided through both the project or company website, and from news sources. The interviews included consultations with both developers and end users.

[168] A full list of interviews conducted in WP1 is included in Table 6..

[169] A longlist of technologies identified in this research is included in Annex C.

[170] A longlist of technologies identified in this research is included in Annex C.

In total, the research team carried out 13 interviews, with some interviews including multiple experts.[171]

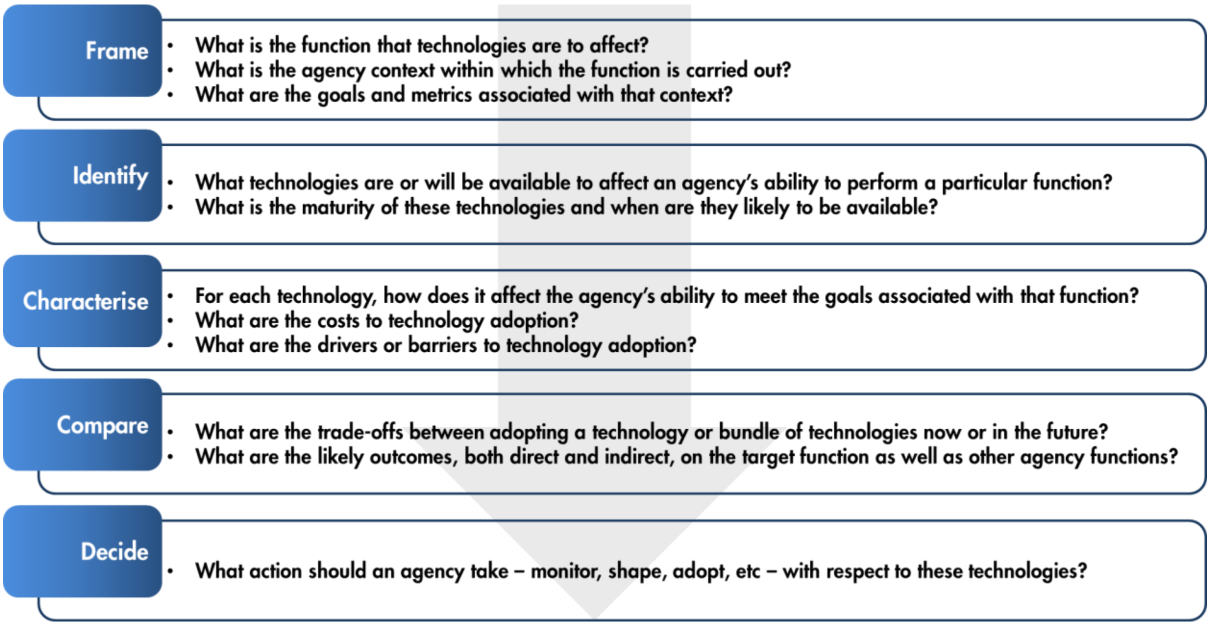
Data collected through case study interviews and targeted document review was synthesised and consolidated through a structured technology brief template, which covered the following issues:

- Title of the AI solution;
- Description of the intended purpose of the AI solution;
- Summary of development history;
- Country (or countries) where the AI solution is applied;
- Description of identified enablers;
- Description of identified barriers; and
- Indication of cost (where available).

A.1.2. Task 1.2 – Analysis

The research team conducted in-depth analysis of the shortlisted technologies through a modified version of the Systematic Technology Reconnaissance, Evaluation and Adoption Method (STREAM). Figure 6. provides a high-level overview of the STREAM methodology.

Figure 6.3 High-level overview of the STREAM methodology



Frame
- What is the function that technologies are to affect?
- What is the agency context within which the function is carried out?
- What are the goals and metrics associated with that context?

Identify
- What technologies are or will be available to affect an agency's ability to perform a particular function?
- What is the maturity of these technologies and when are they likely to be available?

Characterise
- For each technology, how does it affect the agency's ability to meet the goals associated with that function?
- What are the costs to technology adoption?
- What are the drivers or barriers to technology adoption?

Compare
- What are the trade-offs between adopting a technology or bundle of technologies now or in the future?
- What are the likely outcomes, both direct and indirect, on the target function as well as other agency functions?

Decide
- What action should an agency take – monitor, shape, adopt, etc – with respect to these technologies?

Source: RAND Europe

Through this structured approach, STREAM aims to:

- Frame the problem or situation;
- Systematically identify new technologies that might be relevant;
- Assess their potential application to agency-relevant functions;

[171] A full list of these interviews is included in Table 6..

- Evaluate different technologies based on technical, organisational, commercial, regulatory and other barriers, and costs to implementation; and,
- Inform decision making on whether to ignore, monitor or proactively shape and adopt different technologies, allowing a portfolio approach that balances technology risk across a mix of high probability and low probability/high impact investments.

Stakeholders participating at the workshop[172] were asked to provide their expert inputs to a number of structured discussions considering a series of questions about the possible impact and barriers to implementation of the nine selected technology case studies on border security functions. This included a process wherein workshop participants scored selected technology case studies according to:

- **Impact**: Potential impact of individual technologies on functions and desired outcomes in specified capability areas; and
- **Feasibility of implementation**: Potential technical, organisational, commercial, regulatory and other barriers to implementation that could impact the feasibility of adoption of individual technologies.

Definitions for the criteria are described Table 6. (impact) and Table 6. (feasibility of implementation).

Table 6.1 STREAM scoring criteria for impact

If the technology were matured and implemented, what is likely to be the impact on:
• **Speed and efficiency**: ability to perform border security functions more efficiently, e.g. faster or with less resources?
• **Accuracy and quality of results**: ability to perform border security functions more effectively, e.g. with higher quality and accuracy of results?
• **Innovativeness**: ability to carry out a border security function through novel approaches using AI technology?

Source: RAND Europe.

For each technology, participants were asked to allocate the following scores (1–5):

1. **Negative impact** – reduction in capability compared to current practices;
2. **No impact** – negligible or no difference in capability from current practices;
3. **Moderate positive impact** – minor improvement in capability over current practices;
4. **Substantial positive impact** – significant improvement in capability over current practices; or

[172] See further below for more detail concerning how participants were identified, and Table 6. for a full list of workshop participants.

5. **Ground-breaking impact** – paradigm shift in capability compared to current practices (i.e. enables entirely novel approach).

Table 6.2 STREAM scoring criteria for feasibility of implementation

How much of a concern is the following a barrier to implementation?
• **Unfamiliarity with technology or uncertainty concerning actual performance**
• **Financial cost to implement, operate and maintain technology**
• **Additional infrastructure requirements** (e.g. connectivity, computational power, systems, networks, etc.)
• **Data protection and other regulatory barriers**
• **Limits on access to relevant technologies** (e.g. export control restrictions, lack of European suppliers, etc.)
• **Insufficient political or public acceptance** (e.g. ethical and human rights concerns)

Source: RAND Europe.

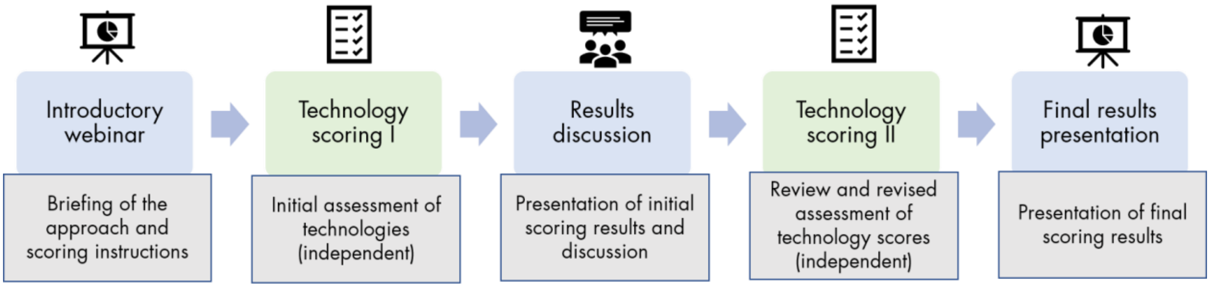
For each technology, participants were asked to allocate the following scores (1–5):

1. **Insurmountable barriers** – barriers could not be overcome;
2. **Grave concern** – barriers unlikely to be overcome without major societal, organisational or economic change or disruption;
3. **Significant concern** – barrier could be overcome with significant change or disruption;
4. **Minor concern** – barriers could be overcome with only minor change or disruption; or
5. **Negligible or no concern** – barriers could be overcome with very minor or no change or disruption.

The workshop included 20 participants, excluding the RAND Europe research team, including experts from Frontex, other agencies and organisations working within or in fields relevant to border security, as well as research and industry experts.[173] Workshop participants were selected and invited by Frontex after we provided a profile for the necessary expertise. Due to the restrictions imposed by the ongoing COVID-19 pandemic, the STREAM workshop, which was originally to take place as a physical one-day workshop, was adapted into a series of virtual webinars and independent scoring exercises carried out by the participants. Figure 6. summarises the adapted structure of the STREAM workshop, which was held in May 2020.

[173] A full list of workshop participants can be found in Table 6.

Figure 6.4 Adapted STREAM workshop structure


Introductory webinar
Briefing of the approach and scoring instructions
Technology scoring I
Initial assessment of technologies (independent)
Results discussion
Presentation of initial scoring results and discussion
Technology scoring II
Review and revised assessment of technology scores (independent)
Final results presentation
Presentation of final scoring results

Source: RAND Europe.

The first round of technology scoring (Technology scoring I) included 18 sets of scoring results, with an additional one set of results and two revised sets of scoring included for analysis of the second round of technology scoring (Technology scoring II).

A.2. WP2 – Roadmapping AI-based technologies for application in border security

Technology roadmaps are used to understand and define the pathway between an existing and desired level of capability. More specifically, technology roadmaps seek to understand the following questions:

1. Where are we now? (the current state of the capability);
2. Where do we want to go? (the future state if new technologies are adopted); and
3. How do we get there? (the pathway to adopting technologies, including risks to implementation).

The technology roadmaps developed in WP2 built on the list of nine AI technology case studies identified during WP1. The roadmaps focused on providing a description of the potential capabilities that could be implemented in border security, examples of technology use cases, the underlying technology required to achieve the stated capabilities, and the necessary actions to successfully adopt AI technologies.

In order to develop accurate, reliable and detailed technology implementation roadmaps, RAND Europe adopted a three-stage approach:

- **Task 2.1: Internal workshop** to develop initial roadmaps based on WP1;
- **Task 2.2: Data collection** through use case mapping and interviews with technology and border security experts; and
- **Task 2.3: Finalisation of roadmaps** through desk-based research and roadmap validation.

This approach built on previous roadmapping approaches that have been used by RAND Europe, but adapted the methodology from the traditional focus on technology development towards an emphasis on technology implementation and adoption. This approach was formulated in line with continued consultation between RAND Europe and Frontex to maximise utility of the analysis. The following sections provide further detail on the methods used in this phase of the study (WP2).

A.2.1. Task 2.1 – Internal RAND Workshop

A common risk when planning the potential adoption of new technology solutions is the tendency or preference to focus on technologies themselves, without fully linking them to the overarching effect on capabilities one wants to achieve. In this context, the risk of selecting the wrong solution because it appeared technologically better than others is quite high. To mitigate these risks, it was important that the analysis for technology roadmaps was done at the capability level, to understand how individual technologies can, or cannot, be linked to specific technological requirements, which in turn enable new capabilities or improve existing ones. Thus, this first step of roadmapping aimed to build on the nine case studies identified in WP1 and, through an internal RAND workshop, develop nine outline roadmaps that describe:

- The desired capability or effect to be achieved;
- The current state of such capability;
- The underlying technologies required to deliver the desired capability;
- Examples of technology use cases, already in use or in development, and which partially or fully address the capability need;
- How the capability might be adopted by European border security organisations; and
- Any dependencies on other factors, assumptions, barriers and enablers from a European perspective (e.g. logistics, training, infrastructure, laws, regulations and policies).

This task provided a framework to ensure coherence across the nine case studies and identify any gaps in the current understanding of how different technologies might be adopted for European border security.

A.2.2. Task 2.2 – Data collection

To develop the roadmaps based on the nine shortlisted AI-based capabilities during WP1, the study team synthesised data gathered during the first phase of the study and conducted additional data collection through interviews with border security and technology experts, as well as desk research to address prevailing data gaps.

Key informant interviews

To gather additional data for the technology adoption roadmaps, the research team carried out 15 semi-structured interviews with technology and border security experts. This included:

- **6 interviews with AI technology experts**: interviews with technology experts were conducted to enhance the evidence base concerning the nature of underlying technologies within the identified use cases and technology areas, identify emerging technology trends and potential future improvements in technology readiness, and identify perspectives of the technology developer on the opportunities and challenges associated with the adoption of AI-based capabilities in border security. AI technology expert interviewees were identified through Google searches and desk research oriented at identifying illustrative use cases for each of the nine technology areas. The research team sought to interview at least one technology expert per technology area and address any potential gaps through triangulation of open-source data with insights gathered during WP1 interviews with technology developers. As such, for each of the roadmaps at least one technology expert was interviewed.

- **9 interviews with border security experts**: the research team consulted with nine border security experts from Frontex in order to enhance the evidence base concerning requirements and potential barriers to adoption of AI-based capabilities in border security, and to gather insights concerning potential priorities for Frontex and end users from the EU Member States. Border security experts were identified in consultation with Frontex and through recommendations by other interviewees.

Interviews were held by telephone and video conference given the restrictions imposed by the COVID-19 outbreak. RAND Europe conducted semi-structured interviews that combined specific questions to explore enablers, challenges and barriers to the implementation of AI-based system for border security with follow-up questions prompted by the discussion with interviewees.

A.2.3. Task 2.3 – Finalising roadmaps

RAND Europe carried out internal analysis and synthesis in order to consolidate the findings of Task 2.1 and Task 2.2 and generate a more refined version of the nine roadmaps. The research team conducted additional targeted desk research through Google searches and review of relevant academic and grey literature to fill prevailing data gaps or triangulate and validate emerging findings. This task resulted in the production of the nine technology roadmaps discussed in **Chapter 4** and **Annex D**.

A.3. List of experts and stakeholders consulted

As noted in the description of the methodologies used in WP1 and WP2, the research team conducted a number of stakeholder and expert consultations in the form of key informant interviews and an external workshop. Table 6.3 List of experts and stakeholdersprovides a list of all experts and stakeholders engaged in all phases of the research.

Table 6.3 List of experts and stakeholders

Interview	Date	Reference
Scoping interviews		
S-INT1	2 December 2019	Anonymous, Frontex
S-INT2	2 December 2019	Anonymous, Frontex
S-INT3	2 December 2019	Anonymous, Frontex
S-INT4	2 December 2019	Anonymous, Frontex
S-INT5	2 December 2019	Anonymous, Frontex
S-INT6	2 December 2019	Anonymous, Frontex
WP1 case study interviews		
WP1-INT01	12 March 2020	Anonymous

WP1-INT02	16 March 2020	Anonymous, Rey Juan Carlos University
WP1-INT03	19 March 2020	Anonymous
WP1-INT04	19 March 2020	Anonymous, Anduril Industries
WP1-INT05	19 March 2020	Anonymous
WP1-INT06	24 March 2020	Anonymous, Centre for Research and Technology Hellas (CERTH)
WP1-INT07	25 March 2020	Anonymous
WP1-INT08	26 March 2020	Anonymous
WP1-INT09	31 March 2020	Anonymous, US Customs and Border Patrol (CBP) Innovation Team
WP1-INT10	1 April 2020	Anonymous, Szekely Family & Co
WP1-INT11	2 April 2020	Anonymous, SparkCogntion
WP1-INT12	10 April 2020	Anonymous
WP1-INT13	12 April 2020	Anonymous
WP2 roadmapping interviews		
WP2-INT01	9 July 2020	Anonymous, Athena security
WP2-INT02	13 July 2020	Anonymous, Echodyne
WP2-INT03	15 July 2020	Anonymous, Fleetrange
WP2-INT04	16 July 2020	Anonymous, Tel Aviv University
WP2-INT05	17 July 2020	Anonymous
WP2-INT06	17 July 2020	Anonymous
WP2-INT07	21 July 2020	Anonymous, Frontex
WP2-INT08	22 July 2020	Anonymous, Frontex
WP2-INT09	22 July 2020	Anonymous, Frontex
WP2-INT10	1 August 2020	Anonymous, T3K-Forensics
WP2-INT11	30 July 2020	Anonymous, Aeorum
WP2-INT12	31 July 2020	Anonymous, Frontex
WP2-INT13	31 July 2020	Anonymous
WP2-INT14	31 July 2020	Anonymous
WP2-INT15	3 August 2020	Anonymous, Frontex

STREAM Workshop		
Workshop	14–28 May 2020	Anonymous, European Defence Agency
Workshop	14–28 May 2020	Anonymous, Kozminski University
Workshop	14–28 May 2020	Anonymous, EU SatCen
Workshop	14–28 May 2020	Anonymous, eu-LISA
Workshop	14–28 May 2020	Anonymous, Information Technology Institute
Workshop	14–28 May 2020	Anonymous, Information Technology Institute
Workshop	14–28 May 2020	Anonymous, Fraunhofer Gesselschaft
Workshop	14–28 May 2020	Anonymous, Satways
Workshop	14–28 May 2020	Anonymous, NATO Centre for Maritime Research and Experimentation
Workshop	14–28 May 2020	Anonymous, Joint Research Centre
Workshop	14–28 May 2020	Anonymous, Joint Research Centre
Workshop	14–28 May 2020	Anonymous, eu-LISA
Workshop	14–28 May 2020	Anonymous, Frontex
Workshop	14–28 May 2020	Anonymous, Frontex
Workshop	14–28 May 2020	Anonymous, Frontex
Workshop	14–28 May 2020	Anonymous, Frontex
Workshop	14–28 May 2020	Anonymous, Frontex
Workshop	14–28 May 2020	Anonymous, Frontex
Workshop	14–28 May 2020	Anonymous, Frontex
Workshop	14–28 May 2020	Anonymous, Frontex
Workshop	14–28 May 2020	Anonymous, Frontex

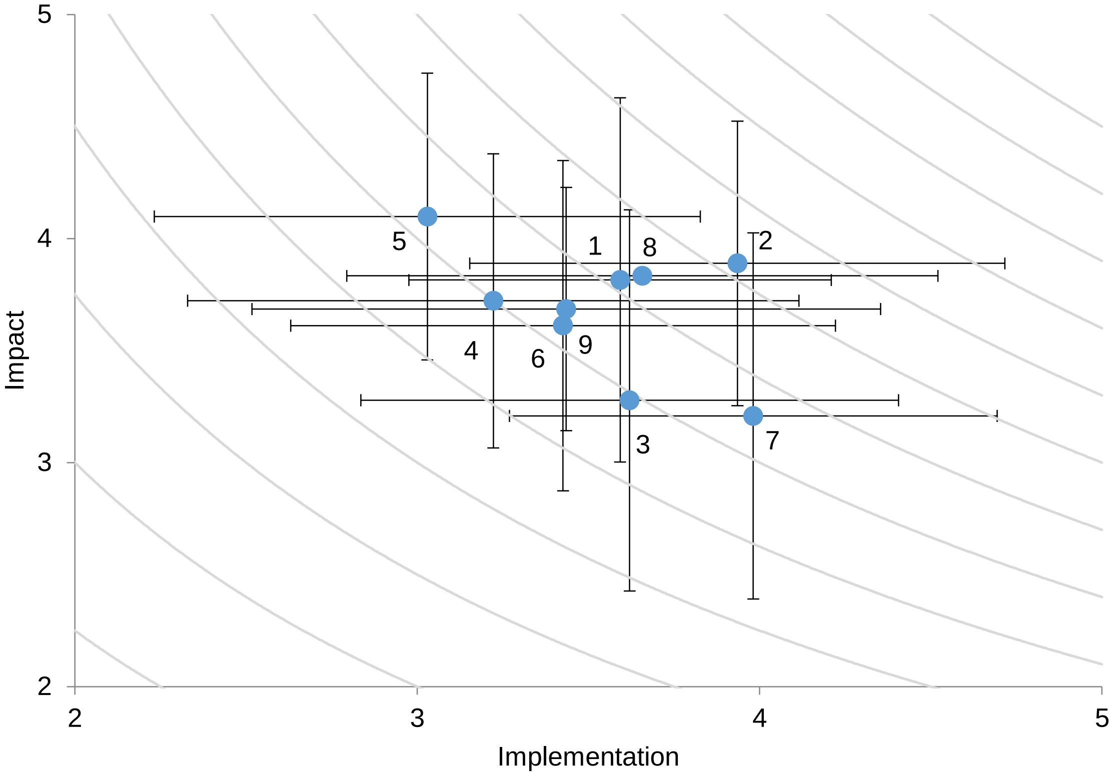
Annex B. Summary of quantitative findings from the STREAM workshop

The STREAM workshop centred on the assessment of the nine technology areas described in **Chapters 3** and **4** against a range of impact and implementation criteria. Figure 6. illustrates the distribution of aggregated scores for all nine technology areas in terms of their average impact and feasibility of implementation. Labels for each technology area are provided in Table 6..

Table 6.1 Figure key – numbered technology area labels

#	Case Study	#	Case Study
1	Automated border control (ABC4EU)	6	sUAS (Planck Aerosystems sUAS)
2	Maritime domain awareness (Marint)	7	Predictive asset maintenance (SparkPredict)
3	Machine learning optimisation (AutoML)	8	Object recognition (Synthetik object recognition)
4	Surveillance towers (Sentry Towers)	9	Geospatial data analytics (GATR)
5	Heterogeneous robotic systems control (Roborder)		

Figure 6.1 Aggregated scores for all nine technology areas with error bars (+- standard deviation)[174]



Source: RAND Europe.

Three notable insights can be observed from Figure 6.:

- The **average scores are clustered between scores 3 and 4 for both impact and implementation.** This is often observed in STREAM workshops, as more extreme scores are rarely assigned by participants, and average scores are more common particularly in the case of technologies that participants might not be fully familiar with. In terms of impact, most technologies received an average score of between 3.5 and 4, indicating that AI-based technologies are generally believed to have at least some positive – and often a significantly positive – impact on the ability of end users to perform border security functions.
- Despite the middle clustering of technologies both in terms of impact and feasibility of implementation, **more variation in average scores can be observed with regards to feasibility of implementation.** This indicates more variation in the assessment of barriers to implementation, and that there is perhaps more confidence regarding the impact of AI-based capabilities in border security rather than the various potential barriers to implementation.
- The error bars, representing standard deviation (SD) values, are relatively large compared to the differences between some of the technologies. This could suggest **considerable discrepancies in the scoring among workshop participants**, as some

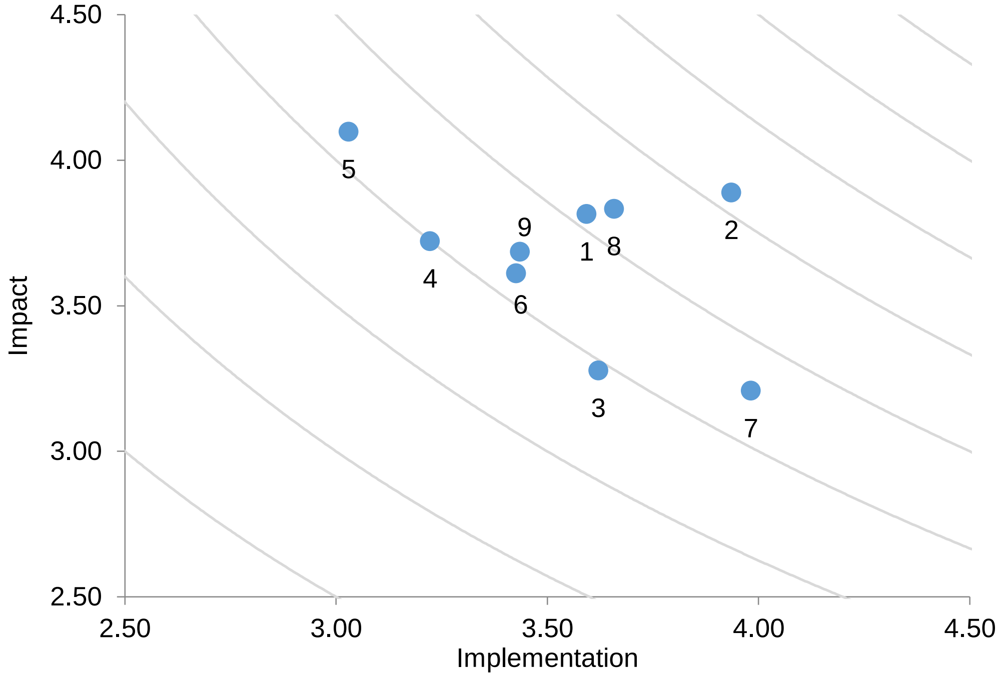
[174] The grey lines are mathematical lines of constant that are used for visual display purposes.

technologies received widely disparate scores despite the central clustering of the scoring overall. However, the wide error bars might also be a product of the relatively small sample size.

Figure B.2 provides a zoomed-in version of the figure above through adjusted scales on the X and Y axis and removal of the error bars. This provides a clearer illustration of the scoring differences between each of the technology areas.

Error! Reference source not found.

Figure 6.2 Comparison of impact and implementation scores for all nine technology areas (adjusted scales)[175]



Source: RAND Europe.

Figure B.2 portrays a number of high-level findings concerning the perceived differences in impact and feasibility of implementation of the technology areas:

- **Maritime domain awareness received the highest combined score for both impact and feasibility of implementation**, as visualised by the numbered label in the furthest top right corner on the graph. This indicates that the technology area scored comparatively highly in terms of both impact and feasibility of implementation, and thus is expected to have a relatively high impact on the performance of border security functions with relatively low barriers to implementation. The technology scored second highest on both average impact and feasibility of implementation.

[175] The grey lines are mathematical lines of constant that are used for visual display purposes.

- **Heterogeneous robotic systems received the highest aggregate impact score** and was thus perceived to have the greatest potential impact on border security functions among the technology areas. However, as can be seen in Figure 2.2, the technology was also seen as having relatively high barriers to implementation. A similar result is found in the case of surveillance towers, which also received a relatively high score in impact and low score on feasibility of implementation. This finding indicates that while AI-enabled border surveillance systems are seen as having high impact on border security functions, particularly in terms of speed and efficiency with which border security functions are performed, there are a number of important barriers to implementation, particularly financial costs and regulatory barriers, including data protection requirements.
- In contrast to technologies with relatively high impact and implementation scores, **some technology areas received relatively low impact scores but were also assessed as having relatively low barriers to implementation**. This includes in particular, predictive asset maintenance and machine learning optimisation Workshop discussions indicated that this might due to the nature of these technology areas as 'enabling' technologies. As such, their impact in border security might be more indirect.

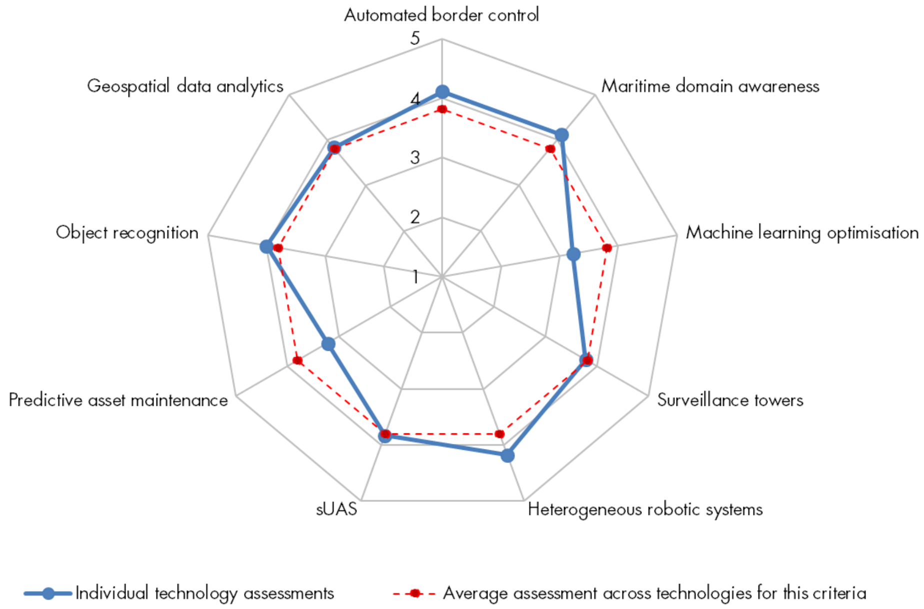
Table 6.3 Overview of top 3 technology case studies

Top 3 combined	Top 3 impact	Top 3 implementation
1. Maritime domain awareness	1. Heterogeneous robotic systems control	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.

Further analysis of the scoring carried out by the research team revealed additional observations concerning the potential impact and feasibility of implementation of AI-based capabilities in border security more broadly. On average, **the scoring indicates AI-based capabilities are expected to have the greatest impact on the speed and efficiency with which border security functions can be carried out**. Figure 6. provides an overview of the scores of the different case studies for the speed and efficiency criteria. The second-greatest impact was assessed in innovativeness, with slightly lower impact in accuracy and quality of results. This could indicate that there is more confidence in the positive contribution of AI to make border security functions more efficient by saving financial and human resources, rather than the ability of AI to qualitatively improve the results of processes underpinning such functions (e.g. in their accuracy).

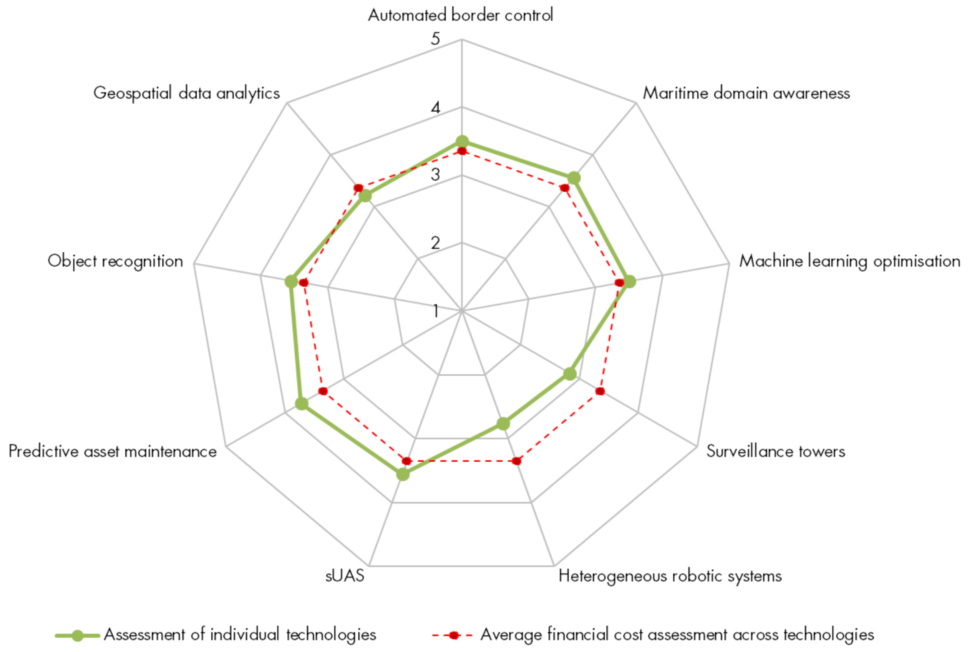
Figure 6.3 Summary of scoring results for speed and efficiency



Source: RAND Europe analysis of expert input.

On average, **financial cost was perceived as the greatest barrier to implementation of AI-based capabilities,** particularly in the case of AI-based surveillance capabilities. Figure 6. provides an overview of the assessment of the nine technology areas based on the degree to which financial cost represents a barrier to implementation. In contrast, **limits on access to relevant technologies and insufficient public or political support were the least significant barriers to implementation**. Workshop discussions corroborated the view that while public perception of AI-based border security technologies remains critical, there is increasing awareness of the benefits of AI, including through the increased fielding of capabilities such as automated border control systems.

Figure 6.4 Summary of case study scores for financial cost



Source: RAND Europe analysis of expert input.

The scoring shows **greatest SD values in the assessment of data protection and regulatory barriers and limits to access of relevant technologies.** This indicates greater scoring discrepancies concerning the influence of these barriers for the technology areas. In contrast, scoring discrepancies were the smallest in the case of the accuracy and quality of results impact criteria, indicating greater alignment among workshop participants concerning the performance of the technology areas in this context.

Annex C. Catalogue of AI technology use cases

Table C.1 Catalogue of AI technology use cases

Technology	Source	Reference/Link
Automated Virtual Agent for Truth Assessments in Real-Time (AVATAR, University of Arizona)	Scoping interviews	https://www.governmentciomedia.com/ai-lie-detectors-could-soon-police-borders
Biometrics on the Move (Frontex)	Scoping interviews	https://frontex.europa.eu/media-centre/news-release/frontex-testing-the-future-of-border-checks-at-lisbon-airport-DI84r4
ABC4EU	Scoping interviews	http://abc4eu.com/
European Travel Information and Authorisation System (ETIAS)	Scoping interviews	https://etias.com/
MARINT (Windward)	Scoping interviews	https://www.ship-technology.com/news/newswindward-to-launch-marint-maritime-intelligence-solution-4582423/
T3K-LEAP (T3K-Forensics)	Scoping interviews	http://www.t3k-forensics.com/en/
Identification of fake stamps in documents (University of Lausanne)	Scoping interviews	N/A
Life Pattern	Scoping interviews	N/A

Technology	Source	Reference/Link
Rekognition (Amazon, ICE)	Scoping interviews	https://www.bbc.com/news/world-us-canada-48907026
iBorderCtrl (Intelligent Portable Control System)	Desk research	https://iborderctrl.no/
Integrated Maritime Services (EMSA)	Scoping interviews	http://www.emsa.europa.eu/operations/maritime-monitoring.html
ID2TRAVEL (IDEMIA)	Desk research	https://www.idemia.com/id2travel
Mface (IDEMIA)	Desk research	https://www.idemia.com/mface
Entity identification and matching algorithms for GTAS (Tamr)	Desk research	https://emerj.com/ai-case-studies/the-department-of-homeland-security-uses-ai-enhanced-entity-resolution-for-its-global-travel-assessment-system-gtas/
Automated Machine Learning (DataRobot)	Desk research	https://www.datarobot.com/wiki/automated-machine-learning/
Metamaterial Electronically Scanning Array (MESA) radar system (Echodyne Corp.)	Desk research	https://www.echodyne.com/products/
Predictive analytics for visa application processing (Canada)	Desk research	https://www.thestar.com/news/immigration/2017/01/05/immigration-applications-could-soon-be-assessed-by-computers.html
Integrated Fixed Towers (IFT) system (Elbit Systems of America)	Desk research	https://www.nextgenborder.com/
Lattice AI and Sentry Towers (Anduril Industries)	Desk research	https://www.anduril.com/lattice-ai
ROBORDER	Desk research	https://roborder.eu/
Project Maven/TensorFlow (Google, US DoD)	Desk research	https://gizmodo.com/google-is-helping-the-pentagon-build-ai-for-drones-1823464533
IFM automated indoor data capture	Desk research	https://www.springwise.com/tech-startup-uses-robotics-automate-data-capture/

Technology	Source	Reference/Link
Raven and Puma UAS system (AeroVironment)	Desk research	http://www.avinc.com/uas/view/raven
Object recognition for TSA (Synthetic)	Desk research	https://www.dhs.gov/science-and-technology/news/2019/11/04/news-release-dhs-awards-200k-ai-based-proof-concept
kvSonata (KickView Corporation)	Desk research	https://www.dhs.gov/science-and-technology/news/2019/10/09/news-release-dhs-st-awards-colorado-start-147k
AUDREY (Assistant for Understanding Data through Reasoning, Extraction and Synthesis)	Desk research	https://www.dhs.gov/publication/st-frg-audrey
Automated self-driving military vehicles for border patrol (IDF)	Desk research	https://mainichi.jp/english/articles/20160824/p2a/00m/0na/020000c
Small unmanned aircraft (sUAS) for Customs and Border Patrol (Planck)	Desk research	https://www.planckaero.com/news
AI reconnaissance platform (Intelleuron)	Desk research	https://www.nextgov.com/emerging-tech/2018/05/dhs-contract-will-help-drones-automatically-spot-border-threats/148088/
AI weapon detection (ZeroEyes)	Desk research	https://zeroeyes.com/
AI weapon detection (Athena)	Desk research	https://athena-security.com/
Automated Biometric Identification System (AwareABIS)	Desk research	https://www.aware.com/biometrics/aware-abis/
Trusted Workforce 2.0 (US National Background Investigation Service)	Desk research	https://www.fedscoop.com/ai-federal-security-clearance/
SparkPredict (SparkCognition)	Desk research	https://www.sparkcognition.com/product/sparkpredict/?utm_medium=direct&utm_source=direct
DeepNLP (SparkCognition)	Desk research	https://www.sparkcognition.com/product/deepnlp/?utm_medium=direct&utm_source=direct

Technology	Source	Reference/Link
Josie Pepper (Munich International Airport)	Desk research	https://www.ikusi.aero/en/blog/5-intelligent-robots-you-can-find-airports-world
Anbot (Shenzhen Airport China)	Desk research	https://www.ikusi.aero/en/blog/5-intelligent-robots-you-can-find-airports-world
Border patrol robots (PSU Bharat Electronics Limited)	Desk research	https://www.businesstoday.in/technology/news/ai-robots-to-patrol-india-borders-prototype-to-come-in-december/story/342591.html
SURVEIRON (AEORUM)	Desk research	https://cordis.europa.eu/project/id/711264
UNFRAUD (TXN SRL)	Desk research	https://cordis.europa.eu/project/id/775707/reporting
Goal-based open-ended autonomous learning robots (Consiglio Nazionale Delle Ricerche)	Desk research	https://cordis.europa.eu/project/id/713010
iTRACK (Universitetet I Agder)	Desk research	https://cordis.europa.eu/project/id/700510
Global Automated Target Recognition (Lockheed) + Maxar	Scoping interviews	https://geoawesomeness.com/lockheed-martin-artificial-intelligence-model-satellite-imagery-analysis/
Artificially intelligent glass	Horizon scanning	https://futurism.com/scientists-create-ai-glass
Self-assembling modular robots	Horizon scanning	https://techcrunch.com/2019/11/01/mits-self-propelled-block-robots-can-now-manage-basic-swarm-coordination/
Biomimetic membranes	Horizon scanning	https://www.nanowerk.com/nanotechnology-news2/newsid=53844.php
Event cameras that help drones avoid moving objects	Horizon scanning	https://spectrum.ieee.org/automaton/robotics/drones/event-camera-helps-drone-dodge-thrown-objects

Technology	Source	Reference/Link
Autonomous training for robots	Horizon scanning	https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/nvidia-brings-robot-simulation-closer-to-reality-by-making-humans-redundant
Robotic hummingbirds	Horizon scanning	https://www.nanowerk.com/news2/robotics/newsid=52784.php
AI for microcontrollers and sensors	Horizon scanning	https://phys.org/news/2019-06-machine-sensors.html
Fuzzy AI system	Horizon scanning	https://www.eurekalert.org/pub_releases/2019-06/caoa-ccm060319.php http://www.ieee-jas.org/article/doi/10.1109/JAS.2019.1911465?viewType=HTML&pageType=en
AI-driven imaging system to detect manipulation of picture and videos	Horizon scanning	https://www.eurekalert.org/pub_releases/2019-05/ntso-odf052919.php
Ability to link senses for robots	Horizon scanning	https://techcrunch.com/2019/06/17/mit-develops-a-system-to-give-robots-more-human-senses/
AI-enabled robot coordination	Horizon scanning	https://spectrum.ieee.org/tech-talk/computing/software/deepmind-teaches-ai-teamwork
All-optical neural network	Horizon scanning	https://spectrum.ieee.org/tech-talk/semiconductors/optoelectronics/ai-at-speed-of-light
AI tools for automating administrative functions	Horizon scanning	https://techcrunch.com/2019/09/09/appzen-nabs-50m-to-build-ai-tools-for-expenses-and-other-finance-team-work/
3D sensing for facial recognition	Horizon scanning	https://spectrum.ieee.org/transportation/sensors/how-3d-sensing-enables-mobile-face-recognition

Technology	Source	Reference/Link
Brain-inspired automated visual object discovery and detection	Horizon scanning	https://www.eurekalert.org/pub_releases/2018-12/usso-nac122018.php https://www.pnas.org/content/116/1/96
Integrative language and vision software for robots	Horizon scanning	https://phys.org/news/2019-01-autonomous-robot-interacts-humans-natural.html
AI-assisted data fusion	Horizon scanning	https://www.eurekalert.org/pub_releases/2019-01/bch-hmd011119.php
CNN facial recognition	Horizon scanning	https://www.eurekalert.org/pub_releases/2019-05/uob-haf050119.php
Robat (bat-inspired robot)	Horizon scanning	https://www.fromthegrapevine.com/innovation/breakthrough-robot-navigates-using-bat-inspired-senses
Walkthrough biometric scanner	Horizon scanning	https://techcrunch.com/2018/10/09/princeton-identity-walkthrough-biometric-scanner-shipping-container/
Thermal-to-visible face synthesis	Horizon scanning	https://www.washingtontimes.com/news/2018/apr/16/army-breakthrough-facial-recognition-technology-no/
Monitoring movement through walls	Horizon scanning	https://www.technologyreview.com/f/611419/we-can-now-use-ai-to-see-through-walls/
AI system for determining personality traits from eye movements	Horizon scanning	https://scitechdaily.com/ai-system-identifies-personality-traits-from-eye-movements/
Smart biometric mirror for identifying personal traits based on facial features	Horizon scanning	https://www.digitaltrends.com/cool-tech/biometric-mirror-judges-your-looks/
Dense Object Nets	Horizon scanning	https://futurism.com/the-byte/computer-vision-mit-robot
AI for operations planning	Horizon scanning	https://phys.org/news/2018-10-smart-algorithms-boost.html

Technology	Source	Reference/Link
Person identification through footsteps monitoring	Horizon scanning	https://futurism.com/the-byte/footsteps-identification-ai
Gun-spotting camera system	Horizon scanning	https://www.digitaltrends.com/cool-tech/ai-camera-spots-guns-in-video/
Biologically inspired skin for robots	Horizon scanning	https://www.sciencedaily.com/releases/2019/10/191010125623.htm
AI-enabled person re-identification	Horizon scanning	https://techxplore.com/news/2019-10-ai-world-leading-technology-visual-recognition.html
Using artificial intelligence to enrich digital maps	Horizon scanning	http://news.mit.edu/2020/artificial-intelligence-digital-maps-0123

Source: RAND Europe analysis.

Annex D. Technology adoption roadmaps

This Annex provides the technology adoption roadmaps for each of the nine selected AI-technology areas (each sub-section describes the roadmap for one technology area). The technology roadmaps draw on data gathered through the case study analysis and expert workshop in WP1, as well as interviews with technology and border security experts and desk research conducted in WP2. Each roadmap is structured as follows:

- Summary of current and desired capability levels and the pathway to adoption;
- Summary of key requirements and potential barriers to adoption in relation to those requirements. The roadmaps include a discussion of seven categories of elements of adoption, namely:
    - Personnel & training;
    - Infrastructure, equipment & logistics;
    - Information;
    - Organisation;
    - Regulatory, legal & ethical;
    - Technology performance;
    - Other requirements/barriers to adoption.
- List of illustrative use cases, including commercial products and R&D projects that are in use or in development, and which could address the defined capability needs. This includes a short description of each use case including any identified potential benefits and challenges associated with the technology.

D.1. Automated Border Control (ABC)

Current Capability	Pathway to Adoption	Desired Capability
Currently, European border controls rely heavily on border guards. Whilst border guards are supported by some new technologies that automate specific aspects of border control, the level of automation remains relatively low and typically requires strong input from operators. However, many governments – across Europe and globally – have begun to test the use of border gate technology to enable more autonomy of processing the passage of goods and people through border points/crossings.	There are a number of capability and technology options available or in development that could enable greater use of ABC gates. A particular area of focus for adopting ABC systems in the next few years is likely to be the acquisition of high-quality images for facial recognition. Research continues to advance recognition models to enable systems to function in non-perfect conditions (e.g. low lighting, travellers wearing glasses, physical position, etc.).[176] Technologies including iris scanning and facial recognition are not able to achieve sufficient accuracy given the current biometrics systems available, despite increased efficiency enabled by AI.[177] In the next few years, the development of AI-based sensors and extraction algorithms is anticipated to lead to enhanced capabilities, with models producing the same results that currently only exist for biometrics data-collection in well controlled settings. [178]	As developments in AI and supporting hardware enable greater efficiency and accuracy in conditions typical of European border control points, ABC gates are expected to become more prominent. It is expected that ABC will provide 'an automated immigration control system that conventionally integrates e-gate hardware, document scanning and verification, facial recognition and other biometric verification to facilitate faster processing of travellers on border crossing while enhancing security through the integration of various AI-enabled tools'.[179] These functions will be integrated as part of automated control points that will help establish whether the passenger is the rightful owner of relevant documents and thus automatically determine whether someone can pass through a border according to pre-defined rules.[180] The system will be able to alert border guards to any potential issues or non-compliance with these pre-defined rules.

[176] Sanchez et al. (2016).

[177] WP1-INT05.

[178] WP1-INT05.

[179] European Commission (2020d).

[180] European Commission (2020d).

Implementation factors

Category	Requirements for adoption	Barriers to adoption
Personnel & Training	Future ABC gates are expected to be designed in a way that makes their operation relatively intuitive and requires little technical knowledge and training for the end user (i.e. border guards). Therefore, this capability is not anticipated to result in any significant cost burden for end users as a result of technical training requirements, though some familiarisation training for operators will be needed to ensure the systems are used effectively.[181] However, the development and implementation of ABC gates and the supporting systems requires technical knowledge of the underpinning hardware and AI technology. European border authorities are likely to require personnel with a good understanding of AI techniques and their application, potentially through contractor support, in order to enable the development of ABC gates through experimentations and determining how this capability can best support border control operations.	There are very few personnel and training barriers to operators adopting many of the underlying AI-based technologies within an ABC gate capability. However, border security authorities will require access to relevant technical support, either in-house or contracted, who can maintain the relevant technologies. There might also be cultural barriers within border guard personnel that have to be overcome through appropriate processes and training. These are likely to arise from the need to 'trust' autonomous systems to conduct functions that traditionally rely on human operators.
Infrastructure, Equipment & Logistics	This capability would require a large amount of computational power and time in order to understand and resolve problems. Advances in computing power mean this requirement is reducing as technology is made more efficient. However, there remains a need for substantial hardware to undertake initially large experiments to develop	Although existing computational capabilities are already at a reasonable level, the process of creating and developing efficient neural Deep Learning networks for ABC gates requires a substantial computational capacity that is likely to limit the speed at which this capability can be run for operational use. [185] The meaningful cost associated with ABC systems could hinder their implementation. Large portions of the expenditure for ABC gates derives from the creation of the database and its maintenance; infrastructure ecosystems to ensure data

[181] WP1-INT05.

[185] WP1-INT05.

Category	Requirements for adoption	Barriers to adoption
	effective algorithms and eventually, from which to operate the systems.[182] Another factor for the successful implementation of ABC gates systems resides in their interoperability. Future systems will need to be interoperable and portable, so they can be used in any location and in combination with other systems at border control points, such as national airports. Systems will also need to be interoperable with the ABC systems of other countries to facilitate data sharing.[183] A further requirement for ABC gates is to develop algorithms that are reliable and ensure gates cannot be manipulated by travellers with no right to cross them.[184]	accessibility at local and EU levels in near real-time while maintaining security for data privacy and general security; and the networking of data and devices, including the security gates themselves.[186]
Information	As is typical for any AI system, there is a significant data requirement for developing and training any system to be effective. This data will need to be accurate, comprehensive and appropriate to the intended end use of the ABC gate (dependent on the scope of the capability to be employed by each nation or authority). ABC gates would also require coherent systems for the collection and distribution of data, including infrastructure to ensure connection to data depositories in order to guarantee effective operation of the ABC system.[187]	In order to guarantee the effectiveness of ABC gates, availability and accuracy of data is critical to the development and ongoing operation of the system. Collecting this data is likely to represent a significant stepping stone that needs to be overcome in order for their deployment to become more favourable.[188] Current gaps in the evidence base also hamper further significant improvement of AI that underpins ABC gates, notably in the context of biometric scanning and verification.[189]

[182] WP1-INT05.

[183] Sanchez et al. (2016).

[184] WP2-INT14.

[186] WP1-INT05.

[187] WP1-INT05

[188] Frontex (2012).

[189] WP1-INT05

Category	Requirements for adoption	Barriers to adoption
Organisation	To maximise the effectiveness of ABC systems, any future capability should seek to develop common standards and practices regarding border management amongst stakeholders for AI-enabled ABC systems and EU Member States. This will be key to an efficient implementation of such systems.[190] The existence of EU-financed pan-European projects related to ABC gate technologies (e.g. ABC4EU, FastPass, etc.) that can monitor current and near-future travel patterns and technologies represents an opportunity to work towards such harmonisation.[191]	The existence of multiple, related organisations across European border security creates a significant organisational challenge that will likely be a barrier to the effective employment of integrated ABC systems that can work together across Europe. For example, there is a large number of systems and regulations (e.g. PNR, ETIAS, GDPR, National Facilitation program – NFP) related to the monitoring of immigration systems, which may lead to duplication of effort and reduced data accessibility.[192]
Regulatory, Legal & Ethical	Due to ethical and privacy-related challenges, especially those related to the collection, storage and processing of personal data, the broader adoption of ABC technologies must be, at the least, accompanied by appropriate measures that guarantee users' acceptability through democratic and public political control.[193] To support the development of the necessary AI-based techniques for implementation in ABC gates, it would be advantageous to establish dedicated scientific databases for future R&D work. These would enable the anonymisation of the data used to develop and test algorithms, enabling more rapid and accurate development and facilitating compliance with existing and future regulations in areas such as facial recognition.[194]	Several challenges exist for the EU regulatory framework in relation to sharing data for future R&D activities. Specifically, the regulations restrict data sharing, which is critical to improving AI-based ABC systems and addressing some of the current gaps in the evidence base, which relate to the technical specifications of AI-enabled biometric scanning techniques. Concerns related to the ethics of AI and human rights (e.g. privacy) protections tend to slow the development of control systems. For example, the risk of algorithmic racial and gender biases in AI-based techniques have led developers, including IBM, to significantly limit or discontinue R&D in facial recognition technology. Increased use of biometric scanning could also fuel concerns over unjustified surveillance of EU citizens, and risks of and breaches of individual privacy and data security.

[190] Lehtonen & Aalto (2017).

[191] Sanchez et al. (2016).

[192] Clabian & Kriechbaum-Zabini (2017).

[193] Lehtonen & Aalto (2017).

[194] WP1-INT02.

Category	Requirements for adoption	Barriers to adoption
Technology Performance	An important requirement for the implementation of ABC gates lies in the development of systems that are able to perform biometric scanning and verification in imperfect conditions. To that end, an increased number of factors and indicators to which a system can refer when performing biometrics scanning – such as facial recognition – are necessary for future R&D.[195] The guidelines for ABC systems suggest the false accept rate (FAR) for facial capture and verification should not be higher than 0.1%, while the false rejection rate (FRR) should not go above 5%.[196] End users need to achieve a balance between accuracy and computational cost of the technologies being developed.[197]	The challenge faced by AI-enabled biometric scanning and facial recognition techniques concerning their performance could be a hindrance for near-future implementation. The development of proper sensors and algorithms to extract relevant information is particularly essential when considering degraded environmental conditions.[198]
Other	No other requirements were identified.	No other barriers were identified.

Illustrative use cases

Use Case 1: ABC4EU	
Description	ABC4EU aims to harmonise the use of AI-enabled automated border control (ABC) gates for processing third-country nationals entering the EU. It includes an AI-enabled biometric scanning capability and a gate and mobile verification system.
Benefits	ABC4EU improves the speed of border crossings across automated and harmonised border control processes in Europe. Providing more flexibility in border control, ABC gates contribute to enhancing the workflow of travellers, significantly reducing the time that travellers queue at border points. ABC4EU further creates a European harmonised ecosystem for the functionalities of ABC gates.[199]

[195] WP1-INT05.

[196] Sanchez et al. (2016).

[197] WP1-INT05.

[198] WP1-INT05.

[199] ABC4EU (2020).

Use Case 1: ABC4EU	
Challenges	Room for improvements exists in light of the necessary harmonisation for ‘e-passports management, biometrics, gate design, human interface, processes, PKD certificate exchange, signalling and interoperability’.[200]

Use Case 2: Biometrics on the Move	
Description	Integration of AI in a biometric corridor/e-gate that screens passengers through facial recognition and fingerprint scanning, but does not include document screening.
Benefits	Biometrics on the Move facilitates border checks by removing the *ante* control of passport and/or other administrative documents. Border crossings therefore become swifter and provide border guards with more time to conduct security checks without strongly impacting regular travellers.[201]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 3: European Travel Information and Authorisation System (ETIAS)	
Description	Electronic travel authorisation system for screening and tracking third-country nationals who lack visa requirements to enter the EU. ETIAS entails a security check of applicants prior to entering the EU, similarly to the ESTA (USA) or eTA (Canada) systems.
Benefits	Enables the collection of information on people travelling visa-free to the EU in order to deny individuals travelling within the Schengen area who pose a security risk. This is a centralised EU system to issue travel authorisations that enhances external and internal security of the EU.[202]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 4: Biometric Exit Program	
Description	AI-enabled biometric verification programme that aims to have the capacity to verify 97% of outbound air passengers within four years, and to support the identification of visa overstayers.

[200] ABC4EU (2020).

[201] Frontex (2019a).

[202] ETIAS (2020).

Use Case 4: Biometric Exit Program	
Benefits	While the majority of undocumented migrants can often be identified in airports, this is a substantial undertaking. This AI-based system would enable airport scans to support the identification of overstayers and illegal migrants more rapidly.[203]
Challenges	There could be privacy concerns over the use of data outside airports. Facial recognition databases could be attacked or accessed for law enforcement in breach of data protection regulations.[204]

Use Case 5: AI-enabled intelligent security check-in system	
Description	AI technology is used in a smart security check-in system, where passengers, tickets and ID documents are automatically linked together. When a passenger enters the luggage check-in area, biometric features are used as tags to match the passenger to their luggage.
Benefits	Across biometric features, the check-in system links passengers, tickets and ID documents together as well as passengers and their luggage. Altogether, the system improves the efficiency of luggage processing and traveller check-in.[205]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 6: ID2TRAVEL	
Description	Integrated security system, includes passenger checks through biometric information-screening and passenger identification.
Benefits	System allowing the faster crossing of checkpoints, airside access and passport control, as well as at boarding control. It also comprises a central system that manages passenger identification through all the identity checks needed for authentication and identification of the passenger.[206]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 7: Dialect biometric identification for asylum seekers	
Description	AI-enabled 'language biometrics' software capable of analysing dialects as a way of determining an individual's true place of origin.

[203] Martin (2019).

[204] Martin (2019).

[205] Zhang (2019).

[206] IDEMIA (.).2020).

Use Case 7: Dialect biometric identification for asylum seekers	
Benefits	Designed to help assess the potential of false statements being made by individuals trying to cross a border – such as by asylum seekers – and their place of origin.
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 8: Automated Biometric Identification System (AwareABIS)	
Description	AwareABIS is used for biometric identification and deduplication, including scanning of fingerprints, face and iris modalities recognition. As a cluster computing platform, it is able to 'perform searches against millions or tens-of-millions of records'.[207]
Benefits	This type of system enables the rapid searching and comparison of biometric data, such that it can be used in virtual real-time for fingerprint, facial and iris recognition.
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 9: 3D sensing for facial recognition	
Description	Three new techniques developed by ams for using 3D sensing to implement facial recognition: time-of-flight sensing, stereo imaging and structured light.
Benefits	3D depth map generates more data of individuals' faces than images that are processed via a conventional 2D camera. Secure 3D authentication enables the use of face recognition in critical applications, such as mobile payments.[208]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 10: CNN facial recognition	
Description	New ML-based method for using convolutional neural networks (CNN) for facial recognition when only ½ or ¾ of a face is visible. This is achieved through drawing on a feature extraction model (VGG) and training the model for recognising faces only from partial images.
Benefits	Possibility to have highly accurate facial recognition from images that only show part of a face.[209]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

[207] Aware (2020).

[208] IEEE Spectrum (n.d.).

[209] University of Bradford (2019).

Use Case 11: Walkthrough biometric scanner	
Description	Biometric Conex is a walkthrough shipping-container-like structure that integrates several biometric technologies into a 'self-contained air-conditioned unit that can process as many as 20 people per minute'.[210] The biometric scanner can detect fingerprints, face and irises, and fuse all data together.
Benefits	Hasten the border crossing process by cutting down on queueing.[211]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 12: Automated Virtual Agent for Truth Assessments in Real-Time (AVATAR)	
Description	AVATAR system aims at providing an AI-enabled ‘lie detector’ through the analysis of eye movements.
Benefits	Enhanced identification of untruthful or potential risk individuals based on eye movements or changes in voice, posture and facial gestures.[212]
Challenges	The performance of AVATAR and other similar systems becomes dubious due to the risk of algorithmic biases, in addition of possible AI systems’ inability to accurately recognise eye movements of individuals provoked by stress.

[210] Whittaker (2018).

[211] Whittaker (2018).

[212] Daniels (2018).

D.2. Maritime domain awareness

Current Capability	Pathway to Adoption	Desired Capability
Existing capabilities for maritime domain awareness focus on intelligence gathering and threat detection to ultimately support decision-making. They can be described as a manifold process that includes data collection via Automatic Identification Systems (AIS) from multiple databases (e.g. satellite imagery, available commercial sources). Once collected, data fusion is undertaken using AI-based infrastructures; mistakes, irrelevances and corruption are filtered and eliminated, and the system generates analysis to support activity-detection of maritime vessels. For example, previous activities from a vessel may be flagged to operators and incorporated into semantic categories that facilitate subsequent analysis.[213]	One of the main challenges with AI for maritime domain awareness lies in processing and analysing data. AI solutions process large amounts of raw data issued from AIS. The data is also sourced from multiple vendors, which can result in redundancies, noise and mistakes in the database. In this regard, to progress the development of maritime domain awareness, investment will be needed to develop data fusion operations that are able to clean data from corruption and errors in order to guarantee that decisions are based on accurate information.[214] Investment in data fusion is likely to focus on improving the accuracy and effectiveness of the underlying layers of fusion that exploits AI-based technology. The next step in the development of AI in this area is likely to enhance the speed of the data fusion process and enhance models to support the generation of new insights from the same data.	The next 5–10 years are likely to see greater use of AI-enabled solutions for enhancing situational awareness and threat detection through automated data processing and analysis.[215] Future capability should provide the ability to rapidly fuse maritime data from various sources, including shipping industry data and the Satellite Automatic Identification System (S-AIS), using AI to enable real-time maritime data analytics and improved detection and management of emerging threats. The operational profiling that results from the data about any maritime assets can provide analysts with insights to inform risk assessments, e.g. allowing a user to know how many times a vessel visited a port at night-time, create a comparative assessment with other vessels, and assess whether an anomaly exists.[216] AI models may also develop profiles of vessel behaviour, which could be used to, for example, learn the features of those involved in illicit activity and provide predictions on the most likely ships to engage in unlawful operations.[217]

[213] WP1-INT07.

[214] WP1-INT07

[215] Peled (2020).

[216] WP1-INT07.

[217] WP1-INT07.

Implementation factors

Category	Requirements	Barriers to adoption
Personnel & Training	It is expected that there will be a minimal burden on personnel and training. Because the relevant data extracted and processed through data fusion is categorised before being presented to operators, very little technical knowledge is required to understand the information being provided for analysis and decision making. Training can be therefore completed in a limited amount of time, around 1–5 days, depending on depth of training.[218]	Any barriers in personnel and training are expected to be minimal and unlikely to prove to be a substantial challenge to adopting this technology.
Infrastructure, Equipment & Logistics	There are only limited costs associated with the system, as it requires no additional infrastructure to be developed and maintained.[219]	Given that existing infrastructure can be used and many of the data sources already exist there are few barriers to employing this type of technology.
Information	The development of AI-based capabilities relies heavily on the sharing of data between vessels and relevant stakeholders. There is also a requirement to be able to use data for intelligence purposes and combine it with the Global Navigation Satellite System (GNSS) to provide a richer picture of what might be happening. This is not simply a question of ranging targets, but of using available data to classify them and support appropriate organisations in understanding potential targets of interest.[220]	Whilst information security has conventionally been a barrier for web-based services such as Marint, these concerns have mostly been resolved and no longer represent a significant barrier. [221]

[218] WP1-INT07.

[219] WP1-INT07.

[220] WP2-INT03.

[221] WP1-INT07.

Category	Requirements	Barriers to adoption
Organisation	No specific organisational issues were identified by participants.	No specific organisational barriers were identified.
Regulatory/Legal /Ethical	To maximise the potential exploitation of AI-based technologies, the relevant regulations must enable the appropriate use of supporting specialist equipment and data sharing.	Legislation is not an issue as such in national waters – nation-states can allow special equipment and modernise regulations should it be required. However, the greatest challenge is likely to be the lack of legislation regarding international waters, which could become an issue for maritime awareness technology.[222]
Technology Performance	Data fusion relies on data cleaning and verification to ensure consistency. As such, sufficient infrastructure and computing power for cleaning, verification and correction of data is needed. Ideally, this 'should be built into systems as a default, both algorithmically and procedurally'.[223] The success criteria for AI-based systems are already extensively defined and include how accurate the position needs to be; which signals can be processed; the range of detection, accuracy of labelling, etc. However, such criteria are often defined from a commercial and operational point of view and are different to the data than the military or border entities.[224]	Whereas the volume of collection used to be the biggest challenge for intelligence, the challenge is now about collecting very specific data points.[225] This is critical to meeting the awareness and intelligence requirements of the EBCG.
Other	No other requirements were identified.	No other barriers were identified.

[222] WP2-INT03.

[223] Primor (2020).

[224] WP2-INT03.

[225] WP1-INT07.

Illustrative case studies

Use Case 1: MARINT	
Description	Windward's maritime domain awareness solution utilises AI to fuse and analyse various maritime data streams. This enables real-time maritime data analytics, object recognition and threat detection.
Benefits	This technology enables the user to understand patterns of activity at sea, highlight behavioural anomalies and assess the potential intent of targets of interest. Anomalies can be determined based on deviations from patterns, and enables analysts to assess and prioritise investigations into targets of greatest interest/highest risk. This technology is intended to enhance operational planning and focus the use of limited resources onto the greatest threats.[226]
Challenges	The system still has some challenges to overcome in the post-data extraction phase of the processing. The AI-based infrastructure available for processing and cleaning the data is still in development and suffers from mistakes and data corruption issues.[227]

Use Case 2: Enhanced Maritime Situational Awareness	
Description	Use of AI to detect suspicious vessels, maritime equivalent of the Automatic Information System (AIS). Provides vessel traffic-data and local maritime information to indigenous and coastal communities.
Benefits	By combining skills, experience and resources, the European Maritime Safety Agency (EMSA) and Frontex can build on synergies to improve the quality of services developed. Cooperation also brings cost savings by avoiding duplication of effort and overlapping infrastructures; and enhancing economies of scale. Information provided to the Member States by Frontex based on the EMSA services is used for various purposes, such as: 1. Surveillance of targeted ports and coasts; 2. Tracking of suspect vessels over high seas; 3. Monitoring sea areas for environmental purposes.
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 3: Artificial Intelligence / Machine Learning Sensor Fusion for Autonomous Vessel Navigation (Maritime AI-NAV)	
Description	The project investigates how European satellites and space programs – such as the Galileo and EGNOS systems – can be used for autonomous vessel navigation. New sensor equipment will combine data from visual images, environmental sound recordings, radar and LiDAR ranging, satellite navigation and vessel transponders.

[226] Windward (2020).

[227] WP1-INT07.

Use Case 3: Artificial Intelligence / Machine Learning Sensor Fusion for Autonomous Vessel Navigation (Maritime AI-NAV)	
Benefits	The goal is to automatically identify and recognise objects – such as navigation aids and other vessels or boats around the ship – and to provide improved situational awareness information by way of sensor fusion.
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 4: Sea Aware	
Description	AI-enabled situational awareness in combination with traditional sensor fusion. Sea Aware fuses radar and electro-optical sensors, together with attitude, positioning and AIS sensor data to provide reliable information on all static and moving objects inside the coverage area. The navigator receives this information from a single source, removing the need for manual tuning of sensors and correlating of outputs – all of this happens automatically in the SeaAware engine.
Benefits	Enhanced situational awareness is designed to mitigate the risks navigators face, especially in poor weather conditions, congested waters or at night. Enhanced interface to receive inputs.
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

D.3. Machine learning optimisation

Current Capability

Machine learning (ML) is already being used in border security across the globe. In particular, it is focused on assisting border security authorities and organisations to operate more efficiently in the gathering and processing of vast quantities of data. Whilst already in operation in a number of countries, including in Europe, many ML-based capabilities are still under development and have yet to be fully optimised. A challenge for current capability is being able to optimise ML models that are in use for data processing. There is also a lack of standardisation amongst ML models, which currently limits the extent to which AI can be used to optimise ML model selection. However, a number of AI-based technologies are in development that seek to automate the selection, testing and optimising of ML models, which currently rely heavily on the use of human operators.

Pathway to Adoption

A key step in improving the optimisation of ML models will be the standardisation of model interfaces and outputs. This process is likely to require a significant amount of effort to develop and refine the AI systems that will be used in optimising ML model selection.

This is also an area of technology that remains relatively unseen by end users. To ensure it is not overlooked or de-prioritised compared to the more obvious uses of AI in some other capability areas, it is important that users are educated to understand the value that this type of 'behind-the-scenes' AI can provide.

Desired Capability

In the future, there are a number of areas that are likely to emerge for optimising ML models. ML model outputs are expected to become more standardised and models are likely to employ common standards in their interfaces to reduce the requirements for human experts who can select an optimal model. The technology that is already in development and should be operational in the near future will allow users to more easily select from a ranked list of ML models, enabling users to make faster but more informed choices based on their individual needs and maximising the efficiency of the ML chosen for each task.[228]

As an example, the identification of human trafficking networks could benefit greatly from the use of facial recognition in conjunction with clustering that employs ML models. By optimising the ML models used, law enforcement organisations will be able to more rapidly develop an understanding of different grouping and behaviours of traffickers, without having to rely on intelligence personnel.[229]

[228] DataRobot (2020).

[229] WP2-INT10.

Implementation factors

Category	Requirements	Barriers to adoption
Personnel & Training	In order to improve the understanding of the value that this type of AI can provide, it will be necessary to enhance AI competency for relevant individuals. Given the need for border guards to train in a wide variety of skills, reducing the training footprint for this type of new technology is necessary to facilitate its uptake. However, such technology should be built to be relatively intuitive to use, requiring only limited user-input once set up.[230] It will also be important to enhance the awareness of the benefits of AI for producing actionable insights and supporting decision makers.[231]	ML optimisation tools are likely to function without most people being aware of it, unlike more visible systems such as surveillance towers. The greatest barrier to adoption is therefore a lack of awareness or understanding among end users of the value this type of 'enabling' AI technology can bring.
Infrastructure, Equipment & Logistics	This technology requires appropriate hardware and software to enable AI and ML to operate efficiently and effectively. The exact level of such requirements could depend on the specific requirements of the software being used. Further requirements are likely to relate to sensor equipment that can provide the data that an ML model will analyse (e.g. cameras for imagery capture).	There are no particular barriers beyond ensuring that appropriate software and hardware are in place. If the use case focuses on the data capture being mobile and not bound to a border control point, for example, then ensuring the hardware is sufficiently mobile may be of concern. Fast, light computers, as well as software developed to make optimal use of computational resources, will be necessary.[232]
Information	In order to function, the ML models rely on various types of input data, although this varies depending on the use case. In order to implement this type of capability it will be important to identify what information is required and how this will be sourced, stored and used.	There is a perceived lack of transparency around the nature of the underpinning processes and workflows within ML models.[233] They can often be treated as 'black boxes'. This prevents end users from making appropriate assessments on the trade-offs concerning the size, accuracy, precision and latency of various ML models. Any

[230] WP2-INT10.

[231] DataRobot (2019a).

[232] WP2-INT10.

[233] Msv (2020).

Category	Requirements	Barriers to adoption
		future system will have to overcome these barriers and ensure the system has adequate information to allow end users to make informed decisions concerning the use of a ML model.
Organisation	The most vital requirement to help improve the use of AI more broadly is to ensure there is appropriate transparency and collaboration across different border security organisations and teams within those organisations. This is vital to ensure that organisations are set up to make effective use of AI and to successfully integrate this type of capability.	A perceived lack of understanding of the operational challenges and requirements of the agencies in charge of maintaining security at borders could hinder further research and development of AI to fulfil border security technology gaps.[234]
Regulatory/Legal /Ethical	Efficient international cooperation on regulation is required. Joint actions and standardisation are prerequisites for maintaining comprehensive control of external borders of the EU and effective judicial or law enforcement cooperation.	Legal and regulatory barriers are the first obstacle to implementing procedures and using AI-based technologies when performing border checks.[235] The specific barriers related to this capability area would need further investigation to understand exactly how current regulations might limit or prevent the use of AI in this case.
Technology Performance	ML models employ a wide variety of performance parameters, including e.g. the explainability of the models, the ratio between false positives and false-negative results in object recognition classes, or detection thresholds. The specific performance parameters to be used should be agreed by end users to determine the overall performance of any model. Different AI systems are also likely to require access to validation data in order to provide an in-depth performance assessment.[236] As such, the definition of performance requirements will depend on the needs of and the systems used by the end user.[237]	The barriers will be a function of performance requirements for individual systems. It will be important for end users to understand and articulate the performance they require, which ciould be a barrier where there is limited understanding of the technology.

[234] WP2-INT10.

[235] WP2-INT10.

[236] WP2-INT10.

[237] WP2-INT10.

Category	Requirements	Barriers to adoption
Other	As the adoption of this technology is contingent upon the pace of ML adoption more widely, and given the challenges in adapting border security to embrace the benefits of this type of capability, it may be useful to establish incentives toward wider organisational process change to allow use of ML.	Establishing incentives will require significant cooperation and agreement in the changes that are desired in border security, and achieving this might constitute a barrier.

Illustrative use cases

Use Case 1: DataRobot AutoML	
Description	Automated Machine Learning (AutoML) is an AI tool based on machine learning methods that facilitates autonomous testing, selection and deployment of AI models. This is intended to enable advanced and predictive analytics.
Benefits	'Automated machine learning makes it easier to build and use machine learning models in the real world by running systematic processes on raw data and selecting models that pull the most relevant information from the data. Automated machine learning incorporates machine learning best practices from top-ranked data scientists to make data science more accessible across the organization.'[238]
Challenges	Whilst this use case has developed potential solutions to automated ML, there remain gaps between the theory and practice in this area. A robust implementation of this type of Auto ML systems is likely to face a number of process and technical challenges that still need to be overcome.

Use Case 2: Entity identification and matching algorithms for GTAS	
Description	Platform for resolving passenger identity from Advanced Passenger Information (API) and Passenger Name Record (PNR) datasets, assists the GTAS system in comparing the passenger data and estimating the match probability for specific subjects, thereby supporting informed decision-making. The platform is trained by human subject-matter experts.
Benefits	Current AI is very capable when there are existing structured massive datasets and access to structured and curated public datasets. In these cases this platform provides excellent identification and matching capabilities.
Challenges	Where there is a lack of substantial datasets, this can reduce the effectiveness of the platform.

[238] DataRobot (2020).

Use Case 3: AUDREY (Assistant for Understanding Data through Reasoning, Extraction and Synthesis)	
Description	Use of AI and situational awareness technologies to support first-responder decision-making through simultaneous inference and real-time learning. AUDREY selects key information and applies 'human-like reasoning' to synthesize information for the human operator.
Benefits	Provides the 'ability to sift through vast amounts of data and intelligently use only the most appropriate information and optimally deliver the relevant and actionable knowledge to the end user. Synthesises high-level actionable information and provides it to the first responder when appropriate'.[239]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 4: kvSonata	
Description	KickView Corporation has been commissioned to adapt a multi-sensor AI software platform to 'provide real-time data analysis of the international customs processing areas of airports', focusing on real-time analysis of passenger flow (queue lengths and wait times) in international customs processing areas.[240]
Benefits	Collection, processing and learning from sensor data in real time, providing the U.S. Customs and Border Protection (CBP) a granular view of passenger flow.
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 5: DeepNLP	
Description	AI applied to automate the management of unstructured data within organisations. The system 'integrates into existing workflows to enable organizations to better respond to changes in their business and quickly get answers to specific queries or analytics that support decision making'.[241] Existing applications are within the aviation sector.
Benefits	Identify patterns, classify documents, extract valuable information from data.
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

[239] U.S Department of Homeland Security (2018).

[240] U.S. Department of Homeland Security (2019).

[241] SparkCognition (b2020b).

Use Case 6: AI-assisted data fusion	
Description	Application of machine learning to combine different forecasting methods and reduce errors in predictions based on data fusion. In the reported case the technique was used to predict influenza activity and mitigate epidemic outbreaks.
Benefits	'Help public health officials mitigate epidemic outbreaks and may improve communication with the public to raise awareness of potential risks' in case of detection.[242]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

[242] Boston Children's Hospital (2019).

D.4. Surveillance towers

Current Capability	Pathway to Adoption	Desired Capability
AI-enabled surveillance towers currently have limited use in border security. The underlying technologies have been developed but remain relatively untested (although iterative testing and use is already expanding). Current capabilities in this area typically involve a static tower equipped with sensor and networking technologies that can be placed in the vicinity of a border. Surveillance towers are relatively quick to deploy or move and can include physical and virtual hardening to protect the system and technology components. The capabilities that exist include onboard collection and fusion of data, as well as object detection that employs AI to reduce the amount of information and intelligence that human operators are required to handle and process.	The next steps in the development of this capability will be focused on the testing and refinement of the technology. For border security authorities to start adopting this technology it will be important to ensure it is tested in different environments and contexts to improve its effectiveness in different settings. EBCG could consider opportunities to test these technologies within a European context and whether there are any regulatory issues to address to allow testing.	Whilst the overarching concept already exists, over the next few years, the focus is likely to be on the broader testing and iterative development of the capability to improve its efficiency and effectiveness. It is also expected that development will continue in the area of automated object detection and surveillance of large areas, to reduce the burden on human operators. It is expected that surveillance towers will provide near real-time analysis of larger areas through onboard sensor data fusion. As the capability develops and larger areas are being monitored, the surveillance towers might become better integrated with sensors from a wider range of platforms such as UAS to provide comprehensive situational awareness, which is fully autonomous.

Implementation factors

Category	Requirements	Barriers to adoption
Personnel & Training	The purpose of surveillance towers is to provide a fully unmanned monitoring and analysis capability. As such, the main personnel requirements will be for relevant users to be trained in deploying and setting up the systems and understanding the outputs generated. The software and sensors that operate on these towers are generally designed	Some training of personnel is required to set up and operate these towers. Relevant personnel would also need training in how to interpret the analysis generated by these towers. This training would incur costs and tie up resources to integrate the towers into

Category	Requirements	Barriers to adoption
	to be user-friendly, with individual components being highly portable.[243]	an operational setting. For example, training is needed on the set-up and use of radars, such as the Echodyne radars.[244]
Infrastructure, Equipment & Logistics	Developers believe that due to the benefits of mesh sensing and full automation of multi-tower installations, surveillance towers are expected to be less costly than physical security measures that might be an alternative, for example, chain link fencing.[245] The towers and their constituent sensors and hardware will need to be maintained, although they are expected to use relatively reliable components. This capability will also require appropriate logistical support to move towers, particularly if they are being used as a mobile asset.	The main barriers to installing this type of system will be the costs involved in placing, maintaining and moving the capability. In many cases it could also be necessary to integrate new surveillance technologies with existing legacy systems. However, the extent of this challenge will vary greatly depending on the chosen solution and what legacy systems are in place.
Information	The systems will require representative data that will allow for comprehensive testing and further (iterative) development in a realistic setting. This will require border security organisations to work with developers to enable access to appropriate information.	There were no specific information barriers identified, beyond the general challenges of data security and sharing. If nations wish to collaborate in testing and developing these systems, there could be barriers to overcome related to how appropriate data and information is shared.
Organisation	There are no specific organisational requirements, beyond developing the appropriate culture and processes to ensure users trust these systems and they are fully integrated into border security operations.	There is likely to be limited awareness of the potential of AI and surveillance towers in replacing alternative physical measures for providing border security. It will be challenging to overcome the belief that AI-enabled technologies are only in their infancy, rather than capable of immediate field deployment.[246]

[243] WP2-INT02.

[244] WP2-INT02.

[245] Anduril.com (2020).

[246] WP1-INT04.

Category	Requirements	Barriers to adoption
Regulatory/Legal /Ethical	Radio frequency band authorisations are required in each EU Member State to use radars, which are a key sensor on these platforms. There are not expected to be any privacy issues to address because radars do not use facial recognition or identify individuals specifically.[247]	Though the absence of a facial recognition capability within this system reduces challenges related to privacy safeguards, the proliferation of AI-enabled surveillance technologies more widely has raised concerns in relation to the impact on communities in border regions. This is due to the perception of the powers of law enforcement and border control authorities expanding with the proliferation of advanced surveillance systems, contributing to the possible erosion of human rights safeguards for local communities.[248]
Technology Performance	This technology is still under development and in order to improve the performance, it requires continual iterative development of the AI systems through field testing. In particular, AI needs to be developed to train radars. The AI will need to be developed for different ranges within which the AI system will operate. This is because the parameters of the radar are set according to the target that should be detected (e.g. UAS).[249]	Radars are more difficult to train through machine learning than cameras even though there are opportunities to do this through field testing an iterative development. There could be opportunities to address this barrier by changing the radar's parameter in real-time through the use of cognitive radars, although this has not yet been developed as a capability.[250]
Other	In order to exploit technology developments such as surveillance towers, governments need to develop quicker processes for adopting technologies than are currently in place.[251] This would enable more rapid integration of technology that is evolving at a rapid pace.	Currently, the slow processes for adopting new technologies in many EU governments means that by the time these rapidly evolving AI technologies can be adopted, they are already out-of-date or have been overtaken by newer systems. In this case there are both procedural and cultural barriers in place that continue to prevent the rapid adoption of new technology.[252]

[247] WP2-INT02.

[248] Fussell (2019).

[249] WP2-INT02.

[250] WP2-INT02.

[251] WP1-INT04.

[252] WP1-INT04.

Illustrative use cases

Use Case 1: Sentry towers	
Description	Sentry Towers are fully unmanned integrated hardware and software surveillance systems, enabled by an AI platform (Lattice AI). The system serves autonomous detection and classification of objects, contributing to threat analysis.
Benefits	This system can be left unattended and provide automated surveillance of border crossings for threats. These systems are also relatively portable and require very little intervention from human operators.
Challenges	This system requires development in a real world setting and this means that border security organisations need to work with developers to test and develop the system and to help train the AI systems to be effective.

Use Case 2: Metamaterial Electronically Scanning Array (MESA) radar system	
Description	Echodyne produce electronically scanned array radars, which provide high-performance radar systems and include an integrated, user configurable software system for controlling the radar. They are used for the purposes of detecting and tracking targets in both the air and on the ground.
Benefits	An all-electronic screening radar system that can help improve border situational awareness. They are portable easily portable and user friendly and are already being integrated onto autonomous surveillance towers.
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 3: Integrated Fixed Towers (IFT) system	
Description	The IFT system provides border surveillance by integrating different radar, camera and sensor capabilities to increase situational awareness and provide intelligence to border guard patrols. Elbit Systems utilises AI for its identification and classification technology to facilitate C2 (TORCH command and control).
Benefits	Provides operators with 'greater situational awareness in challenging geographical areas, providing them a more accurate understanding of any given situation and the ability to act with speed and accuracy'.[253]
Challenges	The system requires further development and testing with field conditions in order to further develop the AI capabilities and fully exploit the potential of this integrated system to operate autonomously.

[253] Elbit Systems of America (2020).

D.5. Heterogeneous robotic systems

Current Capability	Pathway to Adoption	Desired Capability
Whilst a number of robotic systems are already being used in border security operations, there is no fully functional autonomous border surveillance system in place that employs different unmanned and robotic aerial, water-based and ground vehicles as part of an interoperable network. Current capabilities are limited to individual systems that have limited integration of platform and sensor data, requiring significant human resources to operate and supervise the systems.	The key to developing the desired capability will be in integrating both legacy and new systems and ensuring that integrated networks of unmanned vehicles can interoperate effectively, with one operator able to control or supervise a group of – rather than individual – vehicles. These systems will need to be iteratively developed from smaller teams on more focused tasks, subsequently growing towards larger teams conducting more complex or uncertain tasks.	In the next few years, there is an intention from various developers and border security authorities to implement a heterogeneous robotic system, which provides a semi-autonomous border surveillance system with integrated swarms of aerial, water surface, underwater and ground vehicles incorporated directly into the network. Some developers believe that beyond this, there is the opportunity to enhance these types of robotic systems with detection capabilities for early identification of criminal activities at border and coastal areas, along with marine pollution events. The development of such capabilities for border security and law enforcement is likely to go hand in hand with military R&D and the development of improved command and control (C2) architectures that allow operators to control or supervise a multitude of unmanned vehicles.

Implementation factors

Category	Requirements	Barriers to adoption
Personnel & Training	The capability is expected to operate with a large degree of autonomy that will not require a large number of personnel to operate. It is expected that the capability will include autonomous coordination capabilities, with end users focusing on developing the overarching strategy, plans and performance requirements, as well as supervising and	There is likely to be a significant burden in training personnel to work alongside these systems, as they replace functions traditionally carried out by human operators. This burden will be a direct result of the increased sophistication of the new systems and the need to adapt training to enable personnel to operate effectively alongside robotic systems and interpret their data. This

Category	Requirements	Barriers to adoption
	directing the system where desirable or required (e.g. in cluttered or highly complex operational environments).	is likely to be a barrier due to the cost and the number of personnel available to be trained in using these systems. However, personnel training requirements will depend on the advances in C2 architectures and the ability of systems to coordinate autonomously, since more sophisticated capability would reduce the number of required personnel to operate the same system or number of vehicles.
Infrastructure, Equipment & Logistics	The deployment of AI and integrated robotic systems requires robust communication networks and network infrastructure.[254] The capability will require the development of new technical solutions and a substantial investment in the hardware and infrastructure to operate and maintain systems such as the unmanned vehicles. There are some opportunities to reduce costs in some areas, particularly in terms of freeing up costs associated with the labour of human operators. On the other hand, achieving satisfactory levels of autonomy requires investment in more expensive robotic systems, though the costs associated with such systems is likely to decrease in the near future due to mass production.[255]	Further to potential barriers in relation to limited financial resources available for the necessary technological investments, there are also operational challenges in replacing existing systems and the associated challenges of such a wide-scale replacement (although mass production of robotics could mitigate this to an extent).[256] Finally, the requirement for the systems to be secure from both cyber and physical attacks, including a guarantee that the AI does not get compromised, are likely to be barriers to the wider use of such systems.[257]
Information	The system will require an advanced data fusion capability and ability to process disparate streams of sensor data from the individual vehicles in the system. The system is also likely to require extensive testing in different operational environments, with access to relevant contextual and	Data protection safeguards and regulatory barriers could represent barriers for technology developers and end users to ensure sufficient availability of data for the development and testing of the system. Currently, data fusion and C2 infrastructures are not sufficiently advanced to ensure the system is able to

[254] WP1-INT10.

[255] WP1-INT06.

[256] WP1-INT10.

[257] WP1-INT10.

Category	Requirements	Barriers to adoption
	environmental information needed for such testing to ensure robustness of the system for various conditions and operational environments.	operate at the desired capability levels. As such, there could be various technical challenges and barriers that will need to be addressed for the system to operate efficiently and effectively.
Organisation	It is necessary to establish a comprehensive understanding of the technical advantages as well as risks associated with novel AI-enabled solutions, particularly with regards to complex technical systems and surveillance technologies.[258] This is likely to have implications for how organisations ensure they are set up to integrate these systems and manage the new risks that they bring. Learning about and using these systems will make it possible to mitigate and cope with any risks identified in relation to the system.[259]	Uncertainty concerning new technologies and lack of awareness concerning the benefits of AI represent a cultural/psychological barrier to organisations being willing to invest and make effective use of AI solutions such as heterogeneous robotic systems.[260] Lack of public or political support for the operation of advanced robotic surveillance systems could also limit the ability of organisations to invest in developing relevant organisational capacities and expertise.
Regulatory/Legal /Ethical	Regulations will need to be adapted to enable the use of heterogeneous systems and to provide appropriate authorisation for autonomous vehicles and data collection.	Heterogeneity of the regulatory framework has been a notable challenge. Obtaining relevant authorisations for the operation of this type of system – including flight authorisation for UAVs and authorisation to capture images and video footage – has to take place in line with strict regulations, including GDPR.[261] The implementation of AI in customer relations is heavily burdened by ethical challenges. E.g. biometrics challenges, adversary AI and some trafficking networks are already using extensive data mining.[262]
Technology Performance	While the technology readiness levels are high with regard to AI performance in passive intelligence, systems will require	There are not many technological barriers to implementing such systems, given they are already in development, particularly for passive intelligence collection. However, active intelligence-

[258] WP1-INT13.

[259] WP1-INT13.

[260] WP1-INT03.

[261] WP1-INT03.

[262] WP1-INT10.

Category	Requirements	Barriers to adoption
	continued investment and research into improving AI performance in active intelligence.[263]	gathering systems are less well developed and there remain technological barriers to their adoption. Further investment in AI performance within active intelligence-gathering systems is required and could create a barrier to their adoption.
Other	No other requirements were identified.	No other barriers were identified.

Illustrative use cases

Use Case 1: Roborder	
Description	Roborder is an autonomous border surveillance system encompassing an AI-enabled heterogeneous robotic capability including aerial, surface, underwater and ground vehicles. The system includes data fusion and processing, object detection and decision-support capabilities.
Benefits	This system is expected to provide 'early identification of criminal activities at border and coastal areas along with marine pollution events'.[264]
Challenges	Roborder is still under development and requires further testing and investment in order to produce a deployable system.

Use Case 2: Maritime Autonomous Platform Exploitation (MAPLE)	
Description	The purpose of this joint project between Qinetiq, the UK Defence Science & Technology Laboratory (Dstl) and the Royal Navy is to develop and test an integrated and autonomous system of unmanned vehicles that are a seamless part of maritime command and control systems.[265]
Benefits	Unmanned maritime vehicles have been identified as one way in which single Navy ships could have the same level of impact as multiple ships that lack operate unmanned vehicles. Currently the deployment and operation of a collection of these unmanned systems would require multiple operators, so these systems could substantially reduce the resource burden on ships.
Challenges	The key challenges that have yet to be overcome for this system are the development of an appropriately secure and capable communications architecture, the security of the system to expected threats from adversaries and the safe operation of these systems, particularly in congested environments.

[263] WP1-INT06.

[264] Roborder.eu (2020).

[265] Smith & Biggs (2018), Smith & Biggs (2019).

D.6. Small unmanned aerial systems (sUAS)

Current Capability	Pathway to Adoption	Desired Capability
A range of UAS are already employed by border security authorities around the world. These capabilities include the use of AI to augment the ability of drones to identify and track targets. A number of countries are working with contractors to develop and test various AI-based technologies that can improve the use of drones, particularly target identification and tracking, and autonomous flight in challenging environments without the need for human operators to be involved. These technologies are still in development, with some testing already underway.	UAS and sUAS are already a prevalent technology and the integration of AI-enabled capabilities to these platforms is the next step in their evolution. Substantial R&D is already ongoing in this area. Initially, advances in sUAS are likely to encompass the development of on-board sensors and the use of AI to provide object identification and recognition capabilities, as well as precision landing and take-off capabilities and improvements in propulsion systems to allow vehicles to operate longer and with enhanced resilience. Border security authorities should monitor developments in this area and identify opportunities to work with developers to test systems in various operational environments, in order to improve their potential use for border security operations.	In the next 5–10 years, there are likely to be significant advances in the integration of a range of AI technologies that will improve drone capabilities and provide real-time situational awareness to border guard patrols, including 'full-motion video, automatic target detection and geolocation'.[266] There are also likely to be improvements in the ability of sUAS to operate fully autonomously through AI-enabled and computer-vision-based precision landing capability, which enables a sUAS to launch from and land on static as well as moving platforms, such as ground vehicles.[267] Finally, sUAS will be equipped with real-time onboard processing of imagery and video, as well as neural networks for enhanced object detection and classification capability.

Implementation factors

Category	Requirements	Barriers to adoption
Personnel & Training	New UAS that are already available are relatively easy to operate, so there is not expected to be a significant skills or training burden for personnel. Simple training is likely all that will be needed to upskill border guard personnel in how to	Given the ease of operation, there are not expected to be many barriers to adoption for border guard personnel. There might be minor impediments in the employment or contracting of

[266] Planck Aerosystems (2019).

[267] Planck Aerosystems (2020).

Category	Requirements	Barriers to adoption
	operate these drones. The development of AI will also reduce the requirements for training as drones will be able to operate autonomously with humans in the loop.[268] However, UAS will require appropriate maintenance and technical support to ensure they remain serviceable and able to operate effectively.	appropriate technical support, but this should be considered as part of any procurement process.
Infrastructure, Equipment & Logistics	There is a requirement to train UAS and their embedded AI to make sure they can perform the desired data gathering and collection.[269] For EBCG forces, it could be important to develop proprietary tools to be able to train the system without relying on US and Chinese technologies. This will ensure ownership of the technology and the ability to further develop the system within Europe.[270] EBCG should also consider what the requirement will be to migrate all platforms onto a common infrastructure that will enable the solution to be as scalable as possible. [271]	Currently there is a dependency on hardware from non-EU suppliers, specifically Chinese UASs. These are by far the most cost-effective solution on the global market and their low cost cannot be matched by European developers or suppliers. This creates risks as many of the sUAS from China collect and transmit data back to their parent companies in China, which Chinese authorities can then access.[272] Governments do not want to invest substantial sums in the required infrastructure to operate large fleets of drones. This will have an impact on the scalability of any solution and the ability to operate across a common European infrastructure.[273]
Information	The most important component for this capability is the information and data gathered by the UAS.[274] There will be a requirement to invest time and effort into training the AI-	Whilst there is an information security risk if non-EU manufactured drones are used, security solutions are already available to overcome these, so it should not be a significant barrier to adoption.[276] The most significant challenge will be in gathering

[268] WP2-INT04.

[269] WP2-INT11.

[270] WP2-INT11.

[271] WP2-INT11.

[272] WP2-INT11.

[273] WP2-INT11.

[274] WP2-INT11.

[276] WP2-INT11.

Category	Requirements	Barriers to adoption
	enabled UAS to capture and analyse information appropriately for the needs of border security. Given that many sUAS come from China, and the risk that these units might automatically send information back to their manufacturer, there is the need to develop appropriate security measures such as secure VPNs and firewalls to make sure that the information gathered remains with the operator.[275]	appropriate data from which the AI can be trained to operate effectively and reliably in a border security context.
Organisation	No specific organisational requirements to adopting this technology were identified.	No specific organisational barriers to adopting this technology were identified beyond the wider cultural barriers to adopting AI-based capabilities.
Regulatory/Legal /Ethical	A number of regulations related to the operation of smaller drones will need to be considered in establishing this type of capability. However, drones are already used by border security organisations so these requirements should already be relatively well understood, providing an enabler to successful employment of AI-enabled UAS capabilities. Similar to other surveillance technologies (see Section D.4 and D.5), social acceptance of the wide use of drones will also be an important enabler to the wider use of this technology.[277]	Public and political discourse in relation to the use of drones for surveillance is already characterised by significant controversy, despite an increasing use of drones in various functions including by the public sector. There are a number of potential legal and ethical barriers that exist to the use of UAS, especially when enabled by AI, including implications for privacy and other human rights safeguards. The impact of such implications will be dependent on the type of capability being used and context within which it is performing its function.[278] Apart from ensuring ethical and human rights safeguards, regulatory barriers exist in different areas such as production and deployment of UAS in different jurisdictions.[279] Such barriers will require further consideration as the capability is developed.

[275] WP2-INT11.

[277] WP1-INT12.

[278] WP2-INT04.

[279] WP1-INT12.

Category	Requirements	Barriers to adoption
Technology Performance	Multi-modality is a focus for the future of sUAS, as well as the integration of small neural networks on board, which will enable greater autonomy and the training of the system through ML.[280] The performance of AI-enabled UAS depends on their navigation and object identification and classification ability. For classification there are several tasks against which performance can be assessed and improved. For navigation, the mapping of the environment by the UAS is compared to actual maps to improve performance. As one might expect, there is variation in the performance of different UAS, but the detection and precision of visual sensors and object recognition aim to reach around 90%.[281] As 5G technology becomes more prevalent, this should improve UAS performance in terms of communications.[282]	The use of drones remains very limited at the moment. Most sUAS cannot fly for longer than 20 minutes, which limits their range and potential application. Fixed wing vehicles are able to fly for longer periods but are more difficult to operate at present. There are several technological barriers to developing appropriate hardware and software to improve performance.[283] From an AI perspective, the greatest challenge is embedding the algorithm on-board the sUAS and the limited hardware that can be carried, to ensure that it can continue working where there are poor communications.[284]
Other	No other requirements were identified.	No other barriers were identified.

Illustrative use cases

Use Case 1: Planck Aerosystems sUAS	
Description	Planck Aerosystem's small autonomous unmanned aerial systems (sUAS) are drone technologies embedded with AI and computer vision for take-off and precision landing on static and moving platforms, real-time image processing, object recognition and threat detection.

[280] WP2-INT04.

[281] WP2-INT11.

[282] WP2-INT11.

[283] WP2-INT04.

[284] WP2-INT11.

Use Case 1: Planck Aerosystems sUAS	
Benefits	These UAS have the potential to enhance ‘capabilities for surveillance, reconnaissance, real-time situational awareness, and force protection’.[285] They also provide an enhanced capability for take-off and landing compared to most drones currently employed.
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 2: Robotic hummingbirds	
Description	A hummingbird-like robot combines AI with flexible wing structures, allowing it to reach areas which normal drones could not access, it does this by effectively creating a map of its surroundings without seeing them, and adapting/learning based on its experience.
Benefits	This type of UAS is very small and can access hard to reach areas, especially those which are not appropriately mapped. The technology is already being used to help with search-and-rescue missions, and covert Intelligence, Surveillance and Reconnaissance (ISR) operations.
Challenges	These drones have limited persistence due to their small size. This also limits the amount of sensors or hardware that are incorporated onto this package.

Use Case 3: Raven and Puma UAS system	
Description	AeroVironment produces small UAS technologies with automated target detection software that can be used for border surveillance, providing real-time automated target detection and better situational awareness.
Benefits	This UAS is capable of both day and night observation. They are particularly useful for ‘low-altitude intelligence, surveillance, and reconnaissance missions that depend on rapid deployment and pinpoint manoeuvrability’.[286]
Challenges	As for many small UAS, their range and endurance are limited by the size of the UAS (although this size is also what makes them easily deployable and highly manoeuvrable).

[285] Planck Aerosystems (2020).

[286] AeroVironment (n.d.).

Use Case 4: Bat-inspired robot	
Description	Tel Aviv University's Bat Lab has developed an autonomous robot that uses bat-inspired echolocation to map and navigate through unknown environments. The echolocation enables the robot to map borders of objects and determine the path around different objects.
Benefits	Using echolocation has significant potential for developing advanced obstacle avoidance, object recognition and path planning in unknown environments. It is expected that this type of technology will have great applicability in low-visibility environments where other sensors may not be as accurate. It could be employed on drones for conducting search and rescue in caves or guidance of autonomous drones in poor weather.[287]
Challenges	Currently the capability has only been deployed on an unmanned ground vehicle and has yet to be fully developed and tested for use on UAS. However, this is part of the next stage of development for this technology.

Use Case 5: AI reconnaissance platform (Intelleuron)	
Description	Intelleuron is developing drone technology with an adaptive reconnaissance platform that would provide UAS with the ability to automatically detect potential threats, contributing to situational awareness particularly in remote border areas.
Benefits	This technology is focused on providing a capability that can 'automatically locate potential threats like armed smugglers and operate across every type of terrain and weather'.[288]
Challenges	No specific challenges noted beyond the general points raised in this roadmap.

Use Case 6: SURVEIRON (AEORUM)	
Description	SURVEIRON seeks to leverage the use of UAS to provide intelligent surveillance of urban soft targets and critical infrastructure as well as supporting decision making in crisis situations through the automated provision of intelligence. The system can deploy fleets of UAS to a chosen area to scan and analyse the environment with different detection techniques, and the data is then transferred back to a 3D mapping environment within the control centre.
Benefits	This technology provides a centrally controlled UAS capability for help with detailed mapping of remote environments, even in complex areas, such as an urban setting. The system is also capable of providing intelligence analysis of the environment and recommending courses of action (e.g. water required to extinguish a fire). It is intended for use in the prevention and

[287] d'Estries (2018).

[288] Corrigan (2018).

Use Case 6: SURVEIRON (AEORUM)	
	management of potential disasters in urban environments and for critical infrastructures surveillance.[289] This could have applicability to a border security setting. The project is funded by the European Commission.
Challenges	This system is still under development and has yet to be fully developed such that it could be deployed on border security operations. The current system is also focused on disaster management and critical infrastructure surveillance, so may require some adaption for border security.

[289] European Commission (2016b).

D.7. Predictive asset maintenance

Current Capability	Pathway to Adoption	Desired Capability
AI-enabled predictive analytics capabilities are already available, including models that can predict patterns in logistics resupply and asset maintenance. This is particularly true within the logistics industry. The challenge at present is identifying how this can be best utilised within the context of border security. A number of relevant AI-based technologies and software are available to support this capability but require testing and adapting to the specific requirements of EBCG.	EBCG should seek to understand how this technology is already being used in other sectors and what the requirements are for this type of AI-enabled capability within a border security context. From this they will be able to identify potential AI-based solutions that can be adapted to their needs.	EBCG can expect that in the future, software will be available with AI and ML algorithms that can analyse data from various sensors and notify users about possible sub-optimal factors in the operations and logistics workflows, such as factors that could lead to potential damage or failure of a technical system. These technologies will be able to notify a human operator of potential risks and they can decide whether to investigate or take further action. From a logistics perspective, AI is likely to enable greater autonomy in predicting and automating the resupply and maintenance of border security assets, without need for close manual human supervision (although a level of oversight might still be preferred for safety or policy reasons).

Implementation factors

Category	Requirements	Barriers to adoption
Personnel & Training	Personnel will need to be trained to understand their role within asset maintenance and how to work alongside this type of AI-based system. However, predictive asset maintenance systems are designed to be intuitive and operate with a large degree of autonomy.	There is a minor barrier in implementing the training for existing personnel, but this is not expected to be a substantial challenge or undertaking.
Infrastructure, Equipment & Logistics	There are certain hardware and software infrastructure requirements for setting up this type of system. There are likely to be limited costs associated with implementing the relevant software and hardware infrastructure requirements	The initial stage of adapting the relevant AI algorithm to the end user's requirement relies on initial consultation with experts who have extensive technical knowledge of the end user systems and processes for asset maintenance. While this is a crucial step for

Category	Requirements	Barriers to adoption
	for the solution, for example, IT equipment and cloud services.[290] In most cases, existing IT infrastructure should provide sufficient infrastructure for data storage.[291] However, there will be a requirement to implement appropriate security measures.	customising the algorithm to the system's mode of operation, the availability of relevant experts could be limited.[292] The large amount of data storage required, and the potential sensitivity of this data, could create another challenge for ensuring data security.[293]
Information	It is expected that there will be information requirements for implementing such a system in terms of ensuring access to historical and technical data from systems to be monitored, but these will be specific to the solution being implemented and depend on the end user's requirements for the capability.	As described above, data security is likely to be a challenge for any asset maintenance software, as mentioned in the previous row. Beyond this, no further barriers were identified for this technology.
Organisation	Effective operation of a predictive asset maintenance solution requires that the internal organisational policies and procedures of the end user for system maintenance are aligned with the solution being considered.[294] Therefore, it might be necessary for processes to be developed to account for the changes that will result from implementing such an asset maintenance system.	End users with complex technical systems, supply chains and financial and contractual models are typically not well designed to accommodate a predictive asset maintenance analytics solution. This is likely to create substantial barriers to the adoption of this capability in complex organisations. For example, end users might be able to request a subcontractor replace equipment that has failed under existing contractual obligations; however, subcontractors might not have the same obligations when equipment is predicted to fail by the algorithm, rather than actually fail in reality.[295]

[290] WP1-INT11.

[291] WP1-INT11.

[292] WP1-INT11.

[293] WP1-INT11.

[294] WP1-INT11.

[295] WP1-INT11.

Category	Requirements	Barriers to adoption
Regulatory/Legal /Ethical	An organisation wishing to implement such a solution will require appropriate data access and sharing agreements for the area to which the AI solution is being applied.	Overcoming the requirement for any legal agreements for data sharing is likely to be a barrier that would take time to overcome given the challenges of data sharing.
Technology Performance	Predictive asset management relies on access to a wide range of sensor data. While historical data is beneficial for improving the initial algorithm optimisation process, it is not required for the solution to operate effectively.	In order to maximise the effectiveness of the system, the data on which the system relies will need to be technologically accessible.[296] There might be challenges in adapting legacy data in manual or old formats, such that they can be used by any new AI-based system.
Other	No other requirements were identified.	No other barriers were identified.

Illustrative use cases

Use Case 1: SparkPredict	
Description	SparkPredict is a machine learning-enabled advanced analytics platform focused on analysis of sensor data to provide insights to decision makers. The platform serves to identify sub-optimal operations or potential system failures before they occur.
Benefits	The prime benefit of SparkPredict is to save money and time by identifying sub-optimal operations and avoiding maintenance failures before they happen. This ensures that the relevant systems should avoid catastrophic failure, avoid downtime and thus reduce the cost of operations.[297]
Challenges	This technology has not been actively used in the border security sector and as such, there are likely to be some challenges to overcome in implementing such a solution, particularly the replacement of, or integration with, legacy systems.

Use Case 2: UNFRAUD (TXN SRL)	
Description	UNFRAUD seeks to apply AI to improve cybersecurity through recognising fraudulent behaviour, particularly in the application to various types of online fraud.

[296] WP1-INT11.

[297] SparkCognition (2020a).

Use Case 2: UNFRAUD (TXN SRL)	
Benefits	UNFRAUD uses deep learning AI that can detect even sophisticated fraud strategies. This means that it can reduce the cost of anti-fraud services substantially. This system is currently contributing to the fight against international money laundering schemes and seeks to safeguard bank welfare by reducing chargeback procedures as a result of payment card fraud.[298]
Challenges	This system uses pattern recognition AI to be able to detect anomalies and recommend actions; however, it is not currently used in a fashion that is conducive with border security predictive asset maintenance. Therefore, it would need to be adapted to suit this function, which could be a substantial undertaking.

Use Case 3: IBM Resilient Security Orchestration, Automation and Response (SOAR)	
Description	IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform is a platform for orchestrating and automating incident response processes. IBM Resilient SOAR Platform integrates with an organisation's existing security and IT systems to provide valuable intelligence and incident alerts, which enables a rapid and adaptive response to complex cyber threats.
Benefits	This system provides enhanced intelligence and incident context, and enables greater responsiveness to particular events, current within the cyber realm.[299]
Challenges	It is expected that significant adaptation of this system would be required in order to make it suitable for assessing potential threats and enabling asset maintenance.

[298] European Commission (2018c).

[299] IBM Research (2020).

D.8. Object recognition

Current Capability	Pathway to Adoption	Desired Capability
Currently, a number of object detection and recognition systems are used as part of border security operations. These systems are already able to automatically detect and identify objects as they pass through border security screening processes and sensors. However, these systems require a substantial amount of resource and time to train the models behind such systems before they can be reliably employed. There is ongoing development to address the current challenges through the use of AI.	AI-based systems require different types of sensors from which to draw the data for object recognition. These different sensors pose different challenges and require different AI algorithms to enable the processing of image data. Initially, visual and thermal object recognition will continue to be developed and improved. Systems integrating advanced radar and AI-based technologies are also under development, but are likely to be more challenging to implement, so are expected to be available after visual and thermal systems.[300]	In the near term, AI technologies will enable the automation of the data generation process from which models can be trained, substantially reducing the currently resource-intensive process of training object identification models. AI is also expected to continue to improve the accuracy of existing object recognition systems, which will reduce the reliance on human resources for the classification and labelling of model training data. Initially, it is expected that these developments will happen in visual and thermal object recognition, followed by radar object detection.[301] Developers believe that the creation of radar signatures will increase object recognition accuracy and speed, when compared to cameras. The optimal desired capability is likely to arrive in the form of an integrated system that draws on multiple sensors.[302]

[300] WP2-INT01

[301] WP2-INT01.

[302] WP2-INT01.

Implementation factors

Category	Requirements	Barriers to adoption
Personnel & Training	Fewer personnel will be needed in object identification functions. There is significant interest in using AI to automate object recognition and reduce the cognitive burden on human operators, as AI-based object recognition technologies can perform object recognition functions regardless of the length of time it is in operation. This will enable border security resources to focus more on the functions that require human intervention (e.g. dispatching operators pending the validation of an alert from an AI system). This will increase efficiency and automate significant parts of the process of object recognition.[303]	The AI systems should be relatively intuitive to use and require little training to operate or work with. However, the technology is not mature enough to operate without human involvement in the process.[304] The system will require human validation, which could create a barrier due to the need for greater human-machine interaction and the development of appropriate interfaces.
Infrastructure, Equipment & Logistics	The development of an integrated object recognition system would require the different sensor or data capture platforms to be able to communicate with each other and build a usable imagery repository.[305] Any IT hardware and software will also have to be capable of storing and processing large amounts of image data.	Given the need for human validation, any systems will require the infrastructure and equipment system to be such that human operators can be included as part of the validation process. Once the technology reaches sufficient maturity that human validation is no longer needed, this might become less of a barrier.
Information	Online databases have been previously used to generate datasets for training an AI-based object recognition system, though in practice this has limitations for the ultimate effectiveness of the object recognition algorithm. In order to develop the most effective object recognition capability, it has been recommended for organisations to build their own	The greatest barrier will be ensuring appropriate data can be accessed or developed to train the AI-based system effectively. The use of synthetic data should significantly reduce the cost of training object detection models. However, some limited costs may be incurred because of the requirement to ensure diversity and consistency of the data and quality of the models.[307]

[303] WP2-INT01.

[304] WP2-INT01.

[305] WP2-INT01.

[307] WP1-INT01.

Category	Requirements	Barriers to adoption
	representative data or provide access to more realistic images to improve recognition capabilities. The training data set will need to be developed such that the area being scanned can be increased as AI learns, and layers can be added that will perfect the technology over time.[306]	
Organisation	No specific organisational requirements were identified for this capability.	No specific organisational barriers were identified for this capability, beyond the broader issue of cultural acceptance of AI.
Regulatory/Legal /Ethical	There is likely to be a requirement to ensure that this technology adheres to all the appropriate regulations around using visual and radar sensors for object recognition.	Data availability is a key challenge for the development of object recognition systems, due to classification and information security concerns from many government agencies.[308] These regulations are likely to impact on the potential effectiveness of any system, especially when related to the identification or recognition of people. There are specific regulations regarding radar frequencies that can be used on human beings. This could limit the utility of radar as part of this type of system. Finally, there are likely to be cultural and ethical challenges because AI is perceived to be taking away jobs within the border security sector.[309]
Technology Performance	Object recognition is already being developed and used in different sectors. Early lessons with this type of system show that the key to achieving the desired level of performance is to ensure consistency and diversity of data.[310] This increases the accuracy and reliability levels of object recognition.	Whereas 3D imaging is considered more accurate, training models for three-dimensional imaging is significantly more resource-intensive and technologically challenging than two-dimensional modelling.[311]
Other	No other requirements were identified.	No other barriers were identified.

[306] WP2-INT01.

[308] WP1-INT01.

[309] WP2-INT01.

[310] WP1-INT01.

[311] WP1-INT01.

Illustrative use cases

Use Case 1: Synthetik object recognition	
Description	Synthetik's object recognition technology utilises computer vision and deep-learning methods to generate and annotate synthetic model training data. This is aimed at facilitating automated object recognition and threat detection in security checkpoint operations.
Benefits	This system is able to 'automatically detect multiple objects at the same time during the property screening process at an airport, enhancing current human-based capabilities'.[312]
Challenges	This system is being developed by a US-based start-up and is still going through a proof of concept and early development of the system. As such, it still requires further development and any adaptation to the European market may require further investment and development.

Use Case 2: AI weapon detection (ZeroEyes)	
Description	ZeroEyes is marketing an AI system for real-time gun detection for use by law enforcement agencies. The system can detect a weapon using camera imagery and – through integration with local emergency services – notify police forces to respond. The system can also connect to existing security cameras and building infrastructure such as automatic door locks.
Benefits	This system aims to provide an enhanced early warning of potential threats from individuals who could be carrying a gun and can draw on existing cameras and infrastructure to identify objects of interest and alert emergency services.
Challenges	The system and company are very focused on providing a highly capable gun-detection capability. The AI solution will be limited to gun detection for the foreseeable future.

Use Case 3: AI weapon detection (Athena)	
Description	Athena security uses visual and thermal cameras and AI technology for gun detection, including concealed weapons. The purpose of the system is to facilitate automated gun detection and increase security in public spaces. Since the break-out of COVID-19 the company have also added temperature detection as part of their system.
Benefits	This system provides enhanced early warning of individuals holding weapons and can also detect people with abnormal body temperature during border control operations. The system connects directly to existing cameras.

[312] U.S. Department of Homeland Security (2019).

Use Case 3: AI weapon detection (Athena)	
Challenges	No challenges were identified for this particular use case.

Use Case 4: Brain-inspired automated visual object discovery and detection	
Description	An AI system for object identification that mimics human visual learning processes to train and develop the AI system to detect different objects.
Benefits	In contrast to AI computer vision systems that are task-specific, this system is able to learn and identify new objects intuitively rather than based on programming through human input.
Challenges	This is a task-specific system with a limited ability to identify beyond what they have been trained and programmed to by humans.[313]

Use Case 5: Adaptive automated threat recognition for baggage security	
Description	This system employs machine learning for adaptive automatic threat recognition within 3D computed tomography images, and is used for baggage security screening.
Benefits	The AI has demonstrated good performance in both recognition and adaptation, with the probability of detection of a threat inside baggage at around 90% and a probability of a false alarm below 20%. This use case has shown the ability to adapt to varying types of material (even unknown materials, which are not available in the training data), probability of detection requirements and scales of threat object.[314]
Challenges	This system is focused on the detection of threat objects inside baggage and relies on X-ray CT baggage scanning infrastructure to scan the relevant baggage.

[313] UCLA (2018).

[314] Wang et al. (2020).

D.9. Geospatial data analytics

Current Capability	Pathway to Adoption	Desired Capability
Currently, the process of analysing satellite imagery is a resource intensive activity that relies heavily on analysts. These analysts require substantial training and experience built up over several years. Some developers are already using AI to advance the satellite imagery process, with ML tools rapidly emerging as the standard for analysing geospatial data.[315] Currently, there is some limited use of this capability in various functions, such as disaster relief and military operations. However, these developments have yet to achieve full automation and merely support the human analyst.	The use of geographical tools by national border authorities is increasing but remains at a relatively low level. Frontex is currently using geodata for multiple purposes, among others to counter illicit trafficking and smuggling, and the development of this system should continue.[316] The next steps will be the integration of AI to further exploit the use of geospatial data. To achieve this, it will be important that organisations such as Frontex work with AI developers to train and develop the AI systems appropriately and achieve a high level of capability.	This is an area where AI is expected to continue its development over the next few years. In the near term, there is likely to be a transition period as AI models are employed more broadly for automated labelling and classification of geospatial data. Human analysts will increasingly be supported by AI and over time, the intent is that these models will be able to operate autonomously in the analysis of satellite imagery for automated target detection and object recognition. Deep learning methods will also reduce the need for extensive manual training of algorithms, which will speed up automated object recognition as AI models become capable of teaching themselves to identify characteristics of new objects, areas or targets.[317] The longer term aim for this type of AI is to enable the development of an integrated real-time tracking and threat identification system that can improve planning and logistics in border security, as well as other domains. Such systems will provide an integrated decision-support system that provides real-time analysis of geospatial data streams to allow operators to gain understanding

[315] Wegner et al. (2018).

[316] Cantens (2020).

[317] Aerospace Technology (2019).

Current Capability	Pathway to Adoption	Desired Capability
		of threats in real time and thus decrease response times.[318]

Implementation factors

Category	Requirements	Barriers to adoption
Personnel & Training	The reliance on human analysts should reduce, though it is expected that analyst input will remain a requirement, at least initially, to ensure appropriate validation of the model's performance and outputs. As such, training and skills requirements for this capability are focused on the ability of human operators to use AI-based systems effectively to support them in sifting large amounts of imagery (i.e. understanding how the model works and interpreting its outputs).	No significant personnel or skills-related barriers were identified. However, there could be challenges in the changing roles that imagery analysts will play and how they work alongside the AI systems that take on some of their previous responsibilities. This is likely to require some training/adjustment.
Infrastructure, Equipment & Logistics	From a technical perspective, in order to access the appropriate geospatial data, relevant infrastructure will need to be put in place that allows end users to make use of GIS software, the Internet and mobile phone networks to automate the collection and sharing of relevant geospatial data.[319] Steps are being taken to address such requirements in the European context. For example, the European Commission's Infrastructure for Spatial Information in the European Community (INSPIRE) project is developing an infrastructure built for the purposes of spatial-information-sharing between public authorities.	Whilst the data already exists, the infrastructure and equipment required to enable geospatial data to be analysed through AI systems will likely carry high cost for end users to both procure, install and operate. However, relevant infrastructure and equipment might already exist to some extent in government organisations, so barriers might differ for end users in different contexts.
Information	To make effective use of geospatial data, the EU is already establishing common standards for certain types of geodata	Currently, the data relevant to border security is not being collected or considered as part of Project INSPIRE.

[318] European Commission (2020c).

[319] Cantens (2020).

Category	Requirements	Barriers to adoption
	and ensuring the data is appropriately accessible as part of Project INSPIRE. There will need to be common standards in the geodata required by border security in order to make best use of any AI data analytics system.[320]	
Organisation	No organisational requirements were identified.	No organisational barriers were identified.
Regulatory/Legal /Ethical	Regulations for the appropriate sharing of AI and the underpinning geospatial data will need to cover all relevant aspects of this capability within a border security context. Regulations will also need to be adapted to enable higher resolution geospatial imagery, which it currently does not.	The regulatory environment is a barrier for the development and wider adoption of AI. The regulations around the use and sharing of geospatial data are also a potential barrier. Due to restrictions imposed on the exports of AI solutions by the current US administration, in Europe it is only possible to support adoption through individual components of AI solutions, such as providing training data.[321] Current data protection rules limit the resolution of imagery that can be used, which is likely to continue to hinder the performance of any imagery analysis (see Technology Performance).
Technology Performance	Geospatial data is already available and highly prevalent. The availability of extensive amounts of geospatial imagery is ensured e.g. through Maxar's GBDX platform, which is a key enabling factor.	The quality of data being used for geospatial analysis is a potential barrier, as high resolution of imagery is key for the effectiveness of analysis. While there has been increasing demand for high resolution data, progress in this area is limited due to data protection requirements and regulatory barriers.[322]
Other	No other requirements were identified.	No other barriers were identified.

[320] Cantens (2020).

[321] WP1-INT08.

[322] WP1-INT08.

Illustrative use cases

Use Case 1: Global Automated Target Recognition (GATR)	
Description	GATR is an AI model for automated labelling and classification of geospatial data. This is aimed at enabling the analysis of satellite imagery for automated target detection and object recognition.
Benefits	'Deep learning methods reduce the need for extensive algorithm training by automating object recognition. The AI-based GATR teaches itself the identifying characteristics of an object area or target'.[323]
Challenges	Regulations around the resolution of satellite imagery currently limit the performance of this system.

Use Case 2: RoadTagger	
Description	The system uses AI to analyse satellite imagery, tag road features in digital maps and thereby improve GPS navigation. This could improve planning, logistics and disaster relief.
Benefits	This system is able to 'help humans rapidly validate and approve continuous modifications to infrastructure in datasets such as OpenStreetMap, where many maps don't contain lane counts or other details'.[324] This technology aims to substantially reduce the costs involved in creating detailed maps by, for example, using cameras fixed onto cars that drive around taking images.[325]
Challenges	This technology is still under development and the accuracy of some features require further improvement.[326] This is partly due to the resolution of the satellite imagery being used to help train this system.

[323] Aerospace Technology (2019).

[324] Matheson (2020).

[325] Green Car Congress (2020).

[326] Green Car Congress (2020).

References

Ackerman, Evan. 2019. ‘Delivery Drones Use Bird-Inspired Legs to Jump Into the Air’. IEEE Spectrum, 17 January 2019. As of 11 September 2020: https://spectrum.ieee.org/automaton/robotics/drones/delivery-drones-use-birdinspired-legs-to-jump-into-the-air

Ada Lovelace Institute. 2019. ‘Beyond face value: public attitudes to facial recognition technology’. London: Ada Lovelace Institute. As of 11 September 2020: https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

Aerospace Technology. 2019. ‘Lockheed Martin automates satellite image analysis’. Aerospace Technology, 7 June 2019. As of 11 September 2020: https://www.aerospace-technology.com/news/lockheed-martin-satellite-image-analysis/

AeroVironment. N.d. ‘Unmanned Aircraft Systems’. Avinc.com. As of 11 September 2020: https://www.avinc.com/uas/sensors-capabilities/about

ABC4EU (homepage). 2020. As of 15 June 2020: http://abc4eu.com/

ABC4EU. 2016. ‘Automated Border Control Gate for Europe: Project Newsletter 14 (1/2016)’. As of 9 April 2020: http://abc4eu.com/docs/abc4eu_v14.0_newsletter_public_draft.pdf

ABC4EU. 2018. ‘Automated Border Control Gate for Europe: Project Newsletter 20 (1/2018)’. As of 9 April 2020: http://abc4eu.com/docs/abc4eu_v20.0_newsletter_public.pdf

Accenture. 2017. ‘Technology Vision 2017: Shaping the New Digital Border Agency’. Accenture.com. As of 15 June 2020: https://www.accenture.com/_acnmedia/pdf-53/accenture-tv-borders-cut-intro-report.pdf

Anduril.com. 2020. ‘Sentry Tower’. Anduril.com. As of 09 April 2020: https://www.anduril.com/sentry-tower

Aratani, Lori. 2019. ‘DHS withdraws proposal to require airport facial scans for U.S. citizens’. Washington Post, 5 December 2019. As of 16 April 2020: https://www.washingtonpost.com/local/trafficandcommuting/dhs-withdraws-proposal-to-require-airport-facial-scans-for-us-citizens/2019/12/05/0bde63ae-1788-11ea-8406-df3c54b3253e_story.html

Aware. 2020. ‘AwareABIS’. Aware.com. As of 13 August 2020: https://www.aware.com/biometrics/aware-abis/

Baimukashev, Daulet, Alikhan Zhilisbayev, Askat Kuzdeuov, Artemiy Oleinikov, Denis Fadeyev, Zhanat Makhataeva & Huseyin Atakan Varol. 2019. 'Deep Learning Based Object Recognition Using Physically-Realistic Synthetic Depth Scenes'. *Machine Learning Knowledge Extraction* 2019,1(3):883–903. As of 11 September 2020: https://www.mdpi.com/2504-4990/1/3/51

Bathee, Yavar. 2018. 'The Artificial Intelligence Black Box and the Failure of Intent and Causation'. *Harvard Journal of Law & Technology*, 31(2):889–938. As of 7 September 2020: https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf

Beduschi, Ana. 2020. 'Human rights and the governance of artificial intelligence'. Geneva: Geneva Academy. As of 11 September 2020: https://www.geneva-academy.ch/joomlatools-files/docman-files/Human%20Rights%20and%20the%20Governance%20of%20Artificial%20Intelligence.pdf

Berryhill, Jamie, Kevin Kog Heang, Rob Clogher & Keegan McBride. 2019. 'Hello, World: Artificial Intelligence and its Use in the Public Sector'. OECD Working Papers on Public Governance. As of 11 August 2020: https://www.oecd-ilibrary.org/docserver/726fd39d-en.pdf?expires=1597127670&id=id&accname=ocid56013842&checksum=FA6B51AAD02ECA74D3777288B315470E

Binnedijk, Anita, Timothy Marler & Elizabeth M. Bartels. 2020. 'Brain-computer Interfaces: U.S. Military Applications and Implications, An Initial Assessment'. Santa Monica, Calif.: RAND Corporation. As of 7 September 2020: https://www.rand.org/pubs/research_reports/RR2996.html

Boston Children's Hospital. 2019. 'Harnessing multiple data streams and artificial intelligence to better predict flu'. Science Daily, 11 January 2019. As of 11 September 2020: https://www.sciencedaily.com/releases/2019/01/190111143744.htm

Boyd, Aaron. 2019. 'US Testing Autonomous Border-Patrol Drones'. Defenseone.com, 3 September 2019. As of 14 April 2020: https://www.defenseone.com/technology/2019/09/cbp-test-autonomous-drones-use-border/159604/

BusinessToday. 2019. 'AI robots to patrol India borders soon, prototype to come in December'. Businesstoday.in, 2 May 2019. As of 15 June 2020: https://www.businesstoday.in/technology/news/ai-robots-to-patrol-india-borders-prototype-to-come-in-december/story/342591.html

Businesswire.com. 2020. 'DataRobot Named a Visionary in the 2020 Gartner Magic Quadrant for Data Science and Machine Learning Platforms'. Businesswire.com, 19 February 2020. As of 9 April 2020: https://www.businesswire.com/news/home/20200219005572/en/DataRobot%C2%A0Named-Visionary-in%C2%A0the%C2%A02020%C2%A0Gartner%C2%A0Magic-Quadrant-Data-Science%C2%A0and%C2%A0Machine-Learning

Clabian, Markus & Andreas Kriechbaum-Zabini. 2017. 'ABC systems in Europe and beyond - status and recommendations for the way forward'. FastPass Write Paper, 13 September 2017. As of 11 September 2020: https://www.fastpass-project.eu/sites/default/files/FastPass_White_Paper_2017_final.pdf

Copstake, Ann. 2004. 'Natural Language Processing'. University of Cambridge, 2004. As of 31 July 2020: https://www.cl.cam.ac.uk/teaching/2002/NatLangProc/revised.pdf

Corrigan, Jack. 2018. 'DHS Contract Will Help Drones Automatically Spot Border Threats'. Nextgov.com, 10 May 2018. As of 11 August 2020: https://www.nextgov.com/emerging-tech/2018/05/dhs-contract-will-help-drones-automatically-spot-border-threats/148088/

Cox, Kate, Sarah Grand-Clement, Jacopo Bellasio & Giacomo Persi Paoli. 2017. 'From Lab to Field: Challenges and Opportunities for Operationalising Border Security Research'. Santa Monica, Calif: RAND Corporation. Non-public report.

Craglia, Max, A. Annoni, P. Benczur, P. Bertoldi, P. Delipetrev, G. De Prato, C. Feijoo, E. Fernandez Marcias, E. Gomez, M. Iglecias, H. Junklewitz, M. Lopez Cobo, B. Martens, S. Nascimento, S. Nativi, A. Polvora, I. Sanchez, S. Tolan, I. Tuomi & L. Vesnic Alujevic. 2018. *Artificial Intelligence – A European Perspective*. Luxembourg: Luxembourg. As of 15 June 2020: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC113826/ai-flagship-report-online.pdf

d'Estries, Michael.2018. 'Breakthrough robot navigates using bat-inspired senses'. Fromthegrapevine.com, 07 September 2018. As of 11 August 2020: https://www.fromthegrapevine.com/innovation/breakthrough-robot-navigates-using-bat-inspired-senses

Daniels, Jeff. 2018. 'Lie-detecting computer kiosks equipped with artificial intelligence look like the future of border security'. Cnbc.com, 15 May 2018. As of 11 August 2020: https://www.cnbc.com/2018/05/15/lie-detectors-with-artificial-intelligence-are-future-of-border-security.html

Dasgupta, Abhishek & Steven Wendler. 2019. 'AI Adoption Strategies'. Centre for Technology & Global Affairs, Working Paper Series – No. 9, March 2019. As of 6 August 2020: https://www.ctga.ox.ac.uk/files/aiadoptionstrategies-march2019pdf

DataRobot. 2019a. 'Machine Learning Applications for Health and Human Services'. Datarobot.com. As of 09 April 2020: https://www.datarobot.com/wp-content/uploads/2019/11/Machine-Learning-Applications-for-HHS.pdf

DataRobot. 2019b. 'Automated Machine Learning for Human Capital Management in the Government'. Datarobot.com. As of 09 April 2020: https://www.datarobot.com/wp-content/uploads/2019/11/AutomatedMachineLearningforHumanCapitalManagement_intheGovernment_Public-Sector__DataSheet_v5.6.pdf

DataRobot. 2019c. 'Automated Machine Learning for Medical Fraud Prevention in the Government'. Datarobot.com. As of 09 April 2020: https://www.datarobot.com/wp-content/uploads/2019/09/DataRobot_Automated_Machine_Learning_for_Medical_Fraud_Prevention_in_the_Government_v2.0.pdf

DataRobot. 2019d. 'Data Sheet: Improve Counter-Terrorism Measures with DataRobot'. Datarobot.com. As of 09 April 2020: https://www.datarobot.com/wp-content/uploads/2020/01/Improve-Counter-Terrorism-Measures-with-DataRobot_DataSheet_v.2.0.pdf

DataRobot. 2019e. 'Data Sheet: Machine Learning Applications for Federal Departments and Agencies'. Datarobot.com. As of 09 April 2020: https://www.datarobot.com/wp-content/uploads/2019/12/Machine-Learning-Applications-for-Federal-Departments-and-Agencies_DataSheet_v.3.0.pdf

DataRobot. 2020. 'Automated Machine Learning: What is Automated Machine Learning?'. Datarobot.com. As of 11 September 2020: https://www.datarobot.com/wiki/automated-machine-learning/

Davenport, Thomas H. & Rajeev Ronanki. 2019. 'Artificial Intelligence for the Real World'. *Harvard Business Review* (January-February 2018). As of 07 September 2020: https://hbr.org/2018/01/artificial-intelligence-for-the-real-world

Deloitte. 2018. 'Artificial Intelligence'. Deloitte.com, March 2018. As of 31 July 2020: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/deloitte-analytics/deloitte-nl-data-analytics-artificial-intelligence-whitepaper-eng.pdf

Deloitte. 2019a. 'Opportunities for AI in border control, migration and security: Opportunities for the Use of AI – External & Internal processes'. Deloitte, December 2019. Non-public report.

Deloitte. 2019b. 'The democratisation of artificial intelligence'. Deloitte.co.uk, February 2019. As of 7 August 2020: https://www.deloitte.co.uk/consumer-review-digital-predictions/assets/img/download/the-deloitte-consumer-review-digital-predictions-2019-ai-prediction-article.pdf

Department of Homeland Security (DHS). 2005. 'National plan to achieve Maritime Domain Awareness for the National Strategy or Maritime Security'. DHS, October 2005. As of 15 June 2020: https://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf

Department of Homeland Security (DHS). 2019. 'News Release: DHS Awards $200K for AI-Based Object Recognition Proof-of-Concept'. Dhs.gov, 4 November 2019. As of 14 April 2020: https://www.dhs.gov/science-and-technology/news/2019/11/04/news-release-dhs-awards-200k-ai-based-proof-concept

Doyle, Tom. 2011. 'Information and communications technology and modern border management'. In *Border Management Modernization*, edited by Gerald McLinden, Enrique Fanta, David Widdowson & Tom Doyle. 115-124. As of 5 September 2020: http://documents1.worldbank.org/curated/en/986291468192549495/pdf/588450PUB0Bord101public10BOX353816B.pdf

Etherington, Darrell. 2019. 'MIT develops a system to give robots more human senses'. TechCrunch, 17 June 2019. As of 16 June 2020: https://techcrunch.com/2019/06/17/mit-develops-a-system-to-give-robots-more-human-senses/

Elbit Systems of America (homepage). 2020. As of 15 June 2020: https://www.nextgenborder.com/?__hssc=213507147.4.1580913805313&__hstc=213507147.52907790b7d98bff1dd58d2c5e2dd2bd.1580913805312.1580913805312.1580913805312.1&__hsfp=3480816081&hsCtaTracking=77b89bbe-1ead-406b-b865-89a49df09659%7C4e815ed2-565e-4cfc-bd6d-7dd4dfe81afb

Ernst, Douglas. 2018. 'U.S. Army breakthrough: Facial recognition technology now works in the dark'. *The Washington Times*, 16 April 2018. As of 16 June 2020:

https://www.washingtontimes.com/news/2018/apr/16/army-breakthrough-facial-recognition-technology-no/

Etias (homepage). 2020. As of 15 June 2020: https://etias.com/

European Commission. 2016a. 'Migration and Home Affairs: European Border and Coast Guard Agency (Frontex).' Ec.europa.eu. As of 15 June 2020: https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/european-border-and-coast-guard-0_en

European Commission. 2016b. 'SURVEIRON: Advanced surveillance system for the protection of urban soft targets and urban critical infrastructures. Cordis.europa.eu. As of 11 August 2020: https://cordis.europa.eu/project/id/711264

European Commission. 2018a. 'Communication: Artificial intelligence for Europe'. Ec.europa.eu, 25 April 2018. As of 06 August 2020: https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe

European Commission. 2018b. 'Coordinated Plan on Artificial Intelligence'. Ec.europa.eu, 07 December 2018. As of 06 August 2020: https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence

European Commission. 2018c. 'An advanced online anti-fraud software equipped with deep learning Artificial Intelligence thatcan face and detect, current fraudulent techniques and their continued evolution in a cost effective man'. Cordis.europa.eu. As of 11 August 2020: https://cordis.europa.eu/project/id/775707/reporting

European Commission. 2019. 'A definition of Artificial Intelligence: main capabilities and scientific disciplines'. As of 29 July 2019: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

European Commission. 2020a. 'EU Security Union Strategy'. European Commission COM(2020) 605 final, 24 July 2020. As of 14 August 2020: https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf

European Commission. 2020b. 'White Paper: On Artificial Intelligence - A European approach to excellence and trust'. European Commission COM(2020) 65 final, 19 February 2020. As of 14 August 2020: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Commission. 2020c. 'Europe investing in digital: The Digital Europe Programme'. Ec.europa.eu, 29 June 2020. As of 7 September 2020: https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-programme

European Commission. 2020d. 'Automated Border Control (ABC)'. Ec.europa.eu. As of 9 April 2020: https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/automated-border-control-abc_en

European Commission. 2020e. 'Integrated system for real-time TRACKing and collective intelligence in civilian humanitarian missions'. Cordis.europa.eu, 16 July 2020. As of 11 September 2020: https://cordis.europa.eu/project/id/700510

European Organisation for Security (EOS). 2019. 'EU Digital Autonomy: Challenges & Recommendations for the Future of European Digital Transformation'. Eos-eu.com, November 2019. As of 7 September 2020: http://www.eos-eu.com/Files/EOSEUDigitalAutonomyPositionPaper.pdf

European Parliament and the Council of the European Union. 13 November 2019. 'Regulation (EU) 2019/1896 on the European Boarder and Coast Guard'. As of 8 July 2020: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R1896&from=EN#d1e39-1-1

European Political and Strategy Centre (EPSC). 2019. 'Rethinking Strategic Autonomy in the Digital Age'. European Political Strategy Centre, 30 July 2019. As of 5 September 2020: https://op.europa.eu/en/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f-01aa75ed71a1/language-en

European Security Research Advisory Board (ESRAB). 2006. *Meeting the challenge: the European Security Research Agenda*. A report from the European Security Research Advisory Board, September 2006.

Eurotech. 2020. 'Edge AI: enabling Deep Learning and Machine Learning with High Performance Edge Computers'. Eurotech.com. As of 2 September 2020: https://www.eurotech.com/en/page/edge-ai

Feldstein, Steven. 2019. 'The Global Expansion of AI Surveillance'. Carnegie Endowment, 17 September 2019. As of 16 June 2020: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Friedewald, Michael, David Wright, Serge Gutwirth & Emilio Mordini. 2010. 'Privacy, data protection and emerging sciences and technologies: towards a common framework'. *Innovation: The European Journal of Social Science Research* 23(1):61–67. As of 16 June 2020: https://www.tandfonline.com/doi/full/10.1080/13511611003791182

Frontex. 2012. 'Best Practice Operational Guidelines for Automated Border Control (ABC) Systems'. Frontex Research and Development Unit, 31 August 2012. As of 9 April 2020: https://frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_for_Automated_Border_Control.pdf

Frontex. 2016. 'Risk Analysis for 2016'. Frontex.europa.eu, March 2016. As of 04 September 2020: https://frontex.europa.eu/assets/Publications/Risk_Analysis/Annula_Risk_Analysis_2016.pdf

Frontex. 2019a. 'News release: Frontex testing the future of border checks at Lisbon airport'. Frontex.europa.eu, 4 October 20219. As of 15 June 2020: https://frontex.europa.eu/media-centre/news-release/frontex-testing-the-future-of-border-checks-at-lisbon-airport-DI84r4

Frontex. 2019b. 'News release: New Frontex Regulation comes into force'. Frontex.europa.eu, 4 December 2019. As of 19 June 2020:

https://frontex.europa.eu/media-centre/news-release/new-frontex-regulation-comes-into-force-S0luwe#:~:text=Today%2C%20Frontex%2C%20the%20European%20Border,security%20for%20all%20their%20citizens

Frontex. 2020a. 'Risk Analysis for 2020'. Frontex.europa.eu. As of 15 June 2020: https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Annual_Risk_Analysis_2020.pdf

Frontex. 2020b. 'Foreword'. Frontex.europa.eu. As of 19 June 2020: https://frontex.europa.eu/about-frontex/foreword/

Frontex. 2020c. 'Vision, Mission & Values.' Frontex.europa.eu. As of 29 July 2019: https://frontex.europa.eu/about-frontex/vision-mission-values/

Fussell, Sidney. 2019. 'The Endless Aerial Surveillance of the Border'. *The Atlantic*, 11 October 2019. As of 14 August 2020: https://www.theatlantic.com/technology/archive/2019/10/increase-drones-used-border-surveillance/599077/

Goal-robots.eu (homepage). 2020. As of 16 June 2020: http://www.goal-robots.eu/

Green Car Congress. 2020. 'MIT, QCRI use AI to enrich digital maps to improve GPS navigation; RoadTagger'. Greencarcongress.com, 03 February 2020. As of 11 September 2020: https://www.greencarcongress.com/2020/02/20200203-roadtagger.html

Greenfield, David. 2019. 'Technology startups to watch'. AutomationWorld.com, 18 October 2019. As of 14 April 2020: https://www.automationworld.com/products/software/article/15611757/technology-startups-to-watch

Hatmaker, Taylor. 2018. 'Palmer Luckey's defense company Anduril is already leading to arrests at the southern border'. Techcrunch.com, 11 June 2018. As of 9 April 2020: https://techcrunch.com/2018/06/11/anduril-lattice-sentry-palmer-luckey/

Hecht, Jeff. 2019. 'AI at the Speed of Light'. IEEE Spectrum, 29 August 2019. As of 16 June 2020: https://spectrum.ieee.org/tech-talk/semiconductors/optoelectronics/ai-at-speed-of-light

Hirsch, Lauren. 2020. 'IBM gets out of facial recognition business, calls on Congress to advance policies tackling racial injustice'. Cnbc.com, 8 June 2020. As of 19 June 2020: https://www.cnbc.com/2020/06/08/ibm-gets-out-of-facial-recognition-business-calls-on-congress-to-advance-policies-tackling-racial-injustice.html

Hjermitslev, Oliver Gyldenberg. 2020. 'Training Object Detectors with No Real Data using Domain Randomization'. Toward Data Science, 15 January 2020. As of 11 September 2020: https://towardsdatascience.com/training-object-detectors-with-no-real-data-using-domain-randomization-1569cb3b8c6

IARPA. 2020. 'Functional Map of the World Challenge'. Iarpa.gov. As of 14 April 2020: https://www.iarpa.gov/challenges/fmow.html

IBM Research (homepage). 2020. Research.ibm.com. As of 15 June 2020: https://www.research.ibm.com/5-in-5/ai-and-bias/

Idemia. 2020. 'Mface'. Idemia.com. As of 15 June 2020: https://www.idemia.com/mface

IEEE Spectrum. n.d. 'How 3D Sensing Enables Mobile Face Recognition'. Spectrum.ieee.org. As of 11 August 2020: https://spectrum.ieee.org/transportation/sensors/how-3d-sensing-enables-mobile-face-recognition

Ikusi.aero. 2018. '5 intelligent robots that you can find in airports of the world'. Ikusi.aero, June 2018. As of 15 June 2020: https://www.ikusi.aero/en/blog/5-intelligent-robots-you-can-find-airports-world

InBenta. 2020. 'Symbolic AI vs Machine Learning in Natural Language Processing'. Inbenta.com, 04 March 2020: https://www.inbenta.com/en/blog/symbolic-ai-vs-machine-learning/

Jacobsen, Katja Lindskov. 2015. *The Politics of Humanitarian Technology: Good Intentions, Unintended Consequences and Insecurity*. Oxford: Routledge.

Jacques, Natasha, Angeliki Lazaridou, Edward Hughes, Caglar Gulcehre, Pedro Ortega, Dj Strouse, Joel Z. Leibo & Nando De Freitas. 2019. 'Social Influence as Intrinsic Motivation for Multi-Agent Deep Reinforcement Learning'. Proceedings of the 36th International Conference on Machine Learning, PMLR 97:3040-3049, 2019. As of 16 June 2020: http://proceedings.mlr.press/v97/jaques19a.html

Joshi, Naveen. 2019. '7 Types Of Artificial Intelligence'. Forbes, 19 June 2019. As of 31 July 2020: https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/#6eb1f3ad233e

Kimery, Anthony. 2019. 'Novel techniques that can "trick" object detection systems sounds familiar alarm'. Biometricupdate, 22 April 2019. As of 16 June 2020: https://www.biometricupdate.com/201904/novel-techniques-that-can-trick-object-detection-systems-sounds-familiar-alarm

Lee, Yen-Lin, Pei-Kuei Tsung & Max Wu. 2018. 'Technology Trend of Edge AI'. 2018 International Symposium on VLSI Design, Automation and Test (VLSI-DAT). As of 04 September 2020: https://ieeexplore.ieee.org/document/8373244

Lehtonen, Pinja & Pami Aalto. 2017. Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States'. European Security, 26(2):207-225. As of 11 September 2020: https://www.tandfonline.com/doi/full/10.1080/09662839.2016.1276057

Levy, Steven. 2018. 'Inside Palmer Luckey's Bid to Build a Border Wall'. Wired.com, 6 November 2018. As of 09 April 2020: https://www.wired.com/story/palmer-luckey-anduril-border-wall/

Lippert, Barbara, Nicolai von Ondarza & Volker Perthes. 2019. European Strategic Autonomy: Actors, Issues, Conflicts of Interests. Berlin: German Institute for International and Security Affairs. As of 7 September 2020: https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2019RP04_lpt_orz_prt_web.pdf

Lockheed Martin. 2019. 'Deep Learning Model Speeds Up, Automates Satellite Image Analysis'. As of 14 April 2020: https://news.lockheedmartin.com/news-releases?item=128745

Loeb, Eric & Seven E. Moore. 2020. 'Make data science accessible for the Pentagon'. Warontherocks.com, 10 February 2020. As of 9 April 2020: https://warontherocks.com/2020/02/make-data-science-accessible-for-the-pentagon/

Martin, Nicole. 2019. 'U.S. Airports Will Use AI To Scan 97% Of Passengers' Faces Within 4 Years'. Forbes.com, 24 April 2019. As of 11 August 2020: https://www.forbes.com/sites/nicolemartin1/2019/04/24/us-airports-will-use-ai-to-scan-97-of-passengers-faces-within-4-years/#5f3da1c45949

Matheson, Rob. 2020. 'Using artificial intelligence to enrich digital maps'. News.mit.edu, 23 January 2020. As of 11 September 2020: https://news.mit.edu/2020/artificial-intelligence-digital-maps-0123

Maxar. 2020. 'Automated Feature Extraction & Object Detection'. Radiantsolutions.com. As of 14 April 2020: https://www.radiantsolutions.com/capabilities/enrich/automated-feature-extraction-and-object-detection?utm_source=maxar.com-analytics&utm_medium=website

McCaney, Kevin. 2018. 'AI Lie Detectors Could Soon Police the Borders'. Governmentciomedia.com, 18 December 2018. As of 15 June 2020: https://www.governmentciomedia.com/ai-lie-detectors-could-soon-police-borders

McKinsey Global Institute. 2017. 'Artificial Intelligence: The Next Digital Frontier?'. McKinsey.com, June 2017. As of 7 August 2020: https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx

Mikhaylov, Slava Jankin, Marc Esteve & Averill Campion. 2019. 'AI for the Public Sector: Opportunities and Challenges of Cross-Sector Collaboration'. Philosophical Transactions A. As of 7 September 2020: https://core.ac.uk/download/pdf/160809848.pdf

Miskovic, N., S. Bogdan, I. Petrovic & Z. Vukic. 2014. 'Cooperative control of heterogeneous robotic systems'. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). As of 16 June 2020: https://ieeexplore.ieee.org/document/6859711/authors#authors

Misuraca, Gianluca & Colin van Noordt. 2020. 'AI Watch: Artificial Intelligence in public services'. European Commission. As of 6 August 2020: https://ec.europa.eu/knowledge4policy/ai-watch/topic/ai-public-sector_en

Minsky, Marvin. 1961. 'Steps toward Artificial Intelligence'. Proceedings of the IRE 49(1):8–30. As of 31 July 2020: https://courses.csail.mit.edu/6.803/pdf/steps.pdf

Msv, Janakiram. 2020. 'How AWS Attempts To Bring Transparency To AutoML Through Amazon SageMaker Autopilot'. Forbes.com, 27 Feb 2020. As of 09 April 2020: https://www.forbes.com/sites/janakirammsv/2020/02/27/how-aws-attempts-to-bring-transparency-to-automl-through-amazon-sagemaker-autopilot/#19b8adb52acc

Nowruzi, Farzan Erlik, Prince Kapoor, Dhanvin Kolhatkar, Fahed Al Hassanata, Robert Laganiere & Julien Rebut. 2019. 'How much real data do we actually need: Analyzing object detection performance using synthetic and real data'. Conference Proceedings of

ICML Workshop on AI for Autonomous Driving, Long Beach, California, 16 July 2019. As of 11 September 2020: https://arxiv.org/pdf/1907.07061.pdf

NYU Tandon. 2019. 'Outsmarting deep fakes: AI-driven imaging system protects authenticity'. Eurkalert.org, 29 May 2019. As of 15 June 2020: https://www.eurekalert.org/pub_releases/2019-05/ntso-odf052919.php

Oak Ridge National Laboratory. 2019. 'Bio-circuitry mimics synapses and neurons in a step toward sensory computing'. Nanowerk.com, 17 October 2019. As of 16 June 2020: https://www.nanowerk.com/nanotechnology-news2/newsid=53844.php

Offshore-technology.com. 2019. 'Exploring the impact of artificial intelligence on offshore oil and gas'. Offshore-technology.com, 15 May 2019. As of 14 April 2020: https://www.offshore-technology.com/features/application-of-artificial-intelligence-in-oil-and-gas-industry/

Orav, Anita. 2016. 'Hotspots and emergency relocation: State of Play'. European Parliament Briefing, March 2016. As of 15 June 2020: https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/579070/EPRS_BRI(2016)579070_EN.pdf

Panda, Ankit. 'Japan to Invest in AI-Enabled Maritime Surveillance Platforms'. The Diplomat, 11 November 2019. As of 16 April 2020: https://thediplomat.com/2019/11/japan-to-invest-in-ai-enabled-maritime-surveillance-platforms/

Peled, Matan. 2020. 'Maritime security: See beyond the horizon'. Wnwd.com, 27 February 2020. As of 9 April 2020: https://wnwd.com/blog/see-beyond-the-horizon/

Planck Aerosystems. 2019. 'DHS S&T awards $200K to San Diego's Planck Aerosystems Inc. for final testing of small autonomous aircraft system'. Planckaero.com, 29 August 2019. As of 14 April 2020: https://www.planckaero.com/news/2019/9/4/dhs-sampt-awards-200k-to-san-diegos-planck-aerosystems-inc-for-final-testing-of-small-unmanned-aircraft-system

Planck Aerosystems. 2020. 'Next generation drone autonomy'. Planckaero.com. As of 14 April 2020: https://www.planckaero.com/drone-technology

Primor, Omer. 2020. 'Maritime security: No data left behind'. Wnwd.com, 15 January 2020. As of 9 April 2020: https://wnwd.com/blog/no-data-left-behind/

Purdue University. 2019. 'Autonomous robot that interacts with humans using natural language and vision processing'. Phys.org, 9 January 2019. As of 16 June 2020: https://phys.org/news/2019-01-autonomous-robot-interacts-humans-natural.html

Quach, Katyanna. 2019. 'Homeland Security backs off on scanning US citizens, Amazon ups AI ante, and more'. Theregister.co.uk, 9 December 2019. As of 16 April 2020: https://www.theregister.co.uk/2019/12/09/ai_roundup_061219/

Roborder.eu (homepage). 2020. As of 15 June 2020: https://roborder.eu/

Sakhuja, Vijay. 2018. 'Artificial Intelligence and Maritime Domain Awareness'. Society for the Study of Peace and Conflict, 11 June 2018. As of 16 April 2020: https://sspconline.org/index.php/opinion/artificial-intelligence-maritime-domain-awareness-vijay-sakhuja-110618

Salian, Isha. 2018. 'SuperVize Me: What's the Difference Between Supervised, Unsupervised, Semi-Supervised and Reinforcement Learning?'. Nvidia.com, 2 August 2018. As of 31 July 2020: https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/#:~:text=In%20a%20supervised%20learning%20model,and%20patterns%20on%20its%20own

Sanchez del Rio, Jose, Daniela Moctezuma, Cristina Conde, Isaac Martin de Diego & Enrique Cabello. 2016. 'Automated border control e-gates and facial recognition systems'. Computers and Security. 62(September 2016): 49-72. As of 31 July 2020: https://www.sciencedirect.com/science/article/pii/S0167404816300736

SAS. 2020. 'Computer Vision: What it is and why it matters'. Sas.com. As of 31 July 2020: https://www.sas.com/en_us/insights/analytics/computer-vision.html#:~:text=Computer%20vision%20is%20a%20field,to%20what%20they%20%E2%80%9Csee.%E2%80%9D

Ship Technology. 2015. 'Windward to launch Marine maritime intelligence solution'. Ship-technology.com, 20 May 2015. As of 15 June 2020: https://www.ship-technology.com/news/newswindward-to-launch-marint-maritime-intelligence-solution-4582423/

Simonite, Tom. 2019. 'The Best Algorithms Struggle to Recognize Black Faces Equally'. Wired.com, 22 July 2019. As of 14 August 2020: https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

Singh, Mayank. 2020. 'New system with AI to boost maritime security'. New Indian Express, 9 February 2020. As of 16 April 2020: https://www.newindianexpress.com/thesundaystandard/2020/feb/09/new-system-with-ai-to-boost-maritime-security-2100873.html

Smith, Philip & William Biggs. 2018. 'Securing interoperable and integrated command and control of unmanned systems – building on the successes of Unmanned Warrior'. Conference Proceedings of INEC, 2-4 October 2018. As of 11 September 2020: https://zenodo.org/record/2530718/files/INEC%202018%20Paper%20097%20Biggs%20FINAL.pdf?download=1

Smith, Philip & William Biggs. 2019. 'Securing interoperable and integrated command and control of unmanned systems – validating the UK MAPLE architecture'. Conference Proceedings of EAAW, 2-3 July 2019. As of 11 September 2020: https://zenodo.org/record/3381177/files/EAAW%20VIII%20Paper%20007%20Biggs%20Final%20P.pdf?download=1

SparkCognition. 2018. 'White Paper: AI for Defense Applications'. Sparkcognition.com. As of 14 April 2020: https://learn.sparkcognition.com/defense/ai-for-defense-applications?utm_medium=direct&utm_source=direct

SparkCognition. 2020a. 'SparkPredict'. Sparkcognition.com. As of 15 June 2020: https://www.sparkcognition.com/products/sparkpredict/?utm_medium=direct&utm_source=direct

SparkCognition. 2020b. 'DeepNLP'. Sparkcognition.com. As of 15 June 2020: https://www.sparkcognition.com/products/deepnlp/?utm_medium=direct&utm_source=direct

Synthetik Applied Technologies (homepage). 2020. As of 14 April 2020: https://www.synthetik-technologies.com/

The European Parliament and the Council of the European Union. 2016. 'Regulation (EU) 2016/1624'. Official Journal of the European Union, 16 September 2016. As of 14 August 2020: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R1624&from=EN

Tiempo Development. 2019. 'Challenges of Artificial Intelligence (AI)'. Tiempodev.com, 22 December 2019. As of 15 June 2020: https://www.tiempodev.com/blog/artificial-intelligence-challenges/

Tucker, Patrick. 2018. 'It's Now Possible to Telepathically Communicate with a Drone Swarm'. Defense One, 6 September 2018. As of 7 September 2020: https://www.defenseone.com/technology/2018/09/its-now-possible-telepathically-communicate-drone-swarm/151068/

University of Bradford. 2019. 'Half a face enough for recognition technology'. EurekAlert.org, 1 May 2019. As of 16 June 2020: https://www.eurekalert.org/pub_releases/2019-05/uob-haf050119.php

University of California Los Angeles (UCLA). 2018. 'New AI computer vision system mimics how humans visualize and identify objects'. Eurekalert.org, 20 December 2018. As of 11 August 2020: https://www.eurekalert.org/pub_releases/2018-12/usso-nac122018.php

University of Zurich & EPFL. 2018. 'New foldable drone flies through narrow holes in rescue missions'. Epfl.ch, 12 December 2018. As of 11 September 2020: https://actu.epfl.ch/news/new-foldable-drone-flies-through-narrow-holes-in-r/

U.S. Department of Homeland Security. 2018. 'Assistant for Understanding Data through Reasoning, Extraction and Synthesis'. Dhs.gov, 01 May 2018. As of 14 August 2020: https://www.dhs.gov/sites/default/files/publications/NGFR_AUDREY-FactSheet_180501-508.pdf

U.S. Department of Homeland Security. 2019. 'News Release: DHS S&T Awards Colorado Start-up $147K for Intelligent Counting and Measuring Platform'. Dhs.gov, 9 October 2019. As of 14 August 2020: https://www.dhs.gov/science-and-technology/news/2019/10/09/news-release-dhs-st-awards-colorado-start-147k

Vernon, Jack, Adriana Allocato, Massimiliano Claps & Neil Ward-Dutton. 2020. 'Assessing COVID-19's Impact on the Artificial Intelligence Systems Market'. Idc.com, June 2020. As of 11 September 2020: https://www.idc.com/getdoc.jsp?containerId=EUR146393820

Wang, Qian, Khalid N Ismail & Toby P Breckon. 2020. 'An approach for adaptive automatic threat recognition within 3D computed tomography images for baggage security screening.' J Xray Sci Technol 28(1):35-58. As of 11 August 2020: https://pubmed.ncbi.nlm.nih.gov/31744038/

Waring, Jonathan, Charlotta Lindvall & Renato Umeton. 2020. 'Automated machine learning: Review of the state-of-the-art and opportunities for healthcare'. Artificial Intelligence and Medicine 104(April 2020). As of 16 June 2020: https://www.sciencedirect.com/science/article/pii/S0933365719310437

Wegner, Jan Dirk, Ribana Roscher, Michele Volpi & Fabio Veronesi. 2018. 'Foreword to the Special Issue on Machine Learning for Geospatial Data Analysis'. International Journal of Geo-Information, 20187(4):147. As of 11 September 2020: https://www.mdpi.com/2220-9964/7/4/147

Whittaker, Zack. 2018. 'Princeton Identity debuts a new walkthrough biometric scanner — in a shipping container'. Techcrunch.com, 9 October 2018. As of 11 August 2020: https://techcrunch.com/2018/10/09/princeton-identity-walkthrough-biometric-scanner-shipping-container/?guccounter=1

Windward. 2020. 'Use Case: Intelligence Analysis'. Wnwd.com. As of 9 April 2020: https://wnwd.com/solution/intelligence-analysis/

Wirtz, Bernd W., Jan C. Weyerer & Carolin Geyer. 2019. 'Artificial Intelligence and the Public Sector—Applications and Challenges'. International Journal of Public Administration 47(7):596-615. As of 11 September 2020: https://www.tandfonline.com/doi/pdf/10.1080/01900692.2018.1498103

Wong, Yuna Huh, John M. Yurchak, Robert W. Button, Aaron Frank, Burgess Laird, Osonde A. Osoba, Randall Steeb, Benjamin N. Harris & Sebastian Joon Bae. 2020. 'Deterrence in the Age of Thinking Machines'. Santa Monica, Calif.: RAND Corporation. As of 31 July 2020: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf

Yanguas-Rojas, David & Eduardo Mojica-Nava. 2017. 'Exploration with heterogenous robots networks for search and rescue'. IFAC-PapersOnLine 50(1):7935-7940. As of 16 June 2020: https://www.sciencedirect.com/science/article/pii/S240589631731217X

Zeroeyes (homepage). 2020. As of 15 June 2020: https://zeroeyes.com/

Zhang, Bonnie. 2019. 'SenseTime's AI Technology Enables Intelligent Security Check-in System'. Pandaily.com, 17 January 2019. As of 11 August 2020: https://pandaily.com/sensetimes-ai-technology-enables-intelligent-security-check-in-system/

Zhao, Ying, Douglas J. MacKinoon, Shelley P. Gallup & Charles Zhou. 2010. 'Maritime Domain Awareness via Agent Learning and Collaboration'. Proceedings of the15th ICCRTS, International Command and Control, Research and Technology Symposium, Santa Monica, California, 22-24 June 2010. As of 16 June 2020: http://www.dodccrp.org/events/15th_iccrts_2010/papers/106.pdf