euromesco
Policy Study

N. 27

LIBERTY'S DOOM? ARTIFICIAL INTELLIGENCE IN MIDDLE EASTERN SECURITY

Kristina Kausch
Coordinator

Aitor Bonsoms

Can Kasapoglu

Lewin Schmitt

Žilvinas Švedkauskas

IEMed.
European Institute of the Mediterranean

Co-funded by the European Union

euromesco
Policy Study

N. 27

LIBERTY'S DOOM? ARTIFICIAL INTELLIGENCE IN MIDDLE EASTERN SECURITY

Kristina Kausch
Coordinator

Aitor Bonsoms

Can Kasapoglu

Lewin Schmitt

Žilvinas Švedkauskas

IEMed.
European Institute of the Mediterranean

Co-funded by
the European Union

euromesco
research dialogue advocacy

EuroMeSCo has become a benchmark for policy-oriented research on issues related to Euro-Mediterranean cooperation, in particular economic development, security and migration. With 116 affiliated think tanks and institutions and about 500 experts from 30 different countries, the network has developed impactful tools for the benefit of its members and a larger community of stakeholders in the Euro-Mediterranean region.

Through a wide range of publications, surveys, events, training activities, audio-visual materials and a strong footprint on social media, the network reaches thousands of experts, think tankers, researchers, policy-makers and civil society and business stakeholders every year. While doing so, EuroMeSCo is strongly engaged in streamlining genuine joint research involving both European and Southern Mediterranean experts, encouraging exchanges between them and ultimately promoting Euro-Mediterranean integration. All the activities share an overall commitment to fostering youth participation and ensuring gender equality in the Euro-Mediterranean experts' community.

EuroMesCo: Connecting the Dots is a project co-funded by the European Union (EU) and the European Institute of the Mediterranean (IEMed) that is implemented in the framework of the EuroMeSCo network.

As part of this project, five Joint Study Groups are assembled each year to carry out evidence-based and policy-oriented research. The topics of the five study groups are defined through a thorough process of policy consultations designed to identify policy-relevant themes. Each Study Group involves a Coordinator and a team of authors who work towards the publication of a Policy Study which is printed, disseminated through different channels and events, and accompanied by audio-visual materials.

POLICY STUDY

Published by the European Institute of the Mediterranean

Policy Peer Review: Irakli Beridze, Head of the Centre for Artificial Intelligence and Robotics at UNICRI, United Nations
Academic Peer Reviewer: Anonymous

Editing
Justine Leïla Belaïd

Design layout Maurin.studio
Proofreading Neil Charlton
Layout Núria Esparza
Print ISSN 2462-4500
Digital ISSN 2462-4519
Arabic version ISSN 2696-7626
May 2022

This publication has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Union or the European Institute of the Mediterranean.

IEMed.
European Institute of the Mediterranean

The **European Institute of the Mediterranean** (IEMed), founded in 1989, is a think and do tank specialised in Euro-Mediterranean relations. It provides policy-oriented and evidence-based research underpinned by a genuine Euromed multidimensional and inclusive approach.

The aim of the IEMed, in accordance with the principles of the Euro-Mediterranean Partnership (EMP), the European Neighbourhood Policy (ENP) and the Union for the Mediterranean (UfM), is to stimulate reflection and action that contribute to mutual understanding, exchange and cooperation between the different Mediterranean countries, societies and cultures, and to promote the progressive construction of a space of peace and stability, shared prosperity and dialogue between cultures and civilisations in the Mediterranean.

The IEMed is a consortium comprising the Catalan Government, the Spanish Ministry of Foreign Affairs, European Union and Cooperation, the European Union and Barcelona City Council. It also incorporates civil society through its Board of Trustees and its Advisory Council.

The research process for this Policy Study was initiated in the fall of 2021 and the publication was drafted by March 2022. Given that the topic of the study is time sensitive, political developments might have taken place after the study was drafted which may contribute to the discussions triggered by this research.

This Policy Study benefitted from a policy peer review done by Irakli Beridze (UNICRI). The contents of this publication are the sole responsibility of its authors and can in no way be taken to reflect the views of the UNICRI or the United Nations.

euromesco
Policy Study

Content

Executive Summary

The surge of artificial intelligence (AI)-enabled technologies has triggered global debates on the potential risks and opportunities of the use of these technologies to enhance societies' prosperity, security and well-being while ensuring human control and safeguarding fundamental rights. In the area of security, AI has the potential of making key sectors, such as predictive policing, counter-terrorism or border management more efficient, just and humane. At the same time, the risks inherent to AI in the security sector have raised numerous concerns regarding surveillance and data protection, human rights and civil liberties, or the prospect of an arms race in autonomous weapons systems, which have overshadowed debates on opportunities.

The Middle East and North Africa (MENA) region presents particular challenges in this equation. On the one hand, the region's myriad security challenges could greatly benefit from a booster in security-related problem-solving efficiency. On the other, ethical and legal considerations gain particular weight in a region largely governed by authoritarian rulers and with a weak rule of law, as these conditions prevent thorough AI governance and the necessary checks and balances to avoid authoritarian abuse of the ample opportunities presented by AI.

This collection attempts to approach the questions and dilemmas raised by AI in Middle Eastern security through a European policy lens. Zooming in on AI in border management, surveillance, defence and regulation, exploring both risks and opportunities of this set of technologies for the fragile security of the MENA region, each chapter draws conclusions for future European Union (EU) policy and cooperation with MENA partners on AI.

In **the first chapter,** Aitor Bonsoms and Lewin Schmitt explore the ways in which AI systems are – currently and potentially – used in MENA border and migration management. The chapter shows how AI-enabled technologies such as Automated Border Controls, smart fencing and patrolling, AI solutions to enhance situational awareness and prediction, or AI solutions for transnational counter-terrorism, can plausibly contribute to improving crucial aspects of border management. At the same time, the widespread use of biometric ID systems, in conjunction with weak privacy laws and generally weak rule of law and human rights protections in the MENA region, opens the door to authoritarian abuses. In addition, the many technical pitfalls of AI in border management make it crucial to build a sound

understanding of the different technologies, use cases and accompanying challenges. The authors underline how the introduction of intrusive technologies into border control threatens the rights of already vulnerable populations. In the light of the current pace and trajectory of the rollout of facial recognition technology, the authors suggest, it becomes urgent to develop regulatory and governance principles that ensure respect for privacy, proportionality, transparency and accountability in how these technologies are used, including when managing borders.

In **the second chapter,** Žilvinas Švedkauskas explores how the uptake of AI-enabled technologies has boosted digital surveillance in the MENA region. Major advances in AI, including machine learning for clustering, speech recognition and generation, natural language processing, image and video generation, autonomous decision-making and intelligent personal assistance, have provided impetus for upgrading surveillance solutions. Digital surveillance provides a master-key for MENA autocrats, Švedkauskas finds, as it facilitates identification, targeting and tracking of political opposition. MENA law enforcement and security agencies, telecom and internet service providers (ISP) are employing both mass and targeted digital surveillance solutions to track not only criminal suspects but also activists and human rights defenders mashed together by diffusion of blurry cybercrime laws. With the global shift to fifth generation (5G) networks and drastic increases in data capacities and speed, digital surveillance will inevitably rely on further automation and AI algorithms. Without policy interventions, the described surveillance patterns are likely to mushroom as MENA government agencies combine different AI-assisted surveillance solutions from an ever-growing pool of tools. The chapter goes on to show how, unlike in other AI segments, China is not yet a lead player in the MENA deep packet inspection (DPI) or spyware markets as MENA governments have trodden carefully not to get caught up in a global techno-political competition between China and the United States (US).

In **the third chapter,** Can Kasapoglu explains how the shifts in the future of warfare brought on by AI play out in the Middle East as some countries' fast investment in emerging defence technologies has turned them into unexpected pioneers. AI-based investments work as a force-multiplier and strategic enabler for a range of segments of military affairs. Robotic warfare in particular will bring significant impacts for the future of war, creating a battlefield where trade-offs and large-scale destruction are normalised. At the same time, machine-learning algorithms will also be able to foresee a conflict's outcomes and greatly diminish human casualties during conflict. Overall, the chapter shows how AI in defence is

a double-edged sword coming into play fast that will lead to shifts in the geopolitical balance of power, creating new winners and losers. The proliferation of AI in militaries will allow smaller powers and non-state actors to use technology to increase their impact and leverage. In the Middle East, sophisticated AI-powered weapons have already become extremely lethal assets. AI can be a true force multiplier in Iran's proxy wars and asymmetric capabilities, which could nurture further regional destabilisation. The Abraham Accords have led to an emerging Arab-Israeli cooperation on military AI that will hardly be in sync with the EU's restrictive stances on autonomous weaponry and defence use of AI. With AI-boosted militaries, Middle Eastern wars will be faster in tempo and broader in scope. This will inevitably affect the EU's strategic outreach and security calculus in the region.

In **the fourth chapter,** Kristina Kausch looks at early AI regulation efforts in the MENA region and explores how global advances in AI governance may impact both the use and regulation of AI in the EU's Southern Neighbourhood. While an international consensus on ethical principles for AI is emerging and most countries rely on a soft law approach, a nascent trend points towards legislative reform and hard law regulation. AI regulation in the region remains overall low; a number of countries have national AI strategies, a few have soft law guidance, but none has yet drafted legislation specifically on AI. The sensitivity of security-related AI in the MENA region raises special challenges for regulation in preventing unethical uses of AI technologies under authoritarian governance. While the EU lacks jurisdiction beyond its borders, debates on the EU's June 2021 draft AI Regulation have raised expectations that the latter may develop an extraterritorial reach. The prospects of a "Brussels Effect" (Bradford, 2020) on AI in MENA security are reduced, however, by the regulation's carve-out for military systems and third country-law enforcement. At the same time, the EU's newly revamped 2021 Export Control Regulation fails to provide an efficient export regime for high-risk AI. A potential split of the market in two into a highly regulated EU and an under-regulated periphery could generate a comparative advantage for China as a provider of authoritarian tech, turning the aspired regulatory Brussels Effect into a "Beijing Effect".

A number of overarching themes emerge from the chapters.

- Governments in the MENA region have embraced AI as a potential booster of development and growth, albeit presenting significant regional variation in technological maturity and AI uptake. Low AI readiness across the Maghreb contrasts with more affluent and technologically advanced economies in the Gulf and Israel, where we observe a concerted push to introduce AI into all aspects of public life.

- EU policy must conceive AI as a key geopolitical asset and means of empowerment for its user, with both the great opportunities and the great challenges this empowerment entails. In order to fully understand the geopolitical ramifications of its actions and omissions and translate these into policy, the EU should take a more active role and geopolitical vision in the pro-

motion of trustworthy AI technologies and companies, especially considering the increasing competition from China.

- The double-edged sword nature of AI is particularly pronounced in the security sector. AI is a booster to security capacity, potentially raising human security if used in a responsible and accountable manner, and diminishing human security if used in an irresponsible, unaccountable manner.

- Especially salient for the MENA region is the inherent tension between responsible AI governance and authoritarian rule. Beyond technical flaws and quality concerns, the main risk lies in the enormous potential of technology-enabled human rights abuses. Consequently, in the MENA authoritarian setting with a generally weak rule of law and insufficient human rights safeguards, the risks of AI in security currently clearly outweigh the opportunities.

- Digital surveillance, both in mass and targeted form, is a particular, fast-spreading concern, boosted by the COVID-19 pandemic, that requires urgent, concerted action. AI-assisted mass digital surveillance of national internet traffic during the last decade has become the norm across MENA countries. Moreover, increasing evidence of targeted surveillance attacks on European leaders with MENA-produced software also turn the issue into a national security problem for EU member states.

These themes lead to a set of implications for EU policy and cooperation with the MENA region on AI, leading to the following clusters of the more detailed recommendations discussed at the end of each chapter:

- **EU niche for trustworthy AI:** In the field of AI in the MENA region, the EU should push for regulation in line with emerging international standards for trustworthy AI, while at the same time developing its niche in the global AI market as quality AI made in Europe. Not only will this meet high demand but others will try to imitate it, raising the global bar for AI standards and regulation.

- **Sequenced cooperation in the MENA region:** Early-stage EU programmes aiming to support MENA governments in developing their AI capacity should adopt a sequenced approach, which, in a first step, focuses on laying the groundwork by working with MENA lawmakers on the development of both soft and hard law within a framework of the rule of law; establishment of legal and regulatory frameworks for AI, and oversight institutions and mechanisms.

- **Capacity development:** In a second step, EU cooperation should focus on helping to build healthy domestic ecosystems for human-centric, trustworthy AI, which can generate local talent and technological capacity, both from a development and use perspective, as well as from an institutional and civic accountability perspective.

- **Technology transfer/PPP:** EU cooperation should seize the high potential for technology transfers and capacity-building via public-private partnerships (PPP).

EU governments should encourage the piloting of such technology by private sector entities that, in the absence of local rules and regulations, would likely adhere to – and transfer – European standards.

- **Empower digital rights groups:** The empowering feature of AI in MENA security in cooperation with governments must be flanked by parallel empowerment of societal control mechanisms. The EU should set up a Neighbourhood Digital Rights Fund to empower civil society defending fundamental rights in the face of emerging technologies.

- **Sharpen EU regulation:** The critical risks of AI technology in the MENA security sector should inform the EU's cautionary approach to dual use technology exports. To ensure transparency and accountability around exported AI tools, the EU should consider the creation of an algorithmic transparency register. Ongoing debates around the draft AI Act could be used to further sharpen the provisions of the European Export Regulation. Amendments to the draft EU AI Act should consider erasing the carve-out for AI systems used by third-country law enforcement.

- **Impact assessment:** Due to the mentioned concerns, cooperation must be particularly careful and well-designed to avoid empowering the wrong people. Programming and policy must do justice to the geopolitical significance of AI capability, and should therefore be preceded by a multi-dimensional, cross-sectoral impact assessment.

- **EU Tech Strategy:** In the big picture, a deeper understanding of AI as a geopolitical asset across EU institutions and policy-making circles must be embedded in a larger EU strategy on the role and uses of technology in the Union's external relations that aligns strategic thinking on AI with that of other emerging tech from a geopolitical perspective.

Introduction

Kristina Kausch
Senior Resident Fellow, The German Marshall Fund of the United States (GMF)

In the immediate aftermath of Russia's invasion of Ukraine on 24 February 2022, it became clear that the ensuing war and the international reactions provoked by it marked the shift towards a new geopolitical chapter. In a matter of days, the focal point of the Ukraine war firmly anchored the systemic rivalry between democratic and authoritarian great powers that had been building up for years as an emerging paradigm of international relations.

The global tech competition has been a central expression of this simmering systemic rivalry, and it has long been understood that artificial intelligence (AI) is among the elements at the core of this race. With its capacity as a force magnifier in anything digital, AI readiness is often regarded as the new currency for geopolitical stamina – including by Vladimir Putin, as documented in numerous well-publicised statements. The European Union (EU) has – at least nominally – acknowledged the magnitude of the geopolitical potential of AI technologies. Its far-reaching efforts to shape debates on the global rules for AI, including the EU's 2021 draft AI Act as the first-ever horizontal attempt to regulate AI, and the Union's efforts to co-ordinate global AI governance in multilateral fora as well as in the EU-United States (US) Trade and Technology Council, all constitute testimony to this insight.

Aside from accelerating geopolitical shifts, the Ukraine war, and a few years earlier the war in Syria, both triggered or escalated by Russian invasion (in February 2022 and September 2015, respectively), have also reminded Europeans how vulnerable Europe is to authoritarianism in its immediate periphery. Among the grand lessons of these conflicts is the insight that the ultimately unpredictable volatility of authoritarian rulers makes them unfit as key providers for geo-strategically important resources to Europe, be it semiconductors, energy or other raw materials. Decreasing relative dependence on authoritarian suppliers, and investing in partnerships with reliable democratic allies, will be key for European strategic autonomy.

Europe's vulnerability to authoritarian destabilisation of its immediate vicinity shows EU cooperation frameworks with both Eastern and Southern Neighbourhoods in a new light. In the light of the lessons drawn from a fatefully erroneous European appeasement policy vis-à-vis Russia, EU cooperation frameworks for the entire neighbourhood will need to be re-thought, priorities re-ordered, partnerships re-evaluated. In the Middle East and North Africa (MENA) region, this means reducing dependency on volatile suppliers and boosting investment in sustainable partnerships. Above all, however, it means not tacitly helping to prop up an authoritarian model of governance that not only makes Europe vulnerable to MENA rulers' potential volatilities, but equally importantly, which remains a permanent Achilles' heel for Europe as an easy prey for Russian and Chinese hedging and leveraging attempts.

Set against this larger geopolitical background, the way in which AI technologies take root in the MENA security sector is consequential not only for MENA human security but also for Europe's. Rightfully, AI is hailed as a set of technologies that has the potential to boost development, employment governance and prosperity. The sensitive nature of the security sector merits greater scrutiny, however. As this collection will show, AI's nature as a booster technology also means that its use in an authoritarian context, and in a region ridden with armed conflict and transnational security challenges, the challenges are likely to outweigh the benefits unless the governance and use of AI systems can be locked into a reliable (national or international) frame of transparency and accountability. This

will be key for EU regulation, policy and co-operation as the EU considers advancing its cooperation with MENA governments in ways adapted to the changed requirements and priorities of a new geopolitical era.

In defining AI, the present study follows the European Commission (EC)'s broad 2021 formula which defines an AI system as "software that … can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with" (European Commission, 2021).[1] Considering that AI systems are usually embedded as components of larger systems, rather than stand-alone systems, throughout this volume we will synonymously use the terms AI system and AI (-enabled) technology to mean any AI-based component in software and hardware.

[1] See also the detailed deliberations on this topic by the EC's High Legal Expert Group on Artificial Intelligence (2018): *A Definition of AI: Main Capabilities and Scientific Disciplines,* European Commission, 2018.

AI at the Gates: Present and Future of AI Border Management

Aitor Bonsoms
PhD candidate, Institut Barcelona d'Estudis Internacionals (IBEI)

Lewin Schmitt
PhD candidate, Institut Barcelona d'Estudis Internacionals (IBEI)

The rapid advances in artificial intelligence (AI) open doors to benefits and dangers alike, which are often a function of the use case in which the technology is being deployed. One controversial application domain is border control, which the European Commission (EC)'s proposed AI Act classifies as a high-risk area. While this would put strong constraints on its use within the Single Market, much less is known about the use of AI in border management in the Southern Neighbourhood – despite the region's proximity to the European Union (EU) and its subsequent importance for many migration-related files. How advanced are Middle East and North Africa (MENA) countries with regards to the use of AI in border control management? What opportunities and risks does the technology hold, especially for transnational security and effective migration management? What key debates, dilemmas and trajectories are relevant for the EU and its partners when working to strengthen a healthy and sustainable digital transformation in the region?

Although at present the scarce use of AI by the region's security agencies is mainly devoted to domestic surveillance, this chapter discusses the first steps that are being taken towards its implementation in border contexts – with considerable variation across countries. AI can plausibly contribute to improving crucial aspects of border management and counter-terrorism throughout the region. Public institutions often justify the deployment of biometric passports and ID systems with the acceleration of border checks and more convenient passenger flows. This enables border agents – and in later stages, automated solutions – to quickly match passenger records against databases of wanted criminals or terror suspects, which is also relevant for tracing returning foreign fighters. Similarly, AI-assisted border monitoring tools – for instance, analysis of mobile phone network data – can help control irregular migration routes, which are often used by transnational terrorist networks. However, the introduction of AI in the region's security sector also bears many risks. The widespread use of biometric ID systems, in conjunction with weak privacy laws and generally weak rule of law and human rights protections, opens the door to authoritarian abuses, which AI tools will likely aggravate.

The rapid securitisation and digitalisation of border management tools make this subject particularly timely. On the one hand, the security sector's sensitive nature augments the broader ethical concerns related to the technology's risks and opportunities. On the other, the potential of harm reduction (e.g., faster identification of terrorists or better control of irregular border movements) may provide a powerful imperative for fast and unfettered deployment. In order to have informed discussions about the most pressing dilemmas, it is important to shed light on present uses and future developments of AI in border management across the MENA region.

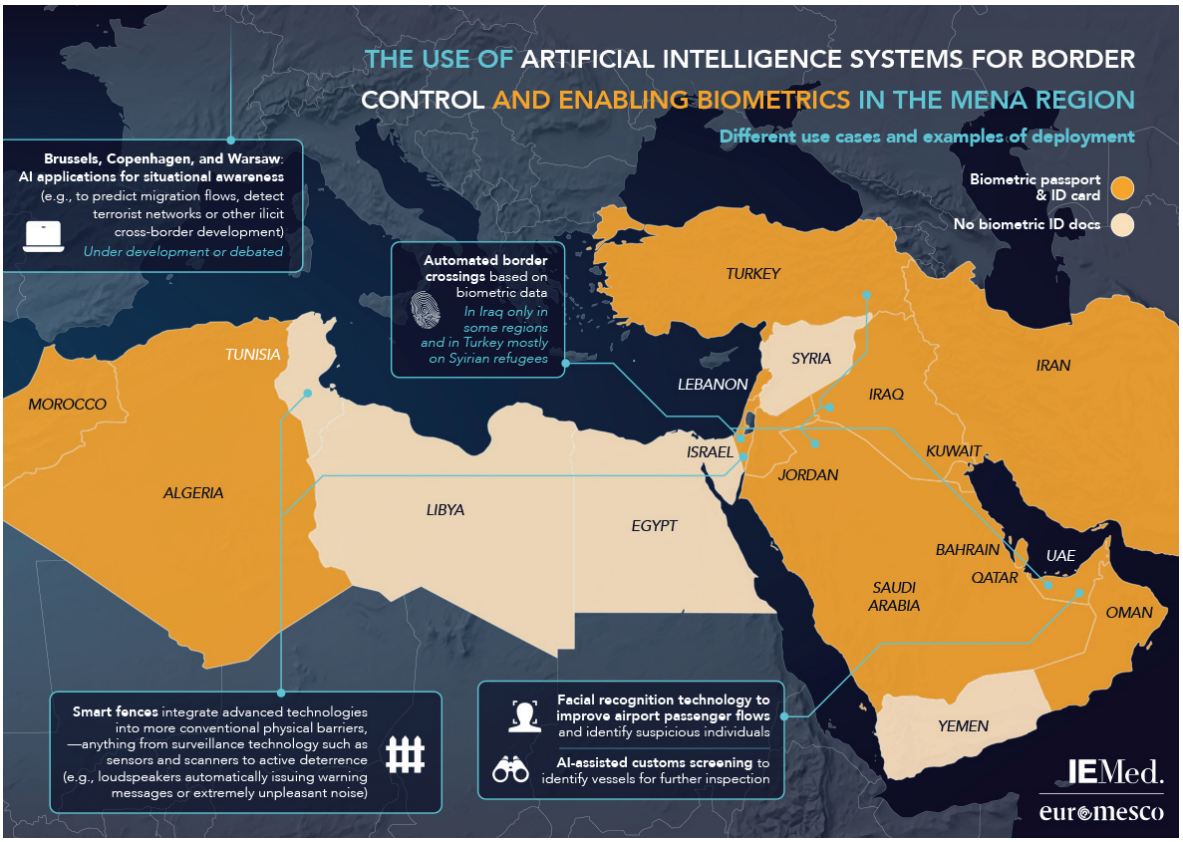
AI in border management

The most prevalent and promising use cases for AI technology in border management and counter-terrorism are automated border crossing (ABC) technology, smart fencing, situational awareness, speech recognition, data mining or natural language processing.[2] In addition, the collection and

[2] Another, highly controversial, application consists of emotion detection technologies, which has been piloted by EU-funded projects to supposedly detect deceptive behaviour of visa applicants. Such AI-based lie-detector techniques are commonly rejected by the research community for their lack of scientific base and potential for unethical uses. As we did not find any instances of the use or development of such technologies in the MENA region, we have decided not to include it in the present report, but agree with warnings regarding the harms associated with such applications.

storage of biometric data is an important technological precursor and enabler in the context of AI for borders. As the infographic shows, biometric systems are in place across most of the MENA region. Furthermore, the infographic highlights exemplary use cases of AI technology in border contexts.

Generally, around the world, the use of AI in border management and counter-terrorism is still in its infancy, which is all the more true for the MENA region, where counter-terrorism actions are largely based on militarised and other more traditional intelligence-based approaches. However, the last few years have seen an increased



interest in the topic both by governments and businesses. At the October 2021 Military Radar and Border Security Summit in Turkey, which brought together more than 100 defence companies from around the world to present their border protection products, Turkey's top procurement official underlined the importance of integrated security solutions, including sophisticated electronic sensor systems, for the continuous monitoring of Turkey's border to prevent unauthorised refugee crossings, terrorist activity and smuggling (Ozberk, 2021).

As justifications for securitising borders with such technologies are context-dependent and contingent on political priorities, their stated goal can vary widely: to prevent terrorists from entering a territory, to undermine contraband or human trafficking, but also to stem migration or spurn refugees. Some of these may seem more inherently ethical than others, which immediately

raises red flags from a human rights perspective. In any case, it is important to note that, once such systems are in place, they rarely distinguish between target groups – no matter whether the original intention was in good faith or not. In other words, a smart fence erected to stop terrorists will most likely make it impossible for legitimate asylum seekers to cross the border. Similarly, many of the discussed technologies and tools can be repurposed relatively easily, underlining their dual use (or, more accurately, "multiple use") character and the associated challenges. For instance, an AI system originally trained to predict terrorist content on social media could easily be targeted to identify government criticism and censor opposition voices. This is why it is crucial to build a sound understanding of the different technologies, use cases, and accompanying challenges. So what are the most relevant present and future use cases for AI technology in border situations and counterterrorism?

It is crucial to build a sound understanding of the different technologies, use cases, and accompanying challenges

Automated border crossings

ABC technology – sometimes referred to as "smart gates" or "eGates" – describes the use of technology to improve identity verifications of travellers crossing borders by automating key steps, such as the scanning of identity documents or biometric markers, and the matching against databases or other alert systems. While not all current technology platforms such as passport terminals rely on AI technology, newer-generation ones increasingly do. Furthermore, once legacy systems without AI are in place, the software and even hardware can usually be upgraded relatively easily to include AI components. Moreover, it prepares security personnel for increasingly automatised procedures and protocols, rendering it a crucial precursor to enable AI technology at border crossings.

To date, there are several cases of ABC technology deployed in the MENA region, and the proliferation of biometric passports is likely to accelerate this trend. Countries such as Israel, United Arab Emirates (UAE), and Saudi Arabia have created biometric civil registries for citizens and expatriates, collecting biometric data from everyone entering or leaving the country. This data predominantly consists of fingerprints, though it is increasingly replaced or complemented with other data points, most notably facial recognition, but also palm and handprints, or digital signatures. Israeli authorities have incorporated facial recognition technologies into the checkpoints and Closed Circuit Television/Internet Protocol (CCTV/IP) video surveillance systems such as those installed in the West Bank for controlling the movement of people in and out of the territory. In 2014, the Iraqi Kurdistan province of Sulaymaniyah introduced a similar system, based on fingerprint data of over one million registered visitors, to protect the Kurdistan region from infiltration by insurgents and terrorists (M2SYS, n.d.). Integrated ABC technology with central biometric registers can facilitate easier, faster and potentially safer border checks. However, they also open the door wide to authoritarian abuses, privacy violations and cyber incidents or attacks.

Other less centralised and less advanced applications of biometric identification in border environments can be found for instance in Egypt, where biometric gateways or biometric access systems have been installed at the airports of Cairo, Hurghada and Sharm El Sheikh in recent years. Notably, they are not currently used to check passengers but instead to facilitate access controls of its airport staff and thus increase onsite security. Following external pressure mainly from Russia after the bombing of Metrojet Flight 9268 in 2015, these systems have been introduced by the private companies running the airport facilities. However,

given the ongoing resistance of local workers, oversight and enforcement of the access control system was transferred to the police, highlighting both the importance of user trust regarding acceptance of AI tools as well as the technology transfer mechanisms between private and state actors.

Smart fencing and patrolling

A second border-related application of AI technology can be found in so-called "smart fencing" projects, also referred to as "smart borders" or "smart walls". The terms describe border enforcement solutions that integrate advanced technologies into more conventional physical barriers, or even replace the latter altogether. These technologies can include anything from surveillance technology such as sensors and scanners (optical, thermal, sonar, radar or otherwise) to active deterrence (e.g., loudspeakers issuing warning messages or extremely unpleasant sounds). In addition, it may consist of supplementary aerial surveillance (drones or satellite imagery) or other patrolling devices (mainly land robots). They are considered "smart" because they feed into and are controlled by an integrated software solution, which may or may not have automated decision-making capabilities (and hence may or may not be categorised as AI). Conversely, these systems are subject to criticism both for technical flaws (some systems are quite susceptible to evasion or interference) and ethical considerations (as they further dehumanise and securitise borders).

The Israeli-built Hourglass Project is a good example of a "smart fencing" project, boasting a 242-kilometre-long fence at the Egyptian border; it is equipped with warnings systems and information collection devices. The visual detection sensors employed are dual cameras, which feed the real-time data to a control unit that can automatically identify and mark objects approaching the fence and decide whether or not to set off an alarm. Magna, the Israeli developer of the system, claims that its "self-learning" algorithm achieves "near 100 percent detection probability and almost a zero chance for false alarms" (MAGMA BSP, n.d.). Israeli authorities also reinforced border security with Syria, Jordan and the Gaza Strip, including fences equipped with sophisticated sensors.

A second border-related application of AI technology can be found in so-called "smart fencing" projects, also referred to as "smart borders" or "smart walls"

Similar projects have been implemented in Tunisia, including at the Tunisian-Libyan border.[3] This border had for a long time been an illegal pass of people and materials (World Bank, 2017). After 2012, the security situation deteriorated further, leading to a rise in cross-border terrorist and insurgent activity. Grim examples of this are the Bardo National Museum terror attack in Tunis and the insurgency of Ben Gardane; in both cases, many of the fighters were trained in Libyan camps near the border. To counter the relatively unrestrained movement into their country, Tunisian authorities – with the support of the US and Germany – are deploying an integrated electronic security surveillance system including high-tech sensors.

AI for situational awareness and prediction

AI and big data analytics are especially advantageous when sifting through large troves of information in a fast fashion and for unearthing patterns that may be hidden

[3] While we could not determine to what extent AI technology is employed at the present stage, it is a first step towards meeting security officials' demand for quick communications with borders and "smart borders", see Hanlon, Q., & Herbert, M. (2015): *Border Security Challenges in the Grand Maghreb.* United States Institute of Peace.

to the human eye. Hence, it lends itself to applications in situational awareness and prediction, where data may come from hundreds of thousands of sources (e.g., social media, mobile phone connection data, CCTV imagery, etc.) that need to be combined and automatically assessed in order to distil relevant insights and conclusions. As such, we found no evidence of current use of this kind of AI technology by MENA governments. However, various global and European stakeholders are developing solutions to use AI for predicting migration flows, in particular from the MENA region towards Europe. Even if still in an exploratory development stage, such tools will eventually spread to the MENA region as well. At the same time, China's growing investments in surveillance technology – although still maintaining a lower profile in the MENA surveillance market, as detailed in chapter 2 – is increasingly offering countries around the world alternative supplies for highly intrusive tools and systems.

Various global and European stakeholders are developing solutions to use AI for predicting migration flows, in particular from the MENA region towards Europe

Other AI-related applications intended for border control and surveillance are autonomous vehicles (land, maritime and air) that can enrich the information domain for live situational awareness. The EU-funded ROBORDER project developed various robots for the early identification and tracking of illegal activities and communications. The PGuard by Tunisian producer Enova Robotics is a fully autonomous and self-driving robot capable of patrolling and detecting intrusions based on AI – though it is mostly exported to European and US markets.

When evaluating these developments, it is important to consider the double-edged nature of such tools. While the technology may be neutral in its predictions, these predictions may lead to highly diverting political decisions. For example, when anticipating an uptick in refugee flows, a government might either decide to set up arrival facilities and prepare asylum procedures, or instead to build up fences and other security measures to stop refugees from entering the territory.

In addition to tools targeted at predicting migration movements, AI tools in border contexts can also be used for trade-related aspects, e.g. to improve customs checks by predicting shipments that qualify for further inspection. This is demonstrated by a pilot project in the UAE. Dubai Customs launched the Siyaj (Fence) initiative in 2020 to improve security and shipment inspection around its ports. The integrated control system is equipped with AI technologies that conduct deep learning on a central database – fed with data from advanced inspection systems and surveillance devices – to detect illegal shipments and deploy drones or rapid intervention teams for manual inspections (Dubai Customs, 2020).

AI technology in counter-terrorism

AI technology can also be used in counter-terrorism, which – given the cross-national nature of many terrorist activities – is often related to border security. AI, machine learning and big data have been used to determine the structure of terrorist organisations and networks, detecting terrorist propaganda, or locating individuals. In this context, new technologies and enablers such as biometrics become relevant for various security-related applications, including both border management and countering terrorism (i.e., identifying terrorist networks or detecting materials suspected to be used to conduct violent acts).

This is reflected in the security-based justification of the Moroccan government for having introduced biometric ID cards: "to simultaneously fight terrorism and guarantee respect for 'citizens' rights and liberty'" (Rutherford, 2009).

Across the MENA region, Israel is most advanced when it comes to using AI technology for counter-terrorism. Shin Bet, Israel's internal security service, invested in technologies related to big data, learning systems and AI for impeding terrorist attacks before they occur. More than a quarter of the Shin Bet's employees have a technological orientation, highlighting the scale of investments and direction of travel. Through the Information Systems Technology division, the agency is developing programmes on computer vision, speech recognition, data mining and natural language processing (Ganor, 2019). The implementation of some of these technologies in border contexts has created concern. The above mentioned automatic facial recognition technology for checkpoints in the West Bank has reportedly been covertly and illegally used by security services to monitor Palestinians in East Jerusalem (Ziv, 2019). AnyVision, the company providing the technology, so far denied the "unlawful or unethical usage" of its technology for surveillance. Still, it markets its products as capable of identifying and tracking suspects in real-time, predicts dubious behaviour and carries out analysis post-incident (Weitzberg, 2021). However, such predictive analysis of terrorism has been repeatedly criticised for being ineffective, risky and inappropriate, with one study finding some 100,000 false positives for every real terrorist detected (Munk, 2017).

In sum, beyond some anecdotal uses and justifications, AI for counter-terrorism is in an early stage of development and use, and there are considerable doubts about its performance. Still, the sensitive nature of the topic and its many possible repercussions for civil liberties and human rights warrants continued and cautious analysis of its developments and rollout.

Obstacles and enablers of AI in border management

As the stocktaking exercise demonstrates, information about the use of AI in border management in the MENA region is varied but overall scarce. This is partially due to a challenging information landscape that makes it hard to come across reliable data, but mainly because of the fact that AI technology is not very advanced throughout most MENA countries – with Israel and some Gulf states being notable exceptions. Across the MENA region, the level of adoption of AI for border management purposes shows considerable variation with regards to the extent, scope and maturity of actions. Overall, though, we only found scattered examples of current use of AI for border management. While this observation applies to many emerging technologies across a range of use cases and sectors in the region, it seems especially pronounced in the field of law enforcement and border management, suggesting that a) the region remains a laggard with relatively low levels of technology uptake; b) there is low demand for AI-based border management solutions; c) there is insufficient supply for AI-based border management solutions; d) the technology is simply not suited for these types of use cases; e) a combination of these factors. Given the region's myriad security challenges, this raises the question of whether there may be missed opportunities here. In this respect, which are the obstacles to the rollout of AI technology in the region's border management systems? Which risks and opportunities are associated to these deployments in the region?

AI for counter-terrorism is in an early stage of development and use, and there are considerable doubts about its performance

Obstacles	Enabling factors
• Economic: Low cost of labour • Operational: Low technical capacity • Legal: Lack of legal frameworks • General lack of maturity of relevant technologies • Linguistic and cultural barriers	• Biometric rollout • Ambitious AI strategies and room for experimentation • Structural factors: Performance gains, unique big data analytics capabilities • External pressure (EU, US, Russia, China)

Source: Compiled by the authors.

The overall maturity of AI-enabled technologies in border control is still quite low, meaning that there are few established products and off-the-shelve solutions available for purchase and deployment

When tracing the factors that are holding back uptake of AI tools amongst the region's least advanced countries, the following appear most relevant: (1) low cost of labour renders automating many security and surveillance tasks cost-inefficient; (2) low technical capacity, especially of law enforcement agencies, is a big obstacle to the introduction and use of AI tools; (3) lack of legal frameworks and coordinated AI policies (or, where they exist, they do not address law enforcement and border management aspects).[4]

This contrasts with other MENA countries, which are more affluent and technologically advanced, such as Israel, Qatar and the UAE. Here, we observe a concerted push to introduce AI into all aspects of public life and, accordingly, the use of biometric identification and other AI tools for border management is much more widespread. Yet, as discussed below, certain regional and cultural idiosyncrasies slow down the rollout of AI technology even in these higher-performing countries.

In addition, the overall maturity of AI-enabled technologies in border control is still quite low, meaning that there are few established products and off-the-shelve solutions available for purchase and deployment.

Two more, region-specific factors seem also to be slowing down the pace of AI development, affecting countries across the MENA region: linguistic barriers limit the power of current text/language-based AI applications, and regional (religious) customs, especially veiling, hamper the more widespread use of facial recognition technology.[5] However, some countries seem eager to turn these regional peculiarities into growth opportunities rather than stumbling blocks. For instance, many Gulf states are rolling out iris scanning technology as a viable alternative to facial recognition, thus avoiding the limitations posed by veils. The pandemic-induced wearing of masks or other face coverings has globalised this issue to basically all producers of facial-recognition technology, though de-masking is still relatively easy as it leaves more facial features visible

[4] It is important to point out that some countries do achieve higher technological uptakes despite or even because of the lack of regulation. Indeed, restrictive or precautionary regulation, albeit enhancing legal clarity, may even establish further obstacles to uptake, especially in a low-income, low-tech business environment. On the other hand, many international technology leaders are cautious about the reputational and operational risks of entering under-regulated markets. This undermines an important channel of technology transfers – a growth driver especially relevant in the emerging AI market.

[5] While some companies declare that they have the ability to overcome the mask and recognise the person, a technical executive of a company affirmed that veiling is one of the main obstacles to facial recognition in Muslim countries. Contrary to mask, no information was found that the companies are able to overcome the veiling and recognise people.

than many forms of veils. Some countries also specifically aim to become leaders in the development of Arabic-language AI tools,[6] which – as one of the five most spoken languages worldwide – has the potential of becoming a huge market. These Arabic-language tools would be essential for the eventual development of region-specific AI-based counter-terrorism or otherwise security-relevant surveillance tools.

We furthermore observed that, across the region, the trailblazers of using AI in border management often seem to be private sector actors, notably airport management and airlines.[7] The Gulf states are exceptions to this pattern, since they are home to some of the world's most experimental and technologically advanced police forces. In addition, the Gulf states tend to be characterised by a blurring between state-owned carriers and public authorities, which may accelerate the introduction of AI tools but also raises concerns over privacy and civil liberties.

Biometric and/or AI-based airport personnel access controls and automated passenger check-ins are of course no substitutes for the traditional, officer-led border checks. Yet, they present a crucial precursor for later advances and, increasingly, countries are piloting the use of fully automated border checks, as in Saudi Arabia or the UAE. The introduction of AI-powered facial recognition and other biometric technology to airports as one of the most prominent border crossings will familiarise both travellers and border agents with the tools and procedures, thus facilitating their eventual integration into border controls. Experiences with dissatisfied workers at Egyptian airports, who were sceptical of biometric controls, highlight the need for gradual implementation and accompanying awareness-raising measures if one wants higher acceptance by target populations. This is especially relevant in authoritarian settings, where citizens may rightly be concerned about ceding critical data to the state. Furthermore, technology and capability transfers from (mainly foreign) private enterprise to government and security agencies are likely to accelerate the spread of AI, a factor even more relevant for those countries that may otherwise lack the necessary technical expertise and talent for cutting-edge technology.

Technology and capability transfers from (mainly foreign) private enterprise to government and security agencies are likely to accelerate the spread of AI

While obstacles are plenty, several enablers are being put in place across the region, which could facilitate the eventual introduction of AI-based border management technology. Amongst those, the most relevant enabler is the rollout of biometric identity documents, which over the past years occurred in most of the countries in the region.[8] Egypt, Syria and Tunisia are prominent cases still without biometric ID cards or passports, with Tunisia standing out for its parliament citing privacy grounds as the reason to reject it. While war-torn Libya and Yemen have also not yet introduced fully-fledged biometric ID systems, the latter has previous experience with a comprehensive biometric voter registration database covering the data of 14 million voters (M2SYS, 2014).

A second enabler may be the rollout of ambitious national AI strategies as the most visible proof that the government is considering the technology (see also the discussion on AI regulation in Kristina

[6] E.g., the Qatar Computing Research Institute or Saudia Arabia's King Salman Global Academy for Arabic Language in cooperation with THIQAH Business Services.

[7] E.g., Emirates or the Egyptian Holding Company for Airports and Air Navigation.

[8] See infographic.

Kausch's chapter of this volume). While there is currently a general lack of legal certainty and political frameworks to steer the development of AI, there are several noteworthy developments to address this gap. Several Arab countries have recently published AI strategies (UAE in 2017, Qatar in 2019, and Jordan in 2020). However, these strategies have in common that there are no mentions of the technology's potential use for law enforcement, border management, counter-terrorism, and/or other security concerns.[9] The same applies to the existing AI strategies of North African countries, notably Algeria (2020) and Egypt (2021), and others in progress like the case of Tunisia. Meanwhile, others such as Morocco have not yet developed a national strategy but dedicate public resources to research on AI (Okechukwu Effoduh, 2020). Saudi Arabia and the UAE stand out for an experimental, trailblazing openness when it comes to implementing AI and other new technologies into their security and law enforcement agencies. Using sandboxes and piloting programmes may be an effective way for governments across the region to enhance the pace of technology uptake, though the often impromptu nature of such initiatives also augments the associated risks.

A third enabler is more structural: the potential of improving law enforcement performance and reducing harm (e.g., faster identification of terrorists or better control of irregular border movements) may provide a powerful imperative for fast and unfettered deployment. In addition, economic benefits (cost cuts), as well as external pressures (e.g., international aviation security standards, requirements in partnerships/funding programmes), may accelerate the transition towards more AI in border management and law enforcement. Indeed, we found that external pressures and cooperation have played a critical role in the deployment of facial recognition technology at Egyptian airports, in the construction of smart border components in Tunisia, and in various instances of technological capacity-building of police and security forces across the region. As the world is accelerating the development and use of AI, this trend will likely increase even further the expectations, demands and supplies for such technologies to law enforcement and security agencies across the region.

De-humanising borders? Risks and opportunities of AI border management

Some of the most pertinent risks and opportunities related to the use of AI in border management reflect universal concerns in the global debate on AI

Some of the most pertinent risks and opportunities related to the use of AI in border management reflect universal concerns in the global debate on AI. However, it is important to highlight how they play out in the MENA region and how regional idiosyncrasies render these concerns more or less salient. There are clear advantages of developing and rolling out certain AI technologies in border-related security domains, such as improved cross-border flows (of passengers and goods) and potential harm reduction (identification of criminal activity, combating cross-border terrorism). However,

[9] The analysis of AI strategies yielded very few examples of the use of AI in border management and even fewer mentions of counter-terrorism strategies, despite the many security problems of the region. There are at least four possible explanations for why law enforcement and border management are not addressed in these strategies. First, it may simply have escaped policy-makers' minds as the initial public debate is focused on less concrete, abstract problems. Second, it was a strategic choice by governments to leave these sensitive issues out of the scope of their AI policies. Third, the broad high-level nature of these documents led their authors to refrain from spelling out such specific use cases, which would be developed in subsequent plans. Fourth, they consider that AI technologies will be not useful or available for their countries for law enforcement and border management. If it was indeed a purposeful omission, was it to stifle debate or because governments do not want to go down this path?

the introduction of AI in the region's security sector also bears many risks. Across the region, there is relatively little debate about these issues. Whether this may be a reflection of political realities in which other more pressing issues dominate the agendas, or in which public criticism of government policy is stifled by repressive regimes, or of more general deficits in AI capacities – it is extremely problematic for the prospects of introducing AI in a way that is compatible with human rights and civil liberties.

In terms of risks, the use of AI in border management suffers from some of the common pitfalls that characterise present-day algorithmic technology across application domains. The underlying data may be biased or inaccurate and, consequently, algorithms often produce erroneous outputs. As a recent report on facial recognition technology deployed in border-crossing contexts such as airports notes, even the best algorithms misrecognise black women twenty more times than white men (Israel, 2020). This in turn might lead to a racialised differential treatment, perpetuate negative stereotypes or discriminate against certain groups. In other settings, high false-positive rates may be costly as patrol units will have to be deployed unnecessarily. Worse yet, individuals that are unwarrantedly flagged for searches or even subjected to pushbacks may see their human rights violated. In the absence of clear and solid legal frameworks on both AI and human rights safeguards, there is no effective path for legal redress or other forms of accountability, meaning that wrong decisions or systematically flawed technology are unlikely to get corrected.

Beyond such technical flaws, the main risk lies in the enormous potential of technology-enabled human rights abuses, and AI tools in border contexts are no exception here. The widespread use of biometric ID systems and weak privacy laws, in conjunction with generally weak rule of law and human rights protections, opens the door to authoritarian abuses. In this regard, the security sector's sensitive nature augments any ethical concerns related to the technology's risks and opportunities. In a border context, AI tools may further inhibit freedom of movement and international travels of potentially persecuted citizens, as highlighted by the case of Patrick George Zaki, an Egyptian student activist who was retained at Cairo airport upon returning from his research stay in Italy (Al Jazeera, 2020). Many of the applications discussed above can easily be repurposed to target different populations or to perform different tasks. Thus, a facial recognition software initially sold to a government to enable it to quickly identify international terror suspects at airport crowds could end up in the hands of the domestic security apparatus of repressive regimes, serving to track down opposition members, critical journalists, or other unwanted individuals. Ample scenarios and examples of how AI technology can bolster authoritarian governments and practices across the region form a common thread across all chapters of this volume.

Furthermore, the introduction of intrusive technologies into border control threatens the rights of already vulnerable populations. As a United Nations (UN) report warns, "governmental and humanitarian biometric data collection from refugees and migrants has been linked to severe human rights violations against these groups" (Achiume, 2020). Data collection by border surveillance systems usually occurs without taking the consent of migrants – or, where it happens, it may be under questionable quasi-coercive conditions.

The introduction of intrusive technologies into border control threatens the rights of already vulnerable populations

Lastly, there are arguments to be made that are familiar from weapons proliferation discussions: what happens when security-relevant digital infrastructure such as

government-level AI tools falls into the wrong hands? Even when assuming that governments and businesses operating under their jurisdiction are benign actors and follow established rule-of-law principles and human rights standards, there would still be grounds for concern in a region ripe with security issues and political instability. Grave issues with rolling out technology that gathers and stores sensitive personal data have been brought to light by recent developments in Afghanistan. The sudden takeover of the Taliban has also given them access over massive biometric databases and equipment, reportedly including iris scans, fingerprints, and other sensitive data of Afghan security forces (Guo & Noori, 2021). While it is unclear whether and how they will be able to use this data – much of which is stored on remote servers – there are reasonable fears of reprisals and targeted retribution against Afghans collaborating with the previous government. Even beforehand, there were reports about Taliban fighters using biometric devices to identify their victims – likely enabled via collaborators who worked for the government and thus had access to the databases. For precisely those concerns, US troops that gathered troves of biometric data on around 3 million Iraqi collaborators decided to not pass over that information to the Iraqi government after their withdrawal, worrying that it could become a hit list if it gets into the wrong hands. Instead, the data is stored and controlled within the US – which ensures data security but also raises numerous ethical questions over the legitimate ownership of the data or the right to privacy of those included therein. This underlines how international partners cooperating on data- and AI-based technologies in volatile environments need to put extra effort on privacy and data security aspects, putting in place contingency plans as well as meaningful ways to control access to critical information. This is especially relevant for border-related applications such as visa or entry/exit registries and biometric databases more widely, all of which contain potentially critical information.

Keeping in mind these substantive risks, there are also opportunities to be found with the introduction of AI technology in border management. Automated identity checks not only allow for more convenient, accelerated passenger flows, but also facilitate the matching of passenger records against local and international databases of wanted criminals or terror suspects. For instance, INTERPOL's facial recognition system has helped identify "almost 1,500 terrorists, criminals, fugitives, persons of interest or missing persons" since its launch at the end of 2016 (INTERPOL, n.d.). Currently, this process is not automatically integrated into border checks, and potential matches require manual review by human INTERPOL officers. Yet, the current pace and trajectory of the rollout of facial recognition technology suggests that, within a few years, the necessary infrastructure will be in place to upscale such systems. Furthermore, besides the INTERPOL database to which access is moderated and relatively restricted, national governments are most likely going to build up their own lists. In this light, it becomes all the more urgent to develop regulatory and governance principles that ensure respect for privacy, proportionality, transparency and accountability in how this technology is used.

Additionally, familiarity with AI tools for a given application often paves the way to other use cases, inspiring security agencies to invest in necessary talent and equipment. For instance, knowledge and tools for airport crowd controls and video recognition may also be useful at smart borders and satellite image analysis, where they can facilitate the control of irregular migration routes, which are often abused by transnational terrorist networks (Monroy, 2020). Likewise, AI-powered surveillance and social media screening tools may flag po-

tentially dangerous passengers and subject them to more detailed screening by border guards. Such software may also serve as a sentinel for migration flows (e.g., by picking up anomalies in the connections of remote cell towers, by tracking social media users' location data, etc.).

Yet, precisely this cross-fertilisation – if left unchecked – could further aggravate the aforementioned risks. For instance, AI tools and knowhow originally developed for legitimate border control and counter-terrorism purposes may also be used to identify protestors, track down critical journalists or identify opposition networks. Accordingly, there are a number of considerations that responsible lawmakers, governing bodies and law enforcement agencies in the MENA countries need to address when rolling out AI-based technologies. These are equally relevant for EU policy-makers aiming to support the region's trajectory towards democratic governance and rule of law.

Conclusions and policy recommendations

At present, the use of AI by the region's security agencies is mainly devoted to lower-level border control, compared to the more advanced uses in domestic surveillance. Although great ambitions laid down in national AI strategies contrast with still rudimentary implementation overall, there is considerable variation in the extent of AI tools being used, and other forms of application are spreading fast. Throughout the region, AI can plausibly contribute to improving crucial aspects of border management and related security aspects. However, precautionary measures, such as those outlined below, are a must if the potential downfalls are to be avoided.

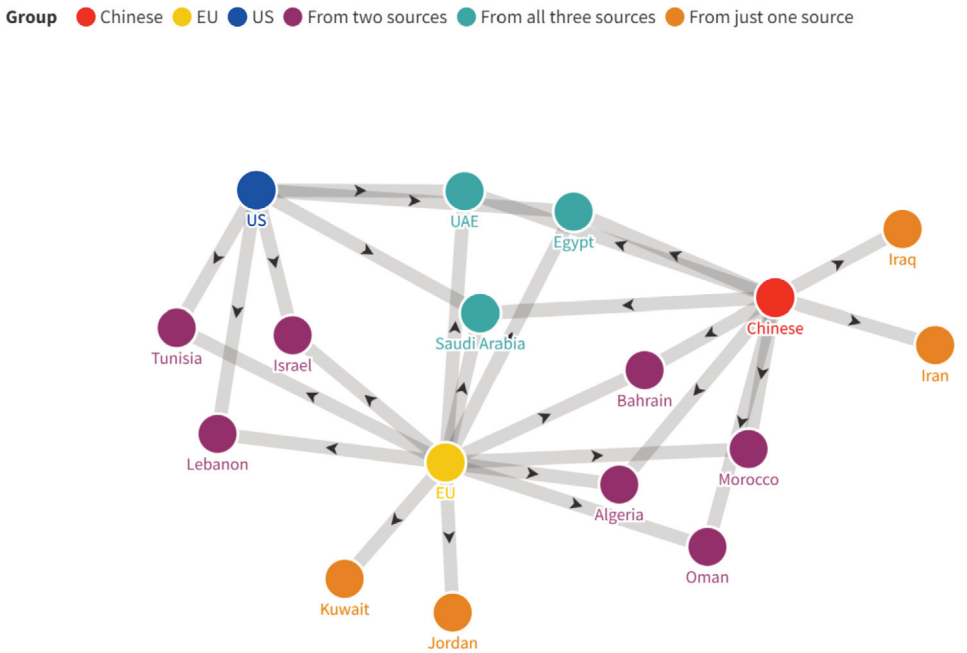
To ensure accuracy, fairness and proportionality of the employed technologies, the relevant authorities should strive for a maximum degree of transparency and accountability. This may contradict long-held instincts of security services, who are used to operating in the dark. However, the immaturity of current AI systems has repeatedly led to systematic errors and built-in biases, which are not easy to detect and may result in unintended consequences. Given the currently low levels of technological capacity in most of the region, transparency and external scrutiny will reduce the likelihood of such malfunctioning. Furthermore, it will add to societal trust in these systems in the long term, which is an essential precursor for their eventual large-scale, frictionless deployment.

There are a number of considerations that responsible lawmakers, governing bodies and law enforcement agencies in the MENA countries need to address when rolling out AI-based technologies

Such confidence-building measures will also increase the appetite for leading international AI developers to engage with MENA partners in on-the-ground projects, as it reduces the reputational and operational risks. There is high potential for technology transfers and capacity-building via public-private partnerships (PPP), especially for emerging technologies such as AI, and this has also been manifested in the context of border control. Additionally, governments can encourage the piloting of such technology by private sector entities – who, in the absence of local rules and regulations, would ideally stick to European standards.

Overall, the use of AI technology in border control and counter-terrorism is still nascent, and MENA countries should not rush their deployment. However, now is a good moment to lay the ground for their eventual gradual introduction so that, as the technologies mature and develop, the countries will already have corresponding frameworks and sufficient capabilities to absorb and integrate them. In this light, there are some steps that the EU side can take to support willing partners from the Southern Neighbourhood.

Figure 1. Supply of AI technologies (by source)



Source: Compiled by the authors based on primary and secondary sources. The figure summarises available information on tech origins for the use cases of AI-related technologies in border contexts (including biometric systems).

1. Early-stage EU programmes aiming to support MENA governments in developing their AI capacity should adopt a sequenced model that focuses on laying the groundwork first: establishment of legal and regulatory frameworks for AI oversight mechanisms/institutions. As the EU is often perceived as a reference actor in regulatory and ethical questions on AI, it should use its standing to leverage the implementation of high standards in its partners from the Southern Neighbourhood, especially for such high-risk applications as border control and counter-terrorism. Where domestic frameworks are lacking – or where there are justified doubts regarding their enforcement – the EU should at the very least require adherence to internationally agreed minimal standards, such as the Organisation for Economic Co-operation and Development (OECD) Principles on Artificial Intelligence.
2. Secondly, they should also focus on building up healthy domestic ecosystems, which can generate local talent and technological capacity, both from a development and use perspective, but also from an institutional, journalistic and civil society "control" perspective.
3. Moreover, it is recommendable to follow the early developments in the applications of AI in counter-terrorism or facial recognition of veiled people through research programmes that consider both technical and socio-political aspects. This is a nascent field where law and ethical standards will need to develop in accordance with EU regulation, which, given their prominent role, can shape standards and rules around the world.
4. The EU should take a more active role and geopolitical vision in the promotion of trustworthy AI technologies and companies. As the infographic shows, EU

Where domestic frameworks are lacking – or where there are justified doubts regarding their enforcement – the EU should at the very least require adherence to internationally agreed minimal standards

and US producers of relevant technologies already have a considerable footprint in the MENA region. Yet, Chinese competition is fast increasing its presence across these markets.

5. In all this, the increasing use of AI technology in critical sectors such as border control should reinforce the EU's cautionary approach to technology exports, especially those considered dual-use. One concrete step to ensure transparency and accountability around exported AI tools would be the creation of an algorithmic transparency register, akin to those developed by the city governments in Amsterdam and Helsinki. Such a register would list all technology exports and deployments which are co-financed by the EU or which had required approval of an EU export licence. Furthermore, the EU should continue to mainstream the so-called "human security" dimension into all of its police training, capacity-building and cooperation missions.
6. Related to dual-use issues, it is furthermore crucial to sharpen the definition and specifically target tools that can affect civilian security concerns. At present, the EC communicates about "civilian goods and technologies with possible military *or security use*" (highlight by authors), whereas the regulation refers only to "civilian and military" uses, thus restricting the scope significantly and potentially circumventing the regulation's applicability regarding border control tools, which are often operated by police forces (and hence considered civilian). A dedicated research programme or commissioned Joint Research Centre study on this potential grey zone may provide clarity and outline paths for addressing this problem.

References

ACHIUME, E. T. (2020). *Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance.* United Nations.

AL JAZEERA (2020, February 9). *Egypt arrests, tortures human rights advocate: Rights group.* Retrieved from https://www.aljazeera.com/news/2020/2/9/egypt-arrests-tortures-human-rights-advocate-rights-group

DUBAI CUSTOMS (2020, August 06). *Dubai Customs launches Siyaj (Fence) Initiative to foster border security, facilitate trade.* Retrieved from https://www.dubaicustoms.gov.ae/en/NewsCenter/Pages/NewsDetail.aspx?NewsID=1515

GANOR, B. (2019). Artificial or human: A new era of counterterrorism intelligence? *Studies in Conflict & Terrorism, 44*(7), 605-624.

GUO, E., & NOORI, H. (2021, August 30). *This is the real story of the Afghan biometric databases abandoned to the Taliban.* MIT Technology Review. Retrieved from https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/

INTERPOL (n.d.). *Facial recognition.* Retrieved from https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition

ISRAEL, T. (2020). *Facial Recognition at a crossroads: Transformation at our Borders & Beyond.* Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.

M2SYS (2014, August 19). *M2SYS Technology deploys TrueVoter biometric voter registration software solution In Yemen.* Retrieved from https://www.m2sys.com/m2sys-deploy-truevoter-yemen-biometric-voter-registration-solution/

M2SYS (n.d.). *Biometric system for Iraqi border patrol security.* Retrieved from https://www.m2sys.com/biometric-fingerprint-software-case-studies-iraqi-border-control/

MAGMA BSP (n.d.). *MAGMA BSP traffic managment solutions.* Retrieved from https://magnabsp.com/about-us/

MONROY, M. (2020, June 28). *EU pays for surveillance in Gulf of Tunis.* Retrieved from Digit.site36 Web site: https://digit.site36.net/2020/06/28/eu-pays-for-surveillance-in-gulf-of-tunis/

MUNK, T. B. (2017). 100,000 false positives for every real terrorist: Why anti-terror algorithms don't work. *First Monday, 22*(9).

OKECHUKWU EFFODUH, J. (2020, October 20). 7 ways that African states are legitimizing artificial intelligence. *openAIR.* Retrieved from https://openair.africa/7-ways-that-african-states-are-legitimizing-artificial-intelligence/

OZBERK, T. (2021). Unmanned tech dominates Turkey's border security summit. *Defense News.* Retrieved from https://www.defensenews.com/unmanned/2021/10/28/unmanned-tech-dominates-turkeys-border-security-summit/

RUTHERFORD, M. (2009, December 1). Morocco issues biometric ID cards. *CNET.* Retrieved from https://www.cnet.com/news/morocco-issues-biometric-id-cards/

WEITZBERG, K. (2021). Biometrics and counter-terrorism: Case study of Israel/Palestine. *Privacy International.* Retrieved from https://privacyinternational.org/sites/default/files/2021-06/PI%20Counterterrorism%20and%20Biometrics%20Report%20Israel_Palestine%20v7.pdf

WORLD BANK (2017). *Impact of the Libya crisis on the Tunisian economy.* Retrieved from https://documents1.worldbank.org/curated/en/517981490766125612/pdf/ACS16340-WP-P158090-PUBLIC-Impact-of-Libya-Crisis-on-the-Tunisian-Economy-Long-Version.pdf

ZIV, A. (2019, November 02). Israeli face-recognition tech used within Israel against law, NBC investigation finds. *Haaretz.* Retrieved from https://www.haaretz.com/israel-news/.premium-israeli-face-recognition-startup-used-in-east-jerusalem-nbc-investigation-finds-1.8057282

Digital Surveillance, Master Key for MENA Autocrats

Žilvinas Švedkauskas
PhD candidate, Eberhard Karls Universität Tübingen

The adoption of artificial intelligence (AI)-enabled technologies has revolutionised surveillance in the Middle East and North Africa (MENA) region. A decade after the Arab uprisings, the question as to how new technological breakthroughs in AI will transform these information operations in the coming years is quickly gaining relevance as authoritarian regimes in the MENA region have consolidated power domestically and seek to expand their influence abroad.

Authoritarian resilience in the region broadly rests on the adaptive capabilities of incumbent governments and their success in utilising advances in digital technologies to enhance political control. As reports by digital rights groups like Citizen Lab, Access Now (2020) or Amnesty International (2022) vividly illustrate, MENA state agencies have continuously weaponised digital tools against non-state actors such as journalists, academics and activists. AI-assisted digital technologies have effectively prolonged the reach of MENA security agencies, enabling them to go after dissidents both at home and abroad (Ševkauskas, 2019). Moreover, recent revelations that the Moroccan secret services used sophisticated spyware to surveil the French President Emmanuel Macron, his ministers, and prominent journalists (Chrisafis et al., 2021) show that MENA governments do not shy away from instrumentalising AI-assisted technologies vis-à-vis a member state of the European Union (EU).

Though cybersecurity is often defined as providing safety "*for* the state *from* decentralised actors" (Egloff, 2022; Abrahams, 2021), evidence from the MENA region turns these assumptions upside down. In the light of the fact that MENA countries come third after China and Russia in contemporary debates on "digital authoritarianism" (Polyakova & Meserole, 2019), this chapter focuses in on AI-enabled digital surveillance as yet another item on the authoritarian "menu of manipulation" (Schedler, 2002).

In a nutshell, digital surveillance provides a master-key for MENA autocrats: it facilitates identification, targeting and repression of dissidents, follow-up tracking of their associates, whereas manipulation of social media platforms via bots and trolls enables the narrative to be reshaped around their surveillance-related deeds. As the following sections narrate, thanks to AI technologies, such information operations are more far-reaching and comprehensive than ever.

Academic and policy literature presents a general distinction between targeted and mass surveillance (Shires, 2021). While most of the public attention and reporting focuses on targeted surveillance of high-profile individuals, like President Macron or Saudi dissident Jamal Khashoggi, in scope it accounts only for a fraction of surveillance of national internet communications via deep packet inspection (DPI). Major progress in AI of the past years, including machine learning for clustering, speech recognition and -generation, natural language processing, image and video generation, autonomous decision-making and intelligent personal assistance, has provided impetus for upgrading both mass and targeted surveillance solutions.

To account for political implications of fast-paced technological transitions, this chapter explains how AI boosts different types of surveillance, and maps known digital surveillance abuse cases involving MENA law enforcement, security agencies and external subcontractors dominating the regional market.

Mass surveillance: automated internet-filtering

DPI technology enables real-time monitoring and analysis of incoming and outgoing internet traffic, packets of data passing through national networking hubs, effectively establishing a gate-keeping filter for all internet traffic to and from servers within national jurisdiction.[10] With DPI in use, network operators can identify the origin and content of data packets, categorise them, and automatically filter the internet traffic. If needed, DPI may be used to monitor all traffic from a specific IP address or a mail server, and even reassemble e-mails as they are typed. Hundreds of thousands of transactions can be monitored each second. With the introduction of machine learning, DPI systems can achieve greater precision in categorisation and are able to automatically update themselves to recognise evolving attempts at DPI circumvention through encryption or virtual private networks (Nguyen & Armitage, 2008; Trivedi & Patel, 2016).[11]

Beyond mere monitoring, DPI is also used to speed up, slow down, block, filter, or otherwise make decisions about the incoming internet traffic. Mostly deployed for benign uses such as network management, targeted advertising or dealing with copyright infringements, DPI is however also instrumentalised as a tool for government surveillance and fine-grained censorship which does not require nationwide internet shutdowns or blanket bans on social media platforms (Mohalski & Schulze, 2011; Parsons, 2009; Shires, 2021).

While government actors such as law enforcement or security agencies themselves do not usually possess the necessary hardware or the right kind of technological expertise to deploy DPI, they subcontract these services to private entities. National telecommunication companies and internet service providers (ISPs) occupy a central position in this ecosystem. Communications ministries, information technology authorities, or national cybersecurity institutions in the MENA region mandate telecom companies and ISPs to install and run DPI solutions and provide access to gathered personal data for security and law enforcement agencies upon request (Shires, 2021). For example, since 2018 the Egyptian cybercrime law obliges ISPs to retain users' personal information and details of their online activity, which must be released to security bodies upon request (al-Abd, 2018).

While MENA countries remain net importers of digital infrastructure (UNCTAD, 2022), regional telecoms and ISPs turn to leading international tech corporations for deploying and upgrading AI-assisted DPI tools.[12] Interestingly, some of these companies have been red-flagged by digital rights groups for breaching guiding principles on business and human rights.[13]

Beyond mere monitoring, DPI is also used to speed up, slow down, block, filter, or otherwise make decisions about the incoming internet traffic

Since most of the deals in the DPI industry remain undisclosed, leaked contracts between MENA governments and international

[10] Interview with a computer science expert, December 3, 2021.

[11] All DPI products currently in use benefit from artificial intelligence/machine learning techniques for making sense of collected data. For example, see CISCO (2021).

[12] According to Research and Markets (2021), the major players in the global DPI market are predominantly American, and include Cisco Systems, IBM, HPE, Palo Alto Networks, and Extreme Networks. American Israeli Check Point Software Technologies, Israeli Allot Communications, Chinese Huawei Technologies, Canadian Sandvine Incorporated also have a stake in the global DPI market.

[13] See UNOHCHR (2021).

In the aftermath of the 2011 Arab uprisings, a fast-paced diffusion of DPI tools in the MENA region has been well documented

DPI suppliers, together with code traces on the world wide web discovered through digital forensics serve as main evidence for deployment of mass digital surveillance solutions. Interestingly, instead of sub-contracting industry's frontrunners, MENA governments seem to prefer to deal with second-tier players in the global DPI market, which may be explained by a lower level of international scrutiny and pressure for applying end-use monitoring faced by these enterprises.[14] Canadian, American and French companies have been red-flagged so far (Dalek et al., 2016; Dalek & Senft, 2011; Privacy International, 2016).

In 2015, the Moroccan government was revealed to have invested 2 million euros in the Eagle surveillance system. After the Arab Spring protests in 2011, it allowed the government to perform censorship and monitoring of internet traffic using AI-assisted DPI. Eagle was developed by Amesys (currently Nexa Technologies), a French company that also sold DPI technology to Libyan security agencies under the former President Muammar Ghaddafi (Champagne-Kitetoa 2015).[15] Around the same time, reports found DPI solutions developed by California-based ICT company Blue Coat being used to monitor web traffic and block access to websites in Syria, Bahrain, Qatar and the United Arab Emirates (UAE) (Valentino-De-Vries et al., 2011; Dalek & Senft, 2011).

In the aftermath of the 2011 Arab uprisings, a fast-paced diffusion of DPI tools in the MENA region has been well documented. Strikingly, in 2013, 400 devices in 61 countries around the world were found to use DPI for mass digital surveillance with the majority of MENA states represented, including Bahrain, Kuwait, Qatar, Saudi Arabia, UAE, Iraq, Lebanon, Egypt and Turkey (Marquis-Boire et al., 2013). Local private actors have facilitated the technical uptake of AI-enabled mass surveillance capacities of the Arab states by mediating between Western companies and law enforcement and security agencies in the region. For example, a reseller in the UAE was sanctioned by the US Bureau of Industry and Security for re-exporting Blue Coat products to the Syrian regime (2020). In another instance, in 2014 Egyptian state security openly announced that it would install Blue Coat DPI acquired via a local reseller "See Egypt" to not only counter radicalisation online, but to also to monitor LGBTQ+ websites and social media platforms *en masse* (Frenkel & Atef, 2014).

Digital repression of MENA civil society and minority groups assisted by Western DPI technologies comes in two forms. First, by blocking freedom of expression online. AI-powered categories curated by Canadian DPI Netsweeper[16] have been found to facilitate miscategorisation and censorship of content associated with LGBTQ+, civil rights and advocacy organ-

[14] Interview with MENA cybersecurity expert, February 15, 2022. It is important to note that the role of frontrunning tech corporations in MENA DPI market may also be overlooked, as most of them provide telecom products across the board and thus receive less attention than companies specialising solely in privacy-sensitive DPI.

[15] In June 2021, executives of Amesys were found complicit in torture for sales to the Libyan government and forced disappearance in relation to product sales to the Egyptian government by the Paris Judicial Court (Business & Human Rights Resource Centre, 2021).

[16] Netsweeper's white paper argues that its multilingual "Artificial Intelligence engine has categorised over 9 billion websites into 67 categories, such as criminal skills, weapons, pornography, adult, social networking, malware, and phishing […] categorising approximately 22 MILLION new URLs every day!" The same document also advertises Netsweeper's capacities for fine-grained filtering of internet traffic incoming through web apps such as Twitter, Facebook, Snapchat, and its decryption functions (Netsweeper Inc, 2016).

isations, HIV/AIDS health resources, and independent media in the MENA region. As early as 2011, Netsweeper was identified to be monitoring and filtering internet traffic for internet providers in the UAE (du), Qatar (Qtel) and Yemen (YemenNet) (Noman & York, 2011), while ensuing reports also found it employed by ISPs in Bahrain and Kuwait (Dalek et al., 2016; 2018; 2021). Mixed internet forensics also demonstrated how Netsweeper had allowed censorship of freedom of expression in the region, from Shia sites in Bahrain, political platforms in the UAE to independent media outlets in Yemen (Dalek et al., 2016). Another Canadian-developed product, Sandvine PacketLogic DPI devices were used to filter and block dozens of human rights, political and news websites in Egypt and Turkey, including Human Rights Watch, Reporters Without Borders, Al Jazeera, Mada Masr, and HuffPost Arabic.[17] As a second instance of digital repression through DPI, Sandvine technology was employed to redirect hundreds of users on Türk Telekom's network in Turkey and Syria to download FinSpy spyware bundled with legitimate applications, which in turn facilitated more fine-grained surveillance of Kurdish political leaders and activists across the Syrian-Turkish border (see below; Marczak et al., 2018a).

In short, AI-assisted mass digital surveillance of national internet traffic during the last decade became a norm rather than an exception in the MENA region (see infographics towards the end of the chapter). With Western companies and their regional resellers on the supplying side, MENA governments can manipulate ISPs to censor national internet traffic, deny freedom of online expression for independent media outlets, and corner activists and opponents into venues of targeted surveillance.

Targeted surveillance: machine learning for infiltrating smart devices

Spyware is a kind of software that attempts to silently monitor the behaviour of users, records web surfing habits, or steals sensitive data such as passwords, photos, or voice recordings. The collected information is sent back to the spyware operator, who may then use it for unauthorised purposes, ranging from advertising or marketing, information gathering to blackmailing the target (Egele et al., 2007). In authoritarian contexts, spyware is frequently used to keep a check on political opposition and preventing pro-democratic mobilisations. While spyware tools have been around since the early 2000s, integration with machine learning techniques since beginning of the 2010s has broadened targeted surveillance capabilities.[18]

In authoritarian contexts, spyware is frequently used to keep a check on political opposition and preventing pro-democratic mobilisations

Machine learning can be deployed at different stages of spyware attacks (UNICRI & UNOCT, 2021). In addition to speech recognition employed by most popular spyware programmes like Pegasus and FinSpy, which constitutes a subdivision of machine listening stream of AI research used to identify people based on intercepted phone

[17] In 2017, Sandvine was acquired by American private equity Francisco Partners, which until 2019 among other investments in dual use technology held a majority stake in Israeli NSO group, developer house behind the infamous Pegasus spyware (see below).

[18] Interview with a cybersecurity expert, February 15, 2022. AI-aspects of spyware have not been systematically researched and only footprints of targeted digital surveillance by MENA law enforcement and security agencies have been identified through open-source research. Nonetheless, cybersecurity debates and characteristics of freely available "consumer" spyware used for surveilling spouses, children, or business partners (Harkin et al., 2020), provides valuable clues on the ways AI can assist targeted surveillance.

calls and derive other meaningful information (Au, 2021), several other AI-enabled capabilities are employed for targeted surveillance.

First, machine learning can assist in identifying the victims through clustering algorithms.[19] Applied to scraped social media content, critics of the government or supporters of social or political causes, say, LGBTQ+ activists can be identified, their posts then analysed with natural language processing to produce tailored phishing messages, reducing chances of early detection. AI-enabled image recognition tools can further narrow the target group down across different online channels. For instance, American facial recognition software Clearview AI, trained on a database of billions of images scraped from social media platforms like Facebook, Instagram, LinkedIn and Twitter, has been reportedly employed by 88 law enforcement and government-affiliated agencies in 24 countries around the world. Abu Dhabi's sovereign wealth fund Mubadala and Saudi Artificial Intelligence Center of Advanced Studies Thakaa reportedly used Clearview AI to match target photos with samples scraped online, plausibly assisting law enforcement and security agencies in the two Gulf countries (Mac et al., 2021).

Just like instrumentalising individual information found on social media, AI may as well be weaponised to "unlock" smart devices. Machine learning techniques allow automated checks on targeted security protocols and minimise time and manual labour needed for spotting software vulnerabilities used in zero-day[20] and other attacks (Polyakov, 2019). Moreover, machine learning algorithms have been proved to easily bypass passwords and popular security tests for access-authorisation like (re)CAPTCHA (Alqahtani & Alsulaiman, 2020; Hitaj et al., 2021).

At the time of writing, most reported cases of spyware attacks are initiated by convincing victims to click on the link by means of impersonation. Machine learning (especially generative adversarial networks, a machine learning framework for data generation) can be deployed for moulding inauthentic messages on scraped social media posts, emails, or messaging material (King et al, 2020). Moreover, with rapid advancements in AI, not only fake texts but also fake AI-generated voice and video messages asking the target to click on the malicious link can be generated.[21]

Finally, once spyware is implanted the attacker gains access not only to information and resources stored on the device, but also receives the keys from AI-powered intelligent assistants like Siri or Alexa, which have capacities to unlock smartphones without fingerprints, forge emails, control smart homes or virtual banking accounts. As demonstrated by proof-of-concept spyware tests, attackers can exploit intelligent assistants' microphone access, record owners' voice samples, and synthesise activation keys through AI-enabled natural language processing. Machine learning based environment-recognisers may also be in use for launching context-aware information gathering attacks (Zhang et al., 2018).

Deployed complementary to one another, different spyware capabilities allow gov-

[19] Interview with computer science expert, December 3, 2021.

[20] "Zero-day" is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems. A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it (Kaspersky, 2021a).

[21] More on AI in so-called "deepfakes", see Westerlund (2019).

ernments in the MENA region to launch comprehensive surveillance operations and, as examples below illustrate, target hundreds if not thousands of high profile civil society actors, political allies and opponents at once. Recent investigations by digital rights groups point to governments around the world purchasing spyware from companies such as NSO Group, Cellebrite, Intellexa, FinFisher, Gamma International, Hacking Team, and others. All of them insist that spyware tools are used exclusively for countering terror attacks, drug traffickers, paedophiles, and other criminals.[22] Yet continuous reports indicate that authoritarian governments around the world do not shy away from abusing these AI-enabled tools against domestic opposition, critics abroad and even regime insiders. MENA countries are no exception.

Israeli cyber-mercenaries

By many estimates, Israel has become a leading exporter of spyware products thanks to industry's frontrunner, the Herzliya-based NSO group, at the time of writing valued at around 2 billion USD (Reuters, 2021).[23] Since its launch in 2010, its flagship spyware Pegasus can be installed on a smartphone through vulnerabilities in apps, or by tricking a target into clicking a malicious link or via over-the-air messaging (Shezaf & Jacobson, 2018). Once installed, Pegasus can harvest any data from the device, and is capable of employing integrated cameras and microphones to snoop on people in its vicinity, record conversations on messaging applications such as Viber and WhatsApp, tracking target's location and transmitting everything back to the attacker (NSO Group, 2015). According to the NSO Group, Pegasus is sold only to military, law enforcement and intelligence agencies in around 40 unnamed countries, vetted by the Israeli Ministry of Defence and spying on small numbers of "elite" terrorists and criminals.

Deployed complementary to one another, different spyware capabilities allow governments in the MENA region to launch comprehensive surveillance operations

Comparable capabilities are offered by several other Israeli companies like Candiru, Quadream and Cytrox, which also echo the rhetoric of partnering only with vetted law enforcement organisations around the world (Marczak et al., 2021a, 2021b; Megiddo, 2021). Nonetheless, independent sources speak about mass deployment of Israeli-developed AI-assisted spyware and lack of end-use monitoring. The infamous case of Jamal Khashoggi, brutally murdered and dismembered at the Saudi embassy in Istanbul, serves as the most vivid illustration. Recent leaks and forensic analysis of smartphones suggest that Khashoggi, his fiancé Hatice Cengiz, close friends, and even Turkish prosecutor responsible for charging 20 Saudi nationals over the killing were targeted with Pegasus spyware before and after the killing by an operator based in the UAE (Deibert et al., 2019; Kirchgaessner, 2021a). Besides Khashoggi, renowned Emirati human rights defender Ahmed Mansoor,[24] Saudi dissidents Yahya Assiri and Ghanem al-Masarir, and Moroccan human rights defenders Maati Monjib and Abdessadak El Bouchattaoui have been monitored with Pegasus implanted on their smartphones (Marczak & Scott-Railton, 2016; Marczak et al., 2018a;

[22] For instance, see NSO Group Human Rights Policy (2019).

[23] In 2019, the company was acquired by the London-based Novalpina Capital, which bought a majority stake along with the founders of NSO in an acquisition from American Francisco Partners (Solomon, 2019).

[24] In 2011, Mansoor was also targeted with FinFisher's FinSpy spyware, and in 2012 he was targeted with Hacking Team's Remote-Control System (Marczak & Scott-Railton, 2016).

Deibert et al., 2019; Amnesty International, 2019b). In a vivid illustration of the scope of underexplored deployment of Israeli spyware in the MENA region, 2018 internet probing located Pegasus associated servers in nearly every country in the MENA region.[25] A number of cross-border surveillance cases, including Gulf operators conducting surveillance in Canada, France, Greece, the United Kingdom (UK) and the United States (US), and Moroccan operators monitoring targets in Algeria, France and Tunisia were also identified (Marczak et al., 2018b).

More recently, in July 2020, NSO Group leaks revealed that since 2016 more than 50,000 phone numbers were selected as targets by NSO Group clients, among them several MENA governments. The leaks also showed that 10,000 people in Morocco and abroad – ranging from prominent Moroccan journalist Omar Radi to French President Emmanuel Macron, former Prime Minister Edouard Philippe and 13 other ministers, as well as French journalists covering protests in the Moroccan Rif – have had their phones spied on by Morocco's security agencies (Gueguen 2021a; Gueguen 2021b). The analysis of the leaked data identified nine more governments complicit in mass deployment of targeted digital surveillance, including Saudi Arabia and the UAE.

A look at the list of Pegasus targets suggests that surveillance has not only been deployed vertically (security and law enforcement agencies monitoring civil society actors) but also horizontally (security agencies spying on regime insiders) and externally (security agencies targeting heads of foreign states). Remarkably, King of Morocco Mohammed VI and the Moroccan Prime Minister Saad Eddine al Othmani became targets of security agencies of their own country (Chrisafis et al., 2021). Also, according to the leaks, Saudi and Emirati security agencies have surveilled Egyptian officials, including Prime Minister Mostafa Madbouly. Numbers of Barham Salih, the President of Iraq, and Saad Hariri, former Prime Minister of Lebanon, were also entered into leaked NSO database by operators in Saudi Arabia and the UAE (Chrisafis et al., 2021).

After the NSO Group leaks, and the inclusion of the company in the US "entity" list and Israel declaring to slash the cyber exports list from 102 to 37 countries in November 2021 (Orbach, 2021), reports about other Israeli spyware vendors stepping into the MENA spyware market have started to accumulate. Tel-Aviv-based Candiru was found to target at least 100 victims in Palestine, Israel, Iran, Lebanon, Yemen and Turkey among other countries (Microsoft, 2021), while Saudi Arabia and the UAE were indicated as purchasers of Candiru spyware as early as 2019 (Marczak et al., 2021). Representatives of another Israeli spyware vendor, Quadream reportedly visited the offices of the Moroccan security services to discuss selling its surveillance systems to the Moroccan government (Gilead, 2021). Through a complex international structure Quadream operates in Cyprus and does not need a green light from the Israeli Defence Ministry to export its products abroad (Megiddo, 2021). Finally, in December 2021, Predator spyware of another transnational Israeli enterprise Cytrox was detected on the phone belonging to a prominent Egyptian opposition figure Ayman Nour. Cytrox is associated with Intellexa con-

[25] Namely, Algeria, Bahrain, Egypt, Iraq, Israel, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Palestine, Qatar, Saudi Arabia, Tunisia, Turkey, and the UAE.

sortium, which has operating history in Cyprus, Greece and Ireland, and describes itself as "EU-based and regulated, with six sites and R&D labs throughout Europe" (Marczak et al., 2021b).

In sum, Israeli spyware ecosystem has been very dynamic throughout the past years, especially when pitching and selling its products to MENA law enforcement and security agencies, unlikely "partners-in-crime" at first glance. In the light of the recent international outcry over Pegasus revelations and at least rhetorical willingness of the Israeli government to introduce tighter controls on surveillance exports, Israeli cyber mercenaries may take a path tried out before and partly relocate to Cyprus or any other European country with a lesser degree of public scrutiny.[26] With a track record of European enterprises providing targeted surveillance tools for MENA governments, mergers between European and Israeli companies are also foreseeable.

European digital surveillance contractors

Much like Pegasus, Candiru or Predator, European developed AI-assisted targeted surveillance tools infect a computer or mobile phone to intercept data, record audio and video calls, emails, instant messages, and passwords typed into a web browser. They can also turn on a device's webcam and microphone to spy on the user (Deibert et al., 2019). Munich-based German company FinFisher, GmbH (formerly a part of the Gamma International UK Ltd), Italian Memento Labs (previously Hacking Team), and Danish subsidiary of UK defence giant BAE Systems – ETI – have all been documented to export targeted surveillance solutions to MENA countries. No different than Israeli products, European spyware has been involved in a number surveillance abuses by Arab law enforcement and security agencies.

In the wake of the Arab uprisings, plans of Egyptian security agencies under Hosni Mubarak to buy FinSpy were revealed, whereas the Bahraini government used FinFisher to monitor tens of journalists, activists, and opposition leaders through spyware implants distributed with phishing messages about presumed acts of state administered torture of civil society activists (Marquis-Boire & Marczak, 2012). In 2014, Citizen Lab traced government operators of Hacking Teams' Remote-Control System in 21 countries, including Egypt, Morocco, Oman, Saudi Arabia, Turkey and the UAE (Marczak et al., 2014).

According to 2015 Hacking Teams leaks, two Moroccan intelligence agencies purchased RCS spyware via Al Fahad Smart Systems, based in the UAE, as a middleman. Moreover, the Moroccan Royal Gendarmerie was listed as "very interested" in Hacking Team's products, "especially for mobile" (Privacy International, 2019). Digital forensics suggests that Hacking Team's products were deployed in a phishing attack against Moroccan civic journalism collective Mamfakinch (Privacy International, 2019). Illustrating the complementarity between different targeted surveillance solutions, years later Mamfakinch contributor Omar Radi was yet again found targeted, this time by Israeli Pegasus.

In 2015, 33 government users of FinFisher services in 32 countries were identified, based on the presence of FinSpy traces left by its master servers and publicly available data (Marquis-Boire & Marczak, 2015). The list includes government entities in Bahrain, Jordan, Turkey and Saudi Arabia. The Egyptian Technology Research De-

Israeli spyware ecosystem has been very dynamic throughout the past years, especially when pitching and selling its products to MENA law enforcement and security agencies

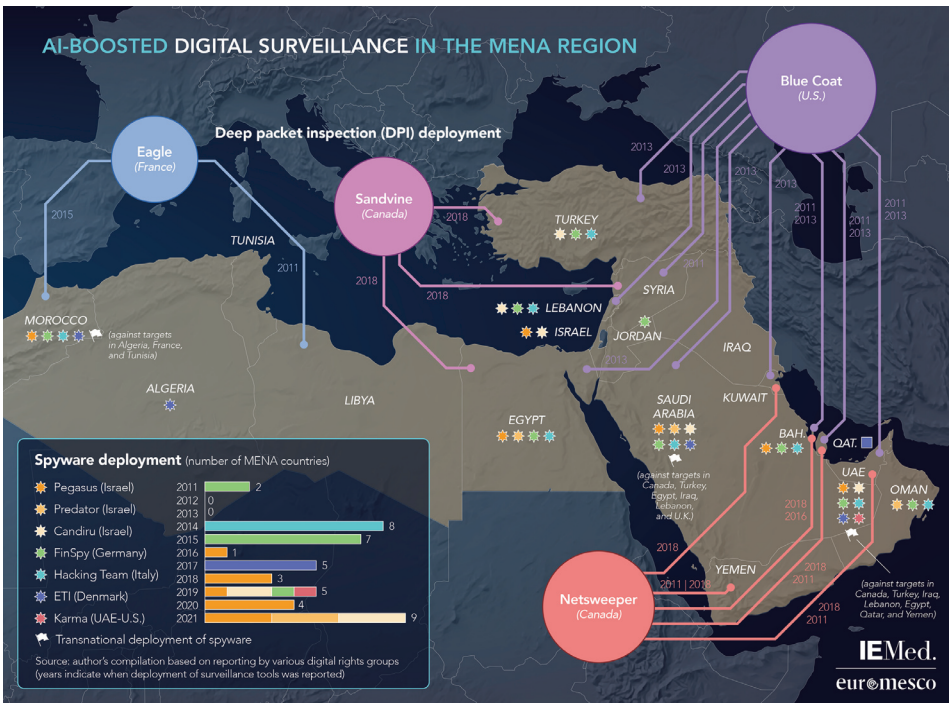
[26] Interview with an Israeli cybersecurity expert, January 26, 2022.

partment, the Lebanese General Directorate of General Security and Internal Security Forces, the Moroccan National Defense Council, and Omani company Eagle Eye Digital Solutions LCC, presumably a subcontractor of the Omani Ministry of Interior, were all identified to operate FinSpy (Marczak et al., 2015).

Reports of European-developed spyware targeting MENA civil society and opposition actors continue up to this date. FinSpy was found to be distributed via a series of phishing attacks targeting Egyptian human rights defenders and media and civil society organizations (CSOs) known as the "Nile Phish" (Amnesty International, 2019a, 2020; Švedkauskas, 2019). Cybersecurity experts have recently found an enhanced version of FinSpy with capabilities of intelligent anti-virus evasion, making it one of the hardest-to-detect spywares in the market (Kaspersky, 2021b).[27] Thus, it is highly likely that new reports about FinSpy deployment in the MENA region are yet to come.

The infographic below summarises the findings on targeted digital surveillance deployment in the MENA region overviewed thus far.[28] As the overlapping dates of reports suggest, MENA law enforcement and security agencies deploy different spyware tools interchangeably and complementary to one another. For instance, in less than a decade Saudi Arabia and the UAE were reported to deploy six out of seven, Morocco and Egypt – four out of seven AI-assisted spyware tools mapped

MENA law enforcement and security agencies deploy different spyware tools interchangeably and complementary to one another



[27] New version of German spyware performs ex- and post-validator tests to ensure that the infected device does not belong to a security researcher, and then validates that the infected device belongs to the targeted individual.

[28] It is important to note here, concerning the infographic, that the lack of reported instances of digital surveillance in some countries could be due to lack of technological sophistication and/or limited capacities of academics, journalists and digital rights groups to track them.

in this chapter with other countries following suit. Concerning the origins of AI-assisted surveillance technology, Israel seems to offer the widest selection of AI-assisted spyware vendors. On the other hand, with the continuing international outcry over NSO Group leaks, Israeli companies may be tempted to (partly) relocate to EU member states with a track record of participating in a surveillance supply chain of their own. As much as a risk, this presents an opportunity for increased European regulatory leverage over targeted digital surveillance in its Southern Neighbourhood.

Conclusions and policy recommendations

The findings of this chapter substantiate claims of previous studies highlighting a defining tension between state and societal cyber-resilience in the MENA region (Pawlak et al., 2021). As sections above show, increased digital surveillance capabilities of law enforcement and security agencies are detrimental to cybersecurity of activists in the region and dissidents abroad. Ironically, it is Western and Israeli corporations providing digital surveillance solutions, which are used not only for undermining digital rights of MENA societies but also for spying on political elites on the other side of the Mediterranean. In this context, three takeaways should be highlighted.

The first takeaway is that MENA's digital sphere, which facilitated coordination of popular movements 10 years ago, can no longer be approached as a bearing ground for "liberation technologies" (as defined by Diamond in 2010). MENA law enforcement and security agencies, telecom and ISPs have been employing mass and targeted digital surveillance solutions to track not only suspects of terrorism, but also activists and human rights defenders mashed together by diffusion of blurry "cybercrime" laws in the region (Shaheed, 2021). As demonstrated by discussions above, machine learning algorithms have so far boosted capacities of DPI for internet filtering and conceivably assist spyware attacks at different stages: from crafting of phishing messages, recognising and recording targets speaking, to context sensitive attacks facilitated by high-jacked intelligent assistants. With the global shift to fifth-generation (5G) networks and drastic increases in data capacities and speeds online, digital surveillance will inevitably rely on further automation and AI algorithms.[29] Thus, without policy interventions, surveillance patterns identified are only likely to expand: MENA law enforcement and security agencies will combine different AI-assisted digital surveillance solutions from an ever-growing pool of mass and targeted surveillance tools to snoop not only on domestic audiences but also on foreign leaders, and their own principals in an increasingly rogue fashion.

Secondly, due to the increasingly transnational nature of digital surveillance, AI-powered surveillance should not only be a domestic concern in the MENA region. Conversely, EU policy-makers should also approach it as a matter of domestic security. Morocco, Saudi Arabia and the UAE have been reported to not only surveil and censor national internet networks, but also to be going after critics abroad and using AI-assisted surveillance tools to spy on leaders in both the MENA region and Europe. As shown by the case of Morocco, MENA security agencies may even choose to digitally surveil their own political leadership. In other words, digital surveillance in the MENA region is multidirectional and much more complex than usually assumed.

MENA's digital sphere, which facilitated coordination of popular movements 10 years ago, can no longer be approached as a bearing ground for "liberation technologies"

[29] Interview with a computer science expert, December 3, 2021.

The third take-away is that MENA's digital surveillance market is well-diversified: American, Canadian, European and Israeli companies are all in the mix. Remarkably, and contrary to other segments of AI and digital technologies at large, China does not yet hold a significant share of the MENA DPI or spyware markets. In the light of advanced AI-enabled digital surveillance infrastructures in China, and its emergence as a global supplier of smart policing, CCTV and facial recognition software and hardware,[30] it is puzzling why MENA countries have not been reported to import Chinese mass and targeted digital surveillance products on a large scale.

In the past decade, China has reached out to MENA governments and offered investment opportunities in 5G networks and digital surveillance through Huawei, ZTE, Hikvision, and other state-backed tech companies (Alhalwaly, 2021). As of 2021, Egypt, Saudi Arabia, Turkey and the UAE have signed a Memoranda of Understanding based on the Chinese Digital Silk Road Initiative (Qiang, 2021). On the other hand, the US has not let this go unnoticed and, for instance, warned the UAE about the risk of "rupturing the long-term strategic relationship" between the two countries for awarding 5G contracts to Chinese Huawei (Kerr, 2020).

By limiting Chinese imports to specific fields as facial-recognition, MENA countries may avoid taking a clear geopolitical stance and assemble digital surveillance structures with building blocks that they deem most suitable

Thus, one possible explanation of the relative Chinese absence from the MENA digital surveillance market is that, finding themselves amid a global techno-political competition between China and the US, regional governments may have taken a pragmatic and cautious approach for diversifying their imports of sensitive AI-assisted digital surveillance technology (Alhalwaly, 2021). By limiting Chinese imports to specific fields as facial-recognition, and remaining open to American, Canadian, European and even Israeli suppliers in other fields, MENA countries may avoid taking a clear geopolitical stance and assemble digital surveillance structures with building blocks that they deem most suitable.

On the other hand, the fact that Western and Israeli rather than Chinese companies dominate the regional AI-enabled digital surveillance market and the tendency of some Israeli surveillance vendors to offshore parts of their operations to Europe provide the EU with leverage to steer digital surveillance deployment in its Southern Neighbourhood away from the current zero-sum game between the state and civil society actors. To that end, Europeans should first speed up regulatory convergence and make a better use of existing tools for controlling exports of dual-use digital surveillance items (see also the discussion in the fourth chapter of this volume). In September 2021, a recast of EU dual use export control regulation entered into force promising a mechanism for coordinating enforcement among member states, and additional checks on cybersurveillance and unlisted items, including emerging technologies (Bromley & Brockmann, 2021). Notwithstanding the recast's plans to connect officials to exchange information about attempted or completed illegal exports for more consistent enforcement across the Union, differences in administrative systems suggest that the task will be time-consuming. Customs, licensing authorities, police and intelligence agencies, prosecutors and other officials from different administrative levels and countries will find themselves at the same table (Bromley & Brockmann, 2021) and will inevitably take time to agree on the formal and informal rules of proceedings.

In the meantime, enforcement of export controls and reacting to cases of non-

[30] See Feldstein (2019) and first chapter of this study.

compliance remains subject mainly to discretion of individual member states. Therefore, national controls, like the German Foreign Trade and Payments Act, should serve as a primary point of reference for countering AI-enabled surveillance misuse. As an illustration, an ongoing investigation was triggered in late 2020 by a successful criminal complaint filed by several human rights organisations, claiming that German FinFisher exported its FinSpy spyware outside the EU without an export licence under the German Foreign Trade and Payments Act (Bannister, 2021).

Secondly, on the EU level, European Council Decision CFSP 2020/1999 concerning restrictive measures against serious human rights violations and abuses, also known as the EU Magnitsky Act, should be deployed more boldly. Among other goals, CFSP 2020/1999 allows for visa bans and asset freezes applied to individuals and organisations complicit in systematic restriction of civil liberties inter alia facilitated by AI-enabled digital surveillance technologies. EU Magnitsky Act in contrast to traditional sanctions at individual countries can be flexibly applied to perpetrators from all over the world, regardless of their location. While only member states and the High Representative for Foreign Affairs and Security Policy have the exclusive right to propose its enactment, the latter should invest resources and effort in reaching out to civil society actors, like the group of non-governmental organizations (NGOs) which called for deployment of the CFSP 2020/1999 against NSO Group for hacking Palestinian human rights activists in December 2021 (Human Rights Watch, 2021). A dedicated Neighbourhood Digital Rights Fund should be established to build and support the forensic and advocacy capacity of civil society actors in the MENA region to map, investigate and advocate against the abuse of AI-enabled surveillance. In turn, these civil society groups could assist the High Representative in attuning its function of a watchdog for human rights and democracy to correspond to emerging challenges of digital authoritarianism in the Southern Neighbourhood.

Finally, these efforts should be coordinated with the US administration in Washington, making use of the momentum surrounding the envisioned transatlantic AI Agreement and policy tracks developing around it. In June 2021, US President Joe Biden and EC President Ursula von der Leyen launched the EU-US Trade and Technology Council (TTC) to "coordinate approaches to key global trade, economic, and technology issues and to deepen transatlantic trade and economic relations based on shared democratic values" (European Commission, 2021a). Among other tasks, TTC is tasked with combating arbitrary or unlawful surveillance and engaging in technical consultations on risk assessments and licensing good practices, and convergent control approaches on sensitive dual-use technologies (European Commission, 2021b). TTC could provide the forum for discussions and facilitate transatlantic coordination on suitable responses to AI-assisted digital surveillance misuse, be it by updating the Wassenaar Arrangement, the only current international export control framework for sensitive dual-use surveillance technology,[31] or synergising between EU policy tools and the 2012 US Global Magnitsky Act or the federal "entity" list, prohibiting private entities from receiving American technologies.[32] Using these counter-measures

European Council Decision CFSP 2020/1999 concerning restrictive measures against serious human rights violations and abuses, also known as the EU Magnitsky Act, should be deployed more boldly

[31] The Wassenaar Arrangement embraces 42 states, including the US and the EU member states. For the full list, see www.nti.org/education-center/treaties-and-regimes/wassenaar-arrangement

[32] In November 2021, NSO Group was added to the federal "entity list" for maliciously targeting officials, activists, journalists, academics and diplomats around the world (Harwell et al., 2021).

in a concerted transatlantic effort would signal a strong commitment to trustworthy AI and communicate that technology abuse would not be inconsequential to both digital surveillance vendors and governmental entities in partner countries, like MENA law enforcement and security agencies. Moreover, by reiterating the pledge to fight digital surveillance misuse in the foreseen transatlantic AI Agreement, the EU and US would send a clear signal that democratic global cooperation on technology indeed "goes beyond the hardware or software" (European Commission, 2021a).

References

ABRAHAMS, A. (2021). *The web (in)security of MENA civil society and media.* POMEPS Studies 43, 22–27.

ACCESS NOW (2020, December 18). *NSO Group WhatsApp hack victims speak out, from India to Rwanda.* Access Now. Retrieved from https://www.accessnow.org/nso-whatsapp-hacking-victims-stories/

AL-ABD, R. (2018, June 5). Parliament passes cybercrime law regulating web content and ISP surveillance. *Mada Masr.* Retrieved from https://www.madamasr.com/en/2018/06/05/news/u/parliament-passes-cybercrime-law-regulating-web-content-and-isp-surveillance/

ALHALWALY, I. (2021, November 18). *Israel is becoming a cybersecurity guarantor in the Middle East. Here's how*. Atlantic Council. Retrieved from https://www.atlantic-council.org/blogs/menasource/israel-is-becoming-a-cybersecurity-guarantor-in-the-middle-east-heres-how/

ALQAHTANI, F. H., & ALSULAIMAN, F. A. (2020). Is image-based CAPTCHA secure against attacks based on machine learning? An experimental study. *Computers & Security, 88,* 101635.

AMIT, H. (2021, August 12). Not Just NSO: Israel and Morocco Cybersecurity Ties Grow Closer. *Haaretz.* Retrieved from https://www.haaretz.com/israel-news/tech-news/.premium-not-just-nso-israel-morocco-working-together-on-cybersecurity-1.10111595

AMNESTY INTERNATIONAL (2019a, March 6). *Phishing attacks using third-party applications against Egyptian civil society organizations.* Retrieved from https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/

AMNESTY INTERNATIONAL (2019b, October 10). *Morocco: Human Rights Defenders Targeted with NSO Group's Spyware.* Retrieved from https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/

AMNESTY INTERNATIONAL (2020, September 25). *German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed*. Retrieved from https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

AMNESTY INTERNATIONAL (2022). *Amnesty Tech*. Amnesty International. Retrieved from https://www.amnesty.org/en/tech/

AU, Y. (2021). *Surveillance as a service: The European AI-assisted mass surveillance marketplace.* Oxford Commission on AI & Good Governance.

BANNISTER, A. (2020, October 15). German police raid tech firm FinFisher over spyware allegations. *The Daily Swig.* Retrieved from https://portswigger.net/daily-swig/german-police-raid-tech-firm-finfisher-over-spyware-allegations

BBC (2017, June 14). How BAE sold cyber-surveillance tools to Arab states. *BBC News*. Retrieved from https://www.bbc.com/news/world-middle-east-40276568

BROMLEY, M., & BROCKMANN, K. (2021). *Implementing the 2021 Recast of the EU Dual-use Regulation: Challenges and Opportunities* (Non-Proliferation and Disarmament Papers No. 77). SIPRI. Retrieved from https://www.sipri.org/publications/2021/eu-non-proliferation-and-disarmament-papers/implementing-2021-recast-eu-dual-use-regulation-challenges-and-opportunities

BUSINESS & HUMAN RIGHTS RESOURCE CENTRE (2021, July 1). *French technology firm charged over Libya cyber-spying.* Business & Human Rights Resource Centre. Retrieved from https://www.business-humanrights.org/en/latest-news/french-technology-firm-charged-over-libya-cyber-spying/

CHRISAFIS, A., SABBAGH, D., KIRCHGAESSNER, S., & SAFI, M. (2021, July 20). Emmanuel Macron identified in leaked Pegasus project data. *The Guardian.* Retrieved from https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data

CISCO (2021). *What is network analytics?.* Retrieved from https://www.cisco.com/c/en_ae/solutions/analytics/what-is-network-analytics.html

COX, J., & FRANCESCHI-BICCHIERAI, L. (2020, March 31). Memento Labs, the reborn Hacking Team, is struggling. *Vice*. Retrieved from https://www.vice.com/en/article/xgq3qd/memento-labs-the-reborn-hacking-team-is-struggling

DALEK, J., DEIBERT, R., MARCZAK, B., MCKUNE, S., NOMAN, H., POETRANTO, I., & SENFT, A. (2016). *Tender confirmed, rights at risk: Verifying Netsweeper in Bahrain* (Citizen Lab Research Report No. 80). University of Toronto. Retrieved from https://citizenlab.ca/2016/09/tender-confirmed-rights-risk-verifying-netsweeper-bahrain/

DALEK, J., DUMLAO, N., KENYON, M., POETRANTO, I., SENFT, A., WESLEY, C., FILASTÒ, A., XYNOU, M., & BISHOP, A. (2021). *No access: LGBTIQ website censorship in six countries* (Citizen Lab Research Report No. 142). University of Toronto. Retrieved from https://citizenlab.ca/2021/08/no-access-lgbtiq-website-censorship-in-six-countries/

DALEK, J., GILL, L., MARCZAK, B., MCKUNE, S., NOOR, N., OLIVER, J., PENNEY, J., SENFT, A., & DEIBERT, R. (2018). *Planet Netsweeper: Executive summary* (Citizen Lab Research Report No. 108). University of Toronto. Retrieved from https://citizenlab.ca/2018/04/planet-netsweeper/

DALEK, J., & SENFT, A. (2011). *Behind Blue Coat: Investigations of commercial filtering in Syria and Burma* (Citizen Lab Research Report No. 1). University of Toronto. Retrieved from https://citizenlab.ca/2011/11/behind-blue-coat/

DEFENCE CONNECT (2021, February 9). *BAE Systems rolls out AI offering to US government.* Retrieved from https://www.defenceconnect.com.au/intel-cyber/7594-bae-systems-rolls-out-ai-offering-to-us-government

DEIBERT, R. J. (2017). *Submission of the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto) to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on the surveillance industry and human rights.*

DIAMOND, L. (2010). Liberation Technology. *Journal of Democracy,* 21(3), 69–83.

EGELE, M., KRUEGEL, C., KIRDA, E., YIN, H., & SONG, D. (2007). *Dynamic spyware analysis.*

EGLOFF, F. J. (2022). *Semi-State Actors in Cybersecurity.* Oxford University Press.

EUROPEAN COMMISSION (EC). (2020, February 19). *White Paper on Artificial Intelligence: A European approach to excellence and trust.* Retrieved from https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

EUROPEAN COMMISSION (EC). (2021a, June 15). *EU-US launch Trade and Technology Council* [Press release]. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990

EUROPEAN COMMISSION (EC). (2021b, September 29). *EU-US Trade and Technology Council Inaugural Joint Statement* [Press release]. Retrieved https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951

EUROPEAN PARLIAMENT (EP). (2021, April 15). *MEPs discuss the impact of AI and tech developments on democracy* [Press release]. Retrieved from https://www.europarl.europa.eu/news/en/press-room/20210408IPR01621/meps-discuss-the-impact-of-ai-and-tech-developments-on-democracy

FELDSTEIN, S. (2019). *The global expansion of AI surveillance.* Carnegie Endowment for International Peace.

FRENKEL, S., & ATEF, M. (2014, September 17). EXCLUSIVE: Egypt Begins Surveillance Of Facebook, Twitter, And Skype On Unprecedented Scale. *BuzzFeed News.* Retrieved from https://www.buzzfeednews.com/article/sheerafrenkel/egypt-begins-surveillance-of-facebook-twitter-and-skype-on-u

FRONT LINE DEFENDERS (2021, November 8). *Six Palestinian human rights defenders hacked with NSO Group's Pegasus Spyware*. Retrieved from https://www.frontlinedefenders.org/en/statement-report/statement-targeting-palestinian-hrds-pegasus

GILEAD, A. (2021, August 10). NSO rival Quadream in talks with Moroccan gov't. *Globes.* Retrieved from https://en.globes.co.il/en/article.aspx?did=1001381146

GUEGUEN, E. (2021a, July 19). ENQUÊTE. Projet Pegasus: En France comme au Maroc, des journalistes ciblés par Rabat. *Franceinfo*. Retrieved from https://www.francetvinfo.fr/monde/afrique/maroc/enquete-projet-pegasus-en-france-comme-au-maroc-des-journalistes-cibles-par-rabat_4707333.html

GUEGUEN, E. (2021b, July 20). Pegasus: Le gouvernement et toute la classe politique française dans le viseur du Maroc. *Franceinfo*. Retrieved from https://www.francetvinfo.fr/politique/gouvernement-d-edouard-philippe/pegasus-le-gouvernement-et-toute-la-classe-politique-francaise-dans-le-viseur-du-maroc_4709413.html

HAARETZ (2021, December 17). *Spyware From Two Israeli Firms Used to Hack Dissidents' Phones in Egypt, India*. Retrieved from https://www.haaretz.com/israel-news/two-israeli-spyware-firms-hacked-dissidents-phones-in-egypt-india-1.10474937

HARKIN, D., MOLNAR, A., & VOWLES, E. (2020). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture: An International Journal, 16* (1), 33–60.

HARWELL, D., NAKASHIMA, E., & TIMBERG, C. (2021, November 3). Biden administration blacklists NSO Group over Pegasus spyware. Washington Post. https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/

HITAJ, B., GASTI, P., ATENIESE, G., & PEREZ-CRUZ, F. (2019). Passgan: A deep learning approach for password guessing. *International Conference on Applied Cryptography and Network Security,* 217–237.

HUMAN RIGHTS WATCH (2021, December 3). *Joint letter urging EU targeted sanctions against NSO Group.* Retrieved from https://www.hrw.org/news/2021/12/03/joint-letter-urging-eu-targeted-sanctions-against-nso-group

KASPERSKY (2021a). *What is a zero-day attack? - Definition and Explanation*. Retrieved from https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

KASPERSKY (2021b, September 27). *FinFisher spyware improves its arsenal with four levels of obfuscation, UEFI infection and more* [Press release]. Retrieved from https://www.kaspersky.com/about/press-releases/2021_finfisher-spyware-improves-its-arsenal-with-four-levels-of-obfuscation-uefi-infection-and-more

KERR, S. (2020, June 2). UAE caught between US and China as powers vie for influence in Gulf. *Financial Times.* Retrieved from https://www.ft.com/content/1ff119ff-50bf-4b00-8519-520b8db2082b

KING, T. C., AGGARWAL, N., TADDEO, M., & FLORIDI, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics,* 26 (1), 89–120.

KIRCHGAESSNER, S. (2021a, July 18). Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests. *The Guardian.* Retrieved from

https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus

KIRCHGAESSNER, S. (2021b, July 23). How NSO became the company whose software can spy on the world. *The Guardian.* Retrieved from https://www.theguardian.com/news/2021/jul/23/how-nso-became-the-company-whose-software-can-spy-on-the-world

KIRCHGAESSNER, S., LEWIS, P., PEGG, D., CUTLER, S., LAKHANI, N., & SAFI, M. (2021, July 18). Revealed: Leak uncovers global abuse of cyber-surveillance weapon. *The Guardian.* Retrieved from https://www.theguardian.com/world/2021 /jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

LEBER, A., & ABRAHAMS, A. (2021). *Social media manipulation in the MENA: Inauthenticity, Inequality, and Insecurity.* POMEPS Studies 43, 48–55.

MAC, R., HASKINS, C., & PEQUENO IV, A. (2021, August 25). Clearview AI offered free facial recognition trials to police all around the world. *BuzzFeed News.* Retrieved from https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table

MARCZAK, B., ABDULEMAM, A., AL-JIZAWI, N., ANSTIS, S., BERDAN, K., SCOTT-RAILTON, J., & DEIBERT, R. (2021). *From Pearl to Pegasus: Bahraini government hacks activists with NSO group Zero-Click iPhone exploits* (Citizen Lab Research Report No. 141). University of Toronto. Retrieved from https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/

MARCZAK, B., ANSTIS, S., CRETE-NISHIHATA, M., SCOTT-RAILTON, J., & DEIBERT, R. (2020). *Stopping the press: New York Times journalist targeted by Saudi-linked Pegasus spyware operator* (Citizen Lab Research Report No. 124). University of Toronto. https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/

MARCZAK, B., DALEK, J., MCKUNE, S., SENFT, A., SCOTT-RAILTON, J., & DEIBERT, R. (2018). *BAD TRAFFIC: Sandvine's PacketLogic devices used to deploy government spyware in Turkey and redirect Egyptian users to affiliate ads?* (Citizen Lab Research Report No. 107). University of Toronto. Retrieved from https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

MARCZAK, B., GUARNIERI, C., MARQUIS-BOIRE, M., & SCOTT-RAILTON, J. (2014). *Mapping hacking team's "untraceable" spyware* (Citizen Lab Research Report No. 33). University of Toronto. Retrieved from https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

MARCZAK, B., & SCOTT-RAILTON, J. (2016). *The million dollar dissident: NSO Group's iPhone Zero-Days used against a UAE human rights defender* (Citizen Lab Research Report No. 78). University of Toronto. Retrieved from https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

MARCZAK, B., SCOTT-RAILTON, J., BERDAN, K., RAZZAK, B. A., & DEIBERT, R. (2021). *Hooking Candiru: Another mercenary spyware vendor comes into focus* (Citizen Lab Research Report No. 139). University of Toronto. Retrieved from https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

MARCZAK, B., SCOTT-RAILTON, J., MCKUNE, S., RAZZAK, B. A., & DEIBERT, R. (2018). *HIDE AND SEEK: Tracking NSO Group's Pegasus spyware to operations in 45 countries* (Citizen Lab Research Report No. 113). University of Toronto. Retrieved from https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

MARCZAK, B., SCOTT-RAILTON, J., RAZZAK, B. A., AL-JIZAWI, N., ANSTIS, S., BERDAN, K., & DEIBERT, R. (2021). *Pegasus vs. Predator: Dissident's doubly-infected iPhone reveals Cytrox mercenary spyware* (Citizen Lab Research Report No. 147). University of Toronto. Retrieved from https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

MARCZAK, B., SCOTT-RAILTON, J., SENFT, A., POETRANTO, I., & MCKUNE, S. (2015). *Mapping FinFisher's Continuing Proliferation* (Citizen Lab Research Report No. 64). University of Toronto. Retrieved from https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

MARQUIS-BOIRE, M., DALEK, J., MCKUNE, S., CARRIERI, M., CRETE-NISHIHATA, M., DEIBERT, R., KHAN, S. O., NOMAN, H., SCOTT-RAILTON, J., & WISEMAN, G. (2013). *Planet Blue Coat: Mapping global censorship and surveillance tools* (Citizen Lab Research Report No. 13). University of Toronto. Retrieved from https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

MARQUIS-BOIRE, M., & MARCZAK, B. (2012). *From Bahrain with love: FinFisher's spy kit exposed* (Citizen Lab Research Report No. 9). University of Toronto. Retrieved from https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

MEGIDDO, G. (2021, June 8). Secretive Israeli cyber firm selling spy-tech to Saudi Arabia. *Haaretz.* Retrieved from https://www.haaretz.com/israel-news/tech-news/.premium.HIGHLIGHT-the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia-1.9884403

MICROSOFT (2021, July 15). *Protecting customers from a private-sector offensive actor using 0-day exploits and DevilsTongue malware*. Microsoft Security Blog. Retrieved from https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

MOCHALSKI, K., & SCHULZE, H. (2009). *Deep packet inspection: Technology, applications & net neutrality*. Ipoque GmbH.

NETSWEEPER INC. (2016). *Netsweeper multilanguage filtering.* Retrieved from https://www.netsweeper.com/wp-content/uploads/2017/06/Multi-Language-Filtering-Whitepaper-V2.pdf

NEWMAN, J. (2021, July 13). Now is the time for transatlantic cooperation on artificial intelligence. *Georgetown Journal of International Affairs.* Retrieved from https://gjia.georgetown.edu/2021/07/13/now-is-the-time-for-transatlantic-cooperation-on-artificial-intelligence/

NGUYEN, T. T. T., & ARMITAGE, G. (2008). A survey of techniques for internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials, 10* (4), 56–76.

NOMAN, H., & YORK, J. C. (2011). West censoring East: The use of Western technologies by Middle East censors, 2010-2011. *OpenNet Initiative.* Retrieved from https://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

NSO GROUP (2015). *Pegasus – Product Description.* Retrieved from https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html

ORBACH, M. (2021, November 25). Israel defense ministry slashes cyber export list, drops Saudi Arabia, UAE. *Calcalistech.* Retrieved from https://www.calcalistech.com/ctech/articles/0,7340,L-3923361,00.html

PARSONS, C. (2009). *Deep Packet Inspection in perspective: Tracing its lineage and surveillance potentials.* Surveillance Studies Centre.

PAWLAK, P., ABDEL-SADEK, A., DOMINIONI, S., & LABAN, A. M. Y. (2021). Great Expectations: Defining a trans-Mediterranean cybersecurity agenda. *EuroMeSCo Policy Study No. 22.* European Institute of the Mediterranean. Retrieved from https://www.euromesco.net/publication/great-expectations-defining-a-trans-mediterranean-cybersecurity-agenda/

POLYAKOV, A. (2018, October 28). *Machine learning for cybercriminals.* Retrieved from https://towardsdatascience.com/machine-learning-for-cybercriminals-a46798a8c268

POLYAKOVA, A., & MESEROLE, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models.* Brookings.

RESEARCH AND MARKETS (2021). *Global Deep Packet Inspection market size by product, by application, by geographic scope and forecast.* Retrieved from https://www.researchandmarkets.com/reports/5301351/global-deep-packet-inspection-market-size-by

SABBAGH, D. (2021, July 21). Data leak raises new questions over capture of Princess Latifa. *The Guardian.* Retrieved from https://www.theguardian.com/world/2021/jul/21/data-leak-raises-new-questions-over-capture-of-princess-latifa

SCHECTMAN, J., & BING, C. (2019, January 30). Exclusive: UAE used cyber superweapon to spy on iPhones of foes. *Reuters.* Retrieved from https://www.reuters.com/article/uk-usa-spying-karma-exclusive-idUKKCN1PO19S

SCHEDLER, A. (2002). Elections without democracy: The menu of manipulation. *Journal of Democracy, 13*(2), 36–50.

SHAHEED, A. (2021). Binary threat: How governments' cyber laws and practice undermine human rights in the MENA region. In M. Lynch (Ed.), *Digital Activism and Authoritarian Adaptation in the Middle East* (pp. 8–16).

SHEZAF, J., & JACOBSON, J. (2018, October 20). Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays. *Haaretz*. https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027

SHIRES, J. (2021). The implementation of digital surveillance infrastructures in the Gulf. In M. Lynch (Ed.), *Digital Activism and Authoritarian Adaptation in the Middle East* (pp. 16–21).

SOLOMON, S. (2019, February 14). NSO founders, management buy stake in firm from Francisco Partners. *Times of Israel*. Retrieved from https://www.timesofisrael.com/nso-founders-management-buy-stake-in-firm-from-francisco-partners/

ŠVEDKAUSKAS, Ž. (2019). Three steps in ensuring digital security of Egyptian activists abroad. *EuroMeSCo Policy Brief N°99*. European Institute of the Mediterranean . Retrieved from https://www.euromesco.net/publication/three-steps-in-ensuring-digital-security-of-egyptian-activists-abroad/

TIMEP (2019, September 23). *TIMEP Brief: Export of Surveillance to MENA Countries.* Retrieved from https://timep.org/reports-briefings/timep-brief-export-of-surveillance-to-mena-countries/

TRIVEDI, U., & PATEL, M. (2016). A fully automated deep packet inspection verification system with machine learning. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 1–6.

UNITED NATIONS OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS (UNOHCHR). (2011). *Guiding Principles on Business and Human Rights.* Retrieved from https://digitallibrary.un.org/record/720245

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). (2022). *Bilateral trade flows by ICT goods categories, annual.* Retrieved from https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx

UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE (UNICRI) & United Nations Office of Counter-Terrorism (UNOCT). (2021). *Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes.*

US DEPARTMENT OF COMMERCE & BUREAU OF INDUSTRY AND SECURITY (BIS). (2020). *Actual investigations of export control and antiboycott violations*. Retrieved from https://www.bis.doc.gov/index.php/documents/enforcement/1005-don-t-let-this-happen-to-you-1/file

VALENTINO-DEVRIES, J., SONNE, P., & MALAS, N. (2011, October 29). U.S. firm acknowledges Syria uses its gear to block web. *Wall Street Journal.* Retrieved from https://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

WESTERLUND, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11).

ZHANG, R., CHEN, X., LU, J., WEN, S., NEPAL, S., & XIANG, Y. (2018). *Using AI to hack IA: A new stealthy spyware against voice assistance functions in smart phones.*

Unexpected Pioneer: The Middle East's Burgeoning AI Defence Industry

Can Kasapoglu
Director of Security and Defense Program, EDAM
Non-Resident Fellow in Euro-Asian Military Affairs,
Jamestown Foundation

The past few years have witnessed significant advances in the European Union (EU)'s broader approach to artificial intelligence (AI) as the Union increased funding for research and development (R&D) and application. However, in techno-geopolitics and military applications of AI, Europe still lags behind current global trends. More critically, while Europe has been busy discussing its draft AI regulation, Middle Eastern countries have been fast investing in emerging defence technologies. To recalibre its foreign policy approach towards the Middle East's burgeoning AI-driven military modernisation programmes, the EU needs to adopt a clear approach to maintain its relevance in the realm of smart algorithms and digitalised geostrategic paradigm.

This chapter will analyse the present AI and defence landscape and the military sphere in the Middle East to find a viable way forward for the EU. It will do so, first, by exploring the horizon of the AI-driven warfare and the future of defence. Secondly, it will provide a sketch of the Middle East and North Africa (MENA) countries pioneering in AI defence technologies. Thirdly, it will explore AI's potential ramifications with the Middle Eastern security landscape. The chapter concludes by presenting relevant policy and security implications for the EU vis-à-vis the growing proliferation of AI in MENA military and defence.

AI in military and defence: a new era of warfighting

Unlike the military technological landscape of the Cold War era, AI is a truly dual-use asset, and innovations come from both commercial circles and traditional defence powerhouses. Thus, differentiating military and non-military AI spending is a difficult, sometimes impossible effort with open-source intelligence. AI-based investments of a nation – be it for civilian use, a commercial asset or a defence modernisation programme – resonate with more than one segment of military affairs as a force-multiplier or strategic enabler. The segment is mainly driven by robotic warfare solutions, command and control systems, and intelligence and surveillance technologies.

A nation that has not developed a robust technological and industrial defence base during the industrial era can well manage to take a quantum leap in the digital age. Put simply, less industrialised nations have an opportunity to catch up with the rest. Thus, with the rise of AI we will be talking about new winners and new losers of the geopolitical bonanza.

With an astonishingly fast proliferation amongst militaries globally, AI is causing a paradigm shift in the military sphere. Some countries have already started using the technology in autonomous weapons. Samsung's autonomous sentry guns with image recognition to enhance target identification and fire precision developed in 2010 is one example of such initiatives. Similar technologies were also used by other countries including Israel. While South Korea and Israel claim that the weapons use a human-in-the-loop mechanism, open-source intelligence suggests that they can indeed operate with no human involvement (De Vynck, 2021).

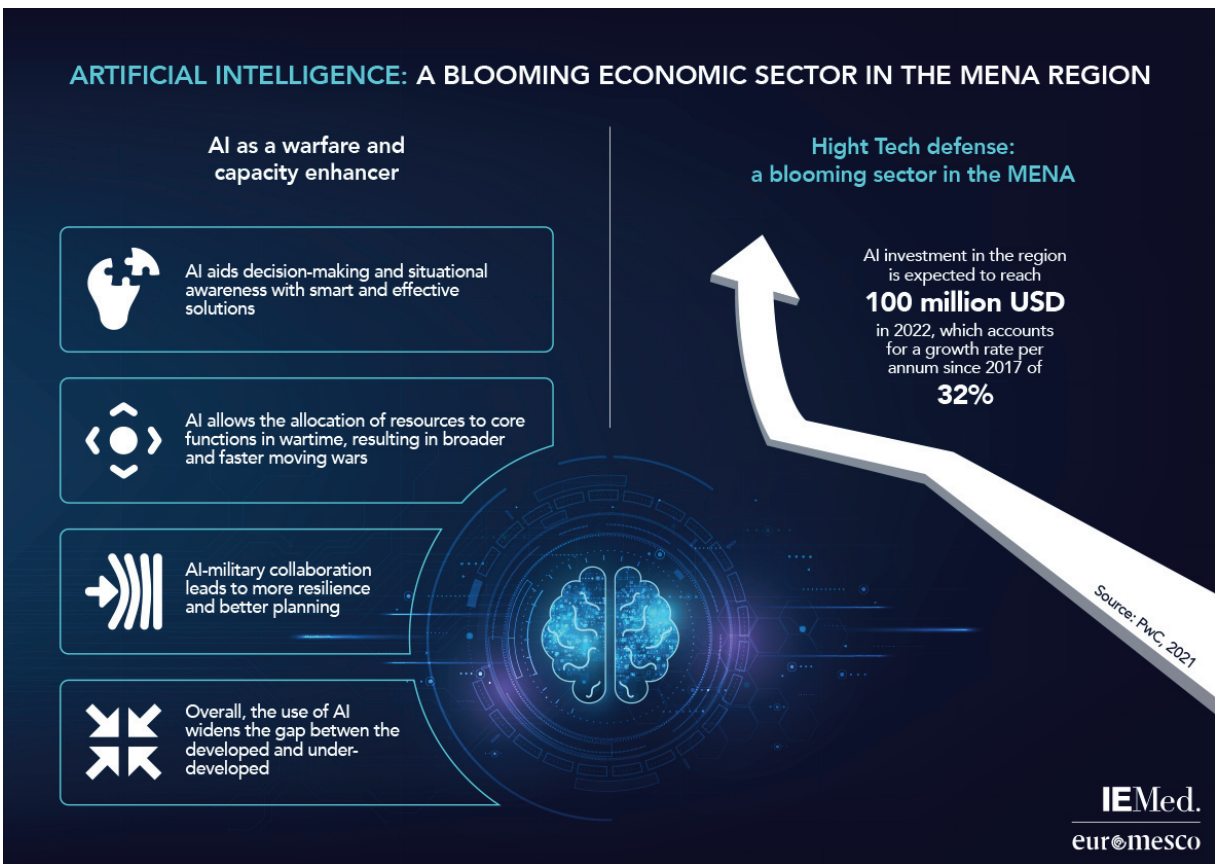
In the physical sphere of warfare, AI manifests itself in robotic systems and more autonomy in warfighting. Robotic warfare is built on a straightforward but effective premise. The more precise, autonomous and network-centric (interconnected with other friendly units on the battlefield) one's systems are, the more combat capability one can generate.

This rather simple reality is attributed to several reasons. First, robotic weapons systems and platforms should operate within minimal target acquisition mistakes (reduced margin of error and improved strike precision). Second, they rely on high-precision fire-power in combat missions, which greatly diminishes friendly losses in high-risk areas (Matei, 2021).

In the coming years and decades, robotic warfare will bring significant impacts for the future of war. The long-anticipated change is not limited to concepts of AI-driven machines that will be characterised by a generous, plain and sustained use of force. Consequently, this trend will likely create a battlefield where trade-offs and large-scale destruction are normalised. However, robotics and machine-learning algorithms can also foresee a conflict's outcomes and greatly diminish human casualties during conflict (Matei, 2021). Thus, it is not only about a technological change. The future of high-tech warfare will also pertain to political decisions such as how to use high-tech weaponry and intelligence systems. Overall, what we are talking about is a double-edged sword coming into play fast.

In order to develop a thorough understanding of how AI-driven weapon systems and military networks can play out, which is the very basis for the role of AI in defence, one has to properly grasp the concept of algorithmic warfare.

The future of high-tech warfare will also pertain to political decisions such as how to use high-tech weaponry and intelligence systems



Defence analysts largely agree that AI and machine learning will change the character of war. Countries' triumphs in future battles will firmly pertain to their algorithmic warfare capabilities. Notably, AI-driven mechanisms greatly catalyse and improve military decision-making (Layton, 2018). Although these technologies can lead to some economic burden at the initial investment and R&D processes, when managed correctly with a good pool of talents, they proliferate fast and can be integrated into various weapon systems in different segments of battle networks. So, they provide governments and militaries with the flexibility to repurpose the algorithms to solve a wide set of different problems swiftly and efficiently. On a similar note, militaries that can utilise data-fed AI systems will drastically improve situational awareness on the battlefield (Layton, 2018).

One recent example of dual-use AI system integration into defence technologies is the United States (US)' Navy's modernisation. Washington is working towards deploying dual-use maritime robotics, which will allow it to place numerous sensors in critical locations. According to US defence authorities, such robotics provide cheap yet effective solutions. They will also greatly enhance maritime situational awareness and assist manned units' activities (Saballa, 2021). Officials believe that in an allied approach different countries cooperating on the use and development of the technology dual-use maritime robotics can be a great asset for deterrence, surveillance and the tackling of illicit activities. For example, one prominent problem that the technology can also be used for is tracking and stopping weapons transfers to the Houthis through the southern Red Sea (Eckstein, 2021). While the US is still the chief country regarding technological advantage in warfare, China is swiftly rising. Today, Beijing surpasses Washington in access to data, which is key to improving the effectiveness and accuracy of algorithmic systems (Walsh, 2021).

The EU attaches importance to AI-driven techno-geopolitical competition. This political vision is centred around the principle of protecting European leadership and independence in several critical technological areas. Because, when it comes to game-changing high-tech, external dependencies can bring about even bigger shortfalls in strategic capacity. The European Commission (EC) already started the interstate discussions and building a narrative that revolves around strategic autonomy and digital sovereignty. Some even claim that the EU's defence policy is now moving away from its traditional approach towards a more tech-related one (Csernatoni, 2021). On this note, the European Defence Agency's 2021 Annual Conference prioritisation of collaborative defence innovation and R&D projects are also prioritised by the EU perspective. Such initiatives would not only catalyse implementation and impact but also strengthen the European Defence Technological and Industrial Base overall. Some other important initiatives such as the European Defence Fund (EDF) and the European Defence Industrial Development Programme (EDID) offer additional boosters for the EU's AI-related ambitions.

While autonomous systems loom large as significant assets for military capabilities, there still is no global ban on Lethal Autonomous Weapon Systems

While autonomous systems loom large as significant assets for military capabilities, there still is no global ban on Lethal Autonomous Weapon Systems (LAWS). Although activists push for it on an international scale, the Silicon Valley, defence industrial giants and strong political figures argue that a comprehensive and supra-nationally binding ban is not needed (De Vynck, 2021).

The EU's approach to AI is, as opposed to the general view in the Silicon Valley, very cautious. In April 2021, the EC proposed a legal framework to regulate AI, asking for

compliance for critical AI-tech developers (as explored in greater detail in the fourth chapter in this volume). The proposal foresees that some AI functionalities should be completely banned, where some other aspects such as high-risk use should be closely monitored. It aims to lay out a normative framework and establish a transparent, human-centred governance of the technology. Remarkably, it also introduces a requirement for "ex-ante conformity assessments to establish that high-risk AI systems meet these requirements before they can enter the market or become operational" (MacCarthy & Propp, 2021). The EC also proposed a mandate to establish a post-market monitoring system to keep track of any potential problems in the implementation of AI.

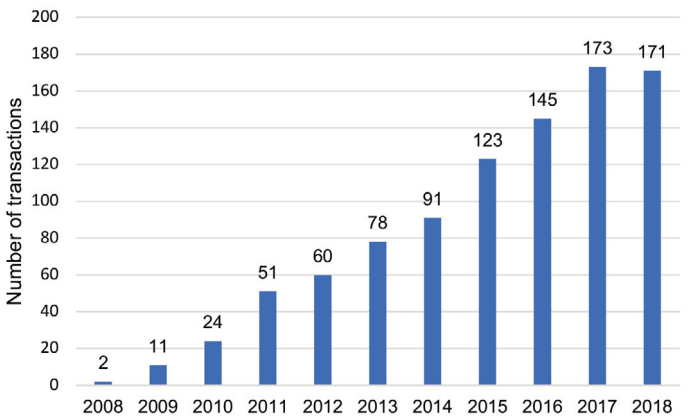
If successful, the EDF can also greatly contribute to the EU's efforts. It can boost collaborative research and investment in defence technologies across the membership. Consequently, it can significantly bolster the EU's position in the strategic tech industry. Brussels already allocated 8% of the EDF to funding emerging disruptive technologies (EDT). Although this number can be higher, it marks the EU's willingness to improve its capabilities in the segment (Csernatoni, 2021).

AI-powered defence trends in the Middle East

High-tech, sophisticated weapons have already become extremely lethal assets in the Middle East. Israel's targeted killing of the Iranian scientist Mohsen Fakhrizadeh by a remote-controlled, AI-assisted weapon system looms large as a remarkable example in this respect (Bergman & Fassihi, 2021).

AI is proliferating fast, and the Middle East is no exception. Several countries in the region have already embraced AI-driven technologies, and prioritised adapting to critical requirements of the digital age. Estimates suggest that AI spending in the MENA region will grow from $37.5 million in 2017 to over $100 million by the end of 2021, which accounts for a growth rate of 32% per annum (PwC, 2018).

Figure 1. The steady increase in Middle East and African AI investment



Note: AI companies invested into, transaction volume, for a selection of 11 countries from the Middle East and Africa (2008-2018).

Source: Elaborated based on data found in a report commissioned by Microsoft and conducted by EY Consulting (2018)

In the Middle East, five countries loom large regarding the strong commitment towards the R&D of AI. In the United Arab Emirates (UAE), Saudi Arabia, Israel and Qatar, businesses already spurred high rates of investment into the development of new technologies, which is supported by governments and the early clients of these new systems. But when the Gulf economies are excluded from the picture, the region's overall adoption of the digital age has been remarkably slower. These differences can be rooted in factors such as the quality of infrastructure and access to skilled labour, which are drivers of AI development and digitalisation (PwC, 2018).

As a North Atlantic Treaty Organization (NATO) nation with Middle Eastern borders, Turkey is generally kept out of the regional stats. However, if one should incorporate Turkey into the Middle Eastern AI landscape, the results would show a tremendous defence investment effort, especially in the autonomous weapon systems and robotic warfare segments.

Despite the financial constraints and the Western sanctions, Iran's indigenous R&D capacity is still growing significantly

Iran is yet another actor that prioritises AI research. The country's human resources remain large in this respect. Yet, although finances are not always the silver bullet, growing economic problems remain restraining for Tehran. However, despite the financial constraints and the Western sanctions, Iran's indigenous R&D capacity is still growing significantly. Tehran is the fifth leading producer of STEM (science, technology, engineering and mathematics). Iranian universities are also increasingly offering programmes on AI and robotic technologies (Pargoo, 2019). Additionally, although it is largely isolated from the international markets, Tehran is quite adept at copying Western technologies to boost its indigenous AI capabilities (Qaidari, 2022).

Aiming to have its autonomous weapon systems on the battlefield by 2024, Tehran has the resources necessary to succeed in its quest (Lisman, 2021). Thanks to the independent innovation capabilities of the Research and Self-Sufficiency Jihad Organization of the Army Ground Force, such a development can occur quite swiftly in the Iranian context (Lisman, 2021). Alarmingly, AI can be a true force multiplier in Iran's proxy wars and asymmetric capabilities, which can be destabilising for the region. In fact, US officials already started to consider AI-driven solutions to counter the growing Iranian threat (Feldscher, 2022). In order to understand and tackle the destabilising effect of Iran's robotic breakthrough, the West should strive to block Iran's main high-tech procurement routes. These are primarily Tehran's R&D cooperation with Russia and China and Iranian espionage. To put it in context, while the EU is heavily focused on the Iranian nuclear programme, but nothing else, the Iranian AI-driven systems can become even bigger trouble in the future. In particular, Iran's ability to transfer dangerous weaponry to its proxies remains a challenge in this framework.

AI breakthrough and its widespread use in various industries will have impressive effects to win future wars. In fact, IBM claims that the race for AI is the "new space race" and that Middle Eastern actors recognise this trend. The UAE already appointed a Minister for AI and established its Artificial Intelligence Strategy 2031. Saudi Arabia followed suit with its Vision 2030 plan, placing AI capabilities at the epicentre of its economic planning (IBM, 2019). Almost 40% of the companies in the UAE and 45% of the companies in Saudi Arabia are already

preparing their staff to adapt to an automated and AI-led working environment (Khaleej Times, 2021).

The Middle East is also witnessing partnerships that merge AI into defence technologies and other segments. Shortly after signing the Abraham Accords, Israel and the UAE agreed to start a new joint venture to develop commercial artificial intelligence and big data technologies. The parties involved are also remarkable. Being a central player in the Israeli defence industry, Rafael is the manufacturer of both Israel's Iron Dome and David's Sling air defence systems. In addition, it leads Israeli R&D efforts on lasers and networked battlefield systems. Rafael makes a good partner for the Emirati Group 42, due to its leading position in AI and cloud computing in the UAE. Some sources claim that the two parties also exchanged views and knowhow on defence and security matters in the International Defence Exhibition and Conference. The companies' executives regarded this partnership as "a move to make the Middle East a better place" (Frantzman, 2021). It is clear that Israeli knowhow and the Gulf Arabs' financial capacities can bring game-changer results for the regional strategic landscape. While the Abraham Accords are politically stabilising, and the best counter-balancer against Iran, the Arab-Israeli cooperation's AI and military developments will hardly be in sync with the EU's restrictive stances on autonomous weaponry and defence use of AI.

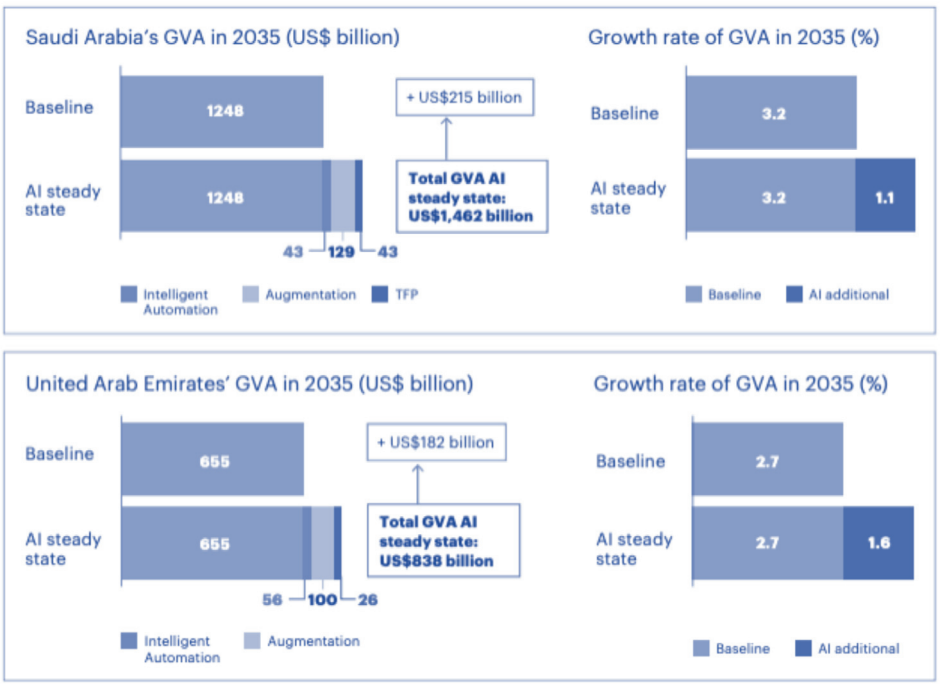
The UAE's AI-driven strategic programmes enjoy a broader outreach. Notably, on 16 September 2021, the country's Prince Mohamed bin Zayed and the deputy supreme commander of the armed forces paid a visit to the United Kingdom (UK) for talks with the British Prime Minister Boris Johnson. The Emirates and the UK then signed a "Partnership for the Future", involving bilateral cooperation on AI as well as on high-end R&D on defence and security tech. The deal also aims to help UAE medium-sized enterprises access to British knowhow (Helou, 2021a). Another example that showcases the UAE's AI science & technology programme looms large through its cooperation with Lockheed Martin. A member of the US defence giant's Center for Innovation and Security Solutions (CISS) stated that the team was able to digitalise the process of inspecting the Emirati Air Force's aircraft manually and achieved significant minimisations in time and cost thanks to digital solutions (Mezher, 2021).

The region's high tech defence economics

International Data Corporation (IDC) expects that investment in AI systems in the Middle East and Africa will reach 100 million USD this year, with an annual growth rate of 32%. The UAE, Saudi Arabia and Qatar loom large as the leading countries driving the region's digitalisation. Businesses in these countries also play a crucial role in the implementation of AI. They are funded and supported by the governments, coming into play as facilitating actors. However, despite the initiatives of these three nations, non-Gulf Middle Eastern states still lag behind in the AI-related technologies. This strategic gap is mainly stemming from economic differences, particularly when it comes to the quality of infrastructure and access to skilled human capital, which remain indispensable for developing a high-tech defence technological and industrial base (PwC, 2018). Soon, the labour force in the MENA region will become increasingly automated and AI-powered. Strikingly, the number of countries gearing for a transition to AI is expected to grow by almost 70%. The private sector and the companies play a foundational role to invest in the workforce to be successful in the future (Accenture Research, 2021).

It is clear that Israeli knowhow and the Gulf Arabs' financial capacities can bring game-changer results for the regional strategic landscape

Figure 2. AI' impact on economic development of Saudi Arabi and the UAE (2035 forecast)



Source: Accenture (2018)

Israel ranks just after the US and China as regards to the number of AI start-ups and innovations, where its AI-enabled defence industry remains to be a pioneer (Khushnam, 2020). On 11 February, Israeli defence authorities claimed that Tel Aviv is working on a strategy that will incorporate AI into the military. Thanks to a data-driven mechanism, officials claim that IDF will be able to counter the future's threats much more flexibly and effectively (Frantzman, 2022). The Israeli defence industry's success in Special Mission Intelligence Aircraft proves to digitise warfare and battlefield, which reduces casualties, as well as bringing operational benefits, such as early warning, deterrence, threat identification and destruction (IAI, 2021). Israel aims to enhance automation to all the sectors in economy, infrastructure and governance.

Funded by EDGE Technologies, ADASI's vertical-takeoff-and-landing drone "Garmousha" looms large as the UAE's first indigenous drone that is equipped with AI algorithms (Helou, 2020). With astonishing investments in AI and automation coupled with significant growth potential, the UAE has the potential to lead the AI industry in the Middle East (Finaud et al., 2021).

Besides the UAE, Saudi Arabia is also an important actor in the AI race. In fact, Abu Dhabi considers AI to be the foundation of technological advancement. The AI International Summit brought together stakeholders from government, academia, private sector and start-ups, with the mission of "Shaping the future of AI, together". The Gulf monarchy aims to become the "Silicon Valley of the Middle East", and the establishment of the National Centre for Robotics Technologies and Intelligent Systems, Robotic services, MiSk Academy for digital programming and AI training, the Prince Mohammed bin Salman College of Cyber

Security, Artificial Intelligence and Advanced Technology serves this purpose. In return, Saudi Arabia aims to replace the country's oil dependency of its economy with AI-driven self-sufficient enhancements within a public-private business model. Industrial automation, AI and big data are essential for the digital transformation in certain sectors in Saudi Arabia, including healthcare, government services, sustainable energy and water, manufacturing, and mobility and transportation (OECD AI Policy Observatory, 2020). Thanks to their AI capabilities, both countries have established a prestige in the defence exports market. According to some experts, the proliferation of such algorithmic solutions will be swift and will be true game-changers for the countries' defence, intelligence and counter-terrorism capabilities (Helou, 2021b).

Overall, the Kingdom of Saudi Arabia comes first as a hub for emerging digital and technological developments, with the highest increase in its digital competitiveness among the G20 countries (Abul-Enein, 2020). Nonetheless, regulations on the local tech ecosystem limits the attractiveness for new entry to the market, raises concerns on the ethical use of AI and the protection of personal data, and restricts cross-border data transfer.

Nevertheless, as observed in the Israel-UAE cooperation case, the Middle East is undergoing a substantial political change. The Abraham Accords enabled the burgeoning dialogue between Israel and Gulf Arab nations. Should this trend persist, one can expect an uptrend in future scientific and tech collaborations across the region (Finaud et al., 2021). Rafael Advanced Defense Systems, Israel's leading defence company, and Group 42 will contribute to the research and development of commercial AI and big data technologies (Frantzman, 2020a). This joint venture with Group 42 is expected to contribute to combat future pandemics, as well as making advances in various areas (Frantzman, 2021).

Saudi Arabia aims to replace the country's oil dependency of its economy with AI-driven self-sufficient enhancements within a public-private business model

Apart from Saudi Arabia and the UAE, we have the rest of the Middle Eastern Arab landscape with their AI-driven strategic visions.

Like its regional counterparts, Morocco also prioritises various industries for its national AI plan, which includes digitalisation and labour market transition (OECD, 2021). Qatar, on the other hand, integrates AI in its Qatar National Vision (QNV) 2030 to improve its businesses, government, society and military with respect to ethical concerns and security (see Qatar National Vision 2030). The New Kuwait Vision 2035 targets enhanced AI adaptation and integration in every aspect of society, business and education. Bahrain, as one of the fastest-growing economies in the Gulf, is also quite proactive in the application of AI and robotics. The country has established an Information and eGovernance Authority, Tamkeen, Central Bank of Bahrain and Economic Development Board. Bahrain also hosts the first AI education and training facility – The Bahrain Polytechnic Academy of Artificial Intelligence (Khushnam, 2020).

How AI changes the Middle Eastern defence landscape

While the EU remains the largest trade partner of, and the second-largest aid provider to, the MENA region, it has very limited political leverage compared to its potential. As the Libyan and Syrian cases showcased, Brussels has little capability to change the political landscape. However, despite this constraint, Europe remains heavily affected by Middle Eastern security problems (Foucher, 2021).

AI-driven military technologies can alter the fundamentals of war, AI-driven defence developments are likely to have a deep impact on the Middle Eastern security environment

As robotic warfare, algorithmic warfare, and AI-driven military technologies can alter the fundamentals of war, AI-driven defence developments are likely to have a deep impact on the Middle Eastern security environment. AI-driven systems provide smart and effective solutions in an environment where information is scarce, and decisions are strictly bound by time. Besides aiding decision-making and situational awareness, AI also improves logistics, administration, maintenance in armies, as well as the training and management of military personnel. By reducing the burden on planning and reducing human labour, it allows more resources to be allocated to core functions during war. AI handles the OODA (observe-orient-decide-act) loop much faster than humans and creates combat intelligence clouds with secure gateways (Kumar Jha & Das, 2021). Overall, with AI-boosted militaries, Middle Eastern wars will be faster in tempo and broader in scope. This will inevitably affect the EU's strategic outreach and security calculus in the region. Moreover, AI-driven military systems significantly contribute command and control capabilities by providing a resilient, data-oriented chain of command. This military-AI collaboration leads to better planning, improved resilience, and a much sharper concept of operations. Some writings even claim that AI will allow for the creation of an interactive, autonomous platform that provides 360-degree, all-round visuals, and analysis of the hostile environment. Such developments would greatly enhance the operator country's capabilities in war, providing it with critical information on the war's trajectory (Kumar Jha & Das, 2021). In other words, while the gap between the developed and underdeveloped is already huge in the Middle East, the AI-driven tech breakthrough will further widen the gap. This can lead to a geopolitical shift in the regional strategic balance of power. More importantly, the proliferation of AI in the military segment will "allow smaller powers and non-state actors to use technology as a force multiplier" to increase their impact and leverage (Helou, 2021b). In other words, the EU might have to revisit its geopolitical focus when judging the regional actors' potentials.

However, being rich does not guarantee a top place in emerging technologies. Because such technologies come with strings attached, as techno-generational and techno-geopolitical trends change swiftly, and it is hard to anticipate where valuable resources should be allocated. Therefore, an accurate, early trend detection and correct resource allocation remains key to success. Every concluded war leaves armies vulnerable to potential future attacks. Times are changing and countries need to re-consider what they spend their budgets on. Additionally, armies need to scan the horizon for emerging trends and invest accordingly. Nonetheless, only a few countries plan far ahead. Governments need to acknowledge that while robots will not replace humans soon, they are key to enhancing human decision-making capabilities. So, they need to be ready and willing to invest whatever it takes in developing their robotic and algorithmic warfighting capabilities to face future threats (Frantzman, 2020b). Any country can develop a good white paper or, if its resources permit, invest billions of Euros into AI. However, it would be that every country's techno-geopolitical intelligence, predictive intelligence and strategic research edge to tell which exact areas it needs to focus its R&D and capability development efforts.

Conclusion and policy recommendations

Compared to the impressive breakthroughs in the Middle Eastern AI sphere (notably in the Gulf), European capitals do not seem to have given much thought to the strategic

implications of AI technologies. Figures seem to prove this claim. In 2018, the top three countries in the global AI start-up ecosystem were the US, China and Israel (Brattberg et al., 2020). Regarding the military applications of AI in Europe, applying research into practice still remains a major issue. According to Boston Consulting Group, the EC must prioritise three points to catch up. First, it should aim to establish a pan-European, common data space for strategic sectors. Second, the EU should maintain and guarantee AI sovereignty. Third, the EU should catalyse the implementation of industrial programmes to boost the deployment of AI in various sectors (Candelon et al., 2020).

Part of the delay may be linked to the fact that Europe adopts a much more critical stance on the ethics of emerging defence technologies, including AI. The European Parliament expressed its position on Legal Autonomous Weapons Systems (LAWS) in successive resolutions (EP, 2018 and 2021), calling for a ban thereof and recalling that the development and use of LAWS raises fundamental ethical concerns. The EC High Level Expert Group referenced the Parliament's position in its Ethics Guidelines for Trustworthy AI (2019). Wary of the potential ethical implications of the AI breakthrough in the MENA region, Brussels can play a pivotal role in preventive governance. Put differently, the EU needs to pioneer the creation of a smart regulation mechanism for AI technologies, and, in parallel, strive to develop its own, "trustworthy" AI. This would not only provide the EU with a much-needed competitive advantage but also with a unique selling point (Csernatoni, 2019).

While this ethical standpoint can easily be shadowed by greedy economic considerations, it might be Brussels' best shot to enter the game in the near future amid MENA's rise. If a Union-wide, unified approach in this respect succeeds, it can also be the only mechanism vis-à-vis the Middle East's AI solutions, which do not come with many ethical strings attached. The concept of AI sovereignty would be key here, as it would mean applying the technologies with a "European touch".

At the same time, the EC could establish cross-regional partnerships with the pioneering Middle Eastern states on developing joint military AI programmes. The Italian-Israeli cooperation on AI technologies is a prime example in this regard. While working on its own alternative to Middle Eastern digital solutions, Europe must also seek ways to work together with leading powers.

- Overall, the Middle Eastern nations, to varying degrees, are aware of the AI-related applications of the military realm, which stands to become a game-changer in terms of military modernisation. That said, there is great variation of defence-relevant AI capacities among actors across the region, with differing comparative advantages. The Gulf Arab countries have economic resources to sustain the heavy investments required to lead on AI. Iran, on the other hand, enjoys a good reverse engineering base, while Israel has the most developed ecosystem along with a robust defence technological and industrial base, as well as the right economic model.

- A major challenge regarding AI in the MENA region is building local expertise. This will restrict black swan events and avoid any negative, high-impact scenarios. If they have not already done so, every country should aim to adopt robust computing power and algorithms to minimise biases or failures. Further, imported AI requires enhanced security measures as it may present the risk "of backdoor access" (Warner, 2021).

The EU needs to pioneer the creation of a smart regulation mechanism for AI technologies, and, in parallel, strive to develop its own, "trustworthy" AI

- Geopolitically, the AI breakthrough will bring about clear winners and losers, including in the MENA region. These winners and losers will have varying degrees of national capacities, pointing to an incoming reshuffle driven by high-tech, including AI. Not only the regional balance of power but also the speed of armed conflict that is likely to change soon. The future Middle Eastern wars will be more high-tech driven, smarter and faster. These shifts must be anticipated and factored into the EU's strategic and security outlook on the MENA region.

- The EU has to be aware of the fact that, under the influence of AI in defence, the MENA regional balance of power could change fast. To keep up, Brussels should prioritise promoting public-private partnerships on AI and create robust guidelines on how to apply the new technologies. In addition to developing its own alternative, Europe should also find itself a place in the Middle Eastern market. With the growing presence of Chinese and Russian solutions, Brussels should act swiftly to guarantee its spot in the region's emerging AI industry.

- There is one conclusive consideration that should guide the EU's take on Middle Eastern AI-investments. Any country in question can develop a good white paper or, if its resources permit, invest billions of Euros in AI. However, it is the country's techno-geopolitical intelligence, predictive intelligence, and strategic research edge that will tell in which exact areas it needs to focus its R&D and capability development efforts.

References

ABDUL-ENEIN, H. (2020, October 22). *Introducing Saudi Arabia's national strategy for data and AI.* Access Partnership. Retrieved from https://www.accesspartnership.com/introducing-saudi-arabias-national-strategy-for-data-and-ai/

ACCENTURE (2018). *Pivoting with AI. How artificial intelligence can drive diversification in the Middle East.* Retrieved from https://www.accenture.com/_acnmedia/pdf-77/accenture-impact-ai-gdp-middle-east.pdf

ACCENTURE RESEARCH (2021). *The rise of forerunners.* Retrieved from https://www.accenture.com/ae-en/insights/research/rise-forerunners

BERGMAN, R., & FASSIHI, F. (2021, September 18). The scientist and the A.I.-assisted, remote-control Killing Machine. *The New York Times.* Retrieved from https://www.nytimes.com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html

BRATTBERG, E., CSERNATONI, R., & RUGOVA, V. (2020). *Europe and AI: Leading, lagging behind, or carving its own way?* Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236

CANDELON, F., BÜRKNER, H., DURANTON, S., LANG, N., CARLO, R., & DE BONDT, M. (2020, June 15). *Europe can catch up in AI, but must act—Today.* BCG Global. Retrieved from https://www.bcg.com/publications/2020/europe-can-catch-up-in-ai-but-must-act-today

CSERNATONI, R. (2019, August 21). *Beyond the hype: The EU and the AI global 'Arms race'.* European Leadership Network. Retrieved from https://www.europeanleadershipnetwork.org/commentary/beyond-the-hype-the-eu-and-the-ai-global-arms-race/

CSERNATONI, R. (2021). *The EU's rise as a defense technological power: From strategic autonomy to technological sovereignty.* Retrieved from https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134

DE VYNCK, G. (2021, July 7). The U.S. says humans will always be in control of AI weapons. But the age of autonomous war is already here. *The Washington Post.* Retrieved from https://www.washingtonpost.com/technology/2021/07/07/ai-weapons-us-military/

ECKSTEIN, M. (2021). Navy's new Middle East task force to find ways to apply AI and unmanned to complex region. *Defense News.* Retrieved from https://www.defensenews.com/naval/2021/10/04/navys-new-middle-east-task-force-to-find-ways-to-apply-ai-and-unmanned-to-complex-region/

EY CONSULTING (2018). *Artificial intelligence in the Middle East and North Africa. Outlook for 2019 and beyond.* Retrieved from https://info.microsoft.com/rs/157-GQE-382/images/report-SRGCM1065.pdf

FELDSCHER, J. (2022, February 8). Iran is 'No. 1 destabilizing' threat In Middle East, CENTCOM Nominee Says. *Defense One.* Retrieved from https://www.defenseone.com/threats/2022/02/iran-no-1-destabilizing-threat-middle-east-centcom-nominee-says/361762/

FINAUD, M., ROBINSON, T., & SALEH, M. (2021). *Is there a new chance for arms control in the Middle East?* Arms Control Association. Retrieved from https://www.armscontrol.org/act/2021-06/features/there-new-chance-arms-control-middle-east

FOUCHER, L. (2021, May 20). *Where is the EU in the great conflicts of the Middle East?* Crisis Group. Retrievd from https://www.crisisgroup.org/middle-east-north-africa/eastern-mediterranean/israelpalestine/agenda-exterior-la-ue-y-oriente-proximo

FRANTZMAN, S. J. (2020a, July 6). Groundbreaking UAE-Israel deal to fight coronavirus unites key defense companies. *The National Interest.* Retrieved from https://nationalinterest.org/blog/coronavirus/groundbreaking-uae-israel-deal-fight-coronavirus-unites-key-defense-companies

FRANTZMAN, S. J. (2020b, October 13). Israel's use of artificial intelligence will change the future of war. *The National Interest.* Retrieved from https://nationalinterest.org/blog/buzz/israel%E2%80%99s-use-artificial-intelligence-will-change-future-war-170415?page=0%2C1

FRANTZMAN, S. J. (2021, April 21). Israel and UAE defense companies partner on Artificial Intelligence. *The National Interest.* Retrieved from https://nationalinterest.org/blog/buzz/israel-and-uae-defense-companies-partner-artificial-intelligence-183274

FRANTZMAN, S. (2022, February 11). Israel unveils artificial intelligence strategy for Armed Forces. *C4ISRNet.* Retrieved from https://www.c4isrnet.com/artificial-intelligence/2022/02/11/israel-unveils-artificial-intelligence-strategy-for-armed-forces/

HELOU, A. (2021a, September 22). UAE, Britain ink defense research and AI tech deals. Here's what comes next. *Defense News.* Retrieved from https://www.defensenews.com/global/2021/09/22/uae-britain-ink-defense-research-and-ai-tech-deals-heres-what-comes-next/

HELOU, A. (2021b, February 24). AI militarization will be 'force multiplier' for UAE, Saudi Arabia. *C4ISRNet.* Retrieved from https://www.c4isrnet.com/artificial-intelligence/2021/02/24/ai-militarization-will-be-force-multiplier-for-uae-saudi-arabia/

HELOU, A. (2020, February 25). Meet Garmousha: A new rotary-wing drone made in the UAE. *Defense News.* Retrieved from https://www.defensenews.com/unmanned/2020/02/25/meet-garmousha-a-new-rotary-wing-drone-made-in-the-uae/

IBM (2019). *Middle East prepares for AI acceleration.* Retrieved from https://www.ibm.com/thought-leadership/institute-business-value/report/ai-middle-east

KHUSHNAM, P. (2020, July 10). Is the Middle East becoming a hub of artificial intelligence? *Diplomatist*. Retrieved from https://diplomatist.com/2020/07/10/is-the-middle-east-becoming-a-hub-of-artificial-intelligence/

KUMAR JHA, M., & DAS, A. (2021). *AI technology in military will transform future warfare.* Retrieved from http://bwdefence.businessworld.in/article/AI-Technology-In-Military-Will-Transform-Future-Warfare/13-08-2021-400557/

LAYTON, P. (2018). *Algorithmic warfare: Applying artificial intelligence to warfighting.* Australia Air Power Development Centre.

LISMAN, E. (2021). Iran's bet on autonomous weapons. *War on the rocks.* Retrieved from https://warontherocks.com/2021/08/irans-bet-on-autonomous-weapons/

MACCARTHY, M., & PROPP, K. (2021). *Machines learn that Brussels writes the rules: The EU's new AI regulation.* Brookings. Retrieved from https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/

MATEI, S. (2021). The first (and only) law of robotic warfare. *The strategy bridge*. Retrieved from https://thestrategybridge.org/the-bridge/2021/11/17/the-first-and-only-law-of-robotic-warfare

MEZHER, C. (2021, February 25). Lockheed to use UAE-designed AI for all aircraft. *Breaking Defense.* Retrieved from https://breakingdefense.com/2021/02/lockheed-uses-uae-designed-ai/

OECD AI POLICY OBSERVATORY (2020). National Data and AI Strategy. Retrieved from https://oecd.ai/en/dashboards/policy-initiatives/%2F%2Faipo.oecd.org% 2F2021-data-policyInitiatives-26934

PARGOO, M. (2019). *Sanctions propel Iran in the global race for terminator-like AI.* Atlantic Council. Retrieved from https://www.atlanticcouncil.org/blogs/iransource/sanctions-propel-iran-in-the-global-race-for-terminator-like-ai/

PWC (2018). *US$320 billion by 2030? The potential impact of Artificial Intelligence in the Middle East*. Retrieved from https://www.pwc.com/m1/en/publications/potential-impact-artificial-intelligence-middle-east.html

QAIDARI, A. (2022, January 4). *There's talk of a military option against Iran. Here's why it's unlikely.* Atlantic Council. Retrieved from https://www.atlanticcouncil.org/blogs/ iransource/theres-talk-of-a-military-option-against-iran-heres-why-its-unlikely/

QATAR GOVERNMENT COMMUNICATIONS OFFICE (n.d.). *Qatar National Vision 2030*. Retrieved from https://www.gco.gov.qa/en/about-qatar/national-vision2030/

REPORT, S. (2021, September 7). Middle East companies training staff for AI-powered jobs. *Khaleej Times.* Retrieved from https://www.khaleejtimes.com/corporate/middle-east-companies-training-staff-for-ai-powered-jobs

SABALLA, J. (2021, October 5). US Navy to apply unmanned AI technologies in Middle East. *The Defense Post.* Retrieved from https://www.thedefensepost.com/2021/10/05/us-navy-ai-middle-east/

WALSH, B. (2021). *An insider's view of "algorithmic warfare."* Axios. Retrieved from https://www.axios.com/robert-work-artificial-intelligence-warfare-5d8d362b-4fc9-4b9e-aef1-4afe97ca39be.html

WARNER, K. (2021, February 21). UAE minister lays out pressing need and challenges of integrating AI in defence. *The National News.* Retrieved from https://www.thenationalnews.com/business/uae-minister-lays-out-pressing-need-and-challenges-of-integrating-ai-in-defence-1.1169491

AI Regulation in MENA: Brussels Effect vs. Beijing Effect

Kristina Kausch
Senior Resident Fellow, The German Marshall Fund of the United States*

* The author would like to thank Peter Chase, Lewin Schmitt and Astrid Ziebarth for their useful comments on an earlier draft of this chapter. She is equally grateful to the officials and experts who granted their time for an interview.

Introduction: The global conversation on AI governance

Acknowledging the regulatory challenges of digital transformation has led policy- and law-makers across the world to think about ways to ensure trustworthy artificial intelligence (AI) and mitigate the risks associated with different uses of AI systems. Since Canada launched the first national AI strategy in 2017, three dozen countries have followed suit. Newly launched multilateral fora such as the Global Partnership on AI (GPAI) or the Organization for Economic Co-operation and Development (OECD) AI Policy Observatory have supported intergovernmental efforts to foster AI for universal benefit. Several of these bodies, including the OECD, the Council of Europe and United Nations Educational, Scientific and Cultural Organization (UNESCO), have developed guiding principles that show an emerging international consensus on what AI regulation should aspire to: a trustworthy, human-centric AI that maximises benefit to humankind while safeguarding fundamental rights and liberties.

Regulatory measures enacted or contemplated to face this challenge range from soft law guidelines to sectoral hard law regulation, including outright bans of specific technologies, regulatory experimentation ("sandboxes"), and technical standardisation. Although countries overall still predominantly retain soft law approaches, and as of March 2021, no comprehensive, horizontal legal framework on AI has been adopted, there is a nascent trend towards legislative reform and hard law regulation (OECD, 2021a). The European Union (EU) gave a boost to global debates on AI governance when the European Commission (EC) released, in June 2021, its draft proposal for a regulation on AI (EC, 2021), the first ever comprehensive attempt to regulate it. Building on the success of the EU's 2016 General Data Protection Regulation ([GDPR] EP, 2016), which set a new global standard through the widespread adoption of data protection and privacy rules across the world, many in Brussels hope to exert a similar global regulatory power in setting global ground rules for AI that will be preemptively adopted by major AI producers thanks to the attractiveness of the Single Market. The proposal, if swiftly adopted by the European Parliament and Council, could enter into force in late 2022 or early 2023. EU ambition to shape global norms is not universally appreciated, however. Although common concerns over Chinese dominance in tech has given birth to the new United States (US)-EU Trade and Technology Council, the US remains fearful that a "Brussels Effect" (Bradford, 2020) in AI could erode US tech companies' freedom and stifle innovation.

The Middle East and North Africa (MENA) region, dominated by different models of authoritarian governance and assembling a range of volatile security hotspots, will be a key testing ground for how the race for AI standard-setting that will impact security and governance quality. In particular when used in the region's sensitive security sector, fears loom large that AI technologies will boost the power of autocratic regimes that have become expert in utilising Western security concerns to silence dissent at home and fend off criticism from abroad.

This chapter will assess the current regulatory state of AI legislation in selected MENA countries, set in the overarching legal and political context of the region. It will analyse a potential extraterritorial impact EU AI regulation may have in the region. Finally, it will determine what these findings mean for MENA security and democratic governance, and the implications for EU policy.

AI regulation in the Middle East and North Africa

Aside from fostering the widespread adoption of AI technology for a range of beneficial ends, AI policies and regulation respond to concerns raised by AI applications, such as the protection of human rights, privacy, fairness, algorithmic bias, transparency, safety, and accountability (OECD, 2021a). Although, at the time of writing, no country has enacted comprehensive horizontal legislation on AI, some countries have adopted bans on specific high-risk technologies (e.g. Belgium on Lethal Autonomous Weapons Systems [LAWS]) or are considering doing so (e.g. US on specific use cases of facial recognition technology). Moreover, AI uses are woven into other pieces of legislation, such as laws regulating data protection, cyber-crime, industrial standards, law enforcement, arms procurement, export controls, and so on. Importantly, the past two years have seen considerable efforts at the multilateral level (Council of Europe [CoE], OECD, EU) to operationalise high-level principles from a risk-based approach, and in addition many countries have introduced soft law guidelines and standards for AI ethics and governance aligned with the OECD AI Principles (OECD, 2020).

In the MENA region, the first country to adopt a national AI strategy was the United Arab Emirates (UAE) in 2017. As shown in table 1, several MENA countries have since followed suit, either by publishing a national AI strategy (Egypt, Jordan, Lebanon, Morocco, Saudi Arabia, Turkey, UAE, Qatar) or announcing their intention to do so (Tunisia, Algeria, Bahrain). MENA countries that have adopted ethical guidelines for trustworthy AI or are in the process of doing so include Israel, Jordan and the UAE (Dubai). Some have established a National AI Council or similar dedicated government institutions to centrally foster AI across sectors (Egypt, Israel, UAE, Qatar, Saudi Arabia), alongside research centres, networks and centres of excellence for AI development.

The past two years have seen considerable efforts at the multilateral level (CoE, OECD, EU) to operationalise high-level principles from a risk-based approach

Table 1. AI policy and regulation in MENA countries

Country	National AI Institutions	Policy	Soft Law	Legislation (AI or related areas)
Algeria	National Council for Scientific Research and Technologies (CNRST)	National Strategic Plan for Artificial Intelligence 2020-2030 (2021, not publicly available)	n/a	n/a
Bahrain	n/a	National Artificial Intelligence Strategy (under development)	Bahrain AI Procurement Guidelines (2020)	n/a
Egypt	National Council for Artificial Intelligence	Egypt National Artificial Intelligence Strategy (2020 tbc) Data Strategy (under development)	Egyptian Charter on Responsible AI (under development)	Cybercrime Law (2018) Personal Data Protection Law (2020)
Iran	n/a	Digital Iran: National	n/a	n/a

		Roadmap 2020-2025 (2019)		
Iraq	n/a	tbc	n/a	n/a
Israel	National Initiative for Secured Intelligent Systems Israeli Innovation Authority Privacy Protection Authority Competition Authority	Report of the National Initiative to the Government (2021)	Guidelines for AI (under development)	Cyber Law (under development)
Jordan	n/a	Jordan Artificial Intelligence Policy (2020)	National Charter on AI Ethics (under development)	n/a
Lebanon	n/a Agency for Digital Development (ADD)	National Artificial Intelligence Strategy in Lebanese Industry 2020-2050 (2019)	n/a	n/a
Morocco	National Commission for Personal Data Protection (CNDP) Directorate-General for Information System Security (DGSSI)	n/a	n/a	n/a
Oman	n/a	Circular on the use of AI in Government Units (2021)	n/a	n/a
Qatar	Qatar Center for Artificial Intelligence (QCAI) Qatar Computing Research Institute (QCRI)	National Artificial Intelligence Strategy for Qatar (2019)	n/a	n/a
Saudi Arabia	Saudi Data and Artificial Intelligence	National Strategy for Data and AI (2020)	n/a	Personal Data Protection Law (2021)

	Authority (SDAIA) National Centre for AI (NCAI)			Anti-Cybercrime Law (2007)
Tunisia	Task Force AI at the Ministry of Education and Science (2018)	National AI Strategy (under development)	Artificial Intelligence Roadmap 2021-2025 (2019), Ministry of Industry and SMEs	n/a
Turkey	Digital Transformation Office at the Presidency of the Republic of Turkey	National Artificial Intelligence Strategy (2021-2025)		Law on Protection of Personal Data (2016)
UAE	UAE Council for Artificial Intelligence and Blockchain Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications Federal RegLab	UAE Artificial Intelligence Strategy (2017)	AI Guide (2018) AI Principles and Ethics Guidelines for the Emirate of Dubai (2019)	Federal Data Protection Law (2021); Cybercrime Law (2021); Electronic Transactions Law (2006)

Source: OECD AI Observatory, MENA governments, interviews conducted by the authors.

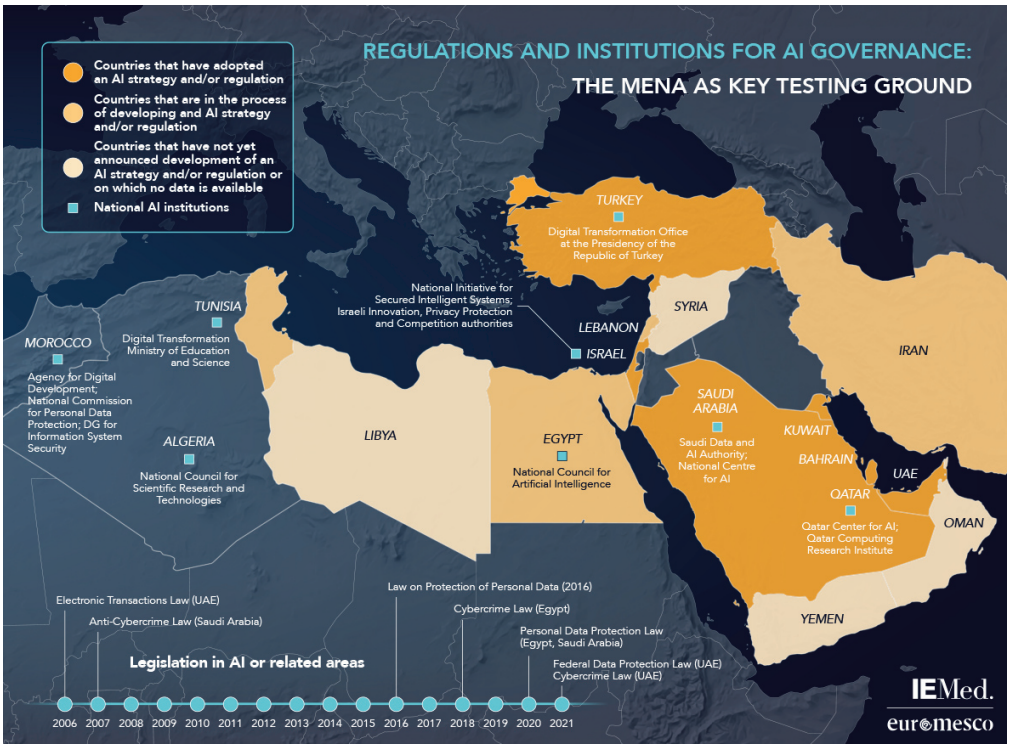
Note: data available for Libya, Syria and Yemen.

Variation across the region is significant, dividing countries into roughly three groups: a vanguard of technologically-advanced countries in the full process of developing a favourable ecosystem for AI (the Gulf Cooperation Council [GCC] states, Israel and Turkey); a middle group with less technological edge but actively developing AI capacity to varying degrees (including Egypt, Iran, Lebanon and Tunisia), and a third group of countries which, due to war and other hardships, have not taken any significant steps in this domain (including Syria, Libya, Yemen).

Variation is also great among the AI strategies that have been formulated in the region. None of the MENA countries has introduced a nationwide AI ethics framework, although some are in the process of developing them while others have introduced such frameworks at the local level (IDRC, 2020), namely the city of Dubai as part of its smart city concept. Despite considerable variation in detail and depth, by and large MENA countries' national AI strategies formulate the countries' objectives in using AI technology to foster and improve industrialisation and productivity, social and economic development, employment, healthcare, and national security. Importantly, however, contrary to the European risk-based approach to AI, available MENA AI strategies overwhelmingly emphasise the opportunities inherent to AI, but barely assess the risks.

Contrary to the European risk-based approach to AI, available MENA AI strategies overwhelmingly emphasise the opportunities inherent to AI, but barely assess the risks

Most frequently mentioned are privacy concerns, as well as quality and safety concerns such as algorithmic bias or data accuracy. Broader mention and assessment of risks to fundamental human rights, however, are notoriously absent. Although references to international soft law norms such as the OECD principles on AI are found in almost all documents, there is little space given to tangible ethics concerns, let alone a clear roadmap on how to mitigate them.



Regulatory efforts in five of the leading AI powers in the MENA region are discussed in greater detail below (selected for AI readiness as well as geographical variation).

The **United Arab Emirates** (UAE) is the frontrunner in the region in terms of AI readiness (IDRC, 2020), helped by an early government vision for the country based on digitalisation which has put the country at the regional vanguard of AI ecosystem development in terms of institutional frameworks, education, data governance, and regulation (Mejri, 2020). The UAE was among the first countries globally and the first in the MENA region to publish a National AI Strategy in 2017, and the first to appoint an AI Minister. With its AI Ethics Guidelines and Toolkit, the city of Dubai also pioneered this kind of soft law in MENA AI regulation. A comprehensive UAE Federal Data Protection Law that came into force in early 2022 largely mirrors the EU's GDPR.

The UAE's AI Strategy notably discusses the opportunities and ambitions regarding AI technology at length but does not discuss AI ethics or human rights concerns. While the AI Ethics Guideline for

the city of Dubai explicitly acknowledges ethics being central to AI research and recommends guiding principles in the domains of ethics, security, humanity and inclusiveness, it also states that "ethics are cultural, and there is not one universal code of ethics" (Smart Dubai, 2020), apparently suggesting that no universal human rights principles should be applied in relation to AI. A particular human rights concern in the UAE, as well as other Gulf states, is AI-enabled surveillance. Having the means to develop and acquire sophisticated technology and helped by the push for implementing broad individual tracking tools in the course of the COVID-19 pandemic, the Gulf states have experienced a boost of AI-enabled surveillance (Jones, 2021). China's domestic surveillance model is likely to provide some inspiration in the context of the UAE's tight technology cooperation with China including on smart cities, AI, big data and 5G, hailed by Chinese officials as "pioneering".

Israel is among the emerging AI economies, ranking 8th among the countries with the highest density of AI players per billion EUR Gross Domestic Product (GDP) (Righi et al., 2021). It also ranks third for AI solutions and has a global AI market share of 11%, equal to China, and 40 times more AI companies per capita than the market leader, the United States (US), leading to a self-description as the "hidden champion of Artificial Intelligence" (Israel Innovation Authority, 2020). Israel views AI as a critical emerging technology directly relevant to its national security. The countries' regulatory efforts in AI have been particularly cautious to strike a balance between innovation and rights protection. A hard law approach such as the European approach to AI regulation is mostly viewed as too rigid and stifling innovation, but a process of soft law development – repeatedly delayed and politicised due to Israeli government reshuffles in recent years – is underway. In 2018, then-Prime Minister Netanyahu launched the National Initiative for Secured Intelligent Systems, a multi-level, multi-stakeholder national task force with the mandate to draft recommendations to the government for an AI guideline, based on the six Israeli AI ethics principles (largely based on the OECD principles for AI). The task force submitted a report to the prime minister, proposing a national strategy for secured intelligent systems (NISIS 2020). The task force's ethics working groups moreover proposed a nuanced model of regulation to match different regulatory approaches based on the risk level associated with a particular activity, with a strong focus on industries' self-regulation ex-ante and dedicated legislation only recommended for medium- and high-risk applications in which the pace of development does not surpass the pace of the legislative process (NISIS Subcommittee, 2019).

Unlawful surveillance is a big topic in Israel's AI sector, too. The country made headlines in 2020 when a list of 50,000 mobile phone numbers, many of them from politicians (including French President Emmanuel Macron), journalists and government-critical individuals, was leaked that had been subject to undue surveillance using the controversial Pegasus malware developed by the Israeli NSO Group. NSO claimed its software was only sold to previously vetted governments for military purposes, law enforcement and crime prevention, but admitted it had no control over the uses of the software post-sale, prompting some Israeli commentators to raise concerns of Israel becoming a hub for authoritarian tech if such software was allowed to be sold to countries without an independent judiciary and a solid rule of law (Ziv,

Israeli export control advocates say it is unlikely that the regulatory measures taken provide a sufficient safeguard to prevent the export of Israeli surveillance malware to authoritarian governments in the future

2021). Israeli legislation on defence exports is generous, meaning that (except in the case of a United Nations Security Council arms embargo) political and diplomatic priorities usually outweigh human rights considerations. In December 2021, the Israeli Ministry of Defence's Export Control Agency imposed additional export control mechanisms on cyber warfare tools in part in response to the international backlash to the Pegasus scandal. However, Israeli export control advocates say it is unlikely that the regulatory measures taken provide a sufficient safeguard to prevent the export of Israeli surveillance malware to authoritarian governments in the future (Gross, 2021). Israel's recent rapprochement with authoritarian MENA countries under the Abraham Accords, widely hailed as peace-making arrangement, is a concern in this regard as it increases the likelihood of such high-risk technology exports.

Egypt has gone to great lengths in recent years to invest in the development of its AI sector. The government has been active in international fora on AI governance and chairs a Cairo-based Arab AI Working Group that seeks to foster harmonised AI policy approaches among Arab countries. In November 2019, the government created a National Artificial Intelligence Council chaired by the Minister of Communication. The multi-stakeholder body eventually outlined Egypt's National AI Strategy and oversees its implementation. In terms of soft law, the Egyptian government has announced its intention to develop a Charter on Responsible AI to include assessment guidelines, technical guidelines and good practices. The National AI Strategy acknowledges processes and norms of international AI governance, and briefly discusses the need for responsible and ethical AI "policies, regulations and legislations to mitigate potential misuse," and as an enabler for the widespread adoption of AI. It also recommends setting up an ethics track within the National AI Council to act as an advisory body and clearing house for AI ethics, including by implementing the aforementioned National Charter for Responsible AI (Egyptian National Council for Artificial Intelligence, 2019).

Concerns regarding AI in Egypt's security sector relate to the country's renewed clampdown on human rights under President al-Sisi's military regime, as well as the growing cooperation with China in approximating Egypt's digital/tech governance to China's. Following the signature of a Digital Silk Road memorandum, Beijing and Cairo moved fast in their cooperation, including visits by Egyptian officials of Chinese big tech firms, talks on increasing Chinese investment in AI, a new Egyptian cloud computing centre built by Huawei, and increased Chinese financing of the Egyptian telecommunications sector. In order to serve its great ambitions in tech, Egypt needs urgent infrastructure upgrades and access to cheap 5G. At the same time, Chinese support could include help on how to use AI and other advanced technologies to silence dissent, as Chinese trainings on censorship for Egyptian officials appear to suggest. In 2018 Egypt adopted a cybercrime law that moves the country closer to China's model, enhancing the government's ability to censor online and sanction those who access or publish information (Kurlantzick, 2020).

Turkey does not yet have a specific piece of legislation governing AI, and the overall regulatory background remains underdeveloped. However, Ankara issued a National AI Strategy in 2021, prepared by the Turkish Presidency's Digital Trans-

formation Office. Turkey also actively contributed to global AI governance discussions, such as in the Council of Europe's Ad-hoc Committee for Artificial Intelligence (CAHAI). Discussions of AI regulation in Turkey are currently evolving around data protection and privacy. Notably, Turkey has a data protection regulation, mostly modelled after the EU's original 1995 Data Protection Directive, but there are plans to reform the law in line with the EU's GDPR (EP, 2016).

Turkey's National AI Strategy refers to the internationally acknowledged ethical principles on human-centric AI to which Turkey is formally ascribed, such as those by the OECD, the G20, the EU and UNESCO (Turkish Ministry of Industry and Technology, 2021). At the same time, the strategy fails to adequately detail how and by whom the application of these principles should be supervised. Two working groups within the strategy's steering body, on AI Law Ethics and Trustworthy and Responsible AI, respectively, will provide advice. Notably, Ankara is a major producer and exporter of AI-powered drones including LAWS. The deployment of Turkish autonomous drone weapons in Libya has been reported as one of the first documented instances of LAWS deployment. There have been discussions on export controls on Turkish LAWS among Turkish academics, but no legislative proposals have been brought forward.

The government of **Tunisia** has made several attempts to develop a national AI strategy. In 2018, the Ministry of Higher Education and Research launched an AI Task Force of experts to this end, including 10 thematic working groups. Political instability in the run-up to the 2019 presidential elections, however, prematurely ended this undertaking. In 2019, the Ministry of Industry launched, as part of its larger industrial development strategy, an internal roadmap to develop Tunisia's AI ecosystem, which, while launching a host of AI-related initiatives in research and training, also stopped short of developing an AI strategy or other draft AI policy or regulation. (Mejri, 2020). The slowly escalating political crisis in Tunisia around the centralisation of power by President Kais Saied, however, is likely to paralyse major advancements in this area in the near future.

AI regulation and authoritarian governance

MENA governments, in speech and policy, emphasise the growth and development opportunities inherent in AI. Used in MENA law enforcement, on the one hand, AI technologies could boost these countries' capacities to face their very real security concerns, such as in countering violent extremism or in curbing irregular migration. On the other hand, where a weak rule of law fails to shield citizens from abuses, fears loom large that AI technologies could turn into a bionic arm of unaccountable rulers, further entrenching authoritarianism at Europe's doorstep.

Where a weak rule of law fails to shield citizens from abuses, fears loom large that AI technologies could turn into a bionic arm of unaccountable rulers, further entrenching authoritarianism at Europe's doorstep

The World Justice Project (WJP) defines four universal principles of the **rule of law:** accountability, just law, open government, and accessible and impartial justice (WJP, 2021). Table 2 below shows the rule of law scores of MENA countries and their ranks in global comparison. Although here, too, we see considerable variation, the overall picture is of a region with weak to very weak rule of law, which draws a worrisome picture with regard to the potential effectiveness of regulation of some of the politically more sensitive use cases of AI.

Table 2. Rule of law in the MENA region, 2021

Country	Global Rank (of 139)	Global Score (0-1)
UAE	37	0.64
Jordan	59	0.55
Tunisia	65	0.53
Algeria	82	0.49
Morocco	90	0.49
Lebanon	104	0.45
Iran	119	0.42
Turkey	117	0.42
Egypt	136	0.35

Source: World Justice Project (2021).

Even under the assumption that an impeccable regulative framework for AI can only be as protective as the judicial system safeguarding its essence, just legislation is a precondition for effective human rights safeguards. The global under-regulation of AI is echoed in the MENA region. As detailed above, despite considerable dynamism in this area in recent years, and governments across the region working on different regulatory documents, AI regulation in the MENA region so far remains largely soft law, lacking avenues of accountability. Notably, the published strategy and guidance documents on AI devote very little space to human rights and ethics, suggesting a box-ticking exercise rather than a serious concern. None of them provides a deep, comprehensive analysis on how AI systems may affect human rights, let alone concrete steps on how to mitigate these risks, contrasting with the significant detail devoted to economic competitiveness and innovation advantage (Stanford, 2021). In addition, any of the laws governing the use of AI in specific use cases (such as the notorious cyber-crime laws) fall short of international standards in their lack of proportionality.

MENA governments, inspired and supported by China, have deliberately built up their (partially AI-enabled) surveillance and control capabilities

The instrumentalisation of national security to suppress dissent has been a central element of MENA authoritarian governments' toolbox for decades. The opportunities presented by AI, including the potential boost to authoritarian control, makes these processes only more salient in the field of AI technologies. The aftermath of the 2011 Arab uprisings has witnessed a sharp clampdown on human rights, political dissent and civic activism across the MENA region. Žilvinas Švedkauskas's chapter in this volume shows in greater depth how digital technologies, hailed as a wand of liberation a decade ago, have been co-opted as control tools by authoritarian regimes. The COVID-19 pandemic has given a further boost to this trend as citizens have volunteered personal data to governments and tracking apps have become household items. MENA governments, inspired and supported by China, have deliberately built up their (partially AI-enabled) surveillance and control capabilities to upgrade their authoritarian control toolbox in the different arms of government.

In sum, if in global debates on AI governance and regulation some use cases raise significant concerns regarding safety and accountability, and human rights and fundamental liberties at large, the lack of effective regulation in an authoritarian context maximises these concerns manifold. Evidence abounds that MENA governments see AI not merely as an opportunity for growth and development but equally for a con-

venient rationalisation of an organised clampdown of political dissent to secure the political status quo. This political premise, and the devastating effect an institutionalisation of largely unregulated AI uses in the MENA security sector might have on the region's politics and security, must take centre stage in any EU cooperation on AI with MENA governments.

Europe's regulatory power in AI

What impact could the EU's draft AI Act have on future AI regulation in MENA countries, and on the use of these technologies in the region's security sector? The Commission's draft act, which proposes rules for the development, placement on the market and use of AI systems in the EU from a risk-based approach, represents a deliberate leap forward in international debates on a global regulatory consensus for emerging tech. Ongoing discussions in the EU-US Trade and Technology Council speak to this overarching theme, and the EU draft rulebook's influence will also be conditioned by how Europeans engage the US and other partners in ongoing debates on the creation of a global AI norms regime (Csernatoni, 2021). In a market dominated by US and Chinese technologies, transatlantic allies have been keen on preventing prevalence of Chinese norms and standards, which notably could create wider opportunities for authoritarian uses of AI technologies and reduce consumers' trust in AI, to the detriment of the far-reaching spread of trustworthy, beneficial uses of AI. In this context, the MENA region presents an interesting case study as to the potential impact the new EU AI regulation could have beyond the EU's borders.

While the EU lacks jurisdiction beyond its borders, debates on the EU's draft AI Act have raised expectations that the regulation may develop an extraterritorial reach. This largely points to an impact by market forces, i.e. the fact that rules and standards set by the regulation will also apply to companies outside of the EU that want to export AI technology or AI-powered goods and services to the Single Market, which might incentivise companies – and potentially even legislators – to adopt EU norms and standards. When discussing the potential impact of EU regulation in AI, we must distinguish between the purchase and use of AI, and impact of regulatory frameworks abroad.

In terms of the purchase and use of AI systems, in a nutshell, the Commission's draft EU AI Act bars certain high-risk AI technologies on the EU market, but not abroad. Importantly, this means that it does not ban European companies from producing and exporting these high-risk technologies to third countries. The degree to which MENA governments and/or private companies could still acquire EU-produced high-risk AI technology hence depends not on the AI Act but on the effectiveness of the EU's export control regime at large. The EU Export Control Regulation, recast in 2021, governs the export of dual use goods, services and technologies to both governments and non-governmental customers (EP, 2021b). It raises the dangers of authoritarian abuse of dual use goods in no uncertain terms and makes export of listed dual use goods subject to mandatory clearance via export licensing. It also creates the possibility for member states to require EU licensing of goods and technologies that could present human rights risks but are not covered by multilateral export regimes. Although the new Regulation is largely focused on goods and technologies but not the end-user, it pays explicit attention to cyber surveillance tools and does allow for human-rights based controls of exports by the EU, thereby creating a mechanism to limit the

In the absence of a highly effective dual use exports control regime, AI-enabled systems and in particular surveillance tools magnify the already ample opportunities for abuse for digital authoritarianism

export of specific AI systems if the EU so chooses. As shown in Žilvinas Švedkauskas's chapter of this volume, the multilateral export control regime enshrined in the Wassenaar Arrangement, of which all EU-27 are members, does not allow for human rights-based licensing requirements. Some leading European experts have therefore called for an immediate moratorium on the sale of spyware technology until a global export regime can identify and place these tools under global restraint (Kaye & Schaake, 2021). In the absence of a highly effective dual use exports control regime, AI-enabled systems and in particular surveillance tools magnify the already ample opportunities for abuse for digital authoritarianism.

The outlook for the export of AI in military technology is not more encouraging. EU treaties reserve national security to the exclusive competence of member states that jealously guard this prerogative, which often constrains or produces deadlock in efforts of regulation in areas which by their nature require a multilateral regulative regime, such as surveillance malware – brought back to the fore of European debates by fresh revelations of Pegasus spying on European politicians in April 2022 – or LAWS.[33] In line with member states' national security prerogative, the scope of the AI Act explicitly excludes AI systems "explicitly developed or used for military purposes."[34] It also excludes AI systems that are used by government authorities outside of the Union "in the framework of international agreements for law enforcement or judicial cooperation with the Union or one or more Member States" (EC, 2021). The latter would apply to most MENA governments, meaning that those that have such cooperation/agreements with the EU or a member state could use high-risk AI in their law enforcement, regardless of the quality of the laws that are being enforced or the autocratic nature of their regimes. Given EU member states' own security interests, no meaningful toning down of these carve-outs that may be introduced by the Parliament is likely to be accepted by the Council, which is necessary to pass the legislation.

In terms of impact on MENA regulation, the EU's AI Act could in theory lead to a *de jure* Brussels Effect as MENA governments seek to adopt similar rules, with smooth access to the EU single market as a big incentive. More likely, as MENA governments are currently not inclined towards horizontal AI regulation, MENA companies – inspired by soft law guidelines or not – may pre-emptively adopt EU AI regulative norms and standards without their legislative bodies adopting any mandatory rules. Such a *de facto* Brussels Effect is already happening as some tech companies in Israel or Tunisia have asked their governments not to bother coming up with AI regulation of their own but to adopt the EU rules instead. The likelihood of a broader regulatory

[33] According to Anja Dahlmann, Head of Project on the Regulation of Autonomous Weapons at the German Institute for International and Security Affairs, international efforts to regulate and define MHC may best be geared not towards an international treaty, but a mix of hard law measures and dynamic soft-law mechanisms – a "Treaty Plus" approach. According to Ms Dahlmann, the EU's contribution to the norm-making process is already well underway, and a definition of meaningful human control can be consolidated through a Common Position, as mentioned in the Parliament's resolution of January 2021, where member states can provide contributions and translate the main principles into national and international law.

[34] The EU only recently agreed to discuss the impact of AI development and digitalisation on the defence sector. The European Parliament has adopted several resolutions on LAWS and AI in defence, and called for a common EU position on LAWS. See EP, 2021b: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0009

Brussels Effect in third countries, *de jure* or *de facto*, is closely linked to the market ties between a given jurisdiction and the EU. As long as the EU remains the biggest consumer market in the world, there is a reasonable expectation of some degree of a global spread of its regulatory standards (Bradford, 2020). At the same time, EU officials maintain that the experience of GDPR is not necessarily transferable to the AI Act, in part because the provisions in the AI Act itself do not make demands of the regulatory environment in third countries in the scope GDPR does (which already regulates the processing of personal information of EU citizens globally, including with AI-enabled systems).

Further, as the MENA region is a net importer of AI technology, the future of AI governance, norms and standards in MENA countries is closely linked to the origins of those technologies. As Aitor Bonsoms and Lewin Schmitt's chapter in this volume shows, AI technology in the MENA region mostly originates from China, the US and the EU. Beijing has specifically courted the MENA region as part of its technological expansionism and has signed Digital Silk Road memoranda of understanding on digital technology cooperation under the Belt and Road Initiative (BRI) with Egypt, Turkey, the UAE and Saudi Arabia[35] (Eurasia Group, 2020). As governments in the MENA region have great demand (and money, in some cases), paired with low scruples, China appears an ideal provider at a political and regulatory level, and more so if US exporters of AI technology voluntarily adapt to higher standards along the lines of the EU's AI regulation (Qiang, 2021). That said, the possibility of US companies not bowing to the AI Act's stipulations for their entire production, as well as the outlook that EU exporters of AI systems may still develop and export "bad AI" products for the global market, would relativise the Chinese comparative advantage in authoritarian tech.

EU officials underline that much of the value of the EU's AI Act lies in the fact that it enshrines technical quality standards that ensure the accurate functioning and safety of AI-enabled applications and will thus be treasured by any user and government regardless of their political leaning or state of regulation. Quality and trustworthiness of AI, they argue, will ultimately prevail as the key features that remain crucial to all who seek to purchase AI technology, be they democratic or authoritarian. While this is certainly true to some degree, the quality metrics do change with an AI system's use case and user interest: a democratic, accountable government is likely to have other quality priorities than an authoritarian regime using AI to keep dissent in check, which will not worry to the same degree about, say, false positives. But even if Chinese AI products do not fully match US and European quality standards, MENA clients may prefer Chinese technology when it is both considerably cheaper thanks to massive Chinese state subsidies (Feldstein, 2020) and comes without a string of regulatory requirements. MENA governments and stakeholders may well choose to retain regulatory ambiguity and purchase high-risk goods that are banned or controlled in the EU from cheaper and/or less-regulated providers such as Israel or China, providing the

As the MENA region is a net importer of AI technology, the future of AI governance, norms and standards in MENA countries is closely linked to the origins of those technologies

[35] As part of an effort to diversify the country's economy away from oil and boost the private sector, the Saudi AI Strategy aims to accelerate AI development and, by 2030, Saudi Arabia intends to train 20,000 data and AI specialists, attract USD 20 billion in foreign and local investment, and create an environment that will attract at least 300 AI and data start-ups. During the summit where the Saudi government released its AI strategy, the country's National Center for Artificial Intelligence (NCAI) signed collaboration agreements with China's Huawei and Alibaba Cloud to design AI-related Arabic-language systems (Stanford, 2021).

latter with a comparative advantage in authoritarian tech supply. The result could be a "Beijing Effect" (Erie & Streinz, 2021) in AI as the counter piece of the Brussels Effect, leading to a global AI market split in two, with a high-quality, highly regulated segment served by EU and US companies, and a lower quality, less regulated "AI Wild West" catered to by China and other upcoming producers of authoritarian tech (possibly also served by EU and US developers, in the absence of effective export controls).

Of course, there are many nuances and caveats to such an outlook, which are likely to condition the large grey zone between these two extremes. For starters, it remains to be seen to what degree recent EU regulations will effectively bar companies located in EU member states from exporting sensitive security-relevant AI technologies abroad (Chase & Windwehr, 2021). Importantly, US companies not applying the same strict rules as Europeans could surpass China's competition in the MENA region and push EU companies out of the market (as chapter 2 in this volume shows, in surveillance technology this is already the case as US, Canadian and Israeli companies, not Chinese, are the main providers to the MENA region). Another scenario is that China might overtake Western competitors in advancing its own AI regulation, as suggested by Beijing's substantial recent ambition in launching new tech laws, such as its proposed draft laws on algorithm management (2021) and deepfakes (2022). Further, emerging regional AI powers such as Israel, the UAE or Turkey could also turn into major providers of authoritarian tech – which in part is already a reality, as evident in Israel's export of Pegasus spyware and other sensitive military and dual use technology across the region. Finally, the fact that the EU's international partners do not necessarily share the Union's enthusiasm about the EU setting global norms and standards in AI by means of pre-emptive regulation – quite the opposite in fact, with Washington fearful of a Brussels Effect in AI (Matthews, 2021) – could further limit the exterritorial reach of the AI Act. On the other hand, while the very notion of extra-territorial intent is likely to create tension, it may equally serve as an incentive for others to move ahead of the EU (Henig, 2021), especially if the EU's draft AI Act lingers in legislative limbo beyond 2022. In a similar vein, it remains to be seen if international efforts of coordinating AI regulation, including in the EU-US Technology Council, lead to concrete results in coordination and joint norm-setting, beyond the shared preoccupation about Chinese dominance in tech.

Conclusion and policy recommendations

The chapter has shown how the MENA region's under-regulation in AI contrasts with its significant interest and investment in AI, including and especially in the sensitive security sector. In the MENA's authoritarian setting and trajectory of recent years, this forms a worrisome trend that must take centre stage for EU policy when considering cooperation with MENA governments on AI.

Importantly, EU policies towards the MENA in the area in AI must be placed within the EU's larger efforts to shape emerging norms on AI governance and promote a human-centric, values-based regulatory global framework for AI that boosts the opportunities of AI and helps innovation to thrive while effectively mitigating the risks associated with some of its uses. This is most urgent in the sensitive area of security and defence where the danger of abuse looms largest, with a potentially devastating impact on neighbourhood geopolitics and EU security. Under this general premise, the EU should:

- In Brussels, systematically assess the external dimension of the EU AI Act, and the impact of its extraterritorial regulatory power, including adverse effects, on security and digital rights in third countries.

- Amend the language on security carve-outs in the final draft of the AI Act, and other relevant regulation, making sure to establish effective safeguards to prevent EU tech companies from exporting high-risk dual use or military AI to authoritarian governments.

- Make sure the human rights and geopolitical dimensions of EU strategy on AI is understood and taken into account across institutions and policies; and in the same vein, ensure EU strategy on AI is embedded in a larger EU strategy on technology as a geopolitical asset in the EU's external relations.

- On the global stage, engage partners bilaterally and in multilateral fora to work towards a global consensus for AI norms, including by explaining the EU regulatory approach on AI and mitigating fears of EU regulatory expansionism.

- In this context, step up efforts to engage international partners on regulating LAWS, where a global norms regime is particularly urgent.

- Support the involvement of MENA governments, research institutions, private sector stakeholders and watchdogs in multilateral fora and consultations on AI governance.

- In the MENA region, as the first step in a sequenced approach of cooperation on AI, work with governments on devising a thorough regulatory framework, including on AI standards, data protection, cyber security, and so on, that echoes the standards of safe and trustworthy AI as reflected in the EU AI regulation, the OECD principles, and other agreed international standards.

- In subsequent steps, help foster a favourable AI ecosystem, including through training/capacity-building in AI standards to MENA bureaucrats, law-makers, and journalists, and fostering public-private partnerships between European and MENA tech companies on AI that respect and promote agreed principles on trustworthy AI.

- Last but not least, aside from designing cooperation with governments on AI, it will be of the utmost importance to strengthen digital rights civil society groups in the MENA region – financially, politically and legally. For the financial dimension, the EU should consider setting up a dedicated Digital Rights Fund for the MENA region, or for the whole EU neighbourhood.

References

BEN-ISRAEL, I., MATANIA, E. & FRIEDMAN, L. (2020). *The National Initiative for Secured Intelligent Systems to empower the national security and techno-scientific resilience: A national strategy for Israel. Special Report to the Prime Minister.* Tel Aviv University.

BRADFORD, A. (2020). *The Brussels Effect: How the European Union rules the world.* Oxford University Press.

CHASE, P., & WINDWEHR, J. (2021). *The EU, export controls, and minding the national security gap.* The German Marshall Fund of the United States.

COHEN, J., & FONTAINE, R. (2020). Uniting the techno-democracies. *Foreign Affairs.*

COUNCIL OF EUROPE (CoE). (2020). *Towards regulation of AI systems.* Council of Europe's Ad-hoc Committee for Artificial Intelligence.

CSERNATONI, R. (2021). *The EU's rise as a defense technological power: From strategic autonomy to technological sovereignty.* Carnegie Endowment for International Peace.

EGYPTIAN NATIONAL COUNCIL FOR ARTIFICIAL INTELLIGENCE (2019). *Egypt National Artificial Intelligence Strategy.* Retrieved from https://mcit.gov.eg/Upcont/Documents/Publications_672021000_Egypt-National-AI-Strategy-English.pdf

ERIE, M., & STREINZ, T. (2021). The Beijing Effect: China's digital Silk Road as transnational data governance. *New York University Journal of International Law and Politics, 54*(1), 2-21.

EURASIA GROUP (2020). *The digital Silk Road: expanding China's Digital footprint.*

EUROPEAN COMMISSION (EC). (2020). *White Paper on Artificial Intelligence: a European approach to excellence and trust, COM(2020) 65 final.* Retrieved from https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

EUROPEAN COMMISSION (EC). (2021). *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final.* Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

EU HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (AI HLEG). (2018). *A definition of AI: Main capabilities and scientific disciplines.*

EU HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (AI HLEG). (2019). *Ethics guidelines for trustworthy AI.* Retrieved from https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf

EU HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (AI HLEG). (2020). *Assessment list for trustworthy artificial intelligence (ALTAI) for self-assessment.*

EUROPEAN PARLIAMENT (EP). (2016). *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679 &from=EN

EUROPEAN PARLIAMENT (EP). (2018). *Resolution of 12 September 2018 on autonomous weapon systems* (2018/2752(RSP)). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018IP0341&from=EN

EUROPEAN PARLIAMENT (EP). (2021a). *The External Policy Dimensions of AI.* Special Committee on Artificial Intelligence in a Digital Age (AIDA).

EUROPEAN PARLIAMENT (EP). (2021b). *Artificial intelligence: questions of interpretation and application of international law. European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)).* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0009

EUROPEAN PARLIAMENT (EP). (2021b). *Regulation 2021/821 of the European Parliament and the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), (Export Control Regulation).* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:206:FULL&from=EN

FELDSTEIN, S. (2019). *The global expansion of AI surveillance.* Carnegie Endowment for International Peace.

FELDSTEIN, S. (2020). *Testimony before the U.S.-China economic and security review commission hearing on China's strategic aims in Africa* [Conference presentation]. Online. Retrieved from https://www.uscc.gov/hearings/chinas-strategic-aims-africa

FREY, C. B., & OSBORNE, M. (2020, June 19). China won't win the race for AI dominance. *Foreign Affairs.*

GROSS, J. A. (2021). Amid fallout from NSO scandal, Israel imposes new restrictions on cyber exports. *Times of Israel.* Retrieved from https://www.timesofisrael.com/amid-fallout-from-nso-scandal-israel-imposes-new-restrictions-on-cyber-exports/

HASHEMITE KINGDOM OF JORDAN (2020). *Jordan Artificial Intelligence Strategy (unofficial translation).*

HENIG, D. (2021, September 9). Will Brussels ruin the Brussels Effect? *Borderlex Perspectives.*

INTERNATIONAL DEVELOPMENT RESEARCH CENTER (IDRC). (2020). *Government AI Readiness Index 2020.* Retrieved from https://mcit.gov.eg/Upcont/Documents/Reports%20and%20Documents_18112020000_Government_AI_Readiness_Index_2020_Report.pdf

ISRAEL INNOVATION AUTHORITY (2020). *Bolstering Artificial Intelligence.* Retrieved from https://innovationisrael.org.il/en/reportchapter/bolstering-artificial-intelligence-0#footnoteref2_bscx727

RIGHI, R., LOPEZ COBO, M., SAMOILI, S., CARDONA, M., VAZQUEZ-PRADA BAILLET, M., & DE PRATO, G. (2021). *EU in the global Artificial Intelligence landscape.* European Commission. Retrieved from https://publications.jrc.ec.europa.eu/repository/handle/JRC125613

KAYE, D., & SCHAAKE, M. (2021. July 19). Global spyware such as Pegasus is a threat to democracy. Here's how to stop it. *The Washington Post.*

KINGDOM OF SAUDI ARABIA, SAUDI DATA AND AI AUTHORITY (2020). *National Strategy for Data and AI: Realizing Our Best Tomorrow – Strategy Narrative, 2020.*

KURLANTZICK, J. (2020, December 17). China's digital Silk Road initiative: A boon for developing countries or a danger to freedom? *The Diplomat.*

LEBANESE MINISTRY OF INDUSTRY (2019). *National Artificial Intelligence Strategy in Lebanese Industry, 2020-2025.*

MATTHEWS, D. (2021, October 5). US-EU agreement on artificial intelligence seen as a swipe at China – but little else for now. *Science Business.*

MEJRI, K. (2020). Maghreb: *Mapping de l'ecosysteme de l'intelligence artificielle,* UNESCO. Retrieved from https://fr.unesco.org/sites/default/files/20210526mappingecosystemeiadsmaghreb.pdf

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). (2020). *OECD Principles on Artificial Intelligence*. Retrieved from https://oecd.ai/en/ai-principles

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). (2021a). State of implementation of the OECD AI principles: Insights from national AI policies. Retrieved from https://www.oecd-ilibrary.org/docserver/1cd40c44-en.pdf?expires=1643038607&id=id&accname=guest&checksum=7508270B0055406674748255B1212274

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). (2021b). *Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.* Retrieved from https://mcit.gov.eg/Upcont/Documents/Reports%20and%20 Documents_2692021000_Recommendation_of_OECD_Council_on_AI_26092021.pdf

PAWLAK, P., ABDEL-SADEK, A., DOMINIONI, S., & LABAN, A. M. Y. (2021). Great Expectations: Defining a trans-Mediterranean cybersecurity agenda. *EuroMeSCo Policy Study No. 22.* European Institute of the Mediterranean. Retrieved from https://www.euromesco.net/publication/great-expectations-defining-a-trans-mediterranean-cybersecurity-agenda/

QATARI MINISTRY OF TRANSPORT AND COMMUNICATIONS (2019). *National Artificial Intelligence Strategy for Qatar, 2019.*

QIANG, X. (2021). Chinese digital authoritarianism and its global impact. *POMEPS Studies 43.*

SCHARRE, P. (2019): Killer apps: The real dangers of an AI arms race. *Foreign Affairs.*

SHAHEED, A., & GREENACRE, B. (2021). Binary threat: How Governments' Cyber Laws and Practice Undermine Human Rights in the MENA Region. *POMEPS Studies 43.*

SHIRES, J. (2021). The implementation of digital surveillance infrastructures in the Gulf. *POMEPS Studies 43.*

SMART DUBAI (2020). *Artificial Intelligence Ethics Principles & Guidelines.* Retrieved from https://www.digitaldubai.ae/initiatives/ai-principles-ethics

STANFORD UNIVERSITY (2021). *Artificial Intelligence Index Report 2021*. Retrieved from https://aiindex.stanford.edu/wp-content/uploads/2021/11/2021-AI-Index-Report_Master.pdf

SUBCOMMITTEE OF THE ISRAELI NATIONAL INTELLIGENT SYSTEMS PROJECT ON ARTIFICIAL INTELLIGENCE ETHICS & REGULATION (NISIS Subcommittee). (2019). *Report to the Prime Minister.*

TURKISH MINISTRY OF INDUSTRY AND TECHNOLOGY (2021). *National Artificial Intelligence Strategy 2021-2025.*

VINCI, A. (2020, August 31). The coming revolution in intelligence affairs. How Artificial Intelligence and autonomous systems will transform espionage. *Foreign Affairs*.

WORLD JUSTICE PROJECT (WJP). (2021). Rule of Law Index 2021. Retrieved from https://worldjusticeproject.org/sites/default/files/documents/WJP-INDEX-21.pdf

WRIGHT, N. (2018, July 10). How Artificial Intelligence will reshape the global order, Foreign Affairs.

ZIV, A. (2021, July 18). The Pegasus project: How Israeli Spy-tech became dictators' weapon of choice. *Haaretz.*

List of acronyms and abbreviations

ABC	Automated Border Crossings
AI	Artificial Intelligence
BRI	Belt and Road Initiative
CAHAI	Ad Hoc Committee on Artificial Intelligence at the Council of Europe
CAPTCHA	Completely Automated Public Touring test to tell Computers and Humans Apart
CCTV	Closed Circuit Television
CoE	Council of Europe
DPI	Deep Packet Inspection
ECR	Export Control Regulation
EDA	European Defence Agency
EDF	European Defence Fund
EDIDP	European Defence Industrial Development Programme
EDT	Emerging Disruptive Technologies
EC	European Commission
EP	European Parliament
EU	European Union
EU-27	The European Union of 27 Member States
GCC	Gulf Cooperation Council
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GPAI	Global Partnership on Artificial Intelligence
G20	Group of Twenty
HIV/AIDS	Human Immunodeficiency Virus / Acquired Immunodeficiency Syndrome
HLEG	High-Level Expert Group
ICT	Information and Communications Technology
IDC	International Data Corporation
IDF	Israeli Defence Force
INTERPOL	International Criminal Police Organization
IP	Internet Protocol
ISP	Internet Service Provider
JRC	Joint Research Centre
LAWS	Lethal Autonomous Weapons Systems
LGBTQ+	Lesbian, Gay, Bisexual, Transgender, Queer/Questioning
MENA	Middle East and North Africa
NATO	North Atlantic Treaty Organization
OECD	Organisation for Economic Co-operation and Development
OODA	Observe-Orient-Decide-Act
R&D	Research and Development
STEM	Science, technology, engineering and mathematics
TTC	EU-US Trade and Technology Council
UAE	United Arab Emirates
UK	United Kingdom
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNOCT	United Nations Office of Counter-Terrorism

UNSC	United Nations Security Council
US	United States
USA	United States of America
WG	Working group
5G	5th generation telecommunications networks

euromesco
Policy Study

IEMed.
European Institute of the Mediterranean

Co-funded by
the European Union