

PANTEION UNIVERSITY

**European Master's Programme in Human Rights and
Democratisation
A.Y. 2025/2026**

Profiles of Dependence in Defense AI: Strategic Autonomy and Human Rights in Israel and the United Arab Emirates

Author: Claire Basbous
Supervisor: Dr. Maria Daniella Marouda

Word Count Declaration: 28909

Abstract

Artificial Intelligence (AI) is a rapidly developing technology especially in the field of defense. And while some countries develop it domestically, others rely on external procurement to obtain it. However, even with domestic production, reliance on different parties whether foreign governments or private firms still exists across the supply chain. Knowing this, this thesis aims to understand why some countries manage to reduce their dependence and produce their defense AI locally while others are unable to. It also aims to understand how the varying levels of dependence differently affect state autonomy, security decision making, and human rights.

To answer these questions, the thesis compares the United Arab Emirates (UAE) and Israel's AI production mechanisms, and relies on four theoretical frameworks, of which an extended version of dependency theory forms the central structure. This theory is complemented by technological sovereignty, Morgenthau's elements of national power, and international humanitarian and human rights law. These frameworks work together, and are adapted when needed to incorporate the modern dynamics brought by AI and the emergence of private companies as players in the field of defense.

The research found that the conditions that determine where a state ends up on the dependence axis are historical, economic, political, and also institutional. These elements interact together and produce unique profiles for each country. The findings confirmed also that full autonomous production is not an attainable goal in the foreseeable future, and that states have shifted toward managing and reducing dependence rather than eliminating it. For Israel, the findings show that the country is dependent in specific areas across its supply chain but in a measurable way that makes it easier to address in the future, unlike the UAE which is reliant on procurement and unequal partnerships pushing itself further into dependence. Findings also show that local production can strengthen a state's autonomy, particularly in security decision-making, and can increase a state's strategic power rather than its operational capability contrary to a procurement heavy model. Local production can also create better conditions for protecting human rights, but in a less straightforward way, as this depends heavily on the political context since the same production capacity can either protect or threaten human rights depending on who controls it.

Contents

List of Abbreviations.....	5
Introduction.....	6
Chapter 1: Military AI and the Global Structure of Power and Dependence	11
1.1 Military AI as a State Asset: How Technology Reshapes Power.....	11
1.2 Amplifier of Vulnerability: How Military AI affects State Power and Human Rights	13
1.3 The Hierarchy of Military AI Capability: Where Production Is Concentrated and How Most States Depend on Others	16
1.4 Infrastructure, Data, and Political Conditionality: A Framework for How Military AI Dependence Threatens Sovereignty and Human Rights.....	19
Chapter 2: The Roots of Reliance: Conditions That Create and Sustain Military AI Dependence	25
2.1 Colonial Legacies and Economic Foundations: Why Historical Conditions Still Determine Who Can Build Military AI	26
2.2 Threat Environments, Alliance Structures, and Export Controls: How Political Conditions Lock States Into or Out of Military AI Independence.....	27
2.3 Beyond Investment: Why Innovation Ecosystems and Civil-Military Collaboration Determine Whether Spending Produces Sovereignty or Procurement	30
2.4 Private Firms as Structural Actors: Strategic and Human Rights Risks	33
Chapter 3: Built to Fight: Israel's Military AI Ecosystem, Supply Chain Vulnerabilities, and Human Rights Record	36
3.1 From Survival Imperative to Global Exporter: How Israel Built Its Military AI Ecosystem Through Security Pressure, R&D, and Civil-Military Relations.....	36
3.2 Strong but Not Sovereign: Where Israel's Military AI Capability Ends and Its Supply Chain Vulnerabilities Begin	39
3.3 Does Production Translate Into Power? Applying Morgenthau's Elements to Israel's Military AI Position.....	43
3.4 Production Without Accountability: How Israel's Domestic AI Systems Created the Conditions for Accountability While Political Choice Blocked It.....	47
Chapter 4: The UAE's AI Ambitions and the Depth of Its Dependencies	53

4.1 Wealth, Vision, and the Procurement Path: How the UAE Assembled Its Military AI Position Without Building Domestic Depth	53
4.2 Rich but Not Independent: Where UAE Investment Ends and Structural Dependence Begins	55
4.3 Does Procurement Translate into Power? Applying Morgenthau's Elements to the UAE's Military AI Position.....	60
4.4 Procurement Without Recourse: How the UAE's Foreign AI Dependence Enables Repression and Forecloses Accountability	63
Chapter 5: Different Paths, Shared Constraints: Comparing Israel and the UAE as Distinct Profiles of Military AI Dependence	66
5.1 History, Depth, and Time: Why Institutional Conditions, Not Resources, Explain the Gap Between Israeli and Emirati Military AI	66
5.2 Procurement and Production: Tools To Manage Dependence	70
5.3 Strategic Autonomy and Security Decision-Making Under Constraint: How Dependence Reshapes What States Can Actually Choose	72
5.4 Different Systems, Different Accountability Architectures: How the Form of Military AI Dependence Shapes Human Rights Risks and the Possibility of Remedy	76
Conclusion	81
Bibliography.....	84

List of Abbreviations

Artificial Intelligence	AI
United Arab Emirates	UAE
United States of America	U.S.
International Humanitarian Law	IHL
International Human Rights Law	IHRL
Natural Language Processing	NLP
Stockholm International Peace Research Institute	SIPRI
International Court of Justice	ICJ
International Covenant on Civil and Political Rights	ICCPR
United Nations Development Program	UNDP
European Union	EU
United Kingdom	UK
Lethal Autonomous Weapons	LAWS
Global Positioning System	GPS
Amazon Web Services	AWS
United States Dollar	USD
U.S. Defense Advanced Research Projects Agency	DARPA
Research and Development	R&D
Total Factor Productivity	TFP
Science, Technology, and Innovation	STI
National Absorptive Capacity	NAC
Realized National Absorptive Capacity	RNAC
Potential National Absorptive Capacity	PNAC
Gross Domestic Product	GDP
Organization for Economic Co-operation and Development	OECD
Israel Defence Forces	IDF
Taiwan Semiconductor Manufacturing Company Limited	TSMC
Memorandum of Understanding	MOU
Terminal High Altitude Area Defence anti-missile system	THAAD anti-missile system
Military Advocate General's Corps	MAG Corps
Military Police Criminal Investigation Division	MPCID
Action on Armed Violence	AOAV
Non-governmental Organization	NGO
United Nations	UN
Mohamed bin Zayed University of Artificial Intelligence	MBZUAI
Chief Executive Officer	CEO
Research in Motion	RIM
U.S. intelligence agency	NSA
International Committee of the Red Cross	ICRC

Introduction

Many countries today can innovate, and create new technologies, but not all of them are able to do so while preserving their full autonomy. As Artificial Intelligence (AI) becomes central to contemporary defense capabilities, questions of who can build and operate these systems are becoming urgent strategic and human rights concerns.

The United States (U.S.) is ranked as having the strongest military in the world, with a defense budget of approximately USD 895 billion, seconded by China at approximately USD 266 billion,¹ which is less than one-third of the U.S.'s budget. On the other hand, India is ranked fourth and Saudi Arabia is ranked fifth with substantial defense budgets,² but unlike the U.S. and China, both have not become major producers of military AI. Meanwhile Israel, with a comparatively smaller budget, widely produces and sells defensive AI innovations.

The previous data shows a fragmented scene, signaling that military spending alone cannot explain variation in defense AI production, and raises questions about the elements that determine production capacity. States that are unable to autonomously develop their technological capability must now depend on foreign governments and private technology firms to boost their defenses. This kind of reliance is introducing new types of risk that this research will explore by focusing on two states, Israel and the United Arab Emirates (UAE).

These two countries were chosen for analysis because they share very important characteristics, while also adopting different approaches to build defense AI capabilities. Both Israel and the UAE are small to mid-sized powers sitting in the Middle East region. Both face the same core threat from Iran and its militias in the region. Both consider AI investment as a priority and aim to be technology leaders. And both deal with opacity when it comes to their human rights systems. But what makes the comparison analytically richer is that these countries differ from each other in terms of how they aim to reach their military AI goals. Israel built its capabilities from the inside out, investing in its own citizen pool and building a strong civil military relation, whereas the UAE

¹ Alexander, "Defense Budget by Country 2026: Global Rankings and Insights", *Military Compare*, February 28, 2026, <https://militarycompare.com/defense-budget-by-country-2025/>, accessed 6 March 2026.

² Ibid.

built its capabilities from the outside in, importing infrastructure and partnering with foreign firms, while bringing in talent it did not have at home.

During the recent war in the Middle East, Israel deployed its AI targeting systems at operational scale for the first time in combat. This deployment raised serious questions about these systems' ability to protect the country independently and about the extent to which they can comply with principles of accountability and human rights. For the UAE, the effects of the same wave of conflict became evident when Iran threatened and hit Amazon Web Services (AWS) data centers on UAE soil, disrupting cloud services across the country³ and leaving it to endure attacks in a war it did not choose.⁴

These two cases will be used to demonstrate that production and procurement have become strategies to manage dependence and not to escape it, and to show that dependence on foreign technology can amplify vulnerabilities, and complicate the road to justice, especially if the government using these systems is known for human rights abuses. Instead of treating Israel as a self-sufficient state, this research will analyse whether it is truly independent across its full supply chain, while also analyzing the full dependency profile of the UAE. The research will also examine how the different forms of AI reliance affect autonomy, security decision making, and human rights outcomes of both states.

Research has examined AI and its positive and negative impacts on national and international security and human rights. Existing studies have analyzed how AI affects international stability by increasing escalation risks and the fear of automation bias, especially in strategic domains.⁵ They also have covered how AI can blur the boundaries between civil military relations and reinforce a

³ Kai Nicol-Schwarz and Emma Graham, "Banking, Payments Services Disrupted After Amazon UAE Data Centers Hit in Drone Strikes," *CNBC*, March 3, 2026, <https://www.cnn.com/2026/03/03/iran-war-uae-drone-strikes-aws-data-centers.html>, accessed 21 March 2026.

⁴ Sahim Salim, "Not party to this war': UAE position on Iranian attacks explained in 9 points", *Khaleej Times*, March 4, 2026, 1:27 p.m., <https://www.khaleejtimes.com/uae/iran-attacks-uae-not-part-of-war-calls-for-dialogue-position-explained-in-9-points>, accessed 21 April 2026

⁵ Vincent Boulanin, Lora Saalman, Petr Topychkanov, Fei Su, and Moa Peldán Carlsson, *Artificial Intelligence, Strategic Stability and Nuclear Risk*, (Stockholm: Stockholm International Peace Research Institute, June 2020), https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf, accessed 29 March 2026.

traditional realist understanding of politics on the international level.⁶ Research in International relations has explored how AI can reshape security policies, and change the balance of power on the international scene through autonomous systems.⁷ Scholars have also studied legal implications of AI, from concerns regarding accountability to compliance with current legal frameworks such as with the Law of War. Human rights have also attracted a lot of research, especially in terms of predictive surveillance, and use of AI by authoritarian regimes.⁸ Moreover, most of the available work focuses on Global North versus Global South trends, and the imbalance between the two parties in technological capability.⁹

After reviewing this literature, three gaps stand out as particularly underexamined. The first is that existing research tends to focus either on the rivalry between great powers or on the unbalanced relationship between the Global North and the Global South. This leaves very little analysis of resource rich middle powers that despite their capabilities, face their own specific and understudied forms of technological dependence. The second gap is that even when scholars do assess the positive and negative implications of AI in international relations, they rarely treat technological dependence itself as a concept that shapes autonomy and human rights, overlooking that these elements interact deeply with each other. The third gap is that the growing role of private

⁶ Opeoluwa Adisa Oluyemi, “The Military Uses of Artificial Intelligence (AI) and Their Implications on International Security”, *International Journal of Research and Innovation in Social Science* 8, no. 3S (2024): 1084–1098, June 7, 2024, <https://dx.doi.org/10.47772/IJRISS.2024.803075S>, accessed 29 March 2026

⁷ Shahid Iqbal, Syed Wajeeh Abbas Rizvi, Muhammad Hasnain Haider Malik, and Saqib Raza, “Artificial Intelligence in Security and Defense: Explore the Integration of AI in Military Strategies, Security Policies, and Its Implications for Global Power Dynamics”, *International Journal of Human and Society*, 3, no. 4 (2023): 341–353, https://www.researchgate.net/profile/Hasnain-Haider-13/publication/377177943_Artificial_Intelligence_in_Security_and_Defense_Explore_the_integration_of_AI_in_military_strategies_security_policies_and_its_implications_for_global_power_dynamics/links/659829ce6f6e450f19ce3a28/Artificial-Intelligence-in-Security-and-Defense-Explore-the-integration-of-AI-in-military-strategies-security-policies-and-its-implications-for-global-power-dynamics.pdf, accessed 28 March 2026.

⁸ H. Akin Ünver, *Artificial Intelligence (AI) and Human Rights: Using AI as a Weapon of Repression and Its Impact on Human Rights* (Brussels: European Parliament, Directorate-General for External Policies, 2024), PE 754.450, https://www.researchgate.net/profile/Hamid-Akin-Uenver/publication/381407889_Artificial_Intelligence_AI_and_Human_Rights_Using_AI_as_a_Weapon_of_Repression_and_Its_Impact_on_Human_Rights/links/666c033a85a4ee7261c1187d/Artificial-Intelligence-AI-and-Human-Rights-Using-AI-as-a-Weapon-of-Repression-and-Its-Impact-on-Human-Rights.pdf, accessed 27 March 2026.

⁹ Sherifdeen Folaranmi Abiade, “Algorithmic Sovereignty and New Security Dependencies: How Foreign AI Surveillance Technologies Reshape Domestic Autonomy in the Global South”, *World Journal of Advanced Research and Reviews* 27, no. 2 (2025): 162–180, <https://doi.org/10.30574/wjarr.2025.27.2.2845>, accessed 30 March 2026.

technology companies as the main providers of military and surveillance AI has not been seriously examined, even as their influence in production and after deployment continues to grow.

To address these gaps, the study aims to answer the following main question:

Why do states develop different forms of reliance on military and surveillance AI, and how do these dependence profiles shape autonomy, security decision making, and human rights outcomes?

To unpack this, the following sub-questions will be analyzed:

1. What factors explain why some states develop domestic military and surveillance AI ecosystems while others remain reliant on foreign suppliers across critical layers of the AI supply chain, and how do production and procurement strategies shape dependence?
2. How do Israel and the UAE illustrate different strategies for managing military AI dependence, and to what extent can local production reduce dependence?
3. How do the varying levels of dependence in the field of military AI influence state autonomy, security decision-making, and human rights?

To answer these questions, the thesis draws on four theoretical frameworks, of which an extended version of dependency theory provides the structural foundation of the analysis. Originally, dependency theory aimed to explain why some countries grow richer, while others remain stuck in underdevelopment.¹⁰ For our research, the theory is extended to examine small to mid-sized powers and not the peripheral and core countries identified in the original theory, in addition to state to firm dynamics and the element of AI that did not exist when the theory was first developed. To better understand what managing dependence well actually looks like for our case studies, the technological sovereignty framework will be deployed as it acts as a benchmark for state capacity to independently develop and make decisions about its technologies. Because states reach

¹⁰ Ingrid Harvold Kvangraven, “Dependency Theory: Strengths, Weaknesses, and Its Relevance Today”, in *A Modern Guide to Uneven Economic Development*, January 2023, https://www.researchgate.net/publication/367336288_Dependency_theory_strengths_weaknesses_and_its_relevance_today, accessed 23 June 2026.

technological sovereignty through different dependence profiles, Morgenthau's elements of national power act as our third framework to analyze the effects of these profiles on power and strategic independence. Finally, and to address how these different profiles affect human rights, a legal framework is deployed, drawing from International Humanitarian Law (IHL) and International Human Rights Law (IHRL). This framework is supplemented by the human security perspective, shifting the question from whether states are secure to whether their own people are,¹¹ and by the Ruggie framework to tackle the relationship between private firms and human rights.¹²

The thesis will use the comparative qualitative research methodology, with Israel and the UAE as case studies. The research will draw on open source materials including scholarly work, official reports, as well as investigative journalism articles. Investigative reports particularly those published by +972 Magazine and Local Call, are used because they provide access to operational information that is otherwise unavailable to the public. The findings of these articles are not treated as conclusive on their own, but are evaluated alongside other available evidence and the broader academic literature.

The defense sector is known to have confidential information by nature, and this is especially true for governments with documented human rights abuses. This is a limitation for our research, alongside the fact that there is not the same amount of publicly available evidence for both of our case studies, as Israel's conduct has been way more documented than the UAE's. To overcome this, the research acknowledges these gaps, and does not make claims beyond what the evidence supports. Where direct evidence is not available, the analysis relies on the theoretical framework developed in this thesis, together with findings from the scientific research on security studies to discuss potential effects. Research also clearly differentiates between observed evidence and arguments supported by theory.

¹¹ United Nations Development Programme, *Human Development Report 1994: New Dimensions of Human Security* (New York, 1994), <https://hdr.undp.org/content/human-development-report-1994>, 17 May 2026

¹² John Gerard Ruggie, *Protect, Respect and Remedy: A Framework for Business and Human Rights: Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises*, A/HRC/8/5 (Geneva: United Nations, April 7, 2008), United Nations Digital Library, <https://digitallibrary.un.org/record/625292?v=pdf>, accessed 30 June 2026.

By answering the main question of our thesis, we aim to contribute to the understanding of technological dependence outside of the traditional north versus south framing, showing that dependence is not simply something a state either has or does not have, but a profile that is shaped by history, institutions, and political conditions that look very different from one case to the next.

Chapter 1: Military AI and the Global Structure of Power and Dependence

1.1 Military AI as a State Asset: How Technology Reshapes Power.

AI refers to computer systems that are capable of performing human intellectual functions, for example learning from experience and also making decisions.¹³ In the defense sector, AI is turned from fulfilling civilian purposes to fulfilling military objectives, and is used in different systems that operate through processing large datasets, producing outputs and recommendations more quickly than humans.¹⁴ To reach this point, a process called machine learning is implemented, where algorithms learn to perform tasks by identifying patterns in large datasets¹⁵ until the system can reliably predict or classify new inputs.

Leading military powers around the world are incorporating AI into their processes, ranging from systems used for surveillance to active operations. Before, armies used to rely on large numbers of humans for data analysis, risking long delays and errors due to fatigue,¹⁶ but with the introduction of AI, the system responsible for transmitting the data can now complete the analysis with unmatched speed and enhanced accuracy. For example, surveillance drones that were tasked with transmitting images for intelligence officers to look into, are now equipped with advanced

¹³ NASA, “Defining Artificial Intelligence”, <https://www.nasa.gov/what-is-artificial-intelligence/>, accessed 21 March 2026.

¹⁴ Graeme Manzi, “Revolutionising Defence Intelligence, Surveillance & Reconnaissance (ISR) with AI”, *Karve International*, February 13, 2024, <https://www.karveinternational.com/insights/revolutionising-defence-intelligence-surveillance-reconnaissance-isr-with-ai>, accessed 21 March 2026.

¹⁵ Dave Bergmann, “What is machine learning?”, *IBM*, <https://www.ibm.com/think/topics/machine-learning>, accessed 21 March 2026.

¹⁶ “How AI Is Enhancing Military Surveillance and Border Security”, *Defence Industries*, <https://www.defence-industries.com/articles/how-ai-is-enhancing-military>, accessed April 2, 2026

systems allowing them to evaluate suspicious movements and faces, eliminating the need for long hours of analysis, and reducing human errors.¹⁷

Throughout history, states that mastered transformative technologies such as gunpowder and nuclear weapons, gained decisive strategic advantages over those that did not. For this reason, AI technologies today are being viewed by states as indispensable tools for strategic advantage. AI is different from previous military technological revolutions as its advantages go beyond destructive potential, and act as an amplifier of nearly every dimension of state power from intelligence processing and logistics, to targeting and strategic planning.

Considering its strategic benefits, AI is being used to protect countries against cyberattacks by identifying potential threats and neutralizing them in the timespan of milliseconds.¹⁸ AI is also used to anticipate mechanical faults and is being incorporated into aircraft, tanks, and in the form of AI sensors that are able to predict faults and mechanical failures before they happen, reducing downtime and sudden failure in battle.¹⁹

More importantly, AI can now act as a second mind that can analyze complex data from different locations and systems, coming up with clear outputs that can assist human commanders before deciding on a strike.²⁰ This analysis process relies on several systems including Natural Language Processing (NLP) systems such as ChatGPT (version adapted for military use) to scan intercepted conversations in multiple languages and identify certain phrases that can cause suspicion.²¹

Being such an important asset, great powers are competing to integrate AI into their military systems, and advance their positions in the field. China unveiled a five year plan from 2026 till 2030 to expand its AI adoption and position itself as an AI pioneer,²² while the United States

¹⁷ Ibid

¹⁸ Science News Today Editorial Team, “15 Most Incredible Uses of AI in Military Technology,” *Science News Today*, October 9, 2025, <https://www.sciencenewstoday.org/15-most-incredible-uses-of-ai-in-military-technology/>, accessed 4 April 2026.

¹⁹ Ibid

²⁰ Ibid

²¹ Ibid

²² Micheal Caster, “The Global Implications of China’s 5-Year Plan AI Ambitions”, *The Diplomat*, March 27, 2026, <https://thediplomat.com/2026/03/the-global-implications-of-chinas-5-year-plan-ai-ambitions/>, accessed 6 April 2026.

committed to its "Third Offset" Strategy, investing heavily in AI and robotics to sustain its defense advantage.²³ Middle powers are also joining the race and intensively investing to build autonomy in the field.²⁴ Considering this, the strategic logic becomes clear; states that can produce AI will gain an unmatched advantage and speed that without it sovereignty and power will face grave dangers.

1.2 Amplifier of Vulnerability: How Military AI affects State Power and Human Rights

Despite all the benefits, AI does not automatically translate into power, as it can also generate vulnerabilities. These vulnerabilities are divided into risks related to AI itself, and risks related to dependence on foreign actors to acquire and operate the AI systems. This distinction is important for our research, because while all countries face the technological risks associated with AI, dependent states face an amplified layer caused by their reliance on foreign actors.

Regarding inherent limitations, AI used for surveillance and targeting does not always behave the way their developers expect them to. These systems, and same as regular AI and chatbots, can make mistakes and inherit biases from their training data.²⁵ For example, if minority groups have been historically falsely labeled as dangerous, the AI can reflect that pattern, if the data used for its learning was biased.²⁶ Once bias is embedded in AI, it starts to amplify itself through the algorithmic procedure, unlike humans who can reassess their own judgments, replicating the same pattern millions of times without adjustment.²⁷

²³ Lisa A. Aronsson, *What Next for the Third Offset Strategy?*, CRS In Focus IF10790 (Washington, DC: Congressional Research Service, December 13, 2017), <https://www.congress.gov/crs-product/IF10790>, accessed 6 April 2026.

²⁴ Boston Consulting Group, "Geopolitics and Generative AI: Will Middle Powers Reshape the Map?", press release, December 9, 2024, <https://www.bcg.com/press/9december2024-geopolitics-genai-middle-powers-reshape-map>, accessed 6 April 2026.

²⁵ Grace Chang and Heidi Grant, "When AI Amplifies the Biases of Its Users", *Harvard Business Review*, January 23, 2026, <https://hbr.org/2026/01/when-ai-amplifies-the-biases-of-its-users>, accessed 14 March 2026.

²⁶ Ibid, 7

²⁷ Alexandra Jonker and Julie Rogers, "What Is Algorithmic Bias?", *IBM*, <https://www.ibm.com/think/topics/algorithmic-bias>, accessed 16 April 2026

Moreover, AI can cause what is known as “algorithmically manufactured suspicion”, that happens when an AI system takes several signals, none of which would count as evidence of a threat on their own, and combines them into a high confidence hostile designation, causing risk of wrongful targeting especially in terms of communities that are already associated with hostility in the training data.²⁸ The use of prepaid phones, the density of family networks, patterns of border crossing, communal male gatherings, or carrying tools that resemble weapons, each of these indicators on its own is not enough to flag someone as a threat, but when these signals are fed into a system that was already trained on data associating these communities with hostility, the algorithm combines them into a profile, and that profile becomes a target.

Biased datasets can also cause AI systems to undercount civilian presence and undervalue civilian objects.²⁹ When military commanders are required to strike certain locations, they have to abide by the customary IHL principles of distinction³⁰ and proportionality,³¹ to make sure civilians are protected, and that a good faith assessment of expected civilian harm have been done and weighed against anticipated military advantage. If the gain is greater than the loss of civilian lives and objects, a strike order is issued. When AI becomes biased, commanders end up doing their calculations on numbers that the system got wrong.³² This shows that the problem is not only that AI may misidentify targets, but that it can distort the math on which proportionality assessments depend.

Norms of IHRL remain applicable during armed conflict, as this was confirmed by the International Court of Justice (ICJ) in two of its advisory opinions, the first on Nuclear Weapons in 1996,³³ and the second on the construction of a Wall in the Occupied Palestinian Territory in

²⁸ Laura Bruun and Marta Bo, *Bias In Military Artificial Intelligence and Compliance With International Humanitarian Law*, (Stockholm International Peace Research Institute, August 2025), 12, https://www.sipri.org/sites/default/files/2025-08/0825_ai_military_bias.pdf, accessed 30 April 2026.

²⁹ Ibid, 8-23

³⁰ International Committee of the Red Cross (ICRC), “Rule 1: The Principle of Distinction between Civilians and Combatants”, International Humanitarian Law Database, <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule1>, accessed 1 May 2026

³¹ ICRC, “Rule 14: Proportionality in Attack”, International Humanitarian Law Database, <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule14>, accessed 3 June 2026.

³² Bruun and Bo, *Bias in Military Artificial Intelligence...*, 16

³³ International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, *Advisory Opinion of 8 July 1996*, I.C.J. Reports 1996, <https://www.icj-cij.org/node/103787>, accessed 24 April 2026.

2004.³⁴ One of the applicable IHRL norms is the right to life under Article 6 of the International Covenant on Civil and Political Rights (ICCPR),³⁵ and is challenged when a military AI system flags individuals as threats due to biased data leading to an arbitrary loss of life. Another norm is the principle of non-discrimination under Articles 2 and 26 of the same Covenant,³⁶ and is challenged when a system trained on historically discriminatory data reproduces that discrimination regardless of the designer's intent.

IHL is also used to verify war crimes and hold the right people accountable, but with AI entering the field of weapons, a new layer of complexity has been added to the identification of perpetrators, as everyone involved has now the possibility to point the finger elsewhere. A producing company can say the military used the system incorrectly, and the military can say that the company did not disclose all necessary information or did not do proper testing. Moreover, and because many AI systems operate in ways that even their creators cannot fully explain, it is often impossible to know the truth of what actually happened, leading to not only problems in accountability but also to a risk of not wanting to fix the issue to avoid being held responsible in the long run.

Operational risks follow naturally from this, as commercial AI is built and tested in controlled environments and not in the chaos of a battlefield. During war, the AI can behave very differently especially if the enemy is actively trying to confuse it, or when the situation changes faster than the system can adapt, or even for reasons no one can actually explain, even the makers.³⁷ In today's world no clear guidelines exist to what is considered safe and acceptable when it comes to AI in weapons, as the threshold of what is considered acceptable and ready for operations might greatly differ between armies.

³⁴ International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, I.C.J. Reports 2004, <https://www.icj-cij.org/case/131>, accessed 25 April 2026.

³⁵ United Nations, *International Covenant on Civil and Political Rights*, December 16, 1966, Art. 6, Office of the High Commissioner for Human Rights (OHCHR), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>, accessed 25 April 2026.

³⁶ Ibid, articles 2 and 26

³⁷ "How military AI systems can be attacked and misled", *Swedish Defense Research Institute*, August 22, 2023, <https://www.foi.se/en/foi/news-and-pressroom/news/2023-08-22-how-military-ai-systems-can-be-attacked-and-misled.html>, accessed 15 March 2026.

For states that depend on foreign suppliers, the vulnerabilities go beyond the technical and legal aspects shown above, reaching sovereignty, autonomy, and new dimensions of human rights. A dependent state faces the risk that a supplier withdraws access to systems it produced under political pressure, or even impose conditions on how the technology may be used. Importantly, these risks are not all the same for all countries, as a state that depends on foreign suppliers for its core targeting infrastructure, faces a different order of vulnerability than a state that depends on foreign cloud services for logistics support. These failures are not solely technical in nature, as they can arise from political and structural weaknesses created by dependence, and we will review them in the upcoming sections.

The dynamics discussed above explain why AI shapes power and vulnerabilities simultaneously. What follows will build on this, to show that the risks these technologies create are not distributed equally for all countries, but vary according to each country's position on the axis of dependence.

1.3 The Hierarchy of Military AI Capability: Where Production Is Concentrated and How Most States Depend on Others

Defensive AI is mostly concentrated among a small group of states and private companies that possess the needed means to build and operate advanced AI systems, and this concentration is what determines which states remain the most dependent on external suppliers for critical military technologies. Importantly, the division between states is not strictly binary, as a country does not simply possess or lack military AI capability, but each state occupies a different position across the AI production spectrum, and their location within it shapes the strategic risks they face.

In terms of leaders in the field, the U.S. currently dominates the military AI landscape, supported by over USD 75 billion spent since 2016,³⁸ and an AI accelerating strategy to sustain America's global AI dominance and its national security.³⁹ All of the U.S.'s military command structures are

³⁸ Amos Toh and Emile Ayoub, "The Military's Use of AI, Explained," Brennan Center for Justice, March 12, 2026, <https://www.brennancenter.org/our-work/research-reports/militarys-use-ai-explained>, accessed 9 April 2026.

³⁹ US Department of War, Secretary of War, "Artificial Intelligence Strategy for the Department of War: Accelerating America's Military AI Dominance", memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, and Defense Agency and DOW Field Activity Directors, January 9, 2026,

now supported with an "AI first" approach, giving the country a strategic advantage that is currently unmatched.⁴⁰ China comes next through large scale state investment, and ambitious modernization plans.⁴¹ The Chinese government is encouraging military civil fusion by promoting close coordination between the state owned defense corporations and privately owned ones,⁴² aiming to close the gap with the U.S. and protect itself from the kind of technological pressure it knows Washington is capable of applying.

Below the leaders, the EU, the UK, and Israel, sit among the strongest producers in the field. After the war on Ukraine, the EU expanded its investment in AI-driven military technologies, while supporting innovation of private companies.⁴³ The latter is also taking on an ethical stance for production, and is calling for regulation and a prohibition on lethal autonomous weapons (LAWS).⁴⁴ The UK is working to strengthen its cooperation with the private sector to advance its military AI production,⁴⁵ and it developed a strategy for 2030 to improve its digital infrastructure, and enhance its AI skills base.⁴⁶ Israel, and despite it being a relatively new state, and a small size regional power, is playing a central role in military AI production, combining

<https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF>, accessed 9 April 2026.

⁴⁰ Ibid

⁴¹ Cole McFaul, Sam Bresnick, and Daniel Chou, "Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage", Center for Security and Emerging Technology, September 2025, <https://cset.georgetown.edu/publication/pulling-back-the-curtain-on-chinas-military-civil-fusion/>, accessed 9 April 2026.

⁴² Ibid

⁴³ Sebastian Clapp, *Defence and Artificial Intelligence*, European Parliamentary Research Service, PE 569.580 (April 2025), https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI%282025%29769580_EN.pdf, accessed 9 April 2026.

⁴⁴ Ibid

⁴⁵ UK Ministry of Defence and John Healey "New Strategic Partnership to Unlock Billions and Boost Military AI and Innovation", press release, 18 September 2025, <https://www.gov.uk/government/news/new-strategic-partnership-to-unlock-billions-and-boost-military-ai-and-innovation>, accessed 9 April 2026.

⁴⁶ British Army, *British Army's Approach to Artificial Intelligence*, October 2023, https://www.army.mod.uk/media/24745/20231001-british_army_approach_to_artificial_intelligence.pdf, accessed 9 April 2026.

strong military research with highly innovative private companies, producing defense tools that are widely exported.⁴⁷

Despite them being regional powerhouses, the mentioned players are restricted by their need to partner with global leaders. For example, European states rely heavily on U.S. companies for secure cloud infrastructures.⁴⁸ This illustrates that even states with strong industrial or financial capacities cannot easily achieve full independence across the entire AI supply chain.

In terms of middle capacity states, this group can adopt or partially develop military AI, but depends on foreign actors for essential components or infrastructures. This group includes countries like South Korea⁴⁹ and the UAE⁵⁰. Even when these states have large budgets and political motivation, they run into barriers like a shortage of specialized talent, and limited access to advanced semiconductors. Just like high capacity states, these countries depend on others, but for them getting out of that dependence is considerably harder.

The largest group of states belong to the category of fully dependent states, where governments cannot produce or sustain military AI systems. These states import technologies and their infrastructure from foreign suppliers, and depend on them for software updates and operational support. And since these states do not own the systems, do not control the data, and cannot audit how the technology works, they end up making security decisions inside a framework that someone else built and that someone else can take away.

Alongside state actors, private technology firms have emerged as strong players in the field of military AI. According to historical records, many important technological innovations started

⁴⁷ Elias Aravantinos, "The Fusion of Technology and Defense: Israel's Military-Technology Complex," *Strategy International*, 21 November 2024, <https://strategyinternational.org/2024/11/21/publication150/>, accessed 9 April 2026.

⁴⁸ Clotilde Bômout, *Technical Is Political: When a Cloud Certification Scheme Divides Europe* (Paris: European Union Institute for Security Studies, November 3, 2025), <https://www.iiss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe>, accessed 9 April 2026.

⁴⁹ Tobias Junerfält, *South Korea's Push for Defense Semiconductor Self-Sufficiency*, FOI Memo 8937 (Stockholm: Swedish Defence Research Agency, September 2025), <https://www.foi.se/rest-api/report/FOI%20Memo%208937>, accessed 12 April 2026.

⁵⁰ "The UAE's Technology Ambitions," *Strategic Comments* 30, no. 23 (International Institute for Strategic Studies, October 2024), <https://www.iiss.org/publications/strategic-comments/2024/10/the-uaes-technology-ambitions>, accessed 12 April 2026.

within military establishments before being developed and used by civilians such as the Internet.⁵¹ But with AI, the creation process happened in the civilian world and flourished there, showing that this milestone humanity reached needed strong innovation and creativity that cannot usually be found in military contexts. For this reason, we can see today that the defense sector is relentlessly partnering with private companies, introducing them as strong players in the field of defense. Companies such as Palantir,⁵² Microsoft,⁵³ and AWS,⁵⁴ in the U.S. are now among the primary developers and operators of military and surveillance AI systems. The role of these companies is not only restricted to producing defensive technologies, as in many cases, they are responsible for maintaining the AI systems that states depend on for core defense functions,⁵⁵ meaning that the relationship between a state and its military AI capability would be mediated by a commercial contract, rather than secured through sovereign ownership.

1.4 Infrastructure, Data, and Political Conditionality: A Framework for How Military AI Dependence Threatens Sovereignty and Human Rights

As previously mentioned, not all technological dependence is the same. This is why in this section, we will develop a framework of technological dependence that will guide the comparative analysis of Israel and the UAE in the chapters that follow.

⁵¹ John Naughton, “The Evolution of the Internet: From Military Experiment to General Purpose Technology,” *Journal of Cyber Policy*, 2016, 5–28, https://www.academia.edu/93607010/The_evolution_of_the_Internet_from_military_experiment_to_General_Purpose_Technology, accessed 5 March 2026

⁵² Microsoft, “Palantir and Microsoft Partner to Deliver Enhanced Analytics and AI Services to Classified Networks for Critical National Security Operations”, August 8, 2024, <https://news.microsoft.com/source/2024/08/08/palantir-and-microsoft-partner-to-deliver-enhanced-analytics-and-ai-services-to-classified-networks-for-critical-national-security-operations/>, accessed 12 April 2026

⁵³ Ibid

⁵⁴ Jennifer Conrad, “Anthropic, Amazon, and Palantir Team Up to Bring AI to the Defense Department,” *Inc.*, November 8, 2024, <https://www.inc.com/jennifer-conrad/anthropic-amazon-and-palantir-team-up-to-bring-ai-to-the-defense-department/91001401>, accessed 12 April 2026

⁵⁵ Emily Bienvenue et al., “Private Tech Companies, the State, and the New Character of War,” *Carnegie Endowment for International Peace*, December 1, 2025, <https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies>, accessed 12 April 2026.

The first form we will discuss is infrastructure dependence, which covers more than it might seem. And for military AI development it is divided between the hardware, the platform, and the software needed to produce and operate AI systems.⁵⁶

In terms of hardware, semiconductors are one of the most important components as they are used to build chips, and control the flow of electricity in a reliable and energy efficient way, making them essential for modern electronic devices.⁵⁷ And to build them, core raw materials are needed such as high purity Silicon, and Gallium.⁵⁸ China dominates the field of most silicon metal production which is the most important component for the production process,⁵⁹ but it lags behind in terms of transforming the material into semiconductor wafers, leaving the scene for Shin-Etsu and SUMCO, two Japanese companies, Global Wafers, a Taiwanese company, and Siltronic, a German company, to finalize the production phase.⁶⁰

Knowing this, it is easy to notice that the raw materials required to produce semiconductors are controlled by a very different set of actors. The privatized downstream production but state influenced upstream control creates a structural vulnerability for states that rely on semiconductor imports, as access to critical materials remains susceptible to geopolitical pressure and export controls long before chips enter military or AI systems.

Moreover, the U.S. imposed export controls in 2022, to stop China from obtaining the advanced computer chips it needs for high end defense AI technology.⁶¹ Although the U.S. has no legal authority to impose such rules internationally, its ban worked because nearly every major chip

⁵⁶ Stephanie Susnjara, Mesh Flinders, and Ian Smalley, “What Is AI Infrastructure?” *IBM*, published June 3, 2024, updated April 8, 2026, <https://www.ibm.com/think/topics/ai-infrastructure>, accessed 13 April 2026.

⁵⁷ Britannica Editors, “Semiconductor,” *Encyclopedia Britannica*, history section, <https://www.britannica.com/science/semiconductor>, accessed 13 April 2026.

⁵⁸ “Semiconductor Raw & Refined Materials”, *SemiconductorX*, <https://semiconductorx.com/semiconductor-raw-materials.html>, accessed 13 April 2026.

⁵⁹ WaferPro, “China’s Dominance in the Global Silicon Supply”, June 21, 2024, <https://waferpro.com/chinas-dominance-in-the-global-silicon-supply/>, accessed 13 April 2026.

⁶⁰ Nikita Kumari, “Semiconductor Materials Sourcing: Securing the Supply Chain Behind the Chips,” *BISinfotech*, August 18, 2025, <https://www.bisinfotech.com/semiconductor-materials-sourcing-securing-the-supply-chain-behind-the-chips/>, accessed 13 April 2026.

⁶¹ U.S. Department of Commerce, Bureau of Industry and Security, “Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People’s Republic of China (PRC)”, October 7, 2022. <https://www.bis.gov/press-release/commerce-implements-new-export-controls-advanced-computing-semiconductor-manufacturing-items-peoples>, accessed 16 April 2026.

company rely on at least some U.S. origin technologies, like software tools.⁶² The meaning of this is that firms risk losing essential technologies if they do not comply. As a result, China has been largely cut off from cutting edge chips, slowing its ability to develop advanced AI defense systems.⁶³

The latter shows that hardware dependence is not a simple bilateral relationship between a buyer and a seller, as it is a vulnerability that can be activated by a third party with leverage over the production chain, and that it is a bottleneck that not even leaders can escape from fully.

In terms of platforms, cloud computing clusters are very important for modern AI production and utilization. Big cloud companies such as Google Cloud⁶⁴ and Microsoft Azure,⁶⁵ own large data centers filled with interconnected high-performance machines that work together to train AI and store data and software for remote use, which is a task that a single machine cannot perform.⁶⁶ Only a few countries and companies in the world can supply such services considering the substantial amount of energy and money needed to do so, and 90% of these centers are located in both the U.S. and China.⁶⁷

Considering the large amount of space to store data and the lack of these mega centers in most countries, foreign AI powered surveillance systems are usually hosted on foreign infrastructure belonging to a different country than the host state or to a private technology company. The storage of data raises serious questions about the right of the state to retain full ownership of its population's data,

⁶² Shakhboz Juraev, "EDA Industry in the US–China Tech War: De-Americanization and Sinification of the EDA Industry in China", *Technology Global (Substack)*, August 22, 2024, <https://technologyglobal.substack.com/p/eda-industry-in-the-us-china-tech>, accessed 16 April 2026.

⁶³ Gregory C. Allen, *Choking off China's Access to the Future of AI: New U.S. Export Controls on AI and Semiconductors Mark a Transformation of U.S. Technology Competition with China* (Center for Strategic and International Studies), October 11, 2022, <https://www.csis.org/analysis/choking-chinas-access-future-ai>, accessed 18 April 2026.

⁶⁴ Dhruv Shishodia, "The Role of AI in Cloud Platforms – AWS, Azure, and Google Cloud Compared," *ThinkCloudly*, November 12, 2025, <https://thinkcloudly.com/blog/the-role-of-ai-in-cloud-platforms-aws-azure-and-google-cloud-compared/>, accessed 14 April 2026.

⁶⁵ Ibid

⁶⁶ Amazon Web Services, "What Is Cluster Computing?", <https://aws.amazon.com/what-is/cluster-computing/>, accessed 14 April 2026.

⁶⁷ Aminu Abdullahi, "Global Divide: Only 32 Countries Host AI Data Centers," *TechRepublic*, June 23, 2025, <https://www.techrepublic.com/article/news-only-32-countries-host-data-centers-2025/>, accessed 14 April 2026.

especially with the presence of laws such as the U.S. CLOUD Act or China's 2017 Cybersecurity Law,⁶⁸ that force companies in these two countries to hand over data, even if it belongs to the population of a different country. For a state that relies on foreign cloud platforms, especially for data storage, it can become exposed to competing territorial and extraterritorial jurisdictional claims⁶⁹ especially where foreign governments exercise jurisdiction *ratione personae* over technology companies incorporated under their laws.⁷⁰ The risk of such a thing to happen is not theoretical, as in 2023, concerns about precisely this vulnerability led several European governments to begin negotiating and regulating the use of American cloud providers for classified defense data, citing CLOUD Act exposure as an unacceptable sovereignty risk.⁷¹

What this means for civilians is a serious matter, as when a state's surveillance data is stored on foreign infrastructure, and subject to foreign law, the data about them can be accessed and used in ways that leaves them with no explicit legal channels to fight for their privacy.

In terms of software, it is the full set of programs and instructions that make a computer work.⁷² In the context of military AI, software dependence refers specifically to reliance on foreign developed and trained AI models, usually resulting in what is known as the black box problem.⁷³ Many advanced AI systems cannot explain to buyers how they arrive at their outputs as the internal logic of the system is effectively opaque⁷⁴. The meaning of this is that a state using a foreign AI model for military purposes cannot fully audit what assumptions are embedded in it, and why it produces the recommendations it does. For example, if the system produces a flawed targeting recommendation that leads to civilian harm, the dependent state cannot point to the reasons of what

⁶⁸ Abiade, "Algorithmic Sovereignty and New Security Dependencies"

⁶⁹ Patrik Hummel et al., "Data Sovereignty: A Review", *Big Data & Society* 8, no. 1 (January–June 2021): 7, <https://doi.org/10.1177/2053951720982012>, accessed 28 May 2026.

⁷⁰ Cedric Ryngaert, "Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts," *German Law Journal* 24, no. 3, May 2023, 544–546, <https://doi.org/10.1017/glj.2023.24>, accessed 28 May 2026.

⁷¹ Konrad Wolfenstein, "Why the US Cloud Act Is a Problem and Risk for Europe and the Rest of the World: A Law with Far-Reaching Consequences," *Xpert.Digital*, April 16, 2025, <https://xpert.digital/en/us-cloud-act/>, accessed 16 April 2026.

⁷² Britannica Editors, "Software," *Encyclopaedia Britannica*, May 22, 2026, <https://www.britannica.com/technology/software>, accessed 14 April 2026.

⁷³ Abiade, "Algorithmic Sovereignty and New Security Dependencies"

⁷⁴ Vikas Hassija et al., "Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence", *Cognitive Computation* 16, no. 1 (2024): 45–74, <https://doi.org/10.1007/s12559-023-10179-8>, accessed 14 April 2026.

actually went wrong, as the failure is distributed invisibly across millions of parameters that the state cannot read. In 2017 The U.S. Defense Advanced Research Projects Agency (DARPA) launched the Explainable AI program because military operators were being asked to act on AI recommendations that they could not interrogate or verify.⁷⁵ If the world's leading AI producer identified this as a critical gap in systems it built itself, the implications for dependent states using systems they did not build are considerably more serious.

Software dependence also introduces a distinct risk, which is the problem of bias that comes from machine learning and algorithm creation. As explained above, AI models learn their behavior from data and from the algorithmic procedure of the machine learning process, and if this process integrates any pattern of discrimination, those patterns become encoded in the model's outputs, which are then replicated at a larger scale.⁷⁶ The AI model may carry assumptions about what constitutes suspicious behavior, or what environments signal danger. These assumptions are usually drawn from contexts completely different from where the system is actually being deployed.⁷⁷ In surveillance applications, this can produce systematic misclassification of civilian populations, with serious human rights consequences that the dependent state may not be able to detect, or correct.

The second form of dependence we will tackle is data dependence. Data dependence refers to reliance on foreign generated or foreign controlled datasets for the training and operation of military AI systems. This form is not about where data is stored, but about what the data has taught the AI system to think. Military AI systems learn from the data on which they are trained,⁷⁸ meaning that biased datasets can shape how these systems assess situations. As with software dependence, this can reproduce external biases, although the source of the problem differs, and it may also result in dependent states deploying foreign AI systems that apply learned judgments

⁷⁵ Defense Advanced Research Projects Agency (DARPA), “Explainable Artificial Intelligence (XAI)”, <https://www.darpa.mil/research/programs/explainable-artificial-intelligence>, accessed 16 April 2026.

⁷⁶ Jonker and Rogers, “What Is Algorithmic Bias?”

⁷⁷ Chenruo Liu et al., “Bridging Distribution Shift and AI Safety: Conceptual and Methodological Synergies”, *arXiv preprint arXiv*, 2505.22829v2, last revised June 18, 2026, 2-10, <https://arxiv.org/pdf/2505.22829>, accessed 16 April 2026.

⁷⁸ Jonker and Rogers, “What Is Algorithmic Bias?”

developed in different conflict environments, reflecting the strategic priorities and operational assumptions of the supplying state rather than those of the dependent state.

The consequence of data dependence can also produce a distinct technical risk which is labelled as distributional shift. The latter phenomenon is simply the situation where the world the model is applied to, looks enough different from the world it was taught in, that the model's knowledge no longer applies correctly.⁷⁹ A dependent state using a foreign system may therefore be making operational decisions based on outputs that are systematically less reliable in its own operational environment than they were in the environment the system was designed for. When those unreliable outputs are used to make targeting or surveillance decisions, the amplified human rights cost is borne by the civilian populations on the ground. People who had no role in the procurement decision that put a foreign trained system in charge of decisions about their lives.

The third form is political conditionality dependence, which refers to the conditions that supplier states, or private firms, force on buyers before selling them the AI systems, and during its operational period. Examples of this are when a supplier restricts how a technology can be used, or threatens to withdraw access in response to political disagreement. For dependent states, this means that the boundaries of sovereign decision making are at risk of being partially drawn by foreign actors outside their borders. Back in 2025, the U.S. threatened Ukraine with the possibility of cutting its access to Starlink satellite internet if a deal on critical minerals was not reached.⁸⁰ Threats ended up forcing President Zelenski to sign the deal he initially refused,⁸¹ illustrating the real effects of conditionality on the ground.

Moreover, it is important to note that conditionality is not only bilateral between states, as technology firms today are playing a major role in the field. The U.S. designated Anthropic which is an American tech firm as an AI supply-chain risk after the company imposed its own ethical restrictions on its models, illustrating how unpredictably the dynamic between a state and a firm

⁷⁹ Liu et al., “Bridging Distribution Shift and AI Safety”

⁸⁰ Maximilian Mayer and Yen-Chi Lu, “Global Structures of Digital Dependence and the Rise of Technopolis”, *New Political Economy* 30, no. 5 (2025): 755–774, <https://doi.org/10.1080/13563467.2025.2497766>, accessed 16 April 2026.

⁸¹ Ibid

can be. If a government can be threatened by the self-imposed limits of its own domestic firm, the vulnerability of a foreign dependent state to the commercial decisions of that same firm is considerably greater.

The three discussed forms of dependence are not mutually exclusive, and states typically face several at the same time. States that are unable to produce military AI systems depend on producing states and companies to strengthen their army capabilities, risking the amplification of human rights vulnerabilities and losing autonomy over their security decision-making. These forms of dependence tend to deepen over time, as states that integrate foreign AI systems into their military doctrine embed foreign military values into their own, and build their systems on foreign infrastructure making it too expensive to change course. Decisions about AI procurement made today will shape what options are available tomorrow, and for a long time after that.

The comparative analysis of Israel and the UAE in the upcoming chapters will use this framework that we developed to examine the forms of dependence each face, in addition to their combined effects on both countries' autonomy, security, and human rights outcomes. As will become clear, Israel and the UAE do not represent opposite ends of a spectrum from dependence to independence, but they represent two different profiles of dependence shaped by different structural conditions, and carrying different consequences as a result.

Chapter 2: The Roots of Reliance: Conditions That Create and Sustain Military AI Dependence

Dependency theory was first proposed by economist Raúl Prebisch, and it aims to explain why and how underdeveloped countries remain reliant on developed states.⁸² In this chapter, we draw on this theory as an analytical starting point and adapt it to examine broader forms of technological reliance. The analysis will further accommodate the inclusion of middle power countries, and the emergence of AI and private companies as strong players in the defense sector.

⁸² André Munro, "Dependency theory", Encyclopaedia Britannica, <https://www.britannica.com/topic/dependency-theory>, accessed 28 May 2026.

Chapter 2 argues that the conditions which determine how deep a state can fall into dependence are historical, economic, political, and institutional in nature, and that they interact with one another in ways that make dependence self-reinforcing once it takes hold. These conditions will be later used in Chapter 3 and 4 to analyze the roots of reliance of both Israel and the UAE.

2.1 Colonial Legacies and Economic Foundations: Why Historical Conditions Still Determine Who Can Build Military AI

According to dependency theory, colonialism plays a major role in the unequal distribution of development between countries, dividing the global economy into a dominant "Core" and a dependent "Periphery". After the two world wars, countries in Western Europe recovered faster than many other regions considering their long legacy of statehood, and adoption of welfare capitalistic market principles.⁸³ On the other hand, countries that were ruled by foreign powers faced the challenge of building infrastructure, and independent legal and financial institutions.⁸⁴ This compounded pressure affected the ability of the latter states to focus on technology development, as the needed foundation for their development was mostly lacking. Today, colonial history interacts with international and internal political realities, which can either slow or accelerate national development, and ultimately determine whether a state becomes a producer of military AI, or remains fully dependent on external players.

One of these internal realities is the difficulty diverse societies often face when trying to build strong institutions. Former colonies with multiethnic or multireligious societies face extended difficulties as they try to maneuver internal tensions and external interference from states that benefit from keeping them weak. This extends the time these countries need to build healthy democratic foundations,⁸⁵ resulting in delayed innovation structures and making it more difficult

⁸³ Aurélie Dianara Andry, "The 'Social Dimension' of Postwar Europe," in *Social Europe, the Road Not Taken: The Left and European Integration in the Long 1970s* (Oxford: Oxford University Press, 2022), 27–59, <https://doi.org/10.1093/oso/9780192867094.003.0002>, accessed 17 April 2026.

⁸⁴ James A. Robinson and Daron Acemoglu, "The Economic Impact of Colonialism", Center for Economic Policy and Research, January 30, 2017, <https://cepr.org/voxeu/columns/economic-impact-colonialism>, accessed 17 April 2026.

⁸⁵ PolSci Institute, "The Uneven Path of Democracy in Post-Colonial Nations", last updated October 18, 2025, <https://polsci.institute/political-processes-institutions/uneven-path-of-democracy-post-colonial-nations/>, accessed 17 April 2026.

to build advanced technologies such as military AI. Corruption is another factor that continues to weaken the institutional base that technological production relies on, standing as a barrier to innovation, and preventing states from developing the financial credibility required to support domestic military AI industries.⁸⁶

Despite this, a strong economy plays a major role that allows countries to jumpstart their AI production journey. Intertwined with historical factors, it explains why some countries are able to innovate faster and better than other countries. Adopting advanced technology is risky and expensive.⁸⁷ To fund it, you need good financial institutions.⁸⁸ If a country has weak financial markets and a poor rule of law then investors cannot trust firms.⁸⁹ This fact discourages funding risky advanced technologies, so firms adopt simpler, less productive technologies reducing the country's Total Factor Productivity (TFP) and income, which in turn limits their ability to develop advanced technologies.

The technology adoption barrier is exceptionally high in military AI production. States have to confront their historical and economic barriers which in turn face international restrictions caused by the international power play and fight for dominance. Developing local military AI capability requires strong financial systems capable of sustaining long term high risk investment, and the ability to maneuver the complexities of international relations. States that lack these foundations, will have to rely on foreign systems which will pull them deeper into dependence.

2.2 Threat Environments, Alliance Structures, and Export Controls: How Political Conditions Lock States Into or Out of Military AI Independence

The historical and economic conditions discussed in the previous section explain why some states have the ability to enter the military AI competition while others do not, and it explains why some states enter with a stronger foundation than others. Historical and economic factors alone do not

⁸⁶ Feng-Shang Wu and Hong-Ji Huang, “Why Do Some Countries Innovate Better than Others? A New Perspective of Science, Technology, and Innovation Policy Regimes and National Absorptive Capacity”, *Sustainability* 16, no. 7 (2024), 2840, 9, <https://doi.org/10.3390/su16072840>, accessed 17 April 2026.

⁸⁷ Ibid

⁸⁸ Ibid

⁸⁹ Ibid

fully explain the picture, and here comes the role of political and strategic conditions, to explain how the producing state manages its relationships with foreign suppliers and how much sovereignty it is willing to trade for security.

Political and strategic conditions operate on two levels which are the domestic and the international. Both levels matter for understanding the different positions of Israel and the UAE in the later chapters.

At the domestic level, one of the most important conditions that can shape why a country decides to invest heavily in military technology is the security risk.⁹⁰ States that perceive themselves as facing grave security threats tend to prioritize investment in defense technology. But this risk is not an external issue only, as a lot of states also face fear of regime change from within, and invest in strengthening their capabilities to self-preserve such as the case of the Islamic Regime in Iran.⁹¹ Threat environments create the needed political conditions for sustained long term investment in domestic defense industries, but in reality, these conditions do not always translate into autonomous production.

Another internal condition that drives governments to invest in military AI is the ambition to become regional, or international leading powers, protecting themselves from the geopolitical risk of domination.⁹² In this case, investment in surveillance and military AI serves political functions that go beyond battlefield capability. Saudi Arabia for example, made large AI investments and signed major defense technology deals as part of its Vision 2030, and its ambition to be a regional power.⁹³

⁹⁰ Dale Swartz, Ryan Brukardt, and Karl Hujsak, “Creating a Modernized Defense Technology Frontier”, McKinsey & Company, February 12, 2025, <https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/creating-a-modernized-defense-technology-frontier>, accessed 18 April 2026.

⁹¹ Insikt Group, "Iran's AI Ambitions: Balancing Economic Isolation with National Security Imperatives", Recorded Future, April 17, 2025, <https://www.recordedfuture.com/research/irans-ai-ambitions-balancing-economic-isolation-national-security-imperatives>, accessed 18 April 2026.

⁹² Jared Cohen and George Lee, “The Generative World Order: AI, Geopolitics, and Power”, Goldman Sachs Global Institute, December 14, 2023, <https://www.goldmansachs.com/insights/articles/the-generative-world-order-ai-geopolitics-and-power>, accessed 18 April 2026.

⁹³ Andrea Benito, “Saudi Arabia Launches \$100 Billion AI Initiative to Lead in Global Tech”, *CIO*, November 12, 2024, <https://www.cio.com/article/3602900/saudi-arabia-launches-100-billion-ai-initiative-to-lead-in-global-tech.html>, accessed 18 April 2026.

Drawing from this, neither threats nor prestige ambition alone determine whether a state ends up dependent or not. A state can have a powerful security imperative, and still remain deeply reliant on foreign suppliers, especially with a weak economy and a history of colonial domination. So, the political condition that translates into dependence in this case, is the same condition that can lead a country to break the cycle of reliance.

Coming to the international political and strategic conditions that shape dependence, alliance structures and export controls are the two most important ones to discuss. Beginning with alliance structures, it is known as a fact that states that are close allies of major AI producers tend to have preferential access to advanced military technologies.⁹⁴ Despite this, this access might come with conditions that can deepen dependence rather than reduce it, as a state that receives an external AI system ends up depending on the supplier for maintenance and for keeping that access open.⁹⁵ The political cost of this reliance is often invisible during peacetime, but becomes visible when the interests of the supplier and the dependent state become different. When this happens, the dependent state can face major security risk limiting its freedom of action.

In regard to export control, the most important element to know is that transfer restrictions are major tools in the arena of geopolitical competition. Export controls on advanced semiconductors and software are not mere policies, but are strategic instruments used by powerful states to limit the power of adversaries. The U.S.'s ban on exporting semiconductors to China is the perfect example to illustrate this, as the ban enforcement also included major chip companies outside the U.S., severely limiting China's ability to access advanced chips.⁹⁶ For middle capacity states navigating relationships with multiple suppliers simultaneously, this dynamic introduces serious political risk as each supplier may impose conditions that conflict with the requirements or expectations of the other, forcing the dependent state into difficult choices about which relationships to prioritize and at what cost.

⁹⁴ NATO, Summary of NATO's Revised Artificial Intelligence (AI) Strategy, 10 July 2024, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>, accessed 18 April 2026.

⁹⁵ Abiade, "Algorithmic Sovereignty and New Security Dependencies"

⁹⁶ Allen, Choking off China's Access to the Future of AI.

Taken together, we can see that both internal and international political and strategic conditions shape dependence, and that dependence is not restricted to small and middle powers only, but it is felt at different intensities for all players, even the leaders as we saw with the China example. The conditions we discussed do not operate in isolation, but they interact with the historical and economic foundations to determine the position of each state on the axis of dependency.

2.3 Beyond Investment: Why Innovation Ecosystems and Civil-Military Collaboration Determine Whether Spending Produces Sovereignty or Procurement

Even when a state has the economic foundations and the political and strategic capacity to develop military AI, it can still remain dependent if the right technological and institutional conditions are not met. The reason is simple, without the right conditions in place, political ambition tends to produce procurement rather than production, and procurement means dependence. In this section we will look into these technological and institutional conditions and we will analyze their importance and their relation to the concept of dependence.

One of the most important technological and institutional conditions is the presence of a functioning innovation ecosystem. Feng-Shang Wu and Hong-Ji Huang argue in their research on science, technology, and innovation (STI) policy regimes that innovation performance is shaped by a wide set of conditions including national values, key decision-makers, culture, and how policies are created, in addition to the broader regime within which innovation happens.⁹⁷ Wu and Huang divide countries between two types of STI policy regimes, which we will refer to in our analysis of both the innovation model of Israel and the UAE. A democratic STI policy regime is society centered and shaped by openness, freedom, and equality. Such a society supports innovation in several ways, including the freedom that gives people room to generate creative ideas and start new businesses.⁹⁸ The meritocratic regime on the other hand is a state centric regime that

⁹⁷ Wu and Huang, “Why Do Some Countries Innovate...”

⁹⁸ Ibid

relies on technical expertise and education guided by technocrats who design and implement policies based on logic and evidence.⁹⁹

Both regimes provide states with the capacity to innovate and create military AI innovations, either through open market competition, or through directed state strategy and technocrat opinions. States that seek to lead can also adopt both regimes creating a balance between them to achieve the best results. When states fail to adopt either regime, or if they adopt one without effective planning and long term strategic vision, this could lead them to fall deeper into dependence as they will not be able to generate the domestic innovation needed to produce military AI independently. This is one of the most direct paths into dependence, because a state that cannot innovate domestically has no alternative.

The balancing of regime adoption and the long term strategic vision needs good policy planning of what is known as National Absorptive Capacity (NAC). Wu and Huang define NAC through dividing the concept into two parts; Potential NAC (PNAC) and Realized NAC (RNAC).¹⁰⁰ PNAC is the ability to find, absorb, and learn from external knowledge, and RNAC is the ability to use and commercialize that knowledge.¹⁰¹ Too much PNAC can cause a country to focus too much on exploration while neglecting the application side, while too much RNAC can make a country focus too much on exploitation while neglecting exploration.¹⁰² What this means in practice is that a state needs both capacities working together. Without PNAC, a state cannot learn from what others are producing. Without RNAC, a state cannot turn what it learns into something it can use and own.

For military AI dependence, this balance greatly matters, as a state that can learn foreign knowledge, but cannot produce it, remains dependent on foreign systems even if its researchers understand the technology. And a state that can scale existing technologies but cannot generate new ones, also remains dependent on foreign producers for the next generation of systems. Getting

⁹⁹ Ibid

¹⁰⁰ Ibid

¹⁰¹ Ibid

¹⁰² Ibid

out of dependence requires both, and a state that only has one side of this will keep going back to foreign suppliers, turning what could have been a temporary reliance into a permanent condition.

STI policy regimes and NAC jointly shape a country's innovation performance, and states that lack balance between the indicators whether because their institutions are too closed to absorb external knowledge, or too underdeveloped to commercialize what they absorb, will find that even large investments in military AI produce dependence rather than autonomy, because they end up acquiring foreign systems that they cannot replicate, or improve independently.

A second condition of dependence is the absence of effective civil military collaboration. To understand why this matters so much today, we need to go back to something we touched on earlier in previous sections. For most of modern history, big technological breakthroughs came from inside military institutions, before eventually finding their way to civilians. But AI did not follow this pattern, as it was not born in a military lab or a government research facility, it grew in universities and in corporate research centers, in the competitive environment of the private technology sector.

This fact presents real consequences for dependence, because a state that wants to build military AI today simply cannot do it from within its military institutions alone, as the stronger knowledge and infrastructure are elsewhere. States that manage to build real working relationships between their defense establishments and their private technology sectors can channel civilian innovation into military applications while states that fail to build these relationships are left with developing military AI slowly and at great expense in isolation, or buying it from foreign suppliers. Most buy, and buying is dependence. This kind of collaboration between the private and public sector does not just appear because a government decides it wants it, as states need to adapt their laws and policies to promote a strong civil military collaboration which will enable them to keep pace with technological change. Private companies need strong intellectual property protections before they will share their most valuable work with any government,¹⁰³ and without those protections,

¹⁰³ Michael Seeds, "Policy Points: The Balance of Protecting IP and Data Rights," *National Defense Magazine*, October 4, 2024, <https://www.nationaldefensemagazine.org/articles/2024/10/4/policy-points-the-balance-of-protecting-ip-and-data-rights>, accessed 19 April 2026.

cooperating with the military means handing over what took them years to build. Military institutions on the other side need to develop openness to civilian input, which does not come naturally to organizations built around command structures and secrecy.¹⁰⁴ The quality of this collaboration also determines how quickly a state can respond to technological change. States that fall behind from this track will face more dependence with each new generation of innovation, making the reliance gap harder and harder to close.

Innovation ecosystems and civil military collaboration, together explain why political will and money alone are not enough to escape from military AI dependence. A state without strong and balanced innovation ecosystems, and a state that cannot connect military demand to private sector innovation, will fill the gap with foreign systems. And these conditions do not work in isolation, they sit on top of the historical, economic, political, and strategic foundations from the previous section, and all of it together determines not just whether a state is dependent, but how deep that dependence goes, and how difficult it is to exit.

2.4 Private Firms as Structural Actors: Strategic and Human Rights Risks

We have talked in the previous sections about strong civil military relations in the sector of military AI as a determinant of dependence. We have also discussed how a strong economy, rule of law, and R&D systems are necessary for the private tech sector to flourish in a certain country. Throughout the sections, it became evident how important the influence of private firms has become, making it urgent to discuss and analyze their role in terms of dependence and better understand the associated risks that can come with it.

Militaries are now heavily relying on private AI to enhance their capabilities, but this reliance is raising serious questions about sovereignty and human rights. The central problem is not only that private firms carry risks, but also that states which depend on them cannot easily exit the relationship once it is established, because the cost of switching systems and rebuilding

¹⁰⁴ Neil Ashdown, "Unity or Coherence: Shaping Future Civil-Military Intelligence Collaboration in the Cyber Domain," in *CyCon 2024: Over the Horizon*, 16th International Conference on Cyber Conflict, ed. C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, and D. Štrucl (Tallinn: NATO CCDCOE Publications, 2024), https://ccdcoc.org/uploads/2024/05/CyCon_2024_Ashdown-1.pdf, accessed 19 April 2026.

infrastructure is extremely high. This creates a form of dependence that is self-reinforcing and commercially driven rather than strategically managed.

Private tech companies, like all other firms, cannot be established without a registered headquarters, usually tying them to their home countries. The latter tie could mean little from a free market point of view, as the company can sell its products internationally with a few restrictions, and maintain its own profit above all else. But at the same time the tie could mean everything especially if the country has strong policies to support the private sector, and if the players in that sector benefit from having a strong home country that they could potentially influence, for example in the form of lobbying¹⁰⁵ to protect their interests and informally take part in the drafting of laws and policies. For a dependent state relying on a foreign private firm, this dynamic means that the political relationship between the firm and its home government can directly shape whether access to critical military AI systems is maintained or withdrawn, and the dependent state has no seat at that table.

The worrying thing about this status quo is its unpredictability. National security is a key driver of international relations, and politicians draft long term strategies to protect it. But with the addition of an unpredictable element that can defy the government, and with the great reliance the world is seeing on that particular element, national security and sovereignty will find themselves to be in grave danger.

In order to illustrate this idea, we can go back to the Anthropic example presented in this research. The latter company tried to enforce its own ethical considerations on the government, aiming to prevent the army from using its products in fully autonomous weapons and mass surveillance.¹⁰⁶ The answer from the U.S. Government came quickly with designating Anthropic as a security risk, and with a statement from the American Defense Secretary Pete Hegseth saying that “America's warfighters will never be held hostage by the ideological whims of Big Tech”.¹⁰⁷ The altercation

¹⁰⁵ Will Henshall, “There’s an AI Lobbying Frenzy in Washington. Big Tech Is Dominating”, *TIME*, April 30, 2024, 10:05 a.m. PT, <https://time.com/6972134/ai-lobbying-tech-policy-surge/>, accessed 22 April 2026.

¹⁰⁶ Selina Wang, “Trump Orders US Government to Cut Ties with Anthropic; Hegseth Declares Supply Chain ‘Risk’,” *ABC News*, February 28, 2026, <https://abcnews.com/Politics/anthropic-latest-pentagon-contract-bar-ai-autonomous-weapons/story?id=130558898>, accessed 22 April 2026.

¹⁰⁷ Ibid

that led to a lawsuit later, proved that the tech firms can affect national security as they can withdraw their services and dictate their limitations, leading the government to face costly consequences if they had to switch their systems and infrastructure.¹⁰⁸

If this dynamic plays out between a private firm and its own home government, the implications for a foreign dependent state are considerably more serious. A state that has built its defense infrastructure around a foreign private firm's systems may not have a diplomatic channel to escalate through, and no quick alternative to turn to. This situation is made more difficult by the absence of a comprehensive binding framework governing the role of private actors in military AI and determining responsibility when their decisions affect national security.

Even when a tech firm has no links to any foreign governments, the risk of hacking its systems still exists. In 2020, a group of Russian hackers by the name “Cozy Bears” hacked a private U.S. IT firm called SolarWinds, and inserted malicious code into its software update, reaching thousands of organizations including U.S. government agencies like the Treasury, and Homeland Security.¹⁰⁹ For dependent states, the problem is bigger than just getting hacked, as a state that runs its military AI on foreign private infrastructure has no way to check it for weaknesses on its own, and if something goes wrong, cutting it off is not a decision it can make alone.

The above risks can also deeply affect civilians as their data can end up in the hands of private actors and foreign governments that can potentially use it against them. Private firms can also produce AI systems with varying levels of accuracy and data quality threatening to increase collateral damage in battle and diffuse responsibility between different actors. The most prominent framework to tie private firms to human rights is known as the Ruggie Framework.¹¹⁰ The latter is not specific to military AI and is not binding in nature, meaning that states can refuse to abide by its principles. No legally binding unified mechanism exists today to force companies to abide by

¹⁰⁸ Open Source AI Review Editorial Team, “Why Your AI Provider Switch Will Cost More Than You Think,” Open Source AI Review, April 16, 2026, <https://www.opensourceaireview.com/blog/why-your-ai-provider-switch-will-cost-more-than-you-think>, accessed 22 April 2026.

¹⁰⁹ Sila Özeren Hacıoğlu, “APT29 Explained: Cozy Bear’s Evolution, Techniques, and Notorious Cyber Attacks,” Picus Security, last updated April 6, 2026, <https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques>, accessed 22 April 2026.

¹¹⁰ Ruggie, *Protect, Respect and Remedy*

human rights principles. Ongoing UN efforts are underway to produce a legally binding treaty on the subject, but until date such framework does not exist¹¹¹.

In the end, the presence of tech companies as players in the field of military AI is not inherently bad or incompatible with human rights norms. These players, as much as they can create risk, are also the backbone of innovation, and it is up for governments to create legally binding frameworks to lessen the associated risks with their work. But until those frameworks exist, the states most exposed to the risks described in this section are not the powerful ones with leverage over private firms but they are the dependent ones, who bear the consequences of a system they did not design and cannot fully control. This is what makes the role of private technology firms not just a governance problem, but a structural condition of dependence that Chapters 3 and 4 will examine directly through the cases of Israel and the UAE.

Chapter 3: Built to Fight: Israel's Military AI Ecosystem, Supply Chain Vulnerabilities, and Human Rights Record

3.1 From Survival Imperative to Global Exporter: How Israel Built Its Military AI Ecosystem Through Security Pressure, R&D, and Civil-Military Relations

After the fall of the Ottoman Empire and the establishment of the British Mandate in Palestine, both Jewish and Arab Palestinian populations developed political aspirations for self-determination in the region. On 14 May 1948, Israel declared its independence, and was quickly recognized by the U.S. and the Soviet Union.¹¹² A foreign Jewish state on the same land that the Arab Palestinians wanted to declare their own independence was considered unacceptable for the

¹¹¹ OHCHR, “BHR Treaty Process”, <https://www.ohchr.org/en/business-and-human-rights/bhr-treaty-process>, accessed 6 July 2026.

¹¹² Eliahu Elath et al, “Establishment of Israel”, Encyclopedia Britannica, April 23, 2026, <https://www.britannica.com/place/Israel/Establishment-of-Israel>, accessed 23 April 2026.

Arabs, leading to many conflicts and wars fought between the two parties.¹¹³ Being in that position, and with a hostile environment all around it, the newly established Israeli state prioritized its security and survival as central policy objectives.

For survival, Israel knew that it had to build a strong army, and establish the right political connections with strong countries like the U.S. But building a strong army in a resource-scarce, internationally contested, and economically fragile new state required more than political will. It required turning every available structural advantage into a driver of defense capability.

In the years before 1967, France was Israel's primary weapons supplier.¹¹⁴ But on the eve of the Six-Day War in June 1967, French President Charles de Gaulle imposed a total arms embargo on Israel, for reasons related to French foreign policy.¹¹⁵ The shock of this moment made Israel understand the dangers of dependence especially relying on a single foreign supplier. At that moment, production became a matter of necessity and not preference.

The above historical conditions shaped Israel's security policy, and acted as an imperative to strengthen its economy and institutions for domestic military production. Taking a closer look at these institutions, we find that Israel is a state that over time managed to build a strong economy and a functioning democratic STI policy regime, combined with strong national absorptive capacity on both ends. Israel today leads the world in spending as a percentage of Gross Domestic Product (GDP), investing approximately 6.35% of GDP in R&D¹¹⁶ which is the highest among the Organization for Economic Co-operation and Development (OECD) countries.¹¹⁷ This figure is not a product of natural resources, but is the result of a deliberate and sustained policy choice to treat technological innovation as the primary instrument of national survival. The private sector

¹¹³ Ibid

¹¹⁴ Gadi Heimann, "Israeli-Franco relations and the crisis of May to June 1967, in *Franco-Israeli Relations*", 1958–1967, 1st ed. (Routledge, 2016), <https://www.taylorfrancis.com/chapters/mono/10.4324/9781315604688-18/israeli-franco-relations-crisis-may-june-1967-gadi-heimann?context=ubx>, accessed 24 April 2026.

¹¹⁵ Ibid

¹¹⁶ Israel Central Bureau of Statistics, *The National Expenditure on Civilian R&D 2023*, Media Release 320/2024 (Jerusalem: Israel CBS, October 8, 2024), https://www.cbs.gov.il/he/mediarelease/DocLib/2024/320/12_24_320e.pdf, accessed 23 April 2026.

¹¹⁷ Organization for Economic Co-operation and Development (OECD), "Gross Domestic Spending on R&D", OECD Data Indicators, <https://www.oecd.org/en/data/indicators/gross-domestic-spending-on-r-d.html>, accessed July 2, 2026

drives approximately 92% of this R&D investment,¹¹⁸ meaning that Israel's innovation ecosystem is genuinely competitive and shaped by the democratic STI model that Wu and Huang describe as producing organic breakthrough innovation through competition and individual creativity.

In terms of national absorptive capacity, Israel demonstrates a strong balance between PNAC and RNAC. On the PNAC side, Israeli researchers and companies are plugged into global knowledge networks, with Israeli tech companies raising approximately USD 12 billion in private funding in 2024, with global investors participating in the majority of funding rounds.¹¹⁹ On the RNAC side, Israel has built one of the most effective commercialization ecosystems in the world, turning absorbed knowledge into working products and companies at a pace that has nothing to do with how small the country is. High tech accounts for approximately 17% of Israel's GDP¹²⁰ and 57% of its total exports.¹²¹ This commercialization capacity is not separate from Israel's defense ecosystem, but it is its product.

In Israel there is an institutional arrangement that connects military technical training to a competitive civilian innovation ecosystem. The IDF acts as a technical talent incubator whose graduates can move into an open and competitive private technology sector and apply what they learned operationally.¹²² This requires several conditions to exist at the same time including a military that invests seriously in technical and scientific training, a private sector that is capable of absorbing and commercializing that talent, and an economic and legal environment open enough for those individuals to find companies and operate competitively. Israel has all of these

¹¹⁸ Davide Bonaglia, Lorena Rivera León, and Sacha Wunsch-Vincent, “End of Year Edition – Against All Odds, Global R&D Has Grown Close to USD 3 Trillion in 2023”, World Intellectual Property Organization (WIPO) – Global Innovation Index Blog, December 18, 2024, <https://www.wipo.int/en/web/global-innovation-index/w/blogs/2024/end-of-year-edition>, accessed 23 April 2026.

¹¹⁹ Startup Nation Central, “Israel’s Tech Sector Surpassed \$12 Billion in Funding in 2024, Solidifying Its Role as a Scale-Up Powerhouse, According to New Report.” PR Newswire, January 16, 2025. <https://www.prnewswire.com/il/news-releases/israels-tech-sector-surpassed-12-billion-in-funding-in-2024-solidifying-its-role-as-a-scale-up-powerhouse-according-to-new-report-302353152.html>, accessed 23 April 2026.

¹²⁰ Israel Innovation Authority, “Israel Innovation Authority 2025 High-Tech Report”, Press Releases, September 17, 2025, https://innovationisrael.org.il/en/press_release/innovation-report-2025/, accessed 23 April 2026.

¹²¹ Ibid

¹²² Gavin Suss, “The Role of IDF and the Israeli Military Industry in the Technological and Economic Development of Israel”, Research Papers on Knowledge, Innovation and Enterprise 13, no. 1 (July 2025): 58, <https://kiecon.org/wp-content/uploads/2025/07/Gavin-Suss-Role-of-IDF-in-Israel-Tech-Economic-Development.pdf>, accessed 24 April 2026.

conditions,^{123 124} and the most important military institutional mechanism connecting them is Unit 8200.¹²⁵

Unit 8200 is an intelligence unit in Israel, described by experts as technically comparable to the U.S. National Security Agency (NSA).¹²⁶ Every year, young recruits are selected from elite academic tracks to join it, and enter one of the most demanding technical training programs in the world, working on real operational problems in intelligence and cybersecurity.¹²⁷ Members of the unit are given complicated tasks with minimal supervision preparing them for the entrepreneurial mindset when they leave.¹²⁸ After graduating, many of the unit's alumni find tech companies,¹²⁹ greatly contributing to the country's innovation landscape.

Through the framework we prepared in Chapter 2, it becomes clear that Israel saw technological capacity as a core element to sustain its security. This led to the development of a private sector that is able to absorb skilled graduates, and the development of a legal and economic environment to support it. The result of this today is seen through the numbers of defense exports that reached a record of USD 14.7 billion in 2024,¹³⁰ making Israel one of the world's top arms exporters.

3.2 Strong but Not Sovereign: Where Israel's Military AI Capability Ends and Its Supply Chain Vulnerabilities Begin

Section 3.1 showed how Israel managed to build its AI ecosystem in the defense sector, and how it leveraged its unique conditions to become a major high tech arms producer. In this section, the research will identify the gaps in the Israeli ecosystem, aiming to see the extent of dependency the

¹²³ Ibid, 59-72

¹²⁴ U.S. Department of State, "2025 Investment Climate Statements: Israel", 2025, <https://www.state.gov/reports/2025-investment-climate-statements/israel>, accessed 24 April 2026.

¹²⁵ Gavin Suss, "The Role of IDF and the Israeli Military Industry in the Technological and Economic Development of Israel", 64

¹²⁶ Ibid 64

¹²⁷ Carmen Valache, "Israel's Unit 8200, a Conveyor Belt of High-Tech Startups," *Interesting Engineering*, August 17, 2020, <https://interestingengineering.com/innovation/israels-unit-8200-a-conveyor-belt-of-high-tech-startups>, accessed 24 April 2026.

¹²⁸ Ibid

¹²⁹ Ibid

¹³⁰ Israel Ministry of Defense. "Israel Sets New Record in Defense Exports: Over \$14.7 Billion in 2024", Ministry of Defense Press Releases, April 6, 2025, <https://www.mod.gov.il/en/press-releases/press-room/israel-sets-new-record-in-defense-exports-over-147-billion-in-2024>, accessed 24 April 2026.

country suffers from and how well it manages it. The Israeli position will be analyzed using the framework developed in Chapter 1.

In terms of infrastructure, Israel has built a world class semiconductor ecosystem of approximately 200 companies employing 45,000 people, including 70 active Israeli owned startups that have raised USD 5.5 billion collectively, alongside major R&D centers operated by Intel, Nvidia, Apple, Amazon, and Qualcomm.¹³¹ Israeli engineers designed Intel's Gaudi AI processors, Amazon's Graviton CPUs, and Nvidia's data center interconnects entirely in Israel.¹³² Israel is also home to two semiconductor fabrication plants which are Intel's facility in Kiryat Gat, and is American owned, and Tower Semiconductor's plants in Migdal Haemek,¹³³ and is Israeli owned. In February 2026, Tower announced a collaboration with Nvidia to produce 1.6T silicon photonics optical modules for next generation AI data centers,¹³⁴ demonstrating that Israeli owned fabrication is producing genuinely advanced chips for AI infrastructure. Despite this, Israel faces a gap that is shared by almost every state in the world including the United States, and it is dependency on Taiwan Semiconductor Manufacturing Company Limited (TSMC)¹³⁵ and foreign fabs for the most advanced logic chips used in large scale AI training at the highest performance levels.

TSMC produces 90% of the world's needs of advanced logic chips¹³⁶ supported by distinct talents, and a political neutrality in business. The risk of this dependence is evident considering that any geopolitical tension with Taiwan or any crisis that it might face can disrupt the supply to foreign countries. The risk of this concentration became visible during the COVID-19 pandemic, when chip demand surged dramatically, affecting TSMC and other fabs' ability to meet it, and triggering

¹³¹ Jerusalem Post Staff, "A Global Powerhouse: The Current State of Israel's Semiconductor Start-Up Ecosystem" *The Jerusalem Post*, September 29, 2025, 09:12 (updated September 29, 2025, 18:28), <https://www.jpost.com/business-and-innovation/article-868925>, accessed 25 April 2026.

¹³² Anna Ahronheim, "Israel's Semiconductor Sector Powers \$40B in Chip Exits," *The Jerusalem Post*, November 4, 2025, 21:47, <https://www.jpost.com/business-and-innovation/article-872760>, accessed 25 April 2026.

¹³³ Jerusalem Post Staff, "A Global Powerhouse: The Current State of Israel's..."

¹³⁴ Tower Semiconductor. "Tower Semiconductor Teams with NVIDIA to Advance AI Infrastructure with 1.6T Data Center Optical Modules." Press Release, February 5, 2026, <https://towersemi.com/2026/02/05/02052026/>, accessed 25 April 2026.

¹³⁵ Mateus Lee, Ming-Hung Weng, and Show-Ling Jang, "The Competitiveness and Future Challenge of the Taiwan Semiconductors Industry," in *Technology Rivalry Between the USA and China*, ed. Peter C. Y. Chow, Palgrave Studies in Global Security (Cham: Palgrave Macmillan, 2025), 161–206, https://link.springer.com/chapter/10.1007/978-3-031-76169-0_6, accessed 25 April 2026.

¹³⁶ Ibid

a worldwide chip shortage that affected industries and militaries globally.¹³⁷ Considering this, we can see that Israel is facing a universal chokepoint when it comes to logic chip fabrication, a structural feature of the global military AI landscape.

In terms of cloud dependency, Israel relies heavily on American cloud infrastructure for its AI development and deployment. During the recent wars Israel took part in after the events of October 7, a surge of usage of American AI by the Israeli Army was noticed, through increased contracts with companies such as Google Cloud, Palantir, and Microsoft Azure.¹³⁸ According to an article by AP news, the amount of Israeli data stored on Microsoft's cloud doubled between October 7, 2024, and July 2024 to reach 13.6 petabytes, which is “roughly 350 times the digital memory needed to store every book in the Library of Congress”.¹³⁹ Microsoft launched a new Azure cloud region in Israel back in 2023,¹⁴⁰ and AWS maintains significant infrastructure in the country,¹⁴¹ meaning that much of Israel's AI compute capacity runs on foreign owned platforms subject to U.S. law and the CLOUD Act, which gives the U.S. a reach over Israeli data.

To try and break free from this dependency, an Israeli company called Binat, launched Israel's first sovereign cloud in partnership with VMware which is an American company.¹⁴² Binat will be responsible for running the cloud center, while VMware will provide the software and ensure that the center meets the company's security standards.¹⁴³ Even with elements of reliance present, the project is located in Israel and will follow Israeli jurisdiction.

¹³⁷ Ian King, Debby Wu, and Demetrios Pogkas, “How a Chip Shortage Snarled Everything From Phones to Cars”, Bloomberg, March 29, 2021, <https://www.bloomberg.com/graphics/2021-semiconductors-chips-shortage/>, accessed 25 April 2026

¹³⁸ Sam Mednick, Garance Burke, and Michael Biesecker, “How US Tech Giants Supplied Israel with AI Models, Raising Questions About Tech's Role in Warfare”, *AP News*, updated February 18, 2025, <https://apnews.com/article/israel-palestinians-ai-weapons-430f6f15aab420806163558732726ad9>, accessed 25 April 2026

¹³⁹ Ibid

¹⁴⁰ Dan Swinhoe, “Microsoft Quietly Launches Israeli Azure Cloud Region,” DatacenterDynamics, October 31, 2023, <https://www.datacenterdynamics.com/en/news/microsoft-quietly-launches-israeli-azure-cloud-region/>, accessed 25 April 2026.

¹⁴¹ Amazon Web Services. “AWS Israel (Tel Aviv) Region”, <https://aws.amazon.com/local/israel/>, accessed 25 April 2026.

¹⁴² Yehuda Sharoni, “First Israeli Sovereign Cloud Launched amid Rise in Information Economy”, The Jerusalem Post, April 12, 2023, 15:17, <https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-739033>, accessed 26 April 2026.

¹⁴³ Ibid

For a state that has built its strategic identity around technological self-sufficiency, this is a meaningful gap as the infrastructure layer beneath its most advanced AI systems is not entirely Israeli to date. Building a large scale cloud infrastructure needs massive capital, making it an extremely difficult sector to achieve autonomy in.

In terms of data dependence, Israel holds an advantage that most states lack. Israel's AI systems are trained on decades of real operational data from the country's own conflict environment,¹⁴⁴ providing it with data sovereignty that most buyers of foreign systems cannot replicate. Most states that buy Israeli AI systems do not have decades of comparable operational data to train what they bought to their own conditions. The meaning here is that the form of data dependence which is having a foreign state's assumptions embedded in one's targeting logic, does not apply to Israel's domestically produced systems.

In terms of political conditionality, the biggest dependence of Israel comes from the same source of its strength in the field, from the United States of America. Under the current Memorandum of Understanding (MOU) signed in 2016, the U.S. provides Israel with USD 3.8 billion annually in military aid, making Israel the largest cumulative recipient of American military assistance since World War 2, with total aid since 1948 reaching approximately USD 174 billion (current, or non-inflation-adjusted, dollars).¹⁴⁵

In the years prior to the Gaza war, U.S. aid accounted for approximately 14% of Israel's defense budget,¹⁴⁶ rising to an estimated 35% during the peak of the post-October 7 surge as emergency assistance flooded in.¹⁴⁷ This relationship comes with real strings, as in the year 2000, the Clinton administration vetoed a nearly USD 1 billion Israeli sale of Phalcon surveillance aircraft to

¹⁴⁴ Tal Mimran, Magda Pacholska, Gal Dahan, and Lena Trabucco, "Israel - Hamas 2024 Symposium - Beyond the Headlines: Combat Deployment of Military AI-Based Systems by the IDF," Lieber Institute West Point, February 2, 2024, 4, <https://lieber.westpoint.edu/beyond-headlines-combat-deployment-military-ai-based-systems-idf/>, accessed 26 April 2026.

¹⁴⁵ Jeremy M. Sharp, U.S. Foreign Aid to Israel: Overview and Developments since October 7, 2023, RL33222 (Washington, DC: Congressional Research Service, May 28, 2025), https://www.congress.gov/crs_external_products/RL/PDF/RL33222/RL33222.51.pdf, accessed 27 April 2026

¹⁴⁶ Ibid, 22

¹⁴⁷ Ibid, Figure 6

China,¹⁴⁸ demonstrating that Washington holds effective veto power not only over what Israel receives, but over who Israel sells to. Under the current MOU agreement that governs aid money between the U.S. and Israel, the latter's ability to spend the money domestically gets progressively reduced each year reaching zero by 2028. Most of that aid money must be spent purchasing American made weapons, creating what Israeli analysts described as a growing disincentive to produce arms domestically.¹⁴⁹ Netanyahu has since announced plans to taper off U.S. military aid entirely within ten years, framing it explicitly as a lesson learned from the war.¹⁵⁰

In the end, the analysis shows that Israel's dependence is not the dependence of a weak state, but it is the dependence of a strong producer that has specific and identifiable gaps at critical points in its supply chain. Knowing Israel's dependence profile and how it strengthened its sovereignty, the next sections will tackle how much power the country gained, and the human rights and security decision making landscape produced by its dependence profile.

3.3 Does Production Translate Into Power? Applying Morgenthau's Elements to Israel's Military AI Position

In the following section we will assess Israel's strategic strength using Morgenthau's work in the realist theory, which identifies eight elements of national power: geography, natural resources, industrial capacity, military preparedness, population, national character, national morale, and quality of diplomacy.¹⁵¹ But for the purposes of this study we focus on four which are geography, industrial capacity, military preparedness, and population. The reason for this choice is that we determined the elements most directly affected by military AI. Geography is deeply relevant because it is where AI infrastructure is located and questions of jurisdiction and control are raised, industrial capacity is very important since military AI is a big part of the industrial chain, military

¹⁴⁸ Nava Freiberg, "Israel Looks to Wean Itself Off US Aid, but Breaking Free Could Cost Both Sides", *The Times of Israel*, February 13, 2026, 8:22 a.m., <https://www.timesofisrael.com/israel-looks-to-wean-itself-off-us-aid-but-breaking-free-could-cost-both-sides/>, accessed 27 April 2026.

¹⁴⁹ Herb Keinon, "Netanyahu begins a farewell to US military aid - analysis", *The Jerusalem Post*, January 12, 2026, 20:44 (updated 21:58), <https://www.jpost.com/israel-news/defense-news/article-883141>, accessed 27 April 2026

¹⁵⁰ Ibid

¹⁵¹ Stefano Guzzini, "Hans J. Morgenthau and the Three Purposes of Power," DIIS Working Paper 2018:4, 27, <https://research.diiis.dk/da/publications/hans-j-morgenthau-and-the-three-purposes-of-power/>, accessed 20 April 2026.

preparedness is the most relevant out of the elements considering how deeply it intertwines with the topic, and finally population matters, because AI production depends greatly on the human element, and technological talent within the citizen population. The other elements are affected by AI but on a weaker level. Applying these elements to Israel through the lens of military AI production, will help us show where production strengthens Israel's position in international relations, and how military AI contributes to that strengthening.

Morgenthau treats geography as the most stable of the material elements of national power, because location does not change easily.¹⁵² For Israel, geography should have been its weakest point considering the small size of the country, its disputed border with Palestine, Syria, and Lebanon, and its historically hostile regional environment. The current size of Israel is 20,770 km²,¹⁵³ but this was not always the case as its size grew bigger with every piece of land it annexed.¹⁵⁴ The size of Israel could also change in the future to include strategic lands in South Lebanon and Gaza,¹⁵⁵ according to political statements made by Israeli officials looking to annex more lands, making Israel a striking exception to the stability of the geographical element. Beyond borders and size, hostility sentiment towards Israel remains, even with more Arabs signing or negotiating the signing of peace treaties, shifting the weight of resistance from the Arab Sunni axis, to the Shia Iranian axis. Producing Military AI in this case acts as support for the weak geographical element, as the country relies heavily on technologically advanced weapons for its defense strategy and military operations. Leveraging its production abilities, Israel maintained itself against the will of its neighbors and increased its size, while making significant recent advances in Gaza and South Lebanon. Israel also maintained a strong hold over the West Bank and

¹⁵² Curran Flynn, "Political Geography and Morgenthau's Early American Works", *Cambridge Review of International Affairs* 29 (4): 1582–1602, <https://www.tandfonline.com/doi/full/10.1080/09557571.2016.1241757>, accessed 28 April 2026.

¹⁵³ Real Country Sizes, "Real Size Of Israel: How Small Israel Actually Is? (USA Is Almost 500x Bigger)", <https://realcountrysizes.com/true-size-of-israel/>, accessed 28 April 2026.

¹⁵⁴ Harvey Sicherman et al., "Establishment of Israel," *Encyclopedia Britannica*, June 17, 2026, <https://www.britannica.com/place/Israel/Establishment-of-Israel>, accessed 28 April 2026.

¹⁵⁵ Mireille Rebeiz, "Israeli threats to occupy or annex south Lebanon dust off a decades-old playbook", *The Conversation*, April 8, 2026, <https://theconversation.com/israeli-threats-to-occupy-or-annex-south-lebanon-dust-off-a-decades-old-playbook-279704>, accessed 28 April 2026.

conducted operations in Yemen and Iran, proving that technology and AI in defense can compensate for location and size without totally eliminating the threat.

The second power element identified by Morgenthau is industrial capacity, which is considered one of the most decisive elements of national power in the modern era. Israel is a small country with no significant natural resources, and an average industry share of GDP at 17.35%.¹⁵⁶ Despite this, the country has built a strong defense export industry, turning itself into one of the top 10 arms exporters in the world,¹⁵⁷ with a sector valued at USD 14.8 billion in 2024, the fourth consecutive record year for Israel.¹⁵⁸ Moreover, Israel closed a deal with Germany in December 2025, as part of an Arrow 3 deal, valued at USD 6.5 billion, the largest single Israeli defense export in history.¹⁵⁹ The shared numbers show that Israel has built an industrial capacity that major powers now depend on, particularly in advanced defense technologies and that military AI production can greatly strengthen an average industrial capacity parameter.

The third element identified by Morgenthau is military preparedness, and this element is automatically strengthened by the development of military AI. In the case of Israel, the country's domestically developed systems such as the Iron Dome, David's Sling, Arrow, Lavender, and Gospel, give Israel genuine operational capabilities and preparedness to protect itself against attacks. Despite this, and during the recent war with the Iran axis, military preparedness in Israel proved to be shaky as multiple reports emerged about a shortage in the stockpile of interception missiles especially for the Iron Dome.¹⁶⁰ To protect its ally in case Israel's stockpile ran out, the

¹⁵⁶ Trading Economics, "Israel – Industry, Value Added (% of GDP)", <https://tradingeconomics.com/israel/industry-value-added-percent-of-gdp-wb-data.html>, accessed 28 April 2026.

¹⁵⁷ Mathew George, Katarina Djokić, Zain Hussain, Pieter D. Wezeman, and Siemon T. Wezeman, Trends in International Arms Transfers, 2024 (Stockholm: SIPRI, March 2025), https://www.sipri.org/sites/default/files/2025-03/fs_2503_at_2024_0.pdf, accessed 28 April 2026.

¹⁵⁸ Emanuel Fabian, "Israeli Arms Sales Break Record for 4th Year in Row, Reaching \$14.8 Billion in 2024", *The Times of Israel*, June 4, 2025, 1:09 p.m., <https://www.timesofisrael.com/israeli-arms-sales-break-record-for-4th-year-in-row-reaching-14-8-billion-in-2024/>, accessed 28 April 2026.

¹⁵⁹ Joel Beinin, "Israel's Economy Has Problems, but It's Not Collapsing Yet," *Jacobin*, February 21, 2026, <https://jacobin.com/2026/02/israel-economy-tech-weapons-trade>, accessed 28 April 2026.

¹⁶⁰ Joshua Nelken-Zitser, "Israel's Interceptor Missiles Are Under Pressure as Threats Loom Larger", *Business Insider*, October 15, 2024, <https://www.businessinsider.com/israel-interceptor-missiles-shortage-iran-threats-loom-large-iron-dome-2024-10>, accessed 29 April 2026.

U.S. sent the THAAD anti-missile system to be installed in Israel as an extra layer of protection.¹⁶¹ It is true that a state that produces world class air defense systems, but risks running out of interceptors during active conflict, requiring a foreign ally to fill the gap, has not achieved full military preparedness through production alone. But at the same time, the same state without production would find itself in an even worse situation, proving the importance of military AI production for military strength and military preparedness. Production strengthens preparedness, but does not necessarily make it fully sovereign.

Population is the fourth element identified by Morgenthau that we will discuss, and it is one of Israel's strongest advantages. Israel's population of under ten million is small by measures of traditional power, but the quality of that population, in the specific technical and military sense, has been worked on and enhanced through mandatory military service, and the Unit 8200 pipeline discussed in section 3.1. This pipeline converts young people into capable tools that can serve the technology industry at a rate disproportionate to Israel's size. The result is a defense sector that employs tens of thousands of highly skilled workers and a tech sector that accounts for 57% of total exports.¹⁶² In the case of Israel, military AI production played an important role to sustain the population element and increase its strength and uniqueness.

Finally we can clearly see that reduced dependency on external players through local production can increase the state power across several elements. But it is important to note that the relationship between power and autonomy is not always linear, as a state can be powerful but remains reliant on external players as we saw with the relationship between the U.S. and Israel. Increased local production increases power, which in turn offers more tools to protect autonomy, but this exact line of action is not to be expected for all countries.

¹⁶¹ Tom Bateman, "Why the US Is Sending Israel a Powerful Thaad Anti-Missile System", *BBC News*, October 15, 2024, <https://www.bbc.com/news/articles/c39le0dp4p7o>, accessed 29 April 2026

¹⁶² Israel Innovation Authority, "Israel Innovation Authority 2025 High-Tech Report"

3.4 Production Without Accountability: How Israel's Domestic AI Systems Created the Conditions for Accountability While Political Choice Blocked It

The previous three sections established that Israel is a genuine producer of military AI, and that its remaining supply chain vulnerabilities are real, but specific, and identifiable. What remains to be identified in this section is the human rights cost that Israel bears from depending on foreign AI tools in its military operations, and whether the locally produced AI increases or diminishes the standard human rights risk in the Israeli case.

In terms of dependence on foreign systems, it is already established in this research that Israel mainly uses American language models and foreign cloud infrastructure for its operations, and that these systems are subject to U.S. law and the CLOUD Act, which allows the U.S. government to request access to Israeli data stored on them, causing risk of potential human rights violations, especially to the right to privacy and the right to life protected under Article 17 and Article 2 of the ICCPR.¹⁶³ The risk of breaching these two rights already exists in Israel, but dependence changes the form of how it is breached, and how it gets dealt with.

During the war on Gaza, the reliance of Israel on the American cloud systems deepened dramatically, and Israel's Military Intelligence Directorate used AWS to store mass surveillance data on Gaza's population including billions of audio files, and this data was on occasions used to confirm aerial assassination strikes.¹⁶⁴ And since the data is stored on the cloud of a foreign company, recourse to legal remedy will be subject to competing territorial and extraterritorial jurisdictional claims, complicating the road to justice and making it almost inaccessible to people living under blockade.

Leaked documents from the Nimbus contract, which is an agreement signed with Google and Amazon to provide cloud computing and machine learning services to the Israeli defense

¹⁶³ UN, ICCPR, art.17 and art.2

¹⁶⁴ Yuval Abraham, “‘Order from Amazon’: How tech giants are storing mass data for Israel’s war”, *+972 Magazine*, In Partnership with Local Call. August 4, 2024, <https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/>, accessed 30 April 2026.

establishment, revealed that Israel inserted two highly unusual clauses into the agreement, with one prohibiting Google and Amazon from restricting how their products are used, even if use breaches their own terms of service, thereby effectively preventing the companies from suspending or limiting services in response to controversial or potentially unlawful uses, and a second requiring the companies to secretly alert Israel, using a coded mechanism if a foreign court orders disclosure of Israeli data.¹⁶⁵ By doing this, Israel would have tried to protect itself from external legal accountability, while simultaneously limiting the companies' capacity to check on how their technologies are being used, and continuing to expose Palestinian civilians to mass surveillance. The fact that Israel managed to insert these two clauses highlights the danger of having private companies as players in the field of military AI, as these companies operate with a profit oriented mindset, pointing up to the tension between formal legal protections and contractual arrangements that tries to limit the scope of that protection.

In terms of whether producing locally reduces the human rights cost of AI, Israel mainly utilizes three advanced AI systems which are Gospel, Lavender, and Where is Daddy. Gospel is responsible for facilitating the collection and analysis of data regarding people or objects that have the potential to qualify as a military target, but is not qualified to automatically do the targeting.¹⁶⁶ On paper, the Israel Defense Forces (IDF) has emphasized that its analysts do not rely solely on Gospel's suggestions, and that its outputs are always reviewed by senior analysts to approve the target.¹⁶⁷ In addition to this, the IDF has admitted that the system does not assess potential collateral damage for a proportionality analysis,¹⁶⁸ raising the alarm in regards to compliance with rule 14 of customary IHL which is the principle of proportionality,¹⁶⁹ especially in cases of automation bias¹⁷⁰

¹⁶⁵ Harry Davies and Yuval Abraham, "Revealed: Israel Demanded Google and Amazon Use Secret 'Wink' to Sidestep Legal Orders", *The Guardian*, October 29, 2025, 09:15 EDT, <https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code>, accessed 30 April 2026.

¹⁶⁶ Michael N. Schmitt, "Israel – Hamas 2024 Symposium – The Gospel, Lavender, and the Law of Armed Conflict", Lieber Institute West Point, 28 June 2024, <https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/>, accessed 24 March 2026.

¹⁶⁷ Ibid

¹⁶⁸ Ibid

¹⁶⁹ ICRC, "Rule 14: Proportionality in Attack"

¹⁷⁰ Michael C. Horowitz and Lauren Kahn, "Bending the Automation Bias Curve: A Study of Human and AI-Based Decision Making in National Security Contexts", *International Studies Quarterly* 68, no. 2 (June 2024), <https://academic.oup.com/isq/article/68/2/sqae020/7638566>, accessed 18 May 2026.

where commanders consider AI outputs as the truth without verification. Lavender on the other hand is labeled as a “smart database” that sorts information on individuals who might be potential targets.¹⁷¹ And same as for Gospel, Lavender’s suggestions are not automatically approved according to the IDF, and they are governed by the same investigation procedures.¹⁷² Where is Daddy operates as a real-time location tracker, monitoring when a designated target enters their family residence so that a strike can be authorized at that moment, deliberately timing attacks to when families are present.¹⁷³

In theory, the IDF’s procedure of using both Gospel and Lavender seems compatible with the precautions needed to comply with IHL and IHRL, but does the actual practice match the theory? First we need to specify that the conflict between Israel and Gaza falls under occupation law as per the ICJ advisory opinion of 19 July 2024, which means that the conflict is mainly governed by the Fourth Geneva Convention, the Hague regulations, certain human rights treaties such as the ICCPR, and the Oslo Accords.¹⁷⁴ Even though Israel did not sign Additional Protocol 1, it is still bound by its customary rules particularly the principle of distinction and unnecessary suffering prohibition, as recognized by the ICJ in its *Legality of the Threat or Use of Nuclear Weapons Advisory Opinion*¹⁷⁵. The country is also bound by IHRL as affirmed by the ICJ in both its *Legality of the Threat or Use of Nuclear Weapons Advisory Opinion* (1996)¹⁷⁶ and its *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory Advisory Opinion* (2004).¹⁷⁷

According to a striking investigative report published by the Israeli Palestinian “+972” magazine and the Hebrew Language outlet “Local Call”, the IDF considered the outputs of its AI systems as

¹⁷¹ Michael N. Schmitt, “Israel – Hamas 2024 Symposium...”

¹⁷² Ibid

¹⁷³ The Economic Times, “How Israel Is Using ‘Lavender’ and ‘Daddy’ to Identify 37,000 Hamas Operatives”, April 9, 2024, 1:15 p.m. IST, <https://economictimes.indiatimes.com/news/defence/how-israel-is-using-lavender-and-daddy-to-identify-37000-hamas-operatives/articleshow/109155124.cms>, accessed 1 May 2026.

¹⁷⁴ International Court of Justice, *Legal Consequences Arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem*, Advisory Opinion, 19 July 2024, para. 3, <https://www.icj-cij.org/index.php/node/204160>, accessed 3 June 2026.

¹⁷⁵ International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*...

¹⁷⁶ Ibid

¹⁷⁷ International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*...

if they were human decisions after the events of October 7th.¹⁷⁸ The investigation mainly relied on the testimonies of six Israeli Intelligence Officers who were on active duty during the war on Gaza, and according to them, the army gave its approval for officers to adopt Lavender's kill lists without double checking or investigating the data.¹⁷⁹ More on this and according to the officers, the IDF made sure to attack most of its targets while they were at home, even if their families were present to make sure they would be there.¹⁸⁰

This practice directly implicates the customary principle of distinction, which requires that attacks be directed only at combatants.¹⁸¹ It also implicates the right to life under Article 6 of the ICCPR,¹⁸² considering the arbitrary loss of life caused by not checking the systems outputs, and waiting for targets to be at home with their families before striking them. The meaning here is that local production in this case disregarded human rights as a result of a political decision, and not as a result of reliance and operating the system itself.

Moreover, both Lavender and Gospel collect and analyze data from specific geographical locations, where people share similar living conditions, daily routines, and movement constraints under blockade.¹⁸³ In such area where the entire population is under continuous surveillance, an AI system trained on biased data against that population will face a high probability of flagging civilians as combatants because of the lack of variations in the data.¹⁸⁴ Considering that the IDF has historically designated entire categories of Palestinian civil society as hostile organizations¹⁸⁵, the risk of these designations and other biased data contaminating Lavender's training logic is not

¹⁷⁸ Yuval Abraham, "'Lavender': The AI machine..."

¹⁷⁹ Ibid

¹⁸⁰ Ibid

¹⁸¹ ICRC, "Rule 1: Principle of Distinction"

¹⁸² UN, ICCPR, art.6

¹⁸³ UNRWA, "Real Stories, Real Lives – What the Gaza Blockade Means", <https://www.unrwa.org/what-the-gaza-blockade-means>, accessed 1 May 2026

¹⁸⁴ Laura Bruun and Marta Bo, "'Constant Care' Must Be Taken to Address Bias in Military AI," ICRC Humanitarian Law & Policy Blog, August 28, 2025, <https://blogs.icrc.org/law-and-policy/2025/08/28/constant-care-must-be-taken-to-address-bias-in-military-ai/>, accessed 1 May 2026.

¹⁸⁵ Amnesty International, "Israel/OPT: Designation of Palestinian Civil Society Groups as 'Terrorists' a Brazen Attack on Human Rights", October 22, 2021, <https://www.amnesty.org/en/latest/news/2021/10/israel-opt-designation-of-palestinian-civil-society-groups-as-terrorists-a-brazen-attack-on-human-rights/>, accessed 1 May 2026.

speculative, but structural and highly probable, and can lead to breaching the customary principle of distinction, and the principle of non-discrimination in Articles 2 and 26 of ICCPR¹⁸⁶.

In addition to this, Chapter 2 identified the black box problem as one of the core risks of dependence on foreign AI systems, as a dependent state cannot audit the assumptions embedded in a foreign system, and cannot explain what went wrong when harm occurs. Israel, having built and trained Lavender and Gospel itself, does not face this problem in the same way, as it can in principle, access the internal logic of its own systems, trace how outputs were generated, and audit for bias. However, Israel might not be able to fully audit its systems, as like with all modern AI, Lavender and Gospel may still exhibit forms of opacity that even their developers cannot fully resolve. Despite this, having built the system offers Israel a genuine advantage that matters for accountability procedures, and proves that local production can have a positive impact on human rights outcomes when the system is effectively audited, as long as institutions are willing to act on it.

The Israeli military justice system contains several bodies, including the Military Advocate General's Corps (the MAG Corps), which is responsible for overseeing investigations and conducting prosecutions of alleged misconduct by IDF soldiers, and of alleged violations of IHL.¹⁸⁷ It also includes the Military Police Criminal Investigation Division (MPCID),¹⁸⁸ and military courts.¹⁸⁹ Civilian oversight also covers the IDF through the Attorney General of Israel, the Supreme Court, and the Independent Public Commission of Inquiry.¹⁹⁰

As of June 2025, Action on Armed Violence (AOAV) has found through an investigation, that Israel closes 88% of cases related to war crimes and abuses by its forces, without filing charges or finding wrongdoing¹⁹¹. Yesh Din, an Israeli NGO specialized in protecting the human rights of

¹⁸⁶ UN, ICCPR, art.2 and art. 26

¹⁸⁷ Israel Defense Forces (IDF) Editorial Team, "The IDF Military Justice System," updated August 20, 2024, <https://www.idf.il/en/mini-sites/military-advocate-generals-corps/the-idf-military-justice-system/>, accessed 1 May 2026.

¹⁸⁸ Ibid

¹⁸⁹ Ibid

¹⁹⁰ Ibid

¹⁹¹ Iain Overton and Lucas Tsantzouris, "88% of Israeli Investigations into Recent Gaza Abuse Allegations Stalled or Closed without Findings, with Just One Leading to Criminal Sentencing", Action on Armed Violence (AOAV),

Palestinians living under occupation found that only 0.9% of complaints between 2016 and 2024, ended with an indictment.¹⁹² UN Special Rapporteurs in Gaza, and UN experts warned that torture has become a state doctrine in Israel.¹⁹³ The former MAG in Israel was also arrested after leaking a video of Israeli soldiers sexually abusing a Palestinian detainee, and resigning from her post¹⁹⁴. The new MAG General Itai Ofir dropped the charges against the soldiers, and his decision was welcomed by Israeli right wing politicians.¹⁹⁵ This pattern shows that the formal accountability architecture exists in Israel, but it has been made largely inoperative through political pressure and deliberate obstruction. From a human security perspective, this matters because the people bearing the cost of that political choice are not the state, they are the civilians in Gaza whose safety was made subject to a system the state understood but chose not to limit.

In the end, the Israeli case revealed that foreign cloud dependence helped strip Palestinian civilians of legal protection over their own data. It also revealed that local systems, and despite the state's ability to audit them, were intentionally used without human oversight as part of a political and systematic choice. A positive human rights outcome could have been achieved, but was disregarded due to political considerations, making the Israeli case analytically important. The consequences of AI dependence are not the same for everyone, and this will become clearer in the next chapter, where we will see that the UAE faces a different kind of dependence, with different types of risks.

August 2, 2025, <https://aoav.org.uk/2025/88-of-israeli-investigations-into-recent-gaza-abuse-allegations-stalled-or-closed-without-findings-with-just-one-leading-to-criminal-sentencing/>, accessed 1 May 2026.

¹⁹² Yesh Din, Data Sheet: Duration of Processing of Complaints Concerning Israeli Soldiers' Offenses against Palestinians in the West Bank – 2016–2025 Data, December 30, 2025, <https://www.yesh-din.org/en/data-sheet-duration-of-processing-of-complaints-concerning-israeli-soldiers-offenses-en/>, accessed 1 May 2026.

¹⁹³ OHCHR, "UN Expert Warns Torture Has Become 'State Doctrine' in Israel, Making Prisons Instruments of Genocide and Torture," March 23, 2026, <https://www.ohchr.org/en/press-releases/2026/03/un-expert-warns-torture-has-become-state-doctrine-israel-making-prisons>, accessed 1 May 2026

¹⁹⁴ Matthew Doran, "Israel's military drops prosecution of reservists who allegedly raped Palestinian detainee", *ABC News*, 12 March 2026, <https://www.abc.net.au/news/2026-03-13/israel-idf-drops-sde-remain-reservist-palestinian-abuse-case/106449540>, accessed 1 May 2026.

¹⁹⁵ Ibid

Chapter 4: The UAE's AI Ambitions and the Depth of Its Dependencies

4.1 Wealth, Vision, and the Procurement Path: How the UAE Assembled Its Military AI Position Without Building Domestic Depth

The UAE chose to invest in military AI from a place of financial strength and political stability, driven by a leadership that wanted to turn the country into a regional and global power.¹⁹⁶ While this direction was set by leadership, the way it developed was shaped by the country's demographics, its geopolitical environment, and its economic capacity.

The UAE is a federation of seven emirates that came together in 1971 after six emirates reached an agreement to establish one sovereign country.¹⁹⁷ The seventh emirate acceded to the federation in 1972, forming what the world currently knows as the UAE.¹⁹⁸ The country's biggest economic strength was oil production, and it relied heavily on imported labor. With a citizen pool of less than 400,000 in 1971,¹⁹⁹ the UAE had to rely on external talent to build its economy, and it keeps on relying on them today with a total population of over 11 million people, and only around 1.4 million being actual Emirati citizens.²⁰⁰ Building a genuine domestic AI ecosystem requires decades of accumulated education and a scientific knowledge rooted in the citizen population itself, but the UAE's development model was built on imported expertise and external talent, which delivered speed and economic growth but contributed to limiting the development of domestic AI capabilities within the citizen population.

¹⁹⁶ "UAE Strategy for Artificial Intelligence", Telecommunication and Digital Government Regulatory Authority, <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-strategy-for-artificial-intelligence>, accessed 3 May 2026.

¹⁹⁷ Official website of the United Arab Emirates Ministry of Foreign Affairs, A brief outlook on the history of the United Arab Emirates <https://www.mofa.gov.ae/en/Missions/Athens/The-UAE/History>, accessed 3 May 2026

¹⁹⁸ Ibid

¹⁹⁹ Population Pyramids, "United Arab Emirates 1971", <https://www.populationpyramid.net/united-arab-emirates/1971/>, accessed 3 May 2026.

²⁰⁰ Liam Doherty, "How Many Emiratis are in UAE? – Population Figures", EmiratiStation Gate, 7 March 2025, <https://emiratisationgate.org/how-many-emiratis-are-in-uae/>, accessed 2 May 2026

Moreover, geopolitical events also shaped the style of the ecosystem that the UAE relies on today, and one of the primary security risks that the Gulf countries suffer from, comes from Iran and its militias. In 2014, Houthi insurgents, which are an Iran backed Shia group, took control of the Yemeni capital²⁰¹ posing a huge threat in the backdoor of the Sunni Gulf. To fight off the danger, the UAE joined the Arab coalition,²⁰² and purchased Wing Loong drones from China to deploy them in Yemen, while also relying on a variant of the American Predator XPs that were designed not to carry any munitions.²⁰³ The XPs were tailored to meet U.S. export requirements to the UAE, signaling an American distrust.

In terms of economy, the UAE is one of the wealthiest countries in the world,²⁰⁴ and it possesses 6% of the world's total oil reserve,²⁰⁵ and one of the world's largest sovereign wealth funds, the Abu Dhabi Investment Authority.²⁰⁶ These resources among others give the UAE the capacity to make large and sustained investments in technology, without the fiscal pressures that limit most states, and the country chose to use them to support AI investment. In October 2017, the UAE government launched its National Strategy for Artificial Intelligence, the first of its kind in the region and the world.²⁰⁷ It also established the world's first dedicated Ministry of State for Artificial Intelligence,²⁰⁸ and in 2019, it established the Mohamed bin Zayed University of Artificial Intelligence (MBZUAI) as the world's first graduate research university dedicated entirely to AI.²⁰⁹

²⁰¹ Kali Robinson, "Yemen's Tragedy: War, Stalemate, and Suffering", Council on Foreign Relations, 1 May 2023, <https://www.cfr.org/backgrounders/yemen-crisis>, accessed 3 May 2026

²⁰² Ibid

²⁰³ Paul Iddon, "Saudi Arabia And The UAE Are Acquiring Lots Of High-Tech Drones", *Forbes*, 9 August 2025, <https://www.forbes.com/sites/pauliddon/2025/08/09/saudi-arabia-and-the-uae-are-acquiring-lots-of-high-tech-drones/>, accessed 3 May 2026.

²⁰⁴ Luca Ventura, "Richest Countries in the World 2025", *Global Finance*, 3 September 2025, <https://gfmag.com/data/richest-countries-in-the-world/>, accessed 4 May 2026.

²⁰⁵ Worldometers, "United Arab Emirates Oil", 2025, <https://www.worldometers.info/oil/united-arab-emirates-oil/>, accessed 4 May 2026.

²⁰⁶ Sovereign Wealth Fund Institute, "Top 100 Largest Sovereign Wealth Fund Rankings by Total Assets", <https://www.swfinstitute.org/fund-rankings/sovereign-wealth-fund>, accessed 4 May 2026.

²⁰⁷ "UAE Strategy for Artificial Intelligence", Telecommunication and Digital Government...

²⁰⁸ UNESCO, "Minister of state for artificial intelligence", <https://www.unesco.org/creativity/en/policy-monitoring-platform/minister-state-artificial-intelligence>, accessed 4 May 2026.

²⁰⁹ Emirates News Agency – WAM, "Abu Dhabi announces establishment of the Mohamed bin Zayed University of Artificial Intelligence", 16 October 2019, <https://www.wam.ae/en/article/hszr9b3g-abu-dhabi-announces-establishment-the-mohamed-bin>, accessed 4 May 2026.

MBZUAI has contributed to science with over 3000 publications in top journals to date.²¹⁰ To further support its defense ambitions, the UAE established EDGE Group in November 2019, merging companies from across the Emirati defense sector into a single state owned group with an explicit mandate to reduce foreign reliance, and build sovereign defense production capacity.²¹¹

Taken together, we can see a clear and sustained national effort to build a military AI ecosystem, with the economic factor being the strongest tool in favor of the UAE. Despite this, the young Emirati institutions and dependence on imported talents significantly weakens the UAE's ability to reach autonomous production, and implies to a procurement model that we will analyse in the upcoming section.

4.2 Rich but Not Independent: Where UAE Investment Ends and Structural Dependence Begins

We have seen that the UAE possesses strong elements that can help it build a sovereign AI industry. With substantial wealth and vision, the country made strong efforts to build itself a competitive military AI ecosystem. But how sovereign it managed to make it, and how it affected its security decision making is something we will measure against the frameworks developed in Chapter 1 and 2.

The UAE is operating through a meritocratic model, with very little innovation coming from below. That model can work, but it requires a strong connection between the capacity to absorb external knowledge, and the capacity to actually use it domestically. The UAE's ability to access knowledge through procurement and imported talent is exceptionally high, but its ability to turn that knowledge into something it can independently build and audit is still limited. Constrained by how young its institutions are, and how thin its domestic technical base remains, the UAE is importing knowledge faster than it can produce.

²¹⁰ “MBZUAI Fact Sheet”, Mohamad Bin Zayed University of Artificial Intelligence, December 2025, https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fstaticcdn.mbzuai.ac.ae%2Fmbzuaiwpprd01%2F2025%2F12%2FSummarized_MBZUAI-Factsheet-Eng-Nov-2025_revised-1.docx&wdOrigin=BROWSELINK, accessed 4 May 2026.

²¹¹ Edge Group Official Website, About Us, <https://edgegroup.ae/about>, accessed 4 May 2026.

The MBZUAI example perfectly illustrates this as the university has recruited impressive but foreign faculty members from places like Carnegie Mellon and Berkeley,²¹² and out of its 650 students enrolled, only 17% of them are Emirati.²¹³ The numbers show that the university's model is dependent on importing human capital rather than growing it from within the citizen population, increasing the risk of that human capital leaving and choosing to work in different countries.

In terms of infrastructure, it is important to talk about one of the most important components of UAE military AI infrastructure which is EDGE Group. According to their website, the state owned company is dedicated to positioning the UAE as a “leading global hub for future industries”.²¹⁴ In 2024, EDGE’s revenue reached USD 4.9 billion,²¹⁵ and its international orders increased from USD 18.5 million in 2019 to over USD 2.1 billion in 2024,²¹⁶ which is genuinely impressive. But taking a look at what the internal and external sales comprises of, we can see that the overwhelming majority of products sold are not advanced AI solutions, but mostly traditional or regular technologically advanced weaponry. Of these, USD 1 billion comes from a contract with the Angolan Navy to produce Corvette Vessels, and over USD 1.5 billion comes from munition sales.²¹⁷ In terms of strictly advanced military AI, the company relies heavily on external partnerships with foreign companies to co-develop systems and access to core technologies.²¹⁸ While the company has developed a big capacity to assemble and produce complex AI systems, it still relies on joint ventures with established manufacturers like Leonardo,²¹⁹ where it works to develop products with elements already offered on the market.²²⁰ This indicates that many advanced systems are developed in partnership with external partners rather than independently.

²¹² “MBZUAI: Mohamed bin Zayed University of Artificial Intelligence”, Economic Vision 2030, <https://economicvision2030.com/encyclopedia/universities/mbzuai-profile/>, accessed 4 May 2026.

²¹³ MBUZAI Fact Sheet, Mohamad Bin Zayed University of Artificial Intelligence

²¹⁴ EDGE Group Official Website, About Us Section

²¹⁵ EDGE, “EDGE Group Marks Five Years of Innovation, Growth, and Global Success”, 9 December 2024, <https://edgegroup.ae/news/edge-group-marks-five-years-innovation-growth-and-global-success>, accessed 6 May 2026.

²¹⁶ Ibid

²¹⁷ Ibid

²¹⁸ EDGE Group Official Website, About Us Section

²¹⁹ Reuters, “Leonardo and EDGE to launch defence joint venture in UAE in 2026”, November 19, 2025, <https://www.reuters.com/business/aerospace-defense/leonardo-edge-launch-defence-joint-venture-uae-2026-2025-11-19/>, accessed 6 May 2026.

²²⁰ Ibid

Another layer of UAE dependence in the field of AI can be seen through the G42 case which is an Emirati company that offers AI solutions for different industries, in addition to cloud computing services and a wide range investments in the field.²²¹ G42 also implements and operationalizes key components of the UAE's AI strategy.²²² In April 2024, Microsoft invested USD 1.5 billion in G42 and the company committed to using Microsoft Azure as its platform for AI development and deployment.²²³ The deal came after pressure from the U.S. urging the company to cut its ties to Chinese military companies.²²⁴ This shows that the UAE's access to technology is many times conditional, and that external actors can use technology to influence Emirati security decision making.

Moreover, and in May 2025, G42 announced a project called Stargate and it is a 1-gigawatt AI compute cluster built by G42 in partnership with OpenAI, Oracle, Nvidia, Cisco, and SoftBank.²²⁵ The fact that the UAE is a major partner in this project and the fact that it sits on Emirati soil is a big achievement for the country and a step towards moving away from a pure cloud renting situation. Despite this, the agreement was developed in close coordination with the U.S. government,²²⁶ and includes a commitment by UAE entities to invest in U.S. Stargate infrastructure,²²⁷ in addition to requiring explicit American export authorization for the Nvidia chips it runs on,²²⁸ as U.S. officials expressed concerns that the UAE lacked sufficient institutional

²²¹ G42 Official Website, About G42 section, <https://www.g42.ai/about-g42-2026>, accessed 6 May 2026

²²² UECN, "The G42 Enigma: Inside the UAE's AI Champion and its Global Partnerships", September 27, 2025, <https://uecn.org/the-g42-enigma-inside-the-uaes-ai-champion-and-its-global-partnerships/>, accessed 6 May 2026.

²²³ Microsoft, "Microsoft invests \$1.5 billion in Abu Dhabi's G42 to accelerate AI development and global expansion", April 16, 2024, <https://news.microsoft.com/source/2024/04/16/microsoft-invests-1-5-billion-in-abu-dhabis-g42-to-accelerate-ai-development-and-global-expansion/?msoclid=0366bf639ea966eb1647a9759f1267a9>, accessed 6 May 2026.

²²⁴ House of Representatives Select Committee on China, "Gallagher Calls on USG to Investigate AI Firm, G42, Ties to PRC Military, Intelligence-Linked Companies", January 9, 2024, <https://chinaselectcommittee.house.gov/media/press-releases/gallagher-calls-usg-investigate-ai-firm-g42-ties-prc-military-intelligence>, accessed 6 May 2026.

²²⁵ Samantha Subin, "OpenAI, Oracle and NVIDIA will help build Stargate UAE AI campus launching in 2026", CNBC, May 22, 2025, <https://www.cnbc.com/2025/05/22/stargate-uae-openai-nvidia-oracle.html?msoclid=0366bf639ea966eb1647a9759f1267a9>, accessed 7 May 2025.

²²⁶ Open AI, "Introducing Stargate UAE", May 22, 2025, <https://openai.com/index/introducing-stargate-uae>, accessed 7 May 2025

²²⁷ Ibid

²²⁸ Reuters, "US authorizes export of advanced American semiconductors to companies in Saudi, UAE", November 20, 2025, <https://www.reuters.com/business/us-authorizes-export-advanced-american-semiconductors-companies-saudi-uae-2025-11-19>, accessed 7 May 2026.

capacity to prevent advanced American AI infrastructure from reaching Chinese entities. The infrastructure is on UAE soil, but the chips require American permission, the models are American, the operating partners are American, and the entire arrangement was structured under American government coordination, meaning in the end that the road to full sovereignty in the UAE in terms of infrastructure is still long.

The UAE also remains dependent on foreign AI chip producers that are required to train and help operate advanced AI systems.²²⁹ The country does not have an open access to these chips, and has to rely on foreign approval especially from the U.S. as we saw above. The UAE's ability to expand its domestic AI infrastructure depends not only on financial investment, but also on whether foreign governments continue to allow access to the necessary hardware.

The broader dependence on American cloud infrastructure and its effects on security were made visible in March 2026 when Iran targeted AWS data centers on UAE soil, disrupting cloud services across the country.²³⁰ The constant targeting experienced by the UAE showed that a state that builds its AI on foreign infrastructure has to accept the risks that come with dependency in both peacetime and wartime.

More on political conditionality, the UAE deals with the external pressure of both of the AI world leaders, China and the USA. The relationship with American firms means that access to the most advanced AI technologies comes with the condition of aligning with U.S. strategic preferences, and the G42 divestment from China is the clearest example of that. But the UAE also has a continued interest in Chinese technology, which means Beijing can still apply political pressure on the country. And the month after the Microsoft-G42 deal was announced, UAE President Sheikh Mohamed bin Zayed Al Nahyan traveled to China and described AI as an area of deeper UAE-

²²⁹ Chris Hamill-Stewart, "UAE seeks chip sovereignty with design-only approach", *Arabian Gulf Business Insight*, December 16, 2025, <https://www.agbi.com/analysis/ai/2025/12/uae-seeks-chip-sovereignty-with-design-only-approach/>, accessed 7 May 2026

²³⁰ Dennis Murphy, "Why Iran targeted Amazon data centers and what it means for future of warfare", *The Independent*, April 1, 2026, <https://www.independent.co.uk/news/world/middle-east/iran-amazon-data-centers-warfare-b2950213.html>, accessed 3 May 2026.

China collaboration,²³¹ which shows exactly how difficult it is for the UAE to fully commit to either partner without exposing itself to the other. Managing the relationship with the two leaders is itself a constraint on the UAE's ability to make autonomous decisions, and that constraint has not been reduced by any of the domestic investments the country has made so far.

In terms of data dependence, not many sources are available on the origins of the used data to train Emirati AI systems. One example manages to illustrate the issue and it is the Falcon Eye surveillance system set in Abu Dhabi, which was installed by an Israeli firm.²³² Because the system was developed outside the UAE, serious questions are posed about whether the data used reflects the population where it operates. This issue is relevant here because the UAE's population is made up of around 90% of non-citizens from regions including South Asia, Southeast Asia, and Africa,²³³ and research showed that facial recognition systems trained on non-representative datasets, produce higher error rates for darker-skinned populations.²³⁴ Whether these errors are reproduced inside the UAE is something that cannot be confirmed, because the country has no publicly documented mechanism for auditing the performance of foreign-sourced surveillance AI across its own population, which poses human rights concerns that we will tackle in section 4.4.

The UAE has invested heavily in AI development and has committed substantial resources to expanding its capabilities. However these investments do not appear to have changed the country's reliance on external actors and technologies. Despite progress in infrastructure and AI-related initiatives, important parts of the ecosystem remain dependent on foreign suppliers and systems. This creates a difference between developing AI capabilities and exercising independent control

²³¹ The National, "President Sheikh Mohamed Discusses Trade Relationship with China's Xi Jinping in Beijing", May 30, 2024, <https://www.thenationalnews.com/news/uae/2024/05/29/president-sheikh-mohamed-arrives-in-china-for-state-visit/>, accessed 6 May 2024.

²³² Rori Donaghy, "Falcon Eye: The Israeli-installed mass civil surveillance system of Abu Dhabi", *Middle East Eye*, July 15, 2015, <https://www.middleeasteye.net/news/falcon-eye-israeli-installed-mass-civil-surveillance-system-abu-dhabi>, accessed 7 May 2026.

²³³ World Population Review, "United Arab Emirates", <https://worldpopulationreview.com/countries/united-arab-emirates>, accessed 7 May 2026.

²³⁴ David Leslie, *Understanding Bias in Facial Recognition Technologies: An Explainer* (The Alan Turing Institute, 2020), https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf, accessed 7 May 2026

over them. The next sections examine what this may mean for security decision-making and human rights outcomes.

4.3 Does Procurement Translate into Power? Applying Morgenthau's Elements to the UAE's Military AI Position

In the previous sections, it was established that the UAE's military AI ecosystem has high levels of dependency, but it was also established that the Emirates is trying to beat this dependence by heavily investing in AI and building a local base for technology. In this section, we will see if the model adopted by the UAE, managed to increase the state power using Morgenthau's elements.

The geographical element for the UAE is both a strong and a weak point. In terms of strength, its location is to the southern border of the Strait of Hormuz²³⁵ where more than 20% of global oil and liquefied natural gas exports pass annually,²³⁶ giving the country a geopolitical weight. In terms of weakness, the same proximity to the Strait, also places it directly within the Iranian line of fire. This was seen and confirmed through the recent Iranian strikes on UAE soil.²³⁷ What those strikes revealed is that a country's physical location determines its exposure to risks and opportunities, but the character of its infrastructure determines the effects of that exposure on its benefits. The UAE's decision to build its AI strategy on foreign infrastructure increased the strategic vulnerabilities associated with its geographic position, and weakened the geographical element position as a determinant of state power.

Industrial capacity is where the procurement model shows its clearest limits, and this is established in section 4.2 with the EDGE group example. The company has grown and achieved genuine production capacity in domains like precision-guided munitions, but the transition from assembling and integrating foreign systems, to independently designing AI military platforms remains incomplete, simulating industrial capacity without actually building it. A state that can assemble or create advanced systems depending on the continued goodwill of its suppliers, cannot

²³⁵ John Misachi, "Strait Of Hormuz", *World Atlas*, March 4, 2021, <https://www.worldatlas.com/straits/strait-of-hormuz.html>, accessed 7 May 2026.

²³⁶ Ibid

²³⁷ Dennis Murphy, "Why Iran targeted Amazon data centers..."

solemnly rely on these systems to sustain its industrial capacity and advance the state power on the long run. Even if the momentary and short-term benefit is high, the long-term risk remains present.

In terms of population, the UAE faces big limitations as the country has a small citizen pool of around 1 million people, comprising around 10% of the residents in the country.²³⁸ Procurement can compensate for population limits in the short term by buying capability the citizen base cannot yet produce, but it cannot replace the decades of research culture and R&D investment needed to build genuine capability within the population. The procurement decision in the short term can support the population element as a determinant of state power, and the Emirati example perfectly proves this, but it cannot replace investing in the citizen pool for the development of autonomous capability.

In terms of military preparedness, the UAE is very well equipped to defend itself from attacks through procurement. In the recent war on Iran beginning on 28 February 2026, Iran retaliated against attacks by the U.S. and Israel by targeting American infrastructure in the region, and since the UAE hosts a lot of American infrastructure on its soil and has built many of its technological systems using that infrastructure, it became a major target for Iran. Nevertheless, the UAE managed to defend itself with a 96% interception rate²³⁹, using a multilayered system in which the American THAAD sits at the highest level to intercept ballistic missiles, the second level of defense relies on the American Patriot system, while the third level depends on the South Korean M-SAM and the Israeli Barak-8 systems, which are used against a diverse range of threats such as precision-guided munitions and drones. The fourth level relies on the Russian Pantsir-S1 system to counter low-altitude attacks, while the final layer depends on the SkyKnight system developed by the EDGE Group, with a range of 10 km.²⁴⁰

²³⁸ Liam Doherty, “How Many Emiratis are in UAE...”

²³⁹ Luigi Martino, “UAE Air Defense Network Stands Against Iranian Fire”, Trends Research & Advisory, March 15, 2026, <https://trendsresearch.org/insight/uae-air-defense-network-stands-against-iranian-fire/>, accessed 8 May 2026.

²⁴⁰ Ibid

What this shows is that Emirati air defense system is almost 90% dependent on procurement. Even though the installed system have highly increased the country's military preparedness in times of war, the risks it carries and the conditions attached to it can pose serious disadvantages in the long run, such as the refusal to provide interceptor missiles needed to operate them in case of political disputes. In 2021, the Biden Administration in the U.S. froze the sale of F-35 Lightning II warplanes to the UAE, out of fear that their use of Chinese 5G technology could compromise American technology through telecommunication channels,²⁴¹ and the U.S. sold the UAE a variant of the Predator XP that was specifically designed not to carry munitions.²⁴² Which proved in the end that while procurement can protect and increase military preparedness, it remains highly unreliable and risky in the long run.

In the end, and through Morgenthau's framework, it becomes clear that procurement can strengthen some elements of national power, especially military preparedness and geography, but these gains remain vulnerable to political decisions and supply disruptions outside the UAE's control. Moreover, it also becomes clear that procurement cannot support the elements that only domestic production and investing in local capabilities can produce over time, especially industrial capacity, and a strong technical talent base rooted in the citizen population. The UAE spent a lot of money trying to close that gap, and the gap is smaller than it was a decade ago. But it is still there, and it shows up every time a supplier attaches conditions to a sale, every time an interceptor stockpile runs low, and every time a foreign infrastructure decision made in Washington or Beijing reshapes what is possible in Abu Dhabi. The UAE's procurement model has made it a more capable state than its size and demographic base would otherwise allow, but power and sovereignty are not the same thing, and the difference between them is exactly what becomes visible when the conditions attached to a procurement relationship get activated.

²⁴¹ Elisabeth Gosselin-Malo, "Emirati F-35 prospects languish amid high-stakes Chinese, US courting", *Defense News*, May 1, 2024, <https://www.defensenews.com/global/mideast-africa/2024/05/01/emirati-f-35-prospects-languish-amid-high-stakes-chinese-us-courting/#:~:text=The%20Biden%20administration%20froze%20the%20sale%20of%20F%2035,Washington%20arms%20sales%20to%20its%20Middle%20East%20ally>, accessed 8 May 2026.

²⁴² Paul Iddon, "Saudi Arabia And The UAE Are Acquiring Lots Of High Tech Drones"

4.4 Procurement Without Recourse: How the UAE's Foreign AI Dependence Enables Repression and Forecloses Accountability

This section looks at the Emirati policing and surveillance AI ecosystem from a human rights lens to assess the impact of procurement on the lives of people whom the systems are deployed against. Due to the lack of data on Emirati military operations outside its borders, this section will look into the surveillance dimension of defense and security.

When a state builds its own systems, it not only owns them, but also understands how they work and can audit them to identify responsibility to some extent. Through this mechanism, a state can in principle be held responsible for any human rights breach caused by the AI system, but that does not mean that it will be in fact held responsible, especially in an authoritarian context. Still, the possibility of this to happen exists because the chain of responsibility stays within the country's own institutions and laws. When a state instead buys its surveillance capability from foreign companies, that chain breaks, as the tools were built by foreign parties, under foreign laws. In this case, the state using them gets the capability without the full responsibility, and the people being targeted by them face legal limitations if they sought to seek justice. That gap is what makes the UAE's dependence a human rights issue, not just a sovereignty one, and the examples below will illustrate this.

The UAE did not build its military and surveillance infrastructure from scratch, but it assembled it over years through a series of foreign deals and partnerships, adding more capability while bit by bit, removing more and more oversight.

In 2010, the UAE threatened to ban Blackberry services entirely because the data sent through Blackberry devices was processed through Research in Motion's servers (RIM) in Canada, outside UAE jurisdiction, meaning the government could not access it even if it wanted to.²⁴³ Emirati officials declared the devices a national security threat specifically because they operated beyond the reach of national laws and sent data abroad to be managed by a foreign commercial

²⁴³ Daniel Emery, "BlackBerrys pose 'security risk' say UAE authorities", *BBC*, 26 July 2010, <https://www.bbc.com/news/technology-10761210>, accessed 10 May 2026.

organization.²⁴⁴ What the UAE was frustrated about was not that its citizens' data was being held by a foreign company, but it was that it could not get to that data itself. This was not the first attempt either, as the UAE's state owned mobile operator Etisalat had already tried a year earlier to push spyware onto Blackberry users' phones disguised as a service upgrade, which RIM caught and removed.²⁴⁵ The Blackberry episode illustrates the compounded human rights problem that runs through the UAE's entire approach to foreign technology, as on one side, users' private data was sitting on foreign servers governed by foreign law, with no meaningful protection for the people it belonged to, and on the other side, the UAE was not worried about that at all as what it wanted was to access that data for itself, and it was willing to ban a device used by hundreds of thousands of people to get it. The foreign company held the data, the UAE wanted the surveillance, and the users had no say in either.

Rather than using its position to push foreign companies to protect its residents' data, the UAE consistently pushed them to hand it over, and when the technology made that impossible, it found other ways in. Project Raven was a secret team of former U.S. intelligence operatives recruited to help the UAE spy on governments, militants, and human rights activists seen as threats to the monarchy,²⁴⁶ with targets that quickly expanded to include a Saudi women's rights activist, who was imprisoned and tortured because of the leaked data.²⁴⁷ In 2016, the project moved inside DarkMatter, an Abu Dhabi cybersecurity firm run by UAE intelligence officials,²⁴⁸ where former NSA employees worked until 2019 before entering a prosecution agreement with the U.S. and paying over USD 1.6 Million in penalties for export control and hacking related violations.²⁴⁹ These people were never prosecuted in the UAE, and the people they surveilled had no clear and

²⁴⁴ Ibid

²⁴⁵ Ibid

²⁴⁶ Christofer Bing, and Joel Schectman, "Inside the UAE's Secret Hacking Team Of American Mercenaries", *Reuters Investigates*, January 30, 2019, <https://www.reuters.com/investigates/special-report/usa-spying-raven/>, accessed 10 May 2026

²⁴⁷ Connor Jones, "DarkMatter and former NSA officers sued over alleged phone hack of Saudi human rights activist", *IT Pro*, December 10, 2021, <https://www.itpro.com/security/hacking/361811/darkmatter-and-former-nsa-officers-sued-over-alleged-phone-hack-of-saudi>, accessed 10 May 2026.

²⁴⁸ Christofer Bing, and Joel Schectman, "Inside the UAE's Secret Hacking Team Of American Mercenaries"

²⁴⁹ Archives of the U.S Department of Justice, "Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More Than \$1.68 Million to Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign Government", September 14, 2021, <https://www.justice.gov/archives/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million>, accessed 10 May 2026.

explicit legal pathway to challenge foreign contractors working under UAE direction.²⁵⁰ The accountability gap was not something that developed by accident, but it was built into the law to protect the government from any liability.

Moreover, the UAE is not fully dependent in its surveillance operations and uses its own domestically produced systems to surveil people for both militarized and policing purposes. In December 2019, the New York Times revealed that ToTok, an Emirati messaging app that had been downloaded millions of times, was being used by the government to track the conversations, movements, locations, and contacts of everyone who installed it, with users believing it was simply a communications platform.²⁵¹ ToTok was not imported but was made by an Emirati company, marketed to Emirati and resident users, and deployed against millions of people without their knowledge, and yet no independent investigations were opened on this subject and no effective recourse was available for the millions of people whose data was taken without their consent. What ToTok shows, is that the UAE's accountability problem is not only about where its tools come from, but it is about a system that was built with challenging accountability mechanisms on purpose. Foreign dependence makes the problem worse, by adding legal complexity and jurisdictional distance that put responsibility even further out of reach, but the root of the problem is a government that never wanted to be held accountable in the first place, and ToTok is the clearest proof of that because it removes every possible excuse.

Finally, this section showed that the UAE is dealing with serious human rights violations most notably against the freedom of expression and the right to privacy. Despite deploying foreign military AI systems outside its borders, no audits or reports have been made to see if these systems caused civilian harm, and most of the reports come from the policing and surveillance sector. The UAE has a long history, as shown, of using both foreign and domestically built surveillance tools to monitor human rights activists and ordinary people. Some individuals targeted by surveillance

²⁵⁰ Ibrahim Sulieman Al Qatawneh, Wesam Almobaideen, and Mohammad Qatawneh, "A Comparative Study on Surveillance and Privacy Regulations (the UAE vs. the USA and the EU)," *Journal of Governance & Regulation* 11, no. 1 (2022), 6, file:///C:/Users/clair/Downloads/A_comparative_study_on_surveillance_and_privacy_re.pdf, accessed 17 May 2026.

²⁵¹ BBC, "Google and Apple remove alleged UAE spy app ToTok", December 23, 2019, <https://www.bbc.com/news/technology-50890846>, accessed 10 May 2026

were later imprisoned, and organizations including Human Rights Watch have described aspects of their detention and treatment as potentially amounting to torture.²⁵² The UAE is not a signatory of the ICCPR which limits the protection scope of its people further, and even though it signed the Arab Charter on Human Rights, the charter itself lacks any enforcement mechanisms to date.²⁵³ The UAE is in breach of the *jus cogens* prohibition against torture, and through procurement it allowed foreign companies to hold its population's data, beyond the reach of any domestic legal protection.

What the UAE case ultimately shows is that procurement is not the root cause of human rights violations, but it weakens the structural conditions that make accountability possible through competing jurisdictions. A government genuinely committed to protecting its people could have used the same leverage it applied to BlackBerry, to force data protection rather than data access. The UAE chose the opposite, and that choice repeated across every procurement decision this section examined, is what turned foreign AI dependence from a sovereignty problem into a human rights one.

Chapter 5: Different Paths, Shared Constraints: Comparing Israel and the UAE as Distinct Profiles of Military AI Dependence

5.1 History, Depth, and Time: Why Institutional Conditions, Not Resources, Explain the Gap Between Israeli and Emirati Military AI

Israel and the UAE, despite sharing similarities and a clear understanding of the importance of military AI for the future, leveraged their conditions in two different ways to join the AI race.

²⁵² Human Rights Watch, "UAE: Tolerance Narrative a Sham", October 1, 2021, <https://www.hrw.org/news/2021/10/01/uae-tolerance-narrative-sham-0>, accessed 10 May 2026.

²⁵³ Ahmed Almutawa, "The Arab Court of Human Rights and the Enforcement of the Arab Charter on Human Rights," *Human Rights Law Review* 21, no. 3 (September 2021): 510, <https://doi.org/10.1093/hrlr/ngab008>, accessed 28 May 2026.

Israel, driven by its need for survival, reduced its dependencies and became a genuine producer of military AI that the world's most powerful armies buy from, while the UAE, driven by a state strategy to increase its power, still faces major dependency problems. When a country buys foreign capability, the pressure to build it slowly from within starts to lose its urgency, and that difference in pressure is one of the reasons why the two countries ended up where they are on the dependency spectrum.

Alliance structures also play a role in explaining the position of the two countries. For Israel, its alliance with the United States, gave it preferential access to technology. However, this access did not come without restriction, as the U.S. enforced veto power over an Israeli arms sale, and enforced its own conditions on how their aid money could be spent. This double edged relationship provided Israel with access to advanced technology, but it also made it realize the importance of autonomous production. The UAE on the other hand, and unlike Israel, does not have as strong of a relationship with the U.S. which is translated through the strict conditions attached to any arm sale operation it conducts with them, meaning that the country's access to advanced technologies is limited with restrictions and political conditionalities. Moreover, the UAE's relationship with China means that the country bears the burden of balancing the relationship with the two opposing powers, adding an additional difficulty into its path.

The economic foundations of the two countries are both strong and both managed to build financial systems and a rule of law that support long term investment in advanced technologies. Despite this, the two countries ended up in very different positions on the dependence spectrum, and that alone shows that economic strength is a necessary condition to enter the field, but not what determines where a country ends up in it. Knowing how the elements of Chapter 2 interact together, a strong economy is a key driver of production, but it needs the strong presence of other elements for a country to reach its full potential in the field.

Historical legacies also help explain why countries start their journey from different positions, and in Chapter 2, we saw that colonial experiences can have long term effects on how strong a country's institutions become, and how fast it can innovate. Neither Israel, nor the UAE experienced colonialism in the same way as many countries in the Global South. Israeli lands were ruled by the

Ottomans and after by the British, but the people of Israel were scattered all around the world before being called into the new Jewish nation, hence they did not experience colonialism in their collective memory, and they came to build their country with international support and determination to build strong institutions. The UAE on the other hand only became a unified country in 1971 after being a British protectorate for decades, and being divided into several emirates with different rulers. This historical reality meant that the UAE was always going to start this journey later and from a different view of security. These different starting points shaped how both countries approached military AI, and are part of what explains why they ended up with such different dependence profiles today.

AI is a rapidly developing sector and it is built on decades of accumulated knowledge, knowledge that if a country does not realize itself will have to buy elsewhere, and in the realist geopolitical world we live in, no country will sell its knowledge fully, and put itself at risk of competition. Even if a country reaches the first wave of knowledge by itself, it will still be late facing countries that have years and years of knowledge and billions spent on R&D.

Israel started early, and its historical conditions helped it accumulate knowledge even from before the official independence of the state such as with the establishment of Israel Institute of Technology (Technion) in 1912.²⁵⁴ But the UAE started late, and it started not because of existential risks which reduce the pressure for sovereign production. MBZUAI and EDGE are also too young to have produced the kind of depth that takes decades of pressure to accumulate. The UAE is bringing in knowledge faster than it can make it its own, and as long as that gap exists, procurement will always feel like the more rational choice because it delivers results that domestic production cannot yet match.

Going back to the STI framework from Chapter 2, Wu and Huang argue that a state needs two things to actually build sovereign capability. It needs to be able to learn from external knowledge, and it needs to be able to turn that learning into something it can use, build on, and own

²⁵⁴ Jewish Virtual Library, “Higher Education in Israel: The Technion - Israel Institute of Technology”, <https://jewishvirtuallibrary.org/jsource/Education/technion.html>, accessed 28 June 2026.

domestically²⁵⁵. Israel already established that it excels in this through its decades of accumulated knowledge, but the UAE on the other hand showed a weaker RNAC potential.

In terms of the STI regime type, the two countries have significant differences as Israel operates through a democratic STI model, and the UAE operates through a meritocratic state-directed model. Both models can produce results, but as Chapter 2 showed, the democratic model tends to generate more organic and lasting innovation capacity, while the meritocratic model risks focusing too much on exploiting existing knowledge while neglecting the generation of new ones, which is exactly the gap the UAE is still working to close today. Civil-military collaboration is another area where the two countries show a deep difference. Israel built a direct pipeline between its military institutions and its private sector, where technically trained soldiers graduate into a competitive tech sector, and continues to solve defense problems there, while the UAE has invested in building this relationship through EDGE and a pipeline that does not run through its own citizens.

Investment in human capital shows one of the biggest gaps between Israel and the UAE, as for example in Israel, Unit 8200 has been running for decades, taking young Israelis, and putting them inside real operational problems, allowing the graduates to carry their experience into the private sector while never fully leaving the defense ecosystem behind.²⁵⁶ The UAE has no equivalent rooted in its own citizens, and MBZUAI has 650 students and only 17% of them are Emirati.²⁵⁷ The institution is real but the pipeline feeding it is mostly foreign, and imported talent leaves when better opportunities appear elsewhere, because nothing binds it to the country the way shared citizenship and a common security experience bind an Israeli graduate to their own country.

In terms of the relationship with private firms, Israel developed a domestic private tech sector where most of the firms producing military AI are Israeli, and their relationship with the state is rooted in shared institutions and law. For the UAE, the most important private actors in its AI ecosystem are foreign, and as Chapter 2 showed, a state that depends on foreign private firms for core defense functions is exposed to commercial decisions it cannot control. EDGE Group is a

²⁵⁵ Wu and Huang, “Why Do Some Countries Innovate Better than Others?”

²⁵⁶ Carmen Valache, “Israel’s Unit 8200, a Conveyor Belt of High-Tech Startups”

²⁵⁷ MBZUAI Fact Sheet, Mohamad Bin Zayed University of Artificial Intelligence

clear example of the UAE trying to move away from procurement, but a single company that mostly relies on foreign partnerships proved to be insufficient for real autonomous production.

Wealth can get a country into the military AI field, but it cannot shield the country from geopolitical tensions, or buy it time to produce local knowledge. Historical factors and economic conditions mostly determine which country can start and how strongly it can begin its journey, but it is up to political conditions, a strong private sector, and well maintained innovation ecosystems to determine how a country can sustain and deepen this journey. All elements of the framework developed in Chapter 2 are important to build and maintain a strong AI ecosystem, and all of these elements interact with each other, placing different countries on different locations on the dependence axis.

Usually, the distinction between states that produce military AI internally, and states that procure their systems from foreign countries is presented as a distinction between sovereign and dependent actors. But looking at Israel and the UAE, we can see that this binary does not hold, because both countries did not manage to fully escape structural dependence, but produced different dependence profiles.

5.2 Procurement and Production: Tools To Manage Dependence

It is true that Israel moved from procurement to production, and that it stopped depending on foreign firms to build its systems. But at the same time, Israel still depends on foreign companies for the most advanced semiconductors²⁵⁸ and cloud infrastructure,²⁵⁹ and depends on its political alignment with the U.S. for monetary aid, and to maintain intelligence cooperation and weapons supplies.²⁶⁰ What this shows is that the dependencies moved but did not disappear. For the UAE, the country accelerated the path of reaching an AI military ecosystem through procurement and

²⁵⁸ Mateus Lee, Ming-Hung Weng, and Show-Ling Jang, “The Competitiveness and Future Challenge of the Taiwan Semiconductors Industry”

²⁵⁹ Sam Mednick, Garance Burke, and Michael Biesecker, “How US Tech Giants Supplied Israel with AI Models, Raising Questions About Tech’s Role in Warfare”,

²⁶⁰ Jeremy M. Sharp, U.S. Foreign Aid to Israel: Overview and Developments since October 7, 2023

foreign partnerships.²⁶¹ That got the UAE capability fast, but the infrastructure underneath it remained externally owned, and externally controlled.

Dependence elements today run through the supply chain reaching infrastructure, software, maintenance and semiconductor access among other things. A state can produce a certain weapon, but it can also depend on a foreign company for the material needed for its production, it can also build a system but depend on foreign cloud infrastructure to store its data. This is what makes the comparison between Israel and the UAE important as it shows that production and procurement have become strategies to manage dependence and not to escape it.

Classical dependency theory predicted that moving from procurement to production is the way that countries must take to move from the cycle of dependence.²⁶² In our research, the UAE confirmed that staying in procurement deepens dependence, but Israel challenged that prediction, because even after building domestically, the chip supply and the cloud infrastructure, in addition to political conditionalities, remained outside its full control, and that is what makes military AI different from what the original theory was designed to explain.

Escaping dependence has become an unrealistic goal in the short to mid-term, especially for middle power states given the global AI structures. Hence, the goal changed to become managing dependence in order to have a better control over it and safeguard political and military agency. Israel has achieved some of this through production, and is on the right path to reduce its dependency further. The UAE on the other hand has not been able to achieve this goal through its procurement strategies and is pushing itself further into a dependence cycle. From the perspective of technological sovereignty, neither country achieved complete sovereignty, but Israel was able to exercise a higher degree of autonomous decision-making than the UAE. Both states depend on systems they do not fully control, and that dependence can be weaponized against them the moment geopolitical conditions shift.

²⁶¹ EDGE Group Official Website, About Us Section

²⁶² Charles A. Frankenhoff, "The Prebisch Thesis: A Theory of Industrialism for Latin America," *Journal of Inter-American Studies* 4, no. 2 (April 1962): 195, https://www.jstor.org/stable/pdf/165226.pdf?refreqid=fastly-default%3Aee49acba8d2c2a7b70787960375cc70c&ab_segments=&initiator=&acceptTC=1, accessed 29 June 2026.

5.3 Strategic Autonomy and Security Decision-Making Under Constraint: How Dependence Reshapes What States Can Actually Choose

Strategic autonomy is usually understood as the ability of states to pursue security goals independently and without external influence. Traditionally, and in order to protect autonomy, states used to work on increasing their power, which can be understood through Morgenthau's elements of national power. But with military AI, power no longer depends only on these traditional elements, as it also depends on access to technological systems that states do not fully control, and that is where the cases of Israel and the UAE reveal that strategic autonomy for middle powers in the age of AI is no longer about eliminating dependence, but about managing it in ways that preserve the state's ability to make security decisions independently.

Military AI can be understood as an emerging element that strengthens and sustains the traditional elements of national power. This AI needs to come from an autonomous production process to obtain the long term effects, because if obtained mostly through procurement, a surge in power can be observed for the short to mid-term period, with risks accumulating for the longer term. Hence, military AI contributes to strategic autonomy only when states retain meaningful control over the technologies on which these systems depend, otherwise, security decision making risks becoming partially shaped by the interests and conditions of suppliers.

In practice, each state that develops military AI will face a set of distinct limitations, for Israel, it is mostly political, even though the country faces some operational vulnerabilities related to infrastructure and supply chains, but for the UAE it is a more direct mix of political and operational restrictions. Here it is important to note that not all limitations are equally dangerous or limiting in nature, political constraints can be negotiated or gradually reduced over time, but operational limitations cannot be maneuvered so easily, because AI systems built on dependence might need access to foreign technologies, and partnerships, that are entangled to different forms of conditionalities.

Starting with Israel, domestic production gave the country genuine operational autonomy. For example, it decided to deploy Lavender and Gospel at operational scale during the war in Gaza,

without the need for foreign approval, while retaining control over the targeting logic and the operational parameters of these systems.²⁶³ Achieving this, is a direct product of building AI locally. However, operational autonomy does not automatically translate into full strategic autonomy. Political conditionalities still affect Israel as we saw with many examples especially the Phalcon veto case,²⁶⁴ showing that even highly capable producing states may face limitations on how they use or export their technologies. Moreover, and during the war on Gaza, the stockpile of the iron dome ran low during active conflict²⁶⁵ and required the United States to deploy its THAAD system as an additional layer of protection.²⁶⁶ A state that produces world class air defense systems, but needs a foreign ally to fill gaps during active war, has not achieved full strategic autonomy through production; it has achieved operational capability with conditions attached to it.

For the UAE, political autonomy is constrained by the relationship with AI leaders as we previously saw, and by the country's decision of building its AI on foreign platforms. The country initially tried to maintain a degree of distance from the Iran conflict in its early stages,²⁶⁷ but its dependence on foreign systems made neutrality difficult to sustain. Iran attacked Emirati soil aiming to target American and Israeli infrastructure,²⁶⁸ despite them being there to support Emirati capability. What this shows is that infrastructure dependence can transform the territory of a dependent state into a legitimate target during periods of geopolitical tension.

Coming to operational effects, the UAE's air defense is built almost entirely from foreign procurement,²⁶⁹ and its offensive weapons are also largely imported.²⁷⁰ The UAE is able to effectively defend itself against foreign attacks and also fight outside of its borders, and it proved

²⁶³ Roos Creighton, "The Lavender Precedent: Automated Kill Lists and the Limits of International Humanitarian Law," Action on Armed Violence (AOAV), November 6, 2025, <https://aoav.org.uk/2025/the-lavender-precedent-automated-kill-lists-and-the-limits-of-international-humanitarian-law/>, accessed 29 June 2026.

²⁶⁴ Nava Freiberg, "Israel Looks to Wean Itself Off..."

²⁶⁵ Joshua Nelken-Zitser, "Israel's Interceptor Missiles..."

²⁶⁶ Tom Bateman, "Why the US Is Sending Israel a Powerful..."

²⁶⁷ Sahim Salim, "Not party to his war..."

²⁶⁸ Dennis Murphy, "Why Iran targeted Amazon..."

²⁶⁹ Luigi Martino, "UAE Air Defense Network"

²⁷⁰ Robert Czulda, "UAE Transitions From Arms Importer to Competitor With the West", STIMSON, February 26, 2025, <https://www.stimson.org/2025/uae-transitions-from-arms-importer-to-competitor-with-the-west/>, accessed 15 May 2026.

so through joining the war on Yemen,²⁷¹ and defending its lands against the 2026 attacks by Iran.²⁷² Despite this, effectiveness does not equal independence, and that is because the used systems cannot be autonomously maintained, or replenished by the UAE, raising the alarm about the potential negative effects if one of the suppliers decided to stop a partnership, or attaches a certain conditionality for a sale process, potentially affecting its effectiveness in battlefield. What this means in practice is that Emirati security decision making remains conditioned by the preferences and availability of external suppliers.

Through this comparison we can see that both the UAE and Israel can make sovereign decisions and can decide who to partner with and who to buy from, but both of these countries face distinct limitations attached to these decisions. A state that depends on systems it cannot fully control, cannot achieve complete technological sovereignty, affecting its autonomy when the moment comes to make a security decision on its own terms. Reduced autonomy affects power by opening the door for foreign interference, and this is where Morgenthau's elements come into play again, because production and procurement both increase operational strength, but only production sustains strategic power for the long run.

In practice, Israel's most imminent risk is the iron dome stockpile dependence, and the longer term risk is related to cloud and chip dependency. Considering this, Israel needs to continue investing in its domestic interceptor production capacity, knowing from its historical lessons that it can be attacked from multiple locations and for a long period of time, and continue investing in sovereign cloud capacity for classified and sensitive data. Considering that the country does not have major natural resources to power cloud computing spaces, Israel needs to look into alternative power sources. Large AI companies are already securing nuclear energy agreements worth billions to power their systems, showing that energy capacity itself is becoming tied to technological autonomy, and Israel cannot afford to ignore this.²⁷³ Coming to the relationship with the U.S.,

²⁷¹ Kali Robinson, "Yemen's Tragedy"

²⁷² Luigi Martino, "UAE Air Defence..."

²⁷³ Jonathan Vanian, "Meta signs nuclear energy deals to power Prometheus AI supercluster", *CNBC*, January 9, 2026, <https://www.cnbc.com/2026/01/09/meta-signs-nuclear-energy-deals-to-power-prometheus-ai-supercluster.html?msockid=0366bf639ea966eb1647a9759f1267a9>, accessed 28 April 2026.

Israel is already planning to reduce U.S. aid dependence through a 10 year plan²⁷⁴, and continuing down this path will earn it a more powerful position in the geopolitical world. Finally, and regarding logic chips dependence, Israel cannot overcome this dependence in the short term considering that it is a worldwide bottleneck that no single country has been able to resolve yet,²⁷⁵ but it can continue to invest in R&D to reach a competitive edge in the field.

For the UAE, the biggest risk it is currently facing comes from building everything on foreign foundations, from procuring foreign weapons and defensive systems, to building local AI systems on foreign infrastructure, showing that the country needs a different approach, including investing more seriously in its own citizens, and increase Emirati participation in AI education institutions like MBZUAI. Imported talent leave when better opportunities appear elsewhere, and a country cannot build lasting technological depth on a workforce that is not rooted in it. The UAE needs to also direct serious investment toward domestically built cloud computing centers, taking advantage of its wealth in energy that can power the centers. Finally, the UAE needs to encourage a broader startup ecosystem around technology and logic chip development because competition is a driver of innovation, and state-owned entities alone cannot replicate it.

For middle powers more broadly, the lesson from both cases is the same in basis, a country seeking to increase its defense power needs to invest in locally produced AI, but the how becomes different depending on each country's resources and conditions. Dependence mapping needs to become a strategic priority on the same level as capability development, as countries such as Israel and the UAE discover their most dangerous vulnerabilities under operational pressure and not through forward planning, and a state that waits to discover its dependencies until they are activated has already lost some of its ability to manage them effectively.

²⁷⁴ Herb Keinon, "Netanyahu begins a farewell to US..."

²⁷⁵ Mateus Lee, Ming-Hung Weng, and Show-Ling Jang, "The Competitiveness and Future..."

5.4 Different Systems, Different Accountability Architectures: How the Form of Military AI Dependence Shapes Human Rights Risks and the Possibility of Remedy

To analyze the differences between the two profiles of Israel and the UAE, we will use the principles of IHRL, and IHL, including the Arab Charter, in addition to the Human Security Theory and the UN Guiding Principles on Business and Human Rights, known as the Ruggie Framework since existing scholarship has not addressed enough the role of private technology firms in enabling human rights violations connected to military AI.

Starting with the right to life, this right is protected under article 6 of the ICCPR,²⁷⁶ Article 5 of the Arab Charter,²⁷⁷ and under the principles of distinction, proportionality, and precaution under Articles 48, 51, 52 and 57 of Additional Protocol I of IHL.²⁷⁸ The use of defense AI in battle deeply challenges this protected right, and raises serious questions on whether foreign automated systems can decrease compliance with it. And to answer this dilemma it is important to look into whether the state deploying the system understands how it works.

For Israel, and since the country built its own AI systems such as Gospel and Lavender, it owns the right and the capability to audit them, despite the black box problem.²⁷⁹ In addition to this, Israel has developed specific mechanisms to deal with these systems to avoid automation bias and loss of civilian lives.²⁸⁰ Despite the policies created by the country to abide by the right to life, Israel allegedly treated the outputs of its automated systems as verified human decisions during

²⁷⁶ UN, *ICCPR*, art.6

²⁷⁷ Office of the United Nations High Commissioner for Human Rights and League of Arab States, Arab Charter on Human Rights, ST/HR/CHR/NONE/2004/40/Rev.1 (Geneva: Office of the United Nations High Commissioner for Human Rights, 2004), art.5, <https://digitallibrary.un.org/record/551368?v=pdf>, accessed 30 June 2026.

²⁷⁸ International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), adopted June 8, 1977, entered into force December 7, 1978, <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977>, accessed 30 June 2026.

²⁷⁹ Sarah H. Cen and Rohan Alur, “From Transparency to Accountability and Back: A Discussion of Access and Evidence in AI Auditing,” in Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO ’24) (New York: ACM, 2024), <https://dl.acm.org/doi/epdf/10.1145/3689904.3694711>, accessed 16 May 2026.

²⁸⁰ Michael N. Schmitt, “Israel – Hamas 2024 Symposium...”

the war on Gaza,²⁸¹ signaling that despite its ability to audit and despite the available mechanisms, it still chose to disregard human rights, not a result of dependence, but as a result of political decisions within the state. Meaning that local production can strengthen the conditions for protecting the right to life depending on political choice.

Coming to the UAE, the risk of breaching the right to life exists according to scientific research, and it may be amplified by the state dependence as in most cases procuring countries do not have a full access to the internal logic of systems they buy,²⁸² limiting their capability to perform thorough auditing actions. If AI outputs undercount civilian presence and cause an arbitrary loss of life, and if no auditing procedure was performed, machine failure could happen, resulting in more arbitrary loss of life, and a decreased compliance with the right to life protection.

Moreover, the Israeli systems are trained on conflict data related to the environment where they are deployed,²⁸³ whereas for the UAE, procuring means that many of its systems might have been trained on foreign unrelated data, which connects directly to the distributional shift problem identified in Chapter 1, that says if a system is trained on one conflict environment, it may classify civilians as threats in a completely different one.²⁸⁴ This signals that procurement may increase the risk of breaching the right to life, but in the case of the UAE and due to the lack of transparency, it becomes very difficult to obtain real data from their AI systems' usage, limiting the ability to connect theory with example.

In terms of the right to privacy, this right is protected under Article 17 of the ICCPR,²⁸⁵ and Article 21 of the Arab Charter²⁸⁶ and both Israel and the UAE violated it through their different dependence profiles. For Israel, violation came through the mass collection of data from civilians in Gaza, and its storage on foreign cloud infrastructure subject to the American CLOUD Act. The meaning of this is that the right to privacy was violated simultaneously by the collection itself, and

²⁸¹ Yuval Abraham, “‘Lavender’: The AI machine directing Israel’s bombing spree in Gaza”, *+972 Magazine*, In partnership with Local Call, April 3, 2024, <https://www.972mag.com/lavender-ai-israeli-army-gaza/>, accessed 1 June 2026.

²⁸² Abiade, “Algorithmic Sovereignty and New Security Dependencies”

²⁸³ Tal Mimran, Magda Pacholska, Gal Dahan, and Lena Trabucco, “Beyond the Headlines...”

²⁸⁴ Liu et al., “Bridging Distribution Shift...”

²⁸⁵ UN, ICCPR, art.17

²⁸⁶ OHCHR and League of Arab States, Arab Charter on human rights, art.21

by the legal framework governing where the data sat. For the UAE a similar story unfolds as the country also uses a mixture of local and foreign systems and clouds to surveil its population and activists.

In addition, the people living in the UAE, have no recourse to explicit legal channels to challenge mass surveillance, making access to justice very hard.²⁸⁷ Autonomously produced systems can offer a protection against breaching the right of privacy, if the breach is only coming from foreign built systems, but when it comes from locally made ones, political and legal systems will have to play the bigger role in safeguarding the right.

A dimension that cuts across both cases is the discriminatory impact of biased AI systems that especially affects Article 2 of the ICCPR,²⁸⁸ Article 3 of the Arab Charter,²⁸⁹ and the International Convention on the Elimination of All Forms of Racial Discrimination.²⁹⁰ As Chapter 1 explained, AI systems do not just reflect existing discrimination in their training data, but they amplify it, and can also create what is called algorithmically manufactured suspicion, that happens when an AI system takes several signals, none of which would count as evidence of a threat on their own, and combines them into a high confidence hostile designation.²⁹¹

For Israel, both Lavender and Gospel collect and analyze data from specific geographical locations, which as previously discussed can lead to a heightened probability of flagging civilians as combatants due to the lack of variations in the data.²⁹² Meaning that even with autonomously produced systems, danger to human rights is never entirely gone if other conditions are not met, and here data quality proves to be a major condition that needs to be seriously considered and checked before deployment of systems.

²⁸⁷ Al Qatawneh, Almobaideen, and Qatawneh, “Comparative Study on Surveillance...”

²⁸⁸ UN, ICCPR, art.2

²⁸⁹ OHCHR and League of Arab States, Arab Charter on human rights, art.3

²⁹⁰ United Nations General Assembly, International Convention on the Elimination of All Forms of Racial Discrimination, adopted December 21, 1965, entered into force January 4, 1969, Resolution 2106 (XX), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial>, accessed 30 June 2026

²⁹¹ Laura Bruun and Marta Bo, “Bias In Military Artificial Intelligence...”

²⁹² Ibid

For the UAE no publicly available data explain how its military and surveillance systems were trained, but considering that the country operates both locally made and foreign systems, and considering that universally speaking, the research concludes that facial recognition systems produce significantly higher error rates for darker-skinned individuals when trained on non-representative datasets,²⁹³ then the probability of misidentification of the UAE's South Asian and African population remains high.

Both states also face serious concerns under the Convention Against Torture²⁹⁴ and Article 7 of the ICCPR,²⁹⁵ and Article 8 of the Arab Charter,²⁹⁶ considering that the right against torture carries jus cogens status and cannot be derogated from under any circumstances. UN Special Rapporteurs and as previously mentioned, warned that torture has become state doctrine in Israel in the context of the Gaza war, and Human Rights Watch also as previously mentioned, described aspects of detention and treatment in UAE prisons as potentially amounting to torture. When AI systems are used to identify individuals as targets, and those individuals are then detained or killed under conditions that may involve torture or unlawful treatment, then the AI system that generated the initial designation becomes part of the chain of harm. By analyzing this through the lens of production versus procurement, we can see that local production improves the state capacity to protect human rights through auditing procedures. Procurement is not a direct reason for torture but it shapes its form, and makes access to remedy more difficult with decreased auditing capabilities.

In terms of the Ruggie Framework, it establishes three pillars, of which one is the state duty to protect against human rights abuses by business enterprises, two is the corporate responsibility to respect human rights, and three is access to remedy.²⁹⁷ For Israel, the Nimbus contract clauses that prevented Google and Amazon from restricting how their products were used, even when that use

²⁹³ David Leslie, "Understanding bias..."

²⁹⁴ United Nations General Assembly, Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, adopted December 10, 1984, entered into force June 26, 1987, Resolution 39/46, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-against-torture-and-other-cruel-inhuman-or-degrading>, accessed 30 June 2026.

²⁹⁵ UN, ICCPR, art.7

²⁹⁶ OHCHR and League of Arab States, Arab Charter on human rights, art.8

²⁹⁷ Ruggie, *Protect, Respect and Remedy...*

breached their own terms of service, show a direct failure of the state duty to protect, and a failure of the private companies to respect human rights. Access to remedy is also contested in the Israeli case, showing a total failure to respect human rights. For the UAE, and through the examples we saw in section 4.3, the UAE almost never requires a human rights assessment to be done by their partners, and it does not provide explicit legal pathways for remedy against them, failing to sustain the protection mechanisms to safeguard its population.

Going through all of these violations, we can see that the human security theory is in many places in tension with how AI is being currently handled. The UNDP's 1994 Human Development Report, argued that security is only meaningful if it extends to the personal, community, and political dimensions of human life, which shifts the focus from the protection of states, to the protection of individuals.²⁹⁸ Both Israel and the UAE invested in military AI systems that increased their security, but decreased the security of individuals within, or under their control, and a state that is strategically strong but whose residents are surveilled and exposed to biased systems, and are further from any meaningful remedy is not more secure. It has simply moved the costs of its security onto the people least able to resist them.

What Israel and the UAE show together is something that neither case reveals alone, which is that production and procurement do not just produce different strategic profiles, but they produce different human rights architectures, that can fail or protect their people through different mechanisms. For Israel, local production made accountability possible but it remained tied to political choices, and for the UAE, increased dependence made accountability harder to reach. Even if political will existed in the Emirates, jurisdictional complexity would make reaching justice more complicated, showing the negative effect of dependence on human rights.

In terms of what this means for policy, reforms in both Israel and the UAE are needed as well as changes in policy at the international level to make sure that harm against human rights is reduced when AI systems are deployed. Beginning with Israel, the changes needed are political, because the accountability channels already exists, but what is missing is the political will to let it function without interference. The MAG Corps, the MPCID, the Attorney General, and the Supreme Court

²⁹⁸ UNDP, *Human Development Report...*

all have the capacity to function as meaningful oversight mechanisms, but their action has been limited through political pressure coming from inside the country.

For the UAE, domestic reform alone is not enough because the accountability problem is mostly connected to actors beyond the borders of the country. For this reason, the changes needed extend to the international level, where suppliers are needed to exercise better quality control over the machine learning process.

Moreover, the UN Human Rights Council should consider addressing the human rights obligations of states and firms developing, and deploying AI in military and surveillance contexts through due diligence reporting, and a clear complaint mechanism capable of providing remedy to affected populations.

Conclusion

The aim of this research was to offer an understanding of why some states are able to innovate in the world of military technology better than others, despite having comparable resources or even sometimes lower defense budgets than others, in addition to demonstrating that even countries that manufacture and sell defensive AI, can still suffer from dependencies throughout their supply chain, producing distinct dependence profiles from procuring states, with each showing unique effects on autonomy, security decision making, and human rights. Israel and the UAE were chosen as case studies for the research, considering their comparable resources, geopolitical locations, and opaque human rights systems.

In terms of the roots of reliance preventing an effective domestic military AI production environment in a certain country, this research identified several interconnected ones that work together to explain why some states build domestic military AI ecosystems, while others depend on foreign suppliers. Historical and economic conditions showcase that countries subjected to colonialism face complex barriers in building a strong rule of law and advanced economic systems, directly affecting their innovation capabilities. Political environments, especially threat perception act as significant drivers for a country to start innovating and autonomously develop its own

systems to minimize outside risk. Other than threat, alliance structures are key to which country can reach technology faster than the others, and to which country can protect itself from limitations and export controls. Institutional conditions are also important especially having a system that can learn from outside knowledge, and has the capacity to replicate it and add to it, and a strong civil military relation to help technology flow from the private sector to the military institution. Identifying these elements answered sub-question one, and provided a comprehensive perspective on why some countries manage to innovate better than others, regardless of wealth and ambitions.

Israel and the UAE acted as the case study to illustrate that the roots of reliance exhibited in the three discussed elements are real and applicable, and that even when a country manages to overcome some of them, it can still face distinct challenges when depending on foreign infrastructure, data, and actors, making escaping dependence a very hard goal, and showing that the challenge for states is no longer eliminating dependence altogether, but managing it in ways that reduce its costs.

Israel showed that it managed dependence primarily through domestic production, driven by a long term plan supported with substantial R&D investments. Despite this the country still suffers from infrastructure dependence and political conditionalities, but in a more limited and measurable way, showing a more controlled dependence profile. The UAE on the other hand managed dependence through procurement and partnership building to expand its capabilities, but this strategy also pushed the country into deeper external dependence.

The research also found that dependence limits autonomy and security decision making differently, depending on the profile of the dependent country. Political conditionality is the most immediately felt, as the Phalcon veto and the G42 divestment both showed that it can be activated the moment interests between the dependent and the stronger country becomes evident, limiting the capacity of the weaker country to make full autonomous decisions regarding its security. Infrastructure dependence is the hardest to exit, because rebuilding autonomously after decades of depending on foreign cloud and foreign chips can take a lot of time and a lot of money. Data dependence is the most invisible when it comes to impacting autonomy, and therefore the hardest to manage because

of the opacity of AI systems and the limited auditing procedures that can be done by dependent states.

Dependence also affects human rights, and the case studies showed that the form dependence takes shapes how human rights violations occur and how clearly they get amplified. Depending on foreign cloud systems to store data can result in breaching the right to privacy, and depending on biased or inappropriate data on the battlefield where it is deployed can cause arbitrary loss of life, breaching the right to life and the concepts of proportionality and distinction in IHL. Dependence on private firms can also amplify human rights risks as no worldwide binding mechanism exists today to enforce auditing procedures on the quality of data used in machine learning, and on how the company's products are used after being sold. Israel demonstrated that production alone is not enough, and that a country can leverage its power and autonomy over its data, to purposefully discriminate against a certain group, while the UAE showed that procurement can intensify the risks surrounding human rights protection, especially when the political system favors self-preservation over protection. In that sense, dependence increases the intensity of human rights vulnerabilities, and amplifies risks already associated with AI itself, shaping both how violations occur and how accountability is distributed.

This research contributes to current scholarship by drafting a framework on the roots of reliance, which can be used to analyze the status of countries on the axis of production and procurement, and explain why they are in their position and how they can overcome it. The research also included technology and private companies into dependency theory to highlight their importance as players in the field, which is something that is fairly understudied, and used Morgenthau's elements of power to provide a more modern view of the military landscape today. Finally, the research contributed by making a connection between the form of military AI dependence and the kind of human rights accountability failures it produces, linking international relations debates on autonomy to human rights scholarship in a way that existing research has not fully developed.

Ultimately, this thesis showed that dependence is not something that can be simply escaped, but a condition to be reduced and managed to avoid its negative effects not only on state autonomy and decision making, but also on the rights of people that the AI systems are meant to protect.

Bibliography

A

- 1- Abiade, Sheriffdeen Folaranmi. “Algorithmic Sovereignty and New Security Dependencies: How Foreign AI Surveillance Reshapes Global Power”. *World Journal of Advanced Research and Reviews* 27, no. 2 (2025): 162–180. <https://doi.org/10.30574/wjarr.2025.27.2.2845>.
- 2- Abraham, Yuval. ““Order from Amazon’: How tech giants are storing mass data for Israel’s war”. +972 Magazine, In partnership with Local Call. August 4, 2024. <https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/>
- 3- Abraham, Yuval. ““Lavender’: The AI machine directing Israel’s bombing spree in Gaza. +972 Magazine, In partnership with Local Call. April 3, 2024. <https://www.972mag.com/lavender-ai-israeli-army-gaza/>
- 4- Abdullahi, Aminu. “Global Divide: Only 32 Countries Host AI Data Centers.” *TechRepublic*. June 23, 2025. <https://www.techrepublic.com/article/news-only-32-countries-host-data-centers-2025/>
- 5- Abdallah, Nayera. “UAE-based G42 working with US to meet AI standards amid China concerns”. *Reuters*. August 1, 2024. <https://www.reuters.com/technology/uae-based-g42-working-with-us-meet-ai-standards-amid-china-concerns-2024-08-01>
- 6- Ahronheim, Anna. “Israel’s Semiconductor Sector Powers \$40B in Chip Exits.” *The Jerusalem Post*. November 4, 2025. <https://www.jpost.com/business-and-innovation/article-872760>
- 7- Alexander. “Defense Budget by Country 2026: Global Rankings and Insights.” *Military Compare*. February 28, 2026. <https://militarycompare.com/defense-budget-by-country-2025/>.
- 8- Allen, Gregory C. *Choking off China’s Access to the Future of AI: New U.S. Export Controls on AI and Semiconductors Mark a Transformation of U.S. Technology Competition with China*. Center for Strategic and International Studies. October 11, 2022. <https://www.csis.org/analysis/choking-chinas-access-future-ai>.

- 9- Almutawa, Ahmed. "The Arab Court of Human Rights and the Enforcement of the Arab Charter on Human Rights". *Human Rights Law Review* 21. no. 3 (September 2021): 510.
<https://doi.org/10.1093/hrlr/ngab008>
- 10- Al Qatawneh, Ibrahim Sulieman, Wesam Almobaideen, and Mohammad Qatawneh. "A Comparative Study on Surveillance and Privacy Regulations (the UAE vs. the USA and the EU)." *Journal of Governance & Regulation* 11, no. 1 (2022),
file:///C:/Users/clair/Downloads/A_comparative_study_on_surveillance_and_privacy_re.pdf
- 11- Amazon Web Services. "What Is Cluster Computing?". <https://aws.amazon.com/what-is/cluster-computing/>
- 12- Amazon Web Services. "AWS Israel (Tel Aviv) Region".
<https://aws.amazon.com/local/israel/>
- 13- Amnesty International. "Israel/OPT: Designation of Palestinian Civil Society Groups as 'Terrorists' a Brazen Attack on Human Rights". October 22, 2021.
<https://www.amnesty.org/en/latest/news/2021/10/israel-opt-designation-of-palestinian-civil-society-groups-as-terrorists-a-brazen-attack-on-human-rights/>
- 14- Andry, Aurélie Dianara. "The 'Social Dimension' of Postwar Europe." In *Social Europe, the Road Not Taken: The Left and European Integration in the Long 1970s*, 27–59. Oxford: Oxford University Press, 2022.
<https://doi.org/10.1093/oso/9780192867094.003.0002>
- 15- Aravantinos, Elias. "The Fusion of Technology and Defense: Israel's Military-Technology Complex". *Strategy International*. November 21, 2024.
<https://strategyinternational.org/2024/11/21/publication150/>.
- 16- Aronsson, Lisa A. *What Next for the Third Offset Strategy?*. CRS In Focus IF10790. Washington, DC: Congressional Research Service, December 13, 2017.
<https://www.congress.gov/crs-product/IF10790>
- 17- Archives of the U.S Department of Justice. "Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More Than \$1.68 Million to Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign

- Government". September 14, 2021. <https://www.justice.gov/archives/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million>
- 18- Ashdown, Neil. "Unity or Coherence: Shaping Future Civil-Military Intelligence Collaboration in the Cyber Domain". In *CyCon 2024: Over the Horizon*, 16th International Conference on Cyber Conflict, edited by C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, and D. Štrucl, 311–25. Tallinn: NATO CCDCOE Publications, 2024. https://ccdcoe.org/uploads/2024/05/CyCon_2024_Ashdown-1.pdf.

B

- 19- Bateman, Tom. "Why the US Is Sending Israel a Powerful Thaad Anti-Missile System." *BBC News*. October 15, 2024. <https://www.bbc.com/news/articles/c39le0dp4p7o>.
- 20- BBC. "Google and Apple remove alleged UAE spy app ToTok". December 23, 2019. <https://www.bbc.com/news/technology-50890846>
- 21- Benito, Andrea. "Saudi Arabia Launches \$100 Billion AI Initiative to Lead in Global Tech." *CIO*. November 12, 2024. <https://www.cio.com/article/3602900/saudi-arabia-launches-100-billion-ai-initiative-to-lead-in-global-tech.html>.
- 22- Bergmann, Dave. "What is machine learning?". *IBM*. <https://www.ibm.com/think/topics/machine-learning>.
- 23- Beinín, Joel. "Israel's Economy Has Problems, but It's Not Collapsing Yet." *Jacobin*. February 21, 2026. <https://jacobin.com/2026/02/israel-economy-tech-weapons-trade>
- 24- Bienvenue, Emily, et al. "Private Tech Companies, the State, and the New Character of War." *Carnegie Endowment for International Peace*. December 1, 2025. <https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies>
- 25- Bing, Christofer and Scheetman Joel. "Inside the UAE's Secret Hacking Team Of American Mercenaries". *Reuters Investigates*. January 30, 2019. <https://www.reuters.com/investigates/special-report/usa-spying-raven/>
- 26- Bômônt, Clotilde. *Technical Is Political: When a Cloud Certification Scheme Divides Europe*. Paris: European Union Institute for Security Studies, November 3, 2025.

- <https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe>.
- 27- Boulanin, Vincent, Lora Saalman, Petr Topychkanov, Fei Su, and Moa Peldán Carlsson. *Artificial Intelligence, Strategic Stability and Nuclear Risk*. (Stockholm: Stockholm International Peace Research Institute, June 2020).
https://www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf.
- 28- Boston Consulting Group. “Geopolitics and Generative AI: Will Middle Powers Reshape the Map?”. Press release. December 9, 2024.
<https://www.bcg.com/press/9december2024-geopolitics-genai-middle-powers-reshape-map>.
- 29- Bonaglia, Davide, Lorena Rivera León, and Sacha Wunsch-Vincent. “End of Year Edition – Against All Odds, Global R&D Has Grown Close to USD 3 Trillion in 2023.” World Intellectual Property Organization (WIPO) – Global Innovation Index Blog. December 18, 2024. <https://www.wipo.int/en/web/global-innovation-index/w/blogs/2024/end-of-year-edition>
- 30- British Army. *British Army’s Approach to Artificial Intelligence*. October 2023.
https://www.army.mod.uk/media/24745/20231001-british_army_approach_to_artificial_intelligence.pdf.
- 31- Britannica Editors. “Semiconductor.” *Encyclopedia Britannica*. History section.
<https://www.britannica.com/science/semiconductor>
- 32- Britannica Editors. “Software.” *Encyclopedia Britannica*. May 22, 2026.
<https://www.britannica.com/technology/software>
- 33- Bruun, Laura, and Bo, Marta. *Bias in Military Artificial Intelligence and Compliance with International Humanitarian Law*. Stockholm: Stockholm International Peace Research Institute. August 2025. https://www.sipri.org/sites/default/files/2025-08/0825_ai_military_bias.pdf.

- 34- Bruun, Laura and Bo, Marta. “‘Constant Care’ Must Be Taken to Address Bias in Military AI”. ICRC Humanitarian Law & Policy Blog. August 28, 2025. <https://blogs.icrc.org/law-and-policy/2025/08/28/constant-care-must-be-taken-to-address-bias-in-military-ai/>
- 35- Bruun, Laura, and Marta Bo. “‘Constant Care’ Must Be Taken to Address Bias in Military AI.” ICRC Humanitarian Law & Policy Blog. August 28, 2025. <https://blogs.icrc.org/law-and-policy/2025/08/28/constant-care-must-be-taken-to-address-bias-in-military-ai/>

C

- 36- Caster, Micheal. “The Global Implications of China’s 5-Year Plan AI Ambitions”. The Diplomat. March 27, 2023. <https://thediplomat.com/2026/03/the-global-implications-of-chinas-5-year-plan-ai-ambitions/>
- 37- Cen, Sarah H., and Rohan Alur. “From Transparency to Accountability and Back: A Discussion of Access and Evidence in AI Auditing.” In Proceedings of the 4th ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO 24). New York: ACM, 2024. <https://dl.acm.org/doi/epdf/10.1145/3689904.3694711>
- 38- Chang, Grace and Heidi, Grant. “When AI Amplifies the Biases of Its Users”. *Harvard Business Review*. 23 January 2026. <https://hbr.org/2026/01/when-ai-amplifies-the-biases-of-its-users>
- 39- Clapp, Sebastian. Defence and Artificial Intelligence. European Parliamentary Research Service. PE 569.580 (April 2025). https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI%282025%29769580_EN.pdf
- 40- Cohen, Jared, and George Lee. “The Generative World Order: AI, Geopolitics, and Power.” Goldman Sachs Global Institute. December 14, 2023. <https://www.goldmansachs.com/insights/articles/the-generative-world-order-ai-geopolitics-and-power>

- 41- Conrad, Jennifer. “Anthropic, Amazon, and Palantir Team Up to Bring AI to the Defense Department.” *Inc.* November 8, 2024. <https://www.inc.com/jennifer-conrad/anthropic-amazon-and-palantir-team-up-to-bring-ai-to-the-defense-department/91001401>
- 42- Creyghton, Roos. “The Lavender Precedent: Automated Kill Lists and the Limits of International Humanitarian Law.” Action on Armed Violence (AOAV). November 6, 2025. <https://aoav.org.uk/2025/the-lavender-precedent-automated-kill-lists-and-the-limits-of-international-humanitarian-law/>
- 43- Czulda, Robert. “UAE Transitions From Arms Importer to Competitor With the West”. STIMSON. February 26, 2025. <https://www.stimson.org/2025/uae-transitions-from-arms-importer-to-competitor-with-the-west/>

D

- 44- Davies, Harry, and Yuval Abraham. “Revealed: Israel Demanded Google and Amazon Use Secret ‘Wink’ to Sidestep Legal Orders”. *The Guardian*. October 29, 2025. <https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code>
- 45- Defense Advanced Research Projects Agency (DARPA). “Explainable Artificial Intelligence (XAI)”. <https://www.darpa.mil/research/programs/explainable-artificial-intelligence>.
- 46- Doran, Matthew. “Israel's military drops prosecution of reservists who allegedly raped Palestinian detainee”. *ABC News*. 12 March 2026. <https://www.abc.net.au/news/2026-03-13/israel-idf-drops-sde-temain-reservist-palestinian-abuse-case/106449540>
- 47- Doherty, Liam. “How Many Emiratis are in UAE? – Population Figures”. EmiratiStation Gate. 7 March 2025. <https://emiratisationgate.org/how-many-emiratis-are-in-uae/>
- 48- Donaghy, Rori. “Falcon Eye: The Israeli-installed mass civil surveillance system of Abu Dhabi”. *Middle East Eye*. July 15, 2015. <https://www.middleeasteye.net/news/falcon-eye-israeli-installed-mass-civil-surveillance-system-abu-dhabi>

E

- 49- EDGE Group Official Website. About Us. <https://edgegroup.ae/about>
- 50- EDGE. “EDGE Group Marks Five Years of Innovation, Growth, and Global Success”. December 9, 2024. <https://edgegroup.ae/news/edge-group-marks-five-years-innovation-growth-and-global-success>
- 51- Elath, Eliahu and Britannica Editors. “Establishment of Israel”. Encyclopedia Britannica. April 23, 2026. <https://www.britannica.com/place/Israel/Establishment-of-Israel>
- 52- Emery, Daniel. “BlackBerrys pose 'security risk' say UAE authorities”. *BBC*. July 26, 2010. <https://www.bbc.com/news/technology-10761210>
- 53- Emirates News Agency – WAM. “Abu Dhabi announces establishment of the Mohamed bin Zayed University of Artificial Intelligence”. 16 October 2019. <https://www.wam.ae/en/article/hszr9b3g-abu-dhabi-announces-establishment-the-mohamed-bin>
- 54- European Parliamentary Research Service. *Defence and Artificial Intelligence*. EPRS Briefing 769580. Brussels: European Parliament, 2025. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI%282025%29769580_EN.pdf

F

- 55- Fabian, Emanuel. “Israeli Arms Sales Break Record for 4th Year in Row, Reaching \$14.8 Billion in 2024”. *The Times of Israel*. June 4, 2025. <https://www.timesofisrael.com/israeli-arms-sales-break-record-for-4th-year-in-row-reaching-14-8-billion-in-2024/>
- 56- Flynn, Curran. 2016. “Political Geography and Morgenthau’s Early American Works.” *Cambridge Review of International Affairs* 29 (4): 1582–1602. <https://www.tandfonline.com/doi/full/10.1080/09557571.2016.1241757>
- 57- Freiberg, Nava. “Israel Looks to Wean Itself Off US Aid, but Breaking Free Could Cost Both Sides.” *The Times of Israel*. February 13, 2026.

<https://www.timesofisrael.com/israel-looks-to-wean-itself-off-us-aid-but-breaking-free-could-cost-both-sides/>

- 58- Frankenhoff, Charles A. "The Prebisch Thesis: A Theory of Industrialism for Latin America". *Journal of Inter-American Studies* 4, no. 2 (1962): 185–206.

<https://www.jstor.org/stable/165226>

G

- 59- George, Mathew, Katarina Djokić, Zain Hussain, Pieter D. Wezeman, and Siemon T.

Wezeman. *Trends in International Arms Transfers, 2024*. Stockholm: SIPRI, March 2025. https://www.sipri.org/sites/default/files/2025-03/fs_2503_at_2024_0.pdf

- 60- Gosselin-Malo, Elisabeth. "Emirati F-35 prospects languish amid high-stakes Chinese, US courting". *Defense News*. May 1, 2024.

<https://www.defensenews.com/global/mideast-africa/2024/05/01/emirati-f-35-prospects-languish-amid-high-stakes-chinese-us-courting/#:~:text=The%20Biden%20administration%20froze%20the%20sale%20of%2050,Washington%20arms%20sales%20to%20its%20Middle%20East%20ally>

- 61- Guzzini, Stefano. "Hans J. Morgenthau and the Three Purposes of Power". DIIS Working Paper 2018:4. <https://research.diis.dk/da/publications/hans-j-morgenthau-and-the-three-purposes-of-power/>

- 62- G42 Official Website. About G42 section. <https://www.g42.ai/about-g42-2026>

H

- 63- Hacıoğlu, Sila Özeren. "APT29 Explained: Cozy Bear's Evolution, Techniques, and Notorious Cyber Attacks." *Picus Security*. Last updated April 6, 2026.

<https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques>

- 64- Hamill-Stewart, Chris. "UAE seeks chip sovereignty with design-only approach". *Arabian Gulf Business Insight*. December 16, 2025.

- <https://www.agbi.com/analysis/ai/2025/12/uae-seeks-chip-sovereignty-with-design-only-approach/>
- 65- Hassija, Vikas, Vinay Chamola, Atmesh Mahapatra, Abhinandan Singal, Divyansh Goel, Kaizhu Huang, Simone Scardapane, Indro Spinelli, Mufti Mahmud, and Amir Hussain. “Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence.” *Cognitive Computation* 16, no. 1 (2024): 45–74. <https://doi.org/10.1007/s12559-023-10179-8>.
- 66- Heimann, Gadi. “Israeli-Franco relations and the crisis of May to June 1967, in Franco-Israeli Relations”. 1958–1967. 1st ed. (Routledge, 2016). <https://www.taylorfrancis.com/chapters/mono/10.4324/9781315604688-18/israeli-franco-relations-crisis-may-june-1967-gadi-heimann?context=ubx>
- 67- Henshall, Will. “There’s an AI Lobbying Frenzy in Washington. Big Tech Is Dominating”. *TIME*. April 30, 2024. <https://time.com/6972134/ai-lobbying-tech-policy-surge/>
- 68- “How AI Is Enhancing Military Surveillance and Border Security”. *Defence Industries*. <https://www.defence-industries.com/articles/how-ai-is-enhancing-military>.
- 69- “How military AI systems can be attacked and misled”. *Swedish Defense Research Institute*. August 22, 2023. <https://www.foi.se/en/foi/news-and-pressroom/news/2023-08-22-how-military-ai-systems-can-be-attacked-and-misled.html>
- 70- House of Representatives Select Committee on China. “Gallagher Calls on USG to Investigate AI Firm, G42, Ties to PRC Military, Intelligence-Linked Companies”. January 9, 2024. <https://chinaselectcommittee.house.gov/media/press-releases/gallagher-calls-usg-investigate-ai-firm-g42-ties-prc-military-intelligence>
- 71- Horowitz, Michael C., and Kahn, Lauren. “Bending the Automation Bias Curve: A Study of Human and AI-Based Decision Making in National Security Contexts”. *International Studies Quarterly* 68. no. 2 (June 2024). <https://academic.oup.com/isq/article/68/2/sqae020/7638566>
- 72- Human Rights Watch. “UAE: Tolerance Narrative a Sham”. October 1, 2021. <https://www.hrw.org/news/2021/10/01/uae-tolerance-narrative-sham-0>

73- Hummel, Patrik, et al. “Data Sovereignty: A Review.” *Big Data & Society* 8, no. 1 (January–June 2021): 7. <https://doi.org/10.1177/2053951720982012>

I

74- Iddon, Paul. “Saudi Arabia And The UAE Are Acquiring Lots Of High-Tech Drones”. *Forbes*, 9 August 2025. <https://www.forbes.com/sites/pauliddon/2025/08/09/saudi-arabia-and-the-uae-are-acquiring-lots-of-high-tech-drones/>

75- International Court of Justice. *Legality of the Threat or Use of Nuclear Weapons*. Advisory Opinion of July 8, 1996. *I.C.J. Reports* 1996. <https://www.icj-cij.org/case/95>

76- International Court of Justice. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*. Advisory Opinion of July 9, 2004. *I.C.J. Reports* 2004. <https://www.icj-cij.org/case/131>

77- International Court of Justice, *Legal Consequences Arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem*, Advisory Opinion, 19 July 2024, para. 3, <https://www.icj-cij.org/index.php/node/204160>

78- International Monetary Fund. *Money Matters, an IMF Exhibit—The Importance of Global Cooperation, Destruction and Reconstruction (1945–1958)*”. https://www.imf.org/external/np/exr/center/mm/eng/mm_dr_01.htm

79- International Committee of the Red Cross (ICRC). “Rule 1: The Principle of Distinction between Civilians and Combatants.” *International Humanitarian Law Database*. <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule1>

- 80- International Committee of the Red Cross (ICRC). “Rule 14 – Proportionality in Attack”. International Humanitarian Law Database. <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule14>
- 81- International Committee of the Red Cross. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). adopted June 8, 1977. entered into force December 7, 1978. <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977>
- 82- Insikt Group, "Iran's AI Ambitions: Balancing Economic Isolation with National Security Imperatives", Recorded Future, April 17, 2025, <https://www.recordedfuture.com/research/irans-ai-ambitions-balancing-economic-isolation-national-security-imperatives>
- 83- Iqbal, Shahid, Syed Wajeeh Abbas Rizvi, Muhammad Hasnain Haider Malik, and Saqib Raza. “Artificial Intelligence in Security and Defense: Explore the Integration of AI in Military Strategies, Security Policies, and Its Implications for Global Power Dynamics.” *International Journal of Human and Society* 3, no. 4 (2023): 341–353. https://www.researchgate.net/profile/Hasnain-Haider-13/publication/377177943_Artificial_Intelligence_in_Security_and_Defense_Explore_the_integration_of_AI_in_military_strategies_security_policies_and_its_implications_for_global_power_dynamics/links/659829ce6f6e450f19ce3a28/Artificial-Intelligence-in-Security-and-Defense-Explore-the-integration-of-AI-in-military-strategies-security-policies-and-its-implications-for-global-power-dynamics.pdf

84- Israel Central Bureau of Statistics. The National Expenditure on Civilian R&D 2023.

Media Release 320/2024 (Jerusalem: Israel CBS, October 8, 2024).

https://www.cbs.gov.il/he/mediarelease/DocLib/2024/320/12_24_320e.pdf

85- Israel Innovation Authority. “Israel Innovation Authority 2025 High-Tech Report”. Press Releases. September 17, 2025.

https://innovationisrael.org.il/en/press_release/innovation-report-2025/

86- Israel Ministry of Defense. “Israel Sets New Record in Defense Exports: Over \$14.7 Billion in 2024.” Ministry of Defense Press Releases. April 6, 2025.

<https://www.mod.gov.il/en/press-releases/press-room/israel-sets-new-record-in-defense-exports-over-147-billion-in-2024>

87- Israel Defense Forces (IDF) Editorial Team. “The IDF Military Justice System.”

Updated August 20, 2024. <https://www.idf.il/en/mini-sites/military-advocate-generals-corps/the-idf-military-justice-system/>

J

88- Jerusalem Post Staff. “A Global Powerhouse: The Current State of Israel’s Semiconductor Start-Up Ecosystem.” The Jerusalem Post. September 29, 2025.

<https://www.jpost.com/business-and-innovation/article-868925>

89- Jewish Virtual Library, “Higher Education in Israel: The Technion - Israel Institute of Technology”, <https://jewishvirtuallibrary.org/jsource/Education/technion.html>

90- Jonker, Alexandra, and Julie Rogers. “What Is Algorithmic Bias?”. IBM. <https://www.ibm.com/think/topics/algorithmic-bias>

91- Jones, Connor. “DarkMatter and former NSA officers sued over alleged phone hack of Saudi human rights activist”. *IT Pro*. December 10, 2021.

<https://www.itpro.com/security/hacking/361811/darkmatter-and-former-nsa-officers-sued-over-alleged-phone-hack-of-saudi>

- 92- Junerfält, Tobias. *South Korea's Push for Defense Semiconductor Self-Sufficiency*. FOI Memo 8937. Stockholm: Swedish Defence Research Agency. September 2025. <https://www.foi.se/rest-api/report/FOI%20Memo%208937>

K

- 93- Keinon, Herb. "Netanyahu begins a farewell to US military aid - analysis". *The Jerusalem Post*. January 12, 2026. <https://www.jpost.com/israel-news/defense-news/article-883141>
- 94- King, Ian, Debby Wu, and Demetrios Pogkas. "How a Chip Shortage Snarled Everything From Phones to Cars". *Bloomberg*. March 29, 2021. <https://www.bloomberg.com/graphics/2021-semiconductors-chips-shortage/>
- 95- Kumari, Nikita. "Semiconductor Materials Sourcing: Securing the Supply Chain Behind the Chips." *BISinfotech*. August 18, 2025. <https://www.bisinfotech.com/semiconductor-materials-sourcing-securing-the-supply-chain-behind-the-chips/>.
- 96- Kvangraven, Ingrid Harvold. "Dependency Theory: Strengths, Weaknesses, and Its Relevance Today." In *A Modern Guide to Uneven Economic Development*. January 2023. https://www.researchgate.net/publication/367336288_Dependency_theory_strengths_weaknesses_and_its_relevance_today

L

- 97- Lee, Mateus, Ming-Hung Weng, and Show-Ling Jang. "The Competitiveness and Future Challenge of the Taiwan Semiconductors Industry." In *Technology Rivalry Between the USA and China*, edited by Peter C. Y. Chow, 161–206. Palgrave Studies in Global Security. Cham: Palgrave Macmillan, 2025. https://link.springer.com/chapter/10.1007/978-3-031-76169-0_6

- 98- Leslie, David. *Understanding bias in facial recognition technologies: An Explainer*. The Alan Turing Institute. 2020. https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf
- 99- Liu, Chenruo, Kenan Tang, Yao Qin, and Qi Lei. “Bridging Distribution Shift and AI Safety: Conceptual and Methodological Synergies.” *arXiv*, preprint 2505.22829v2, last revised June 18, 2026. <https://arxiv.org/pdf/2505.22829>

M

- 100- Manzi, Graeme. “Revolutionising Defence Intelligence, Surveillance & Reconnaissance (ISR) with AI”. *Karve International*. 13 February 2024. [Revolutionising Defence Intelligence, Surveillance & Reconnaissance \(ISR\) with AI](#).
- 101- Martino, Luigi. “UAE Air Defense Network Stands Against Iranian Fire”. *Trends Research & Advisory*. March 15, 2026. <https://trendsresearch.org/insight/uae-air-defense-network-stands-against-iranian-fire/>
- 102- Mayer, Maximilian, and Yen-Chi Lu. “Global Structures of Digital Dependence and the Rise of Technopoles.” *New Political Economy* 30, no. 5 (2025): 755–774. <https://doi.org/10.1080/13563467.2025.2497766>.
- 103- “MBZUAI Fact Sheet”. Mohamad Bin Zayed University of Artificial Intelligence. December 2025. https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fstaticcdn.mbzuai.ac.ae%2Fmbzuaiwpprd01%2F2025%2F12%2FSummarized_MBZUAI-Factsheet-Eng-Nov-2025_revised-1.docx&wdOrigin=BROWSELINK
- 104- “MBZUAI: Mohamed bin Zayed University of Artificial Intelligence”. *Economic Vision 2030*. <https://economicvision2030.com/encyclopedia/universities/mbzuai-profile/>
- 105- McFaul, Cole, Sam Bresnick, and Daniel Chou. “Pulling Back the Curtain on China’s Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage”. *Center for Security and Emerging Technology*. September 2025. <https://cset.georgetown.edu/publication/pulling-back-the-curtain-on-chinas-military-civil-fusion/>.

- 106- Mednick, Sam, Garance Burke, and Michael Biesecker. "How US Tech Giants Supplied Israel with AI Models, Raising Questions About Tech's Role in Warfare." *AP News*. Updated February 18, 2025. <https://apnews.com/article/israel-palestinians-ai-weapons-430f6f15aab420806163558732726ad9>
- 107- Microsoft. "Palantir and Microsoft Partner to Deliver Enhanced Analytics and AI Services to Classified Networks for Critical National Security Operations". August 8, 2024. <https://news.microsoft.com/source/2024/08/08/palantir-and-microsoft-partner-to-deliver-enhanced-analytics-and-ai-services-to-classified-networks-for-critical-national-security-operations/>
- 108- Microsoft. "Microsoft invests \$1.5 billion in Abu Dhabi's G42 to accelerate AI development and global expansion". April 16, 2024. <https://news.microsoft.com/source/2024/04/16/microsoft-invests-1-5-billion-in-abu-dhabis-g42-to-accelerate-ai-development-and-global-expansion/?msockid=0366bf639ea966eb1647a9759f1267a9>
- 109- Mimran, Tal, Magda Pacholska, Gal Dahan, and Lena Trabucco. "Israel - Hamas 2024 Symposium - Beyond the Headlines: Combat Deployment of Military AI-Based Systems by the IDF." Lieber Institute West Point. February 2, 2024. <https://lieber.westpoint.edu/beyond-headlines-combat-deployment-military-ai-based-systems-idf/>
- 110- Misachi, John. "Strait Of Hormuz". *World Atlas*. 4 March 2021. <https://www.worldatlas.com/straits/strait-of-hormuz.html>
- 111- Munro, André. "Dependency theory." Encyclopaedia Britannica. <https://www.britannica.com/topic/dependency-theory>
- 112- Murphy, Dennis. "Why Iran targeted Amazon data centers and what it means for future of warfare". *The Independent*. April 1, 2026. <https://www.independent.co.uk/news/world/middle-east/iran-amazon-data-centers-warfare-b2950213.html>

- 113- NASA, “Defining Artificial Intelligence”, <https://www.nasa.gov/what-is-artificial-intelligence/>.
- 114- NATO. Summary of NATO’s Revised Artificial Intelligence (AI) Strategy. 10 July 2024. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
- 115- Naughton, John. “The Evolution of the Internet: From Military Experiment to General Purpose Technology.” *Journal of Cyber Policy*. 2016: 5–28. https://www.academia.edu/93607010/The_evolution_of_the_Internet_from_military_experiment_to_General_Purpose_Technology
- 116- Nelken-Zitser, Joshua. “Israel’s Interceptor Missiles Are Under Pressure as Threats Loom Larger.” *Business Insider*. October 15, 2024. <https://www.businessinsider.com/israel-interceptor-missiles-shortage-iran-threats-loom-large-iron-dome-2024-10>.
- 117- Nicol-Schwarz, Kai, and Emma Graham. “Banking, Payments Services Disrupted After Amazon UAE Data Centers Hit in Drone Strikes.” *CNBC*. March 3, 2026. <https://www.cnn.com/2026/03/03/iran-war-uae-drone-strikes-aws-data-centers.html>.

O

- 118- Official website of the United Arab Emirates Ministry of Foreign Affairs. A brief outlook on the history of the United Arab Emirates. <https://www.mofa.gov.ae/en/Missions/Athens/The-UAE/History>
- 119- Office of the United Nations High Commissioner for Human Rights and League of Arab States. Arab Charter on Human Rights. ST/HR/CHR/NONE/2004/40/Rev.1 (Geneva: Office of the United Nations High Commissioner for Human Rights, 2004). <https://digitallibrary.un.org/record/551368?v=pdf>
- 120- OHCHR. “BHR Treaty Process”. <https://www.ohchr.org/en/business-and-human-rights/bhr-treaty-process>

- 121- Oluyemi, Opeoluwa Adisa. “The Military Uses of Artificial Intelligence (AI) and Their Implications on International Security.” *International Journal of Research and Innovation in Social Science* 8, no. 3S (2024): 1084–1098. June 7, 2024. <https://dx.doi.org/10.47772/IJRISS.2024.803075S>.
- 122- Open Source AI Review Editorial Team. “Why Your AI Provider Switch Will Cost More Than You Think”. Open Source AI Review. April 16, 2026. <https://www.opensourceaireview.com/blog/why-your-ai-provider-switch-will-cost-more-than-you-think>
- 123- Open AI. “Introducing Stargate UAE”. May 22, 2025. <https://openai.com/index/introducing-stargate-uae>
- 124- Organization for Economic Co-operation and Development (OECD). “Gross Domestic Spending on R&D”. OECD Data Indicators. <https://www.oecd.org/en/data/indicators/gross-domestic-spending-on-r-d.html>
- 125- Overton, Iain, and Lucas Tsantzouris. “88% of Israeli Investigations into Recent Gaza Abuse Allegations Stalled or Closed without Findings, with Just One Leading to Criminal Sentencing”. Action on Armed Violence (AOAV). August 2, 2025. <https://aoav.org.uk/2025/88-of-israeli-investigations-into-recent-gaza-abuse-allegations-stalled-or-closed-without-findings-with-just-one-leading-to-criminal-sentencing/>

P

- 126- PolSci Institute. “The Uneven Path of Democracy in Post-Colonial Nations.” Last updated October 18, 2025. <https://polsci.institute/political-processes-institutions/uneven-path-of-democracy-post-colonial-nations/>
- 127- Population Pyramids. “United Arab Emirates 1971”. <https://www.populationpyramid.net/united-arab-emirates/1971/>

Q

R

- 128- Real Country Sizes, “Real Size Of Israel: How Small Israel Actually Is? (USA Is Almost 500x Bigger)”, <https://realcountrysizes.com/true-size-of-israel/>
- 129- Rebeiz, Mireille. “Israeli threats to occupy or annex south Lebanon dust off a decades old playbook”. *The Conversation*. April 8, 2026. <https://theconversation.com/israeli-threats-to-occupy-or-annex-south-lebanon-dust-off-a-decades-old-playbook-279704>
- 130- Reuters. “Leonardo and EDGE to launch defence joint venture in UAE in 2026”. 19 November 2025. <https://www.reuters.com/business/aerospace-defense/leonardo-edge-launch-defence-joint-venture-uae-2026-2025-11-19/>
- 131- Reuters. “US authorizes export of advanced American semiconductors to companies in Saudi UAE”. November 20, 2025. <https://www.reuters.com/business/us-authorizes-export-advanced-american-semiconductors-companies-saudi-uae-2025-11-19>
- 132- Robinson, James A., and Daron Acemoglu. “The Economic Impact of Colonialism.” Center for Economic Policy and Research. January 30, 2017. <https://cepr.org/voxeu/columns/economic-impact-colonialism>
- 133- Robinson, Kali. “Yemen’s Tragedy: War, Stalemate, and Suffering”. Council on Foreign Relations. 1 May 2023. <https://www.cfr.org/backgrounders/yemen-crisis>
- 134- Ruggie, John Gerard. *Protect, Respect and Remedy: A Framework for Business and Human Rights: Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises*. A/HRC/8/5. (Geneva: United Nations, April 7, 2008). <https://digitallibrary.un.org/record/625292?v=pdf>
- 135- Ryngaert, Cedric. “Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts.” *German Law Journal* 24, no. 3 (May 2023): 544–546. <https://doi.org/10.1017/glj.2023.24>

S

- 136- Salim, Sahim. “Not party to this war’: UAE position on Iranian attacks explained in 9 points”. *Khaleej Times*. March 4, 2026. <https://www.khaleejtimes.com/uae/iran-attacks-uae-not-part-of-war-calls-for-dialogue-position-explained-in-9-points>
- 137- Schmitt, Michael N. “Israel – Hamas 2024 Symposium – The Gospel, Lavender, and the Law of Armed Conflict”. Lieber Institute West Point. 28 June 2024. <https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/>
- 138- Science News Today Editorial Team. “15 Most Incredible Uses of AI in Military Technology”. Science News Today. October 9, 2025. <https://www.sciencenewstoday.org/15-most-incredible-uses-of-ai-in-military-technology>
- 139- Semiconductor Raw & Refined Materials.” *SemiconductorX*. <https://semiconductorx.com/semiconductor-raw-materials.html>.
- 140- Seeds, Micheal. “Policy Points: The Balance of Protecting IP and Data Rights”. *National Defense Magazine*. October 4, 2024. <https://www.nationaldefensemagazine.org/articles/2024/10/4/policy-points-the-balance-of-protecting-ip-and-data-rights>
- 141- Sicherman, Harvey. “Establishment of Israel”. Encyclopedia Britannica, June 17, 2026, <https://www.britannica.com/place/Israel/Establishment-of-Israel>
- 142- Shishodia, Dhruv. “The Role of AI in Cloud Platforms – AWS, Azure, and Google Cloud Compared.” *ThinkCloudly*. November 12, 2025. <https://thinkcloudly.com/blog/the-role-of-ai-in-cloud-platforms-aws-azure-and-google-cloud-compared/>
- 143- Sharoni, Yehuda. “First Israeli Sovereign Cloud Launched amid Rise in Information Economy.” *The Jerusalem Post*. April 12, 2023. <https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-739033>
- 144- Sharp, Jeremy M. U.S. Foreign Aid to Israel: Overview and Developments since October 7, 2023. RL33222. Washington, DC: Congressional Research Service, May 28, 2025. https://www.congress.gov/crs_external_products/RL/PDF/RL33222/RL33222.51.pdf
- 145- Shakhboz Juraev. “EDA Industry in the US–China Tech War: De Americanization and Sinification of the EDA Industry in China.” *Technology Global*

- (Substack). August 22, 2024. <https://technologyglobal.substack.com/p/eda-industry-in-the-us-china-tech>
- 146- Sovereign Wealth Fund Institute. “Top 100 Largest Sovereign Wealth Fund Rankings by Total Assets”. <https://www.swfinstitute.org/fund-rankings/sovereign-wealth-fund>
- 147- Startup Nation Central. “Israel’s Tech Sector Surpassed \$12 Billion in Funding in 2024, Solidifying Its Role as a Scale-Up Powerhouse, According to New Report.” PR Newswire, January 16, 2025. <https://www.prnewswire.com/il/news-releases/israels-tech-sector-surpassed-12-billion-in-funding-in-2024-solidifying-its-role-as-a-scale-up-powerhouse-according-to-new-report-302353152.html>
- 148- Subin, Samantha. “OpenAI, Oracle and NVIDIA will help build Stargate UAE AI campus launching in 2026”. *CNBC*. May 22, 2025. <https://www.cnbc.com/2025/05/22/stargate-uae-openai-nvidia-oracle.html?msockid=0366bf639ea966eb1647a9759f1267a9>
- 149- Susnjara, Stephanie, Mesh Flinders, and Ian Smalley. “What Is AI Infrastructure?” *IBM Think*. Published June 3, 2024. Updated April 8, 2026. <https://www.ibm.com/think/topics/ai-infrastructure>
- 150- Suss, Gavin. “The Role of IDF and the Israeli Military Industry in the Technological and Economic Development of Israel”. *Research Papers on Knowledge, Innovation and Enterprise* 13, no. 1 (July 2025). <https://kiecon.org/wp-content/uploads/2025/07/Gavin-Suss-Role-of-IDF-in-Israel-Tech-Economic-Development.pdf>
- 151- Swartz, Dale, Ryan Brukardt, and Karl Hujsak. “Creating a Modernized Defense Technology Frontier.” *McKinsey & Company*. February 12, 2025. <https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/creating-a-modernized-defense-technology-frontier>
- 152- Swinhoe, Dan. “Microsoft Quietly Launches Israeli Azure Cloud Region.” *DatacenterDynamics*. October 31, 2023.

<https://www.datacenterdynamics.com/en/news/microsoft-quietly-launches-israeli-azure-cloud-region/>

T

- 153- The Economic Times. “How Israel Is Using ‘Lavender’ and ‘Daddy’ to Identify 37,000 Hamas Operatives”. April 9, 2024. 1:15 p.m. IST. <https://economictimes.indiatimes.com/news/defence/how-israel-is-using-lavender-and-daddy-to-identify-37000-hamas-operatives/articleshow/109155124.cms>
- 154- The National. “President Sheikh Mohamed Discusses Trade Relationship with China’s Xi Jinping in Beijing”. May 30, 2024. <https://www.thenationalnews.com/news/uae/2024/05/29/president-sheikh-mohamed-arrives-in-china-for-state-visit/>
- 155- "The UAE’s Technology Ambitions". Strategic Comments 30. no. 23 (International Institute for Strategic Studies, October 2024). <https://www.iiss.org/publications/strategic-comments/2024/10/the-uaes-technology-ambitions>
- 156- Toh, Amos, and Emile Ayoub. “The Military’s Use of AI, Explained.” Brennan Center for Justice. March 12, 2026. <https://www.brennancenter.org/our-work/research-reports/militarys-use-ai-explained>.
- 157- Tower Semiconductor. “Tower Semiconductor Teams with NVIDIA to Advance AI Infrastructure with 1.6T Data Center Optical Modules.” Press Release. February 5, 2026. <https://towersemi.com/2026/02/05/02052026/>
- 158- Trading Economics, “Israel – Industry, Value Added (% of GDP)”, <https://tradingeconomics.com/israel/industry-value-added-percent-of-gdp-wb-data.html>

U

- 159- “UAE Strategy for Artificial Intelligence”. Telecommunication and Digital Government Regulatory Authority. <https://u.ae/en/about-the-uae/strategies-initiatives->

[and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-strategy-for-artificial-intelligence.](#)

- 160- UECN. “The G42 Enigma: Inside the UAE’s AI Champion and its Global Partnerships”. September 27, 2025. <https://uecn.org/the-g42-enigma-inside-the-uaes-ai-champion-and-its-global-partnerships/>
- 161- UK Ministry of Defence and John Healey. “New Strategic Partnership to Unlock Billions and Boost Military AI and Innovation.” Press release, 18 September 2025. [https://www.gov.uk/government/news/new-strategic-partnership-to-unlock-billions-and-boost-military-ai-and-innovation.](https://www.gov.uk/government/news/new-strategic-partnership-to-unlock-billions-and-boost-military-ai-and-innovation)
- 162- UNESCO. “Minister of state for artificial intelligence”. <https://www.unesco.org/creativity/en/policy-monitoring-platform/minister-state-artificial-intelligence>
- 163- United Nations Development Programme. *Human Development Report 1994: New Dimensions of Human Security*. New York. 1994. <https://hdr.undp.org/content/human-development-report-1994>
- 164- United Nations. International Covenant on Civil and Political Rights. Adopted December 16, 1966. Office of the High Commissioner for Human Rights (OHCHR). <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- 165- United Nations General Assembly. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. adopted December 10, 1984. entered into force June 26, 1987. Resolution 39/46. <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-against-torture-and-other-cruel-inhuman-or-degrading>
- 166- United Nations General Assembly. International Convention on the Elimination of All Forms of Racial Discrimination. adopted December 21, 1965. entered into force January 4, 1969. Resolution 2106 (XX). <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial>

- 167- UN Human Rights Office, "UN Expert Warns Torture Has Become 'State Doctrine' in Israel, Making Prisons Instruments of Genocide and Torture," March 23, 2026, <https://www.ohchr.org/en/press-releases/2026/03/un-expert-warns-torture-has-become-state-doctrine-israel-making-prisons>
- 168- UNRWA. "Real Stories, Real Lives – What the Gaza Blockade Means." https://www.unrwa.org/what_the_Gaza_blockade_means
- 169- Ünver, H. Akin. *Artificial Intelligence (AI) and Human Rights: Using AI as a Weapon of Repression and Its Impact on Human Rights*. Brussels: European Parliament, Directorate-General for External Policies, 2024. PE 754.450. https://www.researchgate.net/profile/Hamid-Akin-Uenver/publication/381407889_Artificial_Intelligence_AI_and_Human_Rights_Using_AI_as_a_Weapon_of_Repression_and_Its_Impact_on_Human_Rights/links/666c033a85a4ee7261c1187d/Artificial-Intelligence-AI-and-Human-Rights-Using-AI-as-a-Weapon-of-Repression-and-Its-Impact-on-Human-Rights.pdf.
- 170- U.S. Department of Commerce, Bureau of Industry and Security. "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)". October 7, 2022. <https://www.bis.gov/press-release/commerce-implements-new-export-controls-advanced-computing-semiconductor-manufacturing-items-peoples>
- 171- U.S. Department of State. "2025 Investment Climate Statements: Israel". 2025. <https://www.state.gov/reports/2025-investment-climate-statements/israel>
- 172- US Department of War. Secretary of War. "Artificial Intelligence Strategy for the Department of War: Accelerating America's Military AI Dominance". Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, and Defense Agency and DOW Field Activity Directors, January 9, 2026. <https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF>

- 173- Valache, Carmen. "Israel's Unit 8200, a Conveyor Belt of High-Tech Startups". *Interesting Engineering*. August 17, 2020. <https://interestingengineering.com/innovation/israels-unit-8200-a-conveyor-belt-of-high-tech-startups>
- 174- Ventura, Luca. "Richest Countries in the World 2025". *Global Finance*. 3 September 2025. <https://gfmag.com/data/richest-countries-in-the-world/>
- 175- Vanian, Jonathan. "Meta signs nuclear energy deals to power Prometheus AI supercluster", CNBC, January 9, 2026, <https://www.cnbc.com/2026/01/09/meta-signs-nuclear-energy-deals-to-power-prometheus-ai-supercluster.html?msocid=0366bf639ea966eb1647a9759f1267a9>

W

- 176- WaferPro. "China's Dominance in the Global Silicon Supply". June 21, 2024. <https://waferpro.com/chinas-dominance-in-the-global-silicon-supply/>.
- 177- Wang, Selina. "Trump Orders US Government to Cut Ties with Anthropic; Hegseth Declares Supply Chain 'Risk'." *ABC News*. February 28, 2026. <https://abcnews.com/Politics/anthropic-latest-pentagon-contract-bar-ai-autonomous-weapons/story?id=130558898>
- 178- Wolfenstein, Konrad. "Why the US Cloud Act Is a Problem and Risk for Europe and the Rest of the World: A Law with Far Reaching Consequences". *Xpert.Digital*. April 16, 2025. <https://xpert.digital/en/us-cloud-act/>
- 179- Worldometers. "United Arab Emirates Oil". 2025. <https://www.worldometers.info/oil/united-arab-emirates-oil/>
- 180- World Population Review. "United Arab Emirates". <https://worldpopulationreview.com/countries/united-arab-emirates>
- 181- Wu, Feng-Shang, and Hong-Ji Huang. "Why Do Some Countries Innovate Better than Others? A New Perspective of Science, Technology, and Innovation Policy

Regimes and National Absorptive Capacity.” Sustainability 16, no. 7 (2024). 2840.
<https://doi.org/10.3390/su16072840>.

X

Y

- 182- Yesh Din. Data Sheet: Duration of Processing of Complaints Concerning Israeli Soldiers’ Offenses against Palestinians in the West Bank – 2016–2025 Data. December 30, 2025. <https://www.yesh-din.org/en/data-sheet-duration-of-processing-of-complaints-concerning-israeli-soldiers-offenses-en/>

Z