

LEBANON'S STRATEGIC POSITION IN THE AGE OF AI-DRIVEN DEFENSE AND CYBERSECURITY

Sarkis KARAGUEZIAN*

ORCID ID: 0009 - 0008 - 7575 - 329X

Declaration*

Abstract

The application and integration of artificial intelligence (AI) and cybersecurity technologies are rapidly advancing within Lebanon's defense and national security sectors. This research investigates how AI can enhance Lebanese military capabilities, with particular emphasis on cyber defense functions and related operational applications. It assesses current and prospective uses of AI in the Lebanese military context, analyzing their strategic, operational, and institutional impacts. The study further examines how AI-powered systems affect military effectiveness, resilience, and threat reduction, identifying capability gaps and operational challenges in deploying these technologies within resource-limited and politically complex settings. Special focus is given to Lebanon's evolving cyber threat environment, marked by rising exposure to cyberattacks, hybrid threats, and asymmetric security risks. Additionally, the research evaluates the strategic importance of implementing AI-driven solutions in the Lebanese defense sector, while carefully considering ethical issues, governance needs, and institutional preparedness.

Keywords: Lebanon, Non-State Actors, Artificial Intelligence (AI), Cybersecurity, Military Strategy, National Security, Cyberattacks, Intelligence Gathering, Geopolitics of the Middle East, Counterterrorism

Introduction

In this analysis, the strategic impact of artificial intelligence (AI) on the defense system of the state of Lebanon is assessed. As one of the nations positioned at the center of the Middle East, Lebanon faces a variety of defense-related challenges triggered by its complex geopolitical position. Situated at the crossroads of regional power struggles, the country contends with a fragile internal security architecture while simultaneously navigating external pressures from

* PhD is affiliated with Haigazian University, Beirut, Lebanon. He is a university lecturer and Senior Policy Advisor at the International Center for Geopolitical and Economic Research (ICGER).

* The author acknowledges the use of artificial intelligence (AI)-assisted tools during the preparation of this manuscript for purposes including idea organisation, improving manuscript structure, language refinement, and proofreading. All intellectual contributions, theoretical analysis, arguments, and conclusions are the sole responsibility of the author.



state and non-state actors (Norton, 2014; Traboulsi, 2007). Its weak political system is compounded by possible dangers posed by hostile entities from outside its borders, rendering traditional defense paradigms increasingly insufficient. Under such conditions, turning towards more advanced defense system innovations is warranted with the intention of securing the state's sovereignty and territorial integrity (Harris, 2014).

The contemporary global security landscape has witnessed a profound transformation driven by the rapid advancement of artificial intelligence technologies. AI has gained increasing significance within state defense systems, cybersecurity frameworks, and intelligence processes, offering unprecedented capabilities in threat detection, predictive analytics, and autonomous decision-making (Horowitz, 2018; Geist, 2016). For nations like Lebanon, which operate within resource-constrained environments yet face asymmetric and multidimensional threats, AI represents both a critical opportunity and a strategic imperative. The integration of intelligent systems into national defense architectures promises to enhance situational awareness, streamline command and control structures, and fortify cyber resilience against an expanding threat landscape. However, realizing these benefits requires navigating complex technical, institutional, and geopolitical hurdles that are particularly acute in the Lebanese context.

41

This analysis aims to investigate the potential beneficial effect artificial intelligence is bound to have on military capabilities, cybersecurity, and intelligence processes within Lebanon's defense system (World Economic Forum, 2019). To achieve this objective, the research employs a qualitative methodological approach designed to capture the multifaceted nature of AI integration in a complex operational environment. The study synthesizes existing scholarship through a comprehensive literature review to establish a robust background on Lebanon's technological infrastructure and defense posture. This foundational understanding is complemented by primary data collection through interviews with military officials, cybersecurity professionals, and AI specialists, whose firsthand perspectives reveal both the practical opportunities and the systemic challenges of deploying AI in Lebanon's defense sector.

Historical Context of Lebanon's Defense Strategy

The defense system of Lebanon has been shaped by a history dotted with civil rifts, foreign incursions, and inter-regional conflicts. The impact of such influences still prevails and continues to shape the current defense and cybersecurity environment for the Lebanese. It is



important to explain the influence of artificial intelligence on the defense and security environment for the Lebanese by exploring the history underpinning the defense system of this particular state.

The Lebanese Civil War (1975–1990): Sectarian Fragmentation and the Erosion of State Monopoly on Violence

The Lebanese Civil War (1975–1990) represents a critical turning point in contemporary Lebanese history, marked by deep-seated internal conflict fueled by sectarian differences and sustained international interference. Groups including Lebanese Christians and Muslims, as well as Palestinians, vied for state power, while Syria, Israel, and Iran were among the international actors who made a significant impact on the trajectory of the conflict (Khalaf, 2002; Traboulsi, 2007; U.S. Department of Defense, 2025). The war fundamentally fractured Lebanon's institutional framework, dispersing armed authority across militias and non-state actors and establishing a pattern of fragmented sovereignty that persists in the country's defense architecture today. This historical legacy of divided loyalties and weakened state institutions continues to complicate efforts to build a unified, technologically advanced national defense system capable of integrating AI-driven capabilities.

42

The Israel-Lebanon Conflict: Persistent Asymmetric Warfare and the Struggle for Sovereign Defense

The close geographical proximity between Israel and Lebanon has contributed to several clashes between the two nations; however, the most consequential modern conflict was the 2006 Lebanon War between Israel and Hezbollah. During this conflict, significant harm was inflicted on Lebanese military infrastructure and civilian assets alike, with over 1,100 Lebanese civilians and combatants killed and approximately one million people displaced (Britannica, 2024; Matthews, 2011). Despite the passage of nearly two decades, the threat posed by both Hezbollah's military posture and Israel's periodic military operations continues to undermine Lebanese sovereignty, while the chronic lack of development and modernization within the Lebanese Armed Forces leaves the state perpetually vulnerable (Harris, 2014; Norton, 2014).

This ongoing asymmetry wherein non-state actors possess more advanced military capabilities than the national army creates a uniquely challenging environment for AI integration, as defense modernization must navigate internal political sensitivities while



addressing external security gaps. The 2024 conflict between Israel and Hezbollah introduced a new dimension to this asymmetric relationship: the deployment of advanced AI-driven targeting systems by Israel. Israeli forces utilized an AI tool named “Habsora” (The Gospel) to maintain a comprehensive “target bank” cataloguing Hezbollah operatives, their locations, and routines, enabling rapid and precise strikes that decapitated much of Hezbollah’s leadership (Jerusalem Post, 2026; Arab Center Washington DC, 2025).

Regional Instability and the Syrian Civil War: Spillover Effects on Lebanese Security and Cyber Vulnerability

For Lebanon, the Syrian Civil War has intensified the complex threat environment within which its defense institutions must operate. The Syrian conflict has posed multidimensional threats to the Lebanese state, including a massive refugee crisis, cross-border militant activity, and the risk of direct military escalation. In this context, the Lebanese Army operates under conditions whereby non-state groups and jihadist militias represent as significant a threat as state-based adversaries (Salem, 2017; European Parliament, 2017). The conflict has further eroded the state’s capacity to maintain territorial control and has strained an already burdened security apparatus.

43

The Syrian civil war has equally impacted the cyber capacity and vulnerability of the Lebanese state. As the Syrian government is known to be engaged in cyber activities and information operations within the broader Middle East context, Lebanon is exposed to heightened risks of state-sponsored cyberattacks relative to other states in the region (CSS ETH Zurich, 2017). In this regard, the adoption of artificial intelligence by the Lebanese state can be viewed as a necessary preemptive measure to secure the Lebanese cyber environment and detect sophisticated intrusion attempts before they compromise critical national infrastructure.

Lebanon’s Security Landscape: Non-State Actors, Asymmetric Warfare, and Cyber Vulnerabilities

The Lebanese state is threatened by multiple non-state actors, including Palestinian factions, jihadist groups such as ISIS and Al-Qaeda, which operates as both a political party and an armed militia with capabilities exceeding those of the national army (Norton, 2014; U.S. Department of State, 2021). This fragmentation of armed authority has compelled the Lebanese Armed Forces (LAF) to adopt unconventional combat tactics, including guerrilla



and cyber warfare, while navigating a political environment where external patrons principally Iran for Hezbollah, and the United States and France for the LAF compete for influence (Harris, 2014; Salem, 2017).

Adding to these conventional security challenges is Lebanon's increased vulnerability to cyber threats. The state is susceptible to various cyber threats such as state-sponsored espionage activities and cyber terrorism, correlating with the growing reliance on cyberspace for state and military activities (CSS ETH Zurich, 2017; Singer & Brooking, 2018). Israeli and Syrian cyber activities have targeted Lebanese communication networks and military infrastructure during periods of high tension, while cyber-criminal gangs have increasingly targeted Lebanese banks and governmental entities (CSS ETH Zurich, 2017; CSS ETH Zurich, 2020). These vulnerabilities highlight the need for a proactive and comprehensive approach to cybersecurity that leverages artificial intelligence to bolster preparedness and response capabilities.

The Lebanese Armed Forces and Cybersecurity Infrastructure

The Lebanese Armed Forces (LAF) have faced persistent difficulties regarding resources and weaponry, yet have made significant advancements in force structure and operational capabilities, particularly in response to the Syrian Civil War and the 2006 Israel-Hezbollah War (Harris, 2014; Salem, 2017). France and the United States have been at the forefront of assisting Lebanese military strength, with the U.S. continuing to provide advanced military platforms, equipment, and training (U.S. Department of State, 2021; Lebanese Armed Forces, 2025). However, the LAF's ability to secure the state independently remains contested due to the significant role that non-state actors play, which maintains de facto military autonomy (Norton, 2014; The Public Source, 2026).

In the cyber domain, Lebanon has taken incremental steps toward institutionalizing cybersecurity governance. The establishment of the National Cyber Security Center in 2017 was followed by the adoption of a comprehensive National Cyber Security Strategy in November 2024, which proposes eight strategic pillars: defending against cyber threats; developing international cooperation; enhancing state ICT capacities; promoting cybersecurity education; strengthening industrial and technical capabilities; supporting Lebanese cybersecurity companies; fostering public-private collaboration; and reinforcing law enforcement and intelligence agency roles (National Cybersecurity Committee, 2024). The strategy mandates the creation of the National Cyber Security and Information System



Agency (NCSIA) as a centralized coordinating body. However, the Lebanese cyber defense system still faces significant challenges, including a lack of expert personnel, outdated infrastructure, and inadequate funding, creating a gap between strategic ambition and operational reality (UNESCWA, 2020; Factosecure, 2025).

AI Applications in Lebanon's Defense and Security Sector

Military Operations

The application of artificial intelligence within a military context offers several potential benefits for the Lebanese government. AI can be implemented in intelligence collection, autonomous surveillance, predictive analysis, and military decision support. AI-powered drones and robotic platforms may be employed by the Lebanese Armed Forces for surveillance and precision targeting, limiting collateral damage and enhancing operational efficiency (Horowitz, 2018; Boulanin & Verbruggen, 2017). Machine learning and image recognition can process vast quantities of satellite imagery and signals intelligence for real-time anomaly detection, providing vital information on activities and potential threats from non-state actors such as Palestinian groups and jihadists (Geist, 2016; Horowitz, 2018).

The 2024 Israel-Hezbollah conflict demonstrated the transformative potential of AI-augmented surveillance. Israel deployed high-altitude drones that orbited the border continuously, monitoring cell signals, tracking vehicles, and transmitting data to intelligence systems in real time, creating what analysts described as a “testing ground for remote territorial control” (Peoples World, 2025). For Lebanon, developing comparable capabilities scaled to its resources could provide early warning of cross-border threats without requiring massive troop deployments.

Cyber Defense

In the field of cybersecurity, artificial intelligence is poised to be a game-changer for the Lebanese state. AI-powered intrusion detection solutions can identify unusual behavior on government and military networks, while machine-learning algorithms can examine network traffic to detect malicious attacks such as Denial-of-Service (DoS) and phishing before they cause pervasive network disruptions (Palo Alto Networks, n.d.; Syracuse University, 2025). Natural language processing (NLP) technologies can monitor social media platforms and online forums to detect threat indicators, allowing anticipatory measures against cyber threats that may also cause physical harm (Singer & Brooking, 2018).



The application of AI-based cybersecurity solutions can help defend Lebanon's government, financial infrastructure, and military networks from advanced cyberattacks. In light of the region's tendency to fall victim to proxy cyberwars, especially those involving state-sponsored cyberattacks, the ability to identify and eliminate cyber threats in real time is critical for Lebanese national security (CSS ETH Zurich, 2020).

Intelligence Processes

AI-driven predictive analytics can transform Lebanon's approach to threat assessment by analyzing patterns from multiple data sources including satellite imagery, communications intercepts, social media monitoring, and historical conflict data to anticipate potential security incidents before they materialize (Singer & Brooking, 2018). Social network analysis using machine learning algorithms can identify the structure and key nodes of terrorist and criminal organizations operating within Lebanon, supporting targeted counterterrorism operations while minimizing collateral impact on civilian populations.

Ethical and Legal Considerations

Despite the apparent benefits of artificial intelligence in military and cyber defense scenarios, there is a vital need for the Lebanese state to examine the ethical and legal repercussions of deploying such technologies. The reliance on autonomous machines for strategic defense decision-making raises concerns regarding accountability and human control (Heyns, 2016; Sharkey, 2018). AI systems can perpetuate and amplify existing biases present in training data, potentially leading to discriminatory outcomes in security operations (Etzioni & Etzioni, 2017). Ensuring accountability for decisions made or informed by AI systems presents significant challenges, particularly when algorithmic reasoning is opaque even to system operators.

A clear ethical framework for the use of AI in military and cyber operations should be created and implemented by the Lebanese state, including transparency within decision-making processes and ensuring that human review is maintained as a core element within AI deployment (Floridi et al., 2018). Lebanon should bring its AI policy into alignment with international norms and principles on humanitarian law, ensuring that AI-based technologies are used responsibly, do not impact the rights of civilians, and do not increase the potential for conflict (ICRC, 2020). Active participation in international forums on AI regulation for military use, such as the UN Convention on Certain Conventional Weapons (CCW) Group of



Experts on Lethal Autonomous Weapons Systems, would further strengthen Lebanon's ethical posture (Heyns, 2016).

Recommendations for Lebanon's Future Defense Strategy

For greater benefit and risk reduction with the application of artificial intelligence, this research proposes the following recommendations tailored specifically to the Lebanese context:

1. Develop a Dedicated National AI Defense Strategy

While the National Cyber Security Strategy (2024) provides a foundation, Lebanon needs a dedicated strategy for AI integration in defense that coordinates efforts across military, intelligence, and civilian cybersecurity domains. This strategy should explicitly address how to enhance state capabilities without triggering destabilizing responses from non-state actors and should prioritize non-lethal applications (surveillance, cyber defense, predictive analytics) in the initial phase to build institutional confidence and capability.

2. Leverage Educational Assets for Human Capital Development

Rather than relying on expensive foreign consultants, Lebanon should mobilize its existing academic infrastructure AUB, LAU, CNRS-L, and the BDD ecosystem to train LAF personnel in AI fundamentals, data science, and cybersecurity. The Google AI grant to AUB demonstrates that such partnerships are feasible. A "train-the-trainer" model, where Lebanese academics train military officers who then train their subordinates, would maximize impact while minimizing cost and external dependency.

3. Direct International Assistance Toward AI-Enabled Priorities

The \$117 million in expanded U.S. security assistance announced in January 2025, and the approximately \$496 million in total FY2024 aid, should be strategically directed to include AI-enabled capabilities. Specifically, donor funds should support: (a) AI-driven border surveillance pilots along the Syrian frontier; (b) machine-learning-based cyber threat detection systems for critical infrastructure; and (c) predictive analytics tools for counterterrorism operations. Donors should condition assistance on transparent governance frameworks to prevent misuse for domestic repression.



4. Establish Ethical and Legal Safeguards Before Deployment

Lebanon must enact comprehensive data protection legislation and establish ethical guidelines for AI use in security applications before deploying systems operationally. These frameworks should mandate meaningful human control over lethal decisions, require algorithmic auditing for bias, and create independent oversight mechanisms. Lebanon should actively participate in the UN CCW Group of Experts on Lethal Autonomous Weapons Systems to align its policies with emerging international norms.

5. Build Domestic Cybersecurity Industry Through Public-Private Partnerships

The National Cyber Security Strategy's call for supporting domestic cybersecurity companies should be operationalized through government contracts, tax incentives, and research grants. Lebanese firms such as CME Cybersecurity, LIRIS, and others already possess baseline capabilities that could be scaled with modest investment. A domestic industry reduces dependency on foreign suppliers mitigating supply chain risks demonstrated by the 2024 pager attacks while retaining technical talent that would otherwise emigrate.

6. Address Infrastructure Barriers as a Security Priority

Electricity and internet connectivity are not merely economic development issues but fundamental enablers of AI defense capabilities. Lebanon should treat infrastructure rehabilitation as a national security priority, exploring innovative solutions such as solar-powered computing centers for military installations and satellite internet connectivity for rural border posts. International assistance programs should explicitly include infrastructure components, recognizing that advanced AI systems are useless without reliable power and data transmission.

Conclusion

The defense system of Lebanon is beset by a peculiar set of circumstances, ranging from the dynamic interplay between state and non-state entities to the escalating threat of cyberattacks and AI-enabled asymmetric warfare (Harris, 2014; Norton, 2014). The 2024 Israel-Hezbollah conflict demonstrated that AI is no longer a future prospect but an operational reality reshaping the regional security landscape. For Lebanon, artificial intelligence represents both an urgent necessity and a formidable challenge.



The question is not whether Lebanon can afford to integrate AI into its defense architecture, but whether it can afford not to, particularly when its adversaries are already weaponizing AI capabilities that may soon render conventional defenses obsolete. Lebanon possesses underappreciated assets for this transformation: a robust higher education sector with dedicated AI programs, a nascent private cybersecurity industry, and a newly adopted National Cyber Security Strategy that provides institutional foundation. However, realizing these benefits requires navigating severe economic constraints, infrastructural deficiencies, political fragmentation, and the unique complications posed by Hezbollah's parallel military capacity.

The path forward requires neither technological determinism nor institutional fatalism, but a pragmatic, phased approach that leverages Lebanon's existing assets, addresses its structural constraints, and maintains the ethical and legal standards befitting a state committed to international humanitarian law and human rights. With the proper policies and investments, the Lebanese state has the potential to increase national security and defense power within the context of a complex threat environment.

References

Arab Center Washington DC. (2025). The impact of Israeli cyber operations on Hezbollah. Retrieved from <https://arabcenterdc.org/resource/the-impact-of-israeli-cyber-operations-on-hezbollah> (Accessed Time: 18 February 2026)

Atlas of Urban Tech. (2022, April 7). Beirut Digital District. Retrieved from <https://atlasofurbantech.org/cases/lbn-beirut-bdd> (Accessed Time: 20 January 2026)

Boulanin, V., & Verbruggen, M. (2017). Mapping the development of autonomy in weapon systems. Stockholm International Peace Research Institute (SIPRI). Retrieved from <https://www.sipri.org/publications/2017/sipri-background-papers/mapping-development-autonomy-weapon-systems> (Accessed Time: 25 January 2026).

Britannica. (2024). 2006 Lebanon War. Encyclopaedia Britannica. Retrieved from <https://www.britannica.com/event/2006-Lebanon-War> (Accessed Time: 12 February 2026)

CSS ETH Zurich. (2017). Cyber activities in the Syrian conflict. Center for Security Studies. Retrieved from <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-05.pdf> (Accessed Time: 08 March 2026)



CSS ETH Zurich. (2020). Israel's national cybersecurity and cyberdefense posture. Center for Security Studies. Retrieved from <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf> (Accessed Time: 08 March 2026)

Elgar Online. (2026). Artificial intelligence in contemporary conflicts and the future of military law. In Research Handbook on Artificial Intelligence and International Law. Edward Elgar Publishing. Retrieved from <https://www.elgaronline.com/edcollchapoa/book/9781035353507/chapter9.xml> (Accessed Time: 15 June 2026)

Etzioni, A., & Etzioni, O. (2017). Incorporating ethics into artificial intelligence. *The Journal of Ethics*, 21(4), 403–418.

European Parliament. (2017). Syrian crisis: Impact on Lebanon. European Parliamentary Research Service. Retrieved from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599379/EPRS_BRI\(2017\)599379_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599379/EPRS_BRI(2017)599379_EN.pdf) (Accessed Time: 30 January 2026)

Factosecure. (2025, June 11). Top 10 cybersecurity companies in Lebanon. Retrieved from <https://factosecure.com/top-10-cybersecurity-companies-in-lebanon/> (Accessed Time: 20 June 2026)

Floridi, L., Cowls, J., Taddeo, M., & van Wynsberghe, A. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28, 689–707.

Geist, E. (2016). It's already too late to stop the AI arms race. *Bulletin of the Atomic Scientists*, 72(5), 318–321.

Harris, W. (2014). *The Levant: A Land of Conflict*. Routledge.

Heyns, C. (2016). Autonomous weapons in armed conflict and human rights law. UN Human Rights Council, A/HRC/32/L.36.

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, 1(3), 36–57.

ICRC. (2020). *Artificial intelligence and autonomous weapons: Ethical and legal challenges*. International Committee of the Red Cross.



Jerusalem Post. (2026, May 10). Inside Israel's AI targeting system: How data from a phone becomes a death sentence. Retrieved from <https://www.jpost.com/defense-and-tech/article-895697> (Accessed: 18 May 2026)

Khalaf, S. (2002). *Civil and uncivil violence in Lebanon: A history of the internationalization of communal conflict*. Columbia University Press: New York.

Lebanese Armed Forces. (2025). Army capabilities development plan (CDP) 2023–2027. Retrieved from <https://www.lebarmy.gov.lb/en/content/army-capabilities-development> (Accessed: 20 April 2026)

Matthews, M. M. (2011). *We were caught unprepared: The 2006 Hezbollah-Israeli war*. Long War Series, Occasion Paper 26. U.S. Army Combined Arms Center.

MDPI. (2026, March 6). Governing artificial intelligence for sustainable territorial development in fragile contexts: Insights from North Lebanon. *Administrative Sciences*, 16(3), 130.

National Cybersecurity Committee. (2024). Lebanon national cyber security strategy. Retrieved from <https://dig.watch/resource/lebanon-national-cyber-security-strategy> (Accessed Time: 22 January 2026)

Norton, A. R. (2014). *Hezbollah: A short history* (3rd ed.). Princeton University Press.

Palo Alto Networks. (n.d.). What is the role of AI in threat detection? Cyberpedia. Retrieved from <https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection> (Accessed Time: 05 April 2026)

Peoples World. (2025, November 12). Israel turns Lebanon into testing ground for high-tech 'remote occupation' tools. Retrieved from <https://peoplesworld.org/article/israel-turns-lebanon-into-testing-ground-for-high-tech-remote-occupation-tools/> (Accessed Time: 02 July 2026)

Salem, P. (2017). The Syrian conflict and its impact on Lebanon. Carnegie Middle East Center. Retrieved from <https://carnegie-mec.org/2017/04/06/syrian-conflict-and-its-impact-on-lebanon-pub-68617> (Accessed Time: 08 February 2026)

Sharkey, N. (2018). *Meaningful human control and autonomous weapons*. Working paper prepared for the CCW Group of Experts Meeting, Geneva.



Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.

Syracuse University. (2025). AI in cybersecurity: How AI is changing threat defense. School of Information Studies. Retrieved from <https://ischool.syracuse.edu/ai-in-cybersecurity/> (Accessed Time: 22 June 2026)

The Public Source. (2026). Sovereignty without defense: The army, the state, and Hezbollah's weapons. Retrieved from <https://thepublicsource.org/lebanese-army-hezbollah-sovereignty> (Accessed Time: 08 July 2026)

Traboulsi, F. (2007). *A history of modern Lebanon*. Pluto Press.

U.S. Department of Defense. (2025, April 7). Lebanese Civil War 1975–90. Defense Technical Information Center. Retrieved from https://media.defense.gov/2025/Apr/07/2003683785/-1/1/0/20250407_LEBANESECIVILWAR_1975-90_FINAL.PDF (Accessed Time: 18 April 2026)

U.S. Department of State. (2021). Country Reports on Terrorism 2020: Lebanon. Retrieved from <https://2021-2025.state.gov/reports/country-reports-on-terrorism-2020/lebanon/> (Accessed Time: 28 January 2026)

UNESCWA. (2020). Advisory report on the development of an artificial intelligence strategy for Lebanon. United Nations Economic and Social Commission for Western Asia. Retrieved from <https://www.unescwa.org/sites/default/files/event/materials/advisory-report-development-artificial-intelligence-strategy-lebanon-en.pdf> (Accessed Time: 14 February 2026)

World Economic Forum. (2019). Artificial intelligence in the Middle East. Retrieved from <https://www.weforum.org/reports/artificial-intelligence-in-the-middle-east/> (Accessed Time: 12 January 2026)

52

